Appendix W

Chapterwise List of All References

Chapter 1: Introduction to Cybercrime

References

[1] *Information Security Glossary* can be visited at: http://www.yourwindow.to/information-security/gl_cybercrime.htm (14 March 2009).

[2] http://qanda.encyclopedia.com/question/cybernetics-related-84610.html (2 February 2009).

[3] http://www.pangaro.com/published/cyber-macmillan.html (26 February 2009).

[4] http://www.catunesco.upc.es/ads/beer.pdf (26 February 2009).

[5] http://www.gwu.edu/~asc/cyber_definition.html (26 February 2009).

[6] http://en.wikipedia.org/wiki/Cybernetics (20 February 2009).

[7] Site for *Information Technology Act 2000 Amendment* can be visited at: http://-cybercrime.planetindia.net/new–cyber-security–infrastructure.htm (14 March 2009).

[8] 2008 CSI Computer Crime and Security Survey can be assessed at: http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf (15 March 2009).

[9] Israeli Trojan Horse scandal can be visited at: http://www.msnbc.msn.com/id/8064757/ (18 March 2009).

[10] To understand the technical details involved inW32.Myfip.A, visit the technical document available at: http://www.symantec.com/avcenter/reference/when.malware.meets.rootkits.pdf (12 February 2009).

[11] Loza, B. http://www.safepatrolsolutions.com/papers/Crackers.pdf (1 February 2010).

[12] Find out more on Children's Online Privacy Protection Act (COPPA) in the following links:
COPPA FAQS – http://www.ftc.gov/privacy/coppafaqs.shtm (13 March 2009).
COPPA Compliance – http://www.coppa.org/comply.htm (13 March 2009).
The official COPPA website coming up soon, visit the site at: http://www.mccoppa.co.uk/home1/index.html (13 March 2009).
Another good site on COPPA – http://epic.org/privacy/kids/ (13 March 2009).

[13] To know about *Net-Nanny* and *Cybersitter*, visit the following links:
Net-Nanny
http://www.netnanny.com/competition (2 February 2010).
http://www.netnanny.com/ (2 February 2010).
http://internet-filter-review.toptenreviews.com/netnanny-review.html (2 February 2010).
http://personalweb.about.com/cs/viewingsites/a/403siteblocking.htm (2 February 2010).
Cybersitter
http://cexx.org/censware.htm (How to Disable Internet Filtering Programs) (5 February 2010).
http://www.yourwindow.to/information-security/gl_cybersitter.htm (5 February 2010).

[14] For *global software piracy scenario*, readers can refer the reports in the following links:
Fourth Annual BSA and IDC Global Software Piracy Study.
http://www.ifap.ru/library/book184.pdf (2 March 2009).
(Software) piracy. http://w3.bsa.org/globalstudy/ (10 February 2010).
2006 IDC Report on Software Piracy. http://www.adobe.com/de/aboutadobe/antipiracy/pdfs/IDC_Piracy_Study_REPORT.pdf (12 February 2009).

[15] To know more about Y2K viruses, visit: http://www.kumite.com/myths/opinion/thoughts/1999/y2kvirus.htm (2 February 2010).

[16] To know about *PCI DSS (Payment Card Industry Data Security Standard)*, visit the following links:
PCI DSS FQAs (frequently asked questions and myths).
http://www.pcicomplianceguide.org/pcifaqs.php (12 April 2009).
Visit this page for the standard. http://www.scribd.com/doc/6486863/PCI-DSS-v-12 (11 April 2009).
To understand the difference between the latest version of PCI-DSS and the older version, visit:
PCI DSS version 1.1 and 1.2 differences and updates.
http://www.pacifica.ru/download/pci_dss/pci_dss_summary_of_changes_v1-2.pdf (12 April 2009).
http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1326025,00.html (10 April 2009).

[17] http://economictimes.indiatimes.com/Internet_/Cyber_crimes_record_50_per_cent_jump_in_India /articleshow/3855662.cms (3 March 2009).

[18] Following links can be referred for the *UNCITRAL Model Law on Electronic Commerce*
http://www.genghinieassociati.it/acrobat/it%20security/Leggi/UNCITRAL%20Model%20Law%20on%20Electronic%20Commerce%20 (English).PDF (16 August 2009).
http//www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf (16 August 2009).
http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf (16 August 2009).
UNCITRAL-Model-Law-on-Electronic_Signatures-with-GuideToEnactment_2001 (16 August 2009).
http://www.jus.uio.no/lm/un.electronic.commerce.model.law.1996/ (16 August 2009).
http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html (16 August 2009).

[19] Schjølberg, S. and Hubbard, A.M. (2005) *Harmonizing National Legal Approaches on Cybercrime*, International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity, 28 June–1 July 2005, Geneva, Document: CYB/04 Dated 10 June 2005.
http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf (3 March 2009).

Further Reading

Additional Useful Web References

1. NASSCOM, Types of Cybercrimes, visit: http://www.indiacyberlab.in/cybercrimes/types.htm (22 February 2009).
2. SRI International for the US Department of Justice (1979) *The Criminal Justice Resource Manual on Computer Crime*, Menlo Park, CA, USA.
3. Ibid, p. 3.
4. Schjolberg, S. (1983) *Computers and Penal Legislation – A Study of the Legal Politics of a new Technology*, CompLex 3/86, Universitetsforlaget, Norway.
5. The Indian ITA 2000, http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN010239.pdf (22 February 2009).
6. NASSCOM, www.INDIACYBERLAB.in—http://www.indiacyberlab.in/news/190706.htm
7. India occupies the 3rd position in the world in terms of mobile phone usage, visit: http://www.expressindia.com/news/fullstory.php?newsid=61762 (28 January 2010).
8. For detailed *statistics on growth of cybercrimes* in India, visit: http://cybercrime.-planetindia.net/byteby_byte.htm (1 March 2009).
9. To understand the Indian Position on Cyber Defamation, visit: http://jurisonline.in/2009/11/cyber-defamation-%E2%80%93-position-in-india/ (29 January 2010).
10. Visit Law website at: http://www.findlaw.com/scripts/search.pl?CiRestriction=cyberterrorism
11. The Terrorism research center, http://www.terrorism.com/
As quoted at: http://terrorism.about.com/od/whatisterroris1/ss/DefineTerrorism_6.htm (25 March 2010), FBI definition "*Terrorism is the unlawful use of force or violence against persons or property*

to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." Department of State definition: "*The term '-terrorism' means premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents.*"

12. Martinez, S.M. FBI Report on *Trends and Developments in Cyber Crime in the Information Age*, http://www.adbi.org/files/2005.09.07.cpp.trends.cybercrime.presentation.pdf (27 March 2009).
13. Denning, D.E. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy* can be accessed at: http://www.nautilus.org/info-policy/workshop/papers/denning.html
14. Borland, J. *Analyzing the Threat Of Cyberterrorism*, TechWeb News, http://www.techweb.com/wire/story/TWB19980923S0016
15. Verton, D. *Are cyberterrorists for real?* Federal Computer Week, http://www.fcw.com/fcw/articles/2000/0626/pol-terror-06-26-00.asp
16. Hacked Sites Archive can be visited at: http://www.2600.com/hacked_pages/ (6 March 2009).
17. The following link shows how certain sites were hacked for a website hacked by a Turkish Hacker. http://www.youtube.com/watch?v=_2d Nz2TUhpk http://search.yahoo.com/search?p=examples+of+websites+hacked+by+hackers&ei=UTF-8&fr=msgr-buddy&xargs=0&pstart=1&b=11&xa=XOcfu0P0c_8YS_U8TQak_g–,1236412181
18. To know what *hacking software* is, visit: http://www.hackingalert.com/hacking-articles/free-hacking-program.php (6 March 2009).

    The entire *hacking panorama* is explained here – topics such as: *Computer Hacking*, *Basics of Hacking*, *Hacking Tutorial*, *History of Hacking*, *Hackers and Crackers*, *Catching a Hacker*, *Hacking Culture*, *Employee Internet Policy*
19. The Ponemon Institute (2009) Survey done on the *Business Risk of a Lost Laptop* (A Study of US IT Practitioners), visit: http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/The%20Business%20Risk%20of%20a%20Lost%20Laptop%20Final%201.pdf (1 February 2010).
20. To know about *Online Gambling* in India, visit the following links: http://answers.google.com/answers/threadview?id=294632 (1 February 2010). http://www.onlinecasinoreports.in/facts.php (1 February 2010). http://www.onlinecasinoreports.in/articles/ 2009/12/24/india-online-gambling-review-2009.php (1 February 2010).
21. For Tips on how to protect your child on the Internet, visit: http://www.indiacyberlab.in/cyberkids/index.html (13 March 2009).
22. The SC Magazine has published the story about NASA site attack by hackers through the use of SQL injection. To know more on this, visit: http://www.scmagazineus.com/nasa-sites-hacked-via-sql-injection/article/159181/ (1 February 2010).
23. To understand about *Cybercafes under ITA 2008* (ITA 2008 is the Indian IT Act 2000 amended), visit: http://www.naavi.org/cl_editorial_09/edit_jan07_itaa_analysis_7_cyber_cafe.htm (14 March 2009).
24. To understand views on whether the Amended ITA 2000 (ITA 2008) is stringent enough for cybercriminals, visit: http://cybercrime.planetindia.net/ita-08-more-stringent-00.htm (19 March 2009).
25. Information on *Cyber Crime Police Stations in Different States of India* (telephone numbers and E-Mail addresses of contact personnel) can be found in: http://infosecawareness.in/cyber-crime-cells-in-india/ (17 March 2009).
26. For Indian numbers on Internet connections, mobile phone usage, etc., visit: http://www.medianama.com/2008/10/223-quarterly-india-internet-mobile-numbers-and-a-wireless-internet/ (17 March 2009). http://www.watblog.com/statistics-internet-and-mobile/ (17 March 2009). http://internetthought.blogspot.com/2008/03/mobile-growth-in-india-is-something.html (17 March 2009).

    According to the article at the links just mentioned above, there is something different about the growth of mobile computing in India. Statistics on Indian Mobile Users' Internet Usage can be visited at the following link: http://trak.in/tags/business/2008/05/20/indian-top-10-mobile-sites/ (15 March 2009).

To know more about India's Internet Market Statistics (2001–2010), visit: http://www.reportbuyer.com/telecoms/broadband/india_internet_market_statistics_ 2001_2010.html (2 March 2009).

27. To find out another way of cybercrime classification, visit: http://www.b4usurf.org/index.php?page=types-of-cybercrime (21 March 2009).
28. For the full Defense *Paper on Information Warfare*, visit: http://cryptome.org/iwdmain.htm (12 April 2009).
29. Read article *Namesake Cybersquatting, An IPR Evil* at: http://www.legalserviceindia.com/articles/namesake.htm

Books

1. Godbole, N. (2009) Chapter 3 (Section 3.11), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India, New Delhi.
2. ibid, Appendix AI – Cybercrime and Information Security.
3. ibid, Chapters 1, 11, 14, 17, 29–31, 32, 35 and 38.
4. ibid, pp 64, 167, 260 (viruses and worms).
5. ibid Chapter 1 (Information Systems in Global Context) and Chapter 18 (Business Applications Security: An EAI Perspective) – for understanding the extended enterprise context for cyber crime and security.
6. Jain, N.C. (2008) *Cyber Crime*, 1st edn, Allahabad Law Agency, Faridabad.
7. Gregory, K. (2007) *Wireless Crime and Forensic Investigation*, Auerbach Publication, New York.
8. Bryant, R.P. (2008), *Investigating Digital Crime*, Wiley.
9. Denning, D.E. (1999) *Information Warfare and Security*, Addison-Wesley.
10. Bologna, G.J. and Shaw, P. (2000) *Avoiding Cyber Fraud in Small Businesses: What Auditors and Owners Need to Know*, Wiley.
11. Mehta, R. and Mehta R. *Credit Cards: A Legal Guide with Special Reference to Credit Card Frauds*, 2nd edn), Universal Law Publishing Company.

Articles and Research Papers

1. Read article *China Mounts Cyber Attacks on Indian Sites* at: http://timesofindia.indiatimes.com/india/China-mounts-cyber-attacks-on-Indian-sites/articleshow/3010288.cms (29 January 2010).
2. Read article *3,286 Indian Websites Hacked in Five Months* at: http://www.siliconindia.com/shownews/3286_Indian_websites_hacked_in_five_months-nid-63485.html (29 January 2010).
3. Read article *40-50 Indian Sites Hacked by Pak Cyber Criminals Monthly* at: http://archives.infotech.indiatimes.com/articleshow/35371176.cms (20 January 2010).
4. Read article *Pakistani Cyber criminals Deface 50 to 60 Indian Websites per day* at: http://www.webnewswire.com/node/480067 (15 January 2010).
5. A white paper on Click Frauds can be accessed in the following links:
   http://www.hitslink.com/whitepapers/clickfraud.pdf (24 March 2010).
   Additional links on the topic of "Click Fraud" can be visited at:
   http://www.marketingtilt.com.au/what-is-click-fraud/ (23 March 2010).
   http://en.wikipedia.org/wiki/Click%5Ffraud (24 March 2010).
   http://www.wisegeek.com/what-is-external-click-fraud.htm (24 March 2010).
   http://www.wisegeek.com/what-is-click-fraud.htm (24 March 2010).
   http://www.clickprotector.com/faq.asp (24 March 2010) (FAQ on detecting and stopping Click Frauds).
   http://help.yahoo.com/l/uk/yahoo/ysm/sps/faqs/accclickthru/click_fraud.html (24 March 2010).
   http://www.bukisa.com/articles/186305_what-is-advertising-click-fraud (24 March 2010).
6. A paper on *Anti-Spam Laws and their Effectiveness* can be accessed at: http://www-users.rwth-aachen.de/guido.schryen/publications/Schryen%20-%20Anti-spam%20legislation%20-%20ICTL.pdf (8 May 2010).

Chapter 2: Cyberoffenses: How Criminals Plan Them

References

[1] To know more on patriot hacking, visit: http://en.wikipedia.org/wiki/Patriot_hacking (25 June 2009).

[2] To know more on port scanner, visit: http://en.wikipedia.org/wiki/Port_scanner (10 February 2010).

[3] To know more on cyberstalking, visit: http://en.wikipedia.org/wiki/Cyberstalking (2 April 2009).

[4] To know more on cyberbullying, visit: http://en.wikipedia.org/wiki/Cyber-bullying (2 April 2009).

[5] To know more on cyberstalking, visit: http://cyberlaws.net/cyberindia/2CYBER27.htm (2 April 2009).

[6] To know more on cybercafe, visit: http://www.business-standard.com/india/news/cyber-cafe-audience-captive-power/351936/ (25 June 2009).

[7] To know more on cybercafe, visit: http://www.merinews.com/catFull.jsp?articleID=155371 (25 June 2009).

[8] To know more on cybercafe, visit: http://punekar.in/site/2009/02/04/city-cyber-cafes-install-deep-freeze-software-for-security/ (27 June 2009).

[9] To know more on cybercafe, visit: http://www.icicibank.com/pfsuser/temp/-cybersec.htm (27 June 2009).

[10] To know more on cybercafe, visit: http://www.icicibank.com/pfsuser/webnews/virtualkeyboad.htm (27 June 2009).

[11] To know more on Botnet, visit: http://en.wikipedia.org/wiki/Botnet (19 March 2009).

[12] To know more on Botnet, visit: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt132.shtm (30 March 2009).

[13] To know more on Botnet, visit: http://www.viruslist.com/en/analysis?pubid=204792068 (30 March 2009).

[14] To know more on attack vector, visit: http://searchsecurity.techtarget.com/-dictionary/definition/1005812/attack-vector.html# (17 July 2009).

[15] To know more on attack vector, visit: http://searchsecurity.techtarget.com/sDefinition /0,,sid14_gci214475,00.html (17 July 2009).

[16] To know more on attack vector, visit: http://www.net-security.org/article.php?id=949 (17 July 2009).

[17] To know more on zero-day attack, visit: http://en.wikipedia.org/wiki/Zero_day_attack (9 October 2009).

[18] To know more on attack vector, visit: http://cybercoyote.org/security/vectors.shtml (17 July 2009).

[19] To know more on cloud computing, visit: http://en.wikipedia.org/wiki/Cloud_-computing (9 October 2009).

[20] To know more on cloud computing, visit: http://communication.howstuffworks.com/cloud-computing2.htm (9 October 2009).

Further Reading

Books

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India, New Delhi.
2. Graves, K. (2007) *CEH – Official Certified Ethical Hacker Review Guide*, Wiley Publishing Inc., IN, USA.
3. Milhorn, H.T. (2007) *Cybercrime: How to Avoid Becoming a Victim*, Universal Publishers, USA.

Chapter 3: Cybercrime: Mobile and Wireless Devices

References

[1] Quocirca Insight Report (2009), *Addressing a Growing Problem: An Explosion of IP Addresses*, visit: http://www.quocirca.com (31 March 2010).

[2] Research In Motion Inc., *Research in Motion Annual Report*, 2009, visit: http://www.rim.com/investors/pdf/RIM09AR_FINAL.pdf (21 March 2006).

[3] To know more about mobile computing and types of mobile computing, visit: http://en.wikipedia.org/wiki/Mobile_computing (28 March 2010).

[4] To know more on *Mobile Security – Problem in Hand, Solution in Mind*, visit: http://www.it-analysis.com/blogs/Quocirca/2009/4/mobile_security_problem_in_hand_so_.html (31 March 2010).

[5] Quocirca Insight Report (2005), *Mobile Devices and Users*, visit: http://www.quocirca.com (15 May 2010).

[6] To know more about "3G Mobile Networks – Security Concerns," visit: http://fanaticmedia.com/infosecurity/archive/April09/3G%20Mobile%20Networks.htm (10 April 2010).

[7] To learn about credit card transactions using mobile cell phone, visit: https://www.frontlineprocessing.com/news/wireless-credit-card-processing/ (15 May 2010).

[8] To know how to avoid credit and charge card fraud, visit: http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre07.shtm (24 February 2010).

[9] CLEW Technology (*Closed-Loop Environment for Wireless*) comes from Alacrity, an Australian company who specifically created to deliver on the promise of mobile Internet. Alacrity's patented CLEW technology provides instant interactivity with their clients for time critical information. For further details, visit:http://www.alacritytech.com.au (15 May 2010).

[10] To know more about Types of Credit Card Fraud, visit: http://people.exeter.ac.uk/watupman/undergrad/owsylves/page3.html (22 May 2010). http://en.wikipedia.org/wiki/Credit_card_fraud (22 May 2010).

[11] For a news item *Microsoft Paves over Media Player Flaws*, visit: http://news.com.com/2100-1023-940050.html (19 May 2003).

[12] To know how to protect a mobile phone from being stolen, visit: http://www.wikihow.com/Protect-a-Mobile-Phone-from-Being-Stolen (20 February 2010).

[13] To know more about Mobile Phone Virus Hoax, visit:http://www.hoax-slayer.com/mobile-phone--virus-hoax.html (22 May 2010).

[14] To know more about Help protect against mobile viruses, visit: http://www.microsoft.com/uk/protect/computer/viruses/mobile.mspx (22 May 2010).

[15] To know more about Vishing, visit: http://en.wikipedia.org/wiki/Vishing (20 February 2010).

[16] To know more about how to protect from Vishing attacks, visit: http://news.cnet.com/8301-1035_3-10244200-94.html (18 February 2009).

[17] To know more about pretexting, visit: http://en.wikipedia.org/wiki/Social_engineering_(security) (18 February 2009).

[18] To know more about sexting, visit: http://en.wikipedia.org/wiki/Sexting (18 February 2009).

[19] To know more about VoIP spam, visit: http://en.wikipedia.org/wiki/VoIP_spam (18 February 2009).

[20] To know more about US Businesses Losing Millions from Illegal Interception of cell phone calls, visit: http://www.darkreading.com/insiderthreat/security/perimeter/showArticle.jhtml?articleID=223101287 (22 May 2010). http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100302006258&newsLang=en (22 May 2010).

[21] To know more about Laptop Security, visit: http://www.securitydocs.com/pdf/3399.PDF (22 May 2010)

Further Reading

Additional Useful Web References

1. Alexander, Z. (1997) *Is RAS Safe?*, WindowsITPro magazine – http://www.windowsitpro.com/article/networking/optimizing-nt-ras.aspx (15 May 2010).
2. To see interesting information in the article *Protecting your Laptop Computer*, visit: http://itso.iu.edu/Protecting_Your_Laptop_Computer (15 May 2010).
3. For *Windows Media Player Control Registry Settings*, visit: http://msdn.microsoft.com/en-us/library/ms909920.aspx (15 May 2010).
4. To study the projects done by the *Security Research Group*, visit: http://research.microsoft.com/en-us/groups/security/ (15 May 2010).
5. For another similar news item titled *Real Networks Warns of Media Player Security Flaws*, visit: http://www.networkworld.com/news/2004/0206realnwarns.html (15 May 2010).
6. For a very informative article on secure operation of the RAS system, visit: http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm/s/s4112.htm (15 May 2010).
7. For an interesting article titled *Butter-Fingered Mobile Device Users create IT Risk*, visit: http://www.networkworld.com/newsletters/wireless/2005/0214wireless2.html?fsrc=rss-wireless (15 May 2010).
8. For an eye opening article titled *Corporate Laptop Users put Businesses at Risk*, visit: http://www.pcw.co.uk/computing/news/2071216/corporate-laptop-users-put-businesses-risk (15 May 2010).
9. For radio frequency identification (RFID), visit: http://www.rfidjournal.com/faq (15 May 2010).
10. To read about PCMCIA cards, visit: http://support.3com.com/infodeli/inotes/techtran/4bba_5ea.htm (15 May 2010).
11. Jackson, W. (2005) *GCN Staff, Survey: Digital Gadgets take a Back Seat – and Stay there*, available at: http://gcn.com/articles/2005/01/24/survey-digital-gadgets-take-a-back-seatand-stay-there.aspx (15 May 2010).
12. Middleton, J. (2001) Lost Mobile Devices drive Security Fears, Web article from the VNU Network VNU Business Publications, available at: http://www.vnunet.com/articles/print/2115935 (15 May 2010).
13. For further technical details of the AES algorithm, visit Rijndael home page at: http://csrc.nist.gov/archive/aes/index.html (15 May 2010).
14. Shriraghavan, S., Sundaragopalan, S., Yang, F., and Jun, J. (2003) *Security in Mobile Computing – Focus on Wireless Security*, November 25, -available at: http://www.cc.gatech.edu/classes/AY2004/cs4235a_fall/presentations/NetSecPres. pdf (15 May 2010).
15. To learn about the RIM November 2006 report, visit: http://www.computing.co.uk/itweek/news/2169730/55-mobile-phones-left-london (15 May 2010).http://www.theregister.co.uk/ 2001/08/31/62_000_mobiles_lost/ (15 May 2010).
16. Strang, T. (2003) *Trends in Mobile Computing – From Mobile Phone to Context-Aware Service Platform*, German Aerospace Center (DLR), Oberpfaffenhofen, Germany, available at http://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt38/Bln_Release.pdf (15 May 2010).
17. For Windows advice on protecting sensitive information residing on mobile devices, *Windows Mobile-based Devices and Security: Protecting Sensitive Business Information*, available at: http://download.microsoft.com/download/4/7/c/47c9d8ec-94d4-472b-887d-4a9ccf194160/6.20WM_Security_Final_print.pdf#search='RAS%20Server%20Security%20for%20Mobile%20Devices' (15 May 2010).
18. To know scams that target you or your small business, visit: http://www.scamwatch.gov.au/content/index.phtml/itemId/693900 (20 February 2010).
19. To learn about mobile device security, visit: http://www.securelist.com/en/analysis?pubid=170773606 (15 May 2010).
20. To know about PCI-DSS Standard, visit: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (18 July 2010).
21. For PCI compliance guide, visit: http://www.pcicomplianceguide.org/ (18 July 2010).

Books

1. Mallick, M. (2003) *Mobile and Wireless Design Essentials*, Wiley DreamTech (India) Ltd., New Delhi, India.
2. Nanvati, S., Thieme, M., and Nanavati, R. (2002) *Biometrics*, 1st edn, Wiley DreamTech (India) Ltd., New Delhi, India.
3. Unhelkar, B. (2006) *Handbook of Research in Mobile Business: Technical, Methodological, and Social Perspectives*, IDEA Group, Hershey, PA, USA.
4. Siegemund, F. and Flörkemeier, C. (2003) *Interaction in Pervasive Computing Settings using Bluetooth-enabled Active Tags and Passive RFID Technology together with Mobile Phones*, Institute for Pervasive Computing, Department of Computer Science, ETH Zurich, Switzerland.

Articles and Research Papers

1. Godbole, N. (2003) *Mobile Computing: Security Issues in Hand-Held Devices*, Paper presented at NASONES 2003 National Seminar on Management and Business, 13–16 February 2006, Sydney, Australia. The paper is available in the following link: http://www.au-kbc.org/bpmain1/Security/EMO_SecurityWhitepaper.pdf#search='RAS%20Server%20Security%20for%20Mobile%20Devices' for Ericsson Mobile Organizer (EMO) Security Whitepaper (15 May 2010).
2. Sadlier, G. (October 2003), Mobile Computing Security, INS White Paper.
3. Godbole, N. and Unhelkar, B. (2006) *Security Issues in Mobile Computing*, Proceedings of the 2nd International Conference on Information Management and Business, February 13–16, 2006, Sydney, Australia.

Chapter 4: Tools and Methods Used in Cybercrime

References

[1] To know more about anonymizer, visit: http://en.wikipedia.org/wiki/Anonymizer (6 September 2009).
[2] To know more about Google cookie, visit: http://www.google-watch.org/bigbro.html (2 October 2009).
[3] To know more about DART cookie, visit: http://www.doubleclick.com/privacy/faq.aspx (2 October 2009).
[4] To know more on G-Zapper, visit: http://www.dummysoftware.com/gzapper.html (2 October 2009).
[5] To know more on Phishing, visit: http://computer.howstuffworks.com/phishing.htm (29 May 10).
[6] To know more about password, visit: http://en.wikipedia.org/wiki/Password_cracking (2 October 2009).
[7] To know more about MITM attacks, visit: http://en.wikipedia.org/wiki/Man-in-the-middle_attack (2 October 2009).
[8] To know more about strength of a password, visit: http://www.microsoft.com/protect/fraud/-passwords/checker.aspx (2 October 2009).
[9] To know more about keyloggers, visit: http://en.wikipedia.org/wiki/Keystroke_-logging (4 October 2009).
[10] To know more about software keyloggers, visit: http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci962518,00.html (4 October 2009).
[11] To know more about antikeylogger, visit: http://www.anti-keyloggers.com/products.html (4 October 2009).
[12] To know more about Spyware, visit: http://en.wikipedia.org/wiki/Spyware (5 October 2009).
[13] To know more about malware, visit: http://en.wikipedia.org/wiki/Malware (5 October 2009).
[14] To know more about Trojan Horses visit: http://en.wikipedia.org/wiki/Trojan_horse_(computing) (8 October 2009).

[15] To know more about rootkit, visit: http://en.wikipedia.org/wiki/Rootkit (8 October 2009).
[16] To know more about backdoor, visit: http://en.wikipedia.org/wiki/Backdoor_(computing) (8 October 2009).
[17] To know more about viruses, worms and Trojans, visit: http://en.wikipedia.org/wiki/Computer_virus (1 March 2010).
[18] To understand difference between computer virus and worm, visit: http://www.diffen.com/difference/Computer_Virus_vs_Computer_Worm (1 March 2010).
[19] To know types of viruses, visit: http://www.spamlaws.com/virus-types.html (1 March 2010).
[20] To know more on worm, visit: http://en.wikipedia.org/wiki/Computer_worm (1 March 2010).
[21] To understand various aspects of viruses, visit: http://www.kernelthread.com/publications/security/vunix.html (1 March 2010).
[22] To know more about Trojan Horse, visit: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213221,00.html (11 January 2010).
[23] To know more about threats by Trojan Horses, visit: http://www.techsupportalert.com/best-free-trojan-scanner-trojan-remover.htm (11 January 2010).
[24] To know more about backdoor, visit: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci962304,00.html (10 January 2010).
[25] To know more about what a backdoor does, visit: http://www.2-spyware.com/backdoors-removal (10 January 2010).
[26] To know more about SAP backdoors, visit: http://blog.c22.cc/2010/04/14/blackhat–europe-sap-backdoors-a-ghost-at-the-heart-of-your-business-4/ (29 May 2010).
[27] To know more about what is P2P network, visit: http://en.wikipedia.org/wiki/Peer-to-peer (29 May 2010).
[28] To understand different levels of P2P networks, visit: http://disco.ethz.ch/theses/ss05/freenet.pdf (29 May 2010).
[29] To know more about steganography, visit: http://en.wikipedia.org/wiki/Steganography (11 October 2009).
[30] Visit New York Times reports usage of steganography at: http://en.wikipedia.org/wiki/Steganography (11 October 2009).
[31] To know more about DoS: Teardrop attack, visit: http://en.wikipedia.org/wiki/Denial-of-service_attack (11 May 2010).
[32] To know more about DoS: Nuke attack, visit: http://wapedia.mobi/en/Denial_of_Service (11 May 2010).
[33] To know how to prevent DoS attacks, visit: http://www.cert.org/tech_tips/denial_of_service.html#4 (11 May 2010).
[34] To know more about SQL injection and Blind SQL injection attacks, visit: http://en.wikipedia.org/wiki/SQL_injection (11 May 2010).
[35] To know more about buffer overflow: NOOP, visit: http://en.wikipedia.org/wiki/Buffer_overflow (11 May 2010).
[36] Two know more about wireless network – frauds and misuses, visit: http://www.88450.com/redirect.php? tid=55751&goto=lastpost (11 May 2010).
[37] To know more about wardriving, visit: http://en.wikipedia.org/wiki/War_driving (11 May 2010).

Further Reading

Additional Useful Web References

1. To know how anonymizers work, visit: http://www.livinginternet.com/i/is_anon_work.htm (6 September 2009).
2. To know more about anonymizer FAQs, visit: http://www.anonymizer.com/company/about/anonymizer-faq.html (6 September 2009).
3. To understand a framework for classifying -denial-of-service attacks, visit: http://isi.edu/div7/publication_files/tr-569.pdf (30 May 2010).
4. To understand wireshark frequently asked questions, visit: http://www.wireshark.org/faq.html (30 May 2010).

5. To understand classification of DoS attack, visit: http://www.technospot.net/blogs/types-of-dos-attacks-and-introduction-to-ddos/ (30 May 2010).
6. To understand types of DoS attacks, visit: http://www-rp.lip6.fr/~blegrand/cours/MIAIF/secu1.pdf (30 May 2010).
http://www.topbits.com/denial-of-service-dos-attacks.html (30 May 2010).
7. To understand blind SQL injection, visit: http://www.net-security.org/dl/articles/Blind_SQLInjection.pdf (30 May 2010).
8. To know more about SQL injection protection, visit: http://www.owasp.org/images/7/7d/Advanced_Topics_on_SQL_Injection_Protection.ppt (30 May 2010).
9. To know how to protect from injection attacks in ASP.NET, visit: http://msdn.microsoft.com/en-us/library/ff647397.aspx (30 May 2010).
10. To know more about buffer overflow attacks and their countermeasures, visit: http://www.linuxjournal.com/article/6701?page=0,0 (30 May 2010).
11. To know more about article *Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade*, visit: http://www.ece.cmu.edu/~adrian/630-f04/readings/cowan-vulnerability.pdf (30 May 2010).
12. Stealing your neighbor's Net, visit: http://money.cnn.com/2005/08/08/technology/personaltech/internet_piracy/index.htm (30 May 2010).
13. Is "Stealing" Wireless Internet Illegal?, visit: http://journalism.nyu.edu/pubzone/wewantmedia/node/10 (30 May 2010).

Books

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India, New Delhi.
2. Kimberly, G. (2007) *CEH: Official Certified Ethical Hacker Review Guide*, Wiley Publishing, Inc., IN, USA.
3. Milhorn, H.T. (2007) *Cybercrime: How to Avoid Becoming a Victim*, Universal Publishers, USA.

Video Clips

1. To know more about *Demonstration of Scareware*, visit: http://www.youtube.com/watch?v=nRgkFt0NLsw (16 February 2010).
2. To know more about *Crime: The Real Internet Security Problem*, visit: http://www.youtube.com/watch?v=rZ1rkIy0dMM (16 February 2010).
3. To know more on how wardriving is conducted, visit: http://www.metacafe.com/watch/1708061/i_quit_movie_scene_24_stealing_internet_access/ (16 September 2009).

Chapter 5: Phishing and Identity Theft

References

[1] To know more about the world Phishing map, visit: http://www.avira.com/en/threats/section/worldphishing/top/7/index.html (25 July 2010).
[2] Phishing statistics into graphical illustrations can be visited at: http://www.m86security.com/labs/phishing_statistics.asp (25 July 2010).
[3] To monitor Phishing attacks daily, visit: http://www.phishtank.com/stats.php (25 July 2010).
[4] May 2009 Phishing Report complied by Symantec Security Response Anti-Fraud Team can be visited at: http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_phishing_report_05-2009.en-us.pdf (25 July 2010).
[5] Phishing Activity Trends Report of Q4-2009 published by APWG can be visited at: http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf (25 July 2010).
[6] To find definition of Phishing, visit: http://en.wikipedia.org/wiki/Phishing (9 September 2009).
[7] To find definition of Phishing, visit: http://www.webopedia.com/TERM/P/phishing.html (9 September 2009).

[8] To find definition of Phishing, visit: http://www.techweb.com/encyclopedia/defineterm.jhtml?term=phishing (9 September 2009).
[9] Visit Phishing attacks launched on most reputed and popular organizations' websites at: http://www.brighthub.com/computing/smbsecurity/articles/64477.aspx#ixzz0qFgacNDU (9 September 2009).
[10] To know tactics employed by the phisher, visit: http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx (9 September 2009).
[11] Ways to reduce the amount of Spam E-Mails we receive: http://en.wikipedia.org/wiki/E-Mail_spam (2 December 2009).
[12] To know more about hoax E-Mails, visit: http://en.wikipedia.org/wiki/Hoax (5 December 2009).
[13] To know methods of Phishing, visit: http://www.crime-research.org/articles/phishing-in-cyberspace-issues-and-solutions (9 September 2009).
[14] To know more about website Spoofing, visit: http://en.wikipedia.org/wiki/Website_spoofing (5 December 2009).
[15] To know more about cross-site scripting, visit: http://en.wikipedia.org/wiki/Cross-site_scripting (5 December 2009).
[16] To know more about cross-site request forgery, visit: http://en.wikipedia.org/wiki/Cross-site_request_forgery (5 December 2009).
[17] To know more about Phishing techniques, visit: http://www.brighthub.com/internet/security-privacy/articles/67339.aspx (26 July 2010).
[18] To know more about Phishing Net survey, visit: http://www.consumerreports.org/cro/magazine-archive/june-2009/electronics-computers/state-of-the-net/state-of-the-net-2009/state-of-the-net-2009.htm (26 July 2010).
[19] To know more about whaling, visit: http://netforbeginners.about.com/od/w/f/whatiswhaling.htm (18 June 2010).
[20] To know more about Phishing scams, visit: http://pcworld.about.com/od/emailsecurity/Types-of-Phishing-Attacks.htm (6 July 2010).
[21] To know more about Pharming, visit: http://en.wikipedia.org/wiki/Pharming (9 September 2009).
[22] To know more about Phoraging, visit: http://en.wikipedia.org/wiki/Phoraging (9 September 2009).
[23] To know definition of DNS hijacking, visit: http://en.wikipedia.org/wiki/DNS_hijacking (18 June 2010).
[24] To know definition of DNS hijacking, visit: http://www.pcmag.com/encyclopedia_term/0,2542,t=DNS+hijacking&i=41622,00.asp (18 June 2010).
[25] To know definition of Click Fraud, visit: http://en.wikipedia.org/wiki/Click_fraud (18 June 2010).
[26] To know definition of Click Fraud, visit: http://www.webopedia.com/TERM/c/click_fraud.html (18 June 2010).
[27] To know more about SSL certificate forging, visit: http://www.symantec.com/connect/blogs/phishing-toolkit-attacks-are-abusing-ssl-certificates (30 July 2010).
[28] To know more about search engine optimization (SEO), visit: http://en.wikipedia.org/wiki/Search_engine_optimization (26 July 2010).
[29] To know more about search engine optimization (SEO), visit: http://www.securityfocus.com/brief/701 (26 July 2010).
[30] To know more about techniques used for Black hat SEO attacks, visit: http://www.net-security.org/secworld.php?id=9084 (26 July 2010).
[31] To know more on Phishing kits – Xrenoder Trojan Spyware and Cpanel google, visit: http://www.anti-phishing.info/phishing-kit.html (30 July 2010).
[32] How to avoid to be victim of Phishing attack – http://articles.techrepublic.com.com/510010878_115818568.tml?tag=rbxccnbtr1 (2 December 2009).
[33] To know more on anti-Phishing plug-ins, visit: http://www.brighthub.com/computing/smb-security/articles/42784.aspx (8 June 2010).
[34] To know more about definition of identity theft, visit: http://en.wikipedia.org/wiki/Identity_theft (8 September 2009).

[35] To know more about identity theft statistics, visit: http://www.spendonlife.com/blog/2010-identity-theft-statistics (30 March 2010).
[36] To know more about identity theft statistics, visit: http://www.spendonlife.com/guide/2009-identity-theft-statistics (30 March 2010).
[37] To know uses of victim information, visit: http://www.spamlaws.com/id-theft-statistics.html (18 December 2009).
[38] To know more about ID theft statistics, visit: http://www.howstuffworks.com/identity-theft.htm (2 December 2009).
[39] To know myths and facts about identity theft, visit: http://www.networksecurityedge.com/content/ten-common-identity-theft-myths-dispelled (2 December 2009).
[40] The article *Identity Theft: The 'Business Bust-Out'* can be visited at: http://www.businessweek.com/smallbiz/content/jul2007/sb20070723_261131.htm?chan=smallbiz_smallbiz+index+page_top+stories (5 January 2010).
[41] To know more on business sensitive -information, visit: http://www.businessdictionary.com/definition/sensitive-information.html#ixzz13BzGtac2 (5 January 2010).
[42] To know more on business identity theft – countermeasures, visit: http://sbinfocanada.about.com/od/insurancelegalissues/a/identitytheft.htm (5 December 2009).
[43] To know more on medical ID theft, visit: http://www.webopedia.com/DidYouKnow/Internet/2009/medical_identity_theft.asp (9 June 2010).
[44] To know more on how to protect/eradicate your online identity, visit: http://www.net-security.org/article.php?id=1366 (5 January 2010).

Further Reading

Additional Useful Web References

1. To more about the article *Evolutionary Study of Phishing*, visit: http://www.cc.gatech.edu/projects/doi/Papers/DIrani_eCrime_2008.pdf (26 July 2010).
2. To know more about the article *Learning to Detect Phishing Emails*, visit: http://www2007.org/papers/paper550.pdf (26 July 2010).
3. To know more about the article *Detecting Phishing E-Mails by Heterogeneous Classification*, visit: http://digital.csic.es/bitstream/10261/21694/1/detecting.pdf (26 July 2010).
4. To know more about the article *What is Phishing?*, visit: http://antivirus.about.com/od/emailscams/ss/phishing.htm (6 July 2010).
5. To know more about tabnapping, visit: http://www.computerworld.com/s/article/9177326/Sneaky_browser_tabnapping_phishing_tactic_surfaces (9 July 2010).
6. To know more about tabnapping technique, visit: http://www.exploit-db.com/papers/13950/ (9 July 2009).
7. To know more about *Security Labs Report*, visit: (January–June 2010): http://www.m86security.com/documents/pdfs/security_labs/m86_security_labs_report_1H2010.pdf (26 July 2010).
8. To know more about the article *There is No Free Phish: An Aanalysis of "Free" and Live Phishing Kits*, visit: http://www.usenix.org/event/woot08/tech/full_papers/cova/cova_html/ (26 July 2010).
9. Visit DIY Phishing kits introducing new features at: http://www.zdnet.com/blog/security/diy-Phishing-kits-introducing-new-features/1104 (26 July 2010).
10. To know more about Phishing attacks and countermeasures, visit: http://www.cert-in.org.in/knowledgebase/whitepapers/ciwp-200-03.pdf (26 July 2010).
11. To know more on article *How Identity Theft Works*, visit: http://www.howstuffworks.com/identity-theft.htm (8 September 2009).
12. To know more on identity theft, visit: http://www.identitytheft.org/ (8 September 2009).
13. To know more on identity theft, visit: http://www.321identitytheftnews.com/ (8 September 2009).

14. To know about article *2009 Identity Theft Statistics*, visit: http://www.spendonlife.com/guide/2009-identity-theft-statistics (8 September 2009).
15. To know more on article *Your Growing Exposure for Identity Theft Risks*, visit: http://www.idtheft101.net/articles/wiley_rein_white_paper.pdf (26 July 2010).
16. To know about article *NCUA – Guidance on Identity Theft and Pretext Calling*, visit: http://www.ffiec.gov/ffiecinfobase/resources/info_sec/frb-sr-01-identity_theft_pretext_calling.pdf (26 July 2010).
17. To know about article *Privacy and Identity Theft Conference*, visit: http://blogs.technet.com/privacyimperative/archive/2008/12/23/privacy-identity-theft-conference.aspx (27 June 2010).
18. To know about article *Identity Theft and the Internet*, visit: http://www.student.cs.uwaterloo.ca/~cs492/papers/idTheft.pdf. (27 June 2010).
19. http://money.howstuffworks.com/identity-theft4.htm (Accessed on)
20. To know about article *CID, Mumbai: Phishing Case*, visit: http://www.cybercellmumbai.com/case-studies/case-of-fishing (27 June 2010).
21. To know more about identity theft, visit: http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf (27 June 2010).
22. To know more about identity theft, visit: http://www.nacrc.org/events/annualconfpresentations2005/idtheftnacojuly05.pdf (27 June 2010).
23. To know more about the article *Identity Theft – Case Studies*, visit: http://www.id-theft-info.com/Case-Studies.html (10 June 2010).

Books

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India, New Delhi.
2. Ibid Chapter 29 (*Privacy – Fundamental Concepts and Principles*), Chapter 30 (*Privacy – Business Challenges*), Chapter 31 (*Privacy – Technological Challenges*) and Chapter 32 (*Web Services and Privacy*).
3. Hayward, C.L. (2004) *Identity Theft*, Nova Science Publishers Inc., USA.
4. Milhorn, H.T. (2007) *Cybercrime: How to Avoid Becoming a Victim*, Universal Publishers, USA.

Articles and Research Papers

1. To read article *Who Is Fighting Phishing*, visit: http://www.markmonitor.com/download/wp/wp-fighting-phishing.pdf (8 June 2010).
2. To read article *MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You*, visit: http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf (8 June 2010).
3. Dr. Kamlesh Bajaj's scholarly paper *The Cybersecurity Agenda Mobilizing for International Action* is available at: http://www.dsci.in/sites/default/files/cybersecurity_-_mobilizing_for_international_action_0.pdf (28 October 2010). It was presented at the EastWest Institute.
4. Proceedings of "Hack.in 2009" – the 3rd Hacker's Workshop on Computer and Internet Security, organized by IIT Kanpur, can be downloaded at: http://www.security.iitk.ac.in/hack.in/2009/repository/proceedings_hack.in.pdf (28 October 2010).
5. To know more about article *Stopping Distributed Phishing Attacks* by Alex Tsow, Markus Jakobsson and Filippo Menczer, visit http://archive.nyu.edu/bitstream/2451/15020/2/Infosec+BOOK_Tsow+Jacobson.htm (10 October 2010).

Chapter 6: Cybercrime and Cybersecurity: The Legal Perspectives

References

[1] To understand the *Privacy Threats from Social Networking Sites*, readers should visit:

A good write up on Indian Laws for use of Social Networking Sites can be downloaded by visiting: http://www.indiasafe.com/image/PDF-sep-08/social-networking.pdf (12 July 2009).
A paper of Privacy and Social Networks is available at the link mentioned below http://www.w3.org/2008/09/msnws/papers/tilt.pdf (10 May 2009).
ENISA Guidance – Security Issues and Recommendations for Online Social Networks, is available at:
http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf (10 August 2009).
Another Paper on *Privacy Threats from Social Networking Sites* can be downloaded from http://www.digiwebbs.com/research_paper.pdf (14 April 2009).
Another site worth visiting about Privacy Issues in Social Networking site is http://privacyinsocialnetworksites.wordpress.com/ (3 September 2009).

[2] For the *Indian ITA 2000*, refer to the URL at:
http://www.legalserviceindia.com/cyber/itact.html (2 May 2009).

[3] http://www.naavi.org/importantlaws/itbill 2000/preamble.htm (29 December 2009).

[4] The European Union and the EU Member Countries can be visited at:
http://en.wikipedia.org/wiki/European_Union (20 July 2009).
http://en.wikipedia.org/wiki/European_Union_member_state (20 July 2009).
http://geography.about.com/od/lists/a/eumembers.htm (20 July 2009).
http://en.wikipedia.org/wiki/European_Union_Monitoring_Mission (20 July 2009)

[5] http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf (29 December 2009).

[6] To know more about the country-wise -position on data protection laws, visit:
http://www.guardianedge.com/resources/data-protection.php (20 July 2008).

[7] COPPA is Children's Online Privacy Protection Act – the FAQs are available at:
http://www.ftc.gov/privacy/coppafaqs.shtm (18 August 2009).

[8] A thematic paper (presented at Rio de Janeiro, Brazil on November 25–28, 2008) on *Child Pornography and Sexual Exploitation of Children Online* can be read at:
http://www.meldpunt-kinderporno.nl/files/Biblio/Thematic%20Paper_ICTPsy_ENG.pdf.

[9] For *Council of Europe's Convention on Cyber Crime*, visit:
http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (11 August 2009).
http://www.coe.int/t/dc/files/themes/cybercrime/default_EN.asp (11 August 2009).
Computer Crime & Intellectual Property Section, United States Department of Justice can be visited at:
http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm (11 August 2009).

[10] For Organization for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*, visit:
http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (20 August 2009).
http://www.oecdbookshop.org/oecd/display.asp?K=5LMQCR2JGG0T&DS=OECD-Guidelines-on-the-Protection-of-Privacy- and-Transborder-Flows-of-Personal-Data (20 August 2009).

[11] For the *Indian Penal Code* and its Amendment Bill, visit:
http://rajyasabha.nic.in/bills-ls-rs/2000/XXXVIII_2000.pdf (1 January 2010).
http://chddistrictcourts.gov.in/THE%20INDIAN%20PENAL%20CODE.pdf (5 January 2010).
http://www.netlawman.co.in/acts/indian–penal-code-1860.php (5 January 2010).

[12] Visit the following links for the *Indian Evidence Act at:*
http://chddistrictcourts.gov.in/THE%20INDIAN%20EVIDENCE%20ACT.pdf (29 December 2009).
http://www.indianrailways.gov.in/RPF/Files/law/BareActs/Evidenceact.doc (29 December 2009).
http://en.wikipedia.org/wiki/Indian_Evidence_Act (29 December 2009).

[13] For *Bankers' Books Evidence Act* of 1891, visit:
http://www.indianrailways.gov.in/RPF/files/law/BareActs/Bankbookact.doc (15 August 2009).
http://indiacode.nic.in/rspaging.asp?tfnm=189118 (15 August 2009).
http://www.vakilno1.com/bareacts/Laws/The-Bankers-Book-Evidence-Act-1891.htm (15 August 2009).

[14] Visit the following links for the *Reserve Bank of India Act* 1934 at:
http://www.helplinelaw.com/docs/THE%20RESERVE%20BANK%20OF%20INDIA%20ACT%201934 /CHAPTER%20V%20PENALTIES (1 August 2009).
http://en.wikipedia.org/wiki/Reserve_Bank_of_India (1 August 2009).

[15] The article about *National Netizen's Rights Commission* can be read at:
http://www.merinews.com/catFull.jsp? articleID=154783 (13 August 2009).
http://www.bloggernews.net/119210 (13 August 2009).

[16] Regarding the *Personal Data Protection Act of India*, visit:
http://www.legalserviceindia.com/article/ l37-Data-Protection-Law-in-India.html (11 August 2009).
http://www.legalserviceindia.com/article/l368-Data-Protection-Law-In-India.html (11 August 2009).
http://www.indlawnews.com/display.aspx?4530 (11 August 2009).

[17] Refer to the following link for an Interactive Map of *Data Security Breach Disclosure Laws in the United States* presented by Guardian Edge Technologies and powered by Google Maps:
http://www.guardianedge.com/resources/breach-disclosure.php (23 August 2009).

[18] For an explanation about "viruses" visit: http://cybercrime.planetindia.net/viruses.htm (22 August 2009).

Further Reading

Additional Useful Web References

1. For Cyber Crime Investigation Cell and contact E-Mail, visit:
http://www.cybercellmumbai.com/contact-us (9 August 2009).
2. For the list of cybercrime police station in different states in India, with the names of officers in charge, you can visit: http://www.naavi.org/cl_editorial_04/cyber_Crime_ps.htm (8 May 2009).
3. To know about a 720 pages book with comprehensive coverage on cyberlaws in India, readers can visit:
http://www.naavi.org/archives/archive_edit_feb_28_04.htm (12 July 2009).
4. The following link has very useful information about Internet censorship: law and policy around the world: http://www.efa.org.au/Issues/Censor/cens3.html (25 July 2009).
5. Internet Security and Computer Crime, A Guide to Selected Government Information, available at WIU's Government Publications Library, can be accessed at:
http://www.wiu.edu/library/govpubs/guides/internet.htm (1 June 2009).
6. Visit the following URL for *The Electronic Commerce Support Act* – 1998; it is an Act to amend various Central Acts to facilitate electronic commerce:
http://www.indianembassy.org/policy/Commerce/eCommerce/eCommerce_support_act_1998.htm (20 April 2009).
7. The following link is about Child Online Safety discussion at the Internet Governance Forum (IGF):
http://www.intgovforum.org/cms/index.php/component/chronocontact/?chronoformname=WSProposals2009View&wspid=288 (19 February 2010).
8. To understand digital signatures, visit:
http://asclonline.com/images/d/d4/Simple_Guide_to_Digital_Signatures.pdf (15 April 2009).
9. The following links can be visited for the *Indian IT Act 2000* at:
http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN010239.pdf
(22 February 2009).
http://vlex.in/vid/the-information-technology-act-29635830 (21 July 2009).
http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002090.pdf (17 December 2008).
http://www.itwire.com/index2.php? option=com_content&do_pdf=1&id=4957 (31 July 2008).
10. The following links can be visited to understand about the amendments to the Indian IT Act 2000 that were made toward the end of year 2008, that is, the ITA 2008.
http://www.cyberlaws.net/itamendments/index1.htm (21 July 2009).
http://www.alertindian.com/?q=node/23 (21 July 2009).
http://www.alertindian.com/?q=node/33 (21 July 2009).

11. For a good debate as to whether India needs a Data Protection Legislation, refer to the following URL: http://www.algindia.com/publication/article3200.pdf (21 July 2009).

12. Following are some good links on electronic commerce for those who are not familiar with E-Commerce (building blocks of E-Commerce are explained in this paper): http://www.cs.berkeley.edu/~tygar/papers/Building_blocks_atomicity_e-comm.pdf (12 May 2008). For understanding the basics of E-Commerce, visit: http://thestar.com.my/maritime/news/ 2000/2/27edi1.html (21 July 2009). http://www.nvcc.edu/home/kvu/eCommerce_a.pdf (21 July 2009). An E-Commerce online tutorial is available at: http://www.webdevelopersjournal.com/-columns/eCommerce1.html (15 March 2009). Internet Commerce basics are explained at: http://www.electronicmarkets.org/issues/-volume-8/volume-8-issue-1/internetcommercebasics0.pdf (10 September 2008).

13. For explanation of *digital signatures* in easy and non-technical language, the following site can be visited at: http://www.youdzone.com/signature.html (28 July 2009).

14. Visit the following URL to read the article *Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure*: http://www.schneier.com/paper-pki.html (3 August 2009).

15. To understand about *Use of S/MIME as a security measure for online communication*, visit: http://www.elock.com/S-MIME-article2.html (1 August 2009).

16. To understand about *Privacy-Enhanced Mail (PEM)*, visit: http://www.cs.umbc.edu/~wood cock/cmsc 482/proj1/pem.html (1 August 2009).

17. Visit the following excellent site on *Global Laws & Legislations* (on this site, you can get the links to the cybercrime laws in countries around the world): http://www.ccmostwanted.com/LL/global.htm (5 September 2009).

18. For *Comments of Naavi on the Amendments Proposed to ITA-2000 vide ITAA 2008*, refer to the following link: http://www.naavi.org/cl_editorial_08/edit_dec_28_itaa_analysis_ 5_overview.htm (13 August 2009).

19. Canadian Anti-Spam Laws – for full text of bill S-220, an Act respecting commercial electronic messages, visit: http://www2.parl.gc.ca/content/Senate/Bills/402/public/S-220/S-220_1/S-220_text-e.htm (19 August 2009).

20. For discussion bogs on Canada's proposed Anti-Spam Legislation (Bill S-220; previously S-202), visit: http://groups.google.ch/group/news.admin.net-abuse.email/browse_thread/thread/ e0759ea7928a14e2 (18 August 2009).

21. Also see the following link to read about Canada's fight against spammers: http:// www.spamfighter.com/News-11925-Canada-Prepares-to-Fight-against-Spammers-Anti-Spam-Bill-in-Senate.htm (15 August 2009).

22. Visit the important link for European Committee on Crime Problems (CDPC) Committee of Experts on Crime in Cyber-Space (PC-CY) Draft Convention on Cyber-crime (Draft No. 22 REV) at: http://www.cyber-rights.org/documents/coe22.htm (22 August 2009).

23. For the South African legislation on cybercrime and specifics of Spam specified in their ECT Act, refer to Section 2 on Pg 9 of the document that is available in the following link: http://www2.law.uu.nl/priv/AIDC/PDF%20files/IIIB2/IIIB2%20-%20South%20Africa.pdf (21 August 2009).

24. To read the story about Management Cyber-gang stealing £12.8m from South African Government, refer to the following link: http://www.computerweekly.com/Articles/2008/06/11/231018/cybergang-steals-12.8m-from-south-african-government.htm (11 July 2009).

25. To understand how Spam works, visit: http://computer.howstuffworks.com/spam.htm/printable (30 August 2009).

26. Another view on Spam is available at the following link: http://www.pgts.com.au/pgtsj/pgtsj0309a.html (12 August 2009).

27. To understand about the *Fight against Spam*, refer to the following link: http://www.open-mag.com/features/Vol_39/spam/spam.htm (23 August 2009).

28. A contrary view that Spam should not be legislated is available at: http://www.progoth.com/spam/termpaper.html (20 August 2009).

29. At the following links, there are articles about India's approach to fight against cybercrimes: http://www.goarticles.com/cgi-bin/showa.cgi?C=3128083 (19 August 2010).

Books

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Appendix AG in the CD explains WebTrust – Seal of Approval – the Criteria for Extended Validation Certificates, "EV Certificates"), Wiley India Pvt. Ltd., New Delhi.
2. Ibid, Chapters 29, 30, 31 and 32.
3. Ibid, Chapter 14 (Intrusion Detection for Securing the Networks).
4. Ibid, Chapter 29 (Privacy – Fundamental Concepts and Principles).
5. ibid, Chapter 13 (Cryptography and Encryption).
6. ibid, Chapter 27 (Laws and Legal Frameworks for Information Security).
7. ibid, Chapter 13 (Section 13.5 Digital Signatures – A Method for Information Security and Section 13.6 Cryptographic Algorithms).
8. Ibid, Chapter 38 (Ethical Issues and Intellectual Property Concerns for Information Security Professionals).
9. Broadhurst, R. and Grbosky, P. (2005) Cyber crime in India – the legal Approach, *Cyber-Crime: The Challenge in Asia*, Hong Kong University Press, Hong Kong.
10. Oberoi, S.. *E-Security and You*, Tata McGraw Hill, Delhi.
11. Kienan, B. (2000) *Small Business Solutions E-Comerrce*, Microsoft Press, USA.
12. Shurety, S. (2000) *e-business with Net.Commerce*, IBM Press.
13. Kosiur, D. (1997) *Understanding Electronic Commerce*, Microsoft Press, USA.
14. Laudon, K.C. and Traver, C.G. (2003), *E-commerce: Business, Technology, Society*, Pearson Education, Singapore.
15. Kalakota, R. and Whinston, A.B. (1999) *Frontiers of Electronic Commerce*, Pearson Education, New Delhi.
16. Amor, D. (2000) *The E-business (R) Evolution*, Pearson Education.
17. Shaw, M, Blanning, R. Strader, T., and Whinston, A. (2003), Handbook *of Electronic Commerce*, Springer, USA.
18. Broadhurst, R.G. and Grabosky, P.N. (2005) *Cyber-crime: the Callenge in Asia* Hong Kong University Press, Hong Kong.

Articles and Research Papers

1. *Computer Crime and Computer Fraud*, University of Maryland, Department of Criminology and Criminal Justice, Fall, 2004 can be accessed at: http://www.montgomerycountymd.gov /content/CJCC/pdf/computer_crime_study.pdf (1 January 2009).
2. A paper by *Crime Data Mining: An Overview and Case Studies* by Hsinchun Chen, Wingyan Chung, Yi Qin, Michael Chau, Jennifer Jie Xu, Gang Wang, Rong Zheng, Homa Atabakhsh from Artificial Intelligence Lab, Department of Management Information Systems, University of Arizona, Tucson, AZ 85721, USA can be read at: http://www.fbe.hku.hk/~mchau/papers/CrimeDataMining.pdf (1 July 2009).
3. For *CRS Report for Congress, Cybercrime: The Council of Europe Convention* by Kristin Archick, Specialist in European Affairs Foreign Affairs, Defense and Trade Division, refer to the following links: http://fpc.state.gov/documents/organization/58265.pdf (12 April 2008). http://fpc.state.gov/documents/organization/ 36076.pdf (12 April 2008).
4. For cybercrime outlook in the Middle East, visit: http://www.ask-pc.com/lessons/CYBERCRIME-MIDDLE-EAST.pdf (5 January 2009).
5. Refer to paper on *Cyber Insurance* by Rainer Böhme, Technische Universitt ä Dresden, Institute for System Architecture 01062 Dresden, Germany in the following link: http://infosecon.net/workshop/pdf/15.pdf (19 October 2008).
6. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions about *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*

is available at: http://www.usdoj.gov/criminal/cybercrime/intl/EUCommunication.0101.pdf (21 April 2009).

7. CRS Report for Congress about *Terrorist Capabilities for Cyberattack: Overview and Policy Issues* by John Rollins, Specialist in Terrorism and International Crime Foreign Affairs, Defense, and Trade Division and Clay Wilson, Specialist in Technology and National Security Foreign Affairs, Defense, and Trade Division (Updated January 22, 2007) is available at: http://www.fas.org/sgp/crs/terror/RL33123.pdf (3 July 2009).
8. A presentation based on the Proceedings of WSIS Thematic Meeting on Cyber security, about harmonizing National Legal Approaches on Cyber crime is available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf (3 March 2009).
9. For documents and links concerning digital evidence, visit: http://www.khodges.com/digitalphoto/offtopiclinks.htm (7 July 2009).
10. *The Threat of the Cybercrime Act 2001 to Australian IT Professionals*, a paper by Nelson Chan and Simon Coronel from Department of Computer Science and Software Engineering, The University of Melbourne and Yik Chiat Ong from Faculty of Law, The University of Melbourne. – The paper can be read at: http://www.cs.berkeley.edu/~benr/publications/auscc03/papers/-chan-auscc03.pdf (12 August 2010).
11. UNCITRAL stands for *U*nited *N*ation's *C*ommission on *I*nternet *Tra*de *L*aw. Uncitral Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998 United Nations. The UNCITRAL document (refer to Section 6.3) can be visited at: http://www.genghinieassociati.it/acrobat/it%20security/Leggi/UNCITRAL%20Model%20Law%20on%20Electronic%20Commerce% 20(English).PDF (16 August 2009).

Chapter 7: Understanding Computer Forensics

References

[1] Following are the links for COFEE:
- http://en.wikipedia.org/wiki/Computer_ Online_Forensic_Evidence_Extractor (6 November 2009).
- http://www.groundreport.com/Media_and_Tech/Microsoft-Makes-the-COFEE/2860183 (6 November 2009).
- http://www.postchronicle.com/cgi-in/artman/exec/view.cgi?archive=68&num=144908 (6 November 2009).
- http://www.wired.com/threatlevel/2008/04/microsoft-gives (6 November 2009).
- http://www.technovelgy.com/ct/Science-Fiction-News.asp?NewsNum=1616 (6 November 2009).
- http://www.ghacks.net/2008/04/29/computer-online-forensic-evidence-extractor/ (6 November 2009).

[2] Following are some useful links on *Access Data's FTK tool kit*:
- Access Data's Home Page: http://www.accessdata.com/ (21 December 2009).
- Access Data's products for various types of forensics investigations: http://www.accessdata.com/Products.html (21 December 2009).
- The forensics features of access data's toolkit: http://www.accessdata.com/forensictoolkit.html (21 December 2009).
- This is about FTK 2.0.2 to 2.1 Upgrade Instructions: http://ftk21.accessdata.com/Upgrade_from_2-02_to_2-1.pdf (21 December 2009).

[3] Useful links on *Guidance Software's EnCase* can be visited at:
- http://www.digitalintelligence.com/software/guidancesoftware/encase/ (21 December 2009). Following link is about news accolade on this tool:
- http://investors.guidancesoftware.com/-releasedetail.cfm?ReleaseID=416497 (22 December 2009).
  The SC Maganize has announced this tool to be one of the best; a report on that can be

seen at:

- http://www.scmagazineus.com/guidance–software-encase-forensic-v-6/review/159/ (18 December 2009).

To learn about Guidance Software's EnCase Portable, visit a video demo clip at:

- http://vimeo.com/5702414 (10 December 2009).

To know more about Guidance Software's EnCase® Portable having won Cygnus Law Enforcement Group Award in Forensics Category, visit:

- http://finance.yahoo.com/news/Guidance-Softwares-EnCase-bw-4161315896.html?x=0 (25 December 2009).

[4] Following are some useful links on "*File Carving*" that explains what is "file carving"

- http://www.fim.uni-linz.ac.at/Lva/IT_Recht_Computerforensik/File_carving.pdf (16 December 2009).

A good presentation on the *Advances and Challenges in File Carving* can be read at:

- http://www.korelogic.com/Resources/Projects/dfrws_challenge_2006/DFRWS_2006_File_ Carving_Challenge.pdf (3 April 2010). This is a highly technical presentation.

Visit following links that explains about "file carving":

- http://en.wikipedia.org/wiki/File_carving (16 December 2009).

A useful note on file carving can be read at:

- http://www.file-carving.com/ (22 December 2009).

Read about Foremost's File Carving/Data Carving Tool at:

- http://www.secguru.com/link/foremost_file_recovering_data_carving_tool (21 December 2009).
- To know about *Scalpel: A Frugal, High Performance File Carver*, refer to:
- http://www.digitalforensicssolutions.com/Scalpel/ (24 December 2009).

[5] To know more on *Sleuth Kit*, visit:

- http://en.wikipedia.org/wiki/The_Sleuth_Kit (23 December 2009).

An excellent technical document on the Sleuth Kit is worth reading at:

- http://www.markosworld.com/forensics/cmarko-tskintro.pdf (17 December 2009).

To know more about the Sleuth Kit Informer, visit:

- http://phoenix.calpoly.edu/~kvoelker/cis122/Webpage/current/sleuthkit-informer-2.html (25 December 2009).

The Sleuth Kit (TSK) demonstration can be accessed in a document at:

- http://www.denisfrati.it/pdf/TSK_v201_Demonstration.pdf (23 and 24 December 2009).

[6] For open-source forensics tools-related papers, visit:

- http://www.digital-evidence.org/papers/opensrc_legal.pdf (23 December 2009).
- http://www.opensourceforensics.org/ (2 April 2010)
- http://www.opensourceforensics.org/tools/index.html (30 March 2010).

[7] The Pune Newsline Article of 18 December 2009.

[8] Wireless network forensics resources are available at:

- http://en.wikipedia.org/wiki/Wireless_forensics (25 December 2009).

For a technical article on *802.11 Network Forensic Analysis*, visit the link at:

- http://www.sans.org/reading_room/whitepapers/wireless/802_11_network_forensic_analysis_33023 (1 January 2010).

Tools and techniques for network forensics are available at:

- http://airccse.org/journal/nsa/0409s 2.pdf (11 January 2010).

Network Forensics Solutions paper is available at:

- http://net-forensics.blogspot.com/ (11 January 2010). A compact article on *Network Forensics* can be found at:
- http://www.bitcricket.com/downloads/Network%20Forensics.pdf (11 January 2010).

[9] For STD (a Linux-based security tool), visit: http://s-t-d.org/ (14 January 2010). It is an STD 0.1 security tools distribution.

For Sleuth Kit, visit:

- http://www.sleuthkit.org/ (10 January 2010).

For Portable EnCase Tool, visit:

- http://www.guidancesoftware.com/encase–portable.htm? (10 January 2010).

[10] For *Hard Copy Imaging Techniques*, you can visit the following links:

To understand what Rimage Corporation does, visit:

- http://www.intellistor.co.za/Rimage.htm (12 January 2010)
- http://www.cdmediaworld.com/hardware/cdrom/news/0105/rimage_cd_protection.shtml (12 January 2010).

To know more on Voom Technologies HardCopy 3 Forensics Hard Drive Imager, visit:

- http://www.encoredataproducts.com/Voom-Technologies-HardCopy-III-1-2-Portable-Forensic-Hard-Drive-Duplicator-p-2146.html (10 January 2010).
- http://www.cds.com/Rapid-Image-7020CS-with-2-x-3-5-Drive-Caddies-p/fgr-0021-000b.htm (6 September 2010).

[11] See the paper *Benchmarking Hard Disk Duplication Performance in Forensic Applications* by Robert Botchek, at:

http://www.tableau.com/pdf/en/Tableau_Forensic_Disk_Perf.pdf (10 January 2010).

[12] To know more about the equipment called FastBloc, visit:

- http://www.encase.co.za/solutions/accessories/index.shtm (It shows the two varieties of FastBloc: one for field use and the other for laboratory use).

The Data Sheet for FastBloc is available at:

- http://www.forensics.ie/images/products/guidance_fastbloc_datasheet.pdf (11 January 2010).

For Guidance Software's FastBloc Field Edition Write-Blocking Device Forensically Validated by NIST, visit:

- http://investors.guidancesoftware.com/releasedetail.cfm?ReleaseID=252266 (11 January 2010).

The User Manual for Guidance Software FastBloc Field Edition is available at:

- http://www.agapeinc.in/FastBlocFEmanual RevC.pdf (18 Sept 2010).

[13] Refer to the following links with regard to Box 7.13:

- www.guillermito2.net/stegano/ideas.html (29 October 2009).
- www/guillermito2.net/stegano/jpegx/index.html (29 October 2009).
- http://www.guillermito2.net/index.html (29 October 2009).
- www.guillermito2.net/stegano/invisiblesecrets/index.html (29 October 2009).
- http://www.guillermito2.net/index.html (29 October 2009).
- www.securityfocus.com/tools/1434 (29 October 2009).
- www.guillermito2.net/stegano/imagehide/index.html (29 October 2009).

[14] Covert channel analysis discussion can be found at the following site:

- http://www.cs.rice.edu/~dwallach/courses/comp527_s99/covert-channels.pdf (6 September 2009).

[15] *Watermarking FAQs* are available at the following links:

- http://www.visualwatermark.com/-watermarking_faq.htm (1 November 2009).
- http://www.bluespike.com/technology/-giovanni/faq/ (1 November 2009).
- http://www.watermarkingworld.org/faq.html (1 November 2009).
- http://www.digitalwatermarkingalliance.org/faqs.asp (1 November 2009).
- http://dcl.ipc.kuas.edu.tw/digital_watermarking.htm (1 November 2009).

[16] The three approaches to hiding information are discussed in the paper *Steganalysis: A Steganography Intrusion Detection System* by Angela D. Orebaugh of George Mason University. The paper is available at the following link at:

http://www.securityknox.com/Steg_project.pdf (11 January 2010).

[17] Refer to the excellent 3Com Whitepaper *Under-standing IP Networking: Everything You Eve Wanted to Know* (Class A, Class B, Class C and Class D Networks, Subnetting, Classful IP Addressing etc. are all explained) in the following link:

- http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf (14 January 2010).

To understand TCP/IP addressing and Subnetting Basics, visit the link at:

- http://support.microsoft.com/kb/164015 (16 January 2010).

There is a video clip about A+ Certification: Understanding TCP/IP at the following link:

- http://www.youtube.com/watch?v=fr WeGyes6Ew (12 January 2010).
  Another good technical documentation on Introduction to TCP/IP protocol architecture can be found at the following link:
- http://cit.wta.swin.edu.au/cit/subjects/CITP0040/docs/tcpip.htm (9 January 2010).

[18] Following link lists the social networking sites:

- http://en.wikipedia.org/wiki/List_of_social_networking_websites (22 January 2010).

[19] The case described by Steinhauer. J. (2008) *Verdict in MySpace Suicide Case* is available at the following link:

- http://www.nytimes.com/2008/11/27/us/27myspace.html?ref=todayspaper (12 December 2009).

[20] For NIST Guidelines on Security Incident Response Handling, readers can visit the following links where these documents are available: The Special Publication 800-61 of NIST *Computer Security Incident Handling Guide* is available at:

- http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf (19 February 2010).
  The NIST Special Publication 800-86 *Guide to Integrating Forensic Techniques into Incident Response* is available at:
- http://www.cirosec.de/fileadmin/pdf/vero-effentlichungen/NIST_Booklet.pdf (27 February 2010).

[21] For *Write Blockers*, visit the following links at:

- http://www.forensicfocus.com/write-blocker-review-230709 (29 January 2010).
- http://forensicfocus.blogspot.com/2009/07/write-blocker-review.html (29 January 2010).
- http://blogs.sans.org/computer-forensics/2008/10/01/three-hard-drive--imaging-tools/ (29 January 2010).

[22] The Paper *Live Forensic Acquisition as Alternative to Traditional Forensic Processes* by Marthie Lessing from Council for Scientific and Industrial Research Meiring Naudé Road, Scientia, Pretoria, South Africa and Basie von Solms from Academy for Information Technology University of Johannesburg, Auckland Park Kingsway Campus, Johannesburg, South Africa is available at:

- http://researchspace.csir.co.za/dspace/bitstream/10204/3141/1/Lessing5_2008.pdf (1 March 2010).

[23] For "Daubert Hearing" and "Daubert Test," refer to the following links:

- http://www.helium.com/items/1807122-daubert-hearing-on-expert-and-scientific-evidence (16 February 2011).
- http://www.mobar.org/journal/1997/novdec/bebout.htm (16 February 2011).
- http://en.wikipedia.org/wiki/Daubert_standard (16 February 2011).

[24] The article *Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection* by Erin E. Kenneally is available at:

- http://www.law-techjournal.com/articles/ 2005/05_051201_Kenneally.php (1 March 2010).
  The article *Techno Security Guide to eDiscovery and Digital Evidence* can be found at:
- http://www.scribd.com/doc/ 21581538/Techno-Security-s-Guide-to-E-Discovery-and-Digital-Forensics (25 February 2010).
  The Paper *Automatically Creating Realistic Targets for Digital Forensics Investigation* by Frank Adelstein from ATC-NY, Yun Gao and Golden G. Richard III from Department of Computer Science University of New Orleans, USA is available at:
- http://www.cs.uno.edu/~ golden/Stuff/-falcon 2005.pdf (28 February 2010).
  The Paper *Bringing Science to Digital Forensics with Standardized Forensic Corpora* by Simson Garfinkel, Paul Farrell, Vassil Roussev and George Dinolt from Graduate School of Operational and Information Sciences, Department of Computer Science, Naval Postgraduate School, Monterey, CA 93943, USA is available at:
- http://www.dfrws.org/2009/proceedings/p2--garfinkel.pdf (22 February 2010).

The paper *An Open-Source Forensics Platform*' by R. Koen and M. S. Olivier is available at:
- http://mo.co.za/open/reco.pdf (12 February 2010).

[25] NIST Special Publication 800-92 *Guide to Computer Security Log Management* is available at:
- http://csrc.nist.gov/publications/nistpubs/ 800-92/SP800-92.pdf (1 March 2010).

NIST's Computer Security Incident Handling Guide can be visited at:
- http://www.scribd.com/doc/17921434/nist-sp-800061r1-computer-security-incident-handling-guide-200805

[26] The Paper *Building Evidence Graphs for Network Forensics Analysis* by Wei Wang, Thomas E. Daniels from Department of Electrical and Computer Engineering, Iowa State University Ames, Iowa can be downloaded from the following link:
- http://www.acsac.org/2005/papers/125.pdf (12 January 2010).

[27] The *Dissertation Supporting the Visualization and Forensic Analysis Of Network Events*, submitted to the Department of Computer Science and the Committee on Graduate Studies of Stanford University in partial fulfillment of the requirements for the degree of Doctor of Philosophy can be downloaded at:
- http://graphics.stanford.edu/papers/dphan_thesis/doantam.phan.thesis.pdf (1 March 2010).

Details of the *Workshop on Data Mining for Cyber Threat Analysis* in conjunction with IEEE International Conference on Data Mining 9–12 December 2002, Maebashi TERRSA, Maebashi City, Japan can be found at:
- http://www-users.cs.umn.edu/~aleks/icdm02w/workshop_schedule.pdf (24 February 2010).

The Thesis, *Exploring And Validating Data Mining Algorithms For Use In Data Ascription* by Daniel P. Huynh in June 2008, submitted at the Naval Postgraduate School can be found at:
- http://theses.nps.navy.mil/08Jun_Huynh.pdf (29 March 2010).

For Abstracts of the Technical Papers (Ontology-Driven Text Mining for Digital Forensics, Apply Data Mining Techniques for Cyber Intrusion Detection, Apply Dynamical Bayesian Network to Query Digital Forensics, Intelligent Environmental Query on Spatial Data, Intelligent Land Planning on Relational Spatial Data), refer to:
- http://escience.anu.edu.au/project/subject-Others/NICTA07DMProjectTopicsProposals.doc (4 April 2010).

[28] Kargupta, H., Liu, K. and Ryan, J. *Privacy-Sensitive Distributed Data Mining from Multi-Party Data*. Proceedings of the 1st NSF/NIJ Symposium on Intelligence and Security Informatics, 2003, LNCS 2665, Springer-Verlag, pp. 336–342.

[29] Chau, M., Xu, J.J. and Chen, H. *Extracting Meaningful Entities from Police Narrative Reports*. Proceedings of National Conference on Digital Government Research, 2002, Digital Government Research Center, pp. 271–275.

[30] Hauck, R.V. *et al.* (2002) Using coplink to analyze criminal-justice data, *Computer*, pp. 30–37.

[31] Senator, T. *et al.* (1995) The FinCEN artificial intelligence system: identifying potential money laundering from reports of large cash transactions, *AI Magazine*, 16 (4), pp. 21–39.

[32] Lee, W., Stolfo, S.J. and Mok, W. A Data Mining Framework for Building Intrusion Detection Models. Proceedings of 1999 IEEE Symposium on Security and Privacy, 1999, IEEE CS Press, pp. 120–132.

[33] To understand how "Insider Trading" works, visit:
- http://money.howstuffworks.com/insider–trading1.htm (5 April 2010).
- http://beginnersinvest.about.com/cs/newinvestors/a/102702a.htm (5 April 2010).
- http://www.mysmp.com/stocks/insider–trading.html (5 April 2010).

[34] Privacy issues discussed in the article *Working from Home: Myths and Truths* by Nina Godbole in PCQuest February 2010 issue posted at:
- http://pcquest.ciol.com/content/topstories/ 2010/110020105.asp (4 April 2010).

The write-up based on the topic *Challenges in Mobile Workforce Mgmt* at the IT SummIT 2009 at the Cyber Media event is available at:
- http://pcquest.ciol.com/content/techtrends/ 2010/110010806.asp (4 April 2010).

[35] A table showing feature comparison of the antiforensics privacy products mentioned in Section 7.19 (Antiforensics) is available at:

- http://www.privacy-software- review.toptenreviews.com/ (2 April 2010).

[36] The tool "timestomp" is available at: www.metasploit.com/projects/antiforensics/ (1 April 2010). See the presentation *Metaspolit Antiforensic Project* available at:

- http://www.metasploit.com/data/antiforensics/ToorCon7-Metasploit_AntiForensics.ppt (8 April 2010).

[37] Additional Information about "Slacker" can be accessed at:

- http://www.forensickb.com/2007/10/enscript-to-detect-use-of-slackerexe.html (9 April 2010). Here it is explained how 'Enscript' detected the use of "slacker.exe".
  To know more on "slacker.exe," visit the following site:
- http://www.forensicswiki.org/wiki/Slacker (9 April 2010)

Further Reading

Additional Useful Web References

1. On the International Association of Crime Analysts Page in the following link, there is a complete table containing the listing of Crime Analysis Software:
   http://www.iaca.net/Software.asp (27 February 2010).
2. To understand the meaning of "end-to-end -digital forensics," the following sites can be visited:
   - For Digital Forensics Research Workshop, visit: www.dfrws.org (31 May 2009).
   - For International Journal of Digital Evidence, visit: www.ijde.org (31 May 2009).
3. For *Forensic File Formats*, refer to:
   http://www.forensicswiki.org/index.php?title=Forensic_file_formats (6 June 2009).
4. There is a basic article for non-technical readers to understand what "Rootkits" are and how to remove them. To know more on this, visit:
   - http://www.virus.gr/portal/en/content/rootkits-what-are-they-how-remove-them (8 April 2010).
     A technical paper on *database rootkits* (2005) by Alexander Kornbrust is available at:
   - http://www.red-database-security.com/wp/db_rootkits_us.pdf (8 April 2010).
     Oracle Rootkits are discussed in a paper available at:
   - http://www.red-database-security.com/wp/oracle_rootkits_2.0.pdf (8 April 2010).
     A technical presentation on "*In Memory Rootkits*" is available at:
   - http://www.databasesecurity.com/oracle–backdoors.ppt (8 April 2010).
     To have an overview of *Unix Rootkits Overview and Defense* by Anton Chuvakin, visit:
   - www.rootsecure.net/content/downloads/pdf/unix_rootkits_overview.pdf (8 April 2010).
     Microsoft BlueHat Security Briefings: Spring 2006 Sessions and Interviews are available at:
   - http://www.microsoft.com/technet/security/bluehat/sessions/default.mspx (11 April 2010).
5. Some *free downloadable File Splitting software utilities* can be accessed at readers' own risk by visiting:
   http://www.snapfiles.com/Freeware/downloader/fwfilesplit.html (3 June 2009).
6. The home page of the *Australian Institute of Criminology* can be visited at:
   http://www.aic.gov.au/ (23 April 2009).
7. Those aspiring to pick up a course in cyberforensics with adequate hands-on content, may visit:
   http://blogs.thehindu.com/delhi/?p=20694 (23 October 2009).
8. For *Digital Forensic/Computer Forensic/Cyber Forensic Frequently Asked Questions* (FAQs), visit:
   Computer forensics FAQs at:
   - http://www.evestigate.com/Computer%20Forensics%20FAQ.htm (24 October 2009).
     Forensics examination FAQs at:
   - http://www.patctech.com/faq/forensic.shtml (24 October 2009).
     Digital detective FAQs at:
   - http://www.digital-detective.co.uk/faq.asp (24 October 2009).
     Computer forensics FAQs at:
   - http://www.newyorkcomputerforensics.com/learn/forensics_faq.php (24 October 2009).
   - http://www.ccl-forensics.com/237/FAQ.html (24 October 2009).
   - http://www.evidencetalks.com/faq.html (24 October 2009).

Computer forensics basics FAQs at:

- http://www.computerforensicsworld.com/modules.php?name=News&file=article&sid=1 (24 October 2009).
- http://www.setecinvestigations.com/resources/faqs.php (24 October 2009).

Computing hacking forensics FAQs at:

- http://www.cfila.com/forensicsfaq.htm (24 October 2009).

9. For those interested in seeking a digital forensics career, the following list of links may be useful:
FAQs about digital forensics program, visit the following sites at:

- http://forensics.cs.uri.edu/faq.php (26 October 2009).
- http://www.forensiccareers.com/index.php?option=com_content&task=view&id=23&Itemid=26 (26 October 2009).
- http://computerforensics911.com/ (26 October 2009).

FAQs to Digital Forensics Certification Board, visit:

- http://www.ncfs.org/dfcb/faqs.html (26 October 2009).

10. For covert channels, visit:

- http://en.wikipedia.org/wiki/Covert_channels (1 November 2009).

To know more about covert channels and steganography discussion, visit:

- http://www.covertchannels.org/ (1 November 2009).

11. For *Information Hiding: Steganography & Digital Watermarking*, refer to:
http://www.jjtc.com/Steganography/(1 November 2009).

12. For *Understanding Digital Steganography*, refer to:

- http://fanaticmedia.com/infosecurity/archive/Sep09/Digital%20Steganography.htm (30 October 2009).

All about steganography is explained at:

- http://palisade.plynt.com/issues/2005Apr/-steganography/ (1 November 2009).

13. For those readers who are highly technical minded can refer to:
http://www.defcon.org/images/defcon-15/dc15-presentations/dc-15-smith.pdf (13 January 2010). It is about forensics lessons learned by a person working with the Department of Defense.

14. For *California SB* (Security Breach) *1386*, refer to:
For the SB 1386 Compliance Management Toolkit, visit:

- http://www.sb-1386.com/ (20 February 2010).

For SB 1386, refer to:

- http://en.wikipedia.org/wiki/SB_1386 (20 February 2010).

For SB-1386 Introduction, refer to:

- http://www.sb-1386.com/sb-intro.htm (20 February 2010).

15. Some more links to California's new mandatory disclosure law are as follows:

- http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci901999,00.html (19 February 2010).
- http://www.privacyrights.org/ar/Security Breach.htm (19 February 2010).
- http://www.bitpipe.com/tlist/California-Senate-Bill-1386.html (19 February 2010).
- http://library.findlaw.com/2003/Sep/30/133060.html (19 February 2010).

16. There is an informative document *What Judges Should Know About Computer Forensics* available at:
http://www.craigball.com/What_Judges_Computer_Forensics-200807.pdf (1 February 2010).

17. An interesting article *Sending email: Can you be arrested* ? is available at:
http://specials.rediff.com/money/2008/jul/29cyber.htm (20 February 2010).

18. The article *Chinese Hackers and India Cyber Forensics* can be visited at:
http://www.thedarkvisitor.com/2008/08/-chinese-hackers-and-india-cyber-forensics/ (1 March 2010).

19. Following link explains what Facebook is for: http://www.youtube.com/watch?v=kFKHaFJzUb4&NR=1 (1 March 2010).

20. *Incident Management in the Age of Compliance* is the article that addresses the basics of doing what the laws tell you to do (FISMA, HIPAA, PCI-DSS) at:
http://www.computerworld.com/s/article/9019559/Incident_management_in_the_age_of_compliance?taxonomyName=Disaster_Recovery (21 February 2010).

21. Useful blogs on computer investigation is found at: http://forensic.to/links/pages/Forensic_Sciences/Field_of_expertise/Computer_Investigation/ (14 February 2010).
22. C-DAC releases five new products at Elitex 2008, visit:
    - http://enterthegrid.com/primeur/08/articles/weekly/AE-PR-02-08-61.html (6 September 2010).

    One of the products is *Cyber Investigation and Analysis Tools for Network Forensics* and the Frequently Asked Questions document *Intrusion Detection FAQ: Can you explain traffic analysis and anomaly detection?* is available at:
    - http://www.sans.org/security-resources/idfaq/anomaly_detection.php (1 March 2010).
23. For the Global News on Forensics Computing, visit: http://www.f3.org.uk/modules/news/index.php?storytopic=2&start=95 (5 February 2010).
24. *How Forensics works* is very well explained at: http://computer.howstuffworks.com/-computer-forensic3.htm (9 April 2010).
25. DoD List of Cyber Forensics Tools can be obtained by visiting the link at: http://www.dc3.mil/dcci/dcciCyberFiles.php (9 September 2010).
26. Some free file recovery methods are as follows: http://pcsupport.about.com/od/filerecovery/tp/free-file-recovery-programs.htm (18 September 2010).

    To learn about some of the Recognized Data Overwriting Standards, visit: http://www.dataerasure.com/recognized_overwriting_-standards.htm (18 September 2010). These methods of data sanitization ensure regulatory compliance.
27. The Paper *Open Source Digital Forensics Tools: The Legal Argument* by Brian Carrier is available at: http://www.digital-evidence.org/papers/-opensrc_legal.pdf (25 February 2010).

Books

1. Volonino, L. and Anzaldua, R. (2008) *Computer Forensics for Dummies*, Wiley Publishing.
2. Casey, E. (ed.) (2002) *Handbook of Computer Crime Investigation: Forensic Tools and Technology*, Academic Press, CA.
3. Marjie, B.T. (2003) *Computer Forensics and Cyber Crime: An Introduction*, Prentice Hall.
4. Anthony, R. (2007) *Cyber Crime Investigations: Bridging the Gaps between Security Professionals, Law Enforcement, and Prosecutors*, Syngress.
5. McKenzie, M.A. (2009) *Digital Forensics: Digital Evidence in Criminal Investigations*, Wiley.
6. Johnson, T.A. (ed.) (2006) *Forensic Computer Crime Investigation*, CRC Press, Boca Raton, FL.
7. Casey, E. (ed.) (2004) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 2nd edn, Academic Press.
8. Sood, V. (2010) Leading electronic evidence in the court: critical analysis and the stepwise process, *Cyber Crimes, Electronic Evidence & Investigation: Legal Issues*, 1st edn, NABHI Publication, New Delhi, p. 177.
9. Marcella, A.J., Jr. and Menendez, D. (2008) *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crime*, 2nd edn, Auerbach Publications.
10. Steve, B. (2007) *EnCase Computer Forensics: The Official EnCE – EnCase Certified Examiner Study Guide*, 2nd edn, John Wiley & Sons.
11. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India. Readers can refer to Chapters 11 and 12 and the entire Part III of this book; it is dedicated to logical and network security-related topics. E-Mail security is also discussed in that part of the book. The OSI 7 Layer Model is also explained.
12. ibid – Chapter 2 (Threats to Information Systems).
13. Ibid – Chapter 4 (Information Security Management in Organizations).
14. Ibid – Chapter 5 (Building Blocks of Information Security)
15. Ibid – Chapter 12, Section 12.5 (The OSI Seven-Layer Model) and Section 12.7 (Network Protocols). See p. 210 about Tunneling Protocols.
16. Ibid – Chapter 13 (Cryptography and Encryption).
17. Ibid – Chapter 14 (Intrusion Detection for Securing the Networks).
18. Ibid – Chapter 17 (Security of Wireless Networks).
19. Ibid – Chapter 35, Section 35.9 explains Penetration Testing and Vulnerability Scanning and the difference between the two, etc.

20. EC-Council (2009), *Computer Forensics: Investigating Wireless Networks and Devices*, EC Council Press, New York, USA.
21. Volonino, L and Anzaldua, R. (2008) Computer Forensics for Dummies (For Dummies (Computer/Tech)John Wiley & Sons Ltd., USA
22. Caloyannides, M.A. (2001) *Computer Forensics and Privacy*, Artech House (Artech House Computer Security Series), Boston, MA.
23. Caloyannides, M.A. *Privacy Protection and Computer Forensics*, 2nd edn, Artech House (Artech House Computer Security Series), Boston, MA.
24. To know more on data mining, refer to the -following books:
Han, J., Kamber, M. and Pei, J. (2005) *Data Mining: Concepts and Techniques*, 2nd edn, The Morgan Kaufmann Series in Data Management Systems, Morgan Kaufmann Publishers.
Cios, K.J., Pedrycz, W., Swiniarski, R.W. and Kurgan, A.K. (2007) *Data Mining: A Knowledge Discovery Approach*, Springer.
Shmueli, G., Patel, N.R. and Bruce, P.C. (2006) *Data Mining for Business Intelligence: Concepts, Techniques, and Applications in Microsoft Office Excel with XLMiner*, Wiley.
Thuraisingham, B.M. *Data Mining: Technologies, Techniques, Tools, and Trends*, CRC Press.
25. Microsoft Word version of *FastBloc User Guide/Manual* can be downloaded from the folowing link: http://www.agapeinc.in/FastBloc-IDE_manual.doc (10 September 2010).

Articles and Research Papers

1. A 2008 presentation by Bruce Nikkel titled *Practical Computer Forensics using Open Source Tools* is available at: http://www.ch-open.ch/events/slides/2008/ 080612_nikkel08.pdf (9 April 2010).
2. *Computer Forensics*, 56 (1), January 2008 issue is available at: http://www.justice.gov/usao/eousa/foia_reading_room/usab5601.pdf (12 February 2010).
3. Borck, J. (2001) *Leave the cybersleuthing to the experts* – refer to this article in the following URL: http://www.infoworld.com/articles/tc/xml/01/04/09/010409tccounter.html (22 December 2005).
4. Bitpipe (2005) *Computer Forensics.* This article is available at: http://www.bitpipe.com/tlist/Computer-Forensics.html (27 December 2005).
5. Burdach, M. (2005) *Digital Forensics of the Physical Memory* is available at: http://forensic.seccure.net/pdf/mburdach_-digital_forensics_of_physical_memory.pdf (21 June 2005).
6. A paper by Liu, Q., Sung, A.H. and Qiao, M. *Detecting Information-Hiding in WAV Audios*, Computer Science Department and Institute for Complex Additive Systems Analysis, New Mexico Tech. can be accessed at:
- http://-figment.cse.usf.edu/~sfefilat/data/papers/TuBCT9.47.pdf (7 May 2009).
- Harrill, D.C. and Mislan, R.P. (2007) A small scale digital device forensics ontology, *Small Scale Digital Device Forensics Journal*, 1 (1). The paper is available at:
- http://www.ssddfj.org/papers/SSDDFJ_V1_1_Harrill_Mislan.pdf (1 September 2009).

7. Brinson Ashley, Robinson Abigail, Rogers Marcus (2006) A cyber forensics ontology: Creating a new approach to studying cyber forensics, *Digital Investigation* 3S, S37–S43 can be accessed at: http://www.dfrws.org/2006/proceedings/5–Brinson.pdf (6 Septebmer 2010).
8. Marsico, C.V. and Rogers, M.K., iPod Forensics, The CERIAS Tech Report 2005-13, the Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907-2086. The paper can be accessed at: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-13.pdf (2 August 2009).
9. Marsico, C.V. Digital Music Device Forensics, CERIAS Tech Report 2005-27, Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907-2086. It is a Thesis Submitted to the Faculty of Purdue University and is available at: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-27.pdf (31 August 2009).
10. Some links iPod Forensics are as follows:

https://www.cerias.purdue.edu/apps/reports_and_papers/view/2814 (2 September 2009).
http://www.cerias.purdue.edu/search/site.php?q=forensics (2 September 2009).

11. The following site lists the forensics vendors – the software and hardware tools are alphabetically listed, visit: http://www.e-evidence.info/vendors.html (12 September 2009).

12. For an interesting paper whether Computer Forensics is based on Computer Science or Forensics Science, visit: http://www.ics.heacademy.ac.uk/events/presentations/736_HEA-ICS-TchCompFor_paper.pdf (12 September 2009).

13. For Cisco Router Forensics, the following link can be accessed at: http://www.forensics.nl/-presentations (23 September 2009).
This is an excellent reference for lawyers practicing in cybercrime cases and working with digital forensics experts, here is the link where some excellent technical articles are available. They explain many technical aspects such as – -difference between "clone" and "image" of drive, how do you make a "forensically-sound" duplicate of a drive. How can you prove the duplicate drive is forensically sound. Examining and analyzing E-Mail headers for forensics analysis and how to look for a good forensics expert, etc. is also covered in this set of articles.

14. Van Horenbeeck, M. *Deception on the network*, School of Computer and Information Science at Edith Cowan University. Malicious use of covert channels is explained in this paper. This paper can be accessed at: http://www.daemon.be/maarten/Vanhorenbeeck_covertchannels.pdf (31 October 2009).

15. A 2006 student technical report on covert channel research is available at: http://staff.science.uva.nl/~delaat/snb-2005-2006/p27/report.pdf (25 October 2009).
It is the Research Report for RP1 based on student work by Marc Smeets and Matthijs Koot as part of their work in the course MSc in System and Network Engineering at the University of Amsterdam

16. There is a paper that explains a covert communication channel that exists in virtually all forms of packet switching data networks. It is a paper by Bo Yuan and Peter Lutz, Department of Networking, Security, and Systems Administration, Golisano College of Computing and Information Sciences at the Rochester Institute of Technology, New York 14623. Visit http://www.ist.rit.edu/~byuan/papers/boyuan_peterlutz05.pdf (25 October 2009).

17. Chauhan, S. (2005) *Analysis and Detection of Covert Network Channels*, Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County. The paper is available at: http://www.cisa.umbc.edu/courses/cmsc/444/fall05/studentprojects/sweety.pdf (1 November 2009).

18. Uma Devi G. (2006) *Steganography-Survey on File Systems*, as part of MS by Research – CSE, IIIT (Indian Institute of Information Technology), Hyderabad. The paper can be accessed at: http://researchweb.iiit.ac.in/~umadevi/steg.pdf (1 November 2009).

19. Gulati, K. (2003) A Dissertation on *Information Hiding Using Fractal Encoding*, submitted in partial fulfillment of the requirements for the degree of Master of Technology at the IIT, Bombay. It is under the guidance of Prof. Vikram M. Gadre at the School of Information Technology at the IIT, Mumbai. It is accessible at: http://www.it.iitb.ac.in/~kamal/fractal.pdf (30 October 2009).

20. Llamas, D., Allison, C. and Miller, A. *Covert Channels in Internet Protocols: A Survey* by, the School of Computer Science at the University of St Andrews, St Andrews KY16 9SX, Scotland, UK. The paper is available at: http://gray-world.net/papers/0506-PGNET-Paper.pdf (1 November 2009).

21. Pan, L. and Batten, L.M. *Reproducibility of Digital Evidence in Forensic Investigations*, School of Information Technology, Deakin University, Australia. The paper is available at: http://www.dfrws.org/2005/proceedings/pan_reproducibility.pdf (19 December 2009).

22. Ahmed, I. *Steganalysis in Computer Forensics*, School of Computer and Information Science, Edith Cowan University. The paper is available at: http://scissec.scis.ecu.edu.au/conference_proceedings/2007/forensics/10_Ibrahim%20-%20Steganalysis%20in%20Computer%20Forensics.pdf (6 June 2009).

23. Karp, S. (2007) *Facebook's Vulnerabilities*, refer to the following link: http://publishing2.com/2007/10/31/-facebooksvulnerabilities/ (10 December 2009).

24. Kessler, G.C. and Schirling, M. (2002) *Computer Forensics: The Issues and Current Books in the Field*. The paper can be found at: http://www.garykessler.net/library/computer_forensics_books.html (26 February 2010).
25. Olsson, J. *Computer Forensics Digital Evidence with Emphasis on Time*. The paper can be accessed at: http://www.bth.se/tek/aps/mbo.nsf/bilagor/Digital_Evidence_with_Emphasis_on_Time_pdf/$file/Digital_Evidence_with_Emphasis_on_Time.pdf (2 March 2010).
26. Symon, C. (2009) *Enhanced Event Time-Lining for Digital Forensic Systems*. The paper is submitted in partial fulfillment of the requirements of Edinburgh Napier University for the Degree of Computer Networks & Distributed Systems (Hons), School of Computing. It is available at: http://www.dcs.napier.ac.uk/~bill/colin01.pdf (10 January 2010).
27. Ha, D., Upadhyaya, S., Ngo, H., Pramanik, S., Chinchani, R. and Mathew, S. *Insider Threat Analysis Using Information-Centric Modeling*. The paper can be visited at: http://www.cse.buffalo.edu/~shambhu/-documents/pdf/ifip-chapter-2007.pdf (2 March 2010).
28. Regan, J.E. (2009) *The Forensic Potential of Flash Memory*. The paper is submitted in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis can be read at: http://simson.net/clips/students/09Sep_Regan.pdf (8 April 2010).
29. There is CIO magazine article, *How Online Criminals Make Themselves Tough to Find, Near Impossible to Nab*. The article can be accessed at:
    - http://www.proofspace.com/UserFiles/File/How%20Anti%20Forensics%20Tools%20Make%20Themselves%20Tough%20to%20Find%20Near%20Impossible%20to%20Nab%20CIO%20com%202007-05-31.pdf. (10 April 2010).

    In this article it is explained how antiforensics tools reveal vulnerabilities in computer forensics tools. An argument is made that the rise of antiforensics tools will force computer investigators to change.

    Encase and Sleuth Kit vulnerabilities are described in a technical paper at:
    - https://www.isecpartners.com/files/iSEC-Breaking_Forensics_Software-Paper.v1_1.BH2007.pdf (7 April 2010).

    In this 2007 paper titled *Breaking Forensics Software: Weaknesses in Critical Evidence Collection*. Classes of attacks against forensics software are also described in this paper. Pg. 5 of this paper describes sleuth kit weaknesses and Pg. 9 describe EnCase weakness.
30. There is an interesting article *Catch Me if You Can* at the following link: http:// www.blackhat.com/presentations/bh-usa-05/bh-us-05-foster-liu-update.pdf (8 April 2010).
31. Kessler, G.C. *Anti-Forensics and the Digital Investigator*, Champlain College, Burlington, VT, USA. The paper can be accessed at: http://igneous.scis.ecu.edu.au/proceedings/ 2007/forensics/01_Kessler_Anti-Forensics.pdf (10 April 2010).
32. Swanson, I. and Williams, P.A.H. *Virtual Environments Support Insider Security Violations*, SECAU Security Research Centre, Edith Cowan University. The paper is available at: http://scissec.scis.ecu.edu.au/conference_proceedings/2008/forensics/Swanson20Williams20Virtual%20environments%20.pdf (9 April 2010).
33. ACPO's Official Release version on *Good Practice Guide for Computer-Based Electronic Evidence* is available at: http://www.asianlaws.org/library/cci/acpo-guidelines-computer-evidence.pdf (10 September 2010).
34. Read article *Advanced Forensic Format: An Open, Extensible Format for Disk Imaging* by Garnkel, S.,Malan, D., Dubec, K., Stevens, C. and Pham, C. at: http://www.cs.harvard.edu/malan/publications/aff.pdf (16 December 2010).

Video Clips

Following links present short clips on various topics discussed in this chapter (digital forensics and perils of posting your information on social networking sites, rootkits, etc.)

1. A basic video presentation explaining *What is Computer Forensic* is available at: http://www.youtube.com/watch?v=yfigCH7CcFk& feature=related (7 April 2010).
2. Video clips on *Disk Encryption and other Forensics aspects* are available at:

- http://www.privacylover.com/computer–forensics/video-using-eraser-to-delete-files-for-good/ (27 February 2010).
  This is a video for beginners – some introduction on why you should use a secure data wiper to delete files in your computer. In this video clip, a computer user shows you on screen how to use eraser to safely wipe documents and making them vanish for good.
- http://www.youtube.com/watch?v=9JoX4uxES7Q&feature=related (27 February 2010). Here, a forensics expert explains how to seize the evidence.
- http://www.youtube.com/watch?v=grjIOaE4-aA&feature=related (27 February 2010). This clip explains what computer forensics experts can do to uncover data and online activity.
- http://www.privacylover.com/computer–forensics/interview-with-a-computer-forensics-expert/ (27 February 2010). This clip is an interview with a computer forensics expert.
- http://www.youtube.com/watch?v=hSvswzSy3oA&feature=related (27 February 2010). This is about computer forensics – this video shows how to trace an E-Mail (Hotmail).
- http://www.privacylover.com/encryption/video-crash-course-in-full-disk-encryption/ (27 February 2010).
  This video is a talk held in December 2008 at the 25th Chaos Communication Congress, under the title *Nothing to Hide*. It is a crash course in full-disk encryptCion concepts, products and implementation aspects. An overview of both commercial and open-source offerings for Windows, Linux and MacOS X is provided. A programmer's look at the open-source solutions concludes the presentation.
- http://www.privacylover.com/encryption/review-full-disk-encryption-diskcryptor-v0-7-435-90/ (27 February 2010). This is review of DiskCryptor based on its testing done.
- http://www.privacylover.com/encryption/review-drivecrypt-plus-pack-full-disk--encryption/ (27 February 2010). This clip is review of Drivecrypt Plus Pack v3.95, full-disk encryption.
- http://www.privacylover.com/computer-forensics/video-computer-forensic-investigation/ (27 February 2010). At this link, a computer forensics professional explains the basics of computer forensics, how data is recovered from people's computers and what challenges they face.
- http://www.privacylover.com/computer–forensics/metasploit-anti-forensic-investigation-arsenal-mafia/ (27 February 2010). This clip is about Metasploit Anti-Forensic Investigation Arsenal (MAFIA).
- http://www.youtube.com/watch?v=0HeVx5fkwSY&feature=related (27 February 2010). Here, an expert explains how website traffic myths are uncovered.
- http://www.youtube.com/watch?v=O4ce74 q2zqM&NR=1 (27 February 2010). There is a Demo of EnCase Computer Forensics Tool available in this link.
- http://www.youtube.com/watch?v=kK6Wd7HVyVM&feature=related (27 February 2010). This video clip shows basic keyword searching with forensics Tool EnCase.

3. Video clips on *Perils of Social Networking Sites* are available at:
- http://www.youtube.com/watch?v=ZmQT3SMxATQ&feature=related (27 February 2010). This clip explains the perils of posting your personal information on social networking sites.
- http://www.youtube.com/watch?v=0Ats NyXFg7Y&feature=fvw (27 February 2010). It explains about dangers of social networking,
- http://www.youtube.com/watch?v=azIW1xjSTCo&feature=related (27 February 2010). This is about how social networks such as Facebook and MySpace impacts private life.

4. A video clip explaining "BIOS Rootkits" is available at: http://www.youtube.com/watch?v=G26oZtzluAQ&feature=player_embedded (10 April 2010).

5. A video clip on antiforensics can be viewed at: http://pursuitmag.com/anti-computer-forensics/ (9 April 2010)

6. Fourth Amendment Project video clip can be accessed at: http://www.youtube.com/watch?v=mdT_k6Yj_w8 (7 September 2010).

Chapter 8: Forensics of Hand-Held Devices

References

[1] The following links are for hand-held forensics Paraben Product links:

Paraben forensics device seizure v3.3 − cell phone forensics product information is available at: http://www.paraben.com/catalog/product_info.php?products_id=405 (17 April 2010).
Device Seizure Command Kit − Mobile forensics software and hardware information can be accessed at:
http://www.paraben.com/catalog/product_info.php?products_id=363 (17 April 2010).
Information about Paraben's Device Seizure Toolbox is available at:
http://www.paraben.com/catalog/product_info.php?products_id=343 (17 April 2010).
Information about Device Seizure Field Kit is available at:
http://www.paraben.com/catalog/product_info.php?products_id=501 (17 April 2010).
The pictures of Paraben forensics products and their associated information is available at:
http://www.paraben.com/catalog/product_info.php?products_id=484 (17 April 2010).
Training information about hand-held forensics products is available at:
http://www.paraben.com/catalog/product_info.php?products_id=440 (17 April 2010).
Information about the mobile laboratory kit for hand-held forensics is available at:
http://www.paraben.com/catalog/product_info.php?products_id=490 (17 April 2010).
DS Lite is for analysis and reporting on device -seizure and CSI stick case files; information about this product is available at:
http://www.paraben.com/catalog/product_info.php?products_id=482 (17 April 2010).

[2] Refer to the following link for "3G": http://en.wikipedia.org/wiki/3G (21 April 2010).

[3] Read the document "*Printing to a Xerox Multifunction Device Using Port 9100* " available at: http://www.xerox.com/downloads/usa/en/d/dc00cc0104.pdf (13 April 2010).
TCP port 9100 Protocol information and Warnings are posted at:
http://www.auditmypc.com/port/tcp-port-9100.asp (13 April 2010).
List of TCP and UDP Port Numbers is available at:
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers (12 April 2010).

[4] To know about "*Jailbroken*" *iPhones and the Security Risks* associated with them, visit:
http://en.wikipedia.org/wiki/Jailbreaking_for_iPhone_OS (1 May 2010).
http://www.canada.com/life/Jail+broken+iPhones+hacked+virus/2256956/story.html (1 May 2010).
http://www.ioltechnology.co.za/article_page.php?iArticleId=5257753 (1 May 2010).
http://www.networkworld.com/columnists/2009/111109antonopoulos.html (1 May 2010).
http://www.reuters.com/article/idUKN2325185820091123 (1 May 2010).

[5] Documentation about a suite of iPhone Forensics Software Solutions is available at: http://www.oxygen-forensic.com/en/press/ (18 April 2010). It is the "Oxygen Forensics" suite.

[6] To know about *BellSouth Intelligent Wireless Network* (mentioned in Section 8.3.8), visit:
http://www.answers.com/topic/bellsouth–intelligent-wireless-network (4 May 2010).
http://encyclopedia2.thefreedictionary.com/BellSouth+Intelligent+Wireless+Network (4 May 2010).
http://www.yourdictionary.com/computer/bell-south-intelligent-wireless-network (4 May 2010).
http://www.rimdev.com/Tutorials/IAS_Descr_Prog_Guide.pdf (4 May 2010).

[7] The story about use of an Apple iPod by a gang of thieves in England to store information related to their crimes is posted at: http://news.bbc.co.uk/2/hi/uk_news/england/london/3932847.stm (17 April 2010).

[8] To understand the calibration and standardization aspects to be considered for evaluating digital forensics tools, the paper *Freeware Live Forensics Tools Evaluation and Operation Tips* by Ricci Ieong, Principal Consultant with eWalker Consulting Ltd. can be referred. The paper is available at: http://www.marcomattiucci.it/ieong.pdf (22 April 2010).

Further Reading

Additional Useful Web References

1. Visit the following link for *Forensics o*n Yahoo *Music* at: http://new.music.yahoo.com/forensics/ (16 April 2010).
2. You can gain useful information on *Computer Forensics Toolkits, Digital Evidence Software Suites* by visiting:

http://www.forensics.nl/toolkits (28 April 2010). There is a short information here on a large number of tools.

3. Check out the following link for links to various forensics toolkits http://www.filesrecovery.in/file-recovery-tools/pocket-pc-forensic.asp (25 April 2010).
4. PDA Forensics Tools and Techniques – read about this in the following link (it is a blog). http://www.informit.com/guides/content.aspx?g=security&seqNum=105&rll=1 (2 March 2010).
5. Pictures and specifications for various *Handheld Digital Forensics Products* can be viewed at: http://www.dataduplication.co.uk/details/mobilephoneforensics.html (17 April 2010).
6. Andrew Hoog, Chief Investigative Officer at viaForensics in the US of America is one of the *iPhone forensics experts*. His contact details are quoted below. Phone: +1 312-283-0551 and +1 312-283-0551. The website to contact him is http://viaforensics.com/contact-us
7. Read EzineArticles from the Communications: Mobile-Cell-Phone Category at: http://ezinearticles.com/?Introduction-to-Cell-Phones-and-IMEI-Numbers–What-is-It?-(Pt1)&id=4017473 (12 April 2010).
8. To know *How to Identify the Cell Phone Number* refer to: http://www.ehow.com/how_5486499_identify-cell-phone-number.html (1 April 2010).
9. The *Importance of the IMEI number for Cell Phone Insurance* can be appreciated by reading the article available at: http://www.ensquared.com/content/No_IMEI_no_insurance_for_unlocked_cell_phones.htm (11 April 2010).
10. Compelson Laboratories – To know more about MOBILedit! Forensic, visit WiKi at: http://www.forensicswiki.org/wiki/MOBILedit! (28 September 2010).
11. To know more about Oxygen Software Oxygen Phone Manager II (Forensic version), visit: http://www.opm2.com/forensic/ (8 October 2006).
12. Paraben Corporation (2006). Paraben Forensics Software, Hardware, and Training, visit the URL at: www.parabenforensics.com/index.html (14 September 2006).
13. How iPhone Unlocking Works can be understood by visiting: http://newsblaze.com/story/20070926073901 chil.nb/topstory.html (1 May 2010).
14. Following are some WCDMA-related links: http://www.systemdisc.com/wcdma (20 April 2010). http://www.wisegeek.com/what-is-wcdma.htm (20 April 2010). http://www.topbits.com/wcdma.html (20 April 2010). http://www.answers.com/topic/wcdma (20 April 2010). http://www.mobileburn.com/definition.jsp? term=WCDMA (20 April 2010). http://cellphones.about.com/od/cell_phone_glossary/g/wcdma.htm (20 April 2010). http://www.webopedia.com/TERM/W/WCDMA.html (20 April 2010). http://www.differencebetween.net/technology/difference-between-wcdma-and-hsdpa/ (20 April 2010).
15. Following are some FOMA Links: http://www.mobilemag.com/2004/11/15/ntt-docomo-dual-network-foma-and-lan-voip-phone/ (20 April 2010). http://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_ journal/bn/vol8_1/vol8_1_065en.pdf (20 April 2010).
16. To know about Full Internet Browsing to NTT DoCoMo 3G FOMA™ Handset, refer to: http://www.3g.co.uk/PR/June2005/1658.htm (20 April 2010).
17. For an excellent article "*Recovering and Examining Computer Forensic Evidence*," visit: http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm (22 April 2010).
18. Visit the following links accessed between March 2010 and May 2006: For article *Good Practice Guide for Computer based Electronic Evidence*, visit: http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf For article *Cell Phone Forensic Tools: An Overview and Analysis*, visit: http://csrc.nist.gov/publications/nistir/nistir7250.pdf For article *Toshiba Reports Battery Breakthrough*, visit: http://news.com.com/206110786_35649141.html?tag=nl For article *Guidelines for the Management of IT Evidence*, visit: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

For article *Best Practice Guidelines for Examination of Digital Evidence*, visit:
http://www.ioce.org/2002/Guidelines%20for%20Best%20Practices%20in%20Examination%20of%20Digital%20Evid.pdf
For article *Guidelines on PDA Forensics*, visit:
http://csrc.nist.gov/publications/nistpubs/80072/sp80072.pdf
For article *Guidelines on Cell Phone Forensics*, visit:
http://csrc.nist.gov/publications/drafts/DraftSP800101.pdf
For article *Secure Data Erase Utility*, visit:
http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml (1 May 2010).

19. There is an informative article by Jesse David Hollington, in which he has described his experience with *review of all the 22 applications that run on a typical iPhone.* To read the article, visit the following link: http://www.ilounge.com/index.php/articles/comments/iphone-gems-all-22-wallet-apps-reviewed/ (2 May 2010).

20. Read *Why BlackBerry* by visiting: http://
crackberry.com/lecture-1-why-blackberry (3 May 2010).

21. Learn about advantages of BlackBerry, and BlackBerry FAQs by visiting:
http://black-berryfaq.com/index.php/Why_BlackBerry%3F (3 May 2010).

22. The term "probative evidence" is explained at:
http://legal-dictionary.thefreedictionary.com/probative+value (28 September 2010).
http://legal-dictionary.thefreedictionary.com/probative (28 September 2010).
http://www.answers.com/topic/probative (28 September 2010).

Books

1. Jansen, W. and Ayers, R. (2005) *An overview and analysis of PDA Forensic Tools*, Elsevier.

2. EC-Council, *Computer Forensics: Investigating Data and Image Files*, EC-Council Press.

3. Zdziarski, J. (2008) *iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets*, O'Reilly Media Inc., USA.

4. Jones, A. and Valli, C. (2008) *Building a Digital Forensics Laboratory: Establishing and Managing a Successful Facility*, Butterworth-Heinemann publication, USA.

5. Mart, E.G. (2006) *Getting started in Forensic Psychology Practice: How to Create a Forensic Specialty in your Mental Health Practice*, John Wiley & Sons Inc., USA.

6. Kubasiak, R.R., Morrissey, S. and Varsalone, J. (2008) *Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit*, Syngress Publishing Inc., USA.

7. Morrissey, S. (2010) iPhone Forensic Analysis: A Guide to iPhone and iPod Touch Investigations, Syngress Publishing Inc., USA.

8. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Chapter 3), Wiley India, New Delhi.

Articles and Research Papers

1. Use of "Sterile Media" is very crucial for ensuring that cross examination in the court does not bring up questions to raise the "forensic soundness" of the evidence. Therefore, "sanitization" of the media is very important. NIST (National Institute of Standards and Technology) has published a number of guidelines. *NIST guidelines on Media Sanitization* is available at:
http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf (30 April 2010).

2. There are six excellent articles by Craig Ball. Law students and legal professionals will find a very useful article at: http://www.almfd.org/pdfs/computer20forensics20for20attorneys.pdf (26 April 2010).

3. Ayers, R., Jansen, W., Cilleros, N. and Daniellou, R., *Cell Phone Forensic Tools: An Overview and Analysis*, The NIST Report NISTIR 7250 is available at:
http://csrc.nist.gov/publications/nistir/nistir-7250.pdf (25 December 2009).

4. Sansurooah, K., *An Overview and Examination of Digital PDA Devices under Forensics Toolkits*, the School of Computer and Information Science (SCIS), Edith Cowan University Perth, Western Australia. The paper can be read at:
http://scissec.scis.ecu.edu.au/conference_proceedings/2007/forensics/04_Sansurooah%20An%20

overview%20and%20examination%20of%20digital%20PDA%20devices%20under%20forensics%20toolkits%20Camera%20Ready%20Paper.pdf (12 April 2010).

5. Frichot, C. *An Analysis of the Integrity of Palm Images Acquired with PDD*, The School of Computer and Information Science, Edith Cowan University, Bradford Street, Mt Lawley, Australia. The paper can be read at: http://scissec.scis.ecu.edu.au/conference_proceedings/2004/-forensics/Frichot-2.pdf (1 April 2010).
6. Printer forensics using SVM (Support Vector Machine) techniques are discussed at: http://cobweb.ecn.purdue.edu/~prints/public/papers/nip05-mikkilineni.pdf (14 April 2010).
7. Jansen, W.A. *Reference Material for Assessing Forensic SIM Tools*, IEEE National Institute of Standards and Technology, MD 20899, USA and Aurelien Delaitre National Institute of Standards and Technology Gaithersburg, MD 20899, USA, The paper (paper no. ICCST 2007-74) is available at: http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_forensics/Reference20Mat-final-a.pdf (1 April 2010).
8. Casadei, F., Savoldi, A. and Gubian, P. (2006) Forensics and SIM cards: an overview, *The International Journal of Digital Evidence*, 5 (1). The paper can be accessed at: http://www.utica.edu/academic/institutes/ecii/publications/articles/EFE3EDD5-0AD1-6086-28804D3C49D798A0.pdf (20 April 2010).
9. Breeuwsma, M., de Jongh, M., Klaver, C., van der Knijff, R and Roeloffs, M. (2007) Forensic data recovery from flash memory, *The Small Scale Digital Device Forensics Journal*, 1 (1), The paper can be accessed at: http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf (16 April 2010).
10. Willassen, S.Y. (2003) Forensics and the GSM mobile telephone system, *The International Journal of Digital Evidence*, 2 (1). It can be found in http://www.utica.edu/academic/-institutes/ecii/publications/articles/A0658858-BFF6-C537-7CF86A78D6DE746D.pdf (2 April 2010).
11. Frichot, C. (2004). *Analysis of the Integrity of Palm Images Acquired with PDD*. Second Australian Computer, Information and Network Forensics Conference. Perth, Western Australia.
12. Danker, S., Ayers, R. and Mislan, R.P (2009). Hashing techniques for mobile device forensics-*Small Scale Digital Device Forensics Journal*, 3 (1). The paper can be accessed at: http://www.ssddfj.org/papers/SSDDFJ_V3_1_Dankner_Ayers_Mislan.pdf (26 April 2010).
13. Backer, C. Digital Forensics on Small Scale Digital Devices. The article can be accessed at: http://www.crypto.rub.de/imperia/md/content/seminare/itsss09/baecker_digital_forensics.pdf (26 April 2010).
14. Murphey, R. Automated Windows Event Log Forensics – the Science Digest paper is available at: http://www.dfrws.org/2007/proceedings/p92-murphey.pdf and CERT-In presentation (28 April 2010).
15. Sarma, S.S. and Mohorikar, N., *Logs and Forensics*, Department of Information Technology, Ministry of Communications & Information Technology. To know more on this, visit: http://www.cert-in.org.in/knowledgebase/-presentation/Logs-Forensics.pdf (28 September 2010).
16. Zdziarski, J. (O'Reilly)'s technical documentation on iPhone Forensics is available at: http://www.esearchbook.com/files/4/eSearchBook.1224255173.iPhone%20Forensics.pdf (2 May 2010).
17. To understand the risks from "Jailbroken" devices, read the articles availabe at the following links: "*Jail Broken*" *iPhones Hacked by New Virus*' (posted November 24, 2009 by Reuters) at: http://tech2.in.com/india/news/mobile-phones/jail-broken-iphones-hacked-by-new-virus/96752/0 (25 September 2010).
    In the following link, Reuters has posted another related story: http://in.reuters.com/article/idINIndia-44181320091123 (25 September 2010).
    In the following link, there is an article "*Duh Worm – a new virus targeting "jail broken" iPhones*": http://topnews.us/content/28505-duh-worm-new-virus-targeting-jail-broken-iphones (25 September 2010).
    In the following link quoted, there is an article "*Apple applies for patent to kill jailbroken devices*": (http://publication.samachar.com/pub_article.php?id=9905908&nextids=9908717|9907847|9907654|9905907|9905908&nextIndex=0 (25 September 2010).

18. To understand about "probative value of evidence," you can refer to the paper by Deborah Davis and William C. Follette (2002) Rethinking the probative value of evidence: Base rates, intuitive profiling, and the postdiction of behavior, *Law and Human Behaviour*, 26(2). The article is accessible at: http://www.sierratrialandopinion.com/papers/Probativevalue1.pdf (28 Sept 2010).
19. Regarding Cell Phones without IMEI number (mentioned in Box 8.4) refer to the article at: http://www.dnaindia.com/mumbai/report_phones-without-imei-numbers-to-be-disconnected-from-tomorrow_1318381 (17th December 2010).

Video Clips

1. iPhone Forensics Demo is available at: http://www.youtube.com/watch?v=op-HyBVN2Ek (15 April 2010).
2. To know more about iPhone and its hardware components, visit: http://www.youtube.com/watch?v=mPhciMud0MM&feature=player_embedded (1 May 2010). It is a video clip that shows the *Insides of Apple iPhone* through the exercise of opening one iPhone handset.
   For a closer look at the iPhone, visit:
   http://www.youtube.com/watch?v=YgW7or1TuFk&NR=1&feature=fvwp (1 May 2010).
   To learn how to use an iPhone, you can visit the video clip available at:
   http://www.youtube.com/watch?v=s_f-KK140vM& NR=1 (1 May 2010).
3. A demo of Mobile Recovery System can be seen at: http://www.youtube.com/watch?v=25eBn9 N20C4 (12 April 2010).
4. *Cell Phone SIM Card Spy: Spy On A Cellphone* can be seen at: http://www.youtube.com/watch?v=iUkJlO GgsqM&NR=1 (10 April 2010).
5. Learn how a cell phone can be intercepted at: http://www.youtube.com/watch?v=W28 SOiZ_-8c&NR=1 (11 April 2010).
6. Learn how to track a cell phone by SMS by visiting: http://www.youtube.com/watch?v=WWBvov RI15k&NR=1 (11 April 2010).
7. A short video clip on how to locate a mobile phone is available at: http://www.youtube.com/watch?v=QzwT1UNWyOk&NR=1 (9 May 2010).
8. A video demo of iPhone forensics demo can be accessed at: http://oreilly.com/catalog/ 9780596153595 (18 April 2010).
9. How *Mobile Cell Phone Number Tracking Tracing* is done can be seen through a video clip (especially for locating small children who move with a mobile phone) at: http://www.youtube.com/watch?v=hZKfNRxdUeI&feature=related (13 April 2010).
10. *Cost of Forensics* is explained in the video clip in the following link: http://www.youtube.com/watch?v=ZywiP 4l3ee4 (14 April 2010).

Chapter 9: Cybersecurity: Organizational Implications

References

[1] Below are the links to Nina Gogbole's talk about *Workforce Mobility Challenges and Issues.* The first link below is about Nina Godbole's talk on the topic of "*Working From Home: Myths and Truths*" and the second link is where you will find the copy of the article in PCQuest February 2010 issue.
http://pcquest.ciol.com/content/techtrends/2010/110010806.asp (7 August 2010).
http://pcquest.ciol.com/content/topstories/2010/110020105.asp (7 August 2020).
The pdf copy of Nina Godbole's presentation at the PCQuest SummIT 2009 talk can be downloaded at:
http://pcquest.ciol.com/infrasummit/2009/presentation/Nina-WorkForceMobility5B DelegateCopy-PCQuest%20SummIT%202009%5D.pdf (7 August 2010).

[2] The following link on Top 5 Insider Attacks of 2009 is available at: http://www.networkworld.com/podcasts/panorama/2009/

121609pan-insideattacks.html (1 August 2010). There is an audio MP3 downloadable on this site.

[3] Following are the links quoted for *Websense Tool* mentioned in Section 9.3 (Web Threats for Organizations: The Evils and Perils).
Features of Websense Enterprise Edition are described at:
http://www.securitybrigade.com/products/websense/enterprise.php (12 September 2010).
To learn about *Websense Web Security Protection from Web-Based Threats*, visit:
http://www.guardsense.com/Web-Security.asp (13 Septebmer 2010).
Remote filtering features from Websense are described at:
http://www.ciol.com/Ciol-Techportal/content/Security/News/2005/205091962.asp (12 September 2010).
Read more about what is possible with Websense Remote Filtering Tool in the following URL:
http://www.ciol.com/Ciol-Techportal/content/Security/Interviews/2006/2060620505.asp (14 September 2010).

Further Reading

Additional Useful Web References

1. Five top cybersecurity risks are mentioned in the following link:
http://www.crn.com/news/security/220000395/five-top-cybersecurity-risks.htm (8 October 2010).
2. In the following link, there is a posting titled "Obama Cybersecurity Report Addresses Critical Infrastructure and Privacy Issues": http://www.wired.com/threatlevel/2009/05/5638/ (8 October 2010).
3. *Cyber Security Threat to India is Real* – this article can be accessed at:
http://news.rediff.com/special/2009/aug/05/cyber-security-threat-to-india-is-real.htm (8 October 2010).
4. "Cybersecurity in India: An Ignored World" – the article can be accessed at: http://www.crime-research.org/articles/Cybersecurity-India-Ignored-World/ (8 October 2010).
5. Like the "Big Brother" syndrome, for a very interesting topic whether the Government can know what kind of websites you are visiting, you can visit:
http://computer.howstuffworks.com/government-see-website2.htm (8 August 2010). In this link, on the middle, there is also a link to virus related video. You may run that at your own risk.
6. The *Top 10 Cyber Threats of 2009* are mentioned at: http://www.aakashjain.com/misc/10-cyber-threats-to-look-for-in-2009-648 (1 August 2010). Those threats are (a) collaboration tools, (b) virtualization, (c) Botnet, (d) cyber warfare, (e) phlashing attacks, (f) wireless attacks, (g) threats due to green computing, (h) cloud computing, (i) insider threats, (j) risks for OS other than Windows.
7. In the following link, there is a *US Government Report* about the likelihood of extremists increasing cyberattacks: http://www.fas.org/irp/eprint/leftwing.pdf (8 August 2010).
8. How much of work hours are spent surfing by UK employees? Read some interesting information about this at:
http://www.cbi.org.uk/ndbs/Press.nsf/0363c1f07c6ca12a8025671c00381cc7/94d596bf6bcd69708025745e003b722b?OpenDocument (9 August 2010).
9. Visit the following link for discussion blogs about "Social Media Security":
http://socialmediasecurity.com/ (28 August 2010).
10. *2010 Social Media Marketing Benchmark Report* can be read at:
http://www.marketingsherpa.com/SocialMedia Marketing2010EXE.pdf
(13 August 2010).
11. Following are links to some known companies that claim to provide *security solutions with the use of social media marketing*:
http://www.stonesoft.com/en/ (29 August 2010). A Finland-based security solutions company.
Information about *Social Media Monitoring Tools* can be found at:
http://www.toprankblog.com/2009/12/near-free-social-media-monitoring/ (29 August 2010).

12. *Social Media Marketing* – the following link can be used by those who are interested in reading the view of Rohit Bhargava about where social marketing media is heading. Rohit is a well-respected marketeer and -blogger and frequent speaker at conferences:
https://www.marketingprofs.com/login/join.asp?adref=rdblk&source=http%3A%2F%2Fwww%2Emarketingprofs%2Ecom%2F8%2Fgetting%2Dsocial%2Dwith%2Dsocial%2Dmedia%2Drohit%2Dbhargava%2Dcollier%2Easp (31 August 2010).

13. In reference to Section 9.7 (Protecting People's Privacy in the Organization), some useful weblinks are as follows:
In the following link: read the interesting story about what Nandan Nilekani is up to with 8 gizmos in a case, to give 1.2 billion Indian people an identity!

http://in.news.yahoo.com/48/20100830/804/tnl-with-8-gizmos-in-a-case-nilekani-set_1.html (29 August 2010).

"People" is the difficult link in InfoSec Chain. Access the document *People is the Key Challenge in InfoSec* – NASSCOM survey to support the point at:
http://www.dsci.in/images/pdf/People%20the%20key%20challenge%20in%20info%20security_Survey.pdf (29 August 2010).
In the following link, there is a view point on whether the Unique Identification Authority of India (UIDAI) legally constituted:
http://cyberlawsinindia.blogspot.com/ 2009/09/is-unique-identification-authority-of.html (29 August 2010).
For *Unique Identification Authority of India*, the Wikipedia note is worth reading at:
http://en.wikipedia.org/wiki/Unique_Identification_Authority_of_India (29 August 2010).
Information about *Multipurpose National Identity Card* is available at:
http://en.wikipedia.org/wiki/Multipurpose_National_Identity_Card (29 August 2010).

14. In reference to Section 9.9 (Incident Handling: An Essential Component of Cybersecurity), following are some useful weblinks:
Handling a Security Incident – a useful paper can be accessed at:
http://www.qaiworldwide.org/pdf_files/aug08_pw.pdf (4 October 2010).

15. Following are some useful links for cybersecurity standards:
To know more on cybersecurity standards, visit:
http://en.wikipedia.org/wiki/Cyber_security_standards (1 October 2010).

To know more on cybersecurity regulation, visit:
http://en.wikipedia.org/wiki/Cyber-security_regulation (1 October 2010).

To know more on Cybersecurity – WIKI, visit:
http://www.cybersecuritywiki.com/ (1 October 2010).

16. Following are some useful links about "anonymizers":
http://www.sonntag.cc/teaching/LTAEC_Budapest/Anonymizers/index.html (2 October 2010).
http://en.wikipedia.org/wiki/Anonymizer (2 October 2010).
http://www.livinginternet.com/i/is_anon_work.htm (2 October 2010).
http://www.livinginternet.com/i/is_anon.htm (2 October 2010).
http://www.ucertify.com/article/what-are-anonymizers.html (2 October 2010).
http://www.guard-privacy-and-online-security.com/free-proxy-anonymizers.html (2 October 2010).

17. A useful Wikipedia note about "proxy servers" is available at:
http://en.wikipedia.org/wiki/Proxy_server (5 October 2010).

18. In reference to *Incident Management* discussion in Section 9.9 the *2009 Annual Report of Indian Computer Emergency Response Team India (CERT-In)* can be accessed at:
http://www.cert-in.org.in/knowledgebase/annualreport/annualreport09.pdf (3 October 2010).
To know about ITIL Incident Mangement for Beginners, visit:
http://www.slideshare.net/agnihotry/itil-incident-managementfor--beginners (18 November 2010).
Read about Benefits of Incident Management at:
http://www.helpdesksurvival.com/Benefits of Incident-Management.html (18 November 2010).

Read about Incident Logging and Classification at:
http://itil.osiatis.es/ITIL_course/it_service_management/incident_management/process_incident_management/incident_logging_and_ classification.php (19 November 2010).

19. The *FISMA 2007 DRAFT about National Incident Management System* can be downloaded from the following link: http://www.fema.gov/pdf/emergency/nrf/nrf-nims.pdf (6 October 2010).
20. In the following link, there is a good article about *Incident Response Policies and Procedures*: http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1069767,00.html (4 October 2010).
21. *Security Standard: Computer Incident Handling Process* – A Plain English Guide providing explanation and illustration of this standard can be found at: http://security.rit.edu/ (6 October 2010).
22. For Web 2.0 (mentioned in section 9.5.1) refer to the following links for additional information:
http://webdesign.about.com/od/web20/a/aa021306.htm (What is Web 2.) (17 November 2010).
http://www.vinfotech.com/web_2.0/index.html (Web 2.0 Design and Development) (17 November 2010).
http://www.dotnetuncle.com/Articles/Web-2-and-ASP-NET.aspx (Web 2.0 and ASP.NET (17 November 2010).
Video Clip to Web 2.0 Designing Tips (17 November 2010).

Books

1. Godbole, N. (2009) *Information Systems Security: Management: Metrics, Frameworks and Best Practices*, Chapters 2, 3, 4, 5, 36, 37 and 38, Wiley India, New Delhi.
2. Ibid, Chapter 14 (Intrusion Detection for Securing the Networks) and Chapter 15 (Firewalls for Network Protection).
3. Ibid, Chapter 11 (Network Security in Perspective) and Chapter 12 (Networking and Digital Communication Fundamentals).
4. Ibid, Chapter 31 (Privacy – Technological Impacts) – Section 31.2 (Privacy Implications of RFID Technology).
5. Ibid Chapter 27 (Laws and Legal Frameworks for Information Security) – Section 27.16 Building Security into Software/SDLC).
6. Ibid, Chapter 35 (Auditing for Security) – Section 35.9 (Technology-based Audits – Vulnerability Scanning and Penetration Testing).
7. Ibid Chapter 37 (Asset Management) – Section Managing Access to Organization's Information Assets (under Section 37.10).
8. Ibid Chapter 4 (Information Security Management in Organizations).
9. Ibid Chapter 34 (Business Continuity and Disaster Recovery Planning).
10. Ibid Chapter 21 (Security of Operating Systems) – Section 21.8 Patched Operating System.
11. Ibid Chapter 37 (Asset Management) – Section 37.3 Security Aspects in IT Asset Management.
12. Ibid Chapter 6 (Information Security Risk Analysis).
13. Ibid Chapter 29 (Privacy – Fundamental Concepts and Principles).
14. Ibid Chapter 16 (Virtual Private Networks for Security).
15. T. Mather, S. Kumaraswamy and S. Latif (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, O'Reilly. To read the article, visit: http://oreilly.com/catalog/9780596802769/ (1 July 2010).

Articles and Research Papers

1. Nina Godbole's article based on the talk delivered at the PCQuest SummIT conference, December 2009 can be read at: http://pcquest.ciol.com/infrasummit/2009/presentation/Nina-WorkForceMobility[Delegate Copy-PCQuest%20SummIT202009].pdf (1 July 2010).
2. The DSCI 2009 study on *State of Data Security and Privacy in the Indian Industry* can be accessed at: http://www.naavi.org/cl_editorial_10/data_security_survey_2009_report_final_30th_dec_2009.pdf (1 October 2010).
3. Vicky Shah's article about *Security Incident Handling and Dealing with Law Enforcement Agencies* can be read at: http://searchsecurity.techtarget.in/tip/Security-incident-handling-and-dealing-with-law–enforcement-agencies (3 October 2010).

4. In the following link you can find guidance on *Customizing the Handling of an Unauthorized Access Incident*: http://www.qaiworldwide.org/pdf_files/sept08_pw.pdf (8 October 2010).
5. United States Government Accounting Office (GAO) 2005 comprehensive report on *Emerging Cyber Security Threats and Issues* is available at the following link: http://www.au.af.mil/au/awc/awcgate/gao/d05231.pdf (8 October 2010).