International Journal on New Computer Architectures and Their Applications (IJNCAA) 2(1): 127-137
The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2220-9085)

Cyber Forensics: Computer Security and Incident Response

Virginiah Sekgwathe[1], Mohammad Talib[2]
[1]Directorate on Corruption and Economic Crime, Gaborone, BOTSWANA
veesek@gmail.com
[2]Department of Computer Science, University of Botswana, BOTSWANA
talib@mopipi.ub.bw

ABSTRACT

The intensification of Information and Communications Technology usage in all facets of life exceedingly amplify the incidents of information security policy breaches, cyber crimes, fraud, commercial crimes, cyber laundering etc, hence require a well developed approach to tackle these incidents in order to realize legally defensible digital evidence. Since electronic evidence is fragile and can easily be modified, finding this data, collecting, preserving, and presenting it properly in a court of law is the real challenge. There is a need for use of semantic analysis to discover underlying security policy requirements and internal power structures and institutionalization of anti cyber attack, anti-money-laundering and regulatory schemes. The first responders to cyber security incidents often than always are an organization ICT personnel who are technically sound though may be deficient in investigative skill. The scientific standards of cyber forensics dictates the procedure as it promotes objectivity, a precise and well documented analysis, particularly that the findings maybe used as evidence against the attacker. This paper aims to contribute to the advancement of the cyber forensics discipline with a view to assist the International community in combating this sophisticated, high-tech, dynamic ever changing phenomenon.

KEYWORDS

Cyber Forensics, Digital Evidence, Digital Security, Hacking, Risk Analysis, Prosecution, Incident response

1 INTRODUCTION

The computer crimes affect our daily lives and national security deeply, especially in this information epoch, the expanding wave of Internet connectivity and digital technologies bring us a lot of convenient, at the same time they also offer criminals more

chance to commit crime. Traditional law enforcement tools, methodologies and disciplines do not successfully address the detection [14], investigation and prosecution of cyber crime and this dictates for a pro-active approach, for timely international cooperation, and for effective public private partnerships to ensure the upper-hand over criminals.

Cyber forensics may be defined as the process of extracting and analyzing information and data from computers, network and storage medias and guaranteeing its accuracy and reliability [5] or the process of investigating what has occurred in a computer system, networks etc, how to prevent it from recurring, and establishing the extent of the damage [9]. With the rapid development of electronic commerce and Internet technology, cyber crimes have become more common and sophisticated. Incident Response for the purpose of this paper may be defined as structured approach to addressing and managing the aftermath of a security breach or attack and the countermeasures.

2 BACKGROUNDS

Cyber crime is not actually new the first recorded cyber crime took place in the year 1820. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom and allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened hence committed acts of sabotage to discourage Jacquard from further use of the new technology [1]. However, cyber crime is the latest and perhaps the most complicated problem in the cyber world, and comes in different forms and sizes unlike the conventional crime. This high-tech crime compelled the development of cyber forensics [8] and incident response to address cyber security.

2.1 Cyber Forensics Applicability

Technology is a double edged sword that can be used in economic sustainability, to assist in the arrest of cyber criminals etc, and there are various tools [6] that can assist law enforcement agencies in investigating cyber crime cases and in cyber crime evidence collection, drafting and creating hard evidence, however the same technology maybe used by cyber criminals to commit offences worse still the forensic tools may also be used by these cyber criminals to conceal their tracks for instance a criminal may use the disk wipers to clean the hard disks rendering forensic tools immobilized to recover evidence.

There are major investigative contingents that drive the requirements for forensic techniques and tools and for the purpose of this study emphasis is on five categories;

- Law Enforcement- focuses on gathering evidence
- Organizations, Business or e–commerce - economics for use in keeping the business on track using reasonably effective techniques and ensuring safe online purchasing.
- Academia- ensures accuracy of result driven from precise, repeatable methods.
- Prosecutions- elaboration of the analysis in a court of law
- Judiciary- scrutinizing the findings against judicial standards

When critical assets and systems come under attack, security professionals must be able to gather electronic evidence and utilize that evidence to bring to justice those who are responsible. Cyber criminals, honest and dishonest employees hide, wipe, disguise, conceal, encrypt [4] and destroy evidence from storage media using a variety of freeware, shareware and commercially available utility programs. Such attacks are often the results of multiple instances or can be just an indicator of something larger. Bank accounts can be hacked and credit card details can be stolen. When such cyber

crimes are committed, we need digital evidence [5] for investigators to catch the culprits. Though cyber forensics is doing a great deal to combat this crime, it faces many issues that have to be handled with care.

Computer specialists can draw on an array of methods for discovering data that resides in a Computer / PDA / SIM / Credit / Debit card or recovering deleted, encrypted, or damaged file information [12]. Any or all of this information may help during discovery, depositions, or actual litigation. The analysis could be used in recovering any sort of data from hard disks or other similar storage devices, data like documents, e-mails, images etc, there are other small electronic devices which would be used depending on the nature of the case such as PDA seizing devices, mobile SIM card readers to retrieve information from seized cell phone SIM cards, credit card readers, to retrieve information from credit/debit cards etc.

The anonymity of cyberspace makes identity tracing a significant problem which hinders investigations [20]. The ubiquity of computer technology throughout the civilian population will require full societal engagement if the International objective is a secure cyberspace. As the digital environment grows in scale and scope, so too will the need for a cyber civic culture to emerge to manage it.

2.2 Challenges Faced by the World

Traditionally, crime has been defined as an intentional violation of the legal code that is punishable by the law. Crime occurs within the boundaries of a district, state, country that constitutes a specific jurisdiction [14]. For example, when a conventional case of fraud occurs [16], one of the important considerations is where the actual offense took place so that the appropriate jurisdiction for investigation and prosecution can be addressed. Law Enforcement officials need to know where the victim and offender came into contact with one another in the perpetration of the offense [19] so that investigative and prosecutorial authority can be determined.

The most distinct nature of cyber crime from traditional one is borderless and anonymous [17]. By the help of pervasive network technology cyber crime may cover areas, regions, and countries. For investigators, security professionals it is really hard to get the true picture of the whole crime process because of dispersed elements in different places. Since new cyber crimes arise by the leap development of telecommunication and information technologies, they must face such challenges with a totally different thought and technical skills.

The challenge, of course is actually finding this data, collecting, preserving, and presenting it in a manner acceptable in a court of law. It is simply the application of computer / PDA / SIM / credit / debit card investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. Almost every computer criminal is knowledgeable with computers; some of them are even professional in computer science. They know how to commit computer crimes without leaving a trace, hence computer forensic professionals [13] need higher level of computer science knowledge including hardware and software. They need to understand and be familiar with all kinds of computer forensic software and this is not always the case.

Though cyber crimes are on the rise, less of the reported cases result in conviction therefore cyber forensics is crucial to the outcome of such investigations. The changing world of technology presents a challenge for the courts to keep pace with new laws in addressing evidence and other legal issues involved. Computer forensic experts not only need to investigate and collect the criminal evidence [7] but also need to communicate the results clearly in the court. Actually, the Prosecutor and

Adjudicator (Judge, Magistrate and where applicable the Jury) may not understand computing quite well. Overlooking some of the technologies utilized in investigation, misunderstanding some jargons while prosecuting and passing judgments on such incidents, without proper understanding may lead to inconclusive results, wrong interpretations etc, and subsequently mistaken acquittal and or erroneous conviction of the culprits.

Organizations and business do not want to disclose the attacks they experienced, subsequently internally dealing with such incidents, more especially financial institutions (banks etc) for fear of disclosing vulnerabilities for further attacks, bad publicity, public loss of confidence and possibly losing clients. However if these organizations were assured that they will get professional assistance, from certified professionals [10], successful prosecution and adjudication they would be no fear of disclosure. This discipline is basically understood to belong to the non technical law enforcement group [9], however, there is no how the law enforcement agencies can fully understand the diverse technology in this field, let alone jargons used in this discipline without any proper learning from the academia. The advancement of technology, usage of Information and Communications technology in banking and all daily transactions by organizations, industries and government etc increases the chances of traditional criminals going cyber, becoming invisible [1], even the recent development in technology such as ubiquitous computing. This requires the protection of information and infrastructures that organizations, business, companies and industry invest on, using real time assessment and analysis of perceived and actual cyber attacks without the benefit of guaranteeing the victim computer or taking it off-line as in the law enforcement model [2], as this disrupt the business. However, improper handling of forensics data can destroy an entire case or bring an investigation to a halt, therefore data and information should be collected by a trained cyber forensic expert, this dictate for mission critical real-time systems to provide uniquely qualified team of professionals who can assist in this critical moment after a cyber incident, and certainly there is a shortage of professionals in this area.

If a country's law enforcing agencies have no system in place or procedures to collect or store the electronic evidence, cyber crimes will go unpunished and expert's work of investigation will also go wasted and inadmissible. Conversely in a networked environment cyber [6] criminals can easily evade conviction by acting from a country where the demeanor is either not a contravention of any legislation or not prosecuted due to outdated cyber law or possible no cyber law at all, or there is a high probability of unsuccessful prosecution.

2.3 Private-sectors' limits to guard against cyber crime

The primary responsibility for cyber crime in commercial fields such as cyber banking or e-commerce belongs to individual businesses. However, the reality is that it is not possible to place all the responsibility of cyber crime and security on the business or industry. The government must step in and devise a proper measure in response to cyber crime. However, a bigger problem is that cyber crime is not limited to just to private sector only but also to all individuals who have the opportunity to use technology children as young as five years inclusive. There are no boundaries, no divisions between the government, the industry, academia and the people, in the midst of these good citizens and heinous criminals coexist in the same cyber space.

Organizations may employ prevention methods to prevent hacking [11] by implementing policies since the largest threat is often from within an organization and ensure proper configured firewall protection to computer network as well as

intrusion detection and other filtering software conversely some organizations never consider this. The education of employers, while definitely an important protective measure, is not the only contribution that will be required from organizations.

3 CYBER SECURITY INCI-DENT RESPONSE

In today's multifaceted digital world it is inexorable to extensively prepare, plan and have well documented procedures and strategies in place for incident response, with the knowledge that the incident may be drastic and findings maybe presented before court and the criticality of the incident turnaround time.

3.1 Detection and Protection against Intrusion

The International communities need to be dedicated to fighting cybercrime and helping to protect your online experience. Not only do software vendors develop the world's leading security software to be used worldwide but some even conduct extensive research into the nature and construct of the subversive cybercriminal world. This knowledge is mostly shared internationally to provide global protection against an ever-changing battle ground. Internet Security and other utilities give business and individuals the power to deny cybercriminal attacks and keep them from wreaking devastation on business, family, finances, reputation, and even life.

The best protections are careful system design, the use of products to detect known viruses and system intrusions, and user education, and of course the use of Intrusion Detection System (IDS). Each organization's implementation of cyber security requirements should evolve as technology advances daily and new threats to security arise. The International cyber security is being threatened because an important element in establishing it is not being emphasized enough, citizen awareness and participation is lagging behind. Working against connected but weakly protected computer systems, hackers can steal information [9], make the systems malfunction by sending them false commands and corrupt the systems with bogus information.

Nonetheless, deterrence should be pursued as a mitigation strategy, because even limited accomplishments can prevent some crime incidents and provide some protection from an increasingly serious problem.

4 IMPLEMENTING CYBER ATTACK DETECTION TECHNIQUES

The best detection technique is the strength of the implemented security controls, since attackers always target vulnerabilities and weaknesses therefore security controls offer detection of the potential attacks, deterrence, prevention and corrective capabilities in addition to reduction of the attack probability and may minimize the impact of the attack.

For cyber crime to be detected a team of professionals [10] need to work together and these include but not limited to law enforcement agencies, cyber forensic scientist, lawyers, and computer security professionals also there is appalling need for organization to perform risk analysis and mitigation. Organizations should emphasize secure systems at development stage and software patching if some flaws are realized during systems usage. Detection helps organizations to determine whether or not someone attempted to break into the organization's most critical asset which is systems and communication infrastructure, and what they may have done, if the attempts were successful. Almost daily, new techniques and procedures are designed to provide information security professionals a better means of finding electronic evidence, collecting, preserving, and presenting it to

client management for potential use in the prosecution of cyber criminals.

A need has arisen for global synchronization of the laws especially binding business, organizations and industry to implement security in their systems and organizations failing to comply with the regulations be penalized. Legislation alone cannot adequately combat the prevalence of cyber crime we face today. Private industry want to protect their businesses and customers provide the first line of defense. The private sector is usually ahead of Government on the latest technology, and must be willing to cooperate with law enforcement agencies for this war to be won. Technology holds the key to the future, and private businesses are leading the way in innovation and products, but if left unchecked, cyber crime will stifle that progress thus suppress e-commerce.

5 COLLECTING AND PRESERVING DIGITAL EVIDENCE

While collecting electronic evidence, it is always best for law enforcement officers or security professionals to consider the rules of evidence to support an action against a cyber criminal. Admissibility of evidence and compliance with any existing standards for evidence admissibility and quality of evidence for which a strong evidence trail is indispensable.

Law enforcement agencies need training [14] on how to retrieve information from computer systems, networks, cell phones and other digital devices in a criminal investigation, the availability of tools that help first responders deal with crimes involving digital evidence such as digital pictures, and analysis of technology such as malware and botnets in relation to complex international cybercrime is a breakthrough.

The principle by which the cyber forensics is evaluated, accepted into legal proceedings and credited vary from one country to another and this challenges organization and law enforcement agencies inter-nationally and inhibit organizations from reporting cyber security incidents to relevant investigating authorities.

5.1 Cyber Forensics Process

The increase in computer-related crime has caused law-enforcement agencies to seize digital evidence in the form of network logs, text documents, videos and images. In specific cases like those involving terrorism [19], the need to extract and analyze every possible bit of evidence becomes crucial. Scientifically, the results of the cyber analysis should be able to withstand legal scrutiny. Details of imaging always play a crucial role in establishing the credibility of digital evidence in a cyber crime case.

When investigating the crime scene [15], the forensic experts can only see a computer, several telephone lines, etc. The computer, the network and the mobile device are only device that evidence can be detected from, digital evidence begins to play a significant role at this time, and this is the high-tech scene of crime that the likely non technical law enforcement [9] has to respond to. Knowledge of how to retrieve digital evidence is a prerequisite, how to recover deleted or damaged information, how to preserve digital evidence, etc. Also, Digital evidence, by its very nature, is very fragile and can be altered, damaged, or destroyed because of improper handling or examination. So it is important that digital evidence should be conducted by experienced computer forensic investigators. The expert then examines the digital evidence and gives a final report about the act complained of as a crime. This report is a determination of whether an act on a computer was a breach of any legislation or not. The report must be objective, based on indisputable facts, because law enforcers will connect the suspect beyond reasonable doubt to the crime, and this dictates for professional legal advice especially at this stage. The existence of a regulatory framework and laws catering for cyber

crimes in the country are quite different, what may constitute a crime may not necessarily be a crime in the country that the cyber criminal reside or instigated the crime.

6 RECOMMENDED PRO-BABLE SOLUTIONS

The best that the International community can do is defending humanity's digital rights to help them have complete control of their online experience, through annual training of the public on Cyber Security. The public equipped with this kind of information may know how to implement better online security and ultimately be safe and secure on cyber space.

When law enforcement agents enter computer crime scene, they must know where to look for useful information, where operations history is maintained, how files are deleted and how to use forensic tools [2] to gather or recover deleted files or damaged files. Moreover, computer forensic professionals must know how to protect and preserve digital evidence; they also need to know how to present the digital evidence in court. In this digital era, computer forensics field is in great need of this kind of professionals and this can only be afforded with proper and thorough training of all concerned being adjudicators, law enforcement agents and prosecutors.

Cyber criminals will go to great lengths to obscure their tracks, as such drawing a definitive map of cyber crime is the exact science and assuming any country has sole rights to any crime would be a mistake. The lack of continuity and completeness of evidence can compromise the legal position. It is also required that the court be satisfied that the evidence has not been modified and is absolutely reliable. For this, hi-tech technical facilities, production of access control measures, time stamps or other supporting evidence should be used for digital evidence integrity assurance.

There is dire need for constant review of current legislation on international level, an examination of how governments interact with the private sector and a consideration of the prospects for international cooperation and treaties. Although the world enjoys tremendous economic benefits from Internet development, the respective governments have to try to maintain tight control over the telecommunications industry, and the public usage of Internet, to fight escalating cyber crimes. In order for the world to win the war against cyber crime, there is an astounding need to establish a dedicated Cyber cell [20] in each country and region which will not primarily detect but also prevent various cyber crimes that are committed daily. It is also essential for countries around the globe, academia, business/ industry and the international community to come up with an International Cyber Research Unit to keep Best Practice, policies, training, let alone the Research and Development abreast with the ever changing technology.

The Business and or Industry, academia alike need better support and research on how to meet information security requirements as dictated by the legislation or regulatory agencies including the government. There is a need for better understanding that virtually no investigation, either civil or criminal, comes without digital evidence in some form. Clear reporting of crimes, and subsequent investigations, provide a basis for understanding the nature and extent of cyber crime problem. The development of a strategic approach to dealing with this International issue will allow investigators to collaborate better on investigations over the long term. Additionally, the development of policy will help to guide Investigators and Information Security professionals through the complicated process of cyber crime investigations and intrusion detection. This paper also calls for academic partnership between the academia, business/industry, judiciary and of course the law enforcement agencies in addressing the legal system, forensic curricula and even testing and reviewing the current forensic tools ultimately coming up with best feasible

solutions and the development of state of the art tools that may gather and analyze legally valid digital evidence.

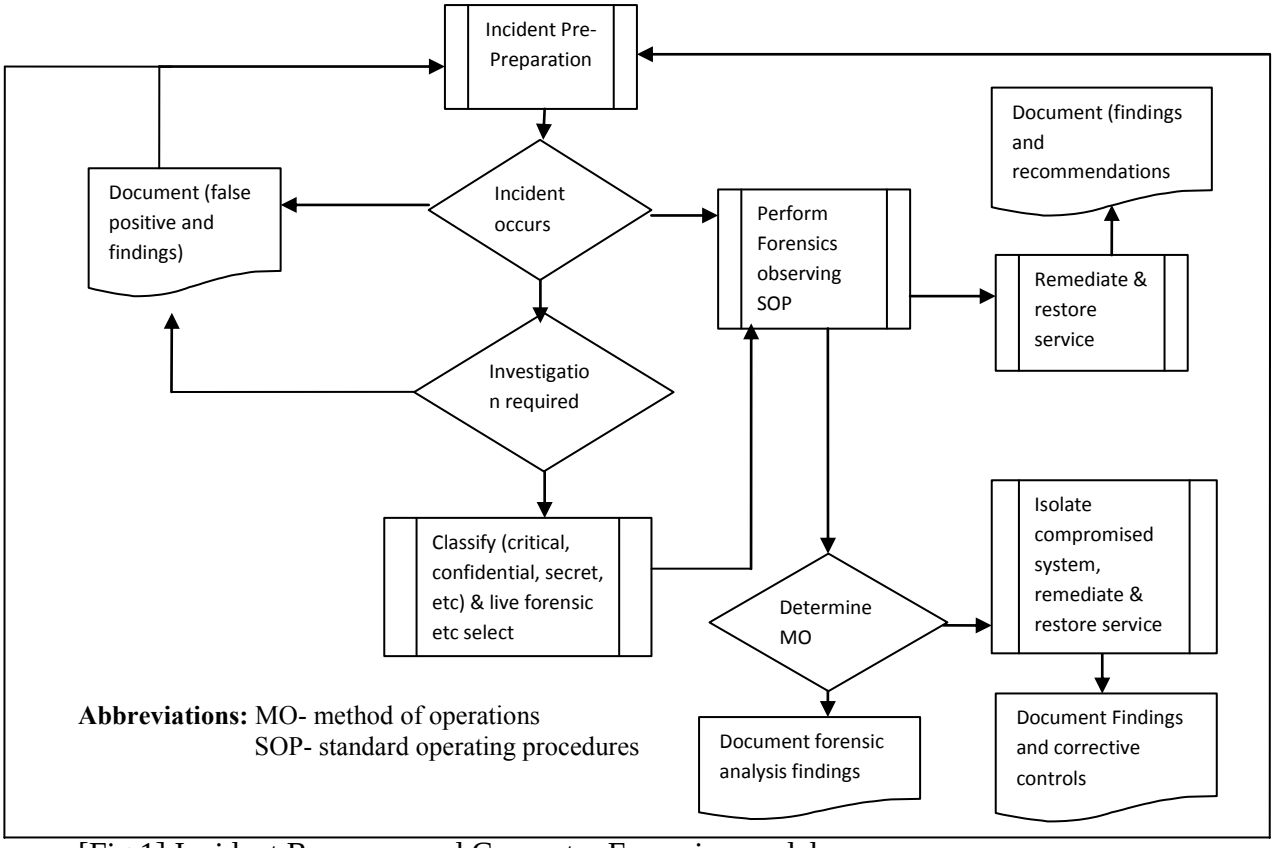
Some companies typically employ hackers certainly to guard against hacking and to deter computer crimes, even so companies and organizations need to be proactive to prevent victimization, regardless of their nature of business and this is one control measure this paper recommends to the international community in order to achieve deterrence. Business or Industry need to start reporting all their victimization incidents to the authorities for investigation and prosecution and this must be mandatory. The current situation, whereby many organizations refrain from reporting incidents to protect their own interests and thereby harming the interest of all businesses, need to be changed because, unless more incidents are reported, cyber crimes are unlikely to be controllable. The benefits and detriments of a mandatory reporting system are debatable, but a reporting requirement would certainly benefit international efforts to manage cybercrimes. This would put law enforcement agents in the position to decide which cases to devote their attention and resources to, rather than be dependent on the willingness of organizations to report their cases for investigations.

6.1 Proposed Cyber Forensics Model

For organizations, business and industry to guard against the intrusion, worm, automated attack against their systems, specific controls, plan of action for responding to attack or computer incident can greatly reduce the resultant cost and also saving them bad publicity, loss of public confidence and loss of business. For this reason the implementation of a Computer Incident Response Team whether formed with internal or external resources is obligatory, to guard against crisis and may have invaluable return on investments. This will only be the first step thereafter standard operating procedures and best practices need to be formulated and the technical research and development be put in place to ensure preparedness in dealing with the evolving, ever changing vulnerabilities.

The proposed model (Fig.1) aims at addressing the problems in both incident response and cyber forensics and its uniqueness is in the fact that it requires thorough documentation and corrective control measures. Incident response always commence with an ongoing phase of pre-incident preparation that takes place even before an occurrence of the incident or attack.

The model requires classification of incidents which will be in two parts the temperament of information and the nature and intricacy of the system involved. This will be contingent on the type of compromised systems to facilitate the medley of expertise to tackle the matter ultimately determine the forensics to be performed whether live or imaging or duplication or in other cases. The selected team may be compelled to perform data restoration etc, for the purpose of circumventing bad publicity the team composition is critical, to sustain so called need to know principle. The model also calls for isolation of the affected system which may include but not limited to network termination, disabling interface at operating system level, disabling switches and or hubs and quarantining of the affected computer or just removing the network cable.



[Fig.1] Incident Response and Computer Forensics model

7 CONCLUSIONS

Cyber crime is an international phenomenon that compels inter-national cooperation, international harmonization of legislation, and implementation of future technology provisions in actual legislation. There is a need for a balanced international strategy [4] to combat cybercrime also for round-the-clock cyber patrol and to equip the law enforcement officials with cyber forensic expertise to enable them to collect legally defensible digital evidence that will withstand legal scrutiny and subsequent successful prosecution. A need has arisen for the International community to work in partnership with industry, business, academia to address cybercrime and security, where challenges can be discussed and effective solutions, and ideas such as the implementation of cyber intelligence programs by organizations, government etc, that do not pose a threat to individual privacy developed.

8 REFERENCES

1. Amber Schroader et al, Computer Forensic Professionals http://www.informatik.unitrier.de/~ley/db/journals/di/di3.html Accessed on 26/10/2009
2. Amol Vyavhare, Cyber Forensic tools http://www.articleswave.com/computer-articles/top-cyber-forensic-tools.html Accessed on 02/11/2009
3. Barkha et al, Cyber Law and crimes, Law Booksellers, Publishers and Distributers, 2007
4. Cashmore C. et al, Business Information systems and strategies, British library Cataloguing in Publication Data, 1991
5. Chong K. et. Al., Digital Evidence search kit http://www.computer.org/portal/web/csdl/doi/10.1109/SADFE.2005.10 Accessed on 30/10/2009
6. Computer Forensics, Cybercrime and Steganography http://www.forensics.nl/links/ Accessed 02/11/2009
7. Computer Forensics World http://www.computerforensicsworld.com Accessed on 01/11/2009
8. Cyber Forensics http://www.cyberforensicsindia.com Accessed on 06/09/2009
9. Cyber Forensics: A Military Operations Perspective http://www.ijde.org.html Accessed on 11/09/2009

10. Computer Professionals for Social Diversity: Computer Crime Directory http://www.cpsr.org/cpsr/computercrime Accessed on 30/08/2009
11. Erickson, J. (2008). *Hacking: The art of exploitation* (2nd ed.) San Francisco: No Starch Press
12. Finny T. et al, Future challenge of cyber crime, September 2010 http://www.futuresworkinggroup.cos.ucf.edu/ Accessed on 31/03/2011
13. Gordon S. et al, (2006). On the definition and classification of cybercrime. *Journal of Computer Virology*, *2*, 13-20
14. Introduction to Cyber Crime http://www.csd.tsu.ru/WebDesign/libra3.nsf/FILE/cybercrime.pdf Accessed on 31/08/2009
15. Jay Albanese et al, Organized Crime, World Perspectives, Library of Cataloguing in Publication Data, 2003
16. John Madinger, Money Laundering, A guide for Criminal Investigators, 2nd Edition, Library of Cataloguing in Publication Data, 2006
17. Kantzavlou I, Computer Forensics http://net.educause.edu/ir/library/SWR0534 Accessed on 28/10/2009
18. Robinson A. et al, A Cyber forensics ontology: Creating a new approach to studying cyber forensics www.sciencedirect.com Accessed on 31/08/2009
19. R.W. Taylor. et al, Digital Crime and Digital Terrorism, Pearson Prentice Hall, 2006
20. Tewari R.K. et al, Computer Crime and Computer Forensics, Select Publishers, 2002