

# 11

# Cybercrime: Illustrations, Examples and Mini-Cases

## Learning Objectives

After completing this chapter, you will able to:

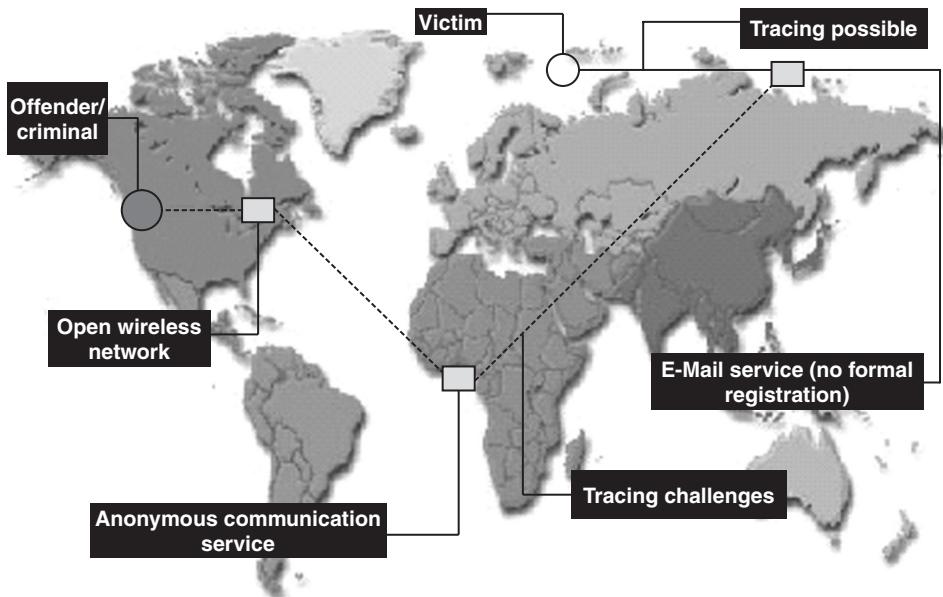
- Relate the examples, illustrations and mini-cases provided here to the cyber-crime categories mentioned in Chapter 1 and to the technical concepts explained in Chapters 2–5.
- Appreciate the interplay of crime and legal perspectives provided in Chapter 6, and relate them to organizational implications discussed in Chapter 9 and to psychological and political dimensions of cybercrimes explained in Chapter 10.
- Learn the practical scenarios of how criminals/fraudsters use methods, tools and techniques to commit cybercrimes and will be able to relate it to concepts learned in Chapter 4.
- Understand how real life instances of cyber-crimes can impact individuals and organizations if due care is not taken.
- Get overview of threats in cybersecurity with the crimes that are committed in the cyberspace.
- Understand how “forensics” discussed in Chapters 7 and 8 is applied in real life.
- Relate to organizational implications of cybersecurity discussed in Chapter 9.

### 11.1 Introduction

Through Chapters 1–9, readers are exposed to various categories of cybercrimes, the tools and techniques used by cybercriminals as well as the forensics and legal aspects involved. We learned about the psychological and ethical dimensions and organizational implications in terms of cybersecurity (Chapter 10).

In Section 1.5 of Chapter 1, we presented classifications of cybercrime and explained the crimes under each category. Chapters 2–5 provide detailed discussion on cybercrimes – cyberstalking and harassment (Chapter 2); Vishing and Smishing (Chapter 3); and Phishing and Spear Phishing (Chapter 5). For the illustrations/case studies on digital forensics investigations, the background and reference chapters are Chapters 8 and 9. *For the reasons of confidentiality and privacy, real names (individuals and/or organizations) are masked in some of the illustrations. Though the names are masked, the situations are real. If the hypothetical names match with actual names of any living or dead person, it is purely a coincidence. A number of cases/illustrations are based on the information released in the public domain; those URLs are mentioned. Neither authors nor the publisher is responsible for false/inaccurate information posted on those public weblinks.*

Cybercrime knows no geographical boundaries! Figure 11.1 illustrates this point effectively. Criminals, the means for the crimes and the impacted victims can be anywhere on the globe! In most cases, however,



**Figure 11.1** | Cybercrimes are boundary less!

they also get caught, as illustrations in this chapter show. Students of a legal course curriculum, from the standpoint of enhancing their knowledge about applicability of prevailing laws in their regions, may like to use the mini-cases, examples and illustrations for discussing which laws and which sections in those laws would be applicable.

Overall, the objective of this chapter is to help readers appreciate the seriousness and implications of computer crime scenarios presented here. The mini-cases, illustrations and examples presented here are cybercrime incidents that have taken place in India as well as other countries.

This chapter is divided into six sections:

1. Section 11.2: Real-Life Examples
2. Section 11.3: Mini-Cases
3. Section 11.4: Illustrations of Financial Crimes in Cyber Domain
4. Section 11.5: Digital Signature-Related Crime Scenarios
5. Section 11.6: Digital Forensics Case Illustrations
6. Section 11.7: Online Scams

At the beginning of each section, there is a table with list of examples/illustrations/case studies addressed in the section. The chapters, in which the underlying concepts are discussed, are mentioned in those tables. This will help you refer back to those chapters. There are no summary and review questions for this chapter.

## 11.2 Real-Life Examples

This section contains real-life examples of E-Mail Spoofing, release of viruses/worms, cyberstalking, hacking, computer intrusion and computer frauds, website attacks, cybersquatting and IPR crimes. Table 11.1 lists the examples provided in this section.

**Table 11.1** | List of examples in Section 11.2

<i>Example No.</i>	<i>Title</i>	<i>Topic</i>	<i>Chapter Cross-Reference</i>
1	Official Website of Maharashtra Government Hacked	Website hacking	Chapters 1 and 10
2	E-Mail Spoofing Instances	E-Mail Spoofing	Chapters 1, 3 and 4
3	E-Mail Bombing involving a Foreigner	E-Mail malpractices	Chapter 1
4	I Love You Melissa – Come Meet Me on the Internet	Virus and worms	Chapters 1–4
5	The “Piranhas” Tragedy with Children	Misleading information on websites	—
6	Doodle me Diddle!	Data diddling	Chapter 1
7	Ring-Ring Telephone Ring: Chatting Sessions Turn Dangerous	Cyberstalking	Chapters 1 and 2
8	Young Lady’s Privacy Impacted	Trojan	Chapters 2–4
9	Job Racket Exposed by Mumbai City Cybercrime Cell	Smishing	Chapter 3
10	Indian Banks Lose Millions of Rupees	Internet fraud	Chapter 1
11	Infinity E-Search BPO Case	Sale of personal information	Chapter 6
12	Charged with Computer Intrusion	Computer network intrusion	Chapter 1
13	Small Shavings for Big Gains!	Computer fraud	Chapters 1–5
14	Man Goes Behind Bars for Computer Fraud Offense	Computer fraud	Chapters 1 and 9
15	“Justice” vs. “Justice”: Software Developer Arrested for Launching Website Attacks	DoS (Denial-of-service attack)	Chapters 1 and 4
16	CAN-SPAM Act Violation through E-Mail Stock Fraud	SPAM, Wire fraud	Chapters 1, 5 and 6
17	Business Liability through Misuse of Organization’s Information Processing Assets	IPF misuse	—
18	Parliament Attack	Computer forensics	Chapter 7
19	Game Source Code Stolen!	IPR theft (source code theft), insider attacks	Chapters 1 and 9
20	The Petrol Pump Fraud	Computer hardware fraud	Chapter 1
21	Xiao Chung’s Story – Life of a Hacker	Hacking and psychology of hackers, zero-day attacks	Chapters 1, 9 and 10
22	Killers take Tips from “26/11 Attack” to Use VOIP	Cyberterrorism using VOIP, E-Mail forensics	Chapters 1 and 7
23	Robertson Brothers Caught for Selling Pirated Software	IPR theft, software piracy	Chapters 1 and 9
24	BSA Uncovers Software IPR Breaches	IPR theft	Chapters 1 and 9
25	Pune City Police Bust Nigerian Racket	Scam	Chapters 1 and 9

### 11.2.1 Example 1: Official Website of Maharashtra Government Hacked

Website hacking was addressed in Chapter 1 (Box 1.4, Figs. 1.6, 1.9 and 1.10). This is an incidence reported in September 2007. The impacted website was <http://www.maharashtragovernment.in>. A few days after the Chief Minister of the state inaugurated the new, citizen-friendly service-based web portal of the Brihanmumbai Municipal Corporation, the Maharashtra government's official website was hacked which lead to the shutting down of [www.maharashtra.gov](http://www.maharashtra.gov). The state officials, however, said that there was no data lost and that there was no serious damage to the website. State Officials further stated that the website gets updated daily with information on various government regulations and decisions, and supports links to all government departments. However, IT experts had to restore the official website of the government of Maharashtra, having succumbed to the attack by the hacker.

As per reports, the site was attacked early in the morning by a person or a group proclaimed as "cool-hacker." The hacker left an imprint of a hand on the hacked website (see Fig. 11.2). The state's information and technology department came to know about the incident next day morning. They immediately blocked all access to the website. The IT department has lodged an FIR (First Information Report) with the police in an attempt to trace the culprit.

Joint commissioner of police, in his official remark, stated that the state's IT officials lodged a formal complaint with the cybercrime branch police following this incidence. He expressed confidence that the hackers would be tracked down. The Commissioner also mentioned that the hacker had posted some Arabic content on the site. According to sources, hackers were suspected to be from Washington. IT experts gave to understand that the hackers had identified themselves as "Hackers Cool Al-Jazeera" and claimed they were based in Saudi Arabia. Officials further added that this might be a red herring to throw



**Figure 11.2** | Maharashtra state website hacked.  
(source: <http://sunnytalkstech.blogspot.com/2007/09/mpsc-website-defaced.html> 22 July 2010).

investigators off their trail. For those who are not familiar with the term “red herring,” it refers to the tactic of diverting attention away from an item of significance.

The State Government website contained detailed information about government departments, circulars, reports and several other topics. IT experts, who were assigned to work on restoration of the website, told Arab News that they feared that the hackers may have destroyed all of the website’s contents. The worrisome part was that according to a senior official from the State Government’s IT department, the official website has been affected by viruses on several occasions in the past, but was never hacked. The official added that the website had no firewall. However, state officials denied there being any data loss or any serious damage to the website. The officials said that the hacker could only manage to damage the homepage.

Point to note here is that the website was hacked for the second time in the past two weeks, the fourth time since July 2007. The previous attack took place on 5 September 2007. This incidence of repeated attack on the website underscores the need for security measures being in place (intrusion detection system – IDS, intrusion prevention system – IPS and firewalls).

### **11.2.2 Example 2: E-Mail Spoofing Instances**

E-Mail bombing was mentioned in Chapter 1 (Section 1.5.16) and explained further in Chapter 4 (Table 4.11). This is an example of that. An American teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misleading information was spread by sending spoofed E-Mails 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 emerged, the values of the shares could not be restored to the earlier levels. This resulted in thousands of investors losing a lot of money. This can be considered as a cybercrime against an organization because the impacted organization was the one about whom false information was spread.

There is another example of E-Mail Spoofing incident in India. A branch of the Global Trust Bank experienced a customer run-down on the bank owing to a certain rumour spread about the bank not doing well financially. Under panic, many customers decided to withdraw all their money and close their accounts. It was revealed later that someone had sent out spoofed E-Mails to many of the bank’s customers announcing that the bank was in a very bad shape financially and could close operations any time. In the next few days, unfortunately, this information turned out to be true. So, can we say that this instance of E-Mail Spoofing saved many customers?

Another shocking example of the E-Mail Spoofing involves a former executive from a well-known company in the state of Gujarat. The executive faked himself to be a lady by adopting a false name. He then created a fake E-Mail ID. Using that ID, the executive contacted a businessman based in the Middle East. The executive posing as a woman then went into a long cybercourting relationship with the Middle East businessman. During this “cyberdating,” the executive used to send many “emotional blackmailing” messages to the businessman. One such message threatened the businessman that if he ended this relationship, “she” (i.e., the executive posing as a woman) would end her life! What is worse, the executive gave another woman’s E-Mail ID to the businessman. This too was a non-existent address. When the Middle East businessman sent a mail at that ID, he was shocked to learn that the executive (who presented himself as a woman) had died and that now the police was searching him as the suspect in that death case! Using this trap and trick the executive exhorted from the businessman several hundred thousands of Indian Rupees threatening that the businessman would get exposed if he did not part with that money. The executive also sent E-Mails to him from different E-Mail IDs making the poor businessman believe that they were mails from high court and police officials. All this was done to extract more money from the gullible businessman. Finally, businessman flew to India to lodge a case with the Police. Internet users indeed enjoy “anonymity” and can get away with many things – recall Fig. 1.5 in Chapter 1.

### 11.2.3 Example 3: E-Mail Bombing Involving a Foreigner

E-Mail bombing is explained in Chapter 1; this example brings out an instance based on that. A foreigner had been residing in Shimla, India for almost 30 years. He wanted to avail a scheme that was introduced by the Shimla Housing Board to buy land at lower rates. His application, however, was rejected on the grounds that the scheme was available only to Indian citizens. Feeling furious, the foreigner decided to take revenge. He transmitted thousands of mails to the Simla Housing Board. He did not stop there. He kept on sending E-Mails till their servers crashed. An interesting question is which law of the land would have been used for filing a case against this non-Indian person.

### 11.2.4 Example 4: I Love You Melissa – Come Meet Me on the Internet

This example involved the VBS\_LOVELETTER virus - also known as the Love Bug or the ILOVEYOU virus. It is said to be written by a Filipino undergraduate. In May 2000, it was proven that this virus is deadlier than the Melissa virus and it became the world's most prevalent virus. It impacted one in every five personal computers in the world. When the virus was brought under control, the true magnitude of the losses was unbelievable. The attack from this virus caused losses to the tune of almost US\$ 10 billion.

It is interesting to see how the virus works. The original VBS\_LOVELETTER thrived on the addresses in Microsoft Outlook. It utilized that address book 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-FORYOU.TXT.vbs." Even with such dubious sounding subject line, even those who had some knowledge of viruses did not notice the tiny .vbs extension. People believed the file to be a text file and this mail also fooled people who are wary of opening E-Mail attachments. The message in the E-Mail read as follows: "Kindly check the attached LOVELETTER coming from me."

Since the initial outbreak, over 30 variants of the virus have been developed, many of them following the original by just a few weeks. The Love Bug propagates itself using the Internet Relay Chat (IRC). It E-Mails itself to users in the same channel as the infected user. However, unlike the Melissa virus this virus does have a destructive effect. The Melissa virus, once installed, merely inserts some text into the affected documents at a particular instant during the day. On the other hand, VBS\_LOVELETTER first selects certain files and then inserts its own code in lieu of the original data contained in the file. Thus, it succeeds in creating ever-increasing versions of itself, that is, self-propagation mode. The world's most famous worm probably was the *Internet worm* let loose on the Internet sometime in 1988 by Robert Morris. At that time, the Internet was in its early formative and developing years. The *Internet worm* affected thousands of computers and almost brought Internet development to a complete halt. It took a team of experts several days to get rid of the Internet worm and in the meantime many of the computers had to be disconnected from the network.

### 11.2.5 Example 5: The “Piranhas” Tragedy with Children

Web Jacking is explained in Section 1.5.8 of Chapter 1. This incident was reported in the US. There was a hobby website for children. The owner of the site received an E-Mail informing her that a group of hackers had gained control over her website. They demanded a ransom of one million dollars from her. The owner was a school teacher. She did not pay due attention to that (threatening) mail because she did not think it was serious. She thought it was just a scare tactic and so she simply ignored the E-Mail. After about three days, she started getting several telephone calls from almost all over the country and then she came to know that the hackers had really web jacked her website. The hackers had altered a portion of the website which was entitled "How to have fun with goldfish." They had replaced the word "goldfish" with the word "piranhas." Piranhas are tiny but extremely dangerous flesh-eating fish! It was sad because, the fatal result of

this apparently minor sounding “find-and-replace” cyberprank was terrible. Many children who visited the popular website believed what the contents of the website suggested. These unfortunate children did not realize what would be in their fate. They followed the instructions to try playing with piranhas, which they bought from pet shops and were very seriously injured!

### **11.2.6 Example 6: Doodle me Diddle!**

“Data Diddling” technique was addressed in Chapter 1; this is a real-life example of that. Indian Electricity Boards suffered as victims of data diddling. Such programs got inserted when private parties were computerizing their systems. The NDMC Electricity Billing Fraud Case in 1996 is a typical example. The computer network was used for preparing receipts and for keeping the accounts of electricity bills by the NDMC, Delhi. Money collection, computerized accounting, record maintenance and remittance in the bank were outsourced to a private contractor who was a computer professional. He misappropriated vast amount of money by manipulating data files to show less receipt and bank remittance. As we know, this kind of attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

### **11.2.7 Example 7: Ring-Ring Telephone Ring – Chatting Sessions Turn Dangerous**

Cyberstalking was mentioned in Chapter 1 and explained in Chapter 2 (Section 2.4). Here is a real-life example of that crime which was registered with Delhi police. “Stalking” is defined as “pursuing stealthily.” As we learned, “cyberstalking” means following a person’s activities, that is, a person’s navigation across the Internet by posting messages (sometimes even threatening messages) on the bulletin boards that are visited by the victims, entering the chat rooms frequented by the victim, constantly bombarding the victim with E-Mails, etc. Richa Sharma was the first lady to register a cyberstalking case. Her husband’s friend provided her a telephone number in the general chat room. Some websites do provide general chatting facility (e.g., websites like MIRC and ICQ) where a person can easily chat without revealing his/her true identity. The friend of Ms. Sharma’s husband also encouraged chatters to speak in profane language to Ms. Sharma. As a result, Ms. Sharma received more than 30 calls in 3 days and many chatters contacted her. Almost all of the calls were made to her at odd hours from all over India and a few of the calls came in from outside India too. This created havoc in the personal life of Ms. Sharma and caused her much mental stress. She got fed-up with these calls and chat drama and complained to the police against a person who she felt was using her identity to chat over the Internet at the website [www.mirc.com](http://www.mirc.com). In her complaint, Ms. Sharma mentioned that the person was chatting on the Net using her ID and also complained about the obscene language used by that person while chatting with her. Ms. Sharma, further complained that the same person was deliberately giving her telephone number to other chatters, asking them to call her at odd hours.

### **11.2.8 Example 8: Young Lady’s Privacy Impacted**

We have explained about Trojan, viruses and other malware in Chapters 2–4. We should be careful, else untoward things can happen as illustrated by this example. A young magazine journalist in Mumbai was working on an article about online relationships. The article was about how people can easily find friendship and even love companions on the Internet. During the tenure of her research work, she happened to make a lot of online friends. One of these “friends” (ill-minded, unfortunately for the young lady) managed to infect her computer with a Trojan. The young journalist lady lived in a small, one-bedroom apartment and her computer

was located in a corner of her bedroom. She had the habit of never powering off her computer. 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 “private” pictures were posted on pornographic sites around the world! Her fiancé broke the engagement and the young lady was thrown into suicidal depression.

### **11.2.9 Example 9: Job Racket Exposed by Mumbai City Cybercrime Cell**

Smishing is explained in Section 3.8.5 in Chapter 3. This example illustrates how cybercriminals use Smishing to cheat people. This case happened in the year 2009. Himesh Kapadia, aged 26 years, received an SMS offering him a job in Marriot Hotel. Himesh, in response, eagerly mailed his resume. He also deposited over ₹ 1.7 lakhs (₹ 1,70,000) as per the instruction of a person who claimed to be a London diplomat. Himesh grew suspicious when he was asked for additional money and finally approached the cybercrime cells of the Mumbai Police. The investigations resulted in the arrest of a couple and five Nigerians allegedly involved in cheating people by promising them housekeeping jobs in Marriot Hotel, London. While the Nigerians, posing as London diplomats, would send SMSs and E-Mails offering jobs in the hotel, the couple operated the bank accounts.

As Himesh recalls, in September 2009, he began exchanging mails with James Richard who claimed to be a London diplomat. He had asked Himesh to pay differing sums of money. Even after paying over ₹ 1.7 lakhs (₹ 1,70,000) he continued to exhort more money from Himesh. The police directed the bank authorities to block the account holder's ATM facilities. In last week of November 2009, the bank informed the police that a couple approached the bank to withdraw money from the account. Mumbai Police arrested the couple and later the Nigerians who came looking for them to collect the money.

### **11.2.10 Example 10: Indian Banks Lose Millions of Rupees**

Numerous types of cybercrimes were mentioned in Chapter 1; frauds using the Internet are some of them. This is a real-life example showing the techniques used by cybercriminals. Banks across the country lost ₹ 6.57 crore (₹ 6,57,00,000) to Internet frauds in 233 incidents of cybercrime, with Tamil Nadu topping the list in last fiscal year. ₹ 2.09 crore (₹ 2,09,00,000) has been lost by various banks in the Indian state of Tamil Nadu in seven cases reported between April and December 2008. The lending institutions in Maharashtra had reported the highest number of incidents, 23 in all. They lost ₹ 55.54 lakhs (₹ 55,54,000) to online fraudulent practices. This was revealed by the erstwhile Minister of State for Home told the Lok Sabha in February 2009.

The banks in other Indian states – Andhra Pradesh, Rajasthan and West Bengal – lost ₹ 89.93 lakhs (₹ 89,93,000), ₹ 64.29 lakhs (₹ 64,29,000) and ₹ 35.72 lakhs (₹ 35,72,000), respectively, while Kerala and Delhi lost ₹ 17.60 (₹ 17,60,000) and ₹ 10.90 lakhs (₹ 10,90,000), respectively, owing to cyberfrauds. A total of 11 cases of Internet frauds were reported from Andhra Pradesh, 8 from Delhi, 7 from Tamil Nadu, 6 from Karnataka and 5 from West Bengal during the said period. Surprisingly, banks in Bihar, Goa and Jharkhand did not lose a single penny to such activities and no case was reported from any of these states.

The Minister presented a state-wise list of number of incidents of Internet frauds that includes cases of fraudulent withdrawal of money from banks through Internet/online banking, as reported by the banks to the Reserve Bank of India. According to a data updated till 2007, out of the total 355 people arrested across the country, a maximum 156 people were arrested in Madhya Pradesh in connection with cheating-related cases under IT Act – Fraud digital signature (Section 64) and Breach of Confidentiality/Privacy (Section 72) – and IPC Crime (Forgery and Criminal Breach of Trust/Fraud). The highest numbers of cases, 153, were also registered in Madhya Pradesh for forgery and Criminal Breach of Trust/Fraud out

of the total of 302 cases in the said period. Similarly, a total of 41 incidents – 38 under IPC crime and 3 under IT Act – were reported in Chhattisgarh for cyberfrauds and 75 persons – 72 under IPC crime and 3 under IT Act – were arrested. A total of 59 people were also arrested in Andhra Pradesh, 36 in Punjab, 16 in Andaman and Nicobar Island and 4 in Delhi in connection with cheating-related incidents in 2007. The amount lost to cyberfrauds during April 2007 and March 2008 were ₹ 5.58 crore (₹ 5,58,00,000) and 374 people were arrested in this connection.

### **11.2.11 Example 11: Infinity E-Search BPO Case**

This case brings to the fore the emerging threat arising from “sale of personal information.” We learn here that the definition of “sensitive personal information” is very important for organizations to be clear on what they wish to protect from theft. This is especially important for the BPO (business process outsourcing) organizations to whom the clients entrust their confidential data.

A fraud discovered at a Gurgaon-based BPO created an embarrassing situation for Infinity E-Search, the company in which Mr. Kapoor was employed. A British newspaper reported that one of its reporters had covertly purchased personal information of 1,000 British customers from an Indian call-center employee. However, Mr. Kapoor, the employee of Infinity E-Search (a New Delhi-based web designing company) was reportedly involved in the case, denied any wrong-doing. The company also said that it had nothing to do with the incident.

It so happened in this case that the journalist used an agent, offered a job, requested for a presentation on a CD and later claimed that the CD contained some confidential data. The fact that the CD contained such data was itself not substantiated by the journalist. In this kind of a situation we can only say that the journalist used “bribery” to induce an “out of normal behavior” of an employee. This is not observation of a fact but creating a factual incident by intervention.



This example breaks the misconception that BPOs in India are not covered under the Information Technology Act and Amendments thereof.

BPOs in India, irrespective whether captive/independent/subsidiary, irrespective whether inbound/outbound, are covered under the Indian IT Act. Indian BPO organizations must understand this: As per Indian IT Act, every business process outsourcing (BPO) organization is an “INTERMEDIARY” – Section 1 (2w) of the Act defines “Intermediary.” Indian BPOs must take cognizance of Sections 43A (*Compensation for failure to protect data*), 67C (*Preservation and retention of information by intermediaries*), 69B (*Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security*), 70B (*Indian Computer Emergency Response Team to serve as national agency for incident response*), 72A (*Punishment for disclosure of information in breach of lawful contract*), 79 (*Exemption from liability of intermediary in certain cases*) and 85 (*Offences by companies*) of the Indian IT Act.



BPOs with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record ... can be classified as “intermediaries”. This is according to Section 2(1)(w) of the Indian IT Act.

### 11.2.12 Example 12: Charged for Computer Intrusion

Computer network intrusion was explained in Chapter 1 (Section 1.5.18); this example is related to that. The story of this incident was released in 4 November 2009. Scott R. Burgess, aged 45, Jasper, Indiana, and Walter D. Puckett, aged 39, Williamstown, Kentucky, were indicted for computer intrusion. This was announced by Timothy M. Morrison, US Attorney, Southern District of Indiana, after an inquiry by the Federal Bureau of Investigation (FBI) and the Indiana State Police.

It is alleged that Burgess and Puckett accessed the Stens Corporation computer systems, based in Jasper, Indiana, from various places on approximately 12 different occasions without authorization. It was further alleged that the computer intrusions were performed for the purpose of gaining commercial and personal financial benefits. Furthermore, it was alleged that Burgess and Puckett were working for a business competitor of Stens at the time of the intrusions.

A maximum of 5 years imprisonment with \$250,000 fine is what Burgess and Puckett had to face. An initial hearing was scheduled before a US Magistrate Judge. However, an indictment was only a charge and is not an evidence of guilt. A defendant was presumed innocent and was entitled to a fair trial at which the government must prove guilt beyond a reasonable doubt.

### 11.2.13 Example 13: Small “Shavings” for Big Gains!

This incident, involving a Salami attack-like technique, was published on 17 September 2009. Michael Largent, aged 22, resident of Plumas Lake area, was sentenced to 15 months in prison and compensation of over \$200,000. This was the punishment given by the US District Judge Morrison C. England Jr. for fraud and related activity in connection with computers. After release from prison, Largent also had to face 3 years of strict restrictions due to illegal use of computers and the Internet. This case was jointly investigated by US Secret Service and the FBI. The US Attorney's Office for the Northern District of California, San Jose Division, also assisted with this case.

The case was prosecuted during the period November 2007 through May 2008. The prosecution was done by the Assistant US Attorney Matthew D. Segal, who worked as prosecutor in the office's Computer Hacking and Intellectual Property (CHIP) unit. According to Attorney Mathew, the accused Michael Largent developed a computer program allowing him to defraud a few companies such as "E-Trade," "Charles Schwab & Co." and Google by opening or attempting to open more than 58,000 brokerage accounts. He did this to steal the "micro-deposits." Michael knew that a financial institution make a micro-deposit when an account is opened to test the functionality of an account. The amounts deposited in this case were in the range \$0.01 to \$2.00.

To cover his identity, Michael Largent used false names, addresses, driver's license numbers and social security numbers, including the names of known cartoon and comic book characters to open the accounts. When the deposits took place, he would divert the funds into his own bank accounts or onto prepaid debit cards, without the authorization or knowledge of his victims. As a result, Michael Largent fraudulently obtained or attempted to obtain tens of thousands of dollars which he used for personal expenses.

Two organizations, namely, E\*TRADE (E-Trade Financial Corporation) and Charles Schwab & Co. Inc., in parallel notified the law enforcement agency when they detected the fraud. Assistant US Attorney Robin R. Taylor, also of the CHIP unit, brought the criminal complaint and the indictment in this case in May 2008 and Segal took over in January 2009. In sentencing, Judge England observed that Michael Largent's scheme took some sophistication, and wondered why he had not used his skills and talents in a lawful way.

### 11.2.14 Example 14: Man Goes Behind Bars for Computer Fraud Offense

Here is another example similar to the previous one (Example 13). This example shows the hazards of not monitoring remote access permissions and the consequences of perhaps too much faith placed in the “insiders” with a naive belief that the “insiders” would never bring harm to their organizations (remember the discussion in Chapter 9). The ill use of administrator account and password also comes to the fore. There are tremendous learning implications for organizational information security practices. Noteworthy is the nature of punishment given to the guilty thereby creating an opportunity for remorse and also to morally guide others to avoid his wrong-doing. Read on for further details on this case.

Jeffrey H. Sloman, US Acting Attorney for the Southern District of Florida, and Jonathan I. Solomon, Special Agent in Charge (from FBI, Miami Field Office) announced that defendant, Lesmany Nunez, on 14 July 2009, was sentenced by Chief US District Judge Federico A. Moreno to 12 months and 1 day imprisonment after pleading guilty to computer fraud, in *violation of Title 18, United States Code, Section 1030(a)(5)(A)(ii)*. Upon his release from prison, Nunez was ordered to serve 3 years of supervised release, with a special condition that he performs 100 hours of *community service* by lecturing young people on the implications of hacking into other people’s computers and networks. Nunez was also ordered to pay \$31,560 in restitution.

As per the facts revealed during in-court statements, Nunez, aged 30, was a former computer support technician at Quantum Technology Partners (QTP), located in Miami-Dade County. QTP provides services such as data storage, E-Mail communication and scheduling for their client companies. Late Saturday night, Nunez remotely accessed QTP’s network without authorization, using an administrator account and password. He first changed the passwords of all of the IT system administrators and then he shut down almost all of the QTP servers. What is more, Nunez also deleted files. Had he not done that, it would have been possible to re-install the data from backup tapes much easily and in less time. As a result of Nunez’s malformed acts, QTP and their clients could not perform their normal business functions for a number of days, suffering a tremendous business loss.

As a result of the unauthorized access to the system and the deletion of data, QTP suffered over \$30,000 in damages. This included the cost of responding to the offense; conducting a damage assessment; restoring the data, system and information to their previous condition; and other costs incurred due to the interruption of network services. Through forensics investigations, Nunez was identified as the perpetrator. Investigators found that the activity on QTP’s computer could be traced to his home network. Additional evidence was also found subsequently when they performed a search of his computer.

*Source:* www.cybercrime.gov; posted on 14 July 2009.

### 11.2.15 Example 15: “Justice” vs. “Justice” – Software Developer Arrested for Launching Website Attacks

Denial-of-service attack (DoS) was mentioned in Chapters 1 and 2. It is explained in Chapter 4 (Section 4.9). Hacking and website defacement were addressed in Section 1.5.11 of Chapter 1. Screen shots of hacked websites were presented in Figs. 1.6–1.10. This real-life example shows the crime by a young software engineer who launched a series of “denial-of-service attacks” on various websites. It shows what misled/confused youth can do and in turn, how they become cybercriminals by embracing false motives. It is a reflection of rapidly changing values in our society. Forensics comes to the fore in the example.

Bruce Raisley, aged 47, was a software developer from Monaca, Pennsylvania, when he was charged with the offense of *computer fraud and abuse*. He quietly surrendered to the FBI on 1 July 2009. More specifically, Bruce was charged with the *unauthorized access of protected computers with the intention of causing denial-of-service*

and/or losses to the websites. A number of websites were impacted – among them were, RollingStone.com and the website of Rick A. Ross Institute of New Jersey (Rick Ross Institute), based in Hudson County, NJ, who run the Internet archive service “for the study of destructive cults, controversial groups and movement” and “Perverted Justice,” a Portland, Oregon-based organization (operated by X. E.). Perverted Justice is an organization that seeks to identify and expose pedophiles and sexual predators targeting minors.

Around 2004, Bruce had volunteered for “Perverted Justice.” *Perverted-Justice.com*, mentioned before, is a loosely organized group of computer gamers, students and the occasional well-meaning but misguided “reactionary” who claimed that their primary purpose was to bring about the complete destruction of the lives of anyone they believe is guilty of chatting with one of their “baiters.” Their baiters troll Internet chat rooms pretending to be young teen-aged girls in the hopes of entrapping men into sexually suggestive conversations. Once targeted, members of “Perverted Justice” organization search the Internet for all available information to publicly identify the “target,” along with complete information about the target – the family, target’s employer, friends, associates, neighbors, etc. Next, they launch a brutal harassment campaign against anyone listed on their site via phone calls, Internet messages, E-Mails, neighborhood flyers, etc.

Another impacted organization was Corrupted-Justice.com – a civil rights advocacy organization. It is a group of like-minded people who are dedicated to bringing about an end, using legal means, to the harassment and terrorism being perpetrated by the vigilante group. In this case, host of attacks were mounted on Corrupted Justice, an organization whose stated purpose is claimed to educate the public on the actions of various purported cybervigilante groups, including perverted Justice. In year 2006 or around that time, Bruce had become a member of “Corrupted Justice,” after becoming disenchanted with Perverted Justice!

According to the criminal complaints received, in September 2006 and July 2007, Radar Magazine and the Rolling Stone published two separate articles (“Strange Bedfellows” and “To Catch a Predator”: The New American Witch Hunt for Dangerous Pedophiles). Both articles presented positive and negative views on the activities conducted by “Perverted Justice” and its volunteers. The articles described what was termed as “questionable tactics” by Perverted Justice to silence critics. One of these tactics was an episode between X.E. and Bruce. In or about 2007, Strange Bedfellows was reprinted on numerous websites.

Around 25 September 2007, the Rick Ross Institute experienced a *distributed denial-of-Service* (DDoS) attack. One of the attacking computers was found to be that of the Academic and Research Network of Slovenia (ARNES). Upon examination, they found a malicious program on their network. Around 20 November 2007, the Slovenian Computer Emergency Response Team (SI-CERT) further determined that the DDOS program downloaded instructions from two locations, dosdragon.com and n9zle.com. These locations instructed the program to repeatedly target the victim websites.

Victim Rolling Stone was subjected to multiple DDOS attacks directed specifically at the webpage which hosted “The New American Witch Hunt.” During the height of the DDOS attacks, the page requests for the article escalated from a few requests per day to millions of page requests per day, causing the website to experience significant slowdown. On 7 March 2008, the US Computer Emergency Response Team (US-CERT) confirmed SI-CERT’s findings. On 16 January 2008 and 8 February 2008, Internet Service Provide records showed that Bruce controlled both command and control systems.

“Corrupted Justice” was the victim of a similar attack on 25 July 2007. As a result of this particular attack, their website was shut down for 4 days. They were attacked again on or about 2 November 2007 and on or about 10 March 2008, resulting in additional 7 days without service. As per the complaint lodged, Bruce had contacted Corrupted Justice to show off that he had again taken down their servers. The complaint also states that Bruce told Corrupted Justice that he “unleashed a virus that could never be stopped,” that [Corrupted Justice] could “kiss goodbye to their website because nothing could protect their servers against this attack.” During a search of his home on 27 March 2008, Bruce admitted to contacting both Rick Ross Institute and Corrupted Justice, asking them to take the articles off from their websites. Additionally, Bruce

stated that he wrote the programs on a memory stick – it was seized by FBI as part of the search. Bruce also admitted that he used these programs to attack the Perverted Justice, Corrupted Justice and Rick Ross Institute websites. A forensics review of the seized electronic media confirmed that it contained copies of programs used in conjunction with the DDoS attack.

This case was prosecuted in the District of New Jersey. Bruce was scheduled for an initial appearance on 1 July 2009 before the Honorable Patty Schwartz, US Magistrate. Upon being convicted, Bruce received a maximum of up to 10 years imprisonment along with the fine of \$250,000. As would be known to readers/students well-versed with law, criminal complaint is merely an accusation. Despite this accusation, every defendant is presumed innocent unless and until proven guilty beyond a reasonable doubt. Special Agent in charge of this case stated that in this situation, this type of “cyberbullying” (the term was introduced in Chapter 2, Box 2.8) was used as a way to silence the media and deny them of their constitutional rights to the freedom of press. The Agent further stated that “cyberbullying” is not acceptable. He thanked all the team members involved for a job well done. This real-life example shows that technology works both ways and the criminal will get caught.

*Source:* <http://www.cybercrime.gov>; posted on 1 July 2009.

### **11.2.16 Example 16: CAN-SPAM Act Violation through E-Mail Stock Fraud**

Spamming is explained in Chapter 1 (Section 1.5 and Box 1.5). Anti-Spam Laws in Canada are explained in Section 6.2.3 of Chapter 6. Here is a real life happening on that. This example involves the CAN-SPAM Act – for those who are not aware of it, refer to the links about this Act in Ref. #30, Additional Useful Web References, Further Reading. The full form of CAN-SPAM Act is “Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003.” Five individuals pleaded guilty on 23 June 2009 in the federal court in Detroit for their involvement in a wide-ranging international stock fraud scheme that had the illegal use of bulk commercial E-Mails or “spamming.” Considering the advanced age of one of the fraudsters in this example, we can say that just like cybercrime knows no national boundaries, criminals seem to have no heed to their age!

Alan M. Ralsky, aged 64, and Scott K. Bradley, aged 38; both pleaded guilty to conspiring to commit wire fraud, mail fraud and of violating the CAN-SPAM Act. This act defines a “commercial electronic mail message” as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose).” It exempts “transactional or relationship messages.” Ralsky and Bradley also pleaded guilty to “wire fraud” and “money laundering” apart from the violation of CAN-SPAM Act. Under the terms of his plea agreement, Ralsky acknowledged facing up to 87 months in prison and a \$1 million fine under the federal sentencing guidelines while Bradley acknowledged facing up to 78 months in prison and a \$1 million fine under the federal sentencing guidelines.

For some time, Alan Ralsky was the world’s most notorious illegal spammer. In fact he was the self-proclaimed “Godfather of Spam.” Today Ralsky, his son-in-law Scott Bradley and three of their co-conspirators stand convicted for their roles in running an international spamming operation that sent billions of illegal E-Mail advertisements to pump up Chinese “penny” stocks and then reap profits by causing trades in these same stocks while others bought at the inflated prices. Using the Internet to manipulate the stock market through Spam E-Mail campaigns is a serious crime. This case shows that federal law enforcement has the both the capability and the will to successfully investigate, prosecute and punish such cybercrimes.

The CAN-SPAM Act was passed by Congress in 2003 to address Spam E-Mails. The Act has certain provisions (criminal provisions) to prohibit falsification of certain information used in E-Mail transmission. John S. Bown, 45, of Fresno, California, pleaded guilty to conspiracy to commit wire fraud, mail fraud and

to violate the CAN-SPAM Act. He also pleaded guilty to conspiring to commit computer fraud by creating a Botnet and violating the CAN-SPAM Act. A Botnet is a network of computers that have been infected by malicious software. Under the terms of his plea agreement, Bown acknowledges he is facing up to 63 months in prison and a \$75,000 fine under the federal sentencing guidelines.

Yet another person, William C. Neil, aged 46, of Fresno, admitted that he had conspired to violate the CAN-SPAM Act. Under the terms of his plea agreement, Neil acknowledged facing up to 37 months in prison and a \$30,000 fine under the federal sentencing guidelines. James E. Fite, aged 36, of Culver City, California, pleaded guilty to conspiracy to commit wire fraud, mail fraud and to violate the CAN-SPAM Act. Apart from this, he also pleaded guilty of making false statements to FBI agents. Under the terms of his plea agreement, Fite acknowledged that he was to face up to 2 years in prison and a \$30,000 fine under the federal sentencing guidelines. Finally, Spam King Alan Ralsky got 4 years in jail.

Assistant Attorney General said "We will not allow criminals to use E-Mail as a conduit for fraud. This prosecution, the Department's largest to date under the CAN-SPAM Act, underscores our strong and steadfast commitment to ridding our financial markets and cyberspace of E-Fraudsters looking to prey on innocent victims." Special Agent in Charge mentioned that cybercrime investigations are a top priority of the FBI who is known to aggressively investigate those individuals who exploit computers for committing various crimes. In today's aggressive international business world, there will always be a select few who illegally manipulate the system for their own profit. According to Special Agent in Charge, Internal Revenue Service Criminal Investigation (IRS-CI), they, that is, IRS CI, diligently follows the money frauds and assists in the seizure and penalty for any illegal gains from their illegal business practices.

According to court records, from January 2004 through September 2005, Ralsky, Bradley, Judy Devenow, Bown, William Neil, Anki Neil, James Bragg, Fite, Peter Severa, Wai John Hui, Francis Tribble, and others engaged in a related set of conspiracies designed to use Spam E-Mails to manipulate thinly traded stocks and profit by trading in those stocks once their share prices increased after recipients of the Spam E-Mails traded in the stocks being promoted. The defendants were indicted in the Eastern District of Michigan in December 2007.

Ralsky served as the Chief Executive Officer and primary deal maker for the Spam E-Mail operation. Bradley, Ralsky's son-in-law, served as the Chief Financial Officer and Director of operations for the Spam E-Mail operation. Bown, who was Chief Executive Officer of an Internet services company called "GDC Layer One," served as the Chief Technology Officer for the Spam E-Mail operation. William Neil, who was an employee of GDC Layer One, built and maintained a computer network used to transmit Spam E-Mails as part of the conspiracy. Fite was a contract spammer who hired others to send Spam E-Mails as part of the conspiracy. Devenow, Hui and Tribble previously pleaded guilty for their roles in the conspiracy.

Devenow managed the Spam E-Mail operation and also sent Spam E-Mails. Tribble took charge of planning and directing the stock trading to further the conspiracy. Hui, CEO of China World Trade, served as the lead dealmaker to represent the companies whose stocks were being promoted via Spam E-Mail. Court documents revealed that many of the Spam E-Mails promoted thinly traded "pink sheet" stocks for US companies owned and controlled by individuals in Hong Kong and China. The Spam E-Mails contained significantly false and deceptive information or omissions. Those E-Mails were created and sent using some peculiar software programs to make it difficult to trace them back to the conspirators. According to the indictment, the conspirators used wire communications, the US mail and common carriers to further their frauds. The conspirators also participated in money laundering involving millions of dollars generated by their manipulative stock trading.

The defendants were indicted to have used several illegal methods in order to maximize the amount of Spam that evaded Spam-blocking devices and tricked recipients into opening, and acting on, the advertisements in the Spam. These included using falsified "headers" in the E-Mail messages, using proxy computers to

relay the Spam, using falsely registered domain names to send the Spam, and also making misrepresentations in the advertising content of some of the underlying E-Mail messages. An accusation is merely an indictment and defendants are presumed innocent until and unless proven culpable at trial beyond a reasonable doubt. The charges arose after a 3-year investigation, led by the FBI with assistance from the US Postal Inspection Service and IRS-CI exposed a sophisticated and widespread spamming operation. The case is being prosecuted by US Attorney Terrence Berg and Trial Attorneys Thomas Dukes and Mona Sedky Spivack of the Criminal Division's Computer Crime and Intellectual Property Section.

*Source:* www.usdoj.gov

### **11.2.17 Example 17: Business Liability through Misuse of Organization's Information Processing Assets**

In Chapter 2, Box 2.7 explains how criminals can create false E-Mail IDs. This example is a real-life scenario of that. In one bank, a management trainee of the bank was engaged with a girl working in the same bank. They were to get married in due course of time. During the post-engagement period, the couple exchanged many E-Mails; however, the boy and the girl used to write the mails during work hours using the company computers. Unfortunately, after some time the relationship went sour and the two broke up. The girl created fraudulent E-Mail IDs such as "indianbarassociations." She used that ID to send E-Mails to the boy's foreign clients. The girl used the bank's computer for sending these mails. The mails had negative publicity about the bank. The boy lost a large number of clients assigned in his portfolio. Moreover, those clients sued the bank. The bank was held accountable for the E-Mails sent using the bank's system. This small example is a lesson – organizations must have well-established computing guidelines (this is addressed in Chapter 9 – Section 9.8) and strict vigilance on how organizations computing and communication facilities are being used.

### **11.2.18 Example 18: Parliament Attack**

Forensics fundamentals were introduced in Chapter 7; this example illustrates the scenario in which it was used. Bureau of Police Research and Development (BPRD) at Hyderabad handled some of the top cybercases. One such case involved analyzing and retrieving information from the laptop recovered from terrorists, who attacked the Parliament. The laptop was seized from the two terrorists, who were gunned down when Parliament was under siege on 13 December 2001. Police sent the seized laptop to Computer Forensics Division of BPRD after computer experts at Delhi failed to trace much out of its contents. Inside the laptop there were a number of evidences that established the motives of the two terrorists, namely (a) the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and (b) the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. It was also found that the emblems (of the three lions) were carefully scanned and the seal was also deviously made along with residential address of Jammu and Kashmir. But careful forensics detection proved that it was all forged and was created using the laptop.

### **11.2.19 Example 19: Game Source Code Stolen!**

Source code theft is considered as an IPR theft (IPR is Intellectual Property Rights) and this example is about source code theft in real life. Given the life style and preferences of the young generation today, one can understand the popularity of game software packages. Game software can be loaded on the mobile handsets as well. Readers can refer to Chapter 3 where cybercrimes are described in the context of mobile devices. The episode described in this example involves game software. It is an episode of IPR theft that took place in 2003.

It so happened that a computer user in China obtained the source code of a popular game “Lineage I” 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](http://www.l2extreme.com), to offer the “Lineage” game at a discount. After noticing this, the South Korean company that owned the Lineage source code sent legal warnings. However, in spite of those warnings, 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.

Even after this action, the source code stealing of this kind did not stop. In 2007, a prominent Korean Newspaper “Chsun Ilbo” had reported that the source code for upcoming MMORPG Lineage III may have been stolen and sold to an undisclosed “major Japanese game company.” It was suspected that this could be an “insider” job. The Seoul Metropolitan Police investigated seven former NCSoft employees in conjunction with this crime. NCSoft estimated a damage value for the lost data at over 1 billion dollars US. This substantial figure was supposedly a projection based off the combined worth of the Lineage IP and its current subscriber value. At present, Lineage has over 1.5 million subscribers worldwide (mainly in Asia) and its current sales is over 1.6 billion dollars (1.5 trillion Korean won) spread across both titles.

“Insider attacks” (they could be by disgruntled employees or even by un-instigated employees with malicious minds) are worse because, when exposed, they can considerably dampen employee spirit, as happened in this case too. Morale at the impacted company NCsoft was in its worst stage even before word of the theft hit mainstream news. The company experienced serious turnover since the sacking of one of its senior game developers for “poor leadership skills.” Since the layoff, most of the 90-person development team has, likewise, decided to follow their chief elsewhere.

Police reported that the data theft may actually have occurred during a job interview! In the interview, one or more ex-NCsoft programmers demonstrated the code for external review. Roots of the problem may actually go all the way back to when program designs for Lineage III were reputedly leaked via E-Mail and/or portable disk.

### **11.2.20 Example 20: The Petrol Pump Fraud**

Thank God that in India, we do not as yet have the system of automated petrol pumps! This feeling of relief comes after reading this example of fraud. The fraud took place in a petrol pump in the US. In India, it is a common practice to keep an “eye” on the delivery of petrol (of course, assuming that the pump has been calibrated and periodically inspected to ensure that it is dispensing as it should). The example here can be considered as “Salami Technique” example, because things got discovered based on “little-by-little” happening! Here is how that happened.

Four men in Los Angeles, US, were charged with fraud for allegedly installing computer chips in gasoline pumps that cheated consumers by overstating the amounts pumped. The problem was noted when a rising number of consumers complaints were received which 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 5 and 10 gallon amounts (precisely the amounts typically used by inspectors).

### **11.2.21 Example 21: Xiao Chung’s Story – Life of a Hacker**

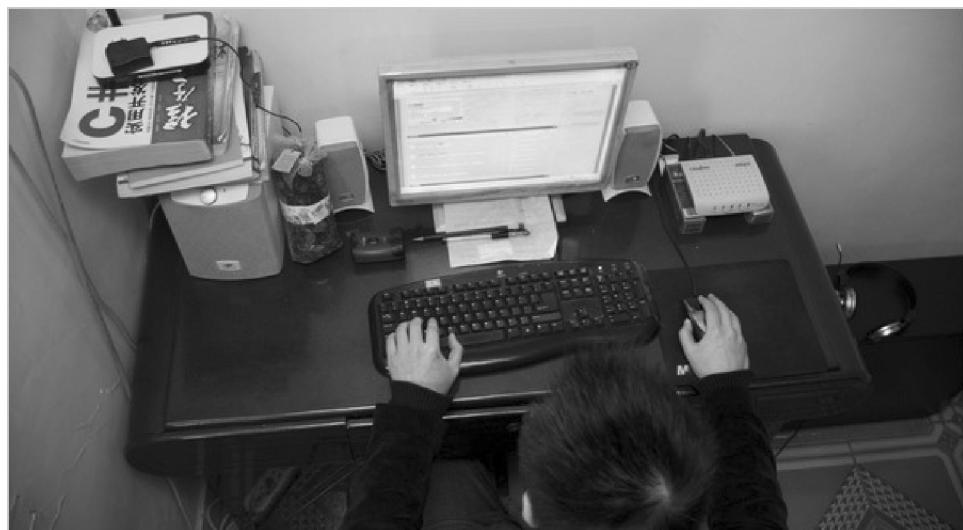
Chapter 1 (Section 1.4 and Table 1.3) and Chapter 10 (Figure 10.3 and Section 10.4.1), we mentioned about “motives” for hacking. Here is story of young hacker Xiao Chung (he has got another pet name in the dark world of the ace hacker community but it is kept confidential) who seemed eager to tell his

story. Like many hackers, he wants recognition for his hacking skills even as he values anonymity to remain un-detected. The New York Times found him through another well-known hacker who belongs to a hacker group and who vouched that Xiao Chung is too skilled. On condition that he should not be identified by his real name, Xiao agreed to allow a reporter to visit his modest home in a poor town outside Changsha, and watch him work.

It is quite eerie – just a few quick keystrokes and Xiao Chung proudly brings up a screen displaying his latest victims. He says with a quite a wicked smile, “Here’s a list of the people who’ve been infected with my Trojan Horse, and they don’t even know what’s gone wrong with them!” You may think that Xiao may be earning a lot from his craft; but that is not true. For all the seemingly terrific power in his hand to “affect” so many people, the hacker has a modest living - he works from a dingy apartment on the outskirts of this city in central China (Fig. 11.3).

Although Xiao Chung’s technical cyberattack claims cannot be verified, he is happy to demonstrate his hacking skills. He met a journalist at a cafe one night in February 2010, and invited him to his home, where he showed how he hacked into the website of a Chinese company. Once the website popped up on his screen, he created additional pages and typed the word “hacked” onto one of them. Further, he goes on to explain that it is an online “trapdoor” which he created just over a week ago, and has already lured 2,000 people from China and overseas – people who clicked on something they should not have, inadvertently spreading a virus that allows him to take control of their computers and steal numerous bank account passwords. It is hard to believe that Xiao Chung, a soft-spoken college graduate in his early 20s, is a cyberthief! He operates secretly and illegally, as part of a community of hackers who exploit flaws in computer software to break into websites, steal valuable data and sell it for a profit. Recall the Zero Day attacks mentioned in Chapter 2, Box 2.10).

According to Internet security experts, China has legions of hackers just like Xiao Chung, and the experts say that they are the culprits for an escalating number of global attacks launched to steal credit card numbers, commit corporate espionage and even wage online warfare on other nations. In some cases, these attacks have



**Figure 11.3** | The young hacker at work.

been traced back to China. In addition to independent criminals like Xiao Chung, computer security specialists say there are so-called patriotic hackers (i.e., “Hacktivists”) who focus their attacks on political targets.

The People’s Liberation Army has got intelligence-oriented hackers. It is said that there are also more shady groups who are believed to work with the State Government. It is said that in China, as well as in parts of Eastern Europe and Russia, computer hacking has become something of a “national sport,” and a lucrative one. It is being done with all the professional aplomb; for example, there are hacker conferences, hacker training academies and magazines with names like Hacker X Files and Hacker Defense, which offer tips on how to break into computers or build a Trojan Horse, step by step. Refer to Ref. #5, Additional Useful Web References, Further Reading.

It is getting easy for hackers; for less than \$6, one can even purchase the Hacker’s Penetration Manual. Books on hacking are also sold, to a lesser extent, in the US and elsewhere. With 380 million web users in China and a sizzling online gaming market, analysts say it is no wonder that Chinese youths are so skilled at hacking. Many Chinese hackers are interviewed to get them inducted into a loosely defined community of computer devotees working independently. They are also selling services to corporations and even the military! Because it is difficult to trace hackers, exactly who is behind any specific attack and how and where they operate remains to a large extent a mystery. And that is just the way Xiao Chung, the young Chinese hacker, wants it.

Xiao Chung’s story is like most young hackers who fall in love with hacking in college. Xiao, too, took to hacking after friends showed him how to break into computer systems during his first year in the college. After earning a degree in engineering, he took a job with a government agency, largely to please his parents, just to show them a “regular” job. However, hacking remains his “passion”! At the end of his work at the “regular” job, Xiao turns to his passion: hacking. He admits that he does it for the lure of money. Many hackers make a lot of money, he says, and he seems to be charting his own path. Exactly how much he has earned, he would not like to disclose. But he does admit to selling Malicious Code to others, and boasts of being able to tap into people’s bank accounts by remotely operating their computers.

Xiao is consumed by the challenges it presents. He reads hacker magazines, swaps information with a small circle of hackers and writes Malicious Code. He uses Trojan Horses to sneak into people’s computers and infect them, so he can take control. “Most hackers are lazy,” he says, smugly seated in front of a computer in his spare bedroom, overlooking a dilapidated apartment complex. According to Xiao “Only a few of us can actually write code. That’s the hard part.”

Computer hacking is illegal in China. Last year, Beijing revised and stiffened a law that makes hacking a crime, with punishments of up to 7 years in prison. Xiao Chung does not seem bothered by the law, largely because he thinks it is not strictly enforced. However, he is clever enough to cover his tracks. Financial incentives motivate many young Chinese hackers like Xiao Chung. Scott J. Henderson, author of “The Dark Visitor: Inside the World of Chinese Hackers,” had spent years tracking Chinese hackers, sometimes with financial help from the US Government. One Chinese hacker who broke into a US Government site later lectured on hacking at a leading university and worked for China’s security ministry. According to Henderson, recently many Chinese hackers have been seeking to profit from stealing data from big corporations or teaching others how to hijack computers. They make a lot of money selling viruses and Trojan Horses to infect other people’s computers. They also break into online gaming accounts and sell the virtual characters. It’s big money for these hackers.

“Hack-star” Xiao Chung lives with his parents, and his bedroom has little more than a desktop computer, a high-speed Internet connection and a large closet. The walls are bare. Most of his socializing occurs online; his “after regular job” hours range from about 6:30 p.m. to 12:30 a.m., starting every evening by perusing computer websites like cnBeta.com. Xiao values his freedom and that is one strong reason he puts forth for not working for any major Chinese technology company. He even claims to know details of the

Google attack. “That Trojan Horse on Google was created by a foreign hacker,” he says, indicating that the virus was then altered in China. “A few weeks before Google was hijacked, there was a similar virus. If you opened a particular page on Google, you were infected.” Oddly, Xiao’s parents did not know that he does the “hack-job” at night. One day, however, he explained the intricacies of computer hacking and stealing data while his mother stood nearby, listening silently. Xiao and his fellow hackers keep secret their knowledge of certain so-called “zero-day vulnerabilities” – software flaws – for future use. When asked whether hackers work for the government, or the military, he says “yes.”

### **11.2.22 Example 22: Killers Take Tips from 26/11 Attack to Use VOIP**

The term “cyberterrorism” was explained in Chapter 1 (Box 1.1 and Section 1.2) and here is a real-life incidence involving cyberterrorism in the country that has just about settled from the shock of 26/11 attacks on Mumbai. Those attacks revealed the wireless communication technology used by the terrorists. This real-life example comes from that background. In Chapter 7, E-Mail forensics is explained – fully aware that electronic mails can be traced, cybercriminals as well as terrorists adopt a technique whereby they do not send attack-related mail and yet they communicate with their counterparts. This real-life example shows how that technique was used.

Investigations in the murder of criminal lawyer Shahid Azmi revealed that the killers had used communication techniques similar to the ones used by terrorists during the 26/11 terror attacks and the 11/7 train blasts. According to crime branch sources, gangster Bharat Nepali, who had hired men to eliminate Azmi, had used Voice over Internet Protocol (VoIP) system to communicate with the killers. During the investigations it was revealed that at least six calls were made, before and after Azmi’s murder, using VoIP service from Hong Kong, Los Angeles, London and Israel. The usage of VoIP for criminal activity came to light during the 26/11 terror attacks in Mumbai. Handlers of the terrorists, who attacked the city on the night of 26 November 2008, were found to be using VoIP service to communicate with the 10 men who laid siege at various locations in the city.

Use of draft E-Mail system was another communication technique used by Azmi’s killers. The same technique was used by terrorists in the 11/7 train blasts that rocked Mumbai city in 2006. According to a crime branch official, a person from Bangkok attached photographs of Azmi in a mail and saved it as a draft in an E-Mail account. The killers, Devendra Jagtap and Hasmukh Solanki, who knew the password of the E-Mail account opened the draft mail and thus identified Azmi.

Azmi’s killing (on 11 February 2010) had shocked the city’s legal fraternity. It was scary – the three men had barged into Azmi’s Kurla office to shoot him dead and then they ran away from the scene. Azmi was defence lawyer in the 26/11 trial for Faheem Ansari, who was recently acquitted by the court due to lack of evidence. The first round of investigations revealed that it was a contract killing undertaken for ₹ 1 lakh (₹ 1,00,000) at the command of Nepali, a former aide of infamous Chhota Rajan.

Later on crime branch officials detained Devendra Jagtap, Pintu Dagle and Vinod Vichare from Mulund, while the fourth accused, Hasmukh Solanki, was taken into custody on 9 March 2010. The police also seized four weapons that were used in the killing, three rounds of live cartridges and five mobile phones from the group. Of the 10 accused, six, including Nepali, his close aide Vijay Shetty, Santosh Shetty, Rajiv Tiwari and two others, were absconding. According to Public Prosecutor Kalpana Chavan, Nepali had given contract to kill Azmi because he believed that the lawyer was defending those who according to him are anti-nationals. The shooting was part of Nepali’s efforts to establish his supremacy in the underworld.

### 11.2.23 Example 23: “Robberson” Brothers Caught for Selling Pirated Software

Investigation of Maurice A. Robberson and his brother Thomas Robberson was commenced by BSA (Business Software Alliance). In early 2002, BSA had received complaints from software publishers and that was the basis for the investigation. After reviewing the reported websites, BSA made undercover purchases and determined that the software sold was pirated. After this, BSA referred the case to the Federal Bureau Washington Field Office. The FBI Field Office conducted independent investigation and subsequently shut the operation down in October 2005. The investigation determined that starting in late 2002 the Robberson brothers sold more than \$5 million of counterfeit software products. In addition to running four for-profit websites, the Robberson brothers were also co-conspirators with Danny Ferrer in the operation of [www.BbuysUSusA.com](http://www.BbuysUSusA.com).

It turned out from the investigations that, during the operation of the websites, Thomas Robberson grossed more than \$150,000 by selling software with a retail value of nearly \$1 million. Maurice Robberson amassed more than \$855,000 through sales of software with a retail value of nearly \$5.6 million. In March 2008, Maurice Robberson was sentenced to 36 months in prison, whereas his brother Thomas was sentenced to 30 months. Both were also ordered to undergo an additional 3 years of supervised release and pay restitution.

### 11.2.24 Example 24: BSA Uncovers Software IPR Breaches

The issue of software piracy as Intellectual Property Offense is addressed in Section 9.2.2, Chapter 9. This is a glaring example of that type of offence. This is one more example of the breach uncovered by BSA happened in Georgia State, US, in July 2008. It involved interaction with eBay. Launched in 1995, eBay started as a place to trade collectables and hard-to-find items. Today, eBay is a global marketplace where institutional buyers as well as individuals can buy and sell practically anything. You do not have to register to take a look at what's available, but you will need to register if you want to buy or sell. Today, eBay is the world's online marketplace – it is a place for both buyers as well as sellers to come together and trade almost anything. People use such facilities for the convenience, at times overseeing the risks involved as we learn in this example.

A woman was stopped from selling counterfeit copies of Corel software on eBay. An investigation revealed that she had sold more than \$212,000 worth of unlicensed software to hundreds of consumers, in the period January–May 2008. A \$250,000 civil judgment was entered against her. In another episode of similar kind, uncovered by BSA, a person from yet another state was found to be involved. Jon Crain of Coraopolis, Pennsylvania, operated nearly 20 websites distributing unlicensed copies of Adobe, McAfee, Microsoft and Symantec software online. He was first targeted in March 2007 as part of an international legal action against five software pirates. The other offenders were located in the UK, Austria, and Germany. In many of these cases, BSA was alerted to the illegal activity by reports or complaints from disappointed consumers who were initially attracted by low price deals. BSA sued Crain, and a civil judgment was entered that included a hefty settlement payment and a requirement to remove the unlicensed software from his website.

Another example is this incidence that took place in July 2008. Jeremiah Mondello, a 23-year Oregon man, was sentenced to 4 years in federal prison for selling more than \$1 million worth of pirated software and distributing malware via instant message networks to steal financial data from dozens of consumers. He then used the stolen bank account credentials to set up more than 40 online auction accounts in the victims' names and withdraw money from their debit accounts. In addition to the prison sentence, federal investigators also seized computers and \$220,000 in cash from Mondello. The government also was entitled to seize his home and surrounding land.

### 11.2.25 Example 25: Pune City Police Bust Nigerian Racket

This story had appeared in Pune Mirror dated 25 October 2010. Name of the victim has been masked to respect the privacy of the person. However, all the events mentioned here are real and are presented exactly as they happened, as mentioned in the chain of events mentioned here is as at the time of writing this. Visit Items No. 19 in Section 11.7 (Online Scams) – Nigerian Scam is explained there. What is described here is a real-life example of that. This example re-emphasizes the need for cybercrime awareness. As you can see in this example, even an educated person working in technology field got fooled by the perpetrators and suffered a big financial loss. It also shows the greed of criminals.

The police succeeded in nabbing two suspects in this fraud case. This fraud happened when the police started probing into a complaint received from a young software engineer working in Pune city. Arjun Changaokar, a resident in Warje area, was duped into parting with ₹ 10.27 lakhs (₹ 10,27,000) by making him believe that he was going to be offered a high profile job in a London hotel called New Climax.

In an E-Mail chat with an alleged UK-based Councillor, Arjun, the techie from Rajiv Gandhi Infotech Park at Hinjewadi, was convinced to pack up and leave India for UK! The fraud got exposed when Arjun found that there was no flight to UK from Indira Gandhi International Airport at the time he was told by the conmen! The efforts expended by Warje police were successful and two perpetrators, including a bank account holder, were arrested. However, the real mastermind Chong-Ching, who is a foreign national, was still absconding. A special squad of cyber experts has been investigating the Nigerian fraud racket run from Meera Road. The three accused in the FIR (First Information Report) filed by the victim include Shailendra Ramesh Soni, aged 24, a resident of Shivajinagar in Govandi in Mumbai, Naresh Shubrakaran Sharma, aged 27, a resident of Queens Park in Mira-Bhayandar in Thane and Chong-Ching, the foreign national whose complete name and address could not be traced (as at the time of writing this). The fraud took place during the period 26 July–24 September 2010. The accused have been charged under various sections of the IPC (Indian Penal Code – see Appendix P in CD) and the Indian IT Act (see Appendix O in CD) for *cheating and conspiracy using Information Technology*.

As per complaint filed by the victim Arjun Changaokar, the fraud started with the mail he received on 26 July 2010. In that mail he was offered a job in UK-based hotel “New Climax.” A person calling himself Chong-Ching claimed to be authority at the hotel and offered to victim the post of Sales Supervisor with a handsome UK salary. The victim responded to the E-Mail and accepted the offer. There onward, the correspondence continued. In another E-Mail, a person called John Smith Levis introduced himself as UK councillor. John claimed to have been given the responsibility by the hotel to provide Visa. To get the Visa and to pay for journey expenses and accommodation in the UK, John asked the victim for various amounts of money in a number of E-Mails. John gave to the victim several account numbers in different branches of Axis Bank and ICICI Bank. Victim Arjun deposited those amounts ranging from ₹ 2 to 5 lakhs (₹ 2,00,000 to 5,00,000) on different occasions. Over a 2-month period, Arjun (the victim) deposited a total amount of ₹ 10.27 lakhs (₹ 10,27,000)! In the words of the victim

*“At first, I received an email offering me a high paying job in UK hotel to get a visa and to pay for journey expenses and accommodation in UK, I was asked for various amounts of money in multiple emails. He gave me several account numbers in different branches of Axis Bank and ICICI Bank. I deposited amounts ranging from Rs. 25 lakh on different occasions. Over a two-month period, I deposited a total amount of Rs. 10,27,700.”*

The victim arranged the money from various sources. He shared with his parents and friends the news of his overseas job. According to the E-Mail, the victim received on 10 October 2010, he was supposed to catch a flight from Indira Gandhi International Airport and a person was going to meet Arjun at the airport with

a Visa and an air ticket. During the correspondence, receipts with fake stamps (as it turned out later) and signatures of the British High Commissioner were sent to victim. When victim (Arjun) reached the airport, he found that there was no such person waiting for him. That is when the victim realized that he had been cheated. Arjun returned to Pune and tried to contact the concerned person but the concerned person never replied to his mails. Arjun then decided to approach the police.

Inspector (Crime Branch) Solankar said "After receiving the complaint, we started investigating the accounts in which Arjun had deposited the requested amounts of money. We identified an account in the name Shailendra Soni in the Shivajinagar branch of Axis Bank. We sent a team to Govandi and laid a trap for him." After the inquiry, the Police discovered that Soni was asked by someone called "Sharma" for permission to use his account. Police nabbed Sharma in Mira-Bhayandar. The investigation revealed that someone hailing from Nigeria asked them to commit the crime. He offered 7% of the total amount to Sharma. Sharma, in turn, got Soni's help by offering him a 5% commission. Sharma had met the suspected foreign national several times and they had been running this racket for many years. Sharma has various cheating crimes registered to his name. The Police took up the investigation aimed at finding out other crimes committed by this gang.

### 11.3 Mini-Cases

In this section, we have provided real-life cases involving cyberpornography, cyberdefamation, Salami attack, Internet time theft, etc. Table 11.2 lists the Mini-Cases of this section.

**Table 11.2** | List of Mini-Cases in Section 11.3

Mini-Case No.	Title	Topic	Chapter Cross-Reference
1	Cyberpornography Involving a Juvenile Criminal	Cyberpornography	Chapters 1 and 2
2	Indian Cyberdefamation Case of a Young Couple	Cyberdefamation, spoofed mails with ulterior motive	Chapters 1 and 7
3	The Zyg-Zigler Case	Salami attack, logic bomb	Chapter 1
4	Internet Time Stealing	Cybertheft	
5	New York Times Company vs. Sullivan Case of Cyber Defamation	Cyberdefamation	Chapter 1
6	The Indian Case of Online Gambling	Online gambling	Chapter 1
7	An Indian Case of Intellectual Property Crime	IPR Theft, Cybersquatting	Chapters 1, 9 and 10
8	The SlumDog Millionaire Movie Piracy Case	IPR theft	Chapters 1, 2, 4 and 9
9	Malicious Hacking Case – Organ Donation Database Deleted	Hacking of computer network, insider attack	Chapters 1, 2, 4 and 9
10	The Case of Counterfeit Computer Hardware	—	

(Continued)

**Table 11.2 | (Continued)**

<i>Mini-Case No.</i>	<i>Title</i>	<i>Topic</i>	<i>Chapter Cross-Reference</i>
11	The Chinese Case of Trade Secret Stealing involving an E-Waste Company	Hacking	Chapter 1
12	Internet Used for Murdering	—	Chapters 7 and 8
13	Social Networking Victim – MySpace Suicide Case	Social networking evils	Chapters 1 and 7
14	State of Tamil Nadu vs. Suhas Katti Case	Cyberdefamation	Chapter 1
15	Pune Citibank MphasiS Call Center Fraud	Data theft	Chapter 9
16	NASSCOM vs. Ajay Sood & Others	Phishing	Chapter 5
17	Indian Case of Cyberdefamation	Cyberdefamation	Chapter 1
18	Indian Cases of Cybersquatting	Cybersquatting	Chapters 1 and 10
19	Swedish Case of Hacking and Theft of Trade Secrets	IPR theft	Chapters 1, 9 and 10
20	IPR Violation	IPR theft	Chapters 1, 9 and 10
21	Indian E-Mail Spoofing Case	Spoofing	Chapter 2

### 11.3.1 Mini-Case 1: Cyberpornography Involving a Juvenile Criminal

Pornography is mentioned in Chapter 1. There was a recent Indian incident involving cyberpornography related to an 8th grade student of a certain Delhi school. The classmates used to tease the boy for having a pockmarked face. This went on for quite some time and the teasing did not stop in spite of student's appeals to his friends and complaints to the school teachers. Tired of the cruel jokes about his face, the boy decided to get back at his tormentors. As revenge, he scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. Action against this student was taken after the father of one of the girls (featured on the website) objected and lodged a complaint with the police.

In another incident that occurred in Mumbai it was found that a Swiss couple would gather slum children and would force them to appear for obscene photographs. The couple would then launch these photographs on to websites expressly designed for pedophiles. The Mumbai police arrested the couple under the charge of cyberpornography. Section 67 B of the ITA 2008 (Indian IT Act amendment of 2008) addresses child pornography and makes searching and browsing also as offenses.

### 11.3.2 Mini-Case 2: Indian Cyberdefamation Case of a Young Couple

Sujata, a young girl, was about to get married to Sudesh whom she met during a social event. She was mighty pleased because she never believed in finding a perfect match through an arranged marriage. Sudesh seemed to be open-minded and pleasant. They used to meet quite often during the pre-marriage period. One day when Sujata met Sudesh, he looked worried and even a little upset. He did not seem interested in talking to her. When she asked, he told her that members of his family had been receiving E-Mails that contained malicious stories about Sujata's character. Some of them were of her past affairs. He told her that

his parents were very upset and he felt they were justified in getting upset; after all, Sujata was going to be their daughter-in-law soon. Sudesh told Sujata that his parents were considering breaking off the engagement. Sujata was shocked obviously, but fortunately, Sudesh was able to convince his parents and other elders of his house to approach police instead of blindly believing the mails. During investigation, it was revealed that the person sending those E-Mails was none other than Sujata's stepfather. Sujata was the main source of income in the family after her mother expired; the father was a drunkard and had no means of livelihood. Sujata's father (when he gave in during the police enquiries) admitted that he had sent those E-Mails to break the engagement. He wanted Sujata to remain with him to continue providing him financial support. He admitted that Sujata's marriage would have caused him to lose control of her property of which he was the guardian till she got married. Sujata's mother had bequeathed her all the property through a registered will because she was not sure if the property would be safe in the hand of her chronic alcoholic husband.

Section 49 of the Indian Penal Code is mentioned in reference to cyberdefamation in Chapter 1 (Section 1.5.3). Readers may like to note that copy of the IPC (Indian Penal Code) is available in Appendix P.



Cyberdefamation is a cognizable offense. Chapter XXI of the Indian Penal Code (IPC) is about DEFAMATION. In Section 499 of Chapter XXI of IPC, regarding "defamation" there is a mention that "*Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.*"

The investigation traced the perpetrators through E-Mail forensics (refer to Section 7.6 of Chapter 7).

Another famous case of cyberdefamation occurred in America. Friends and relatives of a lady were inundated with obscene E-Mail messages appearing to originate from her account. These mails gave the lady a bad name and made her an object of ridicule. The lady was an activist against pornography. In reality, a group of people displeased with her views and angry with her for opposing them, had decided to get back at her by using such underhanded methods. In addition to sending spoofed obscene E-Mails, they also launched websites about her basically meant to malign her character.

### 11.3.3 Mini-Case 3: The Zyg-Zigler Case

It is said that in the US, it is common to fire people from jobs. One employee of a bank in the US was dismissed from his job. The disgruntled man felt offended at have been mistreated by his employers. He decided to take revenge. He first introduced a logic bomb into one of the core banking systems of the bank. The logic bomb was programmed in such a way that the system would take 10 cents off from all the accounts in the bank and would deposit them into the account of the person whose name was alphabetically the last in the bank's rosters. This disgruntled man then opened an account in the name of Ziegler. The amount debited from each of the accounts in the bank was so trivial that neither the account holders nor the bank officials noticed any fault. Finally, this phenomenon came to the notice of the bank officials when another person by the name of Zyger opened his account in that bank. He was astonished to find a substantial amount of money being transferred into his account every Saturday!

### **11.3.4 Mini-Case 4: Internet Time Stealing**

This is a case that took place before the ITA 2000, was enacted. In this case a services person was impacted. As you read on, you will realize how determination led to revelation about the fraud which otherwise would not be detected. The fraud described in this case could be detected due to victim's alertness. Recall the discussion in Section 4.12.2 about "Theft of Internet Hours."

Colonel Bajwa, a resident of New Delhi, asked a nearby net cafe owner to visit for re-installing his Internet connection. For this purpose, the net cafe owner needed to know his username and password. After setting up the connection, the cybercafe owner walked away with the username and password noted down. He then sold this information to another net cafe. After about a week, Colonel Bajwa discovered that his Internet hours were almost over! Out of the 100 hours that he had purchased, more than 90 hours had been used up within the span of that week. He noted that this had happened although he was inactive in that week in terms of his use of the Internet from that connection that was set up with the help of the net cafe owner. Colonel Bajwa was surprised and became suspicious of his suddenly depleting Internet account. So, he reported the incident to the Delhi Police. The Police could not believe that time could be "stolen" because they were not aware of the concept of "time-theft" at all. They could not understand how something "immovable" such as the Internet "hours" could be stolen and so they rejected Colonel Bajwa's report. Colonel Bajwa was not willing to give up and he decided to approach The Times of India, New Delhi. They, in turn, prepared a report about the shortfall of the New Delhi Police in handling cybercrimes. The Commissioner of Police, Delhi took charge of the case and the police under his directions raided the cybercafe and arrested the owner under the charge of theft as defined by the Indian Penal Code. The net cafe owner spent several weeks locked up in Tihar jail till the bail was granted. There are two points to note: (a) the modified IT Act, that is, the ITA 2008 addresses the cybercafe issue and (b) not having encountered such a situation before, the police were perplexed by the theft about something they considered "immovable."

### **11.3.5 Mini-Case 5: New York Times Company vs. Sullivan Case of Cyberdefamation**

Here is the brief for the New York Times Co. v. Sullivan Case – facts of the case decided together with *Abernathy v. Sullivan*; this case concerns a full-page advertisement in the New York Times which alleged that the arrest of the Rev. Martin Luther King, Jr. in Alabama was part of a campaign to destroy King's efforts to integrate public facilities and encourage blacks to vote. L. B. Sullivan, the Montgomery city commissioner, filed a libel action against the newspaper and four black ministers who were listed as endorsers of the advertisement, claiming that the allegations against the Montgomery police defamed him personally. Under Alabama law, Sullivan did not have to prove that he had been harmed. He also did not have to prove the defense claim that the advertisement was untruthful because the advertisement contained factual errors. Sullivan won a \$500,000 judgment. Question presented was "Did Alabama's libel law, by not requiring Sullivan to prove that an advertisement personally harmed him and dismissing the same as untruthful due to factual errors, unconstitutionally infringe on the First Amendment's freedom of speech and freedom of press protections?" Conclusion: The court held that the First Amendment protects the publication of all statements, even false ones, about the conduct of public officials except when statements are made with actual malice (with knowledge that they are false or in reckless disregard of their truth or falsity). Under this new standard, Sullivan's case collapsed.

This was a US Supreme Court case which recognized the actual malice standard before press reports could be considered to be defamation and libel, and hence allowed free reporting of the civil rights campaigns in

the southern US. It is one of the key decisions supporting the freedom of the press. The actual standard for malice requires that the publisher is aware whether the statement is false or acts in an irresponsible manner without regard of the truth. The decision established that for a plaintiff to win a libel ruling against a newspaper, “actual malice” or “reckless negligence” must be proved on the part of the paper if the statement in question is about a public official or a public figure. In the case of a private figure, the petitioner must merely prove carelessness. The background for this case is described below.

On 29 March 1960, the New York Times carried a full-page advertisement titled “Heed Their Rising Voices,” which solicited funds to defend Martin Luther King, Jr. against an Alabama perjury indictment. In the advertisement there was description about actions against civil rights protesters and activists – some was inaccurate and some involved the police force of Montgomery, Alabama. The inaccurate criticism of the actions by the police was considered as defamation against Commissioner L.B. Sullivan, whose duties included supervision of the police department. Though he was not named in the advertisement but he held the position of commissioner.

Alabama law denied a public officer recovery of punitive damages in a libel action brought on account of a publication concerning their official conduct unless they first make a written demand for a public retraction and the defendant fails or refuses to comply, so Sullivan sent such a request. The Times did not publish a retraction in response to the demand. Instead it wrote a letter stating, among other things, that “we...are somewhat puzzled as to how you think the statements in any way reflect on you,” and “you might, if you desire, let us know in what respect you claim that the statements in the advertisement reflect on you.” Sullivan didn’t respond but instead filed this suit a few days later. He also sued four black ministers mentioned in the ad, specifically Ralph Abernathy, S.S. Seay, Sr., Fred Shuttlesworth and Joseph Lowery. Sullivan won \$500,000 in an Alabama court judgment.

Eventually, The Times did, however, publish a withdrawal of the advertisement upon the demand of Governor John Patterson of Alabama, who asserted that the publication charged him with “grave misbehavior and...inappropriate actions and omissions as Governor of Alabama and Ex-Officio Chairman of the State Board of Education of Alabama.” When asked to explain why there had been a retraction for the Governor but not for Sullivan, the Secretary of The Times testified: “We did that because we didn’t want anything that was published by The Times to be a reflection on the State of Alabama and the Governor was, as far as we could see, the embodiment of the State of Alabama and the proper representative of the State and, furthermore, we had by that time learned more of the actual facts which the ad purported to recite and, finally, the ad did refer to the action of the State authorities and the Board of Education presumably of which the Governor is the ex-officio chairman....” On the other hand, he testified that he did not think that “any of the language in there referred to Mr. Sullivan.” The court decision was decreed as described below.

There was the rule of law that was applied by the Alabama courts; however, it was found to be constitutionally deficient. This was seen in the failure to provide the safeguards for freedom of speech and of the press that are required by the First and Fourteenth Amendments in a libel action brought by a public official against critics of his official conduct. The decision further ruled that under the appropriate safeguards, the evidence presented in this case was not constitutionally sufficient to support the judgment for Sullivan.

### 11.3.6 Mini-Case 6: The Indian Case of Online Gambling

There are millions of websites, hosted on many servers, to offer online gambling services. It is believed that many of these websites are actually fronts for “money laundering.” Fraud cases of “Hawala” dealings and money mis-deals over the Internet have been reported in the past (in Ref. #8, Additional Useful Web References, Further Reading, we have provided some links to “Hawala” systems for readers who have not

heard about this informal system of transferring money). It is not yet fully known if these sites have any relationship with drug trafficking. Recent Indian case about cyber lotto is very interesting. Kola Mohan was the man who invented the story of winning the Euro Lottery. He created a website and an E-Mail address on the Internet with the address “eurolottery@usa.net.” Whenever accessed, the site would declare him as the recipient of the 12.5 million pound. A Telgu newspaper published this as news after confirmation. Meanwhile, Kola Mohan collected large sums of money from the public as well as from some banks for mobilization of the deposits in foreign currency. He could have gone on merrily. The fraud, however, got exposed when a discounted cheque from Kola Mohan with the Andhra Bank for ₹ 1.73 million bounced. Kola Mohan had pledged with Andhra Bank the copy of a bond certificate purportedly issued by Midland Bank, Sheffields, London stating that a term deposit of 12.5 million was held in his name.

### **11.3.7 Mini-Case 7: An Indian Case of Intellectual Property Crime**

“Cybersquatting” is explained in Chapter 1 (Box 1.1). Also refer to Box 10.3 in Chapter 10. Satyam vs. Siffy is the most widely known case for that. Bharti Cellular Ltd. made a case in the Delhi High Court with a complaint that some cybersquatters had registered domain names such as barticellular.com and bhartimobile.com with network solutions under different fictitious names. The court ordered Network Solutions not to transfer the domain names in question to any third party and the matter was sub-judice. Similar issues were brought to various High Courts earlier. Yahoo had sued a man called Akash Arora for use of the domain name “Yahooindia.Com” deceptively similar to its “Yahoo.com.” As this case was governed by the Trade Marks Act 1958, the additional defense taken against Yahoo’s legal action for the interim order was that the Trade Marks Act was applicable only to goods. We know from Chapter 1 that intellectual property crimes include software piracy, copyright infringement, trademarks violations, theft of computer source code, etc. In other words, this is also referred to as cybersquatting.

### **11.3.8 Mini-Case 8: The Slumdog Millionaire Movie Piracy Case**

This incident was posted on 23 July 2009. A San Marcos man pleaded guilty to a felony charge of using the Internet to distribute a pirated copy of “Slumdog Millionaire” in violation of federal copyright law. Owen Moody, aged 25, pleaded guilty to uploading a copyrighted work being prepared for commercial distribution, admitting that he uploaded a copy of “Slumdog Millionaire” late 2008 to a website called thepiratebay.org, with the illicit desire that others could download the movie over the Internet. Moody also posted a link to the upload at the Internet websites called demonoid.com and mininova.org. At the time Moody uploaded the movie, it was in limited release in domestic theaters and was not yet available on DVD.

Moody used the Internet screen names “Tranceyo” and “Gizmothekitty.” He found the copy of “Slumdog Millionaire” on an Internet website called funfile.org, where someone had uploaded a digital copy of the movie that had been sent as an Academy Award “screener” to a member of the Academy of Motion Picture Arts and Sciences for voting consideration. When Moody searched the Internet, he realized the movie was not readily available to the general public. Moody then downloaded the movie from funfile.org and uploaded it to piratebay.org. He also created links to the movie on the two other websites, to make the movie available to the general public. Moody uploaded the movie from his home in San Marcos, the US. rights to “Slumdog Millionaire” under copyright ownership of Fox Searchlight Pictures, Inc., which is located in Los Angeles County. At that time, the movie was in limited release in domestic theaters and was not yet available on DVD. Moody pleaded guilty to the charge in front of the US District Judge Gary A. Feess in Los Angeles. Judge Feess scheduled to sentence Moody on 5 October 2009. In the US, if you upload a copyrighted work, such an act carries a statutory maximum penalty of 3 years in central prison and a \$250,000 fine or twice the gross gain or gross loss attributable to the offense, whichever is greater.

**Another case:** In first week of July 2009, a Ventura County man who obtained Academy Award screeners of “The Curious Case of Benjamin Button” and “Australia” pleaded guilty to uploading the films to the Internet. Derek Hawthorne, aged 21, of Moorpark, pleaded guilty to uploading a copyrighted work being prepared for commercial distribution. He was sentenced by the US District Judge R. Gary Klausner on 28 September 2009. The US Secret Service was involved in the investigation of cases running against Moody and Hawthorne.

### **11.3.9 Mini-Case 9: Malicious Hacking Case – Organ Donation Database Deleted**

Hackers are type II criminals (refer to Section 1.4, Chapter 1). As mentioned in that section and in Chapter 10, the typical “motives” behind cybercrime seem to be greed, desire to gain “power” and/or “publicity,” desire for revenge, a sense of adventure, looking for thrill to access forbidden information, destructive mindset, the desire to sell network security services. This is a real life example showing the consequences of computer hacking. We know that disgruntled employees tend to get into criminal acts, seen from the “motive” perspective of cybercrimes. The example shows the “data loss” considering the critical data and systems of an organization that were deleted in a criminal act; an act that was performed with malice and ill intentions.

This is a classic case of an “Insider attack” (recall the discussion in Chapter 9). It involved hacking a former employer’s computer network. In this case, the former IT Director of at a non-profit organ and tissue donation center was sentenced to 2 years in prison for hacking into her former employer’s computer network, announced Assistant Attorney General Lanny A. Breuer of the Criminal Division and US Attorney for the Southern District of Texas Tim Johnson.

The woman called Danielle Duann, aged 51, of Houston, pleaded guilty on 30 April 2009, to criminal indictment charging her with unauthorized computer access. Duann was sentenced to jail by US District Judge David Hittner in the Southern District of Texas. In addition to the 2-year prison term, Judge Hittner sentenced Duann to a 3-year period of supervised release following completion of her prison sentence and ordered her to pay \$94,222 in restitution to compensate her former employer for the damage that resulted from her actions.

While pleading guilty, Duann admitted that she had illegally accessed the computer network of LifeGift Organ Donation Center and then intentionally deleted organ donation database records, accounting invoice files, database and accounting software applications and various backup files, without authorization. LifeGift is the exclusive supplier of organ procurement services for more than 200 hospitals throughout 109 counties in North, Southeast and West Texas.

As per the court documents, LifeGift removed Duann from her position as their director of Information Technology on 7 November 2005, and revoked all of her previous administrative rights and access to the LifeGift computer network. In pleading guilty, Duann admitted that beginning of the evening of 7 November 2005, and continuing until 8 November 2005, she repetitively gained unlawful access to the LifeGift computer network via a remote connection from her home and intentionally caused damage by deleting numerous database files and software applications, as well as their backups, related to LifeGift’s organ and tissue recovery operations.

Duann further admitted that in an attempt to conceal her activities, she disabled the computer logging functions on several LifeGift computer servers and erased the computer logs that recorded her remote access to the LifeGift network. This case was investigated by the FBI and was jointly prosecuted by Trial Attorney Thomas Dukes of the Criminal Division’s Computer Crime and Intellectual Property Section and Special Assistant US Attorney Bret W. Davis of the US Attorney’s Office for the Southern District of Texas. This example emphasizes the point that the possibility of “insider attacks” should never be ignored and that

disgruntled employees do have the potential to cause damage to their organizations. Systems Administrators as professionals possess tremendous amount of technical knowledge about how computer systems perform and, as this example shows, it can get put to malignant use with their motive to settle their personal scores!

*Source: www.usdoj.gov (12 May 2010).*

### 11.3.10 Mini-Case 10: The Case of Counterfeit Computer Hardware

This is a slightly different kind of case reported on 3 December 2009. Christopher Myers, aged 40, and Timothy Weatherly, aged 27 were charged with conspiracy, trafficking in counterfeit goods and smuggling in counterfeit labels. In 2003, Myers founded a company called Deals Express. He conspired with Weatherly, who in 2005 established a company called Deals Direct, Inc to import counterfeit Cisco brand computer hardware from China. For making the hardware look genuine they attached fake Cisco labels to the components and packaged them in counterfeit Cisco boxes along with counterfeit Cisco manuals.

Myers and Weatherly arranged to have the counterfeit components despatched from China to various shipping addresses in Kansas State, including self-storage facilities in Lenexa, Merriam, Mission, Overland Park, and Kansas City, KS, as well as UPS stores in Seattle, WA, and Portland, OR. In November 2005, shipments of counterfeit goods were confiscated in Louisville, KY, Los Angeles, CA and Wilmington, OH. These seized goods included counterfeit hardware items such as network cards, connectors, manuals, labels and boxes. In August 2005, Weatherly established a website for Deals Direct and began using eBay to sell counterfeit Cisco products under the name "direct2technology." Myers and Weatherly made suggestions to their suppliers in Shenzhen, China, and Hong Kong for adjustments to the products to make them appear more authentic. After these counterfeit goods were seized, the defendants made various changes in their shipping arrangements in an attempt to avoid detection, including change of shipment address and having counterfeit goods shipped through other countries including Sweden.

Myers and Weatherly, upon conviction, would face a maximum penalty of 5 years in federal prison and a fine up to \$250,000 on the conspiracy charge and a maximum penalty of 10 years and a fine up to \$2 million on each of the trafficking counts. Immigration and Customs Enforcement and the National Bureau of Investigation worked on the case. Assistant US Attorney Scott Rask prosecuted the case. Legal professionals would know that defendants are considered not guilty until and unless they are proven guilty. The charges filed merely contain accusations of unlawful conduct.

### 11.3.11 Mini-Case 11: The Chinese Case of Trade Secret Stealing Involving an E-Waste Company

This case was published in September 2009 by the US Department of Justice. A citizen of the People's Republic of China was charged in connection with the scheme devised to steal trade secrets and proprietary information relating to computer systems and software with environmental applications from his New Jersey employer, Acting US Attorney Ralph J. Marra, Jr., announced. The indictment charges Yan Zhu, aged 31, a.k.a. "Wesley ZHU," a.k.a. "Westerly Zhu," who resides in Lodi, with conspiracy to steal trade secrets and wire fraud. On the morning of 9 April 2009, FBI Special Agents arrested Zhu at his residence while he was in the US on a work visa. Later that day, the defendant Zhu made an initial appearance in federal court in front of US Magistrate Tonianne J. Bongiovanni. The Magistrate released the defendant Zhu on a \$200,000 secured bond. Zhu was later arrested on the accusation in Federal Court after the case was assigned to a US District Judge.

The indictment describes a scheme in which Zhu, along with other unindicted co-conspirators, used his employment with a business, which is identified in the indictment only as "Company A," to obtain access to the

company's trade secrets and proprietary and confidential information relating to computer software developed for the Chinese market. According to the charges made against Zhu, he (i.e., Zhu) worked with Company A as a senior environmental engineer from May 2006 until his termination in July 2008. Company A is a software development and consulting company with its principal office in Mercer County. The company is in the business of developing supporting, and implementing software and computer systems for ecological applications.

While in the services of Company A, Zhu worked on a comprehensive hazardous waste information management system that Company A developed for the Chinese market. The purpose of this product was to allow a Company A customer, such as an environmental regulatory agency, as well as entities that interact with the environmental regulatory agency, such as hazardous waste producers and shippers, to enter, organize and view certain data regarding pollution and hazardous waste within that agency's jurisdiction. In addition, it was alleged that Zhu worked on Company A database application that was related to this software system.

The allegation further stated that Zhu operated his scheme with at least two co-conspirators, identified only as Co-conspirators 1 (CC-1) and 2 (CC-2), both Chinese nationals residing in China. According to the indictment, CC-1 had been introduced to Company A through Zhu and hired as Company A's sales representative in the Science and Technology High-Tech Zone in Xian City, Shanxi Province, China. Company A rented office space in Xian City. From this office CC-1 represented Company A and hosted the subject software on his/her own computer system. The charges filed allege that Zhu, CC-2 and CC-1, were all associated with a company known only as "Company X," an environment-related software company in China.

It is further alleged that Zhu and his co-conspirators exploited the trust placed in Zhu by Company A by stealing Company A's trade secrets and proprietary and confidential business information, and exploiting an opportunity for Company A to market its product to the Chinese government. The indictment also alleges that, as early as January 2008, Zhu began sending Company A's computer software source code to CC-2 in China. Eventually, the Indictment alleges, the co-conspirators used this computer source code to develop a modified version of the Mercer County company's software in China, which was marketed under the Company X banner. It is further alleged that the co-conspirators took control of the Mercer County company's office in China, and used that space to conduct business for Company X. According to the indictment, Zhu was terminated on 17 July 2008, in part because Company A became aware that Zhu had sent Company A trade secret and confidential and proprietary information to his personal E-Mail account.

The charge of conspiracy to steal trade secrets carries a maximum penalty of 10 years in prison and a fine of \$250,000 or twice the aggregate loss to the victims or gain to the defendants. Each count of wire fraud carries a maximum penalty of 20 years in prison and a fine of \$250,000 or twice the aggregate loss to the victims or gain to the defendants. Despite the accusation, the defendant is presumed innocent unless proven guilty beyond a reasonable doubt. Marra credited Special Agents of the FBI's Trenton Resident Agency, under the direction of Special Agent in Charge Weysan Dun in Newark, with the investigation leading to the indictment. The government was represented by Assistant US Attorney Eric M. Schweiker of the Criminal Division in Trenton.

### **11.3.12 Mini-Case 12 – Internet Used for Murdering**

Refer to Section 8.6 "An Illustration on Real Life Use of Forensics" in Chapter 8 to read this case.

### **11.3.13 Mini-Case 13: Social Networking Victim – MySpace Suicide Case**

This is about "MySpace" suicide case reported in the New York Times. "Myspace" is a social networking sites. In Section 7.14 of Chapter 7 there is a discussion about social networking sites and the potential security/privacy threats arising from them. In that section, there was the mention about *a mother convicted of computer fraud for her involvement in creating a phony account on MySpace to trick a teenager, who later*

*committed suicide.* This case shows that social networking sites, though popular, can result in someone losing his/her precious life, as this real-life case reveals. This case, (a real-life story) was reported in New York Times and posted on 26 November 2008. It is a sad story of the family members and friends of the teenaged girl who lost her life. She was a victim of social networking. Megan Meier, aged 13, committed suicide in October 2008. Apparently, the suicide was caused by cruel messages she received on the social networking site "Myspace." This incidence, in a way, is also sad reality in a "boyfriend-oriented culture."

Readers, who have not yet read previous chapters, may like to read about cyberbullying in Box 2.8 of Chapter 2. According to the legal experts in the US, this was country's first cyberbullying verdict, in which a Missouri woman was convicted of three misdemeanor charges of computer fraud for her involvement in creating a phony account on MySpace to trick a teenager, who later committed suicide. The accused, Ms. Lori Drew went through a 5-day trial. During the trial, prosecutors portrayed Ms. Lori Drew had worked in collusion with her daughter, Sarah, aged 13 at that time, along with Ms. Ashley Grills, a young family friend and also an employee of Ms. Lori Drew's magazine coupon business in Dardenne Prairie. The testimony showed that they "created" a teenage boy, "Josh Evans," as an identity on MySpace. The conspiracy was to make this pseudo character (created on MySpace) to communicate with Sarah's rival, Megan Meier, who was also 13 years old then. Megan was known to have a history of depression and suicidal impulses. According to testimony at the trial there were weeks of online courtship with "Josh." Megan was distressed one afternoon in October 2006, when she received an E-Mail message from "Josh" saying that "*The world would be a better place without you.*"

Ms. Ashley Grills, who is now 20, testified (under an immunity agreement) that shortly after that message was sent, Megan wrote back, "*You're the kind of boy a girl would kill herself over.*" Totally depressed having such a message from her boyfriend (in reality only a pseudo character on MySpace) Megan hanged herself that same afternoon in her bedroom. The jury appeared to reject the government's contention that Ms. Lori Drew had intended to harm Megan. However, the convictions signaled the 12-member Jury's belief that she had, nonetheless, violated federal laws that prohibit gaining access to a computer without authorization. Readers will recall that in Chapter 1, there is discussion about "unauthorized access to computer" (Sections 1.3–1.5 and Table 1.5). Specifically, the jury found Ms. Lori Drew culpable of illegally accessing a computer system on three occasions, in reference to the fraudulent postings on MySpace in the name of "Josh Evans."

The federal Computer Fraud and Abuse Act was passed in 1986 in the US and has been amended several times since then. According to legal and computer fraud experts, the application of the law appeared to be expanding with technology and the growth of social networking on the Internet. In general, prosecutions under the act have been associated with people who are computer systems hackers. Until recently, social networking sites such as MySpace did not exist. Therefore, this case would be simply another important step in the expanded use of this statute to protect the public from computer crime. Although it was unclear how severely Ms. Lori Drew would be punished, the jury reduced the charges to misdemeanors from felonies, and no sentencing date was set. According to computer fraud experts, the conviction was highly significant as it was the first time that a federal statute designed to combat computer crimes was used to prosecute what were essentially abuses of a user agreement on a social networking site.

Under federal sentencing guidelines, Ms. Lori Drew could face up to 3 years in prison and \$300,000 in fines, even though she had no previous criminal record. Her lawyer asked for a new trial. While this is a case from another country, it is a lesson for all of us. This case sends an overwhelming message to users of the Internet and social networking sites.

### 11.3.14 Mini-Case 14: State of Tamil Nadu vs. Suhas Katti Case

Cyberdefamation was addressed in Chapter 1 and that is the concept reference in this fairly well-known and a truly landmark case. It is considered to be India's First cybercrime conviction. People's perception is

that conviction takes a very long time in the jurisdiction. However there are exceptions as seen in this case. This well-known case of Suhas Katti (year 2004) is available in the public domain. It is noteworthy for the fact that the conviction was achieved successfully within a relatively short time of 7 months from the date of filing of the FIR (First Information Report). The case illustrates how the Indian IT was used to file the case. Similar cases have been awaiting judgment in other states for a much longer time. This case had a relatively more efficient handling in the sense that this was the first case of the Chennai Cybercrime Cell going to trial. Therefore, it deserves a special mention.

This case involves posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also sent to the victim for information by the accused. However, this was done through a false E-Mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was said to be interested in marrying her. She, however, married another person. Later, the wedding ended in a divorce, and the accused once again started making contacts with the lady. On her reluctance to marry him, the accused took up the harassment through the Internet. On 24 March 2004, a charge sheet was filed under Section 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore by citing 18 witnesses and 34 documents and material objects. Prosecution examined 12 witnesses and complete documents were marked as "Exhibits."

The Defense argued that the offending mails would have been given either by ex-husband of the complainant or the complainant herself to implicate the accused as accused alleged to have turned down the request of the complainant to marry her.

Further, the Defense Counsel argued that some of the documentary evidence was not sustainable under Section 65B of the Indian Evidence Act. However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the cybercafe owners and came to the conclusion that the crime was conclusively proved. The judgment was submitted in May 2004 as stated below:

*"The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo rigorous imprisonment for 2 years under 469 IPC and to pay fine of Rs. 500/- and for the offence under Section 509 IPC sentenced to undergo 1 year simple imprisonment and to pay fine of Rs. 500/- and for the offence under Section 67 of IT Act 2000 to undergo rigorous imprisonment for 2 years and to pay fine of Rs. 4000/-."*

The accused paid the fine amount and was lodged at Central Prison, Chennai. This is considered as the first case convicted under Section 67 of ITA 2000 in India.

**IMPORTANT NOTE –** *The information contained in this case is meant for informational purpose only and is based on material available in public domain. Authors do not make any claim about its accuracy or authenticity. The name of the victim is masked to protect identity.* The information provided here is based on the extracts from the Judgment pronounced in the First Cybercrime Conviction in India.

### 11.3.15 Mini-Case 15: Pune Citibank MphasiS Call Center Fraud

BPO and call center business is growing in India has become a popular destination for outsourcing back-office work. This case involves a BPO scenario and is an eye opener. US\$ 3,50,000 belonging to four US customers were fraudulently transferred to fake accounts. This was enough to give ammunition to those

lobbying against outsourcing of work from the US to other countries; especially to India. Such cases are not uncommon but media likes to focus on them when it happens in India. It is a case of sourcing engineering, also known as “social engineering.” Some employees gained customer confidence and obtained their PIN numbers to commit fraud. They got these under the guise of helping the customers out of difficult situations. Highest security prevails in the call centers in India as they know that they will lose their business. There was not as much of breach of security but of sourcing engineering/social engineering.

As an industry practice in security, the call center employees are checked when they go in and out of the work place. This is done to ensure that they do not copy down numbers or any other business confidential information. However, in this case, the employees of the call center must have remembered these numbers, gone out immediately to a cybercafe and accessed the Citibank accounts of the customers. All accounts were opened at Pune. The customers lodged a complaint that the funds from their accounts were transferred to Pune accounts. This is how the criminals were traced. Police were able to prove the honesty of the call center and has frozen the accounts where the money was transferred.

The ISO 27001 standard for information security recommends many controls and one such control is about HR checks. As a best practice, there should be strict background check of the call center executives. However, even the best of background checks cannot fully eliminate the bad elements from coming in and breaching security. We must still ensure such checks when a person is hired. There is need for a national ID and a national database where a name can be referred to. In this case first round of investigations did not disclose that the criminals had any criminal history. Customer education is crucial so that customers are not taken for a ride. Most consumers may feel that banks are guilty of not doing this.

### 11.3.16 Mini-Case 16: NASSCOM vs. Ajay Sood and Others

Phishing is explained in Chapter 5 – this case is to be read in that context. The petitioner in this case was the National Association of Software and Service Companies (NASSCOM), India’s premier software association. The defendant was Ajay Sood & Others and the case was delivered in March 2005. In this case, the Delhi High Court declared “Phishing” on the Internet to be an illegal act, entailing an injunction and recovery of damages.

The court elaborated on the concept of “Phishing,” in order to lay down a precedent in India. The court stated that it is a form of Internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company, in order to extract personal data from a customer such as access codes, passwords, etc. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party’s advantage. The court also stated, by way of an example, that typical Phishing scams involve persons who pretend to represent online banks and siphon cash from E-Banking accounts after conning consumers into handing over confidential banking details.

According to the Delhi High Court, even though there is no specific legislation in India to penalize Phishing, it held that Phishing to be an illegal act by defining it under Indian law as “*a misrepresentation made in the course of trade leading to confusion as to the source and origin of the E-Mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused.*” The court held the act of Phishing as passing off and tarnishing the plaintiff’s image.

The defendants were running a placement agency engaged in providing head-hunting and recruitment services. In order to obtain “personal data,” which they could use for purposes of head-hunting, the defendants composed and sent E-Mails to third parties in the name of NASSCOM. The high court recognized the trademark rights of the plaintiff and passed an ex-parte ad interim injunction restraining the defendants

from using the trade name or any other name deceptively similar to NASSCOM. The court further ordered the defendants not to hold themselves out as being associates or a part of NASSCOM. For readers not savvy with legal terms – “Ex–parte” means on behalf of only one party, without notice to any other party. For example, a request for a search warrant is an ex parte proceeding, since the person subject to the search is not notified of the proceeding and is not present at the hearing.

The court appointed a commission to conduct a search at the defendants’ premises. Two hard disks of the computers, from which the fraudulent E–Mails were sent by the defendants to various parties, were taken into custody by the local commissioner appointed by the court. The offending E–Mails were then downloaded from the hard disks and presented as evidence in court. During the progress of the case, it became clear that the defendants, in whose names the offending E–Mails were sent, were fictitious identities created by an employee on defendants’ instructions, to avoid recognition and legal action.

On discovery of this fraudulent act, the fictitious names were deleted from the array of parties as defendants in the case. Later, the defendants admitted their criminal acts and the parties settled the matter through the recording of conciliation in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of ₹ 1.6 million to the plaintiff as damages for violation of the plaintiff’s trademark rights. The court also ordered the hard disks seized from the defendants’ premises to be handed over to the plaintiff who would be the owner of the hard disks.

This case achieves clear milestones (a) It brings the act of “Phishing” into the ambit of Indian laws even in the absence of specific legislation. (b) It demonstrates a point – the perception that there is no “damages culture” in India for violation of IP rights is *not* true. This case reaffirms Intellectual Property owners’ faith in the Indian judicial system’s ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.

### 11.3.17 Mini-Case 17: Indian Case of Cyberdefamation

This is another well-known case available in the public domain. Though an old case, it is considered to be India’s first case of cyberdefamation, in which a Court of Delhi assumed jurisdiction over a matter where a corporate’s reputation was being defamed through E–Mails and passed an important ex–parte injunction. For readers who do not come from legal background, *ex–parte* is a Latin legal term meaning “from (by or for) one party.” An *ex–parte decision* is one decided by a judge without requiring all parties to the controversy to be present. According to legal doctrines in Australia, Canada, the UK, India and the US, “ex–parte” means a legal proceeding brought by one person in the absence of and without representation or notice of other parties. It is also used as a slack reference to unacceptable one-sided contacts with a court, arbitrator or represented party without notice to the other party or counsel for that party.

The Delhi High Court conceded an ex–parte ad interim order in the case entitled “SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra” being Suit No. 1279/2001. This matter was handled by one of India’s leading cyberlawyers. The defendant Jogesh Kwatra was an employee of the plaintiff company. He started sending defamatory, derogatory, vulgar, filthy, obscene and abusive E–Mails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R.K. Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory E–Mails to the plaintiff.

Arguing on behalf of the plaintiffs, the cyberlawyer handling the case contended that the E–Mails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature. The lawyer further argued that the aim of sending the said E–Mails was to malign the impeccable reputation of the plaintiffs all over India and the world. The lawyer further contended that the acts of the defendant in sending the E–Mails had resulted in invasion of legal rights of the plaintiffs. Further, it was argued that the

defendant is under a duty not to send the aforesaid E-Mails. After the claimant company made a discovery that the said worker of their organization was possibly involved in the act of sending offensive E-Mails, the claimant terminated the services of the defendant.

After hearing detailed arguments of the lawyer, Honorable Justice J.D. Kapoor of the Delhi High Court passed an ex-parte ad interim injunction observing that a *prima facie* case had been made out by the plaintiff. As a result, the Delhi High Court stopped the defendant from sending defamatory obscene derogatory, humiliating, vulgar and abusive E-Mails either to the plaintiffs or to its associate companies and/or sister concerns all over the world including their Managing Directors and their Sales and Marketing departments. In addition, Honorable Justice J.D. Kapoor also stopped the defendant from transmitting, publishing, or causing to be published any information in the physical world as well as in cyberspace which is deprecating or slanderous or offensive to the plaintiffs.

The matter was posted for 4 October 2001. This decree by Delhi High Court has remarkable meaning because this is for the first time that an Indian Court assumes authority in a matter concerning cyberdefamation and grants an ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene E-Mails either to the plaintiffs or their subsidiaries.

### **11.3.18 Mini-Case 18: Indian Cases of Cybersquatting**

The term “cybersquatting” is explained in Chapter 1 (Box 1.1). It is reproduced here again for reader’s quick reference to understand the examples presented below. “Cybersquatting” means *registering a popular Internet address – usually a company name – with the aim of selling it to its lawful owner*. After presenting the short examples, we have summarized the learning points.

#### *Yahoo Inc. vs. Akash Arora Case of Cybersquatting*

This is probably the first reported Indian case wherein the plaintiff (the person who lodges the complaint) is the registered owner of the domain name yahoo.com and the plaintiff succeeded in obtaining an interim order restraining the defendants and agents from dealing in service or goods on the Internet or otherwise under the domain name yahooindia.com or any other trademark/domain name which is misleadingly analogous to the plaintiffs trademark Yahoo. As on the date of writing this, there are only a small number of reported judgments in our country; however, newspaper reports and information from dependable sources indicate that there are at least 25 disputes pertaining to domain names pending before the Delhi High Court itself. Refer also to the mini-case under Section 11.3.7.

#### *Tata Sons Ltd vs. Ramadasoft Case of Cybersquatting*

This cybersquatting case involved Tata Sons Ltd vs. Ramadasoft. Tata Sons is the holding company of India’s largest industrial corporation, the Tata Group. Tata Sons won a case to evict a cybersquatter from 10 contested Internet domain names. Tata Sons had filed a complaint at the World Intellectual Property Organization. The respondent was proceeded ex-parte. As explained earlier, an *ex-parte decision* is one decided by a judge without requiring all of the parties to the controversy to be present. The board reached a conclusion that the respondent owns the domain names. These domain names are confusingly similar to the complainant’s trademark TATA, and the respondent has no rights or legitimate interests in respect of the domain names, and he has registered and used the domain names in bad faith. These facts permit the plaintiff to an order transferring the domain names from the respondent.

### *SBI Cards and Payment Services Private Limited vs. Domain Active Pty. Limited*

This is the case that involved SBI Cards and Payment Services Private Limited vs. Domain Active Pty. Limited. Sbicards.com was ordered by the World Intellectual Property Organization (WIPO) to be transferred to the Indian Company from an Australian entity, which hijacked the domain name hoping to later sell it for a hefty sum to the State Bank of India subsidiary. The panel accepted SBI Card counsels argument that the Australian company was in the business of buying and selling domain name through its website.

### *Mahindra & Mahindra Limited (M&M) Case*

Yet another Indian instance of cybersquatting involved Mahindra & Mahindra Limited (M&M). In this case, a young student residing in Andhra Pradesh registered the domain names mahindra.com, mahindra.net and mahindra.org, in his name. M&M made an appeal to the WIPO saying that they had registered the name "Mahindra" as the registered trademark in India and the US. As per the order passed by the panelists, the domain names were to be immediately transferred in favor of the Indian company.

### *Titan Industries Ltd. vs. Prashanth Koorapati and Others*

In this case of Titan Industries Ltd. vs. Prashanth Koorapati & Ors., the Delhi High Court sanctioned an ex-parte ad interim restriction (i.e., in the meantime) to restrain the defendants from using the name TANISHQ on the Internet or otherwise and from committing any other act as is likely to lead to passing off of the business and goods of the defendants as the business and goods of the plaintiff.

### *Bennett Coleman & Co Ltd. vs. Steven S Lalwani Case*

This is another interesting case of cybersquatting. Since 1996, the complainant has been holding the domain name www.economictimes.com, for electronically publishing it in newspapers. The plaintiff had registered in India this mark for literary purposes. However, in 1998, Steven S. Lalwani, US, registered the same domain name.

The WIPO judgment made it clear that the complainant have a very substantial reputation in their newspaper titles arising from their daily use in hard copy and electronic publication. It was also firmly held that the registration and use of the domain names by the respondents is not in good faith in that their use meant an intentional attempt to attract (with commercial gain as the purpose), Internet users to their websites by creating a possibility of misunderstanding with the complainants marks as to the source, sponsorships, affiliation or endorsement of those websites and the services on them.

### *Rediff Communication Limited vs. Cyberbooth Case*

In Rediff Communications Ltd. vs. Cyberbooth, petitioner, the proprietor of the well-known portal and domain name rediff.com filed for embargo against the defendant, registrant of the domain name rediff.com. The Judge was convinced that there was a clear intention to deceive and granted interim relief to the plaintiff. The judge affirmed that a "domain name" is more than an Internet address and is entitled to as much protection as that provided for a trademark.

The terms IPR, Copyright, Trademark, Trade secret, etc. are explained in Ref. #1, Books, Further Reading and also in Chapter 10 (Section 10.2). The discussion here assumes that readers are familiar with these terms.

If not, we recommend readers to refer to the said chapter of the book mentioned. To know about Indian Trademark Law, we have provided links in Ref. #71, Additional Useful Web References, Further Reading. The various statutes dealing with Intellectual Property Laws in India are as follows:

1. Trademarks Act 1999 (see Appendix S).
2. Copyright Act 1957 (see Appendix T).
3. Patents Act 1970 as amended by Patents (Amendments) Act 2005 (see Appendix R).
4. Designs Act 2005.
5. Code of Civil Procedures 1908.
6. Indian Penal Code 1860 (see Appendix P).
7. Geographical Indication of Goods (Registration & Protection) Act 1999.
8. Semiconductor, Integrated Circuit Layout Design Act 2000.
9. Plants Varieties Protection and Farmers' Rights Act 2001.
10. Information Technology Act 2000 (see Appendix O).

From the cybersquatting examples described so far, note the following points:

1. The trademark law has been drastically broadened to accommodate domain name disputes. However, in author's opinion, the trademark law should not be too widely broadened to confer upon trademark owners the rights that they otherwise are not entitled to. The tricky question is whether the law will eventually give large trademark owners property rights in domain names, that is, the ability to exclude others from using them. In deciding how far the trademark laws should reach, it may become essential to revisit the rationale behind trademark protections. Trademark protection is meant to provide consumers with exact information about the merchandise and services presented by the mark, and to provide incentives to companies so that they become interested in investing in their marks and also to enhance quality control. Trademarks, therefore, lower consumer search costs and promote the economic functioning of the market. "Marks" themselves are not protected, but the law protects the goodwill the marks embody.
2. Allowing exclusive rights in domain names will put off companies from using names that are already used. Conventional financial explanation for trademark law rests on the premise that there is an countless number of marks available. However, there are only a limited number of domain names available.
3. One more area of concern with such a right is that it would allow trademark owners to preclude others from using not only one but several marks. It is now a general practice for companies to register all possible domain names they can think of, that contain their company name. For example, Exxon currently holds the rights of over more than 120 domain names incorporating the word "EXXON."
4. The current law seems to endorse protection of large companies more, that is, those who want rights in every possible variations of their name.
5. From a realistic point of view, the current expansion in law gives trademark owners a significant amount of leverage. For example, often people with genuine interests in their domain names cannot pay for fighting with trademark owners. Naturally, this will force many to simply turn over their rights in order to avoid corporate bullying.

Do refer to the "Intellectual Property in the Cyberspace" discussion in Section 10.2 of Chapter 10 – that discussion will provide greater details of IP.

### 11.3.19 Mini-Case 19: Swedish Case of Hacking and Theft of Trade Secrets

Stealing of IPR/trade secrets is one of the major threats to industries and individuals in the modern era. Here is a real-life scenario on that. Two well-known organizations co-operated with Government for the investigation of this case.

Philip Gabriel Pettersson, a.k.a. Stakkato, aged 21, a Swedish national, was indicted on 17 May 2009 on the grounds of intrusion and trade secret theft charges. This was announced by the US Attorney for the Northern District of California and the Justice Department's Criminal Division.

The charges included one intrusion attempt and two attempts of trade secret misappropriation involving Cisco Systems Inc. (Cisco), San Jose, CA, a provider of computer network equipment and producer of Internet routers. As per allegations in the condemnation, Pettersson purposely committed an intrusion between 12 May 2004 and 13 May 2004 into the computer system and network of Cisco. It was alleged that during the suspected intrusion, some Cisco Inter-network operating system code was misappropriated. The accusation also included two intrusion attempts involving the National Aeronautics and Space Administration (NASA), including computers at the Ames Research Center and the NASA Advanced Supercomputing Division, located at Moffett Field, CA. The accusation alleges Pettersson committed these intrusions on 19 May 2004, 20 May 2004 and 22 October 2004.

Cisco and NASA cooperated in the government's investigation. Following the incident, Cisco reported that they could not believe that any customer information, partner information or financial systems were affected. The Department of Justice worked in cooperation with the Swedish authorities on this case. From legal perspective, it is to be noted that an indictment is merely an accusation. All defendants are presumed innocent until proven guilty at trial beyond a reasonable doubt. The maximum penalty for each charge of intrusion and theft of trade secrets is 10 years in prison, a 3-year term of supervised release, and a fine of \$250,000.

The prosecution was the result of an investigation by the FBI; US Secret Service; NASA Office of Inspector General, Office of Investigations, Computer Crimes Division; and numerous additional federal agencies. A senior officer at the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) prosecuted the case with assistance from other officers. CCIPS Senior Counsel also assisted in the prosecution. The Criminal Division's Office of International Affairs assisted on international coordination issues in the case.

*Source:* [www.cybercrime.gov](http://www.cybercrime.gov)

### 11.3.20 Mini-Case 20: IPR Violation

Intellectual property stealing is mentioned in Chapters 1 and 9. Intellectual Property in the Cyberspace is explained in Chapter 10 (Section 10.2). This example involves a counterfeit software program. Below is explained how this crime happened in real life.

On 12 June 2009, Rodolfo Rodriguez Cabrera, aged 43, a Cuban national, and Henry Mantilla, aged 35, of Cape Coral, FL, were accused about a plot to manufacture and sell fake International Game Technology (IGT)-brand video gaming machines, commonly known as "slot machines," and counterfeit IGT computer programs. Cabrera was arrested on 8 June 2009, based on the indictment. Mantilla was scheduled to appear based on a summon in the US District Court for the District of Nevada on 2 July 2009.

As per the indictment, Cabrera was the owner as well as operator of a company called FE Electronic in Riga, Latvia, and Mantilla owned and operated a company named Southeast Gaming Inc., in Cape Coral, FL. The indictment makes an allegation that during the period that spanned between August 2007 and 15 April 2009, Cabrera and Mantilla were part of the conspiracy that involved making illegal copies of IGT

video gaming machine computer programs, placing counterfeit labels bearing IGT's registered trademark on the computer programs, installing the counterfeit computer programs in IGT gaming machine cabinets and then sell the counterfeit computer programs and gaming machines through their respective companies. They did all this without the permission of the trademark and copyright owner, IGT.

The charge against Cabrera and Mantilla indicated that they were involved with a conspiracy of trafficking in counterfeit goods, trafficking in counterfeit labels and criminal copyright infringement. If convicted of all charges, each defendant faces a maximum of up to 45 years in prison and \$5.25 million in fines. The accusation also contains 13 penalty allegations that require the defendants, if convicted, to forfeit any and all counterfeit items and to forfeit up to \$5 million in proceeds from their alleged criminal activity.

The case was investigated by the FBI and prosecuted by Assistant US Attorney of the US Attorney's Office for the District of Nevada and Trial Attorney of the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS). Significant assistance came in this case from the Central Criminal Police Department of the Latvian Ministry of Interior; Latvia's Office of the Prosecutor General, International Cooperation Division; and Senior Trial Attorney Deborah Gaynus of the Criminal Division's Office of International Affairs. CCIPS Trial Attorney also assisted with the prosecution. IGT also provided assistance in this matter. An indictment is merely a formal charge by the grand jury. As legal professionals know, a defendant is assumed to be innocent unless and until proven guilty in a court of law.

*Source:* [www.usdoj.gov](http://www.usdoj.gov)

### 11.3.21 Mini-Case 21: Indian E-Mail Spoofing Case

This is a case registered by the Indian police as the first case of cyberstalking in Delhi. To maintain confidentiality and privacy of the entities involved, we have masked their names. Mrs. Joshi received almost 40 calls in 3 days mostly at odd hours from as far away as Kuwait, Cochin, Bombay and Ahmedabad. These calls created havoc in the personal life destroying mental peace of Mrs. Joshi. She decided to register a complaint with Delhi Police. A person was using her ID to chat over the Internet at the website [www.mirc.com](http://www.mirc.com), mostly in the Delhi channel for 4 consecutive days. The person was chatting on the Internet, using her name and giving her address, talking in profane language. The same person was also deliberately giving her telephone number to other chatters encouraging them to call Mrs. Joshi at odd hours.

While "cyberstalking" does not have a standard definition, it means threatening, unwarranted behavior or advances directed by one person toward another person using Internet and other forms of online communication channels as medium.

This ends all the mini-cases of this section and now we move on to illustrations of financial crimes in the banking domain including the credit card frauds.

## 11.4 Illustrations of Financial Frauds in Cyber Domain

In this section, we have provided illustrations of banking frauds (including credit card-related crimes), online gambling, IPR crimes, digital media piracy, hacking, computer frauds, website attacks, counterfeit hardware, malicious use of the Internet, social networking victims, etc. Table 11.3 lists the illustrations provided in this section.

### 11.4.1 Banking-Related Frauds

#### *Illustration 1: Stolen Credit Card Information*

In the introduction section, it was mentioned that cybercriminals operate beyond geographic boundaries. With the background of credit card frauds addressed in Chapter 5 (under "Phishing"), this case is interesting to read.

**Table 11.3** | List of illustrations in Section 11.4

<i>Illustration No.</i>	<i>Title</i>	<i>Topic</i>	<i>Chapter Cross-Reference</i>
1	Stolen Credit Card Information	Phishing and credit card frauds (banking frauds)	Chapter 5
2	Phishing Incidence	Phishing (credit card frauds)	Chapter 5
3	Online Credit Card Theft Ring	Credit card frauds	Chapter 5
4	Understanding Credit Card Fraud Scenarios	Credit card frauds	Chapter 5
5	ShadowCrew – the Internet Mafia Gang	Credit card frauds	
6	Dirty Relations – Goods Delivery Fraud	Frauds from online purchasing	—
7	Fake Mails Promising Tax Refunds: Beware	Internet banking	Chapters 2 and 4
8	Phone Scam Targets Your Bank Account	DoS (denial-of-service) attack	Chapters 1, 3 and 4
9	Cookies and Beacons – The Facebook Controversy	Cookies and Beacons	—
10	Privacy Loss through Leakage of Users' Facebook Profiles	Personal privacy loss leading to cybercrimes	Chapter 5
11	Debit Card Frauds – Global Wave in Real Life	Financial frauds with debit card	—

Stolen credit card information is savored by cybercriminals. “DarkMarket” is an English-speaking Internet cybercrime forum created by Renukanth Subramaniam in London. It was shut down in 2008 after an FBI agent infiltrated it, leading to more than 60 arrests worldwide. Renukanth Subramaniam admitted conspiracy to defraud and was sentenced to nearly 5 years in prison in February 2010. The website permitted buyers and sellers of stolen identities and credit card data to meet on the Net and establish a criminal enterprise in an entrepreneurial, peer-reviewed environment. It had 2,500 users at its peak, according to the FBI.

To the casual observer, there was not much to differentiate the Java Bean Internet cafe in Wembley from the hundreds of others in the capital. But to the surveillance officers staking it out month after month, this ordinary looking venue was the key to busting an astonishing and complicated network of cybercriminals. There were many computers inside the café and a former pizza bar employee ran an international cyber “supermarket” for selling stolen credit card and account details, costing the banking industry tens of millions. Renukanth Subramaniam, aged 33, was revealed as the founder and a major “orchestrator” of the secret – “DarkMarket website,” where elite fraudsters bought and sold personal data, before it was infiltrated by the FBI and the US Secret Service. Membership to DarkMarket was strictly by invitation. But once vetted, its 2,000 sellers and buyers traded the whole lot – from card details (obtained through hacking, Phishing attacks – visit Chapter 5 for details of “Phishing” and ATM skimming devices), to viruses using which buyers could extract money by threatening company websites. This top cybercrime site in the world offered online tutorials in illicit topics such as account takeovers, credit card deception and money laundering. There were equipments such as false ATM, pin machines as well as everything needed to set up a credit card factory.

Subramaniam, a Sri Lankan-born British citizen, was a past member of ShadowCrew’s predecessor. Subramaniam worked at Pizza Hut and as a dispatch courier. In 2004, the US Secret Service uncovered ShadowCrew. “JiLsi” was one of the uppermost cybercriminal in the country. With this criminal, Subramaniam managed to set up a forum globally. Without JiLsi, DarkMarket was just not possible – that was the close association and deep involvement that JiLsi had with DarkMarket. In spite of this being

so, DarkMarket's 2,000 members could never meet JiLsi in real life – he truly was a “shadow operator”! Somehow, DarkMarket was finicky about banning “rippers” who would deceive other criminals. Honor among thieves was paramount. Subramaniam was one of the top administrators. He stored his operating system on memory sticks. But when one of his memory sticks was stolen, it cost him £100,000 in losses. It also resulted in compromising the site’s security. With this mishap, Subramaniam was downgraded to merely a reviewer. Surveillance officers trapped him logging on to the website when JiLsi was unaware that the fellow criminal MasterSplyntr whom he trusted was, in fact, an FBI agent called Keith Mularski.

### *Illustration 2: Phishing Incidence*

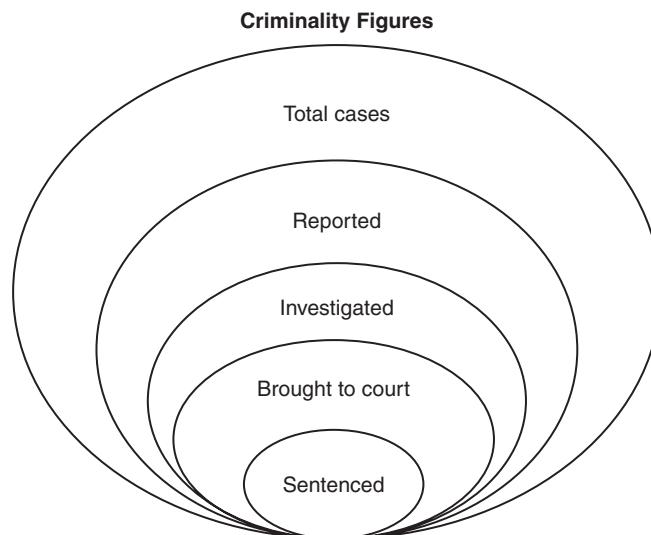
*Phishing* is explained in Chapter 5 and here is an illustration of Phishing attack in real life. According to the news posted on 14 April 2010 (Ref. #72, Additional Useful Web References), it could well be termed India’s first legal adjudication of a dispute raised by a victim of a cybercrime. The judgment for the first case was filed under the IT Act. In this judgment, Tamil Nadu’s IT Secretary ordered ICICI Bank to pay ₹ 12.85 lakhs (₹ 12,85,000) to an Abu Dhabi-based NRI within 60 days – in compensation for the loss suffered by him as a result of a Phishing fraud. Phishing is an Internet fraud through which cybercriminals illegally obtain sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity.

In this case, the reimbursement, that is the compensation, included the loss suffered by the supplicant, the travel expenses and the financial loss incurred due to “complete lack of involvement of the respondent bank – as per order from Tamil Nadu’s IT Secretary. The order came based on an appeal (i.e., petition) that was filed by Umashankar Sivasubramaniam. As per Umashankar’s claim, he received an E-Mail in September 2007 from ICICI, asking him to reply with his Internet banking username and password or else his account would become non-existent. He replied and later he found ₹ 6.46 lakhs (₹ 6,46,000) moved from his account to the account of another company. That company did a withdrawal of ₹ 4.6 lakhs (₹ 4,60,000) from an ICICI branch in Mumbai and retained the balance in its account.

An application was prepared as arbitration for proceedings under the IT Act. The application was presented to the state IT Secretary on 26 June 2008. In that application, Umashankar held the bank responsible for the loss that he suffered. ICICI Bank, however, claimed that the applicant (Umashankar) had failed to protect his confidential information. *According to ICICI Bank, Umashankar carelessly disclosed his confidential information such as password. According to the bank, he became the victim of a Phishing attack because of this carelessness.* Bank spokesperson said that customers are fully apprised on security aspects of Internet banking through various means. ICICI Bank officials empathetically said that bank’s security systems are continuously audited and neither the security nor bank’s processes have been breached.

The bank decided to appeal the order. The bank spokesperson said that ICICI Bank endeavors to offer world-class service to its customers. They further said that they have hundreds types of transactions, which can be completed online without having to walk into a branch. Further, they added that the bank strives for convenience and safety of their customers and uninterrupted availability of services through self-service channels. The bank claims that they also continuously upgrade their systems and technology to ensure that customers get the best experience and a safe environment while transacting online.

Vijayashankar a techno-legal consultant appeared for the petitioner. According to him, while the order may lead to tightening of cyberlaws in the country, the judgment reflects the lack of accountability of using Internet banking. He further opined that, *although Phishing fraud is very common, banks are not accepting the liabilities.* In his view, such a ruling will set a good precedent. In India, although there are 300-odd cases of Phishing attacks recorded or contended, most cases do not get pursued under proper legal framework. Some such cases were filed at consumer courts. Figure 11.4 conceptually depicts the fate of cybercrimes.



**Figure 11.4** | Fate of cybercrime cases (total cases-to-sentenced cases).

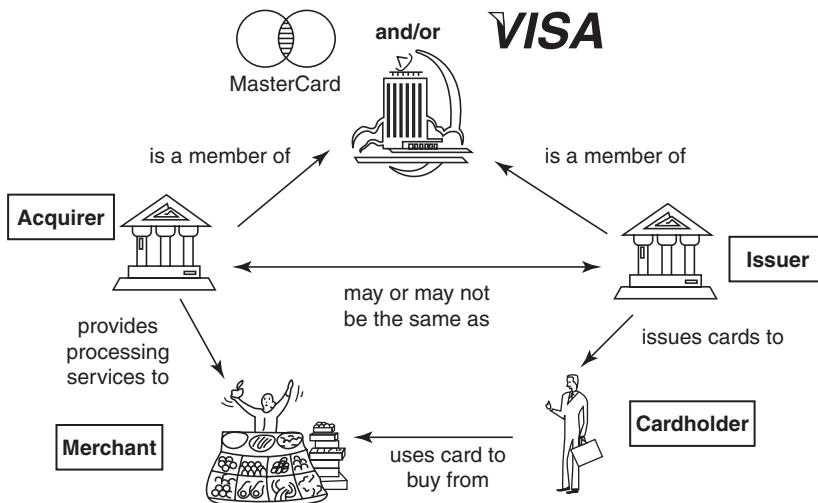
### 11.4.2 Credit Card-Related Frauds

#### *Illustration 3: Online Credit Card Theft Ring*

Phishing and credit card frauds are addressed in Chapter 5. Here is a real-life example about that. This case took place in June 2009 and involved 36-year-old Max Ray Butler (also known as Max Ray Vision) resident of San Francisco, California. Max pleaded guilty in Federal Court in Pittsburgh to wire fraud charges to two counts before Senior US District Judge. In connection with the guilty plea, the attorney mentioned in the court that Butler, known widely on the Internet as “Iceman,” among other aliases, conducted *computer hacking and identity theft on the Internet on a massive scale*. As part of the conspiracy, Butler cracked into financial institutions, credit card processing centers as well as other secure computers with the illicit purpose of acquiring credit card account information and other personal identification information. Several of these cards were made available to Christopher Aragon – he was a partner in crime and was based in the Los Angeles area. Christopher used these cards with the help of a team of associates to buy up commodities for sale. Max sold the remaining card numbers out-and-out over the Internet.

Max and Christopher formed a website known as “CardersMarket.” They devoted this crafty site for the acquisition, utilization and sale of credit card account information. This illicit process is known as “carding.” A main intention of the site was to employ brilliant individuals to assist in carding activity. During the best of times (from criminals’ view point), CardersMarket had approximately 4,500 worldwide members! Refer to Figure 11.5 to understand the entities involved in credit card transactions.

Max was arrested on a criminal complaint on 5 September 2007 in San Francisco. A search of the computer systems in Max’s apartment revealed more than 1.8 million stolen credit card account numbers. When these card account numbers were provided to Visa, MasterCard, American Express and Discover, it was revealed that the amount of fraudulent charges on the cards in Max’s possession totaled approximately \$86.4 million. These losses had to be borne by the thousands of banks that issued the cards. On 20 October 2009,



**Figure 11.5** Entities involved in credit card transactions.

Source: Author's presentation in PCI-DSS awareness sessions for industry professionals.

punishment was handed: 30 years in prison, a fine of \$1,000,000 or both – and that is what the law could provide as a maximum sentence. As per Federal Sentencing Guidelines, the actual sentence imposed was based on the gravity of the offense and the previous criminal history, if any, of the accused. Many agencies were involved in inquiry of Max's illegal activities – Computer Crime and Intellectual Property Section (CCIPS) of the Department of Justice; the Federal Bureau of Investigation; the Vancouver Police Department, Vancouver, Canada; the Newport Beach Police Department, Newport Beach, California; and the Orange County Sheriff's Department, Orange County, California; and the US Attorney's Office for the Northern District of California.

If we wonder what happens to the “stolen” credit card data, the following “dark market” price information below is shocking as well as an eye opener. One can well imagine how this information must be rapidly exchanging hands in the global black market (this information is as current at the time of writing this; authors by no means have any validation responsibility here):

1. Data Dumps from magnetic stripes on batches of 10 cards are sold.
2. Standard cards: \$50. Gold/platinum: \$80. Corporate: \$180.
3. Card verification values information needed for online transactions: \$3–\$10 depending on quality.
4. Complete information/change of billing information needed for opening or taking over account details – \$150 for account with \$10,000 balance; \$300 for one with \$20,000 balance.
5. Skimmer device to read card data – up to \$7,000.
6. Bank log-ins 2% of available balance.
7. Hire of Botnet Software robots used in Spam attacks – \$50 a day (“Botnets” are explained in Section 2.6 of Chapter 2).
8. Credit card images: Both sides of card – \$30 each.

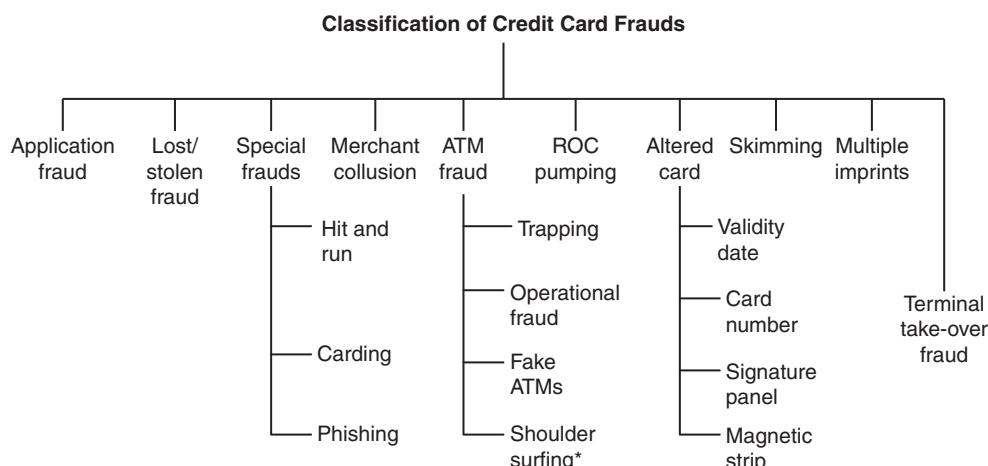
As known to law professionals, an indictment is only a charge and is not an evidence of guilt. A defendant is presumed innocent and is entitled to a fair trial at which the government must prove guilt beyond a reasonable doubt.

*Source:* www.cybercrime.gov

### *Illustration 4: Understanding Credit Card Fraud Scenarios*

In Chapter 5, we learned about Phishing and credit card frauds are addressed in Chapter 3. What is explained here is based on that background. Figure 11.6 presents a schema for categorizing credit card frauds. Figure 11.5 shows main entities involved in the normal credit card transactions. Not all types depicted in Fig. 11.6 fall under “cybercrime”; however, given the rise in the number of electronic transactions handled over the Internet, most would be. Note that a “fraud” can be defined as willful deceit or trickery or a deceptive or spurious act. In an era of advanced technology, it should be easy to catch criminals and fraudsters. However, the reality is far from this. “Credit cards” are not “anonymous like the paper money” and so, their theft can be traced. Criminals and fraudsters do not give up; in fact, they make themselves technology savvy to keep ahead in the game! They are led by the single aim of reaping the monetary benefits and satisfying that ego! The key entities involved in credit card transactions, are shown in Fig. 11.5 – their role is briefly described for reference during the fraud scenarios described in the next section.

There are more than 50 different types of cards available in the market – we have considered only the major ones. Visa and MasterCard are made up of member organizations who can be either acquirers or issuers (or both). “Acquirers” are the members of the Visa or MasterCard organizations that handle “Merchants.” “Issuers” are the members of the Visa or MasterCard organizations that issue the cards to cardholders. “Merchants” are those entities who “accept” card transactions. “Service Providers” are the entities that provide services related to the processing, storing or transportation of card information on behalf of any of the entities mentioned (Issuers, Acquirers, Merchants). With that preamble, a few scenarios relating to credit card frauds are now explained. Keep in mind the classification chart of credit card frauds shown in Fig. 11.6. Some of them are described in the following pages. In the reference section, links to credit card fraud related video clips are provided in Refs. #1, 2, 3 and 4, Video Clips, Further Reading.



**Figure 11.6** | Credit card fraud classification.

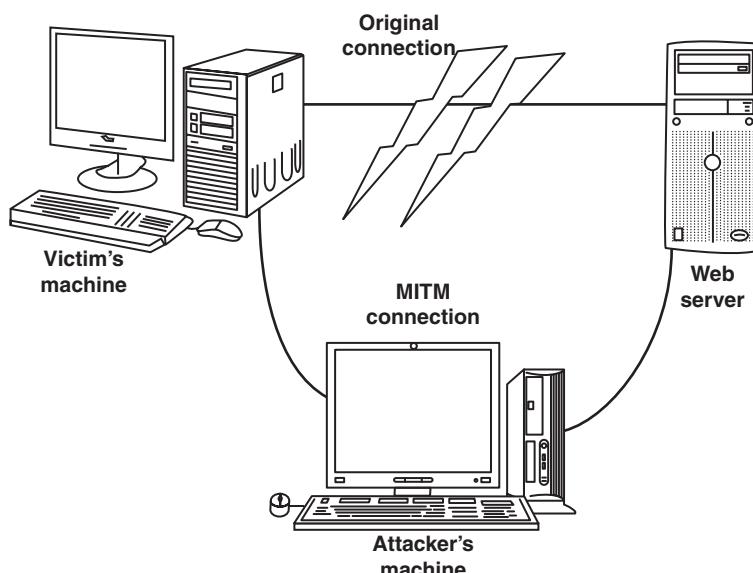
\*Shoulder surfing is explained in Chapter 2 (Section 2.3.1).

### Credit Card Application Fraud

In an “Application Fraud,” the fraudster obtains information about a person who is eligible for getting a credit card and has applied for it. The fraudster then makes his/her application to the “Issuer” with that person’s details except for the residential address. The residential address of the actual applicant is substituted by fraudster’s (mostly temporary) address. The issuer, not being aware of this, would end up sending the card at that address!

In another variety of this fraud scenario, the fraudster obtains the card details of an already existing card member (this is done through Phishing attacks). He then calls up the call center of the issuing organization, pretending to be the actual card owner. He reports the card as “lost” and asks them to issue a “replacement card” at his address, informing them also about the change of address. Now, if the issuing organization (typically a bank) is not security-savvy enough to call the actual card holder to validate if he/she indeed had made such a request, the fraudster will get a genuine card at the cost of the scape goat (the actual card owner) to run up whopping bills for his/her own use (which they normally are smart enough to avoid) or to “sell” the card in the “dark market” – the dark market “rates” for “stolen information” were mentioned in Illustration 3.

With the growing number of Internet-based applications for credit card, obtaining such information would be possible with a man-in-the-middle attack launched. In a typical “man-in-the-middle attack,” electronic messages, transmitted through the Internet, are intercepted. Man-in-the-middle attack is illustrated in Fig. 11.7. Also recall that “passive” and “active” attacks were explained in Chapter 2 (Sections 2.2.2 and 2.2.3, respectively). These attacks are also explained in Chapter 4 (Section 4.4). The “man-in-the-middle” attack intercepts communication taking place between two systems. These attacks are also explained in Sections 4.4.1, 4.12 and Table 4.19 in Chapter 4. For example, in an http transaction the target is the TCP connection between client and server. With the use of different techniques, the attacker divides the original TCP connection into two separate and new connections – one between the client (i.e., the victim’s machine) and the attacker and the other between the attacker and the server, as shown in Fig. 11.7. Once the TCP connection is intercepted, the attacker acts as a proxy, being able to read, insert and modify the data in the intercepted communication.



**Figure 11.7** | Man-in-the-middle attack.

### Frauds Involving Lost and Stolen Credit Cards

In this scenario, it can so happen that a card holder genuinely loses his/her credit card when he forgets to collect it from the ATM (Automatic Teller Machine – most credit cards can be used to also withdraw cash from ATMs). Card holder may also forget to collect his/her credit card after signing for the goods purchased. There are also many other ways to lose the credit card (leaving the wallet/purse behind in which the card is or the card getting dropped out of pocket or wallet, etc.) When the fraudster finds a lost card, either he himself uses that for shopping (which is not what the fraudster would typically do) or he sells the lost card to a gang with whom he works. There are many agencies that specialize in credit card-related crimes. For example, the Russian Business Network (RBN) is a multifaceted cybercrime organization, specializing in some cases monopolizing personal identity theft for resale! RBN was registered as an Internet site in 2006. Initially, much of its activity was legitimate. It appeared that the founders soon found that it was more lucrative to host illegal activities and started hiring criminals for their services. RBN provides web hosting services and Internet access to all types of criminal and offensive activities, with individual activities earning up to \$150 million in 1 year! Recall “DarkMarket” described in Illustration 1.

Such gangs have multiple layers of operations with many counterparts. Some of them are called “runners.” Their job is to show their face in the shops by physically visiting the shops for small amount purchases with the objective of ascertaining whether the “lost” card is put on hold or if it is on “hot list.” In other words, “runners” are hired to find out the validity of lost/stolen cards. If the card is found to be “clean,” the fraudster would either use the card immediately for a high value purchase (by forging the signature of course) or will sell it in the dark market. Dark market rates for stolen/lost credit cards were mentioned in Illustration 3: Online Credit Card Theft Ring.

### The Fraud through Merchant Collusion

This fraud occurs when the “Merchant” joins hands with the fraudster by providing details of the genuine cards in return for a share of the returns from this manipulation. The merchant can allow members of a gang to use his terminal as a host in order to transfer information on credit cards, which are swiped at the merchant’s terminal. One way of doing this is that another “swipe” slot is kept hidden or discreetly near the actual swipe machine at the Point of Sale (PoS) terminal at the merchant’s establishment. Always be wary and be on the look-out if the merchant is scanning your card more than once for one pretext or the other. For example, by asking you to let him scan it again because the first scan was not successful. Also, *never loose site of your credit card*. Always insist that you want your credit card to be swiped in your presence: be it a restaurant or a brand hotel (five stars hotels, etc.). This is important because, as a part of collusion, once the merchant allows his terminal to the members of the fraudster gang in order to transfer the confidential information on the magnetic card on the credit card, that information is gone in the wrong hands! The fraudster’s terminal, known as the “receptor” (because it receives the information), downloads the confidential details of the genuine card from the host terminal. This stolen information can be used in a number of ways to cheat the “Issuers,” at a later date. The information can be used to manufacture counterfeit cards or to obtain genuine cards by reporting the card as “lost” or to defraud by mail order. In the reference section at the end of this chapter, we have provided a video link in Ref. #4, Video Clips, Further Reading to show how they fake a card.

There are instances where the customer also colludes with the Merchant to cheat the Issuer. Customer uses the card at the Merchant establishment, that is, a shop/mall, for a single transaction but allows the Merchant to take multiple prints of the charge slip. The Merchant submits these charge slips with forged signatures and obtains the payment due to him (the Merchant) from the Acquirer (see the transactions flow depicted in Fig. 11.5). At the end of the card holder’s billing cycle, when the credit card statement is

presented for payment, the card holder disputes the charge by claiming that the transactions are fraudulent and refuses to pay. Meanwhile, the merchant has already recovered his sale due amount. Because the card holder refuses to pay the Issuer (typically the bank), it is the Issuer who has to bear the loss. The problem is that it is difficult to “prove” such collusion. Until and unless the same card holder keeps appearing in many such cases of frauds, tracing becomes difficult. It is said that the card issuers assume a certain small percent of their overall transactions volume, as “bad debt” and levy it across their base of card holders (which runs in thousands and thousands). They present it in the charge statement as a line item.

### Frauds at the ATMs

Card frauds and operation frauds are the two main types of ATM frauds. Research by Retail Banking estimates that worldwide, there are more than 1.5 million ATM (Automated Tailor Machines – sometimes jocularly referred as “Any-Time-Money”!). It is said that a new ATM gets installed every five minutes somewhere in the world! All around the world, people carry out successful ATM transactions (withdrawing money from their bank accounts, viewing their bank balance, etc.). For more than three decades, ATM operations have been going on successfully. However, that does not mean that ATMs are completely risk-free. ATMs, like most other devices that are designed to store and dispense valuable items, have been targets of frauds. ATM thefts, burglaries and electronic frauds committed at the ATM make news lines almost daily, all over the world. Most of the “ATM frauds” reported by media as “debit card frauds” are to do with the compromise of “Personal Identification Number” (PIN). PIN and credit card code are explained later in this section. As per reports of Global ATM Security Alliance, only 0.0016% of all ATM transactions are impacted by crime or fraud worldwide. Notwithstanding this claim of “secure” ATM transactions, ATM fraud and security or rather the lack of it is one of the most popular topics in the media!

In Europe, “Card Skimming” (Fig. 11.8 shows how the skimmer device looks) fraud is one of the biggest crimes affecting ATMs. Card skimming at ATMs caused losses of 44 million Euros across Europe and is known to be a source of funding for criminal operations in the East European countries. Cash trapping and transactional reversal crimes are on the rise; especially in Eastern Europe. *Thieves fix a device to the cash dispensing slot of the ATM – this action causes currency notes to get stuck inside the slot.* Criminals return later to remove the cash from inside the dispenser. Trapping attacks like these resulted in losses amounting to 2 million Euros in 2005. ATM market is growing fast in Latin America and highly advanced ATM machines are deployed in this region. ATM card fraud in the Latin American region increased by nearly 15% in the last 5 years. In the Asian region, China and India are the fastest growing ATM markets. China now has more than 86,000 ATMs and the Indian ATM market is growing at the rate of 100% annually as per reports of Frost and Sullivan. The top ATM fraud in Asia is ATM dispenser trapping. Asia has one of the world’s highest Phishing attacks. You can read about Phishing in detail in Chapter 5. Refer to Ref. #5, Video Clips, Further Reading for useful tips to protection from ATM thefts.

### Carding Frauds

It was mentioned that “carding” involves acquisition, utilization and sale of credit card account information. When a credit card is stolen, the thief does not know whether the card is valid. So the thief wants to find out about the status of the card (active, cancelled, etc.). From the thief’s perspective, there are many possibilities – the card holder may have immediately reported the loss of the card or the card limit may have been completely used up. In such cases, the card is of no use to the thief. The smart thief uses the Internet to ascertain if the stolen card is still “good” for use. The thief could use the stolen card to make a small amount purchase using the online purchase facility on the Internet. However, that would involve the “shipping address” and that would expose the thief. So the smart thief uses the stolen card for making a charity donation! That way,

the thief does not have to waste time in searching items on the product catalogues on the sale portal of any online seller. The thief makes the donation amount relatively small so that the card limit is not used up. He does this for one more reason – a large amount would make the transaction immediately noticeable. Carding fraud is also used when the credit card is obtained fraudulently through card “skimming” (explained next) or when a Phishing attack is done on the card.

### Credit Card Skimming

Tips to prevent credit card frauds were addressed in Chapter 3 (see Box 3.2). Section 3.4 of Chapter 3 is about credit card frauds. With that thread, the card skimming fraud is explained here. Card skimming is done with “skimmer” devices; see Fig. 11.8. The relative proportions in those images help us understand how tiny the device is and that makes it simple for fraudster to conceal it out of view of the victim. Skimming is in a way, fraudster’s revenge on the Customer Verification Value (CVV – see the links in Ref. #36, Additional Useful Web References, Further Reading to understand this).

Figure 11.9 depicts where the card security code is located. This code has various terminologies attached with it: *Card Security Code* (CSC), *Card Verification Data* (CVD), *Card Verification Value* (CVV or CV2), *Card Verification Value Code* (CVVC), *Card Verification Code* (CVC), Verification Code (V-Code or V Code), or *Card Code Verification* (CCV). The CVV is an algorithm (software program logic) that is very difficult to break. The fraudster, therefore, does not take the trouble to break the code. He simply colludes with a single merchant or with a group of merchants. He provides the merchant with the terminal number similar to the one provided to the merchant by Acquirer or the bank (because in some cases the bank, that is, the Issuer and the Acquirer, can be the same institution). The only difference is that the fraudster’s terminal is capable of also reading the card data that is recorded on the credit card’s magnetic strip. The swiping equipment provided by the Issuer bank/Acquirer can only process the data by connecting to the bank’s server but it



**Figure 11.8** Credit card skimmer devices.



This number is printed on your Master Card & Visa cards in the signature area of the back of the card. (it is the last 3 digits AFTER the credit card number in the signature area of the card).



You can find your four-digit card verification number on the front of your American Express credit card above the credit card number on either the right or the left side of your credit card.

**Figure 11.9** | Credit card security code.  
Source: <http://www.sti.nasa.gov/cvv.html>

does not have the capability to record the data on the magnetic strip of the card. Now comes the criminal act – the fraudulent merchant or the fraudster working at the Merchant's PoS (Point of Sale) terminal, swipes your credit card *twice* – of course without you realizing it; even if you notice it and bring it to his notice, he will give you one explanation or the other why he swiped your credit card more than once. Now, the card is swiped once across bank-provided swiping equipment and second time on the fraudster's terminal. The security code (CVV, CCV, etc.) which is encoded on the magnetic strip on the back side of the credit card (see the top right object in Fig. 11.9), and is decoded on the terminal, gets recorded on the fraudster's terminal. He now gets the genuine card information (card holder name, card number, date of validity) along with the security code! His job is done and he is ready to use that information for creating fake credit card (in Ref. #2, Video Clips, Further Reading, we have provided a link to the video clip that explains this). See the credit card skimming video clip provided there.

It may so happen that in some restaurants, a waiter could have a collusion with a fraudster gang – he could hide the skimmer device in his socks. As you stand near the payment counter for your credit card to be swiped, after taking the card from you, the waiter may pretend to drop it. Then waiter will bend down to pick up the card – on its way up, the card would get swiped across the skimmer device in his socks and you may never even realize it as this may happen in less than minute! In another variant of this scenario, the skimmer device (with a slit type – see Fig. 11.8) could be located next to the actual card swiping device authorized to the merchant by the Acquirer. If you are not carefully watching, the fraudster colluding with the merchant (he could very well be the PoS staff of the merchant) after swiping the card with the actual credit card swiping machine (see Fig. 11.10), will swipe your credit card also through the skimmer device to read the confidential card details (card number, date of validity and most important the credit card security code – CCV, CVV, etc.) to his benefit! You can watch one such video clip demo by visiting the link mentioned in Ref. #2, Video Clips, Further Reading.



**Figure 11.10 |** Credit card swiping machine.

### Illustration 5: ShadowCrew – The Internet Mafia Gang

This is a case reported in the public domain. It shows how ruthlessly the criminals can operate in the world of credit cards. This illustration has a lesson for all of us that we should take adequate care not to succumb to credit card frauds. In Chapter 4 (Section 4.10), we learned about “SQL Injection.” Criminals used SQL Injection technique in this case. This illustration also brings to fore an important point – today’s cyberfraudsters are tech-savvy people. That is how this hacker gang operated. The links related to this illustration are provided in Ref. #40, Additional Useful Web References, Further Reading.

“ShadowCrew” was an international crime message board. The board offered a haven for “carders” and hackers to trade, buy and sell anything from stolen personal information (through identity theft – the topic is discussed at length in Chapter 5) to hacked credit card numbers and false identification. As we know, a *bank card number* is the *primary account number* found on credit cards and bank cards. It has a peculiar type of internal structure and it also shares a common *numbering scheme*. Credit card numbers are a special case of ISO/IEC 7812 bank card numbers. As mentioned in Illustration 3 (Online Credit Card Theft Ring), “CardersMarket” is devoted to the acquisition, use and sale of credit card account information, a process known as “carding.”

The genesis of this fraud group is interesting – in early 2002, ShadowCrew emerged from an underground site, counterfeitlibrary.com, and was followed up by carderplanet.com, a primarily Russian site. It was created by only a few of people, most notably Kidd (Seth Sanders), MacGyver (Kim Taylor) and CumbaJohnny (Albert Gonzalez, who would later become an informant for the Secret Service beginning April 2003). Other main people who would become Administrators and Moderators were Deck (Andrew Mantovani), BlackOps (David Appleyard) and a handful of others.

Over a period of short time, ShadowCrew grew to over 3,000 members (many were “clones” and inactive accounts) worldwide with a small group of members leading the forums. During its inception, the site was hosted overseas, in Hong Kong. However, shortly before CumbaJohnny’s arrest, the server was in his possession. The server was hosted somewhere in New Jersey. The downfall of the site started although it had flourished initially.

The site was doing well from the time it was launched in 2002 until its shut down in late October 2004. Although there were many criminal activities taking place on the site and all seemed well, the members were not aware of what was going on behind the scenes. Federal agents received a major breakthrough when they found CumbaJohnny. During the period April 2003 to October 2004, Cumba helped in

gathering information and monitoring the site and those who used it. He started by exposing many of the Russians who were hacking databases and selling counterfeit credit cards. Some of the first to be arrested were Bigbuyer, BOA and Wolfrum. Although they were being arrested, no reports of it being linked to ShadowCrew ever came about at the time.

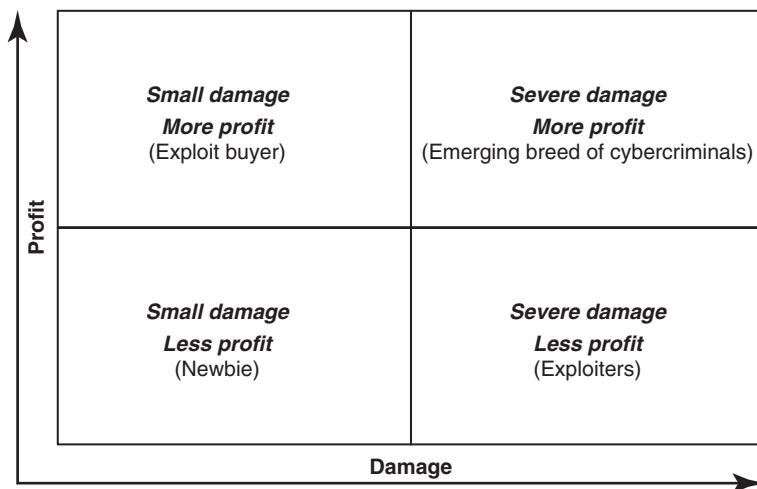
Business continued as usual at ShadowCrew; credit cards were sold and identification forged, all while the Secret Service monitored everything that went on and built cases against high-ranking members. Most members knew that authorities would monitor the site and would institute controls to prevent their identities from being known. These tactics involved Proxies, Virtual Private Networks (VPNs), Wi-Fi and other “anonymizing” techniques (Chapter 9 explains “anonymizers” – Section 9.8, Box 9.7). However, members that trusted CumbaJohnny’s VPN Service would be those who would face their ultimate downfall. CumbaJohnny offered a VPN service as a way for well-known members to connect to the Internet through a secure gateway. VPNs were thought to be a reasonably safe method to stay anonymous in the community, but were always considered slightly risky due to the safety being in the hands of the person who maintained it. Nearly all of the top-ranking members who were still around in 2004 used Cumba’s VPN.

After a year of monitoring and building evidence against the members of ShadowCrew, the Secret Service finally played its cards, hoping no one had caught on. The government, as paranoid as any of the criminals on the site, became worried when a member of ShadowCrew adorning the name “Ethics” (Nicolas Jacobsen), allowed several members to see confidential documents he had obtained through hacking the databases of T-Mobile with an *SQL injection* (explained in Section 4.10 of Chapter 4). The documents belonged to a Secret Service agent who had been tracking both Jacobsen and ShadowCrew. Allegedly, the documents contained a list of names and drop addresses of certain former (now arrested) and perhaps current ShadowCrew Members. Cumba, being the top member of ShadowCrew after Kidd’s departure and MacGyver’s arrest, was made aware of bits of the information by others who had seen it. Although it is not certain who saw the information or what exactly it contained, it must have not been enough to alarm anyone.

The Secret Service rallied around with worldwide police, and on 26 October 2004 conducted a series of raids on 28 members of ShadowCrew, spanning a total of 8 to 10 hours. Within days, the arrests were made public, with evidence presented showing that the ShadowCrew was an “Internet Mafia” with Mantovani as the “Godfather.” Claims made by the media included monetary losses totaling millions of dollars. Allegedly, the members were all users of CumbaJohnny’s VPN Service, which led to their locations. Those who had not been caught did not use the VPN, were not important enough to arrest or had been ostracized from the community.

As of August 2006, most of those indicted after the October 2004 raids pleaded guilty were since then sentenced. The most publicized and longest sentence was that of Mantovani, who was given 32 months in a Federal Prison Camp. Many sites appeared after ShadowCrew’s death – one such site was specifically focused on unraveling the mysteries of what actually happened. This site, [thegrifters.net](http://thegrifters.net), was run by a member (El Mariachi) who was formerly indicted. This site was the result of converting his old fraud site to an investigative site. Members of this group uncovered and compiled many pieces of information on the indicted members of ShadowCrew until [thegrifters.net](http://thegrifters.net) was taken down in early 2006.

The numbers involved in this case are huge. According to the Federal indictment, ShadowCrew was an international organization of approximately 4,000 members. The last available pages before 27 October 2004 on archive.org showed 2,709 registered members. However, this number is not a 100% correct estimate of the true number of members because registration was free which meant that the numbers could easily surpass those stated. People, familiar with the ShadowCrew forum, knew that many members operated under more than one username. There were a few members who were banned from the forum – they would



**Figure 11.11 |** Hackers' motives and goals.

attempt to frequently register under another username. The forum was around for over 2 years, so there were likely many inactive accounts. The loss figures were also big – \$4 million dollars. The government was unable to find any concrete proof that the defendants in operation were responsible for any specific losses. The \$4,000,000 figure was obtained by multiplying the number of credit cards transferred by \$500 each (as per Federal Law when no monetary figure in a fraud case can be determined). The assumption in this figure is that every single card was valid and had been used. Figure 11.11 shows that not only today's hackers and fraudsters are tech-savvy, they are also “professional” in terms of gains they want.

#### *Illustration 6: Dirty Relations – Goods Delivery Fraud*

Internet seems to be breeding ground for many cybercriminals who take advantage of mail Spoofing, ID theft and many other techniques to achieve their fraud objectives (refer to Chapters 2–5). Online purchasing is possible by sending electronic mails using the Internet and there are ample opportunities for fraudulent people to play mischief by hiding their real identity through fake E-Mails. This illustration shows how this happened in a real-life scenario. Interestingly, it also shows the humanitarian approach of the legal system in passing the judgment and giving due consideration in a given context of the crime.

It all started after Sony India Private Ltd filed a complaint. Sony India runs a website called [www.sony-sambandh.com](http://www.sony-sambandh.com), targeting non-resident Indians (NRIs). The website enables NRIs to send Sony products to their friends and relatives in India by purchasing those products online. The company makes delivery of the products to the concerned recipients. In May 2002, a lady visited the website but did not log onto the site with her real name. She assumed the identity of “Barbara Campa” and sent an E-Mail to order a Sony Colour Television set and a cordless phone. In the mail, she provided her credit card number for payment and made a request for getting the products delivered to a person named “Arnavaz Ahmed” in Noida area. The payment was duly cleared by the credit card agency and the transaction was processed. After carrying out the relevant procedures of due diligence and checking, the company delivered the items to Arnavaz Ahmed.

The company was very clever – at the time of delivery, the company took digital photographs showing the delivered goods being accepted by Arnavaz Ahmed. At this time, the transaction closed; however, after

one and a half months, the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. Based on this, the company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case with the Indian Penal Code under Section 418 (*Cheating with knowledge that wrongful loss may ensue to person whose interest offender is bound to protect*), Section 419 (*Punishment for cheating by personation*) and Section 420 (*Cheating and dishonestly inducing delivery of property*). Copy of the Indian Penal Code is provided for readers' reference in Appendix P.

The matter was investigated into and Arnavaz Ahmed was arrested. Investigations revealed that Arnavaz Ahmed, while working at a call centre in Noida, gained access to the credit card number of an American national which he misused on the company's site. The CBI confiscated the color television and the cordless head phone. The CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arnavaz Ahmed under Sections 418, 419 and 420 of the Indian Penal Code – this being the first time that a cybercrime has been convicted. The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. On these grounds, the court released the convict on probation for 1 year.

The judgment is of utmost importance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the *Indian Penal Code* (the IPC) can be effectively applied to certain categories of cybercrimes which are not covered under the ITA 2000. Second, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride. According to Police, these E-Mail originated from an E-Mail Id which was similar to that of the Income Tax department. By investigating into this cyberfraud, at an initial stage, it was learnt that several such E-Mails have been sent to tax payers. The fraudulent E-Mail asks for the receiver's bank account number, customer identification number and Net banking password. There are nearly 3.5 million tax payers in the country and their E-Mail identity can be obtained easily from social networking sites, said a senior police officer.

### 11.4.3 Other Illustrations

#### *Illustration 7: Fake Mails Promising Tax Refunds – Beware*

Internet banking has both advantages as well as perils. Recall the discussion in Chapter 2 (Box 2.7 – Fake E-Mails) and Chapter 4 about fake E-Mails in the context of “Phishing” (Section 4.3.1). This illustration shows how that was used by criminals. If you are a tax payer waiting for refunds at the end of the financial year, beware of fraudulent E-Mails circulating on the Internet. Delhi Police's Economic Offence Wing (EOW) investigated several cases where the complainants claimed to have received E-Mails in which they are asked to provide their bank account details so that the tax refund could be transferred to the accounts.

Such an E-Mail-based fraud came to light after the Police received a complaint from a south Delhi businessman. The plaintiff name was withheld due to the sensitive nature of the case. The E-Mail claimed that the receiver would receive ₹ 2,500 compensation from the Income Tax department if he provided with his bank details, including Net banking password. The person who sent the E-Mail also asked for his credit card details; this raised doubt in the mind of the plaintiff.

Additional commissioner of police (EOW) said that this cyberfraud, under investigation, is similar to attempted Phishing. Once the sender receives the details of the bank account, he can easily transfer the money from that account through Internet banking. As a safeguard, one should not respond to such E-Mails. One should report the matter to Police immediately. In this case, officials at the EOW got into tracing of the server from where these E-Mails originated. They asked the service provider to furnish details about

the E-Mail account through which these mails were sent. Recall E-Mail forensics explained in Section 7.6 of Chapter 7.

This was for the first time that such a cyberscam report went to Police. It is suspected that the gang has been operating since the past several months. It is common for fraudster gang to become active when the dates for tax returns approach. In this case, the police approached the income tax department to take steps to create awareness about such fraud E-Mails. However, this is not the first time that tax returns have come under the scanner. In 2005, the EOW had taken under arrest 12 individuals for encashment of refund challans worth over ₹ 50 lakhs (₹ 50,00,000) through bogus bank accounts that were opened in collusion with bank staff.

### *Illustration 8: Phone Scam Targets Your Bank Account*

This illustration is about DoS attack that was mentioned in Chapter 1 (Table 1.5, Table 1.6, Box 1.5) and explained in Chapter 4 (Section 4.9, Fig. 4.5, Box 4.8). DoS attacks are not a new happening – these attacks are used by computer hackers to bring down websites by flooding them with huge amount of network traffic. The “masquerading” technique used by cybercriminals, mentioned in Chapters 1–4 (Table 4.9). This illustration shows how the technique was used.

What will happen if you get hundreds or thousands of calls on your home, business or cell phone? It will simply tie up the lines. How would you feel if you heard anything coming, as if from thin air, recorded messages, advertisements, or even phone sex menus when you answer? It is not annoying? Be careful, however, because, it could be more than that – it could be a sign that you are being victimized by the latest scam making the rounds. This “telephone denial-of-service attack” could possibly be the predecessor of a crime aimed at your bank accounts. In a current twist, fraudsters have converted this activity into telephones, using automated dialing programs and multiple accounts to overwhelm the phone lines of unsuspecting citizens. Why do you think, the criminals do it? It turns out that the calls are simply a diversionary tactic: while the lines are tied up, the criminals, masquerading as the victims themselves, are raiding the victims’ bank accounts and online trading or other money management accounts.

Here is how these attacks work – recall the discussion in Chapter 2 about the “reconnaissance” and “passive” phase of attacks. Weeks or months before the phone calls start, a criminal uses social engineering tactics or malware to elicit personal information from a victim that victim’s bank or financial institution would have – like account numbers and passwords. Perhaps you as a victim responded to a bogus E-Mail Phishing for information, inadvertently gave out sensitive information during a phone call, or put too much personal information on social networking sites that are trolled by criminals. Using the technology, criminals tie up your phone lines. Next, the criminal either reaches the financial institution pretending to be you or pilfers your online bank accounts using fake transactions. More often than not, the institution calls to verify the transactions, but of course, in this scenario (due to phone lines being made busy) they are unable to get through to the victim over the phone.

Even if you have not made any bank transactions, the criminals sometimes re-contact the financial institution in your name and ask the bank to do those transactions (say transfer of money or something similar). Or they substitute their own phone number to victims’ accounts and just wait for the bank to call. For example, by stealing your password [remember the keylogger ill utility mentioned in Chapter 4 (Section 4.5)]. Using that malware, they will be able to get into the account and update your profile by putting their phone number. Now, the bank will end up calling them thinking it is you! They may have even learned about your other authentication information and would be able to masquerade to the bank. Thus, they will make your bank believe it is YOU who is talking to them! By the time you or the financial institution realizes what happened, it’s too late.

The Federal Bureau of Investigation (FBI, US) first learned about this emerging scheme through one of its private industry partners, who revealed how a Florida dentist lost \$400,000 from his retirement account after a DoS attack on his phones. There has certainly been a obvious rise in the number telephone DoS attacks, with numerous incidents reported in several of the Eastern States in America. To help fight these schemes, the FBI teamed up with the Communication Fraud Control Association – comprising of security professionals from communication providers – to analyze the patterns and trends of telephone DoS attacks, educate the public and identify the perpetrators and bring them to justice.

Remember always that ultimately, it is individual consumers and small- and medium-sized businesses (SMB) on the front line of this battle. So take safety measures: never disclose your personal information to an voluntary phone caller or via E-Mail; change online banking and automated telephone system passwords frequently; check your account balances often; and protect your computers with the latest virus protection and security software. Even if you have the slightest doubt that you are possibly under an attack through cell phone or under a DoS attack, contact your financial institution and your telephone provider, and file a complaint with the appropriate authorities in your location. Recall the discussion about “Mishing” and “Smishing” in Chapter (Section 3.8 – Attacks on Mobile/Cell Phones).

### ***Illustration 9: Cookies and Beacons – The Facebook Controversy***

This illustration refers to “Facebook” a popular tool for “social networking.” As a general privacy principle, whenever a website captures people’s personal information details (such as name, birth date, home address, home telephone number, personal mobile number, etc.), the site is supposed to take an “*Explicit Consent*” known as “*Opt-In*” wherein the person visiting the website will check the box appearing on the consent form displayed on the website. “*Opt-Out*” is considered an “*Implicit consent*” wherein the person is assumed to be giving the permission as long as he/she does not uncheck the box. Thus, “*Opt-Out*” is a method in which personal information will be processed unless the data subject indicates it should be otherwise and “*Opt-In*” is a method in which personal information will be processed only if the data subject indicates it should be so. Refer to Fig. 6.2 in Chapter 6 for Opt-In and Opt-Out.

Recall the dangers of social networking sites explained in Chapter 7; Section 7.14, Tables 7.6 and 7.7. Facebook, the social networking site, is supposed to track visitors to that site and is also supposed to have a customizable privacy setting option. People like both “cookies” (a bakery product) and “Beacon” (a typical breakfast item in the European countries). As much as these items are considered bad for our physical health, so are they also for the health and well being of our confidential data stored on the computers! Let us understand what “cookies” and “Beacons” mean in computer parlance.

Cookies are tiny text files that are stored on a client’s device and may be later retrieved by a web server from a client’s machine. Cookie files allow the web server to keep track of the end-user’s web browser activities, and connect individual web requests into something like a session. Cookies can also be used to prevent users from having to be authorized for every password protected page they access during a session, by recording that they have successfully supplied their username and password already. Since cookies are usually stored on a PC’s hard disk, they are not portable. Cryptic or encrypted cookies with an unclear purpose, and which are set without the user’s knowledge, alarm Internet privacy advocates. They may also violate data protection laws.

“Web Beacon” is a graphic on a webpage or in an E-Mail message that is designed to monitor who is reading the webpage or E-Mail message. Web Beacons are often invisible because they are typically only 1-by-1 pixel in size, with no color. Some information collected is the IP address of the computer that the web Beacon is sent to, the URL of the page the web Beacon comes from and the time it was viewed. Web Beacons are also known as web bugs, 1-by-1 GIFs, invisible GIFs and tracker GIFs (Graphics Interchange Format).

Facebook uses Beacons heavily. Beacon was a component of Facebook's advertisement system that sent data from extraneous websites to Facebook. Apparently for the purpose of allowing targeted advertisements and allowing users to share their activities with their friends. On 6 November 2007, Beacon was launched with 40+ associate websites. The notorious service, which became the target of a class action lawsuit, and the service was shut down in September 2009.

Facebook Beacons raised some privacy concerns. On 20 November 2007, a civic action group called "MoveOn.org" created a Facebook group and online petition demanding that Facebook not publish their activity from other websites without explicit permission from the user. In fewer than 10 days, this group gained 50,000 members. Eventually, Beacon was changed to meet the requirement that any actions transmitted to the website would have to be approved by the Facebook user before being published. In 29 November 2007, a note was published by Stefan Berteau, a security researcher for Computer Associates, about his tests of the Beacon system. The note said that it was found that data was still being collected and sent to Facebook despite users' Opt-Outs whereby users had the choice not to log into Facebook at the time. This finding was in direct disagreement to the statements made by Chamath Palihapitiya, Facebook's vice president of marketing and operations, in an interview with The New York Times published the same day:

***Question to Facebook VP Marketing & Operations:***

In case I purchase tickets on Fandango, and refuse to issue the information to my friends on Facebook, does Facebook still get the information about my purchase?

***Answer by the VP:***

*Not at all! We are still trying to dismiss a lot of wrong information being publicized without cause.*

As per the blog posted by Louise Story of The New York Times on 30 November 2007, not only had she received the impression that Beacon would be an explicit Opt-In program, but that Coca Cola had also had a similar impression, and as a result, had chosen to withdraw their participation in Beacon. Facebook announced on 5 December 2007 that it would allow people to opt out of Beacon. In August 2008, a class action court case was submitted against Facebook and other corporations that activated Facebook Beacon when they released their common member's personal information to their Facebook user friends without members' consent through the Facebook Beacon program. In September 2009, Facebook proclaimed that it would terminate the service. In October 2009, a class action notice was issued to Facebook users who may have used Beacon. The proposed settlement would require Facebook to pay \$9.5 million into a settlement fund. The named plaintiffs (approximately 20) would be compensated a total of \$41,000, and the plaintiffs' lawyers would receive millions from the settlement fund.

Moral of this illustration is: (a) limit your social networking activity; (b) choose the social networking sites that have got privacy guarding features; (c) it is your responsibility to protect your online privacy.

### ***Illustration 10: Privacy Loss through Leakage of Users' Facebook Profiles***

This is one of the latest issues going on as per the story posted end of July 2010 at the link <http://in.news.yahoo.com/43/20100729/860/ttc-profiles-of-100-mn-facebook-users-le.html>. In the introduction of Chapter 5, it is mentioned that "Phishing" and "ID Theft" are emerging as the biggest security and privacy threats online. It is a challenge for people in the digital era to protect their online privacy. Privacy has three dimensions: (a) informational privacy; (b) personal privacy and (c) territorial privacy. The first as well as second aspects are getting impacted in current times as this illustration shows. Read on to understand the issue that arose recently.

Hundred million users lost their personal details! They were all the heavy users of social networking website. These personal details were leaked online and are now available for download! Imagine the impact, people proudly (and at times carelessly too) post all sorts of their personal information on such social websites; be it their honeymoon photos, personal chats with no holds barred opinions expressed and what not. Dangers of social networking sites are explained in Chapter 7 (Section 7.14). Will people ever take the heed and refrain from rampant use of social networking sites? It is a moot question.

An online security consultant scanned Facebook profiles using a certain software tool. When that was done, all the data of people, who had not hidden it through appropriate privacy settings, was collected. The list of such “personal” data was compiled – the list was uploaded for a free download! Now it is just a matter of accessing the URL of every “searchable” Facebook user’s profile, their name and unique ID – this is according to the latest BBC report. Imagine the implications considering the kind of personal information people carelessly leave on their Facebook accounts. According to the enterprising security consultant, he published the data only to highlight privacy issues, but Facebook retort said that the information was already public; apparently the news of personal information availability spread like a wild fire!

As per the basic tenet of “privacy,” people who use Facebook are supposed to own their information and they are supposed to have the right to share only what they want, with those with whom they wish to share and when they want to share. However, it turns out that in this case, information that people have agreed to be made publicly available, was collected by a single researcher and that information (of personal nature) already existed in Google and many other search engines, as well as on Facebook. However, Facebook denied this and said that no private data was available for public consumption or had been compromised. Meanwhile, the list of personal data of so many users was already downloaded by over 1,000 people on Pirate Bay, the world’s biggest file-sharing website.

According to one user (with name “lusifer69”) the list is “terrific” and “scary” at the same time! As per Internet watchdog Privacy International, warnings were issued to Facebook to sensitize them that something like this was likely to happen. The expectation, therefore, was that Facebook should have anticipated the data attack and should have put in place measures to prevent it. People find it hard to believe that a firm employing hundreds of engineers could not possibly imagine a privacy leakage incident of this size. According to people, this is an instance of gross negligence on part of Facebook who have got 500 million user accounts as of June 2010.

### *Illustration 11: Debit Card Frauds*

This story appeared in March 2006 in Computerworld. Most of the major credit card associations and financial institutions refused to identify the origins of data compromises. Those data compromises have resulted in a rise of debit card fraud globally – this raised serious concerns about the scope and extent of the problem. These frauds attracted media and public attention as to what led to attempts by criminal gangs to compromise PIN-based card transactions. As we know “PIN” is considered extremely secure. According to the Director of Fraud Technology operations at Fair Isaac, a Minneapolis-based company, the series of recent breach disclosures points toward a possibly shifted focus by criminals from credit card fraud to PIN-based debit card fraud.

Banks all over the world do reissue thousands of cards as part of their operations when a card lost case is reported. The case in point is Citibank – they acknowledged that a transaction was put on hold for an unspecified number of Citi-branded MasterCard debit cards when they detected fraudulent cash withdrawals in several countries – Canada, Russia and the UK. In a brief statement released by Citibank, it was said that the fraud was the result of a “third-party business information breach” that took place in 2005. To protect its customers, they “blocked PIN-based transactions in those countries (mentioned above), for the customers

affected by the breach." However, a spokesperson for the company refused to disclose the name of the third-party retailer involved in the breach.

With this disclosure, Citibank became the latest in a fast-growing list of financial institutions – they reissued thousands of debit cards or blocked access to certain transactions in countries where ATM cards were used fraudulently to withdraw cash and make purchases on US accounts.

The list comprises big banks such as Bank of America, Washington Mutual Bank and Wells Fargo Bank, along with many credit unions in the US. One of them was \$13 billion North Carolina State Employees Credit Union in Raleigh, North Carolina, which, over the past two weeks, reissued more than 27,500 debit cards after being told by Visa, USA of a security breach involving a US retailer.

According to senior vice president at the credit union (name not disclosed due to confidentiality reason) most of the compromised debit cards were fraudulently put to use in many countries – Romania, Russia, Spain and the UK. This at that time (year 2006) was the largest card reissue – ever done. This is considered to be the largest PIN theft ever. According to Gartner (the analyst firm) combined bank actions reflect the largest PIN theft to date and point to a new wave of PIN block card fraud.

We think "encryption" is hard to break; apparently this is not true as this fraud illustration shows. A PIN-based fraud scheme happened when hackers somehow managed the following to gain access to the encrypted PIN data that was sent along with card numbers to processors that execute PIN debit transactions. The thieves also had stolen terminal keys used to encrypt PINs, which are normally stored on a retailer's terminal controllers as conveyed by Gartner. The encrypted PIN information, along with the key for decrypting it and the card numbers, allow criminals to make counterfeit cards. The increase in such frauds has drawn legal attention in the US.

In February 2006, Representative Barney Frank (D-Mass.), the leading Democrat on the House Financial Services Committee, sent a letter to both MasterCard and Visa urging the companies to disclose the source or sources of the compromise or take responsibility themselves. Visa responded in an E-Mailed statement that it understood the need for quickly giving financial institutions the information needed to protect themselves and cardholders from losses in the event of a security breach. In the statement released it was stated that accusing a single source of the compromise before completion of investigation could be inaccurate and unfair. In the same way, revealing the name of the compromised entity would become a dominant disincentive for the compromised entity to share time-sensitive information with Visa going forward.

MasterCard, on the other hand, did not respond to requests for comment. Let us understand how the fraud started. According to a source, working for a company now, helping law enforcement officials investigate the fraud, most evidence suggests that point-of-sale systems at a California store of retailer OfficeMax were somehow involved in the compromise. As per the source, "All roads are pointing in that direction." However, it is still not clear precisely how the debit card and PIN information was accessed and who accessed it. According to the officials at least 200,000 cards may have been compromised.

OfficeMax did not respond to calls for comment, but a company spokesperson was quoted in various other media reports as denying any breach at the retailer. According to Gartner', OfficeMax officials' outright denial suggests that the source of the compromise may well be a third-party processor used by the company to process card transactions. Another company, whose name got mentioned in connection with the debit card fraud wave, is wholesaler Sam's Club, a division of Bentonville, Arkansas-based Wal-Mart Stores. It was acknowledged by Sam's Club, in December 2005, that it was cooperating with credit card associations in investigating reports of fraud involving approximately 600 cards used to purchase gas at its gas stations between 21 September 2005 and 5 December 2005. The company issued another statement soon in response to persistent rumors and false media reports tying it to the existing wave of PIN debit fraud.

The company denied that any of its internal systems had been compromised and said that a review of its gas payment systems by its own staff and an outside party revealed no breach. As the statement released, if any compromise did take place, it appears to have been limited to the Sam's Club fuel station point-of-sale system and did not involve PIN-based transactions.

## 11.5 Digital Signature-Related Crime Scenarios

In this section, we present examples of crimes related to “digital signatures.” This section has two parts: Part I contains the scenarios illustrating offenses under the Indian IT Act and Part II has the scenarios to illustrate examples of fake or inaccurate data inside a certificate from Public Certifying Authorities (CAs). The scenarios presented in this section are listed in Table 11.4.

### 11.5.1 Part I: Offenses Under the Indian IT Act

Some background is necessary in understanding the scenarios presented in this section; especially for readers who have not yet read the previous chapters. First, the relevant section of the Indian IT is quoted and then the crime scenario is presented. Table 1.1 of Chapter 1 provided *cybercrime statistics* – item number 6 in that table is about *obtaining license or digital signature certificate by misrepresentation/suppression of fact*, item number 7 is about *publishing false digital signature certificate* and item number 8 is about *frauds in digital signature certificate*. The topic of digital signature is a key one in the world of cybersecurity – the topic was addressed in detail in Chapter 6. For understanding cryptography, encryption and digital signatures, Ref. #2, Books, Further Reading.

Digital signatures are electronic signatures. The fundamental idea in digital signature is to use the concept of traditional paper-based signing and turn it into an electronic “fingerprint.” The “fingerprint,” or coded

**Table 11.4** | List of illustrations in Section 11.5

Mini-Case No.	Title	Topic	Chapter Cross Reference
<b>Part I</b>			
1	Situation 1	Digital Signature Certificate – Misinterpretation of Information Provided	Chapters 1 and 6
2	Situation 2	Digital Signature Certificate – Suppression of Information by Applicant	Chapters 1 and 6
3	Situation 3	Digital Signature Certificate – False Certificate	Chapters 1 and 6
4	Situation 4	Digital Signature Certificate – Retaining a Rejected Certificate	Chapters 1 and 6
5	Situation 5	Digital Signature Certificate – Retaining a Certificate Beyond its Validity Period	Chapters 1 and 6
6	Situation 6	Digital Signature Certificate – Fraudulent/Unlawful Use	Chapters 1 and 6
<b>Part II</b>			
1	Illustration 1	Bait to Upgraded Digital Certificates	Chapters 1 and 6
2	Illustration 2	False Certificates Issued by Multiple Public Certifying Authorities	Chapters 1, 5 and 6

message, becomes the unique aspect of both the document and the entity who signs it. It binds the signer of the document to the document. *The purpose of digital signature is to ensure that the entity who has signed the document is authentic.* It helps minimize the risk of “non-repudiation,” that is, any changes made to the document after it is signed will make the signature invalid thereby protecting against signature forgery and information tampering. Digital signature aids organizations to maintain signer authenticity, accountability, data integrity and non-repudiation of electronic documents and forms.

The concept of “digital signature” has a context to the concept of non-repudiation. The most common application of this concept is in the verification and trust of signatures. As per legal practice of traditional days, a signature on a paper contract or memorandum may always be repudiated by the signatory. Such repudiation takes place in two forms: The signatory may claim fraud or forgery – for example, a party might say “I did not sign the document.” Alternately, the party may accept the signature as authentic but dispute its validity due to coercion, that is, the party might state that he/she was asked to sign under gun point, or under the threat of physical torture, etc.

Non-repudiation is a very powerful concept especially in the Internet age where electronic commerce is here to stay. Non-repudiation helps ensuring that one or more parties involved in a contract, especially one agreed to via the Internet, cannot later deny it. In the context of “digital security,” non-repudiation is a means to verify that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively. Put simply, non-repudiation is the ability for a system to prove that a specific user and only that specific user sent a message and that it has not been modified (during transmission), for example, due to a “man-in-the-middle” attack in Chapter 4 (explained in Section 4.4 and Fig. 11.7).

To establish additional context for the discussion in this section as well as for understanding the legal aspects involved, we allude to the Indian IT Act. The key provisions under the Indian ITA 2000 are presented in Table 11.5. Section 71 of the Indian IT Act has not changed after the amendment (refer to Table 6.7 in Chapter 6).



*According to Section 71 “Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, 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.”*

#### *Section 71 of the Indian IT Act applies to:*

1. A person, who, for obtaining a digital signature certificate
  - A. makes a “misrepresentation” to the Certifying Authority;
  - B. suppresses any material fact from the Certifying Authority.
2. A person obtaining a license to operate as a Certifying Authority
  - A. makes a “misrepresentation” to the Controller;
  - B. suppresses any material fact from the Controller.

“Misinterpretation” is interpreted as *presenting information incorrectly, improperly or falsely.* There must be a deliberate intention to deceive. Now, let us understand the implications of these legal provisions in terms of some practical scenarios.

**Table 11.5 | Cybercrimes punishment (partial reproduction of Table 1.7 of Chapter 1)**

<i>Section Ref. and Title</i>	<i>Chapter of the Act and Title</i>	<i>Crime</i>	<i>Punishment</i>
Sec. 71 (Penalty for Misinterpretation)	CHAPTER XI OFFENCES	Making misinterpretation or suppressing material facts for obtaining license or Certificate	Imprisonment to term extendable up to 2 years or with fine up to ₹ 1 lakh (₹ 1,00,000) or both
Sec. 73 (Penalty for publishing Digital Signature** Certificate false in certain particulars)	CHAPTER XI OFFENCES	Publishing false digital signatures, false in certain particulars.	Fine of ₹ 1 lakh (₹ 1,00,000) or imprisonment of 2 years or both.
<i>Note:</i> In the IT Act amendment of year 2008, there is no change made to this section, that is, Section 73			
Sec. 74 (Publication for fraudulent purpose)	CHAPTER XI OFFENCES	Publication of digital signatures for fraudulent purpose.	Imprisonment for the term of 2 years and fine of ₹ 1 lakh (₹ 1,00,000).
<i>Note:</i> In the IT Act amendment of year 2008, there is no change made to this section, that is, Section 73			

\*\* In the IT Act Amendment, you will see the word “Electronic Signature” instead of “Digital Signature.”

### *Situation 1: Digital Signature Certificate – Misinterpretation of Information Provided*

Let us say a person “A” is applying for a digital signature certificate. He fills in his name as “B” and also submits photocopies of B’s passport as proof of identity for example documents such as the Driver License or PAN Card. (which can also be seen as “identity theft”!). Under this circumstance, is liable for misrepresenting information to the CA.

 See Table 11.5 – “Suppress” under this scenario is interpreted as “withholding from disclosure.”

### *Situation 2: Digital Signature Certificate – Suppression of Information by Applicant*

Suppose an organization “XYZ” is applying for a license to become a Certifying Authority (CA). In the application form one of the information required to be filled is “In case any of the company directors been convicted for a criminal offense, then please mention relevant details.” Suppose one of the company directors had been convicted in the past. However, in the submitted form, the company officials do not provide answer to this question, that is, they leave that field on the form blank. Under this circumstance, the officials will be liable for suppressing information from the Controller.



"Material fact" implies something that is relevant, pertinent or essential. The punishment provided is imprisonment up to 2 years and/or fine up to ₹ 1 lakh (₹ 1,00,000) as mentioned in Table 1.7 in Chapter 1.

As defined in Section 2(g) of the Indian IT Act, *Certifying Authority means a person who has been granted a license to issue a Digital Signature Certificate under Section 24.*

As per Section 24, *procedure for grant or rejection of license. The Controller may, on receipt of an application under subsection (1) of Section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the license or reject the application: provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.*

Now let us look at some "false certificate" scenarios. First, let us revisit Section 73 of the Indian IT Act (refer to Table 11.5).



#### As per **Section 73 of the IT Act:**

- (1) No person shall publish a Digital 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 purpose of verifying a digital signature created prior to such suspension or revocation.
- (2) Any person who contravenes the provisions of sub-section:
  - (a) 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.

#### *Situation 3: Digital Signature Certificate – False Certificate*

A person creates a fake digital signature certificate with the illicit intent to make the victim believe that the certificate has indeed been issued by a certain CA. Person A now plans to use this certificate to carry out some financial frauds with the targeted victim. He posts this certificate on his website. The person shall be liable under this Section 73.

#### *Situation 4: Digital Signature Certificate – Retaining a Rejected Certificate*

Person A has applied to a Certifying Authority [refer to "CA" definition in Section 2(g) of the Indian IT Act as mentioned previously] for a digital signature certificate. In due course of time, the said CA issues the certificate to Person A. However, Person A does not accept it on the basis that some of the details are incorrect in the certificate. In the meanwhile, the CA publishes the certificate in their online repository. In this case, the CA will be liable under Section 73 of the Indian IT Act (*Penalty for publishing [Electronic Signature] Certificate false in certain particulars*).

### *Situation 5: Digital Signature Certificate – Retaining a Certificate Beyond its Validity Period*

Person A is employed with XYZ Company. He obtains a digital signature certificate for official purposes on 1st February in a certain year. He quits the job on 1 November of the same year and the certificate is revoked on that very same day. Now suppose, XYZ Company continues to keep Person A's revoked certificate in their online repository even after 1 November, that is, even after the person has quit the organization. Under this circumstance, XYZ Company is liable under this section. However, they will not be liable if the purpose behind keeping Person A's certificate in their repository is to verify documents signed by the person between 1 February and 1 November. The punishment provided for this Section 73 is imprisonment up to 2 years and/or fine up to ₹ 1 lakh (₹ 1,00,000).



**As per Section 74 of the IT Act:** *Whoever knowingly “creates,” “publishes” or otherwise makes available a Digital 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.*

Technologically speaking, creating a Digital Signature Certificate is not very difficult – fraudsters are getting technologically very sophisticated! All that is needed is a computer running the Windows Server operating system and having Certificate Services installed. This way, it is easy for criminals to create and publish digital signature certificates for fraudulent and unlawful purposes.

The word “create” in the context of Indian IT Act means “to bring into existence.”

### *Situation 6: Digital Signature Certificate – Fraudulent/Unlawful Use*

Person A is under possession of a computer with Windows Server operating system running on it. She also has *Certificate Services* installed on that computer. She uses this computer to generate a digital signature certificate for herself and Person B. This means that now she has created the said certificates. Next, Person A puts up Person B's digital signature certificate onto a publicly accessible part of his website. This means that now Person A has published Person B's certificate. Note that “publishing” means “making the certificate known to others.”

The concept of “make available” can also be illustrated by extending the situation just mentioned. Suppose now, Person A using the same computer under her possession and running the services as mentioned before on that computer, issues this certificate to Person C – knowing or not knowing that Person C plans to misuse it to spoof Person B's E-Mails. Under these circumstances, Person A has made the certificate available to Person B for an unlawful/fraudulent purpose. The punishment provided for violation of Section 74 is imprisonment up to 2 years and/or fine up to ₹ 1 lakh (₹ 1,00,000)

#### **11.5.2 Part II: Fake/Inaccurate Data in Certificates from Public Certifying Authorities**

Having presented scenarios of digital signature certificate-related offenses under the Indian IT Act, now let us look at some examples of (a) bait to consumers to lure them to upgrade their digital certificates and (b) fake or inaccurate data inside a certificate from a public CAs.

### *Illustration 1: Bait to Upgraded Digital Certificates*

In a typical scenario, the targeted consumers receive an E-Mail informing them that their financial accounts will be more secure if they are upgrade to digital certificates, or that their current digital certificate has expired and needs to be upgraded. If they follow the link, they are taken to a website where they receive more information about the importance of the upgrade, and are given instructions to “install” their digital certificate, with a link to download the installation program.

If the targeted consumers, fooled in this way, believe the mail and install the program then the result is that, a virus gets installed! The first such digital certificate malware investigated was found to be against Bank of America. It ended in early April 2008; however, the new round of such attacks included Comerica Bank, Colonial Bank and Merrill Lynch. Comerica was nearly a daily target with more than 250 domain names used in the fraud. Colonial Bank was targeted for the attack in 2008, with 22 domain names used. An attack was launched on Merrill Lynch, on 5 May 2008 with the domain names – such as 1291logon.info and 1291logon.com.

The Merrill Lynch version of the malware is called “Papras.dk” by most of the antivirus programs that detect it. The first edition of the Colonial Bank Trojan was called “Papras.dh,” and the first version of the Comerica Bank Trojan that we looked at was called “Papras.dc.” There were more evidences showing that these originated from a common source. As with most up-and-coming threats, common antivirus products are not instantly blocking the threat. For example, F-Prot, McAfee and Symantec do not show on VirusTotal as having discovery for this threat. McAfee engineers are often heard complaining that VirusTotal is not an accurate way of knowing whether they have detection. They say that when McAfee is run on desktops, though an antivirus update is run, it does not detect some of the viruses. Unfortunately, due to the failure of common antivirus engines to detect this virus, the viruses can spread faster.

### *Illustration II: False Certificates Issued by Multiple Public Certifying Authorities*

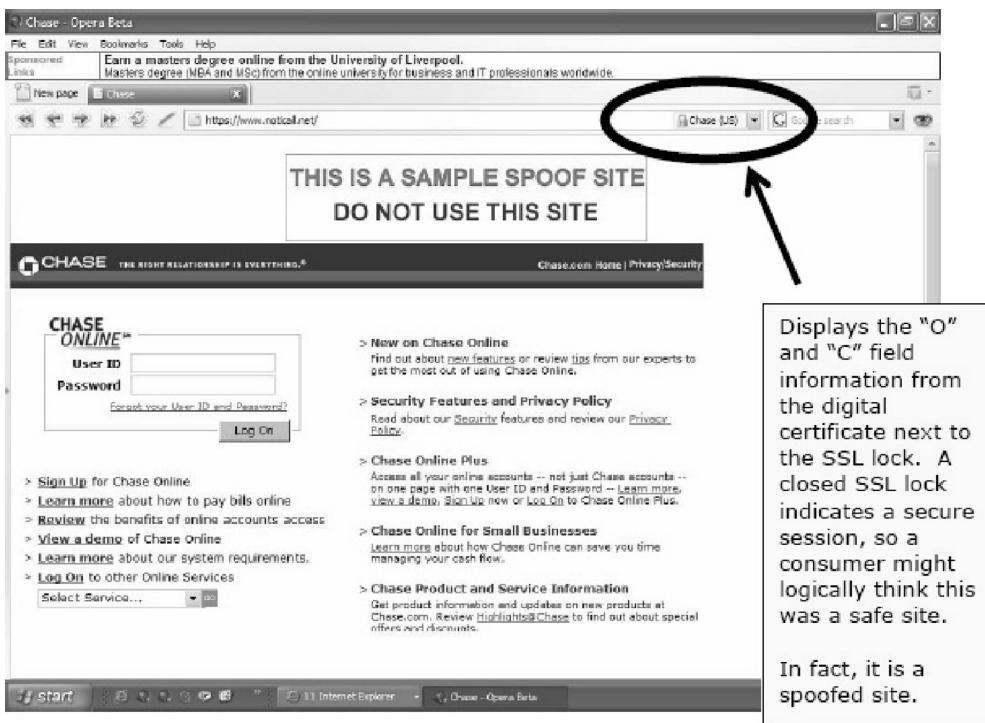
There have been instances wherein false certificates have been obtained on a number of occasions from numerous public CAs without ever submitting any false information in the process. You can visit the link <http://www.geotrust.com/resource/advisory/sslorg/index.htm> to see live examples. For this illustration, we have included three screen shots (Figs. 11.12–11.14) to illustrate how certificates with misleading organizational names could be used to enhance Phishing schemes:

#### **Example 1:**

Refer to Fig. 11.12, it is a spoofed chase site. It shows a misleading organizational name of “Chase” in O Field. Note the display of O (Organization) and C (Country) field data [“Chase (US)"] in the circled (yellow) field at top right of the GUI. This is not a genuine Chase Bank site. It is an example of how the organization field could be used by a phisher to more convincingly perpetrate fraud. Reader should refer to Chapter 5 to understand “Phishing attacks.”

#### **Example 2:**

Refer to Fig. 11.13, it shows another site with a misleading organizational name “Fleet” in the O Field. Note the display of O and C field data [“Fleet (US)"] in the circled (yellow) field at the top right of the GUI. This is not a genuine Fleet Bank site. It is interesting to understand how misleading certificates are obtained. Apparently, certificate containing inaccurate or potentially fraudulent identity information can be easily obtained – typically through Identity Theft crimes as explained in Chapter 5.



**Figure 11.12 |** Spoofed chase site.

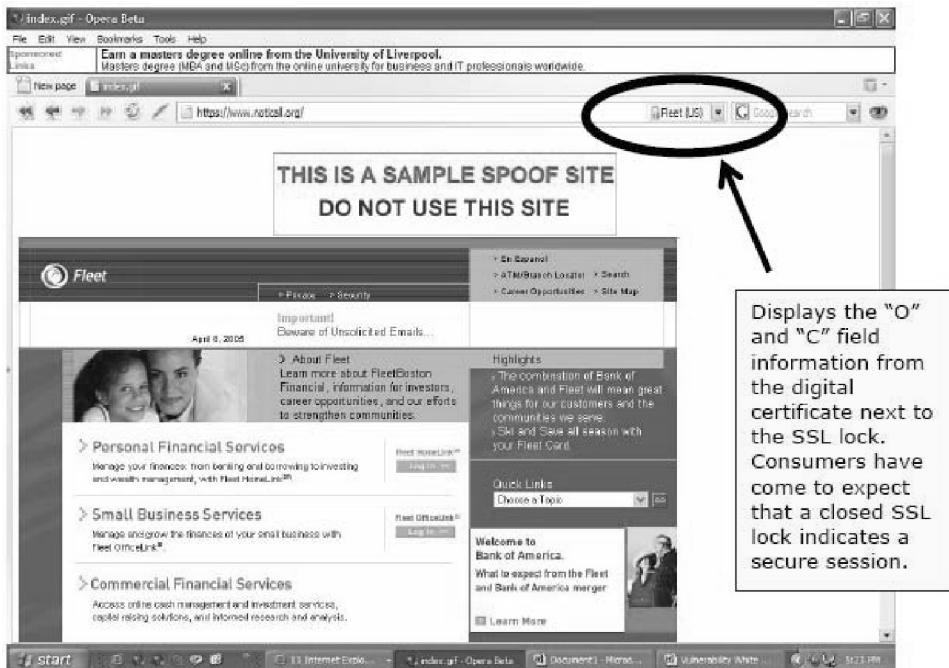
Note: The color version of the figure is also available in the CD.

Fraudulent identity information is often obtained from multiple public CAs without ever submitting any false information in the process. Phishers and fraudsters do not care about obtain fake digital certificates to date because consumers have never looked at or relied upon the identity information in the certificate; in fact, most consumers do not even know it is there – but this will all change if next-generation browser GUIs extract and display certificate data in an attempt to provide users with site identity information for trust decision purposes.

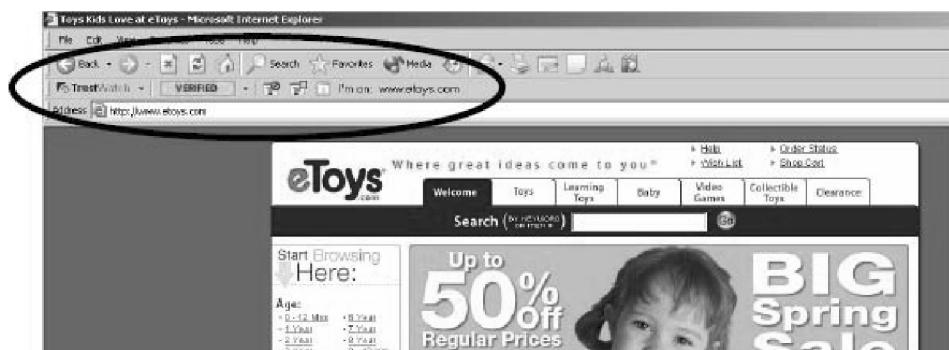
Trust capabilities of websites need to be enhanced and the solution for this is “2nd Generation Digital Certificates” (further details on this are not within the scope of this illustration or this chapter). A variety of browser plug-ins and toolkits are already offered for this purpose, including GeoTrust’s TrustWatch. TrustWatch applies its rules and algorithms in real-time (including checking on certificate CN field data for certificates located anywhere on the visited website, even when the consumer has only started with the site’s unsecured home page) and displays the result in a color-coded GUI that is easily seen and understood by consumers. Additional enhancements are coming in the near future (see Fig. 11.14 – see the color version of this figure in CD).

The private sector has developed a number of seals and certifications designed to provide varying degrees of confidence in the practices or controls over privacy and personal information.

Some Organizations with such programs are: TRUSTe, BBBOnLine, Network Advertising Initiative, US Direct Marketing Association, Japan Information Processing, Development Center (JIPDEC), Health Information Trust Alliance, EuroPrise.



**Figure 11.13** Site with misleading organization name.  
Note: The color version of the figure is also available in the CD.



**Figure 11.14** GUI enhancement.  
Note: The color version of the figure is also available in the CD.

## 11.6 Digital Forensics Case Illustrations

Forensics tool kits are addressed in Chapters 7 and 8. Digital Forensics Case Studies are presented in this section. These illustrations involve use of the forensics tools EnCase and TSK. While going through the cases illustrations in this section, do keep in mind the “chain of evidence” and other related concepts explained in Chapter 7. Table 11.6 lists the digital forensics cases of this section.

**Table 11.6** | Illustrations in Section 11.6

<i>Digital Forensics Case Illustration No.</i>	<i>Title</i>	<i>Topic</i>	<i>Chapter Cross Reference</i>
1	Confidential Data Theft Revealed through Forensics Investigation	Data Theft	Chapters 1 and 9
2	Analysis of Seized Floppy – The Drug Peddler Case	Digital Forensics Evidence Analysis	Chapter 7
3	Vehicle Stealing Racket Revealed Through Computer Forensics Investigation	Digital Forensics Reporting	
4	Child Pornography revealed through Computer Repair	Digital Forensics Reporting	Chapters 1, 6 and 7

### 11.6.1 Digital Forensics Illustration 1: Confidential Data Theft Revealed through Forensics Investigation

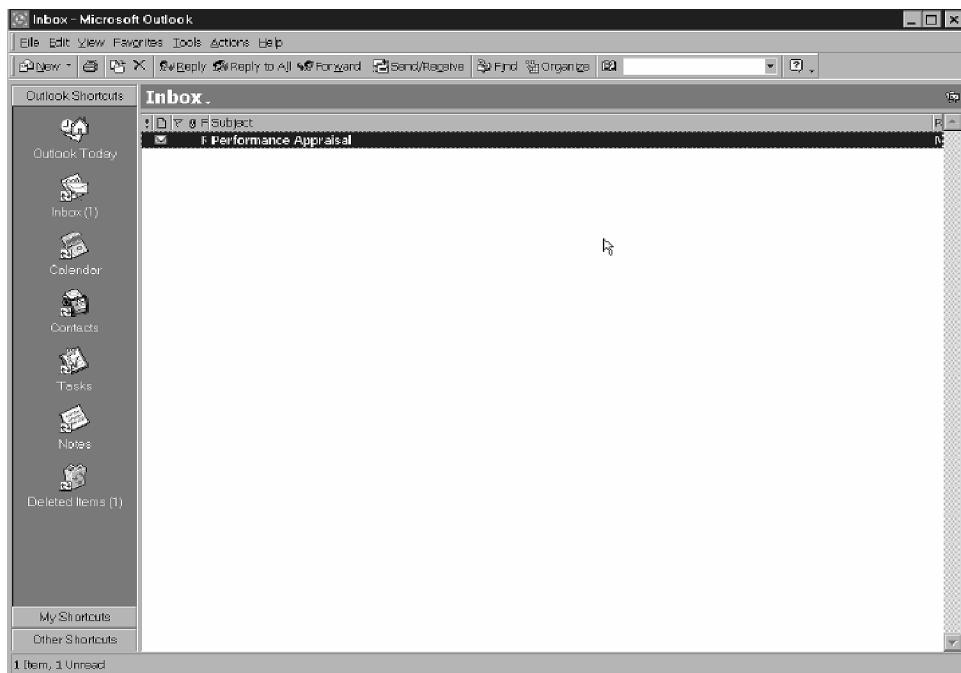
“Data theft” is a wide term ranging for theft and fraud committed by stealing most valuable information. The purpose is to obtain data without any financial as well as manpower investments. Under Section 66 of the amended Indian IT Act, “data theft” definition has become more specific. Stealing data is a crime. In this illustrative example we see what disgruntled employees can seek revenge. In Chapter 1 (Section 1.4) we mentioned about Type II – Cybercriminals – the “Insiders”; these are disgruntled employees or former employees seeking revenge. Chapter 9 also addressed the issue of Data Theft (see Section 9.2). This example shows a scenario with that. All the names are masked for confidentiality; however, the scenario is from real life. This example illustrates the power of forensics investigation. (The topic of forensics is explained in Chapters 7 and 8 and that is the background for this illustrative case.) It is a very educative example for readers and relates to all the concepts learned so far. Read on

Ajay Shirgaokar an employee of POOR-ME COMPANY receives a poor performance appraisal from his manager (see Fig. 11.15). Ajay sends an inquiry to a competitor organization, looking for a position via E-Mail followed by a letter asking for the same, using a company letterhead. Ajay receives a job application from UNSCRUPULOUS\_COMPANY (the competitor company) – see Fig. 11.16.

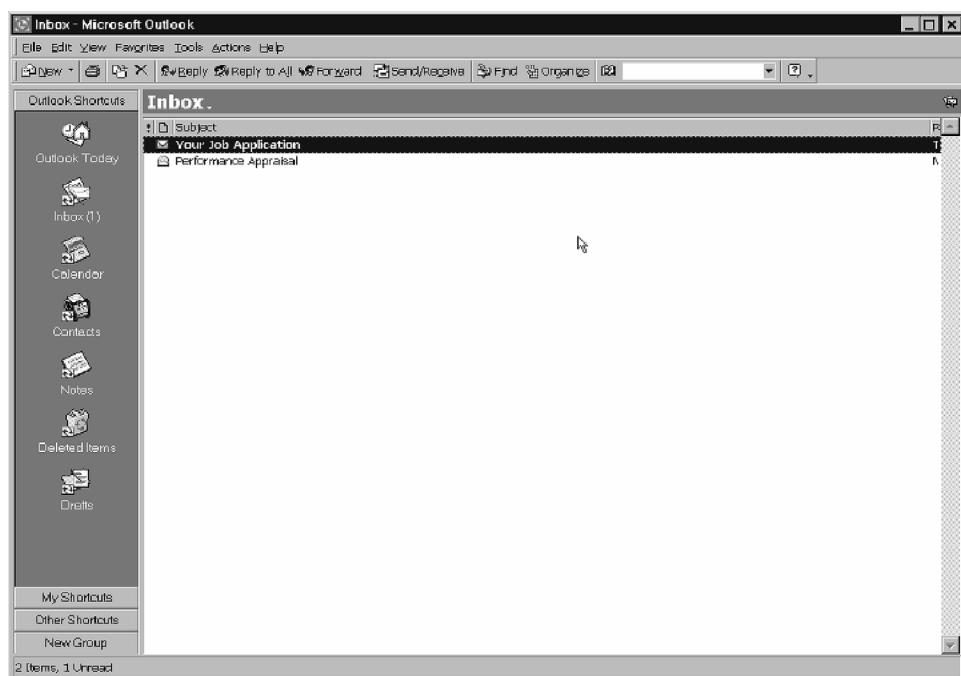
In a meeting with UNSCRUPULOUS\_COMPANY, they propose a plan to him about getting some urgently required information from POOR-ME COMPANY. Ajay Shirgaokar agrees to steal proprietary information in exchange for a job and a payoff. He is given a 4 GB USB Flash drive with detailed guidance describing how to steal and transmit proprietary information. Ajay Shirgaokar reads the directions on how to use a “cracker” program (see Fig. 11.17).

Ajay Shirgaokar sends a Trojan program as an attachment to E-Mail to members of the Product development team (“Trojans” are explained in Chapters 2 and 4). The attachment appears to be legitimate ... a solicitation for a good cause – “donation request” (see the screen shot in Fig. 11.18). A member of the Product team, Madhav Lele of POOR-ME COMPANY opens the E-Mail and the attachment (see Fig. 11.19).

The attachment sent to Lele is a Trojan Horse program that will allow remote access to and control of Lele’s machine. Now Ajay Shirgaokar is in a position to access Lele’s machine remotely. Figure 11.20 shows



**Figure 11.15** | Employee getting performance appraisal mail.



**Figure 11.16** | Employee receives mail from competitor organization.

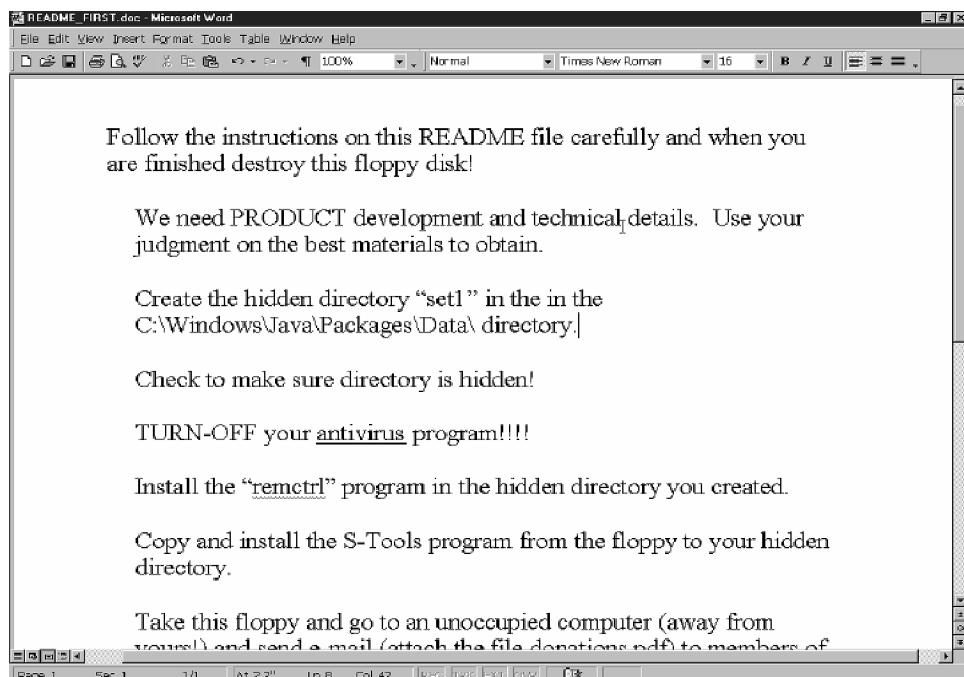


Figure 11.17 | Employee reading a malicious program instructions.

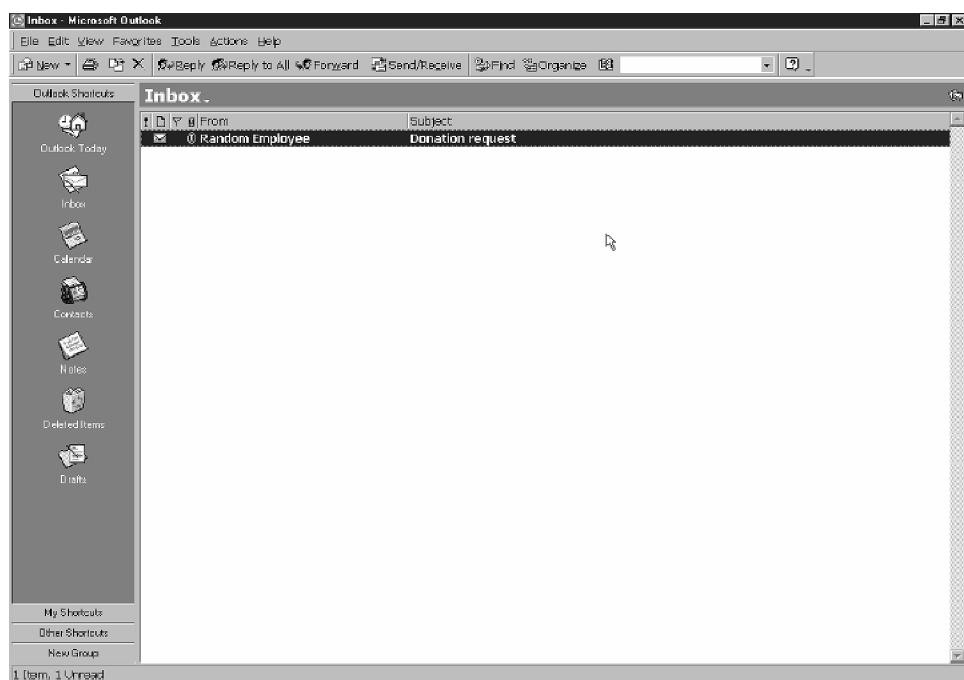
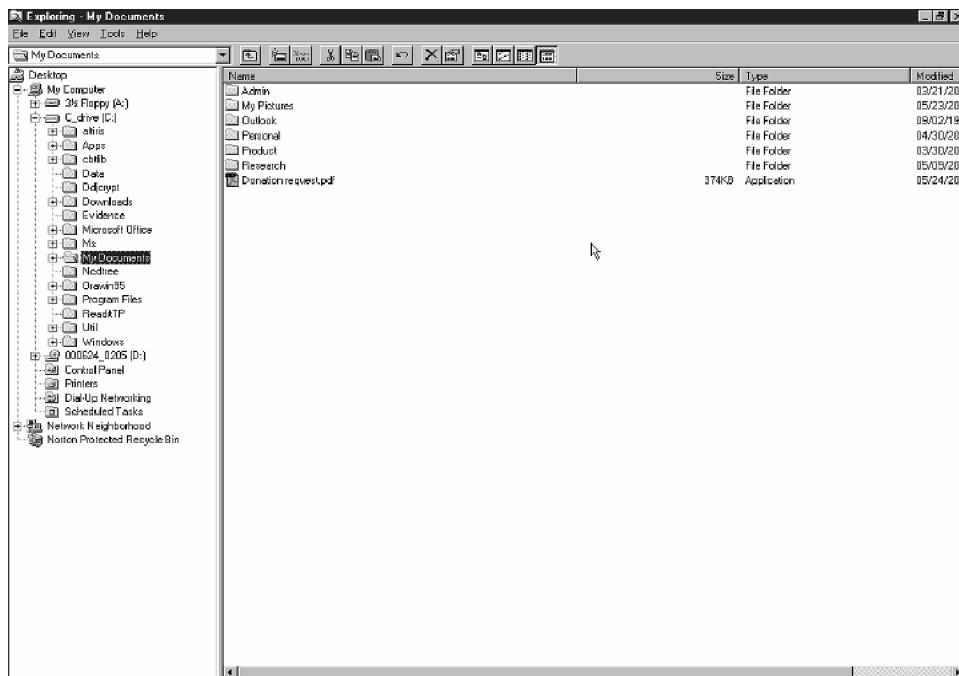
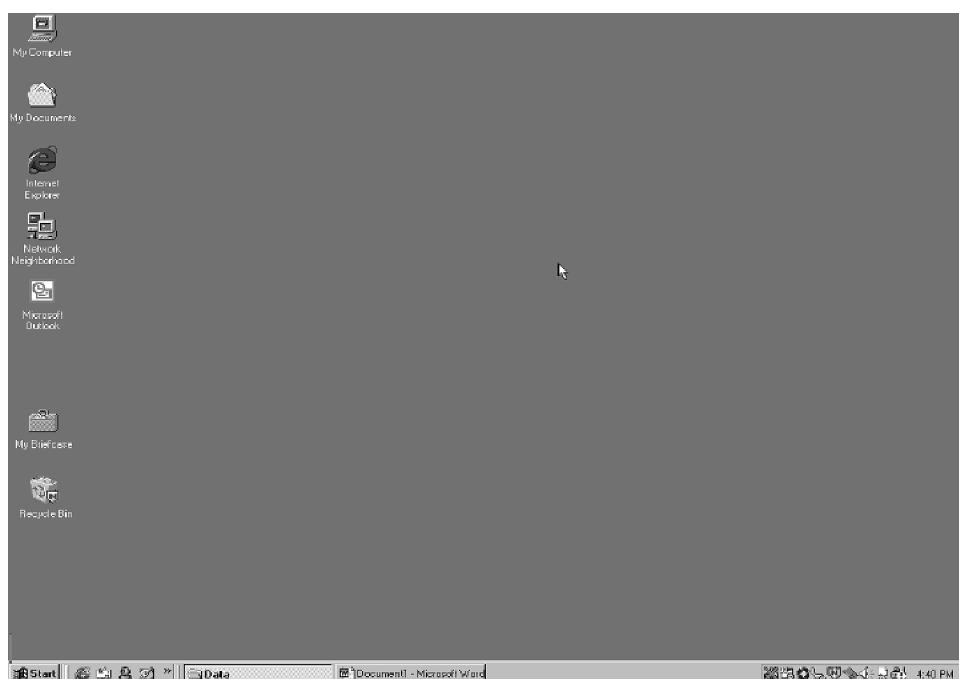


Figure 11.18 | Ex-organization's employee reading the mail containing malicious attachment.



**Figure 11.19** | Donation request mail planted as bait by the revengeful employee.



**Figure 11.20** | Suspect employee's desktop.

Ajay Shirgaokar's desktop. Having stolen the company confidential information, Ajay is now driven by the pressing need to transfer it to his soon-to-be new employer, eager to impress them that he has done the "job." In order to conceal his activities, Ajay uses E-Mail and Steganography (secret writing) to hide the stolen data in plain sight (see Fig. 11.21).

After some days, news about Competition Company (UNSCRUPULOUS\_COMPANY) appears in the media. The news indicates that the company is all poised to demonstrate their next version of the product months ahead of the schedule. The news also mentions that the CEO of the company has sent a special memo congratulating his R&D team for this fantastic achievement. In the same news, the industry analyst are quoted stating that through this early prototype development, the company will be able to introduce their competition product to the market very soon and that the product has the potential to take away a major slice of sales revenues from the competition. Industry analysts, in this news, further add saying that the prospects for other industries in the same product domain are now bleak.

Alerted by this news item, POOR-ME COMPANY engages forensics investigators to determine whether a "foul play" has lead to the loss of their data. The investigators monitor POOR-ME COMPANY's Intranet (with appropriate authority) using forensics monitoring devices (such tools and devices were explained in Chapters 7 and 8). Figure 11.22 shows an intercept of password crack to get into the account of the disgruntled employee.

The forensics monitoring devices used in the investigation provide the investigators with a target to focus their investigation. With client consent, a document likely to be stolen, a document likely to be stolen, is "tagged" to provide tangible proof

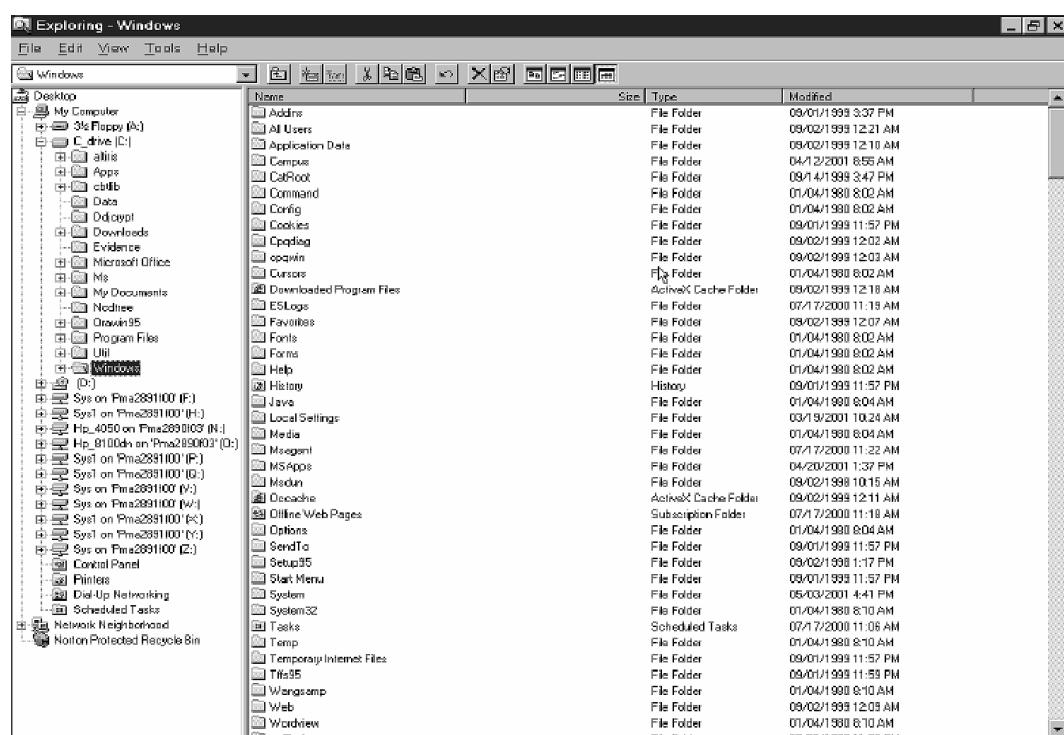


Figure 11.21 | The data dump from suspect employee machine.



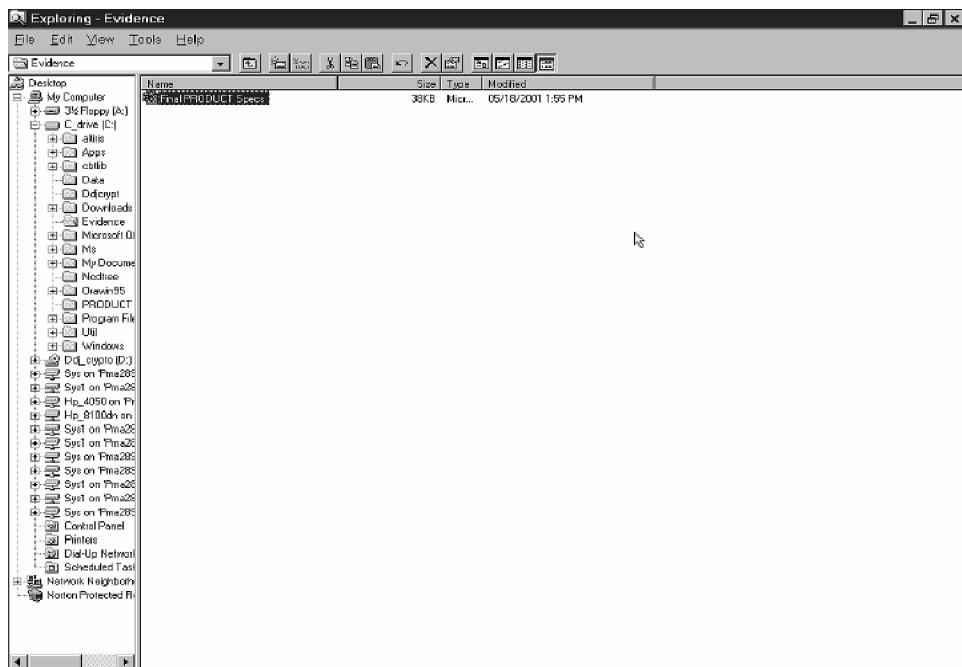
```
[**] SubSeven - Remote Login with Password [**]
05/18-16:41:47.216487 192.168.100.3:1075 ->
192.168.100.30:27374
TCP TTL:128 TOS:0x24 ID:8983 DF
*****PA* Seq: 0x1403328 Ack: 0x41A588 Win:
0x2235
```

**Figure 11.22** | The cracked account.

of intellectual property theft and support later litigation and damages claims. In Fig. 11.23, we see investigators “tagging” a document, followed by its hex dumps seen in Fig. 11.24.

Meanwhile, Ajay once again, covertly accesses Lele’s computer to steal intellectual property (PRODUCT). His actions are the same as explained before. Investigators are keeping a close trail and they record Ajay’s actions as evidence against him (refer to Fig. 11.25). With his final theft complete, Ajay Shirgaokar deletes all stolen documents and exploitation programs from his workstation – see the screen shot of his workstation in Fig. 11.26. Now that Ajay has taken the “bait” document, the investigators perform covert digital evidence recovery on Ajay’s employer who is supplied with a Palm Pilot (a kind of hand-held device) and workstation. Hand-held forensics is explained in Chapter 8. The investigators conduct a forensics review of a copy of the digital evidence (refer to Figs. 11.27–11.30).

The presence of the “stego” pass phrase alerts investigators to look for file types that can be used for Steganography. Using a variety of digital forensics tools, the investigators examine Ajay’s workstation. The Palm Pilot gave away his passwords and account data and other valuable information such as the use of Steganography. The hard drive examination allowed to recover deleted files and to look for “stego” files (Steganography). Steganography in forensics context is explained in Chapter 7 (Section 7.12). Figures 11.31 and 11.32 show how the forensics tool reported the case. Recall that in Chapter 8, we explained the reporting features of the forensics tools (refer to Table 8.4 in Chapter 8).



**Figure 11.23** | The tagged document.

The screenshot shows the 'HexEdit' application window with the file 'C:\EVIDENCE\Final PRODUCT Specs.doc' open. The left pane displays the hex dump of the file, showing memory addresses from 0 to 180 and their corresponding hex values. The right pane shows the ASCII representation of the same data, where most bytes are FF (hex) and some are G, I, F, and other characters. A vertical scroll bar is visible on the right side of the hex dump pane.

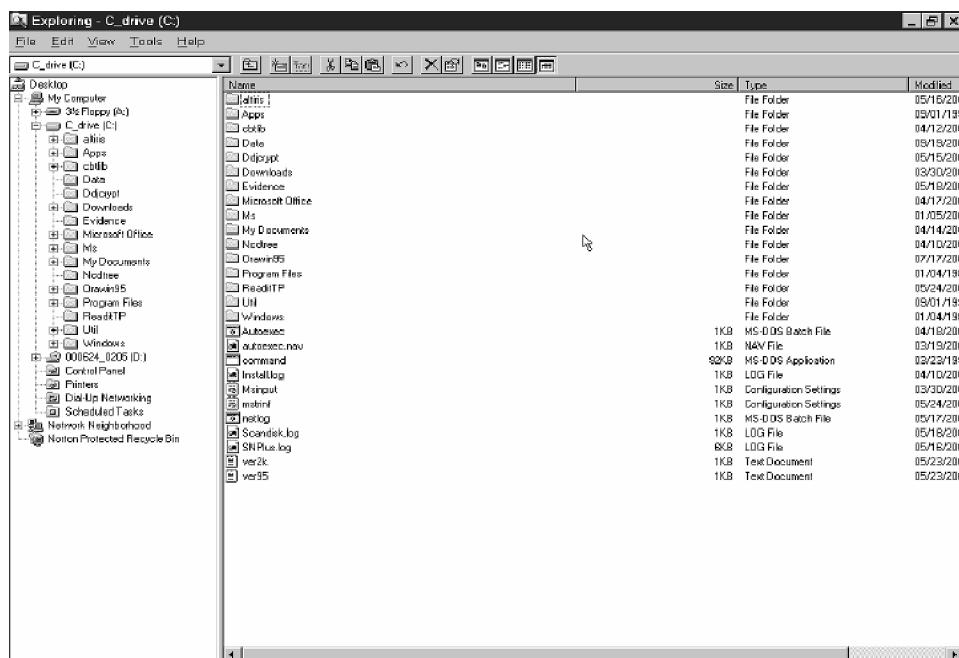
Address	Hex Value	ASCII Value
0	40 cf 11 e0 al b1 la el 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....>.....I.....F.....
10	00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00	.....
20	06 00 00 00 00 00 00 00 00 00 00 01 00 00 00	.....
30	47 00 00 00 00 00 00 00 00 10 00 00 49 00 00 00	.....
40	01 00 00 00 fe ff ff 00 00 00 00 46 00 00 00	.....
50	ff	.....
60	ff	.....
70	ff	.....
80	ff	.....
90	ff	.....
a0	ff	.....
b0	ff	.....
c0	ff	.....
d0	ff	.....
e0	ff	.....
f0	ff	.....
100	ff	.....
110	ff	.....
120	ff	.....
130	ff	.....
140	ff	.....
150	ff	.....
160	ff	.....
170	ff	.....
180	ff	.....

**Figure 11.24** | The hex dumps.

```
[**] SubSeven - Remote Login with Password [**]
05/29-16:58:12.099543 192.168.100.3:1075 ->
192.168.100.30:27374
TCP TTL:128 TOS:0x24 ID:8983 DF
*****PA* Seq: 0x1403328 Ack: 0x41A588 Win:
0x2235

[**] SubSeven - File Manager - Download from C
Drive [**]
05/29-17:01:30.180677 192.168.100.3:1075 ->
192.168.100.30:27374
TCP TTL:128 TOS:0x24 ID:33559 DF
*****PA* Seq: 0x1403361 Ack: 0x42DA32 Win:
0x1FA0
```

**Figure 11.25** | Trail on the forensically cracked account.



**Figure 11.26** | “Cleaning” the tracks act.



Figure 11.27 | Digital evidence recovery-1.

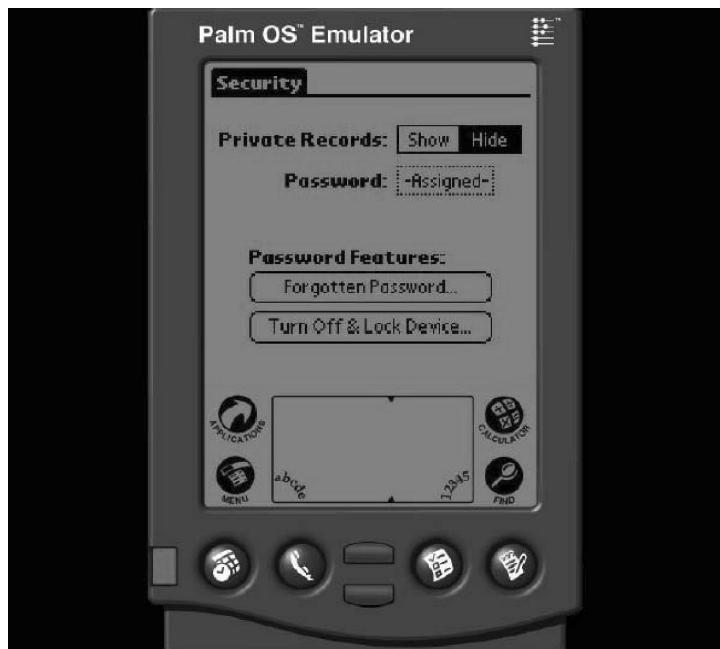


Figure 11.28 | The digital evidence recovery-2.

```
[root@localhost PalmOS]# infodump
Using port /dev/pose
Press the HotSync button now...

Card Info:
-----
Manufacturer: Palm Computing
Name: PalmCard
ROM Size: 3341058
RAM Size: 4194304
Free Memory: 2074818
ROM Version: 53489664

Battery Level = 2.54
(warning marker; 2, critical; 1.6)

Device Clock: 15:57:06 05/19/2001 GHT

User Info:
-----
User name: Mike
User ID: 1256425162
Password hash: ab8c852138b057f5c65c64ad585ca609e58c626df690d47d32bef3675ff9b837
Password clear: adam-12

[root@localhost PalmOS]#
```

Figure 11.29 | The digital evidence recovery-3.

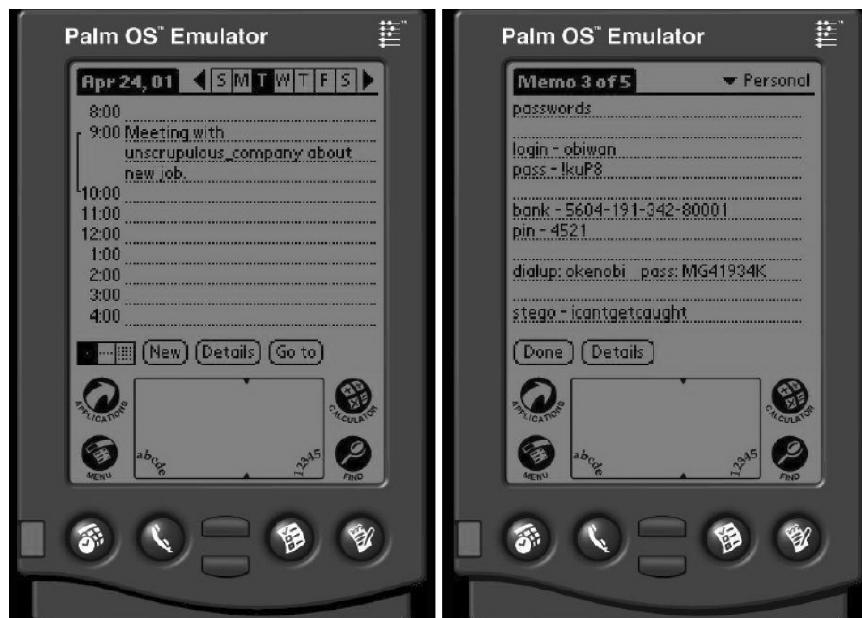


Figure 11.30 | More evidence.

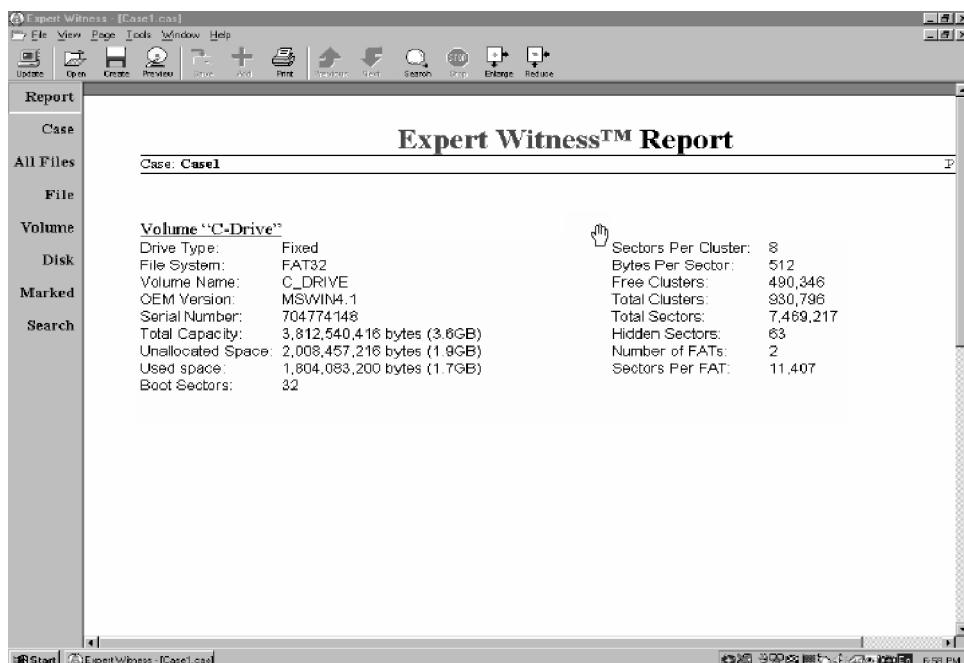


Figure 11.31 | Case report from the forensics tool-1.

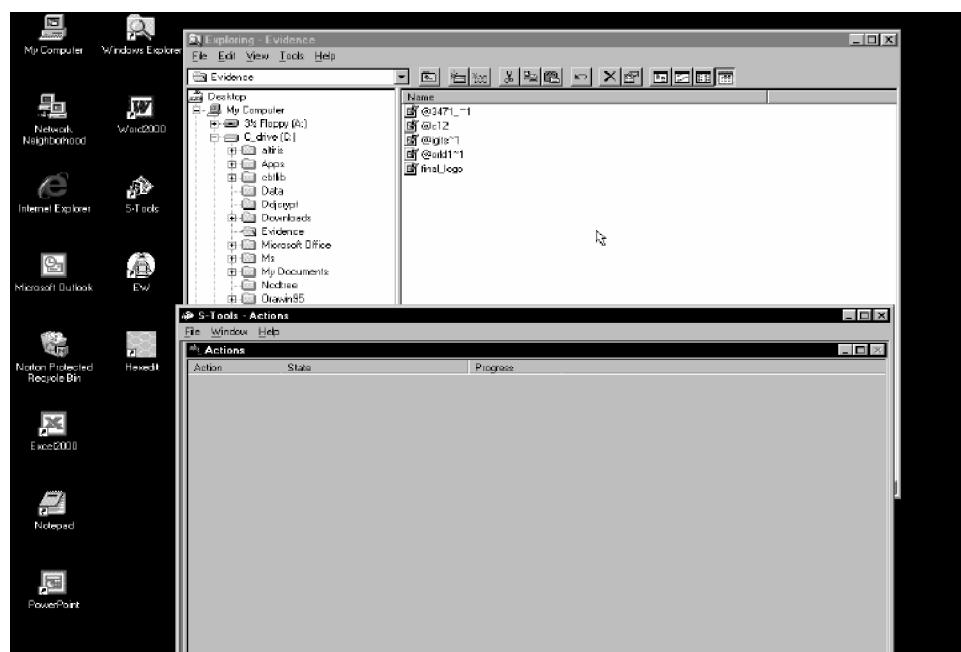
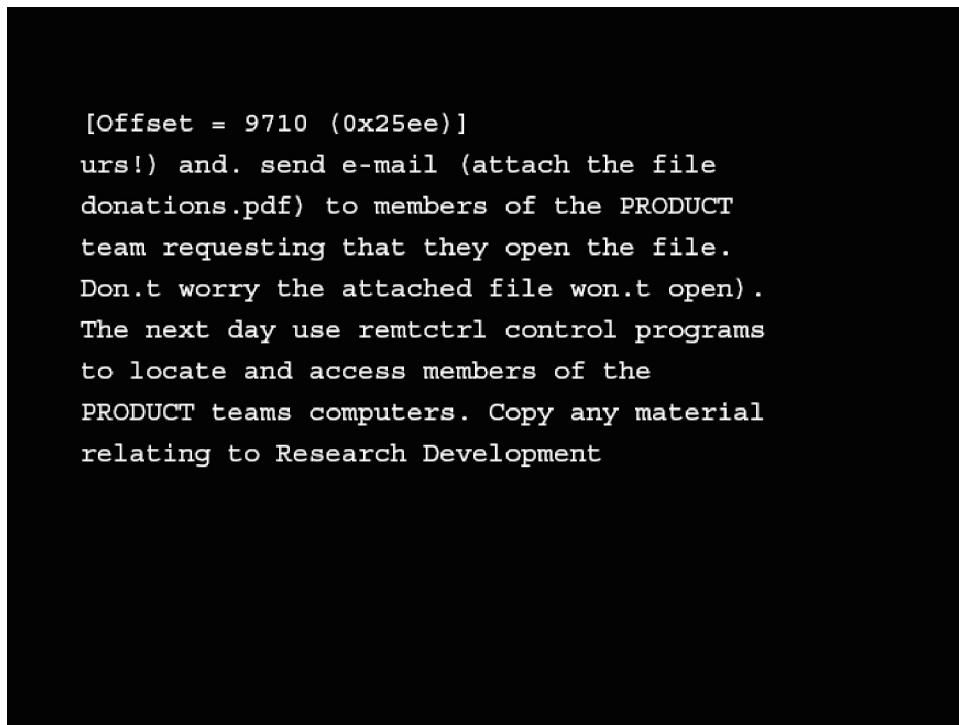


Figure 11.32 | Case screen from the forensics tool-2.



**Figure 11.33** | Evidence on the hard disk.

Figure 11.33 shows the evidence recovered from employee's hard disk drive. With the digital evidence supplied by the investigators (as well as other steps not demonstrated, that is, E-Mail examinations, interviews, analysis of Internet traffic, etc.) POOR-ME COMPANY filed suit against UNSCRUPULOUS\_COMPANY for intellectual property theft. Thus, to conclude, in this example we learned about the extent of malicious damage that disgruntled employees can do.

### 11.6.2 Digital Forensics Case Illustration 2: Analysis of Seized Floppy – the Drug Peddler Case

Use of digital forensics technique in a case of selling drugs to school children is illustrated here. In Chapter 7 types of media were displayed (Fig. 7.6 in Chapter 7). This illustration involves data recovery from a floppy disk. While reading this illustration, keep in mind the “imaging” techniques and forensics tools, etc. described in Chapter 7 (Sections 7.7.1 and 7.7.2). Brian Carrier’s Sleuth Kit/Autopsy is mentioned in Section 7.7.2 (above Box 7.10) of Chapter 7. The Sleuth Kit tools are capable of analysing disk or file system images generated by “dd” or similar applications that create a raw image. The “dd” tool (mentioned in Section 7.16.1, Chapter 7) is found on most UNIX systems. TFS, FAT, FFS, EXT2FS and EXT3FS file systems are supported by the tool.

This illustration has the scenario in which that tool was used. The objective in this scenario was to analyze a seized floppy in the hope of recovering information that would help answer question related to the investigation of the crime. Those questions are mentioned later in this illustration. Note that all the links displayed in the diagrams in connection with this illustration can be accessed.

It was suspected that the required information could possibly be hidden within unallocated areas of the disk image or concealed within other areas of the disk and would, therefore, require a full file system analysis in order to locate it. For the sake of reference, let us call the suspect as "Jaggu Jungle" – the bad guy because the real name cannot be disclosed due to confidentiality and privacy considerations. Any resemblance to this name or locations and/or situation in this illustration is purely a coincidence. Some background information and evidence is presented next to help understand the context for the forensics analysis in this digital forensics case illustration. Table 11.7 shows the background for this case illustration; it is based on a police report.

**The Case Scenario:** Jaggu Jungle, 28 years, was arrested on charges of selling illegal drugs to high school students in Delhi. The police set a trap to catch Jaggu. A local young police officer, who posed as a high school student, was approached by Jaggu in the parking lot of St. Stephen's High School. Jaggu asked the undercover cop if he would like to buy some marijuana (a type of drug). Before the undercover cop could answer, Jaggu pulled some out of his pocket and showed it to the officer. Jaggu "Look at this stuff, it couldn't be better than this; I am selling you the best quality stuff! My supplier not only sells it direct to me, he grows it himself."

As per police reports, Jaggu had been spotted on numerous occasions hanging out at various local high school parking lots around 2:30 pm, the time school usually ends for the day. School officials from multiple high schools had called the police regarding Jaggu's presence at their school and noted an increase in drug use among students since his arrival.

The police needed forensics help. They wanted to try and determine if Jaggu Jungle has been selling drugs to students at other schools besides this school. The problem is that no students will come forward and help the police. Based on Jaggu's comment regarding the drug supplier, the police were interested in finding Jaggu's supplier/producer of marijuana. Jaggu denied selling drugs at any other school besides this school and refused to provide the police with the name of his drug supplier/producer. He also refused to validate the statement that he made to the undercover officer right before his arrest.

Upon issuing a search warrant and searching the suspect's house, the police were able to obtain a small amount of marijuana. The police also seized a single floppy disk, but no computer and/or other media was present in the house. The police imaged the suspect's floppy disk and provided a copy for forensics investigation. They wanted the forensics analysts to examine the floppy disk and provide answers to some questions regarding this drug crime. The police wanted forensics experts to pay special attention to any information that might prove that Jaggu was in fact selling drugs at other high schools besides this school where the undercover police encountered him. Police also wanted forensics experts to try and determine, if possible, who Jaggu's supplier is.

Jaggu's posted bail was set at ₹ 4.5 lakhs (₹ 4,50,000). Considering that Jaggu may attempt to run away from town, the police wanted him to be under police custody as soon as possible. To do so, the police had asked the forensics experts to fully complete the analysis results and wanted the results to be submitted by the given date. Now it was a challenge for the forensics experts to provide the police with a strong case consisting of their specific findings related to the questions police had in mind:

1. Where the findings are located on the disk?
2. What were the processes and techniques used?
3. Any actions that the suspect may have taken to deliberately delete, hide and/or alter data on the floppy disk.

The objective of this examination is to seek answers of the following questions:

1. Who was the supplier of marijuana and what was the address listed for the supplier?
2. What crucial data is available within the “coverage.jpg” file and why is this data crucial?
3. What (if any) other high schools, in addition to St. Stephen’s High School, did the criminal frequent?
4. For each file, what processes were carried out by the suspect to hide them from others?
5. What processes were used to effectively examine the complete contents of each file?

### Step 1: Analysis

The first step of the analysis process was to retrieve the image of the floppy disk. The disk image was downloaded and the MD5 hash value was also copied from the website and placed into a valid “md5sum” input file called “image.zip.md5” – contents of “image.zip.md5” were as follows:

```
b676147f63923e1f428131d59b1d6a72 image.zip
```

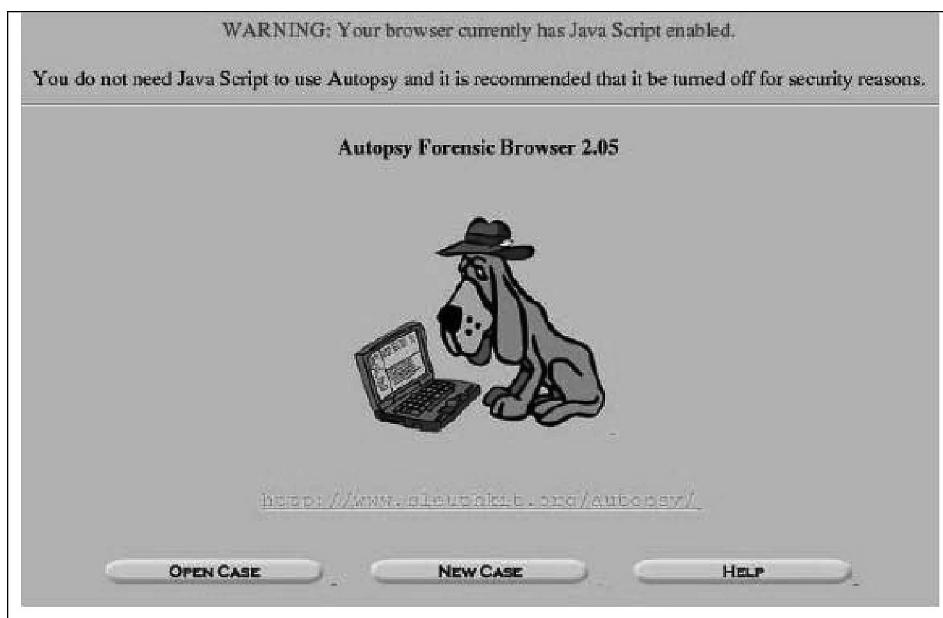
Confirmation that the integrity of the downloaded disk image has not been compromised is as follows:

```
# md5sum -c image.zip.md5
Image.zip: OK
```

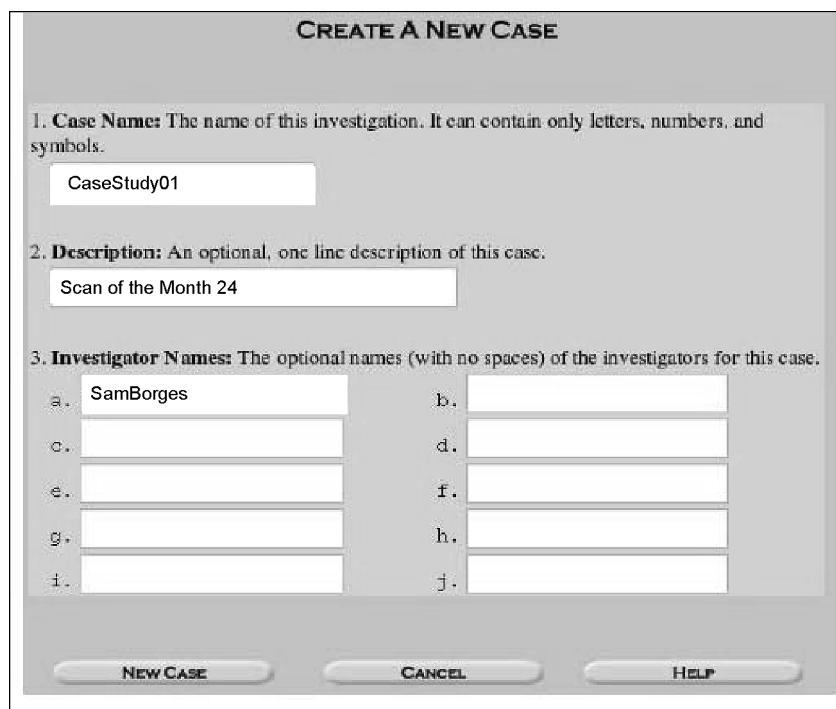
### Step 2: Autopsy Case Creation in the Tool

Having confirmed that the integrity of the downloaded image has not been compromised, a case was configured within Autopsy. Autopsy was setup and configured on the analysis machine and was ready to be used. From the Autopsy main menu (Fig. 11.34), the “New Case” button was selected in order to start the configuration process for a new case.

The next task was to prepare an input from recording the details of the case. Using the “Create a New Case” form (Fig. 11.35), a case name, short description and an investigator’s name were entered. The investigator’s name was used mainly for audit processes. One typical problem with Autopsy is that it does not allow the



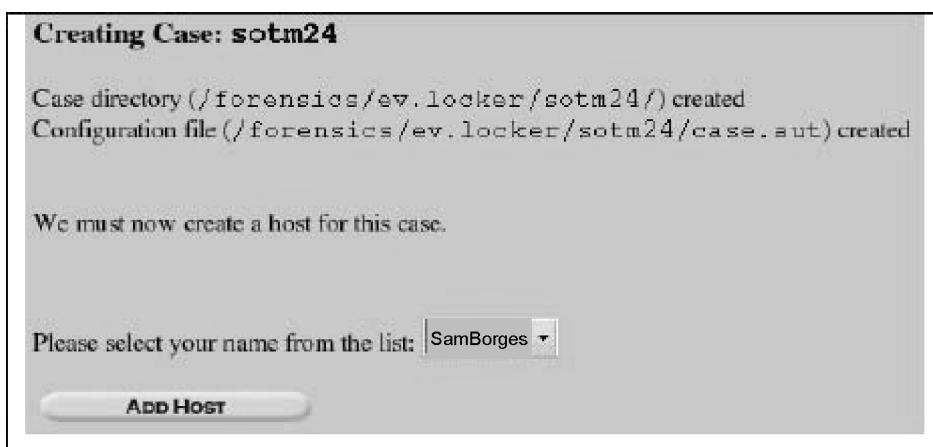
**Figure 11.34** | Autopsy case creation.



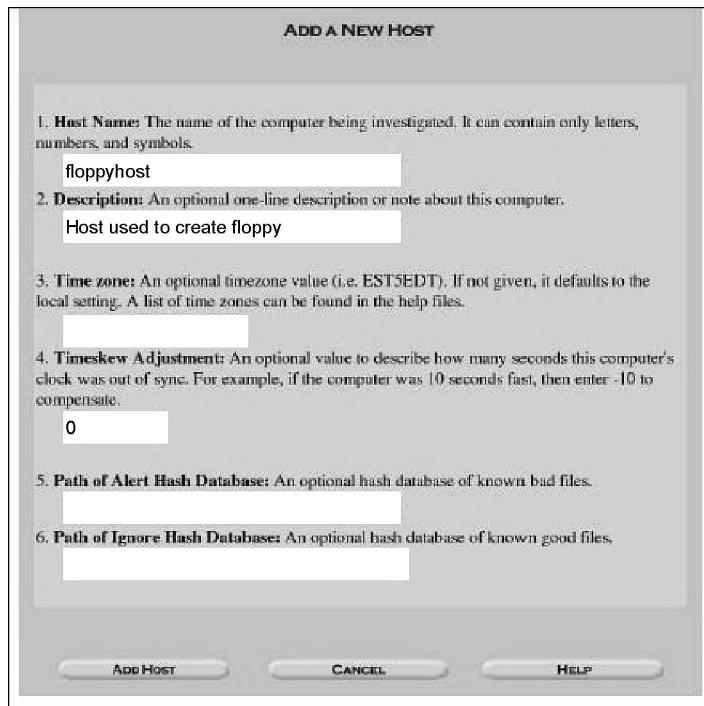
**Figure 11.35** | Autopsy new case creation.

investigator's name to contain any spaces. In order to use an investigator's full name one would need to concatenate it into a single string, for example "Sam Borges" would need to be entered as "SamBorges."

Having configured the initial values, a case directory was created in the evidence locker, and a standard configuration file was created within the case folder (see Fig. 11.36). If more than one investigator would have been assigned to this case, then at this stage, an investigator would need to be selected before adding a



**Figure 11.36** | Autopsy: Case study created.



**Figure 11.37 |** Autopsy: New host added.

host to the case. Autopsy not only saves the output from “The Sleuth Kit” program files to log files named after the investigator, but also the commands that are executed along with other notes entered into the system.

In the scenario involved here, only one investigator’s name was used in the “New Case Creation” form (Fig. 11.35) – so, there was only one name in the drop box. By selecting the “Add Host” button (see Fig. 11.37) the investigator was moved to the next step in the configuration process. This case dealt with an image of a floppy disk rather than an image from a hard disk that was retrieved from a host machine, therefore only generic configuration details are entered into the “Add a New Host” form as illustrated in Fig. 11.37. In this case, the forensics experts knew that they were looking into an IBM compatible floppy disk. These types of disks are formatted with a FAT12 file system. FAT file systems store time stamps without regard to time zones. Therefore, there was no need to enter any time zone information.

In this case, it was not known to the forensics investigators if the time on the machine used to create the floppy disk was skewed from a time source, so nothing was entered for the time skew adjustment value (see Fig. 11.38). An “Alert Hash Database” or “Ignore Hash Database” was not provided for this investigation so these values were left blank. An “Alert Hash Database” is a database that the investigator must create. It contains hashes of known bad files. These are the files that a forensics examiner wants to know about, if they exist on the system. Examples of this include rootkits or illegal photographs. “Rootkit” is a software system that contains multiple programs designed to obscure the fact that a system has been compromised (refer to Box 4.3, Chapter 4 and Section 7.12.1, Chapter 7). An “Ignore Hash Database” is a database that the investigator must create. It contains hashes of known good files and these files can be ignored if the user chooses to do so during File Type Category Analysis. System binaries used for standard builds would be examples of files under this category.



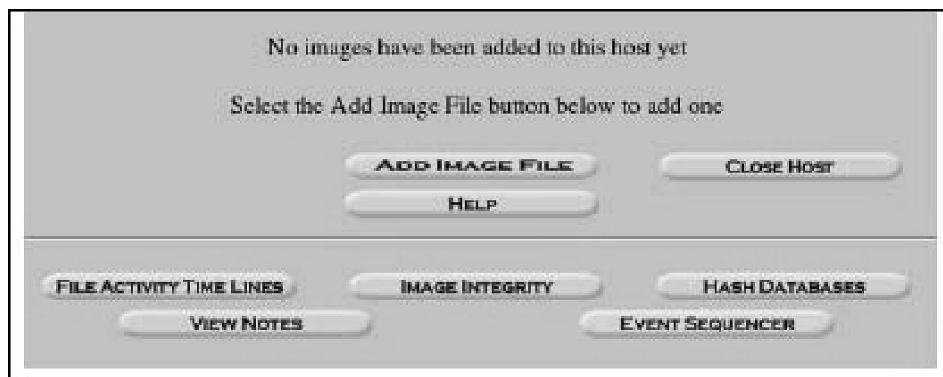
**Figure 11.38 |** Autopsy: Host “floppyhost” added.

Having entered the configuration details for the host, and having selected the button <Add Host>, Autopsy created the Host folder structure within the Case structure inside the evidence locker (see Fig. 11.39). At this stage the Case and Host are created for this investigation. Next, the investigator adds the disk image by selecting the “Add Image File” (see Fig. 11.39).

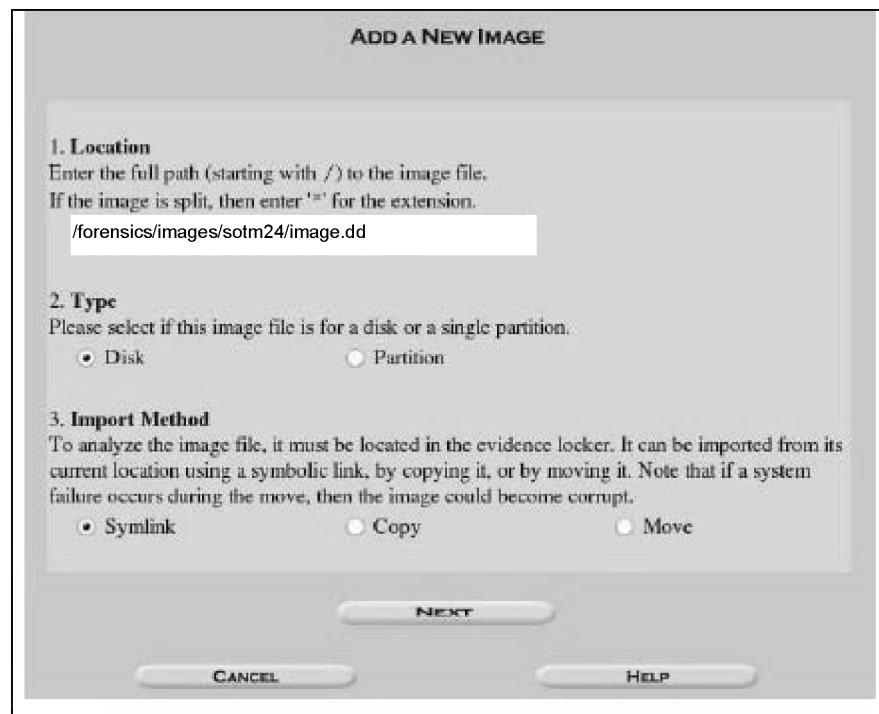
The “Add a New Image” form is now displayed (Fig. 11.40). This form allows the investigator to enter information on the image file. The analysis machine has a separate drive configured for the Evidence Locker to hold the investigation image files, and in order to minimize space requirements the image will be imported as “symlinks” to the original images. In this case, the image file was extracted from the Zip file provided on the website, and it is this image file that was added. A symbolic link (often called “symlink”) is a special type of directory entry in modern UNIX (or Unix-like) file systems that allows the system to almost transparently refer to another directory entry, typically a file or a directory.

Unfortunately, at this stage Autopsy is unable to automatically determine the volume system type for the disk image. Floppy disks are typically single volume; therefore, the investigator had to manually select the “Volume Image” with a “Volume System Type” of “DOS” – refer to Figs. 11.40 and 11.41.

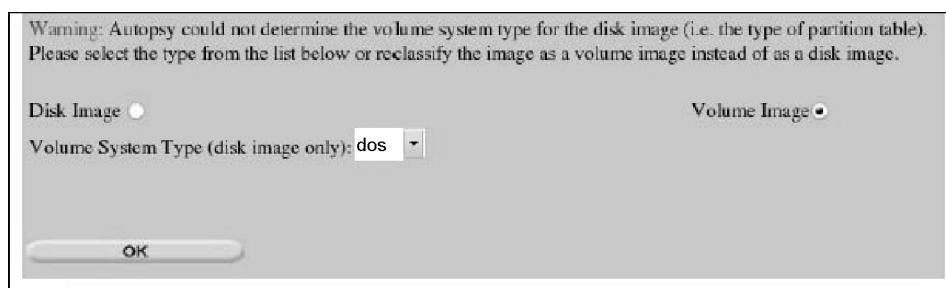
The “Image File Details” section is shown in Fig. 11.42; it allowed the investigator of the case to select options for the data integrity of the image. In Section 7.7.2 of Chapter 7, it is mentioned in that during imaging, a write protection device or application, is normally used to ensure that no information is introduced onto the evidentiary media during the forensics process. The imaging process is confirmed by means



**Figure 11.39 |** Autopsy: Case and host info added.

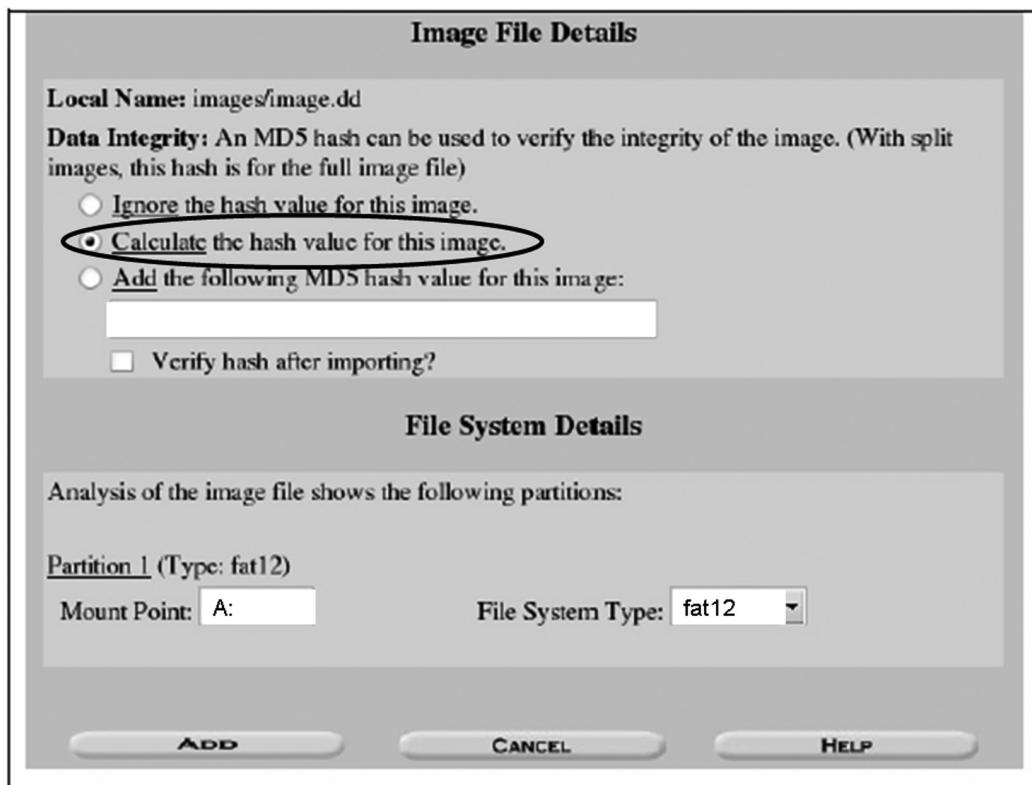


**Figure 11.40** | Autopsy: New image added.



**Figure 11.41** | Autopsy: Image type.

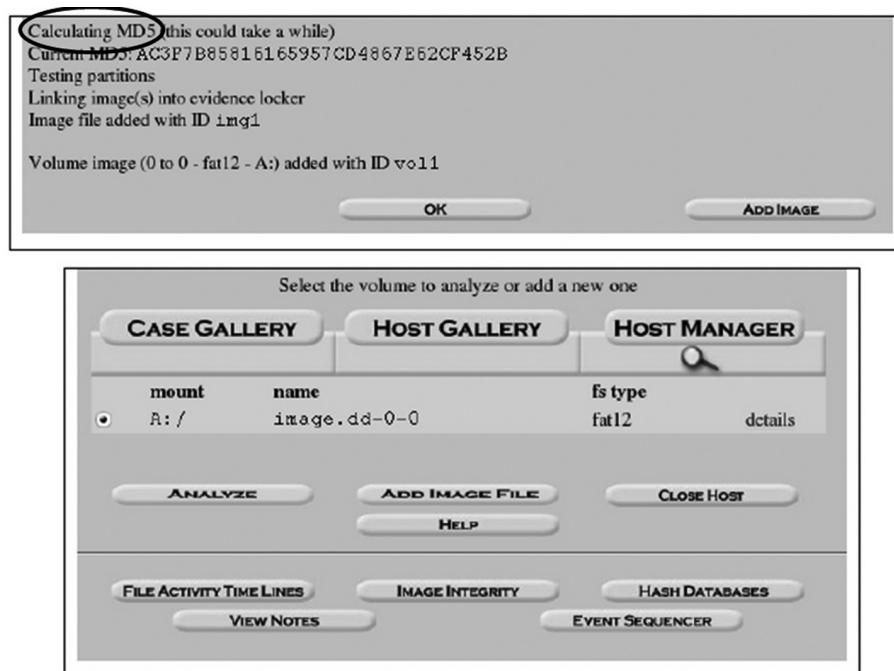
of the SHA-1 message digest algorithm (with a program such as `sha1sum`) or other still viable algorithms such as MD5. If the MD5 hash value for the image file itself was provided, it could be entered here and Autopsy could verify that it is correct. However, for the scenario of this case, no hash value existed for the extracted disk image and therefore the investigator had to select the “Calculate” option because only the MD5 hash value for the compressed archive was provided.



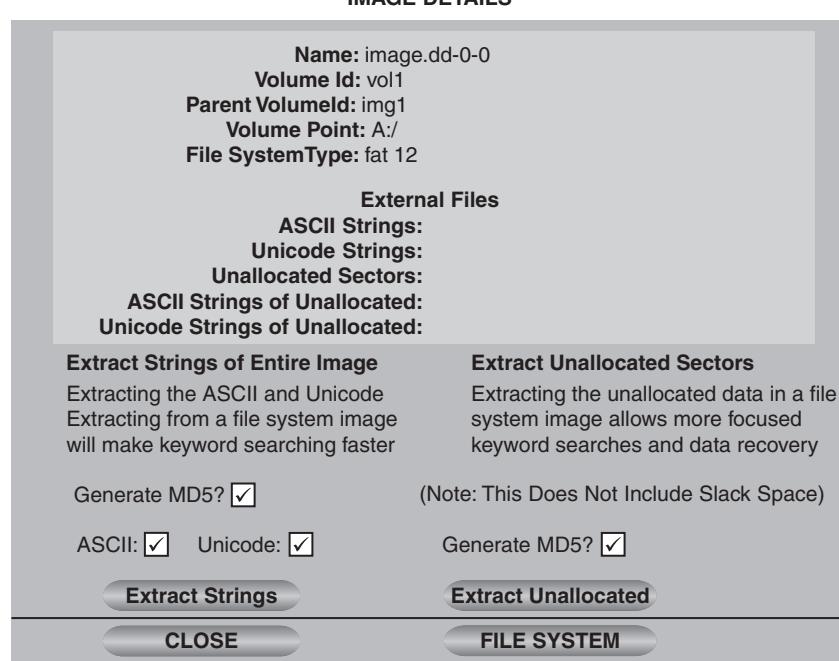
**Figure 11.42** | Autopsy: Image file details.

After entering the Image File Details, Autopsy checks the integrity of the partition image (if the “Verify hash after importing?” option is selected), however for this investigation the “Calculate” option was selected. See Fig. 11.42. Therefore, Autopsy generated an MD5 hash value (these are hexadecimal numbers) and inserted it into the Host configuration – see Fig. 11.43 (upper portion). At this stage a Case has been created, a Host has been created and the floppy disk image has been added to the host. It was explained in Chapter 7 (Section 7.7.1) that to be able to use forensics findings of any type as permissible evidence in court, a data acquisition technique, known as “imaging,” is used. We now see in this illustration, the use of that technique. The Autopsy “Host Manager” is displayed (Fig. 11.43 lower portion) to the investigator and from this point Autopsy can be used to analyze the contents of the floppy disk image.

Now that the investigator came closer to examining the contents of the seized disk, he wanted to create some indexes to help search with keyword searches. By selecting the “details” link from the Host Manager within Autopsy (see Fig. 11.43), the investigators were taken to the “Image Details” form (see Fig. 11.44). This allowed them to extract the strings from the entire image as well as unallocated sectors. Extracting this information caused an index to be created which improved the speed of keyword searches. They selected “Extract Strings,” leaving the default check box marks on “Generate MD5,” “ASCII” and “Unicode.”



**Figure 11.43** | Autopsy – Image File Details (upper) and Host Manager Details (lower).



**Figure 11.44** | Autopsy: String details.

String extraction always depends on the size of the file system. When file systems are larger, the extraction of ASCII and Unicode strings can be quite time consuming; however, the disk image for this investigation was only that of a 1.44 MB floppy disk and therefore the extraction process was quite quick. After extracting the strings, (see Fig. 11.45), the investigation team returned to the “Image Details” screen and selected the “Extract Unallocated” button to extract the unallocated sectors (see Fig. 11.46). Extraction of unallocated sectors also depends on the size of the file system. Much larger time is required on larger file systems and extraction can consume a large amount of disk space, possibly up to the size of the original image. However, as previously mentioned, this investigation involved imaging of a floppy disk of only 1.44 MB in size. Therefore, the extraction process was quick and the extracted data was small.

Having extracted the unallocated sectors (see Fig. 11.47), the investigator returned to the “Image Details” screen and selected the “Extract Strings” button to extract the ASCII and Unicode strings from the unallocated sectors (see Fig. 11.47). Compare the outputs displayed in Fig. 11.47 to the output in Fig. 11.45; you will notice that the values for “String Extraction” are different than those for “Unallocated Sector Extraction.”

When size of file system is large, similar issues, as in the extraction of ASCII and Unicode strings, arise while extracting strings from unallocated sectors. In this investigation, however, the process was relatively quick, because as mentioned previously, this scenario involved an image of a floppy disk. The results of this process are illustrated in Fig. 11.49.

```
Extracting ASCII strings from image.dd-0-0
Host configuration file updated
Calculating MD5 Value

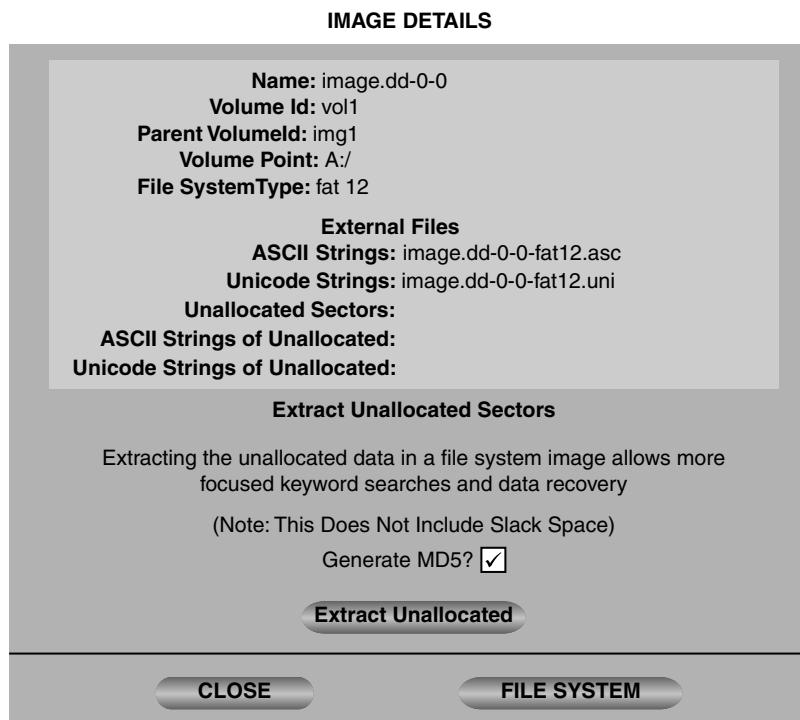
MD5 Value: 662E3DF59F31C8FB8F267DAC585659E3

Extracting Unicode strings from image.dd-0-0
Host configuration file updated
Calculating MD5 Value

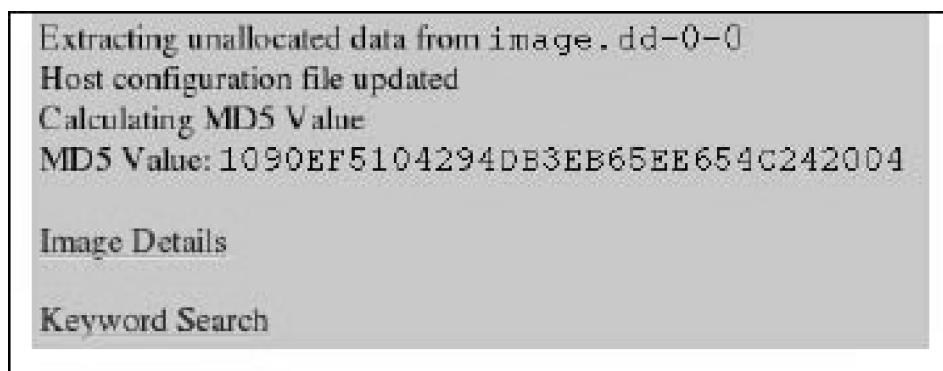
MD5 Value: 69D60C32B05490A54120D1C8D8F8B28A

Image Details
Keyword Search
```

Figure 11.45 | Autopsy: Image details (extracting strings).

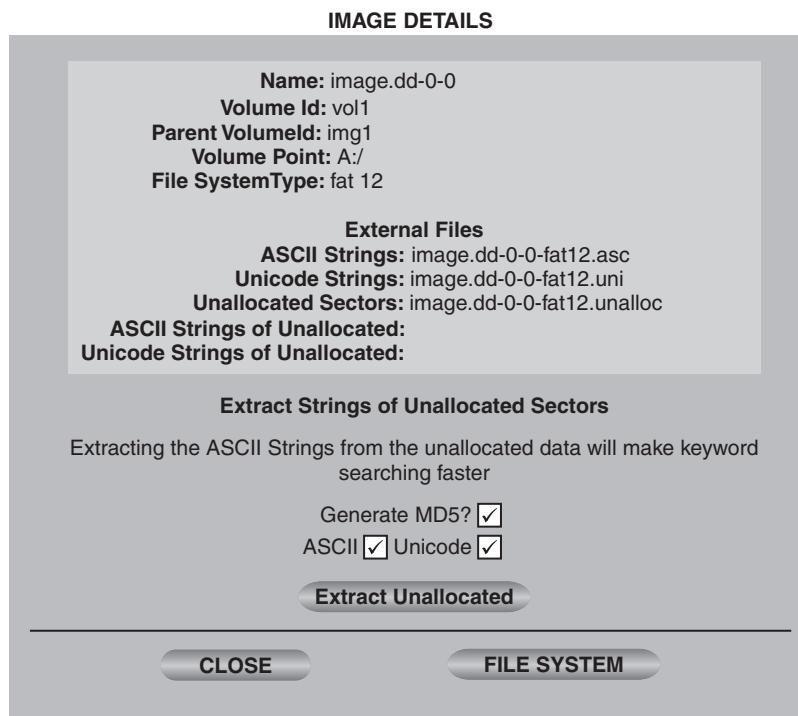


**Figure 11.46** | Autopsy: Image details after extracting strings.



**Figure 11.47** | Autopsy: The result of extracting unallocated sectors.

Next, the investigator created a search index of strings on both allocated and unallocated sectors. With this index constructed, he was able to perform a faster keyword search. All the external files required for the search indexes are seen in Fig. 11.50.



**Figure 11.48** | Autopsy: Image details after the extraction of unallocated sectors.

```
Extracting ASCII strings from image.dd-0-0-fat12.unalloc
Host configuration file updated
Calculating MD5 Value

MD5 Value: 8C574E59AFA549956D0BED8D1F7FF330

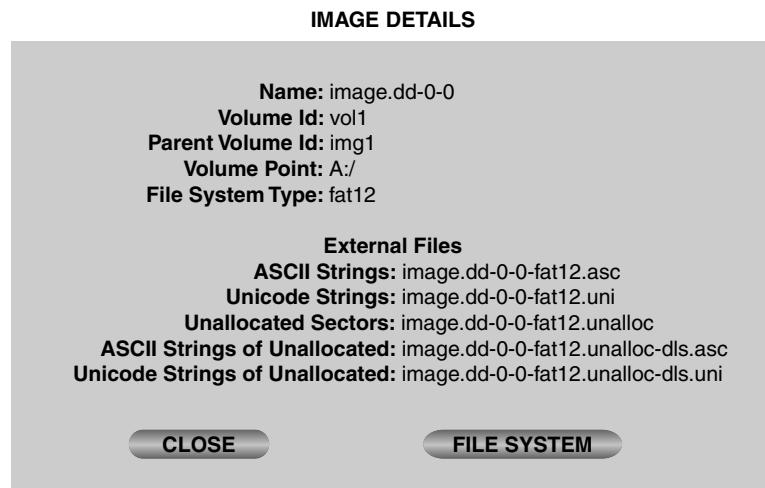
Extracting Unicode strings from image.dd-0-0-fat12.unalloc
Host configuration file updated
Calculating MD5 Value

MD5 Value: 27515A019593B7868FE35C247798AEF1

Image Details

Keyword Search
```

**Figure 11.49** | Autopsy: Result of extracting strings from unallocated sectors.



**Figure 11.50** | Autopsy: Image details of extraction of allocated and unallocated strings.

“File browsing” mode of Autopsy (see Fig. 11.51) was displayed by selecting the “Analyze” button, then selecting the “File from the Host Manager Analysis” button. “File Browsing” mode provided a file manager like view of the contents of the floppy disk image. You can see in Fig. 11.50 that the floppy disk image contains listings for three files as follows:

1. cover page.jpgc (COVERP-1.JPG).
2. Jaggu Jungle.doc (\_IMMYJ-1.DOC) – This file was deleted by Jaggu.
3. Scheduled Visits.exe (SCHEDU-1.EXE).

**FILE ANALYSIS**   **KEYWORD SEARCH**   **FILE TYPE**   **IMAGE DETAILS**   **META DATA**   **DATA UNIT**   **HELP**   **CLOSE**

**Current Directory:** [/](#)

**Directory Seek**  
Enter the name of a directory that you want to view  
**B: /**

**VIEW**

**File Name Search**  
Enter a Perl regular expression for the file names you want to find

**SEARCH**

**ALL DELETED FILES**

**EXPAND DIRECTORIES**

DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	r/r	<u>cover</u> page.jpgc (COVERP-1.JPG)	2002.09.11 08:30:52 (NZST)	2002.09.11 00:00:00 (NZST)	2002.09.11 08:50:26 (NZST)	15585	0	0	8
✓	r/r	<u>Jaggu</u> Jungle.doc (_IMMYJ-1.DOC)	2002.04.15 14:42:30 (NZST)	2002.09.11 00:00:00 (NZST)	2002.09.11 08:49:48 (NZST)	20480	0	0	5
	r/r	<u>Scheduled</u> Visits.exe (SCHEDU-1.EXE)	2002.05.24 08:20:32 (NZST)	2002.09.11 00:00:00 (NZST)	2002.09.11 08:50:38 (NZST)	1000	0	0	11

**File Browsing Mode**

In this mode, you can select a file or directory.  
File contents will be shown in this window.  
More file details can be found using the Metadata link at the end of the list (on the right).  
You can also sort the files using the column headers

**Figure 11.51** | Autopsy: File analysis mode.

Each file was examined to check if it contained information that could be used to answer the questions of this case study accurately. The questions were mentioned under the objectives of this illustration (refer to page 682); they are mentioned below for ready reference of readers:

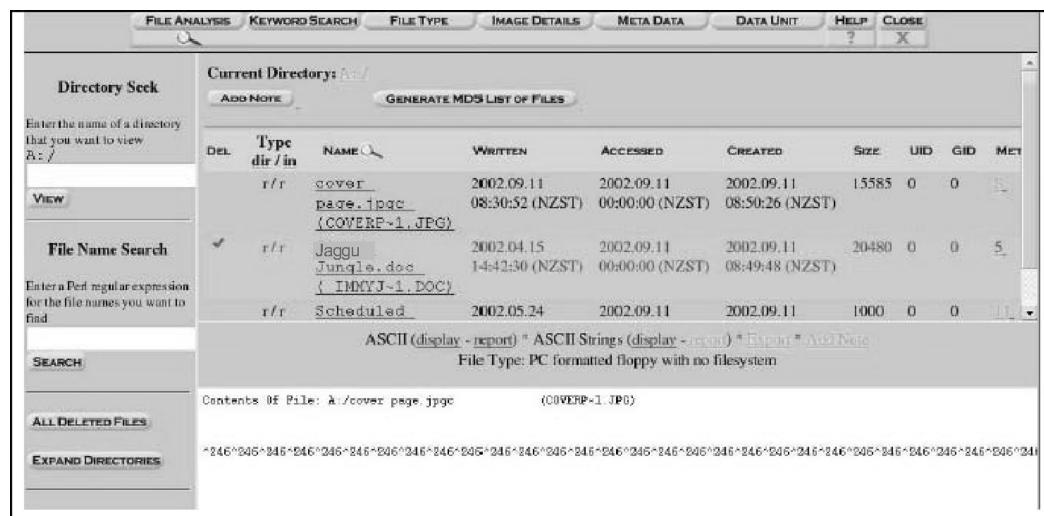
1. Who was the supplier of marijuana and what was the address listed for the supplier?
  2. What crucial data is available within the “coverpage.jpg” file and why is this data crucial?
  3. What (if any) other high schools besides Saint Stephen’s High School did the criminal frequent?
  4. For each file, what processes were taken by the suspect to hide them from others?
  5. What processes were used to effectively examine the complete contents of each file?

Now, let us see what they discovered with the file *cover page.jpgc* file. Within the file analysis mode, selecting the filename “*cover page.jpgc*” displayed the contents of the file as illustrated in Fig. 11.52. Note that Autopsy could not recognize this file as a JPEG file, and the contents returned did not have the JPEG signature “JFIF.” JPEG images should have the “JFIF” signature in the sixth byte of the file.

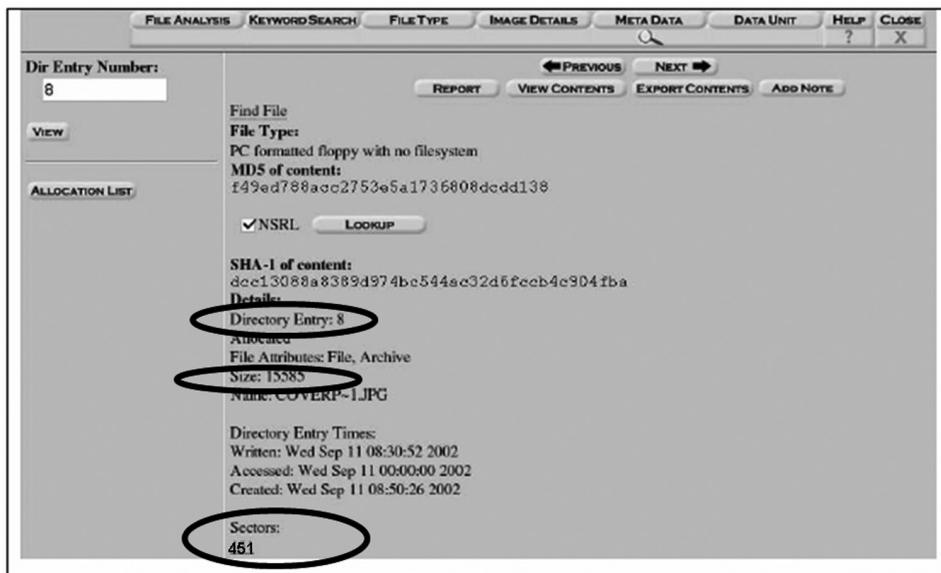
The metadata for this file was viewed by selecting the “8” link in the metadata column where the filename is listed. As illustrated in Fig. 11.53 the file size is reported as 15,585 bytes, yet it has only been allocated to sector 451. A sector is only 512 bytes on a floppy disk, so there is insufficient space to hold this file in a single sector.

Investigators wanted to determine if the metadata had been corrupted for this image file. They also wanted to check if the data for this file exists elsewhere. So, they performed a keyword search for the JPEG signature “JFIF” “Keyword Search” mode of Autopsy as you can see in Fig. 11.54.

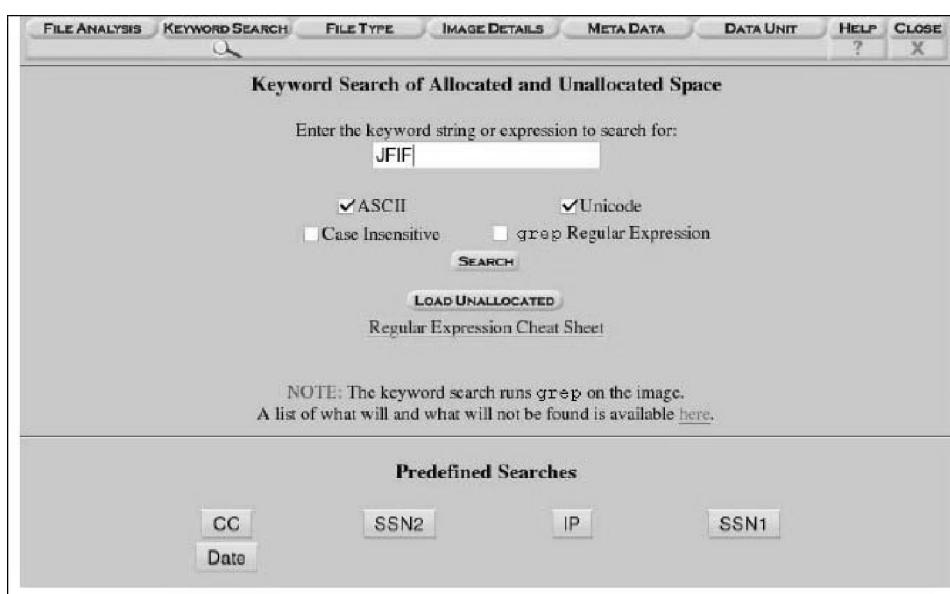
Their search for ‘‘JFIF’’ successfully found an ASCII match at Sector 73 (Fig. 11.55). It is possible to display the HEX or ASCII contents of sector 73 within the image by selecting the links in the search results. However this will only display a single sector, and the image may be bigger than a single sector. The metadata for this file states the size of the image file is 15,585 bytes which would indicate 31 sectors are required (as stated previously, sector sizes on a floppy disk are usually 512 bytes).



**Figure 11.52** | Autopsy: File analysis – “cover page.ipqc” – ASCII display.



**Figure 11.53** | Autopsy: Metadata Analysis – ASCII display “cover page.jpgc”.



**Figure 11.54** | Autopsy: keyword search – JFIF.

The “Data Unit” mode of Autopsy (Fig. 11.56) allows an investigator to view the allocation list of an image; this can be viewed by selecting the “Allocation List” button.

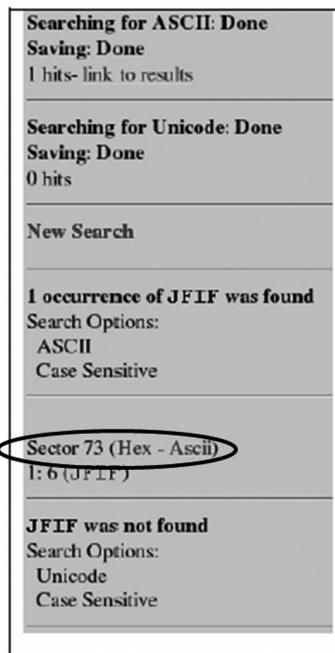
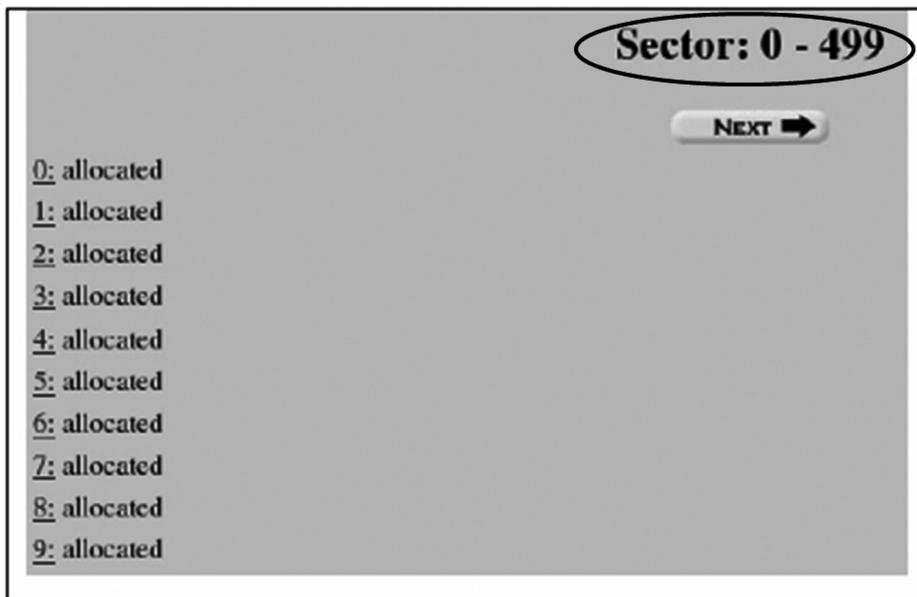


Figure 11.55 | Autopsy: Result of keyword search – JFIF.



Figure 11.56 | Autopsy: Data unit analysis.

The results from the allocation list are displayed in a single list format 500 sectors at a time. A small sample is illustrated in Fig. 11.57. This output is not easy to view, therefore, the information has been summarized in Table 11.7.



**Figure 11.57** | Autopsy: Data unit analysis – allocation list.

**Table 11.7** | Sector allocations (digital forensics using Autopsy Tool Kit)

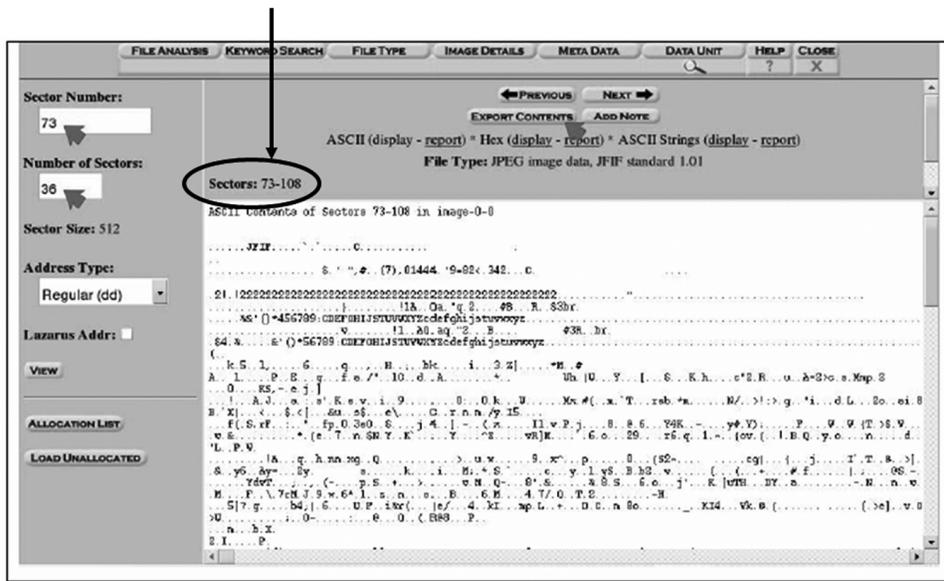
<i>Sector Range</i>	<i>Allocation Status</i>
Sectors 0–32	Allocated
Sectors 33–72	Not allocated
Sectors 73–108	Allocated
Sector 109 onward	Not allocated

We can see from Table 11.7 that 36 sectors are allocated (from Sector 73–108). Of these 36 sectors, only 31 may be associated with the “cover page.jpgc” image file (refer to Fig. 11.51). The “dd” tool can be used to extract all 36 sectors and inspect the results. It is possible to extract the sector content using the “Data Unit” mode of Autopsy to retrieve the appropriate number of sectors, and then selecting the “Export Contents” button as illustrated in Fig. 11.58.

The “dd” command, used to extract sectors 73–108, is shown below; recall that there was a mention of this command in Table 8.4 of Chapter 8.

```
dd skip=73 bs=512 count=36 if=/forensics/ev.locker/CaseIllustration01/
floppyhost/images/image.dd
of=/forensics/ev.locker/CaseIllustration01/floppyhost/output/
coverpage.jpg
```

The data extracted with the “dd” tool normally can be viewed within an image viewer because it may mostly contain data for a JPEG image. In this case, unfortunately, because more data was copied than the



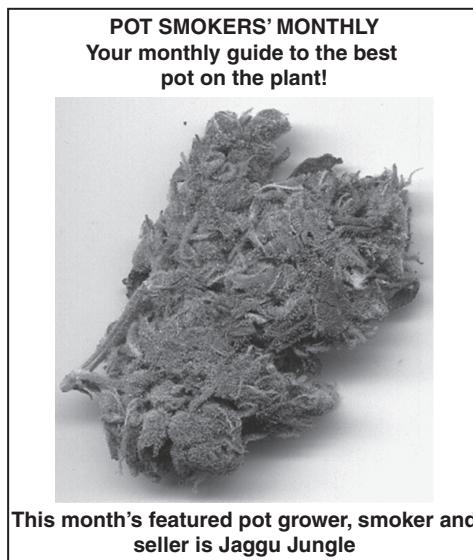
**Figure 11.58** | Autopsy: Data unit analysis – export contents option.

file size stated, it was necessary to inspect the contents of the extracted data with a hex editor to view the extra sectors that were extracted. When the forensics investigators used the “hex dumps” tool and they also manually paged through the file from the end to the start, they found references to a “Scheduled Visits.xls” file, with a “PK” signature at offset 0x3e00. This could possibly mean that this file is contained within a compressed archive (possibly called “Scheduled Visits.exe”). The text “pw=goodtimes” was also visible in the output at offset 0x3d20. JPEG images use an end-of-file signature of “ff d9” and this signature was seen at offset 0x3cdf. This signature, and the fact that when the metadata for the “Scheduled Visits.exe” file is cross-referenced (the metadata for “Schedule Visits.exe” states it had been allocated sectors 104 and 105 – refer to Table 11.5) indicates that only 31 sectors should be extracted for the “cover page.jpgc” image as was stated earlier. In order to get an accurate representation of the JPEG image the correct number of sectors is extracted from the original floppy disk image with the command listed below.

```
dd skip=73 bs=512 count=31 if=/forensics/ev.locker/CaseIllustration01/
floppyhost/images/image.dd
of=/forensics/ev.locker/ CaseIllustration01/floppyhost/output/cover-
page.jpg
```

The string “pw=goodtimes” was still contained within the slack space of the extracted data when the extracted data is viewed with a hex editor. The recovered JPG image extracted with the command (mentioned above) is illustrated in Fig. 11.59.

Now let us look at the file *JagguJungle.doc*. When the investigators selected the filename “Jaggu Jungle.doc” from the file browser within the “File Analysis” mode of Autopsy, contents of the file got displayed – they are illustrated in Fig. 11.60. Due to its extension, Autopsy recognizes this file as a Microsoft Office Document. In Chapter 7, Box 7.10 explained what is meant by metadata. In this illustration, the investigators could view the metadata for this file by selecting the “5” link in the metadata column where the filename is listed. The metadata will detail the sectors where the file was allocated within the floppy disk image.



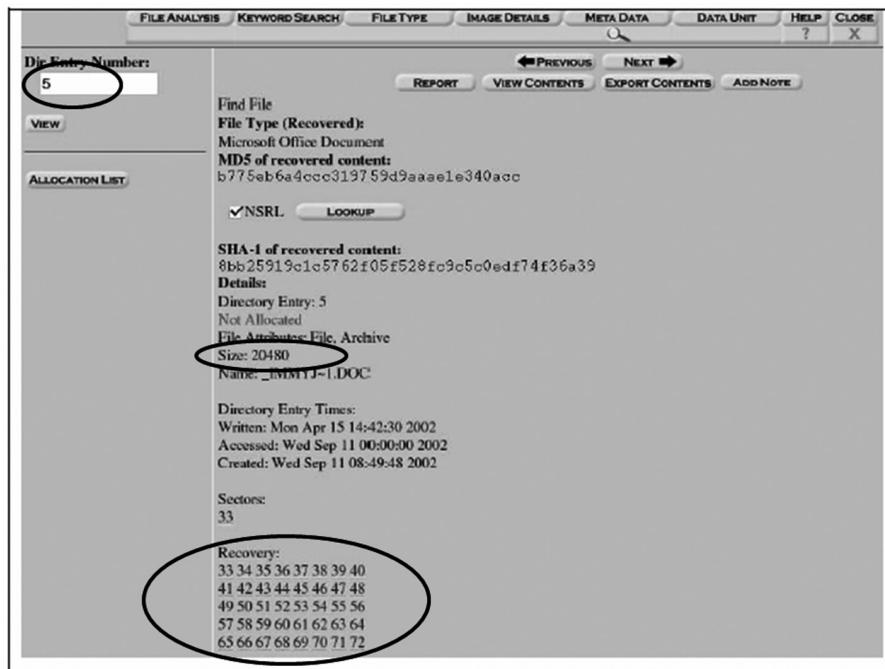
**Figure 11.59** | Image contained in “coverpage.jpg” file.

The screenshot shows the Autopsy interface with the following details:

- Current Directory:** /
- File Analysis Tab:** Active tab.
- File Type:** Microsoft Office Document
- File Name:** Jaggu Jungle.doc
- File Size:** 20480 bytes
- File Creation Date:** 2002.04.15
- File Last Accessed:** 2002.09.11
- File Last Written:** 2002.09.11
- File MD5:** 8
- File SHA1:** 5
- File MD5 (Coverpage.JPG):** 11
- File Content Preview:** ASCII display showing the file's content.

**Figure 11.60** | Autopsy: File analysis – ASCII display of the file “Jaggu Jungle.doc”.

The metadata information (Fig. 11.61) indicated that initially, Sectors 33–72 were allocated to this deleted file. The list in Table 11.7 shows that these sectors were unallocated. Therefore, the investigators thought it may be beneficial to extract these 40 sectors in hope of recovering a copy of the deleted document. The size of the file was checked only to ensure that the appropriate numbers of sectors are being



**Figure 11.61 |** Autopsy: Metadata analysis of the file “Jaggu Jungle.doc”.

extracted. For those who are not aware of floppy disk structure, Fig. 11.62 depicts the same. The metadata indicated that the file size was 20,480 bytes. Considering that there are 512 bytes in a sector, this would require exactly 40 sectors. The “dd” command used to extract the sectors is shown below:

```
dd skip=33 bs=512 count=40 if=/forensics/ev.locker/CaseIllustration01/
floppyhost/images/image
of=/forensics/ev.locker/CaseIllustration01/floppyhost/output/
jaggujungle.doc
```

The extracted file appeared to have been created on 16 April 2002 at 08:30:00, modified on 16 April 2002 at 09:42:00 and could open successfully in a word processor. The text contained within the document is listed below.

Jaggu Jungle  
Tinku Wadi, Naupada  
Thane

Jaggu  
Man, your pot is surely the best - it made the cover of Going High Magazine! Thanks for sending me the Cover Page.

How do work towards cultivating the marijuana plant? What quality of seeds do you use man? I know your growing it and not some guy in Vasai area.

These school kids, they tell me marijuana isn't addictive - Ha! Ha! They just can't stop buying from me! Man, I'm glad you gave me the trick of targeting the high school kids. You must have some experience. It's like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I'm an entrepreneur. Am I only one you sell to or do you patronize others like me too? Common man - be only with me. Maybe I can become distributor of the year!

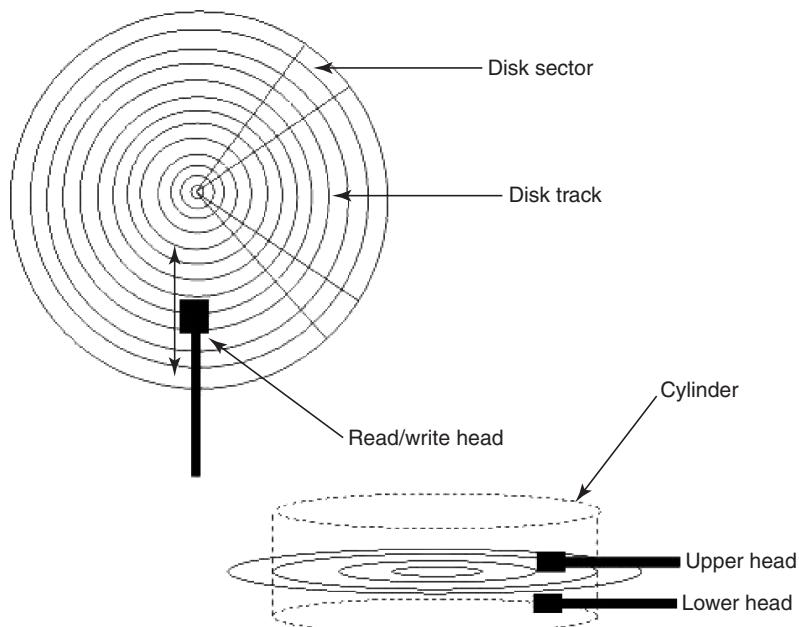
I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Lets talk soon.

Thanks,

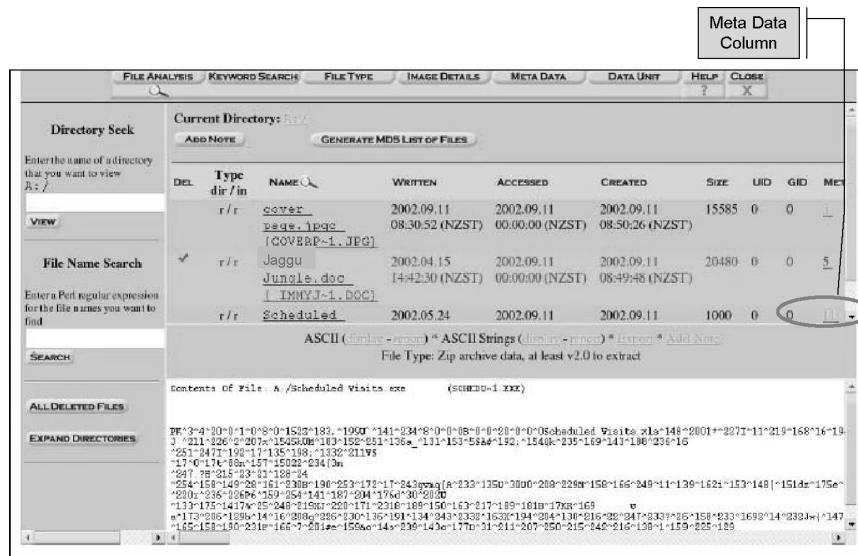
Babu Dangat

Now let us see what was revealed by Scheduled Visits.exe. When the case investigators selected the file-name "Scheduled Visits.exe" from the file browser within the "File Analysis" mode of Autopsy, the contents of the file were displayed – this is illustrated in Fig. 11.63. Autopsy has recognized this file as Zip Archive. The metadata for this file was viewed by selecting the "11" link in the metadata column where the filename is listed (see Fig. 11.64). The metadata had the details of the sectors where the file was allocated within the floppy disk image.

The metadata information (see Fig. 11.64) indicated that this deleted file was initially allocated Sectors 104 and 105. The size of the file was 1,000 bytes, and one sector has 512 bytes – this meant that it would



**Figure 11.62** | Disk structure.



**Figure 11.63** | Autopsy: File analysis – ASCII display of “Scheduled Visits.exe”.



**Figure 11.64** | Autopsy: File analysis – metadata analysis of “Scheduled Visits.exe”.

require only two sectors and this matches the sector allocation list. The two sectors are extracted using the “dd” command listed below:

```
dd skip=104 bs=512 count=2 if=/forensics/ev.locker/CaseIllustration01/
floppyhost/images/image
of=/forensics/ev.locker/CaseIllustration01/floppyhost/output/
scheduledvisits.exe
```

When the investigators attempted to extract this file with the “unzip” tool, it produced the error “End-of-central directory signature not found” – this indicated that the file is incomplete. As listed in Fig. 11.7, sectors were allocated from sectors 73 to 108. Also, as was discovered when data was initially extracted for the JPG image from sectors 73 to 108, the text “Scheduled Visits.xls” was found within the last sector. With these two pieces of supporting evidence, it was decided by the investigators to extract the data from Sectors 104 to 108 and then they try to run the unzip tool. The “dd” command used to extract Sectors 104 to 108 is shown below:

```
dd skip=104 bs=512 count=5 if=/forensics/ev.locker/CaseIllustration01/floppyhost/images/image
of=/forensics/ev.locker/CaseIllustration01/floppyhost/output/scheduledvisits.exe
```

When the investigators attempted extracting this larger file with the “unzip” tool, the Autopsy tool prompted for a password to be entered. At this stage an investigator could use a password cracker; however, the slack space from the JPEG file contained the string “pw=goodtimes.” Therefore, they decided to try that first. Entering the password “goodtimes” allowed the “unzip” tool to extract the “Scheduled Visits.xls” file. Running the “file” command on “Scheduled Visits.xls” indicated that the file was a “Microsoft Office Document” – this would have been an investigator’s first guess because of the file extension. The “Scheduled Visits.xls” file contains a list of dates and school names as illustrated in Table 11.8. All the names in the list have been masked to maintain the confidentiality. If any name happens to match with an existing school, then it is a pure co-incidence.

**Table 11.8** | File contents – “Scheduled Visits.xls”

<i>Month (2002)</i>	<i>Day</i>	<i>High Schools</i>
April	Monday	St. Joseph's High School
	Tuesday	Kale High School
	Wednesday	Lulanagar High School
	Thursday	Barodia High School
	Friday	Rishi High School
	Monday	Haldiram High School
	Tuesday	St. Joseph's High School
	Wednesday	Kale High School
	Thursday	Lulanagar High School
	Friday	Barodia High School
	Monday	Rishi High School
	Tuesday	Haldiram High School
	Wednesday	St. Joseph's High School
	Thursday	Kale High School
	Friday	Lulanagar High School
	Monday	Barodia High School
	Tuesday	Rishi High School
	Wednesday	Haldiram High School
	Thursday	St. Joseph's High School
	Friday	Kale High School
	Monday	Lulanagar High School
	Tuesday	Barodia High School

(Continued)

**Table 11.8 | (Continued)**

<i>Month (2002)</i>	<i>Day</i>	<i>High Schools</i>
May	Wednesday	Rishi High School
	Thursday	Haldiram High School
	Friday	St.Joseph's High School
	Monday	Kale High School
	Tuesday	Lulanagar High School
	Wednesday	Barodia High School
	Thursday	Rishi High School
	Friday	Haldiram High School
	Monday	St.Joseph's School
	Tuesday	Kale High School
	Wednesday	Lulanagar High School
	Thursday	Barodia High School
	Friday	Rishi High School
	Monday	Haldiram High School
	Tuesday	St.Joseph's High School
	Wednesday	Kale High School
	Thursday	Lulanagar High School
	Friday	Barodia High School
	Monday	Rishi High School
	Tuesday	Haldiram High School
	Wednesday	St.Joseph's School
	Thursday	Kale High School
	Friday	Lulanagar High School
June	Monday	Barodia High School
	Tuesday	Rishi High School
	Wednesday	Haldiram High School
	Thursday	St.Joseph's High School
	Friday	Kale High School
	Monday	Lulanagar High School
	Tuesday	Birard High School
	Wednesday	Rishi High School
	Thursday	Haldiram High School
	Friday	St.Joseph High School
	Monday	Kale High School
	Tuesday	Lulanagar h High School
	Wednesday	Birard High School
	Thursday	Rishi High School
	Friday	Haldiram High School
	Monday	St.Joseph High School
	Tuesday	Kale High School
	Wednesday	Lulanagar High School
	Thursday	Birard High School
	Friday	Rishi High School

At the beginning of this illustration, we had placed some questions that were objective of the forensics investigation. Having completed the analysis of the image now the questions could be answered using the information retrieved during the computer forensics analysis. This is shown in Table 11.9.

To conclude on the digital forensics illustration presented, here are the key summary points:

1. Although this illustrative example may be considered extremely small (going by its scope and difficulty), it demonstrates how to utilize some aspects of the Autopsy Forensics Browser to simplify some of the tasks required when performing a file system analysis.
2. This illustration demonstrated Autopsy's ability to process metadata information, perform keyword searches on image files, handle deleted files and provide a basic file manager like interface to all files within an image. Many of the steps required were performed within the browser and without the need to directly interact with the command line tools from The Sleuth Kit.

**Table 11.9** | Answers to the case questions

Case Questions	Answers Found through Computer Forensics
<b>Question 1</b> Who was the supplier of marijuana and what was the address listed for the supplier?	Jaggu Jungle Tinku Wadi, Naupada Thane
<b>Question 2</b> What crucial data is available within the “coverage.jpg” file and why is this data crucial?	The string “pw=goodtimes” was found in the slack space at the end of the files allocation units. This data was crucial as it turned out to be the password for the “Scheduled Visits.exe” which was a password-protected file.
<b>Question 3</b> What (if any) other high schools besides St. Joseph’s High School did the criminal frequent?	The password protected file “Scheduled Visits.exe” contained the Excel spreadsheet file “Scheduled Visits.xls” which listed dates for some more schools other than St. Joseph’s school. <i>Note:</i> The list is given in Table 11.8.
<b>Question 4</b> For each file, what processes were taken by the suspect to mask them from others?	1. “cover page.jpgc” – This file was incorrectly pointing to Sector 451 on the disk for its data units; it should have been pointing to Sector 73. Any attempt to open the file would produce the data units at Sector 451 which had all bytes set to “f6.” 2. The “Jaggu Jungle.doc” file had been deleted. 3. The length of file “Scheduled Visits.exe” stated it was only 1,000 bytes; however, it was actually 2,560 bytes in length. The extension of the file did not match the file type. The file was also password-protected.
<b>Question 5</b> What processes were used to successfully examine the entire contents of each file?	The <i>Autopsy Forensics Browser</i> was able to successfully retrieve information about the files. Information found using the Autopsy Forensics Browser was also used with the “dd” command line tool to extract various sectors from the disk image. All steps have been thoroughly described in the Analysis section presented earlier.

3. In the analysis stages there were some steps that were required to be done outside of the Autopsy Forensics Browser, but aside from file viewers, the only external tools that were utilized were the “dd,” and “hex dumps” tools. The use of the “dd” tool was not required, it was simply utilized for this investigation to demonstrate an alternate method for extracting data from a disk image.
4. Point to note is that each investigation is unique and will require different aspects of forensic tools in order to successfully complete an analysis. This illustration does not represent an exhaustive demonstration of the tools found in The Sleuth Kit and the Autopsy Forensics Browser by any means; it merely provides a valuable introduction to some of the functionality provided by these tools.

### 11.6.3 Digital Forensics Reporting Illustration 1: Vehicle Stealing Racket Revealed through Computer Forensics Investigation

Good citizens are alert and behave in a responsible manner when they notice anything they believe could have to do with cybercrime/cybersecurity matter. This illustration is about one such alert citizen. One evening a concerned citizen contacted the police department regarding possible stolen property. He told police that while he was browsing the Internet, in hope to find a car for a sensible price, he found an advertisement that met his requirements. This advertisement listed a Honda City car for a low price, so he contacted the seller. Upon meeting the seller he became suspicious that it was a stolen car being offered for sale.

After getting this information, police alerted the Auto Theft Unit. The Auto Theft Unit conducted a smart operation to procure the car. Surreptitiously, police officers met with the suspect, who, after receiving the sum (toward purchase prices of the car), provided required details to the police (in disguise) about the vehicle (car registration number, insurance, etc.). The culprit was taken under arrest and the car that he was driving was searched along with his arrest. During the search, a notebook computer was taken into custody. Although the documents provided by the suspect, that is, the culprit, looked genuine, upon examination the documents turned out to be fake. The auto theft examiner got in touch with the computer forensics laboratory to seek help in examining the seized computer. The investigator obtained a search warrant to scrutinize the computer and search for materials used in making fake documents and other proof related to the auto theft charges. The notebook computer was submitted to the computer forensics laboratory for analysis. Table 11.10 shows the initial report prepared. EnCase tool was mentioned in Chapter 7. In this real-life scenario, it was used.

**Table 11.10 |** The primary report (1)

<b>Primary Report</b>	
Type of Computer:	Gateway Solo® 9100 notebook computer.
Operating System:	Microsoft Windows 98.
Offenses:	Theft of Auto, Forgery Fraud, Creating False Documents (document forgery) and Possession of Counterfeit Vehicle Titles.
Agent In Charge of Case:	Auto Theft Unit Investigator.
Place of Forensics Examination:	Computer Forensics Laboratory.
Forensics Tools used:	Guidance Software™ EnCase, DIGIT, Jasc Software® Quick View Plus®, and AccessData Password Recovery Tool Kit.

The case was processed in the manner described here. During the “Assessment” phase:

1. Documentation provided by the investigator was reviewed.
  - a. A special search warrant was obtained for the assessment of the computer in a laboratory location – legal authority was instituted for this.
  - b. Chain of custody was properly documented using appropriate forms defined by the concerned departments.
  - c. The appeal for service and a detailed summary explained the investigation, provided keyword lists, and provided information about the person suspected, the stolen car, the forged documents and the Internet ad. The investigator also provided photostat copies of the forged documents.
2. The computer forensics examiner set up discussion with the case agent to understand the possibilities for additional investigation areas and also to understand potential evidence being sought in the investigation.
3. Evidence input was completed.
  - a. The evidence was noted and photographs were made.
  - b. A file was created and the case details were entered into the laboratory database.
  - c. The computer was safely put in the laboratory’s property room.
4. The case was entrusted to a computer forensics investigator.

During the “Imaging” phase, the following steps were performed:

1. The notebook computer was examined and photographed.
  - a. The hardware was examined and documented.
  - b. A controlled boot disk was placed in the computer’s floppy drive. The computer was powered on and the BIOS setup program was entered. The BIOS information was documented and the system time was compared to a trusted time source and documented. The boot sequence was checked and documented; the system was already set to boot from the floppy drive first.
  - c. The notebook computer was powered off without making any changes to the BIOS.
2. EnCase® was used to create an evidence file containing the image of the notebook computer’s hard drive.
  - a. The notebook computer was linked to a laboratory computer through a null-modem wire, which connected to the computers’ parallel ports.
  - b. The notebook computer was booted to the DOS prompt with a controlled boot disk and EnCase® was started in server mode.
  - c. The laboratory computer, ready with a magneto-optical drive for file storage space, was booted to the DOS prompt with a restricted boot disk. EnCase was started in server mode and evidence files for the notebook computer were obtained and written to magneto-optical disks.
  - d. When the imaging process was completed, the computers were powered off.
    - i. The notebook computer was sent back to the laboratory belongings room.
    - ii. The magneto-optical disks that the EnCase evidence files held on them were write-protected and logged into evidence.

Next, a number of other steps were carried out during the “Analysis” phase:

1. A computer in the laboratory was made ready for investigation by installing – Windows 98, EnCase for Windows and other forensics software tools on it.
2. The EnCase evidence files from the notebook computer were copied to the laboratory computer’s hard drive.

3. A new EnCase case file was opened and the notebook computer's evidence files were examined using EnCase .
  - a. Deleted files were recovered by EnCase.
  - b. File data, including file names, dates and times, physical and logical size, and complete path, were recorded.
  - c. Keyword text searches were carried out using the information furnished by the investigator. When the results were returned, all hits were examined.
  - d. Graphics files were opened and viewed.
  - e. HTML files were opened and viewed.
  - f. Data files were opened for examining the contents; two password-protected and encrypted files were sited.
  - g. Unallocated and slack space was searched.
  - h. Files of evidentiary value or investigative interest were copied/unerased from the EnCase evidence file and copied to a compact disk.
4. Unallocated clusters were copied/un-erased from the EnCase evidence file to a clean hard drive, wiped to DoD 5200.28-STD. DIGit was then used to carve images from unallocated space. The carved images were extracted from DIGit, opened and viewed. A total of 8,476 images were extracted. Recall "File Carving" explained in Box 7.10 in Chapter 7.
5. The password-protected files were copied/unerased to a 1.44 MB floppy disk. AccessData Password Recovery Tool Kit was run on the files and passwords were recovered for both files. The files were opened using the passwords and viewed.

A number of findings emerged – the analysis of the notebook computer resulted in the recovery of 176 files of evidentiary value or investigative interest. The recovered files included:

1. 59 document files included documents having the suspect's name and personal information; text included in the forged documents; scanned payroll, corporate and validated cheques; text about and describing stolen items; and text relating to the recovered car.
2. 38 graphics files consisting of high-resolution image files showing payroll, corporate, and certified cheques; notes; vehicle titles; registration cards and templates of driver's license from many states; insurance cards from different companies; and fake (though certified) checks payable to a computer company in the range of ₹ 125,000 to ₹ 240,000 for the obtaining notebook computers, printers and other accessories. A good number of graphics were scanned.
3. 63 HTML files containing Hotmail and Yahoo E-Mail and confidential advertisements for the recovered car, other vehicles and numerous types of notebook computers; E-Mail text, containing E-Mails exchanged between the culprit and the involved citizen regarding the sale of the recovered vehicle; and E-Mail communication between the culprit and a computer agency regarding the purchase of laptops.
4. 14 graphics files recovered from unallocated space showing checks at different stages of finishing points and scanned imagery of currency notes (recall "File Carving" explained in Box 7.10 in Chapter 7).
5. Two password-protected and encrypted files:
  - a. WordPerfect® document having a list of personal information about quite a few individuals – names, addresses, dates of birth, credit card and bank account numbers and termination dates, current account information, and other information. Password [nomoresecrets].
  - b. Microsoft® Word document having vehicle title details of the recovered car. Password [HELLO].

The documentation about this investigation consisted of the following:

1. **Forensics Report:** All actions, processes and findings were described in a detailed forensics report, which is maintained in the laboratory case file.
2. **Police Report:** The case agent was provided with a police report describing the evidence examined, techniques used and the findings.
3. **Work Product:** A compact disk containing files and file data of evidentiary value or investigative interest was created. The original was stored in the laboratory case file. Copies were provided to the case agent and the prosecutor.

Computer analysis revealed some interesting information and several new avenues of investigation were opened:

1. Investigators contacted the victims listed in the password-protected WordPerfect document, thereby learning that the victims had all been robbed in the same city during the previous summer by an individual whose description was similar to that of the suspect.
2. When the computer company was contacted, it was revealed that the counterfeit cheques found on the suspect's computer had been accepted for the purchase of computers, and that the computers were shipped to him and were the subject of an ongoing investigation. Model numbers and serial numbers furnished by the computer company turned out to match with many of the Hotmail and Yahoo classified advertisements found on the culprit's computer.
3. Many of the counterfeit cheques found on the suspect's computer were already the subject of ongoing investigations.
4. Information gathered about other vehicles led to the recovery of additional stolen vehicles.
5. The particular information hunted in the search warrant regarding the sale of the stolen car and the fake documents was recovered from the suspect's computer.

This led to the arrest of the suspect who eventually pleaded guilty and was imprisoned.

#### **11.6.4 Digital Forensics Reporting Illustration 2: Child Pornography Revealed through Computer Repair**

COPPA (Children's Online Privacy Protection Act) and Child Pornography is addressed in Chapters 1 and 6. Child pornography-related offenses are explained in Chapter 1. In Chapter 7, it was mentioned that computer forensics involves lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and metadata derived from digital devices which may contain information that is notable and perhaps of evidentiary value. This illustration is to be read with that background and is about the reporting part of computer forensics. Reporting is an important phase in a computer forensics/cyberforensics investigation as explained in Section 7.7.2 of Chapter 7. The case brief that follows is an example of what is typically involved in case analysis.



The case scenarios presented are for instructional purposes and information only. Any association to an actual case and litigation is purely coincidental. Names and locations presented in the case scenarios are fictitious and are not intended to reflect actual people or places. Reference herein to any specific commercial products, processes or services by trade name, trademark, manufacturer or otherwise does not constitute or imply its endorsement, recommendation and the information and statements are not meant to constitute any direct or indirect attempt to advertise those products, processes or services.

Here is how the scenario of this illustration goes. The setting is of old times when Windows XP operating system was not around.

Amrish Deshpande was a young entrepreneur who owned a building construction company. Of late, Amrish had noted that his laptop (loaded with Windows 98 systems) had developed a certain problem on the monitor screen. So, he handed his laptop computer to his company staff member for taking it to a computer repair shop to fix the malfunctioning monitor of the laptop. After repairing the laptop, shop's technician powered on the laptop to reconfirm if the monitor had been fixed. A standard procedure of shop was to go to the recent menu on the Start Bar of Windows 98 systems and select files for viewing. While doing that, the technician noticed on the laptop screen what appeared to be an image of a young child depicted in a sexually explicit manner.

Being well-aware of the implications of any pornographic material on a laptop, the technician telephoned the office of the legal authority in the town. The concerned officer from legal authority office observed the image and confirmed it to be a violation of a prevailing law. The laptop was seized because it contained illicit material. The capture operation was conducted in a manner consistent with recommendations found in the manual "Computer Crime Scene Investigation: A Guide for First Responders." The laptop was entered into evidence according to legal policy, and a search warrant was obtained for the examination of the computer. The computer was submitted for examination.

Objective was to determine whether Amrish (here in after referred to as the "SUBJECT") possessed child pornography. The challenge in this case came from the fact that Amrish alone was not the user of the laptop. The laptop was used by the number of people in his office – it was a shared laptop. Note the first primary stage report shown in Table 11.11.

During the "Assessment" phase, Case Investigator's request for service was reviewed. The search warrant provided legal authority. The forensics investigator wanted to dig into all the information regarding child pornography, access dates and ownership of the computer. It was ascertained that the required equipment was present in the forensics laboratory.

For the "Acquisition" phase, the hardware configuration was documented and a duplicate of the hard drive was created in a manner that protected and preserved the evidence. The CMOS details, including the time and date, was documented.

As for the "Examination" phase, the directory and file structures, including file dates and times, were recorded. A file header search was conducted to locate all graphic images. The image files were examined and those files holding the images of what appeared to be children depicted in a sexually explicit manner were preserved. Shortcut files recovered pointed to files on floppy disks containing sexually explicit file names

**Table 11.11 |** The primary report (2)

<b>Primary Report</b>	
Computer type:	Generic laptop, serial # 123456789.
Operating system:	Microsoft®Windows® 98.
Offense:	Possession of child pornography (prima facie suspected).
Case agent:	Investigating Officer Mankame Ulhas.
Evidence number:	052356
Chain of custody:	See attached form.
Where examination took place:	Criminal investigations unit.
Tools used in Forensics Operation:	Disk acquisition utility, universal graphic viewer, command line.

relating to children. The last accessed time and date of the files indicated that the files were last accessed 10 days before the laptop was delivered to the computer repair shop. For “Documentation and Reporting,” the forensics examiner was provided with a report describing the result of the preliminary examination. The investigator decided to conduct interviews.

During the next step, the employee who delivered the laptop computer to the computer repair shop was interviewed. During the conversation, the employee indicated that he had never operated the computer. Further, the employee stated that the SUBJECT had shown him images of a sexual nature involving children on the laptop. As per the employee’s narration, the SUBJECT had once mentioned to the employee that he keeps his pictures on floppy disks at home; he just forgot this one image on the laptop.

The Advocate involved in this case (on behalf of police) was briefed in hope of obtaining a search warrant for SUBJECT’s home based on the examination of the digital evidence and the interview of the employee. A warrant was drafted, presented to a judicial officer, and signed. During the consequent search, floppy disks were found at SUBJECT’s house. Forensics inspection of the floppies showed additional evidences of child pornography – evidences included images in which SUBJECT was an accomplice. This resulted in the arrest of SUBJECT. The case brief report is in Table 11.12.

**Table 11.12 | Case brief report**

<b>Case Brief Report</b>	
<b>REPORT OF MEDIA ANALYSIS</b>	
<b>MEMORANDUM FOR:</b>	Police Officer at the Police Station in Subject’s geographical area Investigator Mankame, Pune, Sahaj-Vihar Road.
<b>SUBJECT:</b>	Forensic Media Analysis Report SUBJECT: Amrish Deshpande
Case Number:	012345 052356
Status:	Closed.
<b>Summary of Findings:</b>	
327 files containing images of what looked like children depicted in a sexually explicit mode were recovered. 34 shortcut files that pointed to files on floppy disks with sexually explicit file names involving children were recovered.	
<b>Items Analyzed:</b>	
<b>TAG NUMBER</b>	<b>ITEM DESCRIPTION</b>
034489	One Generic laptop, Serial # CUFN 457-1
<b>Details of Findings:</b>	
Findings in this paragraph related to the Generic Hard Drive, Model XTPS-30, Serial # 3456ABCD, recovered from Tag Number 012345, One Generic laptop, Serial # 123456789.	
1) The examined hard drive was found to contain a Microsoft®Windows® 98 operating system. 2) The directory and file listing for the media was saved to the Microsoft® Access Database TAG 034489 MDB. 3) The directory C:\ AMRISH DESHPANDE\PERSONAL\FAV PICS\, was found to contain 327 files containing images of what looked like children depicted in a sexually explicit manner. The file directory for 327 files disclosed that the files’ creation date and times are 5 July 2001 between 11:33 p.m. and 11:45 p.m., and the last access date for 326 files listed is 27 December 2001. Additionally, the file directory information for one file showed that the last access date was 6 January 2002.	

(Continued)

**Table 11.12 | (Continued)**

- 4) The directory C:\AMRISH DESHPANDE\PERSONAL\FAV PICS TO DISK\ contained 34 shortcut files that pointed to files on floppy disks with sexually explicit file names involving children. The file directory information about the 34 shortcut files gave away the files' creation date and times as 5 July 2001 between 11:23 p.m. and 11:57 p.m., and the previous access date for the 34 shortcut files was listed as 5 July 2001.
- 5) The directory C:\ AMRISH DESHPANDE\LEGAL\ included five Microsoft® Word documents related to a variety of contract relationships Amrish Deshpande had with other entities.
- 6) The directory C:\ AMRISH DESHPANDE\AMRISH DESHPANDE BUILDING CONSTRUCTIONS\ contained files in relation to operation of Amrishi Deshpande Constructions.
- 7) There were no further user-created files present on the media.

**Shortcut File:** A file created that has associations to another file.

**Items provided:** besides this hard copy report, one compact disk (CD) was submitted with an electronic copy of this report. The report on CD had hyperlinks to the files and directories mentioned above.

KALYANI D. INAMDAR  
Computer Forensic Examiner

Released by \_\_\_\_\_  
Chief Forensics Officer

## 11.7 Online Scams

In this section, we present revealing information about world's most infamous scams. Many of them are related – for example, Nigerian scams (also known as "419 scams" involve one or other form of advance fee to lure the victim for the promise of a long-term gain). The online scams described in this section are listed in Table 11.13.

In a way, "SPAM" and "SCAM" are related because Spam, is often the vehicle used to convey scams and other attempted fraudulent attacks to individuals. A "HOAX" also involves deception; however, it is done without the intention of gain or damage or for depriving the victim; sometimes the intention can be humorous. Types of cybercriminals and their motives are explained in Chapter 1 (Section 1.4). Also recall Fig. 7.12 in Chapter 7. In this section, a number of Scam examples are provided. We hear about scams that are reported occasionally in the news papers. The majority of recipients may not respond to these E-Mails; however, there are a few people who do respond to such mails. From fraudsters' point of view, that is enough to make the fraud worthwhile as many millions of messages can be sent. Invariably sums of money which look large, but are very much smaller than the promised profits, are required in advance for bribes, fees, etc. – this is the money stolen from the victim, who thinks he/she is making an investment for a huge profit.

In the sections that follow, some of the well-known scams are described. The objective is to create awareness for people so that they take due care and do not fall prey to such scams. Read about popular scams in Refs. #61–#65, #67–#69, Additional Useful Web References, Further Reading. *A "fraud" is a deliberate action conducted with the motive of personal gain or an act done to damage another individual.* The specific legal definition varies by legal jurisdiction. *Fraud is a crime and also a civil law violation.* Doing fraud with people or entities (such as organizations, institutions, etc.) for money or ill-gotten gains is a common purpose of fraud, but there have also been fraudulent "discoveries." Fraudsters cleverly exploit human characteristics such as greed and dishonesty, and victimize individuals from all walks of life. "Advance free fraud" is a classic example of this. There are many variants of this scam and they are described in the next section. Advance Fee Scam usually begins with a letter or E-Mail that is sent only to a selected recipient but is actually sent to

**Table 11.13** | Scams described in Section 11.7

<i>Scam No.</i>	<i>Title</i>
<b>1</b>	Foreign Country Visit Bait
<b>2</b>	Follow-up Scamming
<b>3</b>	Purchasing Goods and Services Scam
<b>4</b>	Cheque Cashing Scam
<b>5</b>	Romance Scam
<b>6</b>	Lottery Scam
<b>7</b>	The Hitman Scam
<b>8</b>	The Bomb Scam
<b>9</b>	Charity Scams
<b>10</b>	Fraud Recovery Scams
<b>11</b>	Pet Scams
<b>12</b>	Bona Vacantia Scam
<b>13</b>	Fake Job Offer Scam
<b>14</b>	Rent Scam
<b>15</b>	Attorney Debt Collection Scams
<b>16</b>	Malware Scams
<b>17</b>	The Advance Fee Fraud
<b>18</b>	Babysitting Scams
<b>19</b>	Nigerian 419 Scam
<b>20</b>	Craigslist Scams
<b>21</b>	Pyramid Scheme Scams and Ponzi Scheme Scams

many persons. In the E-Mail an offer is made with a claim of a large payoff for the victim. Often, the subject line of the E-Mail's have some catchy text like "From the desk of Mr. XYZ," "Your assistance is needed," and so on. The details vary, but the usual story is that a person, often a government or bank employee, knows of a large amount of unclaimed money or gold which he cannot access directly, usually because he has no right to it.

The Spam E-Mails used to perpetrate scams are often transmitted from Internet cafes having satellite connection. Addresses and E-Mail content of recipient are duplicated into a webmail interface on a stand-alone storage medium, such as a memory card. During the course of many schemes, scammers look for victims to supply bank account information. Typically this is a "test" devised by the scammer to gauge how gullible the victim could be. Regarding due diligence with cybercafes, refer to Appendix J.

### 11.7.1 Scam No. 1 – Foreign Country Visit Bait

This is a common trick used by fraudsters. Fraudsters take advantage of the fact that generally people are eager to go overseas with the hope of earning more money. Fraudsters devising a plot under such scenario would charm the victim through an "invitation to visit the country." The naive victims are invited to a country to

meet real or fake government officials. Some victims who do travel are instead held for ransom. There are a few rumored cases, where they are illegally brought into the country without a visa and threatened into giving additional money as the penalties for being in a foreign country without a visa may be severe. At times victims are taken for ransom or they are killed – as it happened in the case of the 29-year-old Greek man called George Makronalli who was lured to South Africa and was killed.

### 11.7.2 Scam No. 2 – Follow-up Scamming

This trick is used when scammers know that their victim who has just been scammed, is more likely to fall for scamming attempts rather than a randomly selected target. Often the scammer contacts the victim after a fraud – the scammer is smart enough to make a representation as a law enforcement officer. The victim is given to understand that a group of criminals has been arrested and that they (i.e., fraudsters who are pretending to be the law enforcement folks) have recovered victim's lost money. Further, fraudster/scammer tells the victim that in order to get the money back, the victim must pay a fee for processing or insurance purposes. Even when the victim realizes the scam, this follow-up scam can be successful because the scammer represents himself/herself as a totally different party and yet knows details about the transactions. For the victim, realization that he/she has lost a large sum of money and the prospect of getting it back often leads to the victim ending up paying even more money to the same scammer.

There are many variations on the most common scam stories, and also many variations on the way the scam works. What follows in the section below are some of the most notable deviations from the standard Nigerian Letter scam, but still retain the core elements; the victim is deceived by some disproportionately large gain into sending an advance payment, which once made is irrecoverable.

### 11.7.3 Scam No. 3 – Purchasing Goods and Services Scam

Advertising automobiles on websites has become quite common. For that matter, there is a big boom in “Online Marketing” activities even if, at times, it may be at the cost of your personal information being stolen! In this mode of scam, the fraudsters list a non-existent high value car with a low price as bait to attract buyers eager to buy quickly; specially the young and rich targets. The scammer posts a message to the tune “I am not in the country, but if you pay me first, a friend will drive the car to you.” The required payment may be the full price, or a deposit, but it would not be an insignificant fee. The picture of the car is never posted on the website because the car just does not exist. In this type of scam, the scammers use E-Mail only because they are smart enough to know that the sound of their voice and their attitude will give them away as being high risk.

Another scheme under this type of scam involves advertising fake academic conferences and enticing academics to apply to present papers. As a common practice, the conference would typically subsidize the accommodation but would not reimburse the cost of air journey undertaken by the academicians to be at the conference venue for presenting papers. One method using which the scammer baits the hopeful attendee is that they offer free air travel to the victim, if they agree to pre-pay for hotel accommodation. The scammer can put forth a number of arguments to support why the accommodation must be pre-paid – primarily that they do not trust the victim will attend the conference unless he/she pays upfront. In this scam, fraudsters may use any goods or services – the idea is that they bait the victim with a good deal, and the victim must pay upfront and electronically.

### 11.7.4 Scam No. 4 – Cheque Cashing Scam

Given the workforce mobility scenario, worsening traffic conditions and soaring property prices, working from home is becoming a common pattern now. Some scam schemes are designed to exploit the workforce mobility scenario. Such schemes are based solely on conning the victim into cashing a counterfeit cheque. The scammer gets in touch with the victims and gets them interested in a “work-at-home” opportunity. Alternatively, the scammer may ask the victims to cash a cheque or a money order under the pretext that the instrument (i.e., the cheque or the money order) cannot be redeemed locally. According to a recently used cover story, the perpetrator of the scam wished the victim to work as a “mystery shopper,” evaluating the service provided by MoneyGram or Western Union locations within major retailers such as Wal-Mart. Typically, the scammer sends the victim a cheque or money order, the victim cashes it, sends the cash to the scammer via wire transfer and the scammer disappears. Later the forgery is uncovered and the bank transaction is reversed. This makes the victim liable for the balance. Defrauding plots based solely on cheque cashing typically offer only a small part of the cheque’s total amount, with the assurance that many more cheques will follow. If the victim buys into the scam and cashes all the cheques, the scammer can win big in a very short period of time. There are other scams where overpayment is involved; these usually result in smaller revenues for the scammer, but have a higher success rate as the scammer’s request seems easier to believe.

Some cheque-cashing scammers use several victims at various stages of the scam. A victim in the US or other “safe” country such as the UK or Canada (where typically the cashing victim resides) is sometimes approached with an offer to fill out cheques sent to them by the scammer and mail them to other victims who cash the cheque and wire the money to the scammer. Usually the scammer promises a cut of the money to the mailer of the cheque. However, that promise is usually not met, and the cheque mailer is often conned into paying for the production and shipping costs of the cheques. The information about the cheque is either been stolen or is fictionalized and the cheque is forged. Usually, it is far easier to track the victim mailing the cheques than tracking and prosecuting the scammer. Therefore, when the cheques turn up as fraudulent the person mailing them usually ends up not only facing charges for bank fraud and conspiracy, but also faces the liability for the full amount of the fraudulent cheques. As the mailer of the cheque is taking the call, there is now a lesser likelihood that the scammer will be caught. This makes it a popular variation of the scam; especially in countries where antifraud laws are not very tough.

Another variety of the cheque-cashing scheme involves owners of vacation rentals. The scammer shows interest in renting the unit for a much higher than normal rate, usually for an upcoming honeymoon, business trip, etc. The scammer also offers to pay all fees “up front,” as soon as the unsuspecting unit owner agrees to the windfall rental. In the long run, a very genuine looking money order/bearer cheque arrives. Around this time the scammer makes a request that a part of the rental fee be returned and provides a convincing reason for it – for example, wedding called off, death in the family, business failure, etc. Given the reason of the supposed crises, scammer requests the victim to return most of the rental fee via wire transfer. The owner of the unit is encouraged to keep “a fair amount” as a compensation for his time. The wire transfer is sent, only to find out later that the official looking cheque was indeed bogus and the full amount is charged back to the unit owner by his bank.

### 11.7.5 Scam No. 5 – Romance Scam

Fraudsters exploit human psychology to gain victim’s confidence. Romance scam is based on a “confidence trick.” A confidence trick or confidence game (also known as a bumbo, con, flim flam, gaffle, grift, hustle, scam, scheme, swindle or bamboozle) is an attempt to defraud a person or group by gaining their confidence. The victim is known as the mark; the trickster is called a confidence man, con man, confidence trickster

or con artist. Any accomplices are known as shills (see the explanation for these terms provided in Scam No. 17 – “advance fee scam”). Confident but criminally oriented people exploit human characteristics such as greed and dishonesty. Such people have victimized individuals from all walks of life. The “confidence trick” used in romance scam involves feigned romantic intentions toward victims, gaining their affection, and then using that goodwill to commit fraud. Acts of fraud may involve access to the victims’ money, bank accounts, credit cards, passports, E-Mail accounts and/or national identification numbers or by getting the victims to commit financial fraud on their behalf.

Fraudsters are tech-savvy; they modify their scamming techniques with the changing communication technologies that emerge. Money-for-romance angle is a recent variant of the Romance Scam. The con artist approaches the victim on an online dating service, an instant messenger (like Yahoo IM) or a social networking site. The scammer claims an interest in the victim and posts pictures of an attractive person (not themselves). The scammer uses this communication for his/her confidence and then asks for money. The con artist may claim to be interested in meeting the victim, but needs cash to book a plane, hotel room or other expenses. In other cases, they claim they are trapped in a foreign country and need assistance to return, to escape imprisonment by corrupt local officials, to pay for medical expenses due to an illness while abroad and so on. The scammer may also use the confidence gained by the romance angle to introduce some variant of the original Nigerian Letter scheme – for example, saying they need to get money or valuables out of the country and offer to share the wealth, making the request for help in leaving the country even more attractive to the victim. Recall the discussion in Chapter 7, Section 7.14 about social networking sites. In a newer version of the scam, the con artist claims to have “information” about the fidelity of a person’s significant other, which they will share for a fee. This information is obtained through social networking sites by using search parameters such as “in a relationship” or “Married.” Anonymous E-Mails are first sent to attempt to verify receipt, and then a new Web-based E-Mail account is sent along with directions on how to retrieve the information.

### 11.7.6 Scam No. 6 – Lottery Scam

Probably, this is most often heard term. A lottery scam is a type of advance-fee fraud. It begins with an E-Mail notification that is most unexpected. For example, you may get a mail declaring “You have won!” a large sum of money in a lottery. Next, you, the recipient of the message, would usually be told to keep the notice secret, “due to a mix-up in some of the names and numbers,” and to contact a “claims agent.” After contacting the agent, you, as the target of the scam will be asked to pay “processing fees” or “transfer charges” for the winnings to be distributed. In reality, however, you will never receive any lottery payment. Quite a few E-Mail lottery scams use the names of legitimate lottery companies; however, that does not mean those legitimate companies are in any way involved with the scams.

Fake notices of lottery wins are involved in most lottery scams. The winner is usually lured to send sensitive information to a free E-Mail account. The scammer then informs the victim a small fee is required to release the funds (insurance, registration or shipping). Once the victim sends the fee, the scammer invents another fee.

Similar to the various types of overpayment fraud mentioned above, a new variation of the lottery scam involves fake or stolen cheques being sent to the “winner” of the lottery (these cheques represent a part payment of the winnings). The winner is more likely to assume the win is legitimate, and thus more likely to send the fee (which he does not realize is an advance fee). The cheque and the funds involved are pointed out by the bank when the fraud is discovered, and debited from the victim’s account. In 2004, another form of the lottery scam appeared in the US. Fraud artists, using the scheme, call victims on telephones; a scammer tells a victim that a government has given them a grant and that they must pay an advance fee, usually around \$250, to receive the grant.

### 11.7.7 Scam No. 7 – The Hitman Scam

A “hitman” or “hitwoman” usually is a murderer who people hire to eliminate a target via contract killing. Those of you, who may have watched the Brad Pitt–Angelina Jolie movie “Mr. and Mrs. Smith,” would remember the “contract killing scenario.” In this type of scam, an E-Mail is sent to the victim’s inbox, supposedly from a hitman who has been hired by a “close friend” of the recipient to kill him or her. The scammer tells the victim that hit can be called off in exchange of a large sum of money. This is generally backed up with a warning not to contact the local police or a local investigation agency, or the “hitman” will be forced to go through with the plan. This is less of an advance-fee fraud and more of an outright extortion; however, a reward can at times come in the form of the “hitman” offering to kill the man who ordered the original hit on the victim.

### 11.7.8 Scam No. 8 – Bomb Scams

This type of scam comes closer to “cyberterrorism,” the term introduced in Chapter 1. This scam is similar to “hitman scam” wherein scammers gets in touch with a business, mall, office building or other commercial location and inform them about an impending bomb threat. The scammer threatens that he/she will detonate the bomb unless the management of the business complies with scammers’ demands. Often, scammers say they have the store under surveillance; however, analysis of many such calls by police has established that most of threat calls are made from other states or even from outside the country. Some evidence may exist pointing to the scammers who hacked into the store’s surveillance network, but this has not been confirmed in any case and has been refuted in others. The scammers usually demand that the store management staff or people working in the main office of the store (if the store is a chain) send money via wire transfer to the scammer. Other demands of these scammers have been more personal or humiliating, such as demanding that everyone in the store take off their clothes.

The underlying threat in the scam is a bomb threat – so, local law enforcement is obliged to quickly respond to the site under threat. However, because the scammer is usually nowhere near this location, the scammer is in little, if any, danger of being apprehended while the scam is playing out. In the meantime, law enforcement assumes that the threat is genuine, and therefore can do little to intervene without risking the detonation of the bomb. The fact that the threat was in reality a scam is usually not discovered until long after the situation is over and the extortionist has collected the money demanded.

### 11.7.9 Scam No. 9 – Charity Scams

This is a trick to invoke sympathetic feeling in people’s mind and use it to achieve the ulterior motive. The scammer presents himself/herself as a charitable entity looking for donations to help the impacted victims (e.g., those affected by a natural disaster, terrorist attack – for example the 9/11 World Trade Center attack, regional conflict, epidemic, etc.). Scammers very well know how to exploit people’s penchant for philanthropic work – they used 2004 Tsunami and Hurricane Katrina as the popular targets for perpetrating charity scams. There are other more timeless scam charities exploited as well, in the name of raising money for cancer, AIDS or Ebola virus research, children’s orphanages (the scammer pretends to work for the orphanage or a non-profit organization), or impersonates charities such as the Red Cross or United Way. The scammer asks for donations, often linking to online news articles to strengthen their story of a funds drive. The scammer’s victims are philanthropists who believe in helping a worthy cause and therefore they expect nothing in return. Once sent, the money is gone and the scammer often disappears. Some scammers manage to keep the scam going by asking for a series of payments. At times, the victim may land in legal trouble after

excluding their supposed donations from their income tax submission forms. Tax rules vary from country to country – for example, as per directives of the US Tax Law, charitable donations are tax-exempt only if donations are made to eligible non-profit organizations. The scammer may inform the victims that their contribution is deductible and that the donors should provide all necessary proof of donation. However, the information provided by the scammer is fictional. When audited, the victim faces stiff penalties. These scams have some of the highest success rates especially following a major disaster, but the average loss per victim is less than other fraud schemes. This is because, the victim is far less likely to donate more than what he/she can afford.

In a slight variant of “Charity Scam,” the scammer pretends to have a terminally ill mother, or pretends to be a poor university student, and simply begs the victim for money to pay for medical treatment, to pay for college tuition, to sponsor their children, etc. The scammer assures that the money will be repaid along with the interest by some third party at a later date (often these third parties are some fictitious agency of the Nigerian government, or the scammer themselves once a payment from someone else is made available to them). Once the victim starts “donating” funds for the cause put forth by the scammer, the scammer tells the victim that additional money is needed for unforeseen expenses, similar to most other variants; giving excuses similar to those mentioned earlier. Many scammers would even go to the extent of emotionally blackmailing the victim. For example, a scammer would say that as sponsor of the children, the victim is legally liable for such costs. In some cases, a scammer may pretend to be a student and would claim that a dormitory fire destroyed everything he owned and therefore he needs the money to re-establish himself/herself!

### **11.7.10 Scam No. 10 – Fraud Recovery Scams**

This variant targets former victims of scams. The scammer gets in touch with the victim telling him/her that their organization can trail and catch the scammer and recover the cash lost by the victim, provided the victim is willing to pay for this service. Alternatively, the scammer may tell the victim that a fund has been set up by the Nigerian government toward reimbursement for victims of 419 frauds (refer to Section 11.7.19). Scammer may further tell the victim that all that is required is proof of loss (scammer uses this as a bait to collect personal information of the victim) and a processing and handling fee to send to the victim the amount of the claim. In this ploy, the scammer is trying to exploit victim’s utmost need to recover their lost money, as well as the fact that the victim fell prey to such tricks and are, therefore, prone to get trapped into such scams. Often, these scams are conducted by the same scammer who cheated the victim in the first place, as an attempt to ensure getting every penny possible from the victim. Alternately, the original scammer “sells” information about the people he has scammed. To be on the safe side, the scammer would terminate contact, with another scammer who is also involved in the recovery scam. Sometimes the scammer impersonates the leading “fraud-related crime-fighters” in Nigeria, the Economic and Financial Crimes Commission (EFCC), which not only adds credibility to the scam, but tarnishes the reputation of the EFCC once this second scam is discovered.

### **11.7.11 Scam No. 11 – Pet Scams**

This is a scam derived from the adoption of a puppy or interesting pets such as African parrots, Peacock, Siamese cats, etc. A scammer first places a commercial announcement or sets up a webpage to present puppies for adoption or for sale at an incredibly low price. For this, the scammer typically uses stolen images from other websites and reputable breeders. When a victim calls back the scammer after seeing the advertisement and asks why the price is so low or asks why such expensive pet is being given up for sale/adoption, the scammer tells the victim that they (i.e., scammer and his/her so-called family) is migrating

to some other country for work (usually volunteer work as missionaries – this is to generate sympathy and empathy in targeted victims mind!) or for studies. Further, the scammers claim that he/she will have no time to look after the pet given the movement plan. Additionally, the victim will be told that the weather in the region/country that they are moving to, is like to affect the pet, or the scammer may give the excuse that that they already have too many pets to care for. In most cases it so happens that the potential victim is well targeted by studying victim's fondness for pets. Chapter 5 explains how "Phishing" and social engineering techniques are used for gathering personal information about people such as their hobbies, pets, etc. In Chapter 7, it is explained how social networking sites can be dangerous because you can lose your sensitive personal information if due care is not taken. In a typical "pet scam," the scammer exchanges a few E-Mails with victim to build trust. Once it is known that the victim is able to arrange a right home for the pet, the scammer offers to ship the pet, and requests the victim to only pay for shipping, or the scammer changes the original price substantially to make it sound legitimate. The victim, who by now has an emotional bond with the pet, feels obligated and even happy to do so, as shipping is a small price to pay compared to the pet's full price at a shop or breeder. The scammer assures to complete the transaction in a timely manner so that the pet gets ready to enter a new home and the victim is now thrilled. However, after wiring the money, the victim does not get the pet (because it never existed). If the victim ever hears from the scammer again it is only for extracting additional money [(to get puppy out of airport custody, or to pay unexpected vet bills that have come up due to pet's (pretended) illness due to journey)]. This goes on until the victim stops responding.

### 11.7.12 Scam No. 12 – Bona Vacantia Scam

The English term "bona vacantia" refers to property that does not any more have an owner, and is taken over by sovereigns. Depending on the country, there are different names for this procedure. For example, in the US, there is no official name for this; it just consists of land that is free, that is, not claimed by anybody, and, as a result, the property goes to the government. However, if everyone is not aware of it, you can recover it. In the UK, "bona vacantia" is a property without owner, that is, a property which has been passed to the Crown. The administration of the property rests with the Bona Vacantia Division of the Treasury Solicitor's Department. Some cases of this type of scam show that fake E-Mails and letters, claiming to be from this department, have been reported to inform the beneficiaries that they are going to benefit from an inheritance and that they need to pay a fee before getting more information or releasing the money.

Bank accounts, company assets, property or anything else that is worth the money counts as "unclaimed property" in these situations. There are cases in which people die, but they did not designate their property or items to people. Whichever department is in charge for supervising the money or property, administers them until a heir or other beneficiary can collect them as predetermined in some kind of will. These free properties or money are not kept undisclosed but advertised in the local paper, or through a website and they may request some vital personal information such as a full name or perhaps relations names and that information is validated against the list to see if there is property for the inquirer. At times, names of relatives will be required.

Given this scenario, scammers have used the possibility of this situation to their advantage for a long time. There are people who would be very receptive to the idea of receiving property or funds from a relative they did not know about. Such people can be preyed upon by scammers who just want their money. In "Bona Vacantia Scam," the scammer randomly shortlists some names from the telephone directory, E-Mail Spyware, etc. from where the person's name is available; this could even be from social networking websites.

The victim is then contacted by E-Mail or letter and told he/she is heir to money that has been unclaimed. This communication is made to look very official and genuine.

Availability of bona vacantia, or unclaimed funds, is usually advertised on the Internet or by other means declaring that there are unclaimed funds and one should apply, giving their name and other personal information so that a check can be made to see if they are on the list. You might even have to enter names of family members. If there are unclaimed goods or funds matching the name of the person inquiring then they are contacted asking for more details to be submitted. The entire process takes place via letter or E-Mail and there is no agent involved. Knowledge about how recovery of unclaimed goods really works helps a person stay away from such scams.

The next step is that when the victims respond to the communication, they will be asked to give their contact details. Usually a phone call will be made saying the goods are available but there are expenses or fees that must be paid before they can be released. In almost all cases the victim will not ever hear anything about the money they sent but the requests for additional payments will continue until the victim stops responding, having realized that he/she should not pay more to the con men. In cases like these knowing whom you are speaking to and being able to verify the same with a service such as info-trace.com/area-code-906.jsp, can save much time and money because it would be realized that the agent is not who he claims to be. Personal cheques are even better for scammers, as it allows them to get more out of you. With the information on your cheque, such as your address and account number, they can empty your accounts. Sending a personal cheque to a con artist can result in identity theft. Absolutely avoid these correspondences if you can. If you do want to investigate these claims, consult the appropriate government agency to check up on them.

### 11.7.13 Scam No. 13 – Fake Job Offer Scams

These scams are also known as “employment scams” – they are a form of criminal activity perpetrated by unscrupulous individuals or organizations posing as recruiters with personnel needs and/or hiring agencies that offer, and promise, attractive jobs and big money to people seeking for employment opportunities or interested in working in certain business sector. This scam is aimed at persons who have published their resumes on job sites. The scammer sends a letter with a falsified company logo. Typically, the job offer seems to provide extraordinary remuneration and perquisites. The offer also mentions that the victim needs a “work permit” to be able to work in the country. To make the ploy believable, scammers do not forget to mention the address of a “government official” to contact – obviously it is all bogus. The fake “government official” then starts fleecing the victim by extracting “fees from” the unwary victim for the work permit and other matters. These days everybody is looking for a highly paying job and scammers take advantage of that psychology to create this kind of scam. The result (as seen from the target’s perspective) is that the “targeted” applicants seem to receive bogus job offers via E-Mail with scanned appointment letters, work confirmation, and employment contracts from well-known employer. Later on, the victims are instructed to contact specified tour agencies, immigration agents and solicitors (apparently all abroad). These agencies and agents are supposed to assist them in getting them the required work permits and visas.

To summarize, this is how the “fake job offer scam” works:

**Step 1:** To begin with, applicants are lured by attractive job offers in certain countries. Scammers give impression to the victims that the job does not involve high skills. This is done by using (without the knowledge of victim) the names of well-known companies such as large hotel chains. Section 11.2.25 Example 25 is a real-life example of such scam rackets busted by Pune Police in October 2010. Here is an example of a fake E-Mail the victim might get as a result of this scam (the mail is supposedly coming from the E-Mail ID cost-world\_textileofficebox@yahoo.co.uk – refer the discussion in Chapter 2 about “Fake E-Mails” – Box 2.7).

The typical E-Mail in this scam could look as follows:

**WELCOME TO THE COST WORLD COMPANY**

Dear Sir/Madam,

Am Mrs. Kathy Thomson, payment remittance manager for COST-WORLD contemporary furniture (The Cost-world Company Ltd). Its a young business and need a trustworthy representative in the UNITED KINGDOM, UNITED STATES, CANADA and all other European country and its environ to work with ....who will be engaged 3-6hrs Weekly and earn between US\$700 to US\$1200 weekly. We are into sales of Primitive Artworks & Textile Material which has been a very profitable business and we are a subsidiary ofbizcom\_services ltd.

We sell this within these regions, United Kingdom and also parts of Scandinavian Europe with materials mostly in high demand in the UK.

**WHAT YOU NEED TO DO FOR US?**

The worldwide money transmit tax for lawful entities/companies) in UK is 12.5%, while for the individual it is only 7%. It does not makee sense for us to operate this way, given that the tax for international money transfer made by a private individual is 7%. That is why we need you! We need agents to collect payment for our textiles (in money orders, cheque or bank wire transfers) and to send back the money to us via Money Gram or Western Union Money Transfer. This way we will save money because of tax amount going down.

**JOB DESCRIPTION?**

1. Receive payment from Clients;
2. Cash Payments at your Bank;
3. Deduct 10% which will be your percentage/pay on Payment Processed;
4. Advance balance after deduction of percentage/pay to any of the offices. One of these offices will contact you about sending the payment. The payment is to be forwarded either by Money Gram or Western Union Money Transfer.

**HOW MUCH WILL YOU EARN?**

10% from each operation! For instance: you receive £7000 via checks or money orders on our behalf. You will cash the money and keep £700 (10% from £7000) for yourself! At the beginning your commission will equal 10%, though later it will increase up to 12%!

**ADVANTAGES**

You will have tremendous flexibility - you will not need to go out as you will work as an self-governing service provider right from

your home office. Your job is completely lawful. You can earn up to £4000-5000 monthly - this will depend on the amount of time you will devote to this job. You do not need any funds to start working on this assignment. You can do the work effortlessly and without leaving or without any impact on your current job. For employees, who commit efforts and work hard, there is a good opportunity to be promoted into managerial position. Experience shows that our employees never leave us because to the excellent work conditions we offer.

**MAIN REQUIREMENTS:**

No less than 18 years or preferably older officially capable accountable ready to work 4-5 hours per week PC knowledge E-Mail and Internet experience (minimal) And please know that Everything is absolutely legal.

HERE IS A COPY OF THE EMPLOYMENT FORM FOR YOU  
Reference No:- LSLCA/2031/ 8161/05  
Batch No:- R4/A313/2-60

**IMPORTANT:**

You must be over 21 years of age.  
US, UK, CANADIAN, AUSTRALIAN, OTHER EUROPEAN  
CITIZENSHIP.

**EMPLOYMENT FORM**

First Name:.....  
Last Name:.....  
Address.....  
City.....  
State.....  
Zip.....  
Phone.....  
Marital Status.....  
Age.....  
Nationality.....  
Present Occupation.....  
Thanks for your anticipated action.

Yours Sincerely,

MR KENDRA THOMSON, payment remittance manager for  
COST-WORLD

HOUSE OF BLISS ART GALLERY  
98 Stuart Court, Richmond Hill,  
Richmond, Surrey, England, TW10 6RJ  
<http://www.houseofbliss.com>  
Phone #:+(44) 702-403-7663 or +44703-186-0621

**Step 2:** Having ensured that the victim is hooked, the fraudsters will require the victim to send a small amount of money as compensation for work permit applications or VAF visa applications at embassy in the country where they claim the job is. They may even assure to get the victim the reimbursement for this amount once he/she is in that country.

**Step 3:** After you are tricked with Step 2 you now get into fraudsters' "net." Now they have you as the target for their further requests) such as processing, flights and handling charges. All this is, of course, to extract more money from you! The modus operandi of most of the frauds is to boost your confidence by only asking for a small amount of money at a time and then the fraudsters go for the big kill later on down the line!

A variation of the job scam pretends to take on board freelancers who seek genuine jobs (such as in editing or translation), then a "pre-payment" offer for their work is made. There are ways to keep away from these fake-job-offer scams/employment scams. You should watch out for certain doubtful points and ambiguous information that might make you distrustful about false claims and likely employment scams:

1. Be cautious with job search or training services that promise or imply "guaranteed" results or any other statement assuring job opportunities that look "too good."
2. Be wary about any payment and be careful before even making a slightest amount of payment. Get in touch with official job consultants to seek information on the realistic value of the offered courses and diplomas.
3. Never pay any upfront fee for placement services that offer a "dream job."
4. Be careful with agencies stating limited time reduced rates or special deadlines to apply for a position. They will warn you to apply (and pay) before a date. In other case, the wonderful job opportunity will vanish, and your name will be removed from the list of "lucky" applicants. After the famous deadline, the offer is the same – with another deadline, of course.
5. Be wary of companies or agencies offering salaries too high for the promised job. Many of them offer fantastic starting incomes, which cannot be farther from the reality. In case, you are interested in such services, the best option is phoning or getting in contact with some company to inquire about this specific subject.
6. Of course, never depend on oral promises.
7. Be careful with listing or bank services that provide third parties with access to your resume. In this case, privacy and confidentiality must be sealed and protected, and the activity of such agencies must strictly comply with privacy policy and data protection regulations, and internal security rules that guarantee the highest possible protection of stored data.
8. Job seekers should not be duped by any promise of a refund if no job or lead materializes, which is an excellent incentive to bait those people not willing to pay money for a failed job search.
9. Be aware that fraudulent employment services will use an endless string of excuses for why you are not entitled to a refund. For instance, a request for copies of the rejection letters from the companies. The problem is that, in the most of the cases, you will not receive any of such letter from those companies, which are not obliged to reply.
10. In such cases it is advisable to seek for information on the prospective employers or recruiter through another source and contact them directly or visit their offices in regular business hours.
11. Forget about companies with no legitimate street address and companies or agencies that refuse to provide verifiable references.
12. Be cautious of fake references. Several websites dedicated to scam job seekers draw on remarkable lists of people who supposedly found a job through their services. An assortment of express testimonials from people already working on the ship (e.g., with cruise ships or oil rigs), including photos/images of smiling persons sporting their new safety helmets and dressed in neat company uniforms seen at their workplaces.

13. Keep in mind that there are many cases where such scammers are fully aware that many of their potential victims will go all over the Internet to seek information and references about the “agency” and its services. Therefore, *scammers often post bogus messages in forums and interactive websites devoted to job hunting and career planning.* There have even been cases of websites and forums edited and managed by these same tricksters just to fill them with multiple fake threads started and continued by supposed forum members engaged in long discussions, showing generally favorable opinions and perceptions toward the subject.
14. Watch out for companies or agencies who ask for your financial information. Legitimate employers do not usually need credit card or bank account numbers, which is just an option of direct deposit of paycheck.
15. Wait until the personal interview at the company’s offices before agreeing to a direct deposit option, refusing to accept the job if this is the only option offered by the supposed employer.

Organizations or agencies may ask for non-work-related personal information – such as social insurance number in the US, PAN card in India, passport, etc. or any other piece of “sensitive” information prior to offering a job in writing. Carefully evaluate contact information mentioned in job advertisements or related E-Mails, and specially watch the “spelling errors.” Also check if there is any “free” E-Mail address that does not show the company’s name, and inconsistencies with physical addresses or area or zip codes. All of them are common indicators for spotting job scams. Pay careful attention to website address that look vague – for example, <http://www.theweb.com>. Be particularly careful about websites that make a claim to be dedicated toward providing job opportunities or typical recruiters not inclined toward using links in advertisements, forums or other Internet sites, which may lead to similar websites and fake replicas. All such sites are only meant for taking away your personal information in a form of deception called “Pharming” (addressed in Chapter 5 (see Box 5.10 in Chapter 5).

There are companies or agencies that operate outside of the country or state where they advertise. Usually, these individuals purposefully seek to distance themselves from their victims in order to avoid closer scrutiny and complicate an investigation by police authorities. They do not use a genuine street addresses, but they depend on post office box addresses, or set up their head offices, with little more than a nameplate on the door, in one state but may operate from other far-away place or even from overseas.

### 11.7.14 Scam No. 14 – Rent Scams

News of such scams is rampant in newspapers. People are on constant move – the workforce today is really global and people do travel all over the world in connection of their work, be it students, professionals and many others. Sometimes, people moving from one place to another want to sell or rent their real-estate property (house, apartment, etc.). Scammers take advantage of the fact that people need accommodation or the fact that accommodations are on sale. Scammers are on the look-out for foreign students, doctors, etc. who try to contact a landlord who could offer an accommodation. After the conditions are negotiated, a fake cheque is sent for a larger sum than agreed to. After this, some “emergency” situation is “created” which requires part of that sum to be urgently wired back. It may also happen the other way round, wherein a fraudster advertises on the Net about a lodging facility and indicates that money needs to be wired as an advance payment. The victim ends up realizing that there is no accommodation!

One of the tricks used by rental scammers is to pitch the rent of the “fake” lodging arrangement below the regular rental rate in a certain market. This becomes an attraction for the person looking for inexpensive lodging. This also allows the fraudster to accept as many E-Mails or inquiries as likely. You should not allow yourself to become a prey of such tricks. You can actually scrutinize a “rent scam” mail by looking out for the following:

1. Does the E-Mail begin by addressing you with Sir/Madam?
2. Are there too many wrongly spelt words in the E-Mail?

3. Are there character mistakes in the E-Mail? For example, Hello, my name is Susie.
4. Is there excessive capitalization?
5. Does the E-Mail allude to words such as “UK,” “Cashiers’ Cheque,” “Nigeria,” “Doctor,” “Reverend,” etc.
6. Is the E-Mail from a free E-Mail provider, such as gmail, yahoo, AOL (America Online), hotmail?
7. Does the E-Mail refer to another person or agent?
8. Does the E-Mail mention “wanting to move in site unseen”?

If the E-Mail has most of the elements described above, then there is a good chance that it is a scam. If you are unsure, it is best to not reply to the E-Mail. Table 11.14 shows some of the typical tricks used by rental scammers and has some good advice for you.

Also read about a related scam called “Craigslist Scams”; it is explained in this section under illustration number 20.

**Table 11.14 | Beware of rent scammers**

	<i>Rent Scam Trick 1</i>	<i>Rent Scam Trick 2</i>	<i>Rent Scam Trick 3</i>
<i>Typical Subject Line Used in the Scam Mail</i>	<i>The Property in the Advertisement Is Not Really Mine</i>	<i>I Overpaid You with My Money Order!</i>	<i>Wire the Money to Your Own Friend!</i>
Comment 1	This one has been happening a lot lately. The scammer logs onto home rental sites, makes a copy of the home information, and retransmits that information onto another site.	In this scenario, you are renting out your room or house, and you get this weird E-Mail from someone in Africa or the UK. It could be some pretty African model or a poor missionary that wants to rent your place.	This trick could potentially fool a lot of people, especially if they are not familiar with wire transfers.
Comment 2	One problem – the scammer posts his own contact information instead of yours!	You give them your postal address for them to be able to send you the money ... .	The scammer says, “If you want to rent my place, I need proof that you have funds. So go ahead and wire some money to YOUR OWN friend, but just E-Mail me a copy of the receipt so I can verify that you have the funds.”
Comment 3	As mentioned previously, scammer sets the price really low so that he can lure tons of victims into contacting him for that sweet rental deal.	A week later, you receive the money order for a HUGE amount. You take the money order to the bank and deposit it. The bank confirms the money order, so you leave the matter there, and all seems fine.	YOU (the victim) feel comfortable since you are to send money to your own friend whom you trust.
Watch out!			

(Continued)

**Table 11.14 | (Continued)**

	<i>Rent Scam Trick 1</i>	<i>Rent Scam Trick 2</i>	<i>Rent Scam Trick 3</i>
<i>Typical Subject Line Used in the Scam Mail</i>	<i>The Property in the Advertisement Is Not Really Mine</i>	<i>I Overpaid You with My Money Order!</i>	<i>Wire the Money to Your Own Friend!</i>
	Then he initiates some kind of baloney to tell the victim that he (i.e., the fraudster) is on “vacation” and that he needs you to “wire him the money” before he can hand you the keys to the house.	Then the scammer says “Oops, my guarantor sent you excess money, can you please wire some of it back to me?”	This is what will actually end up happening if you did that – the scammer takes the PASSWORD ON THE WIRE TRANSFER FORM, goes to his nearest western union, and takes the money himself!
CAUTION	Your money is gone forever!	Your money is gone forever!	Your money is gone forever!
	DO NOT WIRE THE MONEY if you are not sure.	DO NOT WIRE THE MONEY if you are not sure.	DO NOT WIRE THE MONEY if you are not sure.

### 11.7.15 Scam No. 15 – Attorney Debt Collection Scams

This type of scam involves law firms collecting money owed typically to Asian companies. The scammers aim at law firms by using certifiable company names. This is a very professional scam, and you could be the target – so watch out if you are lawyer. If the scammers approach you, they will say they represent a manufacturing company somewhere in Asia. When you check on the company, you will be able to verify that it exists and is a legitimate company. Remember that creating fake websites is not at all difficult (refer to Box 2.7 in Chapter 2). The story is that they want you to represent them for collecting a debt owed by a company in your county or state. They will ask you to submit a fee contract, and they will sign this and return it.

Scammers will then inform you that they have informed the debtor about having employed you and that shortly you will be notified that the debtor is paying the debt. You will then receive a certified cashier's cheque delivered by FedEx or DHL. You are required to place this cheque in your trusted account, and when the cheque is cashed you take away your fee and costs, and wire them the balance of the collected firms. The cheque may be drawn on a genuine bank that you would be aware of. Victims are then asked to take a percentage and wire the remainder to a bank in certain country – typically, Korea, China or somewhere else generally in Asia. The bank, which this cheque is drawn on, has nothing to do with the scam. The cheque is bogus!

Bankers advise that instead of depositing a suspicious cheque in your trust account, you can request that your bank send this cheque directly to the “issuing” bank and request collection. This avoids the embarrassment of a bounced cheque in your account and should put everyone on notice that you are concerned about this cheque. One of these scams seen was very well done until the instructions for wiring the funds were given to the attorney. A tip-off was that the address in the wiring instructions had nothing to do with the legitimate front company they claimed to represent.

If the bank did not show due diligence and did not notice that it was a fake cheque, and if they deposited the funds in your account, then you would never ever have any reason to believe that this was a fraud of any kind. However, there was an attorney in Texas who actually had a cheque honoured by the bank, and wired the money to the scam address. Later the bank came back and emptied his account when the forged cheque was discovered. The bank will go against you even if they have some liability. You do not want to get into a major court case trying to protect a forged cheque. You will have a tough time trying to give reason for money that is taken away from the naive bank. If you believe a collection matter or similar scam is occurring, you should find an autonomous source for the “client” address and get in touch with them to confirm that the person who contacted you actually comes from the genuine company. Also you can call the local “debtor” and ask them if they have done business with the so-called creditor company.

What really bothers is that both the “creditor” company and the “debtor” companies are real companies and have nothing to do with the scam. The best tip-off is the bizarre “wiring instructions” which will be sent to someone not related to the “creditor” who “hired” you. Some attorneys experienced that when investigation agencies were contacted about these scams, those agencies showed little interest. So be aware that you could pretty much be on your own. According to some people, the scammers prefer to be located in certain countries where it is easy for them to operate; probably due to weaker laws and possibly for many other reasons. Therefore, it is always good to check on the country mentioned on the envelop that brings the cheque to you. If the envelops originates from certain countries that are known to be infamous for frauds you can pretty well be sure that this is a scam.

Although not common in India, in the US, there are attorneys who do collections, often based on contingency. A scammer contacts the attorney by pretending that he/she represents a big international firm headquartered in another country. The scammer tells the attorney that the organization has no officially permitted representation in the attorney’s state, and needs to collect arrears from another business in that state. Scammer requests the attorney to send via E-Mail a standard retainer contract. As this is a common practice in the US, the attorney sends an E-Mail containing the contract document. The scammer signs the contract and returns it. After some days, the scammer informs the attorney that legal representation has now been obtained and that the debtor has agreed to pay the debt by the end of the month. Red flag #1 is when the scammer urges the attorney not to get in touch with the debtor company since the client wishes to maintain a working relationship with the debtor, saving court case as a last option. The attorney is instructed to make contact with the debtor only if the committed payment is not made on the promised date. On the promised date, the huge cheque is sent to the attorney, who deposits it in the law firm account keeps his, that is, attorney’s emergency fee, and sends back the rest of the amount to the scammer. Red flag #2 is that the scammer will request the money be wired to a foreign country, or insists on speedy payment. Super smart scammers will file articles of organization with both states, will build websites, and will also purchase prepaid cell phones with local phone numbers. This will help scammers to do the job of “dual imposter,” that is, the scammer can pose as both client and debtor. Using the Internet communication that allows “faceless” communication, all of that can be done inexpensively and easily. One Texas law firm lost \$158,000 on one of these fake collection scams.

### 11.7.16 Scam No. 16 – Malware Scams

Malware and Trojans are explained in Chapters 2–4. Discussion about ID theft and Phishing is available in Chapter 5 and zombies and botnets are discussed in Chapters 1 and 2 (Section 2.6). We have got so used to Internet convenience and the search engines running on them. Have you ever thought why it is possible for

you to use the Internet for FREE? It is because there are sponsored links on the Internet and there are banner ads (advertisements) on the sites that you visit.

Be aware, however, that the third-party cookies store information about you, addresses of the sites that you browse, the IP address of your computer, in fact the entire site-to-site traffic flow. The information stored in these cookies is served to organizations that have presence on the Internet for the online marketing of their products. These practices can harm you in that your “personal information” is changing hands. Recall the discussion in Chapter 5 about “Phishing” and “identity theft.” Using malware to infect computers is now a very popular scam (Box 2.9 explains the term “malware,” and the term “zombie” computers is also explained in Sections 2.6 and 2.7 in Chapter 2). At times the objective is to just turn the infected machine into part of a very big Botnet where computers are remotely manipulated to send Spam or attack networks. At other times the objective is to steal the identity.

There are a couple of scenarios under which these scams run. For example, anyone who has a blog has probably seen blog Spam; comments to the blog simply try to entice people to go to some other site. Most of the time, the site being advertised is merely trying to enhance its search engine rankings to create more revenue advertisements. The more links there are to a site, the more popular the search engines becomes. It is often thought that “blog Spam” is a good way to enhance the search engine rankings. In some cases this turns malicious. Some sites participate in extensive intellectual property theft to improve their rankings. In Chapter 9, intellectual property (IP) is discussed – you may like to refer to that chapter.

In yet another scenario, a “business” contacts you saying that your computer is running slow or is infected with malware. They will then direct you to a website and ask you to download some software; this software can be in many forms – it may allow the scammer to gain access to your computer in order to find personal information and bank details. Here is how it works. The person or group launching the attack transmits an E-Mail message. The more authentic it looks the better. The idea is to have the receiver open the attachment that is sent through the E-Mail. Once the receiver (the victim) opens the attachment, a malware gets installed on his/her computer. Although the next happening depends on what has been installed, the results can be catastrophic. Scammers can purchase malware viruses online at a small price. Alternatively, scammers can purchase an entire virus pack with updates and 1-year technical support with an affordable fee. This activity of scammers is rampant, and at the same time more complicated and hard to spot as time goes on. The job search site victims would have no clue about a problem until it was too late.

There are ways to avoid becoming victim to malware scams:

1. Remember never to open an E-Mail attachment from an unknown person. Everybody is a suspect when it comes to online security and online privacy matters! Even those from friends should be suspect unless it's something you expected (their computers could have been taken over without them knowing). Refer to Appendix C – Part 1.
2. Treat every attachment as suspicious. Never open anything with a suffix of .exe, .scr or .rar. Remember always that Trojans can be concealed in many ways, including pictures, which usually have a .jpg or .gif suffix – most of them may not cause harm.
3. Make sure you have a good firewall and antivirus software. Both are crucial and vital assets in your computer. They are definitely less expensive than having a bug removed.
4. It is a good idea to use a mail filter or a Spam guard. It offers you a chance to inspect your mail before you download it onto your computer, and delete any items you do not want on your hard drive, as well as blacklist certain E-Mail addresses. It is gratis, and a very helpful tool to get rid of Spam and well as potential viruses. This is one area where being suspicious works well. Until you

know otherwise, assume everything is malware. If you do banking transactions online, do verify your account transactions regularly for doubtful activity. Depending on your usage, you should review the monthly statements from your credit cards and debit cards. You should also validate your credit file twice a year to see if anyone has attempted opening accounts in your name.

### 11.7.17 Scam No. 17 – The Advance Fee Fraud

Fraudsters often succeed because they are good at exploiting people's confidence or naivety. An "advance-fee fraud" is a self-confidence ploy in which the targeted victim is influenced to move forward financial funds with the expectation of achieving a considerably bigger gain. Thus, as the name suggests, a "confidence trick" or "confidence game" (also known under other terms such as binko, con, flim flam, gaffle, grift, hustle, scam, scheme, swindle or bamboozle) is an attempt to defraud a person or group by gaining their confidence. In this game, the victim is called the *mark*. The trickster, that is, the scammer who pulls the trick is called variously as *confidence man* or *con man* or *confidence trickster* or *con artist*. The accomplices, involved in the game, are referred to as "*shills*." A "*shill*" is the professional help – the shill is paid to help another person or association to sell goods or services. The shill pretends as if he/she has no association with the seller/group and gives onlookers the feeling that he or she is an eager customer. "Shilling" is an unlawful activity in many situations and in many jurisdictions because of the repeatedly fraudulent and detrimental nature of their actions.

People involved in the scam may be real; however, there could be impersonated people or fictitious characters played by the con artist. In this scam, the fraudster looks for many kinds of victims. For example, the victim could be the wife or son of an expelled person who has amassed considerable wealth from illicit means; or it could be a bank employee who is aware about a wealthy person on death bed with no family or any other close relatives; or a rich foreigner who has made a bank deposit just before being killed in a plane crash (leaving no will or known next of kin); or it could be a soldier who by sheer luck has hit upon a hidden cache of gold; or a business being audited by the government; or a disgruntled worker or corrupt government official who has embezzled funds; or a refugee and so on. The money could be in the form of gold ingots, gold dust, money in a bank account, blood diamonds, a series of cheques or bank drafts, and so forth. An interesting thing to note is that typically the sums involved are usually in millions of dollars, and the investor is promised a large share, typically 10% to 40% if they assist the scam character in retrieving the money. In relation to the business of diamond trading, an interesting term "blood diamond" comes into picture. It is also called a "converted diamond," or "conflict diamond," or "hot diamond," or a "war diamond." Blood diamond refers to a diamond obtained through mining in a battlefield and sold to finance a rebellion, invading army's war efforts, or a warlord's activity, usually in the African subcontinent.

Several operations are well organized in Nigeria, with offices, temporary fax numbers, and often contacts at government offices. When the victim tries researching on the backdrop of the offer, he/she will end up finding that all pieces fit together. Scammers operating with "advance-fee fraud" often attract wealthy investors, investment groups, or other business entities into scams and the result is large losses of multi-million dollars. However, there are also scammers who operate as part of smaller gangs who do not operate so "professionally" or gangs that operate independently. Scammers, operating in such scenarios, have lesser access to the connections mentioned above and therefore such small-time scammers may not have big success with wealthier investors or business entities attempting to research them. However, even the small-time scammers are able to convince middle-class individuals and small businesses, and can extract hundreds of thousands of dollars from such victims.

If the victim agrees to the deal, the other side often sends one or more false documents bearing official government stamps and seals. Often a photograph used by a scammer is not of any person involved in

the scheme. Multiple “people” involved in schemes are fictitious; the author of the “WEST AFRICAN ADVANCE FEE SCAMS” article posted on the website of the Embassy of the US in Abidjan, Côte d’Ivoire, believes that in many cases one person controls many fictitious personas used in scams.

### *How the (Advance Fraud) Scam Works?*

A scammer presents a delay or financial challenge and says that it is preventing the transaction from occurring as planned. The mails planned to present the hurdle say things such as “To transmit the money, we need to bribe a bank official. Need your help us for a loan.” or “For you to be a party to the transaction, you must have holdings at a Nigerian bank of \$100,000 or more” etc. Further delays and additional costs are indicated, with scammer assuring a forthcoming large transfer alive. The scammer convinces the victim that the money paid by the victims will be more than compensated by the payoff. At times, the scammer may also add psychological pressure by claiming that on his side, he had to sell off his belongings and had to borrow money on his house to pay certain fee. Or the scammer may refer to various salary scale and living conditions in the African subcontinent, comparing with the conditions in the Western world. Most of the time, however, the psychological pressure is self-applied; once the victim provides the money toward the payoff, the victim has a vested interest in taking the “deal” to the finishing line! Some victims believe that they are smart enough to fool the con artist. This kind of “over confidence” on part of victims is often exploited by the fraudsters. They do this by deliberately writing in an awkward and crude style so that the victim sees them as naive. However, that is all well planned by the scammers!

The crucial aspect of almost all advance-fee scam is that the committed money transfer never happens because the money or gold or diamond never exists! The scammers depend on the fact that, by the time the victims realize this, they victim may have sent large amount of their own money. Sometimes this money can be the large amount of money that has been taken on loan or even stolen, to the scammer via an untraceable and/or irreversible means such as wire transfer. That he is cheated, dawns upon the victim often only after being confronted by a third party who has noticed the transactions or conversation that may get recorded and by then it is too late!

In extreme cases the victim may not realize that he/she has been defrauded. In another version of this scam the con man claims to have the arrangements to facilitate legitimate business loans; the victim here is not persuaded that he is doing anything illegal. The fraudster meets the victim, and is able to act the part of a well-connected and experienced loan broker. He asks for payment in advance, which is normal for large loans. Then the loan gradually comes in and the victim may end up being cheated for a very large amount, thinking only that the deal simply failed. It is a pity that such frauds may go unreported. This can happen mainly due to two reasons: (a) either the victim does not realize he has been cheated or (b) due to unwillingness to admit the facts. Owing to the “non-disclosure clauses” included in the fraudulent contract, victim may feel scared and that would delay the scam reporting till such time that the victim is sure that he/she has been cheated.

A very common trick used by scammers is to request that payments should be made by means of a wire transfer facility. The reason given by the scammer usually relates to the speed at which the payment can be received and processed, allowing quick release of the supposed payoff. The actual motive behind giving that reason is the fact that wire transfers and similar methods of payment are unalterable, undetectable. This is because identification without knowledge of the details of the transaction is often very difficult. Scammers are clever enough to use mobile phone numbers rather than landlines which have a fixed location and are therefore traceable. A scammer may buy a low-price mobile phone or may use a pre-paid SIM card for which it may be necessary to submit subscriber information. This makes it further difficult to trace the scammer. Technology supports the scammers – if they feel they are being traced, they simply throw away their mobile phones and purchase new ones. Refer to Sections 3.2 and 3.5 in Chapter 3.

### The Typical Methods Used in Scams

1. **Fake cheques:** Bogus cheques and money orders are used in many advance-fee scams, such as auction/classified listing overpayment, lottery scams, inheritance scams, etc. They are also used in almost any scam when a “payment” to the victim is required to gain, regain or further solidify the victims’ trust and confidence in the validity of the scheme. The cheques clearing process normally takes 7–10 days and may even take up to a month when dealing with foreign banks. Some amount of time elapses between the finances appearing as available to the account holder and the cheque clearing. This passage of time is known as the “float” – during that time, technically speaking, the bank has floated a loan to the account holder and it is liable to be eventually covered with the money from the bank that clears the cheque.

The cheque given to the victim is typically faked but it is drawn on a real account with real money in it. For example, with accounting software (such as QuickBooks) and/or pre-printed blank cheque books with the correct bank name printed on each leaf of the cheque book, the scammer can easily present a cheque that looks absolutely genuine. Such cheque will pass all verification tests, and may even clear the paying account if the account information is accurate and the funds are available. However, notwithstanding whether the cheque clears or not, it eventually becomes obvious either to the bank or the account holder that the cheque has been forged. This can happen in as short a period as 3 days after the money is available if the bank supposedly covering the cheque finds out the cheque information is not valid. It could take several months for a business or individual to notice the fake draft on their account. It has been seen in some cases that although the cheque is genuine, the fraudster “arranges” to have a friend (or bribes an official to play the “friend”) at the paying bank to claim it is a fake. This can happen even weeks or even months later when the physical cheque comes back at the paying bank.

Notwithstanding how much time is involved, after the cashing bank is notified that the cheque is bogus, the transaction is inverted and the money taken away from the victim’s account. In many cases, this means that the victims could be in debt to their banks. This is because, by that time, the victim has already sent a large portion of the cheque amount (by some non-reversible “wire transfer” means) to the scammer and, since more uncollected funds have been sent than the funds otherwise present in the victim’s account, an overdraft results.

2. **Wire Transfer:** A key element of advance-fee fraud is that the transaction from the victim to the scammer must be untraceable and irreversible. Otherwise, the victims, once they become aware of the scam, can successfully retrieve their money and/or alert officials who can track the accounts used by the scammer. Fraudsters used to find wire transfers via Western Union as an ideal means for this purpose. The Western Union Company has its headquarters in the US and is an economic services and communications company. Before it discontinued the service, Western Union was the best known US Company in the business of exchanging telegrams.

The wire transfer, if sent globally, cannot be cancelled or inverted and that makes it difficult to track the individual who receives the money. What is more, the scammer may not even need to provide identification; they only need to know the transaction identification number and do not need to know the answer to the “secret question.” This is the reason why a large number of big scams involve making payment via wire transfer. Other comparable forms of irreversible payment are postal money orders and cashier’s cheques. However, the wire transfer method is most preferred by scammers because (a) it is the fastest method and (b) it makes the transaction untraceable.

3. **Anonymous Communication:** This mode of communication is used because the scammer's operations must be untraceable to avoid identification and because the scammer is often impersonating someone else. Any communication between the scammer and his victim must be done through channels that hide the scammer's true identity. The following options in particular are widely used:
  - *Web-based E-Mail:* Recall the discussion about "fake mails" in Chapter 2 (Box 2.7); because many free E-Mail services do not require valid identifying information and also allow communication with many victims in a short span of time, they are the preferred method of communication for scammers. Some services provide the masking of sensitive information such as the sender's source IP address. This helps the scammer because the scammer is completely untraceable even to the country of origin. It is possible for scammers to create multiple accounts and often they do that! Even if E-Mail service providers are notified about scammer's fraudulent activities and suspend the account, it is a trivial matter for the scammer to simply create a new account to resume scamming.
  - *E-Mail hijacking/friend scams:* Some fraudsters hijack existing E-Mail accounts and use them for advance-fee fraud purposes. The fraudsters send E-Mails to associates, friends and/or family members of the legitimate account owner with the intent of defrauding them. This trick usually requires the use of "Phishing" or "keylogger," "computer viruses," etc. to glean login information for the E-Mail address. Phishing is explained in Chapter 5 and keylogger tools and computer viruses are explained in Chapters 2 and 4.
  - *Fax transmissions:* Facsimile machines are commonly used tools of business whenever a client requires a hard copy of a document. They can also be computer generated using web services, and can be made unnoticeable by using prepaid phones with connection to mobile fax machines or by use of a public fax machines such as those typically found at a document processing business. Scammers often pretend to be business entities and they use fax transmissions as an unidentified form of communication. This method costs them more, because the prepaid phone and fax machine would generally cost far more than E-Mail; however, to a skeptical victim it presents a more authentic looking scenario.
  - *SMS messages:* Abusing SMS bulk senders such as WASPS, scammers subscribe to these services using fraudulent registration details and paying either via cash or stolen credit card details. They then send out a lot of uncalled for SMS'es to victims declaring that they have won a competition or similar event. Further, the SMS asks the victim to contact somebody to claim and collect their trophy. Typically the details of the person to be contacted will also be an undetectable E-Mail address or a "virtual" telephone number, that is, a telephone number with no phone line directly associated. Generally, these numbers are programmed in such a way that they can be forwarded to either a voice over IP service or to another phone line (fixed or mobile). Typically, scammers send these messages over a weekend when most of the staff in the office of the service providers has taken off. This is a grand opportunity for scammer to abuse the services for a whole weekend.
  - *Telecommunications Relay Services:* Many scams use telephone calls to convince the victim that the person on the other end of the deal is a real, truthful person. The scammer, perhaps pretending to be a citizen of some other nationality, or gender, that is, faking as somebody else, would stir up mistrust by telephoning the victim. Therefore, in such circumstances, scammers use TRS, a relay service (federally funded) whereby an operator or a text/speech translation program serves as the middle layer between someone using an ordinary telephone and a deaf caller using TDD (Telephone Device for the Deaf) or other TeleType device (see Fig. 11.65). A scammer pretending to be deaf would use a relay service. The victim, perhaps caught up by compassion for a physically challenged caller, might be more vulnerable to fall into the trap set by the scammer.



**Figure 11.65 |** TDD device.

Federal Communications Commission (FCC – see Ref. #57, Additional Useful Web References, Further Reading) regulations and confidentiality laws require that operators relay calls verbatim, and that they adhere to a strict code of confidentiality and ethics. Therefore, no relay operator may be able to evaluate the authority and/or legality of a relay call, and as such the operator is able to relay it without intrusion. This implies that the relay operator may not notify victims, even when they believe that the call is part of a scam. According to MCI (an American telecommunications subsidiary of Verizon Communications), about 1% of their IP relay calls in 2004 were used by scammers.

It is relatively easier to track phone-based relay services and therefore, scammers tend to prefer Internet Protocol-based relay services such as IP relay, telecommunications relay service (TRS), relay service or Web-based relay services. It is an operator service that helps physically challenged people (i.e., those who are deaf, hard-of-hearing, speech-disabled, or blind) to establish communication with users of standard telephone via a keyboard or assistive device. During their inception period, relay services were meant to be connected through a TDD (see Figure 11.65) or other telephone device meant to assist physically challenged people. Today, these services embrace any commonly connected device such as a personal computer, laptop, mobile phone, PDA, etc. These services integrate their overseas IP address with a router or server located within the US. At times, TRS is used to transmit credit card information – fraudsters use this feature to make a deceptive purchase with credit cards they steal. In several instances, however, it is merely a means for the fraudster to further lure the victim into the scam.

- *Fake websites:* Typically, 419 scams (another name for Nigerian Scams – they are explained later under illustration No. 19 of this section) are often perpetrated by E-Mail alone. However, to fool their potential victims, some scammers enhance the “believability” of their offer by using a fake website. Scammers construct these websites to imitate real commercial websites (e.g., eBay, PayPal, or say some real banking sites) for Phishing (visit Chapter 5 where “Phishing” is explained). Others scammers pretend to stand for companies or institutions to make scammers’ operations credible - in reality those companies do not exist!

In most scam operations, “Phishing” is the secondary objective. Scammers’ main objective is to cheat the victim by making the victim send the money through legal means. As a common method for this, they use websites for advance-fee fraud. For example, a scammer may construct a website for a fictional bank. Next, the scammer provides the login details to get the victim into that fake website. When the victim visits this bogus bank site created by the scammer, he/she sees the money promised by the scammer credited into his/her account. So, now the victim trusts the scammer and sends the advance payments asked for by the scammer. Fake or hijacked websites are the focus of online scams – an example of spoofed website is shown in Fig. 11.12.

Another twist to scamming comes when the links are provided to real news sites covering events claimed to be relevant to the transaction proposed by the scammer. For instance, a scammer may use news of the death of a prominent government official as a background story for a scam involving millions of dollars of the dead official's money out of the country. These are real websites with legitimate news, but the scammer is typically not associated in any way with the reported events – the scammer is just piggy-backing on the story to win the sympathy of his victim! Refer to Chapter 1, Section 1.5.9.

### 11.7.18 Scam No. 18 – Babysitting Scams

These scams seem to be more common in the western countries. They are also known as “Nanny Scams.” These scams are said to be another variation of the “advance scam” (refer to Section 11.7.17). Babysitting scam\Nanny scam involves recruiting unsuspecting individuals for non-existent babysitting, nanny, or au-pair employment, that is, couple to be employed.

In one variant of this scam, a potential employee may be lured by the offer of an “advance.” In another form of this scam, the victim may be asked to verify pricing and ultimately purchase items for the scammer’s non-existent child. At times, victims are asked to provide résumés, references, etc. to get the victim believe that the “employer” is genuine and that the high remuneration offered are valid. Scammers are smart enough to make the victim stay focussed on his/her worthiness for employment – this way, scammers succeed in making the victim diverted from thinking whether the offer itself is worthy of replying to.

Nanny scams seem to have become a common feature in the online babysitting community. If you receive any E-Mails analogous to the examples mentioned below, be careful! Keep in mind that the names (and ages) used in these scams are constantly changing, so pay close attention to the structure of these E-Mails rather than the details. Also note that most such mails will typically have *many misspellings and grammatical errors*.

As you read on, you will see the examples provided of some typical mails received by the victim. These examples show that under the pretext of the babysitting job, victim’s personal details are being sought! Interestingly, in almost all the babysitting scam mails, the scammer is saying that he/she is currently not in town but will be returning soon. As mentioned before, most of the times the scam mails happen to have lots of misspellings and in most such mails you will find that the grammar is also not upto mark. You will also notice the extremely informal and “slang” language used.



Note that in most of the babysitting scam mails, tempting offers are made, that is, accomodation, transportation for the candidate, etc. Also, in almost all such scam mails, the language sounds very informal, extra sweet and extra friendly; naturally because the scammer wants to lure the victim!

#### -----Typical Babysitting Scam E-Mail Example 1-----

My name is Mrs. Ashleen Joseph. My husband Philip is a Captain of a cruise ship and I have a daughter whose name is Anabella. Currently, we are on my husbands ship on a holiday and will not be back untill about two or three weeks time. We live in a large apartment and I require a babbysitter who would also help me out taking care of grocery purchases. We are OK to pay \$18 per hour. Can you tell us for how many hours you would be available. We can provide a Toyata Camry for you to take care of transportation problems.

I would like to know the following about you to consider you for this job:

- 1) What academic qualifications do you possess?
- 2) Do you have any good certificate to support your prior babysitting/Nanny experience?
- 3) How old are you?

- 4) Are you married?
- 5) Do you have any special aptitude?
- 6) Do you have any crime records?
- 7) Do you have a valid driver's license?
- 8) Tell us more about your temperament.
- 9) Can we have one or two reference(s) from you?
- 10) Can you handle finances if you are given a task to carry out?
- 11) Will your husband/boyfriend/parent support you taking up this job?

Let me know if you will available for the work offer.

Thanks and have a nice day

Mrs Joseph

#### **-----Typical Babysitting Scam E-Mail Example 2-----**

Trust all is well with u. Thank you for your response to my add. Hope you are had a great weekend. Let me start by introducing myself.

My name is Roberto Ferdinand, I am 30 years old and i am a single parent, I lost my wife about 2 months ago like i said in my add in the babysitter site, I have a son named Iyke and he is a year old. My Mom looks after Iyke in London, UK where she stays and she will be away on an apointment for a long time thats why i need a baby sitter between these periods, As i am bringing Iyke back with me, I have gone through your, Profile and resume and I think you are perfect for sitting Iyke, Also what are your rates? I would like you to work from Monday-Friday either in the mornings or evenings. In the Mornings From 8.30 am-6 pm or in the evenings from 6 till 10. Working on wekends is not compulstoyr so if you choose to work on Weekends you are to start by 10 am till 5pm. I can pay \$15/hour If the times are okay by you do let me know if they are not do let me know a favourable working time by you, So we can work something out. So do let me know what your charges are so we can proceede, I want you to start working asap okay. I live at 6562 Barnett St NE Atlanta GA 30306 I am away on a work assignment and i would return in 2/3 days. I would like to hear from you shortly. Heres my telephone number also its a satelite telephone so you can call me anytime 0112348028297715. You should have an international dialing acess or you can use a calling card I would like you to start soon, So please i would be expecting to get a message from you shortly.

So we can start of asap Thank you and see you soon. Do have a great day and stay blessed.

Roberto

#### **-----Typical Babysitting Scam E-Mail Example 3-----**

Hello,

My name is Mrs. Rose Smith wife to Captain John Smith. I am currently away on holiday with my phamily and expected back in a month's time. I have a cute 18-month-old girl called Kathy who i need to be looked after when we come back from our vacation. I would like to have things in order so that you could start up immediately; we arrive because her former nanny will not be available again.

You will be asked to work within the hours of 9am-4pm on Monday, Tuesday and Thursday and sometimes on weekends as well. If you are in to take care of my child i will arrange a car for your use, your private room if you wish to stay or spend the night.

Let me tell you a bit about us, I run a fashion outfit back home and my hubby is the captain of a cruiser ship which enables us to travel to different continents on vacations, we live a very simple life and we have a big

apartment, though its just three of us in the house, hope you can join us on a trip someday as our last nanny did, we are willing to pay \$100(one hundred dollars) upfront (non-refundable in case we change our mind) to show you how serious we need you.

Please get back to us with your resume and references o.k., (your house address and your telephone number inclusive). Illl be expecting your response please do have a lovely day.

Please get back to me.

Mrs. Smith

#### **-----Typical Babysitting Scam E-Mail Example 4-----**

Hello nanny/babysitter, my name is sarah tina martins. I am located In london. I have 2 kids,a male and a female and their ages are 2 and 4yrs old. I am shifting my residence for good to New Jersey because there I have my family business and it is really doing good over there and my arrival date is may 18. After a discussion with my people about proper care-taking arrangement for my children, because I am separated from my spouse, So I've finally decided to search for a good and responsible nanny/babysitter. Below are the offers.

We will be offering weekly,

1) Monday through Friday, from 11.30am-5:00pm.

And the weekly pay: \$960.

I will take care of your transportation which in addition to the weekly salary I will provide you irrespective of the distance you will travel to come to work with us. Please let me know the total trvelling expenses on a weekly basis from your place to our residence if you like to live out and furnish me with the expenses so we include it in your basic weekly salary. We are searching for good well mannered candidates with good attitudes, neatness and good respect for family relationship. If you intererst in this offer, please give answers all the questions below so i can have some idea how your personality is:

- 1) What academic qualifications do you have?
- 2) Do you have any related certificate to back up your babysitting/Nanny experience in the past?
- 3) How old are you?
- 4) Are you single or married?
- 5) Do you have any special skills that we can use in our house apart from baby-sitting work?
- 6) Were you involved in any legal offence in the past – civil or criminal?
- 7) Breifly describe your temperament.
- 8) Can we have a couple of work eference(s) from people you worked for in the past?
- 9) Is your husband/boyfriend/parent in support of you doing this job?

Let me know if you will available for the work offer. If you have anything to ask regards this offer, b free to call us. i await a response at your earliest convenience.

#### **-----Typical Babysitting Scam E-Mail Example 5-----**

How are you today, i am Mrs alice cage, i and my 2 children ( they are twin - a girl and a boy) they are 2 years old and I will be moving to the STATES(Florida) from France. I will be in the state in a couple of Weeks from now and for the next one(1)years during my official work appointment. I am coming with my 2 kids, and i need a lady to look after them, because there is nobody to be with them. so if available Kindly contact me ASAP, so we could make arrangement accordinlgy, will be waiting to read from you soon...

Regards

Mrs. Cage



Note how informal and ill-formed the language used is – it does not sound like formal communication from a person who is looking for engaging a professional help!

#### -----Typical Babysitting Scam E-Mail Example 6-----

Hell Babyseatter,

I m Katherine George I make films and also I co-ordinate with artists. Currently I m in Australia shooting for film project. I will return back to the states soon for another official assignment with other film director with my 3 years old daughter name Verona. I need a babyseatter. She is a good girl, she went with her father to Benin Republic when I m on work here in Australia.

My husband is very busy now and my Verona has to be with us in visiting the US with me. I think you will like my child because she is very lively, friendly and intelligent and will give you no trouble. I want to stay in US for at least 2/3 more months. During this time Verona should be with some babyseatter) from 9am to 4pm when im off to work. I'll pick her up. Let me know if you are interest and dont forger to write to me about how much you want to be paid for this job and also about are for the duration at which you would be babysatting her. Hope to read from you soon.

Have a hapy day

Carolina



Note that here the scammer forgot what name she/he started with! Notice also the grammatical errors, spelling mistakes, the too friendly and extra sweet language in all the scam mails quoted and also the “being away” pretext used.

#### -----Typical Babysitting Scam E-Mail Example 7-----

Good Day, I got your info at sittercity.com I am Pamela, I work as an Interior Decorator, I am 28 years old, i lost my Husband 2 months after i gave birth to this child. I have an assignment which i need to complete – it involves decorating of office and hotel for my client and i have a 6 months old baby boy. His name is Richard, i will be living for my assignment soon as i see someone to look after the boy, till i return. Contact to me with the full details about how you give service out to customer like me. What do you want to know from me about my child? Looking to read from you. My E-mail address: bhush006@gmail.com Have a lovely day. Pamela



Note the “sympathy” wave being created in the mind of the victim and again the “being busy,” “being away,” “having lost the spouse,” etc.

#### -----Typical Babysitting Scam E-Mail Example 8-----

My name is Mrs Jossy mark spouse to Captain Leonard mark who work on board the Royal carribean cruising company. We are located in California for now. Currently I am on holidays with family and I return in one months time. I have a cute 2-year-old boy called Daniel who I need to be looked after till we come

back from our vacation. I wish to put things in order so that you could start as soon as we arrive because her previous baby sitter will not be coming again.

You will need to work within the hours of 8am-4pm on Monday, Tuesday and Thursday and also sometimes on Saturdays and Sundays as well. If you want to look after my child I will make arrangements to provide you with a car when you commute to and from our home. I can also give you separate room because you may need to spend the night when I am away for longer days.

Let me tell little about us, I own small shop back home and my husband is the captain in air cruising company which enables us to be in many continents on vacations, we have very simple life and we have a large apartment with 8/10 rooms although it's just three of us in there, hope you can join us on a trip someday like our past nanny did, we are willing to pay \$150 (one hundred and fifty US dollars) upfront (non-refundable in case we change our mind) to show you how badly we need you.

Please contact us with your biodata, previous work references, telephone number and address o.k, I'll be wanting your reply please do have a lovely day.

Mr/Mrs Jossy mark.



Note again, here too there is the "ship" scenario, tempting offers like car, accommodation, etc. to lure the victim. The characteristic spelling errors are also there!

#### -----Typical Babysitting Scam E-Mail Example 9-----

MY NAME IS SARA BRIGHT. I WANT U AS A BABY SEATTER AND AM GLAD YOUR INTEREST IN THIS TOO. MY DAUGHTERS NAME IS JENINIFER. I WOULD LIKE U TO LOOK AFTER HER WHILE I GO TO WORK IN FAR LOCATION. I WAS STAYING IN WEST AFRICA, BUT NOW THERE IS CHANGE AND I AM COMING TO YOUR LOCATION BECAUSE I WOULD HAVE A CONTRACT WITH LESSLEY MIKE THERE. I WORK AS FASHION MODEL AND THE CONTRACT WILL BE FOR 6 WEEKS PERHAPS EVEN FOR TWO MONTHS. I WANT YOU TO LOOK AFTER MY DAUGHTER WHILE I WORK AWAY. I GO TO WORK 10 AM AND I GET BACK 4 PM BUT SOME DAYS EVEN MORE LATE. I WILL LIKE TO CONFIRM IF YOU WILL LOOK AFTER JENNIFER IN YOUR DAY CARE CENTRE OR THE HOTEL ROOM WHERE I WILL BE LODGING, I AM OK WITH EITHER WAYS. MY DAUGHTER IS 3 YEARS OLD, I WILL SEND YOU SOME PIX OF ME AND HER AS SOON AS WE CONSIDER THIS A DEAL I ASSURE YOU HOW MUCH YOU WILL LIKE MY DAUGHER. HOW MUCH WILL TAKE TO BABY SIT JENINIFER FOR 4/5 WEEKS AND THE TIME I NEED YOUR SERVICE FOR IS 9 AM TO 4 PM. WRITE TO ME WITH THE AMOUNT AND I WILL BE HAPPY TO MAKE THE PAYMENT IN ADVANCE TO SHOW YOU HOW URGENTLY I NEED YOUR SERVICE.

SARA

#### -----Typical Babysitting Scam E-Mail Example 10-----

Hello,

How are you doing today??? I seen your advert on a nanny site and though I ask you if you were available, my name is PAUL WALTERS, I have an adopted daughter her name is Leena she is 2yrs we both are out of the country for a family reunion, and I really need a sitter for Leena when we come back home okay,

Please do tell me how soon you are available, and if so do send me your biodata and some work references to my personal mailbox at  
 EMAIL: paulwalters\_06@gmail.com.

I looking to your response please do have a nice day.

Warm Regards  
 Mr Paul Walters

### **11.7.19 Scam No. 19 – Nigerian 419 Scam**

This scam has got this name because of the Nigerian Criminal Law has a section number that applies to it. You have read about the “advance fee fraud” scheme described earlier (Scam No. 17 in Section 11.7.17). You will realize that the mentioned scams are similar in nature. A typical example of the infamous “Nigerian Scam,” (also known as) “419 Scam” is as follows:

DEAR SIR,

AT THE OUTSET I MUST FIRST ASK FOR YOUR ASSURANCE IN THIS MATTER; THIS IS DUE TO ITS NATURE. THIS MATTER IS EXTREMELY SENSITIVE AND TOP SECRET THOUGH WE KNOW THAT A TRANSACTION OF THIS SIZE WILL MAKE SOMEONE NERVOUS AND AT THE SAME TIME ELATED BUT WE ARE TELLING YOU THAT ALL WILL BE ALL OK BY END OF THE DAY. WE ARE DETERMINED TO CONTACT YOU BECAUSE THERE IS SOME EXIGENCY IN THIS TRANSACTION AS WE HAVE BEEN CONVINCED ABOUT YOUR DISCRETNESS AND CAPABILITY TO WORK WITH SUCH TYPE OF TRANSACTIONS.

LET ME FIRST INTRODUCE MYSELF FULLY. I AM MR. MOHAMED ABBAS WORKING AS CREDIT OFFICER WITH THE UNION BANK OF NIGERIA PLC (UBA) – I AM AT THEIR BENIN BRANCH, I GOT INFORMATION ABOUT YOU WHILE I WAS LOOKING FOR A DEPENDABLE AND HIGHLY REGARDED INDIVIDUAL TO TAKE CARE OF THIS HIGHLY TOP PRIORITY AND CRUCIAL TRANSACTION. THE WORK IS CONCERNED WITH TRANSFERRING LARGE SUM OF MONEY TO AN OVERSEAS BANK ACCOUNT AND THAT IS WHY THIS TRANSACTION IS TO BE UNDERTAKEN WITH DUE CARE.

HERE IS THE OFFER:

A FOREIGNER AND AN AMERICAN, LATE BENINGGR JOHN DUKE (SNR) A DIAMOND MERCHANT WITH THE FEDERAL GOVERNMENT OF NIGERIA, UNTIL HIS UNFORTUNATE DEATH FEW MONTHS AGO IN KENYA AIRWAYS PLANE (AIRBUS A3K-300) FLIGHT KQ430 BANKED WITH US AT UNION BANK OF NIGERIA PLC BENIN AND HAD A CLOSING BALANCE AS AT THE END OF MARCH 2001 WORTH \$36,662,000 USD, THE BANK NOW EXPECTING A NEXT OF RELATIVES AS THE HEIR. THIS BANK HAS PUT IN LOT OF EFFORT TO CONTACT ANY OF THE DUKES RELATION OR FAMILY BUT THE BANK HAS NOT GOT ANY RESPONSE SO FAR. WE BELIEVE THAT THIS IS HAPPENING DUE TO THE ALLEGED PROBABILITY OF FEWER CHANCES TO LOCATE ANY OF BENINGGR JOHN DUKE (SNR) NEXT OF KIN (AS PER OUR RECORDS HE WAS NOT MARRIED NOR HAD ANY CHILDREN FROM HIS AFFAIRS WITH WOMEN).

THE MANAGEMENT IS BEING PRESSURIZED BY OUR CHAIRMAN AND BOARD MEMBERS AS WELL THE DIRECTORS OF OUR BANK. THE BANK HAS MADE ARRANGEMENTS FOR THE FUNDS TO BE DECLARED “UNCLAIMED” AND IF NO CLAIM COMES IN SOON, THE BANK WILL DONATE THE FUNDS TO THE ARMS & AMMUNITION TRUST FUNDS AND IT IS FEARED THAT THIS MAY TRIGGER A WAR IN AFRICA AND THE WORLD IN GENERAL.

IN OTHER TO AVOID THIS NEGATIVE CONSEQUENCE SOME OF MY TRUSTWORTHY COLLEAGUES AND I NOW REQUEST YOUR PERMISSION TO HAVE YOU STAND AS THE NEXT OF FAMILY CONNECTION TO THE LATE BENINGGR JOHN DUKE (SNR) SO THAT THE MONEY WILL BE MADE FREE TO BE PAID INTO YOUR BANK ACCOUNT AS THE RECEIVER AS THE KIN, ALL DOCUMENT AND PROOFS TO ENABLE YOU GET THIS FUNDS WILL BE CAREFULLY HANDLED. OUR BANK MAKES IT MANDATORY FOR US TO OFFICIALY DECLARE THE RECIPIENT OF THIS LARGE FUND AT THE EARLIEST POSSIBLE. THAT IS THE REASON YOU ARE SEEING THIS MAIL. WE ASSURE YOU THAT YOU THAT THERE IS NO RISK INVOLVED IN THIS.

AS SOON AS YOU SEND ACKNOWLEDGEMENT TO CONFIRM THE RECEIPT OF THIS NOTE AND IN ACCEPTANCE OF THIS JOINT BUSINESS PROPOSAL WE SHALL INFORM YOU ABOUT THE MODALITIES INVOLVED AND PAYMENT RATIO TO SUIT BOTH PARTIES WITH FULL CLARITY.

IF YOU ACCEPT THIS PROPOSAL DO NOT TAKE DUE ADVANTAGE OF THE TRUST PLACED IN YOU. KINDLY SEND YOUR REPLY IMMEDIATELY WITH THE E-MAIL ADDRESS PROVIDING US WITH YOUR MOST CONFIDENTIAL TELEPHONE; FAX NUMBER AND YOUR EXCLUSIVE BANK ACCOUNT PARTICULARS SO THAT WE CAN USE THIS INFORMATION TO APPLY FOR RELEASING THE FUNDS INTO YOUR ACCOUNT IN YOUR FAVOUR.

THANKS IN ADVANCE IN ANTICIPATION OF YOUR KIND CO-OPERATION

BEST REGARDS

MR MOHAMED ABBAS

This method of deceit has been in existence through regular postal mail for more than 20 years. Now it is even more rampant due to the advent of the Internet and (free) E-Mail. Recall that it is possible to create E-Mails from fake E-Mail accounts as explained in Chapter 2 (Box 2.7). Over the last few years, literally thousands of people have received countless E-Mails like the one above. With respect to the sample scam text mentioned above, read what follows.

The nature and exact text of the “preposition” varies from letter to letter, as well as the purported author. Even then, there are a number of features common to most (but not all) that instantly identify them as “419” scams/Nigerian scams:

1. Often, but not always, the scam mails are written with ALL CAPS, as shown in the example. The joke in circulation is that there must be an epidemic of keyboards with broken Caps Lock keys in Nigeria!
2. As in this example, the mail/message or letter is characterized with bad syntax, malapropisms and misspellings – not expected of a writer who claims to be in high ranks, for example, a bank manager or oil industry executive, etc. One should indeed find this suspicious given that Nigeria and several other West African nations have English as their official language.
3. Interestingly, in most instances of this scam, E-Mails seem to originate from an African country and/or individual, usually Nigeria although there have been examples of such scams allegedly from Senegal, Ivory Coast, Togo, Ghana, Liberia, Angola, Chad and South Africa as well. Asian and Eastern European countries too are not lagging!
4. Almost always the scam communication mentions about “large amounts of funds” – millions of Dollars and it also mentions about those funds being “trapped” or “frozen” for a variety of ostensible reasons: “double-invoiced oil,” and unclaimed accounts belonging to victims of African air disasters or other (alleged) deceased persons are among the most frequently seen versions.
5. They will typically make an offer to you, as the beneficiary, a hefty portion of these funds as a “commission” or “reward” – saying that all you have to do is to send them your bank account numbers. They will also cleverly indicate that the more such account information you send, the quicker your share of the “proceeds” will start coming into your account. The message will also indicate that your fast response will help them transfer and “release” the funds from the clutches of the inexperienced administrators, greedy bureaucrats, etc.
6. In most cases, they please you to act “immediately” giving some convincing reason or the other to make you swing into action. They often refer to some sort of “statute of limitations” or other legal constraint that is about to run out of time and they also say that they will send back the funds to the government or other entity that would undoubtedly use them for undesirable purposes.

In a way, this scam is similar to the advance-fee scam; there is one point in common – the targeted person is led to believe that he or she has a chance to attain something of very great personal value (financial reward, a romantic relationship, etc.) in return for a small up-front monetary outlay. If you ever receive one of these E-Mails and think that the “Nigerian Scam” has hit you, you should just ignore it and not take any action that the scam would be asking you to. Recall Example 25 in Section 11.2.25 – this is a real-life example of Nigerian scam rackets busted by Pune Police in October 2010.

### 11.7.20 Scam No. 20 – Craigslist Scams

“Craigslist” is the idea that was conceived by Craig Newmark and has become one of the most popular sites on the Internet. Craigslist started in 1995 at San Francisco – it is possibly the definitive site for confidential program. Posted here are advertisements for employment opportunities, personal ads, and advertisements for cars, sale of pets, home supplies and a large number of other options. The website is created for various communities. Today there are 450 cities and countries throughout the world where Craigslist offers sites. A worth over 10 million US dollars (US\$) is attached to Craigslist according to business experts.

Unfortunately, this online classifieds website has been plagued with scammers using advance-fee fraud and similar techniques, usually involving fake cheques, to con people of their money. If you are selling anything under \$1,000 on Craigslist or eBay that cannot be shipped, or if you are renting a room (remember the rental scam described earlier) you are at high risk of a fake cashier’s cheque scam on Craigslist. These scammers are in search of low priced auctions, low sales prices and rental services because they have printed out bogus cheques. Their objective is to send you the bogus cheque for more than your original price or original rent, and have you give them back the extra real cash.

Occasionally, there are fraudsters who contact an individual interested in buying or selling things on Craigslist – the fraudsters then try to pull off the exact same scam. Many of the Nigerian 419 scam features (see the previous illustrations) are used regularly on Craigslist. This includes persons conducting transactions from another country, sending bank cheques that look believable, sending money that is excess over what is owed, and requesting that money be sent back to the scammer through wire transfer.

Lately, there is another advance-fee technique that has been used on Craigslist. In this method, fraudster will contact for the sale of an item and will ask the seller to despatch the item to a location to another country. The seller then despatches the item and furnishes the tracking number. However, the scammer never pays! At times the scammer will use someone who is offering an accomodation for rent and will pose as someone migrating from another country. The fraudster will create a situation in which it looks like there is a dire need to have the accomodation in advance. The fraudster also asks if it is possible to get the occupancy with some deposit money paid. The deposit cheque sent by the fraudster will be a bogus cheque; however, the amount written on that cheque will be far more than the deposit amount asked for by the seller. When the cheque is received by the seller (the target victim), the fraudster will ask for the excess amount to be refunded. The fake cheque will bounce and the victim will lose the amount he/she “refunded” to the scammer!

There is a related con that takes place on the rental model, particularly in the UK – the scammer places an advertisement on a “classifieds” website such as Craigslist or Gumtree pretending to seek an accomodation on rent. The scammer mentions an incredible depiction using photographs borrowed from other advertisements or other websites. The victim gets in touch with the scammer to get a viewing. However, the scammer tells the victim that to do so, the victim must go to a Western Union outlet, must transfer money to a relative to cover the amount of the deposit and must also furnish a scanned copy of the receipt in support of the money transfer made. Supposedly, this is to confirm that the victim has enough money to cover the deposit

before they view the accommodation. The fraudster also tells the victim that he/she will get the money back after the viewing. In reality, however, the place offered for accommodation may or may not exist, and the receipt allows the scammer to have the funds with no viewing ever taking place.

Again, the scammer sends a rental application, or asks for some details that are typically mentioned on a rental application form, such as driver's license number, bank account information, Social Security Number or its equivalent, etc. Recall what was mentioned in Section 11.7.14 – “Rental Scams.” Below are some tips to note about a Craigslist scam mail:

1. When you do a posting on Craigslist you will get lots of E-Mails. You can spot a Craigslist scam because it has the poor wording in the E-Mail. Most of the Craigslist scams come from another country where English is not the native language. Many mails may just be the result cutting and pasting E-Mails together!
2. Craigslist scams typically have the long-wound, that is “verbose” text in the E-Mail. Typically scammers mention lots of unrelated details, that is, they mention things that have nothing to do with what they are dealing with (remember the style of writing seen in the examples for “Babysitting/Nanny Scam” E-Mails). Scammers typically write long rambling sentences about their so-called “family problem” to gain sympathy from their victims, or it could be verbose text about the urgency of getting the transaction done, or they may tell you in a long-wound way that they know you are a good person deep down. Most of the time, there is no need to go that far – the wordy text in the mail is the tale-tale sign of a Craigslist scam!
3. The next step to spot a Craigslist scam is characterized by the mention of “religion” and a huge amount of compliments or apologies for bothering you. Somehow they believe that if they say sorry with words sounding sincere or if they keep on mentioning about religion, they will either baffle you or will make you comfortable. Typical Craigslist scammers will use flowery language in their communication with lots of religious notations thrown in.
4. Another trademark and a good way to spot a Craigslist scam is the payment by cheque or money order. There is always some reason because of which they cannot meet you and send you a cheque. Another one is that they have already sent you the cheque and entered a wrong amount. Regardless of how this Craigslist scam appears, the outcome is the same, the cheque is not good!
5. If there is a mention in the mail about some offer to pay you for your problem, it is a way to guess that it is a Craigslist scam. The trick used by scammers is to make you feel that because they are bothering you so much, they offering you something to compensate for your trouble. Only problem is the cheque, money order or any other method they come up with is always bad and you will wind up losing your money.

### 11.7.21 Scam No. 21 – Pyramid Scheme Scams and Ponzi Scheme Scams

They can also be called as “pyramid scheme frauds.” The way fraudsters in this team operate is in the structure of a pyramid. A pyramid scheme is considered to be a non-sustainable business model – it involves making payment promises to participants mainly for getting other people into the scheme. Any real investment or sale of products/services to customers/consumers is not intended. Basically, pyramid schemes are a form of fraud. Many countries have banned pyramid structures. Although these kinds of schemes have been around for a very long time, some people have a view that multi-level marketing which has been legalized is nothing but a pyramid scheme.

A successful pyramid scheme uses a fake but seemingly believable business with an easy-to-understand yet advanced-sounding money-making method which is used for profit. The basic concept is that "Person A" makes only one payment. To start earning, Person A has to get in the chain like others who will also make one payment each. Person A gets paid out of receipts from those new recruits. This way, they go on to recruit others. As each new recruit makes a payment, Person A gets his share. As the "business" expands, he is promised increasingly greater benefits.

The concern is that "businesses" based on pyramid structure hardly involve actual sales of real products or services with an attached monetary value. To make themselves credible, fraudsters, operating pyramid chains, equip themselves well with fake referrals, testimonials and information. The problem is that there is no end benefit. The monetary benefits only travel "up the chain." Only the originator (referred to as the "pharaoh") and a very few at the top levels of the pyramid make huge amounts of money. The amounts become less and less down the pyramid structure. There is nothing for the individuals at the bottom of the pyramid – these are the people who joined into the pyramid structure, but were not able to get in more members.

A "Ponzi scheme" is a similar fraud. Charles Ponzi was not the actual mastermind in its inception. However, his operation amassed so much money that throughout the US it came to be known as the "Ponzi scheme." A Ponzi scheme is also a fraudulent investment operation. It pays returns to separate investors either paid from their own money or from the money paid by subsequent investigators. The payments are not made from actual profit made.

Basically, a Ponzi scheme is an operation with fraudulent investment. It is a procedure that pays profits to stakeholders from their own funds or money paid by later investors, rather than from any actual revenue made. The Ponzi scheme usually attracts new investors by offering higher returns as compared with other investments. The benefits are promised in the form of short-term returns that are either exceptionally high or unbelievably consistent. The continuity of the returns promised by a Ponzi scheme and its loud/aggressive promotion is what attracts people (who later turn out to be unfortunate victims!). Fraudsters involved with this scheme cleverly create a perception of ever-increasing flow of money to those who are targeted to be hooked in or already hooked in.

Example 25 in Section 11.2.25 shows how gullible people can be! Let us take this imaginary example. Suppose, an advertisement promises amazing returns on an investment – for example, 30% on a 45-day contract. Usually, the motive is usually to cheat ordinary people who do not have deep knowledge of finance or financial jargon. Verbal constructions that sound impressive but are actually meaningless will be used to impress potential investors: watch for words such as "high return investment," "make money in short time without investing," "opportunity for offshore investment," etc.

Initially, without any monetary benefit or objective, or prior information about the investment, only a few investors are attracted to be roped in - usually this is done only for small amounts. About a month later, the investor receives the original capital along with the 30% return. At this point, the investor will have more incentive to invest additional money. As "word-of-mouth" publicity starts growing, other investors would also like to cash the "opportunity" and they communicate their intentions to participate. This results in a snowballing effect based on the promise of returns that are too high to imagine. However, the "return" to the early investors is being paid out of the fund contributed by new entrants and not from the profits made.

One reason that makes Ponzi scheme work so well initially lies in the re-investment that happens initially. The first few investors, who actually get paid the huge returns, tend to reinvest their money in the scheme, in the hope of earning more. This way, the fraudsters who are running the scheme do not actually need to pay far too much net amount. All they need to do is send financial statements to investors to show them the amount earned by keeping the money. In this manner, fraudsters are able to maintain the perception that the scheme is successfully operating with high returns and they continue the deception.

## FURTHER READING

### Additional Useful Web References

1. For readers who are not savvy with cybersecurity terms and/or for readers who have not been to previous chapters of this book, can visit: <http://www.utexas.edu/its/glossary/secure> (13 July 2010).
2. Visit the following URL to understand the difference between a “security professional” and a “hacker”: <http://elamb.org/hacker-vs-security-professional/>
3. An informative document on “*International Financial Scams – Internet Dating, Inheritance, Work Permits, Overpayment, and Money-Laundering*” can be found at: [http://travel.state.gov/pdf/international\\_financial\\_scams\\_brochure.pdf](http://travel.state.gov/pdf/international_financial_scams_brochure.pdf) (6 July 2010).
4. In reference to Example 1 in Section 11.2.1 (*Official Website of Maharashtra Government Hacked*), visit: <http://tech2.in.com/india/news/websites/maharashtra-government-website-hacked/16611/0> (3 June 2010).  
<http://www.thinkdigit.com/forum/technology-news/68555-hacked-maharashtra-government-website.html> (4 January 2011).  
[http://www.marathikatta.com/Infotech/Maharashtra\\_government\\_website\\_hacked/](http://www.marathikatta.com/Infotech/Maharashtra_government_website_hacked/)  
<http://www.thinkdigit.com/forum/technology-news/68555-hacked-maharashtra-government-website.html> (4 January 2011).  
[http://www.dnaindia.com/mumbai/report\\_us-still-to-probe-2007-hacking-of-maharashtra-website\\_1378301](http://www.dnaindia.com/mumbai/report-us-still-to-probe-2007-hacking-of-maharashtra-website_1378301) (4 January 2011).  
<http://www.expressindia.com/latest-news/state-govt-website-hacked-into/218348/> (3 June 2010).
5. In reference to Example 21 in Section 11.2.21, there are following links about “professional hacking conferences”:  
<http://www.google.com/Top/Computers/Hacking/Conventions/> (31 July 2010).  
<http://www.chicagocon.com/2009s/conference.html> (31 July 2010).  
[http://www.computerworld.com.au/article/43697/hacker\\_conferences\\_highlight\\_security\\_dangers/](http://www.computerworld.com.au/article/43697/hacker_conferences_highlight_security_dangers/) (31 July 2010).

Refer to website that claim to teach you how to hack like a Pro!:

<http://www.makeuseof.com/tag/top-5-websites-to-learn-how-to-hack-like-a-pro/> (3 August 2010).

To know more about the ethical hacker network, visit: [http://www.ethicalhacker.net/index.php?option=com\\_smf&Itemid=&topic=1277.msg4492](http://www.ethicalhacker.net/index.php?option=com_smf&Itemid=&topic=1277.msg4492) (3 August 2010).

6. The *Internet Theft Case* of retired Col. J.S. Bajwa was published by The Hindu; it can be accessed at: <http://www.hindu.com/2000/06/01/stories/0201000e.htm> (15 December 2009).
7. *The New York Times Company v. Sullivan Case* is described in the following links:  
<http://www.legalservicesindia.com/articles/defcy.htm> (10 December 2009).  
[http://en.wikipedia.org/wiki/New\\_York\\_Times\\_Co.\\_v.\\_Sullivan](http://en.wikipedia.org/wiki/New_York_Times_Co._v._Sullivan) (15 December 2009).
8. In reference to Mini-Case 6 in Section 11.3.6 – The Indian Case of Online Gambling, the following links can be visited regarding the “Hawala Transactions and Money Laundering”:  
<http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/hawala/default.asp> (1 August 2010).  
<http://www.howtovanish.com/2009/09/modern-hawala/> (1 August 2010)
9. In reference to Mini-Case 9 in Section 11.3.9 – Malicious Hacking Case – Organ Donation Database Deleted, you can refer to the following link:  
<http://www.scmagazineus.com/insider-threats/topic/90/> (1 August 2010).
10. With reference to Mini-Case 16 – *State of Tamil Nadu vs. Subas Katti*, readers can visit the following link:  
<http://indiacyberlab.in/cyberlaws/cyber-crime-conviction.htm> (14 June 2010).
11. The *Movie Piracy example* has been reported in the following link:  
[www.usdoj.gov/usao/cac](http://www.usdoj.gov/usao/cac) (1 December 2009).

12. *The Job Racket exposed case* (mentioned in Example 7) is reported by the Indian Express and is posted at:  
<http://www.indianexpress.com/story-print/548207/> (16 December 2009).
13. A press release on *Man Sentenced in Computer Fraud Offense* may be found on the website of the US Attorney's Office for the Southern District of Florida at: <http://www.usdoj.gov/usao/fls> (17 December 2010).
14. The source for the *FBI Case for Website Attack* is:  
<http://www.cybercrime.gov> (17 December 2010).
15. The source for *Chinese Trade Secret Stealing case* is: <http://www.usdoj.gov/usao/nj/press/index.html> (20 December 2010).
16. For the infamous "*Heartland Payment Systems Fraud*," more information can be found by accessing the documents in the following links:  
The following link explained how the fraud took place: <http://www.presidiobank.com/home/fiFiles/static/documents/HeartlandPaymentSystemsInformation.pdf> (7 March 2010).  
The following link describes the decision taken by the US District Court District of New Jersey: [http://www.huntonfiles.com/files/webupload/PrivacyLaw\\_Heartland\\_Decision.pdf](http://www.huntonfiles.com/files/webupload/PrivacyLaw_Heartland_Decision.pdf) (7 March 2010).
17. Read article *BCBS Data Breach about Patients' confidential information stolen* at:  
<http://www.healthleadersmedia.com/content/TEC-244935/Security-Breach-Puts-500000-BlueCross-Members-Data-at-Risk> (8 March 2010). This should be understood in the context of the HIPAA's Privacy Rule.
18. The article *ICICI Bank case of Compensation to the NRI Customer, due to Phishing Attack* can be accessed at:  
<http://economictimes.indiatimes.com/news/news-by-industry/banking/finance/banking/ICICI-Bank-told-to-pay-Rs-13-lakh-to-NRI-customer/articleshow/5798944.cms> (15 April 2010).
19. *MySpace Suicide Case* is reported at: <http://www.nytimes.com/2008/11/27/us/27myspace.html?r=1&ref=todayspaper> (22 January 2010).
20. In reference to Example 19 in Section 11.2.19 – *Game Source Code Stolen!*, you can visit the following links:  
<http://www.gameguru.in/pc/2007/30/lineage-iii-software-code-stolen/> (22 June 2010).  
<http://www.1up.com/do/newsStory?cId=3159077> (30 June 2010).
21. In reference to fraud examples described in Example 19, visit the following links:  
*Microsoft Online Safety Tips* are available at: <http://www.microsoft.com/protect/fraud/phishing/feefraud.aspx> (19 May 2010). Here guidance to safeguard against scams promising money, gift and prize is provided.  
*Types of fraudulent acts* are described at: <http://en.wikipedia.org/wiki/Fraud> (19 May 2010).
22. One more link to FBI's crime-related reports and publications is: <http://www.fbi.gov/publications.htm> (1 July 2010).
23. In reference to Illustration 7 of Section 11.4.3 about Facebook Beacon, you can visit: [http://en.wikipedia.org/wiki/Facebook\\_features#News\\_Feed](http://en.wikipedia.org/wiki/Facebook_features#News_Feed) (10 July 2010).
24. In reference to Illustration 10 of Section 11.4.3, you can refer to the following links:  
<http://economictimes.indiatimes.com/infotech/internet/Profiles-of-100-mn-Facebook-users-leaked-online/articleshow/6231385.cms> (3 August 2010).  
[http://publication.samachar.com/pub\\_article.php?id=9725948&nextids=9727901|9726856|9725948|9715404|9725947&nextIndex=3](http://publication.samachar.com/pub_article.php?id=9725948&nextids=9727901|9726856|9725948|9715404|9725947&nextIndex=3) (3 August 2010). There is a small video clip also in this link.  
<http://www.bharatchronicle.com/profiles-of-100m-facebook-users-leaked-online-7901> (3 August 2010).  
<http://www.efytimes.com/e1/fullnews.asp?edid=48927> (3 August 2010).  
<http://www.timesnow.tv/Data-of-100-mn-Facebook-users-leaked/articleshow/4350626.cms> (3 August 2010).  
<http://ciol.com/News/News/News-Reports/Facebook-CEO-faces-death-sentence-in-Pakistan/137854/0/> (3 August 2010). Here is the story about Facebook CEO faces death sentence in Pakistan
25. In reference to Digital Forensics Case Illustration 2 – Analysis of Seized Floppy – the Drug Peddler Case in Section 11.6.2, readers

- can refer to the following link to learn about autopsy forensics browser:  
<http://www.sleuthkit.org/autopsy/> (13 July 2010).
26. To know more about the banking fraud cases, you can visit the following sites:  
 For the case involving “Renukanth Subramaniam,” visit the following links:  
<http://www.darknet.org.uk/tag/renukanth-subramaniam/> (12 May 2010).  
<http://en.wikipedia.org/wiki/DarkMarket> (12 May 2010).  
<http://www.192business.com/page/12657/dark-market-mastermind-fraudster-jailed> (12 May 2010).  
[http://article.wn.com/view/2009/10/13/Losing\\_your\\_identity/](http://article.wn.com/view/2009/10/13/Losing_your_identity/) (12 May 2010).  
<http://www.hackinthebox.org/index.php?name=News&file=article&sid=34664> (2010).
27. In reference to the example about killers taking tips from Voice over Internet Protocol, readers can visit the following link:  
<http://www.dnaindia.com/dnaprint910.php?newsid=1382834> (12 May 2010).
28. The second case on banking fraud about victim Umashankar Sivasubramaniam was posted in Economic Times News and can be accessed at:  
<http://economictimes.indiatimes.com/news/news-by-industry/banking/finance/banking/ICICI-Bank-told-to-pay-Rs-13-lakh-to-NRI-customer/articleshow/5798944.cms> (15 April 2010).
29. More about the article *Online Credit Card Theft Ring* can be read in the following links:  
<http://www.docstoc.com/docs/9232256/Iceman-Founder-of-Online-Credit-Card-Theft-Ring-Pleads-Guilty-to-Wire-Fraud-Charges> (12 May 2010).  
<http://www.keylogger.org/news-world/iceman-pleads-guilty-to-massive-computer-hacking-5898.html> (12 May 2010).  
<http://abcnews.go.com/Business/story?id=3641177&page=1> (12 May 2010).  
<http://www.databreaches.net/?p=5817> (12 May 2010).  
<http://www.computerworlduk.com/management/security/cybercrime/news/index.cfm?newsid=15494> (12 May 2010).
30. For CAN-SPAM Act, refer to the following links:  
<http://www.fcc.gov/cgb/consumerfacts/canspam.html> (10 May 2010).  
<http://www.ftc.gov/spam/> (10 May 2010).  
 To know more about CAN-SPAM Tool Kit, visit:  
<http://www.can-spam-act.com/> (10 May 2010).  
 To know more about how to comply with CAN-SPAM Act of 2003, visit: [http://www.wilsonweb.com/wmt9/canspam\\_comply.htm](http://www.wilsonweb.com/wmt9/canspam_comply.htm) (10 May 2010).  
<http://www.spamlaws.com/federal/108s877.shtml> (10 May 2010).  
 Read article *The CAN-SPAM Act: A Compliance Guide for Business* at: <http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm> (10 May 2010).  
<http://www.newvistainc.com/2009/11/the-can-spam-act-a-compliance-guide-for-business/> (10 May 2010).
31. In reference to protection of credit card and the confidential information stored on those cards' magnetic strip, the article *How to Create and Generate Valid Credit Card Numbers* is available at: <http://www.moneybluebook.com/how-to-create-and-generate-valid-credit-card-numbers/> (13 May 2010).
32. Read the article *How Does the Hacker Economy Works* at:  
<http://hubpages.com/hub/hackerworld> (15 May 2010).
33. Read about the article *Stolen Data's Black Market* by visiting: <http://www.darkreading.com/security/encryption/showArticle.jhtml?articleID=208804033> (16 May 2010).
34. Credit card “skimming” related links are important to get yourself educated on how frauds happen and how to protect yourself. Read the article *Credit card Skimming Survey: What's your Magstripe Worth?* at: [http://www.wired.com/threatlevel/2009/10/florida\\_skimming/](http://www.wired.com/threatlevel/2009/10/florida_skimming/) (13 May 2010).
35. For the security of credit cards, there is a worldwide recognized PCI-DSS standard (Payment Card Industry – Data Security Standard) mentioned in the following links:  
<https://www.pcisecuritystandards.org/> (12 May 2010). This is the Home Page of the PCI Security Council.

[http://en.wikipedia.org/wiki/Payment\\_Card\\_Industry\\_Data\\_Security\\_Standard](http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard) (13 May 2010). Here you will find the Wikipedia note on the PCI-DSS standard.

PCI-DSS frequently asked questions (FAQs) and myths are available at: <http://www.pcicomplianceguide.org/pcifaqs.php> (16 May 2010).

PCI-DSS Sample Policy can be visited at:

<http://www.pcidssguru.com/pci-dss/a-sample-policy-for-pci-dss/> (12 May 2010).

Quick Reference Guide to the PCI-DSS Compliance is available at: [http://www.pcifree.com/pdf/pci\\_ssc\\_quick\\_guide.pdf](http://www.pcifree.com/pdf/pci_ssc_quick_guide.pdf) (14 May 2010).

Following URL summarizes the changes from PCI-DSS Standard version 1.1 to version 1.2 [https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_summary\\_of\\_changes\\_v1-2.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_summary_of_changes_v1-2.pdf) (10 May 2010).

A bird's eye view of the PCI-DSS version 1.2 is available at:

[http://www.secureconsulting.net/2009/02/pci\\_dss\\_v12\\_in\\_a\\_nutshell.html](http://www.secureconsulting.net/2009/02/pci_dss_v12_in_a_nutshell.html) (10 May 2010).

Read how to survive a PCI-DSS audit at:

<http://www.businessrecords.com/files/1st%20quarter%202009%20digital%20media.pdf> (12 May 2010).

The following link provides excellent information relating important aspects of credit cards: What type of credit cards to look for, credit card tips, benefits and drawbacks of credit cards, protecting yourself from credit card frauds, etc.

<http://www.equityfoundation.com/creditcards/index-creditcards.htm> (11 May 2010).

36. The *Card Security Code* (CSC), also known as *Card Verification Data* (CVD), *Card Verification Value* (CVV or CV2), *Card Verification Value Code* (CVVC), *Card Verification Code* (CVC), *Verification Code* (V-Code or V Code), or *Card Code Verification* (CCV), is an important aspect for protecting your credit card from fraud. Visit the following links to understand this important aspect.

[http://en.wikipedia.org/wiki/Card\\_Security\\_Code](http://en.wikipedia.org/wiki/Card_Security_Code) (16 May 2010). In this URL card security code concept is explained.

<http://sawaal.ibibo.com/computers-and-technology/what-cvv-number-credit-card-902703.html> (4 January 2011). Examples of CVV, etc. and security code are provided here.

<http://www.celtnet.org.uk/ns/credit-card-ccv.html> (16 May 2010). Credit card CCV number is explained here.

The site mentioned below is about Credit card Do's and Dont's – it has useful information about credit card safety.

[http://www.hdfcbank.com/personal/cards/cc\\_usage\\_dd.htm](http://www.hdfcbank.com/personal/cards/cc_usage_dd.htm) (4 January 2011)

37. To understand the *Scheme for Bank Card Numbering* (with regard to Illustration no. 3 under Credit Card Frauds), refer to: [http://en.wikipedia.org/wiki/Credit\\_card\\_numbers](http://en.wikipedia.org/wiki/Credit_card_numbers) (28 June 2010).
38. For a reading on common credit card frauds, visit: [http://en.wikipedia.org/wiki/Credit\\_card\\_fraud#Carding](http://en.wikipedia.org/wiki/Credit_card_fraud#Carding) (28 June 2010).
39. A wikipedia note on identity theft is available at: [http://en.wikipedia.org/wiki/Identity\\_theft](http://en.wikipedia.org/wiki/Identity_theft) (21 June 2010).
40. The ShadowCrew Board list is available in the following link (this is reference to Illustration 3): <http://web.archive.org/web/20040701194509/http://shadowcrew.com/phpBB2/> (27 June 2010).
41. Read about *Global Trail of an Online Crime Ring* by visiting the link at: [http://www.nytimes.com/2008/08/12/technology/12theft.html?\\_r=1](http://www.nytimes.com/2008/08/12/technology/12theft.html?_r=1) (24 June 2010).
42. The RSA Online Fraud Report for August 2009, can be read at: [http://www.rsa.com/solutions/consumer\\_authentication/intelreport/FRARPT\\_DS\\_0809.pdf](http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_0809.pdf) (15 July 2010).
43. In reference to Digital Forensics Case Illustration 2 – Analysis of Seized Floppy – the Drug Peddler Case, to understand how the disk structure is visit: [http://en.wikipedia.org/wiki/Disk\\_sector](http://en.wikipedia.org/wiki/Disk_sector) (23 July 2010).
44. In the following link you will find a report about Forensics Analysis of a Compromised Intranet Server:  
[http://www.sans.org/reading\\_room/whitepapers/forensics/forensic-analysis-compromised-intranet-server\\_1652](http://www.sans.org/reading_room/whitepapers/forensics/forensic-analysis-compromised-intranet-server_1652) (20 June 2010).

45. Visit a useful link on the topic of Trademark Law, Copyright Act, etc. at:  
<http://www.asianlaws.org/library/cyber-laws/trademark-law-cyberspace.pdf> (16 May 2010). At this link, you will be able to access a document titled *Indian Trademark Law & Cyberspace*.
46. The Indian Copyright Act (1957) can be accessed at:  
<http://www.education.nic.in/CprAct.pdf> (18 May 2010).
47. In the following link, there is a document that provides *Comparison of the Indian Trademark Law with EU and US Laws*:  
[http://www.c11.com/files/INTA\\_IndianTMLawComparison.pdf](http://www.c11.com/files/INTA_IndianTMLawComparison.pdf) (19 May 2010).
48. Visit the following links to read about *Indian Trademark Law*:  
<http://www.hg.org/article.asp?id=4963> (19 May 2010).  
<http://www.hg.org/article.asp?id=5514> (19 May 2010).  
<http://www.universalteacher.com/trademark-law-india/> (19 May 2010).
49. To understand how a *written argument on behalf of the accused*, submitted in the court looks, readers (specially those who do not have a legal background) can take a look at one actual written argument available at:  
[http://www.ceac.in/suhaskatti\\_2.pdf](http://www.ceac.in/suhaskatti_2.pdf) (1 July 2010).
50. Read the DNA article *Make cyber systems secure, AK Antony tells armed forces top brass* at: <http://www.dnaindia.com/dnaprint910.php?newsid=1384102> (2 July 2010).
51. Read the DNA article *Govt should have 500 hackers on call* at:  
<http://www.dnaindia.com/dnaprint910.php?newsid=1372979> (2 July 2010).
52. Read the DNA article *Cyber crime: victims don't know whom to call* at:  
<http://www.dnaindia.com/dnaprint910.php?newsid=1387861> (3 July 2010).
53. According to Department of Telecommunications official, cyberthreat is a global issue; read about this at:  
<http://www.dnaindia.com/dnaprint910.php?newsid=1388357> (4 July 2010).
54. *Net security threats are really serious* – read this article at:  
<http://www.dnaindia.com/dnaprint910.php?newsid=1377191> (3 July 2010).
55. *FBI's Index of Cyber Crimes* with live links (from year 2003 to year 2010) is available at: <http://www.fbi.gov/page2/page2index/cyber.htm> (2 July 2010).
56. In reference to Advance Fee Fraud described in Section 11.7.17, the following links are worth visiting:  
A list of notable frauds: <http://en.wikipedia.org/wiki/Fraud> (3 July 2010).  
[http://en.wikipedia.org/wiki/Advance-fee\\_fraud](http://en.wikipedia.org/wiki/Advance-fee_fraud) (3 July 2010).
57. Federal Communications Commission (FCC) links are provided in the following link:  
For the FCC rules and regulations, visit: <http://www.fcc.gov/oet/info/rules/> (4 July 2010). This is in reference to Scam No. 17: The Advance Fee Fraud in Section 11.7.17.
58. FCC Home Page can be accessed at: <http://www.fcc.gov/> (4 July 2010).
59. Read about online frauds by visiting this RSA website at: [http://www.rsa.com/phishing\\_reports.aspx](http://www.rsa.com/phishing_reports.aspx) (16 July 2010).
60. To learn more about telecommunications relay service (TRS), visit: [http://en.wikipedia.org/wiki/IP\\_Relay](http://en.wikipedia.org/wiki/IP_Relay) (2 July 2010).
61. In reference to Scam No. 12: Bona Vacantia Scam in Section 11.7.12, visit: [http://en.wikipedia.org/wiki/Bona\\_vacantia](http://en.wikipedia.org/wiki/Bona_vacantia) (5 July 2010).
62. In reference to Rental Scams in Section 11.7.14, visit: <http://rentalscams.org/> (6 July 2010).
63. In reference to Attorney Debt Collection Scams in Section 11.7.15 and to learn more about how other attorneys around the country have been scammed on this, visit: <http://www.scamwarners.com/forum/viewtopic.php?t=1578> (7 July 2010).
64. In the following link, there is an article *A sucker for the African E-Mail scam*:  
<http://www.rediff.com/money/2002/dec/09dalal.htm> (10 July 2010).
65. Read about *Kansas Attorney General Warns of Debt Collection Scam* at: <http://www>

- [consumeraffairs.com/news04/2010/01/ks\\_debt\\_collection.html#ixzz0soHCcIIM](http://consumeraffairs.com/news04/2010/01/ks_debt_collection.html#ixzz0soHCcIIM) (10 July 2010).
66. Debt Collection FAQs can be accessed at: <http://www.consumerfraudreporting.org/debtcollection.php> (11 July 2010).
67. In reference to *Malware Scams* in Section 11.7.16, the Anatomy of Malware Scams can be visited at: [http://www.theregister.co.uk/2008/08/22/anatomy\\_of\\_a\\_hack/print.html](http://www.theregister.co.uk/2008/08/22/anatomy_of_a_hack/print.html) (12 July 2010).
68. In reference to Nigerian Scam/419 Scam described in Section 11.7.19, visit: <http://www.snopes.com/fraud/advancefee/nigeria.asp> (6 July 2010).
69. In reference to Craigslist scam described in Section 11.7.17, the following links will provide you additional information:  
[http://askbobrankin.com/what\\_is\\_craigslist.html](http://askbobrankin.com/what_is_craigslist.html) (3 July 2010).  
<http://www.christianet.com/christianpenpals/whatiscraiglist.htm> (3 July 2010).  
<http://www.fraudguides.com/internet-craigslist-scams.asp> (3 July 2010).
70. A large list of *Computer Forensic Analysis Tools* can be visited at: <http://www.caine-live.net/page11/page11.html> (24 July 2010).
71. Regarding *Trade Mark Law in India*, you can visit the following links:  
<http://www.articlesbase.com/trademarks-articles/trademark-law-india-466481.html> (3 January 2011).  
<http://www.tm-india.com/trademark-laws/> (3 January 2011).
72. In reference to Illustration 2: Phishing Incidence in Section 11.4.1 visit the following link to read the story *ICICI Bank told to pay Rs 13 lakh to NRI customer*:  
<http://economictimes.indiatimes.com/news/news-by-industry/banking/finance/banking/icici-bank-told-to-pay-rs-13-lakh-to-nri-customer/articleshow/5798944.cms> (3 January 2011).

### Books

- Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and*

*Best Practices*, Chapter 38, Wiley India Ltd., New Delhi.

- Ibid – Refer to Chapter 13 cryptography, encryption and digital signatures.
- Ibid – Refer to Sections 19.5, 19.6 and 19.7 of Chapter 19 (Security of Electronic Mail Systems).
- Mehta, R. and Mehta, R. (2009) *Credit Cards: A Legal Guide with Special Reference to Credit Card Frauds*, Universal Law Publishing Co.

### Video Clips

- To get educated on credit card-related frauds and be alert, video clips can be seen at:  
<http://www.youtube.com/watch?v=FunpS4QXcRI> (14 May 2010). Here the topic is *World's Worst Credit Card?*  
<http://www.youtube.com/watch?v=6CehJarAIP&NR=1> (14 May 2010). Here the topic is *Credit Card PIRACY!*  
<http://www.youtube.com/watch?v=vmaj1KJIT3U&feature=related> (14 May 2010), Here the topic is *How to Hack RFID-enabled Credit Cards for \$8*  
<http://www.youtube.com/watch?v=V3pElQD8UZg&NR=1> (14 May 2010). Here the topic is *Fake a Credit Card*
- Credit card skimming video clips can be seen at:  
<http://www.youtube.com/watch?v=IEigmCRJ8FA> (14 May 2010).  
<http://www.youtube.com/watch?v=TE1p4ccm-2g&NR=1> (14 May 2010). This video mentions that the skimmer devices are legal and readily available. The video clip mentions that it is frustrating but not illegal in the US. It is said here that do not wait till your bank statement arrives at the end of the month because that gives plenty of opportunity to the fraudster to take forward his plan. It is better to check your bank statements online almost daily.

At the video clip available in the following link demonstrates how the waitress pretends to drop the credit card of customer and how the skimmer devise is used to get the magnetic card information copied – watch the clip at:

- <http://www.youtube.com/watch?v=Ns80IjFHyrg&NR=1> (14 May 2010).
3. ATM Frauds with Credit Cards – Video clips can be seen in the following links:  
To know more on ATM skimming, visit:  
[http://www.youtube.com/watch?v=m3qK46L2b\\_c&feature=related](http://www.youtube.com/watch?v=m3qK46L2b_c&feature=related) (13 May 2010).  
<http://www.youtube.com/watch?v=xQRcmUkcITQ> (13 May 2010).  
<http://www.youtube.com/watch?v=EkBRVWLcKIY&NR=1> (13 May 2010).
  4. Visit the following link about “Faking a Credit Card”  
<http://www.youtube.com/watch?v=V3pElQD8UZg> (accessed 3 January 2011)
  5. For useful tips to protect yourself from ATM thefts, refer to the following URL: <http://www.nigerianelitesforum.com/ng/business-and-money/619-atm-theft-protect-yourself-from-the-most-common-atm-scams.html> (30 October 2010).
  6. *European Payment Council's ATM Security Guidelines* can be downloaded from the following link:  
<http://www.atmia.com/newsletters/mar06/EPC%20DTR413%20ATM%20Security%20Guidelines.pdf> (24 April 2009).
  7. Demo of the New *Bluetooth ATM Skimmer* can be seen at: <http://www.youtube.com/watch?v=GxoqnCYIyf8&NR=1> (16 May 2010).
  8. In the following links, you can see some more video clips about ATM Frauds:  
To know more on ATM fraud – live skimming, visit:  
[http://www.youtube.com/verify\\_age?next\\_url=http%3A//www.youtube.com/watch%3Fv%3DQjvB2vmHj30](http://www.youtube.com/verify_age?next_url=http%3A//www.youtube.com/watch%3Fv%3DQjvB2vmHj30) (30 October 2010).  
To know more about Credit Card Skimming Operation – How a Waiter at a Restaurant does it, visit:  
[http://www.youtube.com/watch?v=U0w\\_ktMotlo](http://www.youtube.com/watch?v=U0w_ktMotlo) (30 October 2010).  
<http://www.youtube.com/watch?v=hx8gliXXbQA> (30 October 2010).  
To know more about fake credit card, visit:
  9. <http://www.youtube.com/watch?v=V3pElQD8UZg&NR=1&feature=fvwp> (30 October 2010).  
To know more about criminal modus operandi – ATM Scam – in non-English language, visit:  
<http://www.youtube.com/watch?v=YyArqeLSyBA> (30 October 2010).  
<http://www.youtube.com/watch?v=xQRcmUkcITQ> (30 October 2010).  
To know more about ATM fraud, visit: <http://www.youtube.com/watch?v=d9Y4WUk2ePw> (30 October 2010)  
To know more about Chip and PIN fraud, visit:  
<http://www.youtube.com/watch?v=X7pjUIxKoEc> (30 October 2010).  
To know more about ATM skimming, visit:  
[http://www.youtube.com/watch?v=m3qK46L2b\\_c](http://www.youtube.com/watch?v=m3qK46L2b_c) (30 October 2010).  
To know more about credit card hack, visit:  
<http://www.youtube.com/watch?v=yIXhsPrf2Yk> (30 October 2010).  
To know more about world's worst credit card, visit: <http://www.youtube.com/watch?v=FunpS4QXcRI&NR=1&feature=fvwp> (30 October 2010).  
To know more about nano skimmer instructions, visit:  
<http://www.youtube.com/watch?v=dMuTXBffao> (30 October 2010).  
<http://www.youtube.com/watch?v=Uu8J3UCcbd4&p=DC5BA9A2DEC3E437&playnext=1&index=11> (30 October 2010).  
To know more about credit card skimming devices on ATMs and gas pumps, visit:  
<http://www.youtube.com/watch?v=hojtvcC-STk> (30 October 2010). One more video clip on credit card skimming.  
To know more about new credit card scam, visit:  
<http://www.youtube.com/watch?v=bmKFHisu5og> (30 October 2010).  
<http://www.youtube.com/watch?v=63heiTqM4pg> (30 October 2010). This link is about ATM Scam, Check Your Machine before Putting Your Card in
  - The following links can be visited in reference to the digital signature-related crimes scenarios presented in Section 11.5:

Demo of *How Digital Signatures Work*, a video clip can be viewed at:

<http://www.arx.com/resources/digital-signature-applications-demo> (15 July 2010).

A Vido clip showing *Demo of Digitally signing a MicroSoft Word 2007* is available at:

<http://www.arx.com/flash/Digital-Signatures-Word2007> (24 July 2010).

In the following link you can view *Demo of digital signature for PDF* <http://www.arx.com/flash/Digital-Signatures-for-Adobe-Reader> (23 July 2010).

In the following link you can view *Demo of digital signature for Excel 2007* <http://www.arx.com/flash/Digital-Signatures-Excel2007> (23 July 2010).

10. There are more Demo Videos for digitally signing other types of documents (Word 2003,

Excel 2003, AutoCAD, Web Applications, IBM Lotus Forms, TIFF docs, Google docs, etc.). These all are available in the following CoSign Digital Signature site:

<http://www.arx.com/resources/digital-signature-applications-demo> (23 July 2010).

To know more about Digital Signature Guidelines Tutorial, visit: <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html> (25 July 2010).

To know more about *Digital Signature Guidelines*, visit: <http://www.abanet.org/scitech/ec/isc/dsg.pdf> (23 July 2010).

To know more about *VeriSign Guide to Digital Signatures*, visit: <http://www.verisign.com.au/repository/tutorial/digital/intro1.shtml> (23 July 2010).

---

The appendices that serve as extended material for the topic addressed in this chapter are: A–V. These are provided in the companion CD.

---