International Journal of Science and Technology
(STECH)
Bahir Dar- Ethiopia
Vol. 6 (1), S/No13, February, 2017: 59-73
ISSN: 2225-8590 (Print) ISSN 2227-5452 (Online)
DOI: http://dx.doi.org/10.4314/stech.v6i1.5

Computer Forensics Investigation; Implications for Improved Cyber Security in Nigeria

Chigozie-Okwum, Chioma C.
LearnTech4allInituative Nigeria
No 9 Mbonu Ojike Street, Ikenegbu, Owerri
Imo State, Nigeria
Phone: +2348038798153.
E-mail: chiomaokwum@gmail.com

Michael, Daniel O.
Department of Information and Communication Technology
Alvan Ikoku Federal College of Education, Owerri
Imo State, Nigeria

Ugboaja, Samuel G.
Department of Computer Science
Michael Okpara University of Agriculture, Umudike,
Abia State, Nigeria

Abstract

The rapid growth of computers, mobile devices and digital media has changed the way we communicate and interact in the techno-age. This rapid growth of technology has also birthed new ways of engaging in crimes in ways that seem easy but very difficult to trace, investigate and prosecute. Cyber-crimes are on the increase making the Nigerian cyber space very insecure. Computer forensics investigation is relatively new in Nigeria but promises to serve as a watch dog in curbing and checkmating cyber-crimes and ensuring cyber security. This paper aimed at examining the concepts of cyber-crime, cyber security and the implications of computer forensics investigation on cyber security in Nigeria.

Key Words: Computer Forensics, National Security, Cyber Security, Cyber Crime, Forensics Investigation

Introduction

Computer forensics is the discipline that uses computer investigation and analysis techniques, to collect evidence regarding what happened on a computer that is admissible in a court of law. Computer forensics requires a well-balanced combination of technical skills, legal acumen, and ethical conduct. Computer forensics specialists use powerful software tools to uncover data to be sorted through, and then must figure out the important facts and how to properly present them in a court of law. Cyber-crime rates are accelerating and computer forensics is the crucial discipline that has the power to impede the progress of these cyber criminals.

This paper aimed at explaining the concepts of computer forensics, cyber security, and cyber-crimes, while highlighting the implications of computer forensics to national cyber security.

The Concept of Computer Forensics

Margaret Rouse defined computer forensics as the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. Computer forensics examination performs structured investigation while maintaining documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it. Computer forensics (sometimes known as computer forensic science, Michael, (2000)), is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information. Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail. Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high-profile cases and is becoming widely accepted as reliable within court systems. With the passage of the evidence act of 2011 and the cybercrime bill of 2015, by the Nigerian National Assembly a new way is created for computer forensics, digital evidence and its admissibility in the Nigerian law enforcement and legal proceedings.

In the early 1980s personal computers became more accessible to consumers, leading to their increased use in criminal activity (for example, to help commit fraud). At the same time, several new computer crimes were recognized (such as hacking). The discipline of computer forensics emerged during this time as a method to recover and investigate digital evidence for use in court. Since then computer crime and computer related crime has grown, and has jumped 67% between 2002 and 2003, Leigland, (2004). Today computer forensics is used to investigate a wide variety of crime, including child pornography, fraud, espionage, cyber stalking, murder and rape. The discipline also features in civil proceedings as a form of information gathering (for example, Electronic discovery). Forensic techniques and expert knowledge are used to explain the current state of a digital artifact; such as a computer system, storage medium (e.g. hard disk or CD-ROM), an electronic document (e.g. an email message or JPEG image), Yasinsac et al, (2003).

Computer Forensics Investigation Procedure

Computer forensics investigations entails carrying out a structured investigation while documenting a chain of evidence to discover exactly what happened on a computer and who was responsible for it. The main priority of computer forensics is accuracy. Forensic practitioners must follow strict guidelines and maintain the highest standards of work ethics to achieve accuracy because emphasis must be on evidential integrity and security. A Computer Forensic investigation must follow a rigid set of methods to ensure that computer evidence is correctly obtained. These steps are outlined below:

1. Protect — Protect subject computer system from alteration, data corruption, virus infection, and physical damage.
2. Discover — Uncover all files: normal, hidden, deleted, encrypted, and password- protected.
3. Recover — Recover as many of the deleted files as possible.
4. Reveal — Reveal the contents of hidden and temporary files.
5. Access — Access the protected and encrypted files, if legal.
6. Analyze — Analyze all relevant data, including data located in unallocated file space and file slack.

7. Report — Print out a listing of all relevant files, and provide an overall opinion on the system examination.
8. Testimony — Provide expert testimony or consultation, if required.

Techniques in Computer Forensics Investigation

A number of techniques are used during computer forensics investigations, these include;

Cross-drive analysis: This is the forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and to perform anomaly detection (Garfinkel, 2006).

Live analysis: The examination of computers from within the operating system using custom forensics or existing sys-admin tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.

Deleted files: A common technique used in computer forensics is the recovery of deleted files. Modern forensic software have their own tools for recovering or carving out deleted data, Aaron et al, (2009). Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.

Stochastic forensics: This method uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.

Steganography: One of the techniques used to hide data is via steganography, the process of hiding data inside of a picture or digital image. An example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available.) While the image appears exactly the same, the hash changes as the data changes (Dunbar, 2001).

The Meaning of Cyberspace

Cyberspace as defined by the oxford dictionary is the notional environment in which communication over computer networks occurs. The term cyberspace became popular in the 1990’s when the uses of the internet, networking, and digital communication were all growing dramatically and the term cyberspace was able to represent the many new ideas and phenomena that were emerging (Strate, 1999). Cyberspace is a domain characterized by the use of electronic and electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures (Cox, 2016). In effect cyberspace can be thought of as the interconnection of human beings through computers and telecommunication, without regards to physical geography.

Cyber Security: An Overview

The Merriam-Webster Dictionary defines Cyber Security as measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack. According to TechTarget.com, Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies cyber security. Morrie (1998) refers to Cyber Security as the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures (Rouse, 2015). Cyber Security is of growing importance due to the increasing reliance on computer systems in most societies, and the growth of smart-devices, including smart phones, televisions and tiny devices, the Internet and wireless network such as Bluetooth and Wi-Fi.

Threats and Attacks to Cyber Security

To secure a computer system and ensure cyber security, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of the categories below:

Backdoors: Backdoor in a computer system is a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration. They may also have been added later by an authorized party to allow some legitimate access or by an attacker for malicious reasons; but regardless of the motives for their existence, they create vulnerability.

Denial-of-service attack: Denial of service attacks are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points – and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet, but a range of other techniques are possible including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

Direct-access attacks: An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, key-loggers, covert listening devices or using wireless mice. Even when the system is protected by standard security measures, these may be able to be by passed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and Trusted Platform Module are designed to prevent these attacks.

Eavesdropping: Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware.

Spoofing: Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security.

Tampering: Tampering describes a malicious modification of products. So-called "EvilMaid" attacks and security services planting of surveillance capability into routers are examples (Gallangher, 2014).

Privilege escalation: Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. So, for example a standard computer user may be able to fool the system into giving them access to restricted data; or even to "become root" and have full unrestricted access to a system.

Phishing: Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Preying on a victim's trusting; phishing can be classified as a form of social engineering.

Click Jacking: Click jacking, also known as "UI redress attack or User Interface redress attack", is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page. This is done using multiple transparent or opaque layers. The attacker is basically "hijacking" the clicks meant for the top-level page and routing them to some other irrelevant page, most likely owned by someone else. A similar technique can be used to hijack keystrokes. Carefully drafting a combination of stylesheets, i-frames, buttons and text boxes, a user can be led into believing that they are typing the password or other information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

Social engineering: Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer. A popular and profitable cyber scam involves fake CEO emails sent to accounting and finance departments.

Cybercrimes

The growth of the threat of cyber-crime has outpaced that of other cyber security threats. Nowadays cyber criminals are increasingly skilful at gaining unnoticed access and maintaining a relentless low profile. In the meantime, many organizations may be leaving themselves susceptible to cyber-crime based on a false sense of security, using agile security tools and processes. Many fail to recognize cybercrimes in their IT environments and misallocating limited resources to minor threats.

Cyber-crime may be committed irrespective of organizations trying to prevent hackers and blocking pornography. This has generated major risk exposure, including exposure to financial losses, regulatory issues, data loss, damage to brand, and loss of client and public assurance.

According to Manali (2012), computer crimes are criminal activities, which involve the use of information technology to gain an illegal or an unauthorized access to a computer system with intent of damaging, deleting or altering computer data. Computer crimes also include the activities such as electronic frauds, misuse of devices, identity theft and data as well as system interference. Computer crimes may not necessarily involve damage to physical property. They rather include the manipulation of confidential data and critical information. Computer crimes involve activities of software theft, wherein the privacy of the users is hampered. These criminal activities involve the breach of human and information privacy, as also the theft and illegal alteration of system critical information. The different types of computer crimes have necessitated the introduction and use of newer and more effective security measures.

Cyber-crimes refer to criminal offenses that have been created, committed or made possible by the advent of computer technology, or a traditional crime which has been so transformed by the use of a computer that law enforcement investigators need a basic understanding of computers in order to investigate the crime. There are two distinct sub-categories: Computer Crime and Computer-related Crime. Computer crime refers to any crime that involves a computer and a network. Moore, (2005) argued that the computer may have been used in the commission of a crime, or it may be the target as also supported by Warren et al (2002)**.** According to Mann (2011) Cyber-crime refers to criminal exploitation of the Internet. Jaishankar (2011), defined cybercrimes as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones such as SMS or MMS. Such crimes may threaten a nation's security and financial health. Govil (2007) regarded Cybercrime as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Cyber-crimes describe criminal activity in which the computer or network is a necessary part of the crime.

From these definitions, it is evident that the computer is the key source of cyber-crime. Cyber-crime is increasing in the list of internet-Aided offenses. This crime is almost overtaking street crimes, because street crime is almost contained and may soon be regarded as the thing of the past. Street crimes do take place but computer crime is more expedient. Cyber-crime has demonstrated to be accurate, easy, and reliable; detection is difficult and hence it has become hard to prevent it.

In early 2016, the FBI reported that social engineering and associated cyber-crimes, cost US businesses more than $2bn in about two years (Scannell, 2016). As Internet usage is growing daily the world is coming closer. The World Wide Web sounds like a vast phenomenon but surprisingly one of its qualities is bringing the world closer making it a smaller place to live in for its users. However, it has also managed to create another problem for people who spend long hours browsing the Cyber World – which is cyber-crimes. While law enforcement agencies are trying to tackle this problem, cyber-crime is growing steadily and many people have become victims of hacking, theft, identity theft and malicious software.

Categories of Cyber Crime

Cyber-crimes can be principally divided into three major categories, Cyber-crimes against persons, Cyber-crimes against property, Cyber-crimes against government. All these Cyber-crime categories affect us in one way or another. Cyber-crimes are broadly categorized into three categories, namely crime against

1. Individual
2. Property
3. Government

Each category can use a variety of methods and the methods used vary from one criminal to another.

Individual: This type of cyber-crime can be in the form of cyber stalking, distributing pornography, trafficking and grooming. Today, law enforcement agencies are taking this category of cyber-crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

Property: Just like in the real world where a criminal can steal and rob, even in the cyber world criminals resort to stealing and robbing. In this case, they can steal a person's bank details and siphon off money; misuse the credit card to make numerous purchases online; run a scam to get naïve people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

Government: Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism. If successful, this category can wreak havoc and cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations.

Types of Cyber-Crimes

When any crime is committed over the Internet it is referred to as a cyber-crime. There are many types of cyber-crimes and the most common ones include but are not limited to -:

Hacking: This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

Intellectual Theft: This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the law enforcement agencies. Today, the justice system in Nigeria is addressing this cyber-crime and there are laws that prevent people from illegal downloading as stipulated in the just passed Cyber-crime Bill of 2015.

Cyber Stalking: This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Identity Theft: This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber-crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.

Malicious Software: These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

Child soliciting and Abuse: This is also a type of cyber-crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

Cyber Terrorism: this refers to the intentional use of computers, networks, and public internet to cause destruction and harm for personal objectives (Matusitz, 2005). These objectives may be political or ideological since this can be seen as a form of terrorism. Cyber terrorism includes acts of deliberate, large scale disruption of computer networks, especially personal computers connected to the internet by the means of tools such as computer viruses. Cyber terrorism also involves politically motivated use of computers and information technology to cause severe disruption and wide spread fear.

Cyber Espionage: Cyber Espionage is the use of computer networks to gain illicit access to confidential information, typically information held by a government or other organizations. Cyber espionage is also referred to as Cyber Spying. It entails the act of obtaining secrets without the permission of the holder of the information from individuals, competitors, rivals, groups, government and enemies for personal, economic, political or military advantage using on the internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware.

Causes of Cyber Crime

Wherever the rate of return on investment is high and the risk is low, you are bound to find people willing to take advantage of the situation. This is exactly what happens in cyber-crime. Accessing sensitive information and data and using it means a rich harvest of returns and catching such criminals is difficult. Hence, this has led to a rise in cyber-crime across the world.

Implications of Computer Forensics Investigations on Cybersecurity in Nigeria

Until cyber criminals in Nigeria are convinced that no matter how crafty they are or the expertise they possess, that their crimes can be forensically investigated and that they will possibly face long jail terms or huge fines, Nigerian cyber security will not be assured. It has been seen that most cyber criminals have a loose network wherein they collaborate and cooperate with one another. Unlike the real world, these criminals do not fight one another for supremacy or control. Instead they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals. While law enforcement agencies are trying to keep pace with cyber criminals, it is proving to be a Herculean task. This is primarily because the methods used by cyber criminals and technology keeps changing too quickly for law enforcement agencies to be effective. That is why commercial institutions and government organizations need to look at other methods of safeguarding themselves. One of the best ways to avoid being a victim of cyber-crimes and protecting your sensitive information is by making use of impenetrable security that uses a unified system of software and hardware to authenticate any information that is sent or accessed over the Internet. Secondly a formidable frame work should be put in place to track, detect, investigate and prosecute cyber-crimes, hence making it unsafe for cyber criminals to thrive. This is can be achieved if the computer forensics investigation profession and its practice is promoted in Nigeria

Once a threat to cyber security is detected, the computer forensics investigator and information security experts spring into action. An effective incident response procedure includes the following steps:

- **Identification** of the threat agent which hit the infrastructure.
- **Containment** of the threat, preventing it from moving laterally within the targeted infrastructure.
- **Forensic investigation** to identify the affected systems and the way the threat agent has penetrated the computer system.
- **Remediate/Recover** by restoring IT infrastructure back online and in production once forensics investigations are complete.
- **Report and share threat data** to higher management and share the data on the incident through dedicated platforms that allow rapid sharing of threat data with law enforcement and other companies.

In Nigeria, perpetrators of cyber-crimes engage in these activities because of the following

1. The huge financial benefits accruing from cyber-crimes.
2. Cyber-crimes attracted mild punishment as provided by law.
3. Cyber-crimes are always almost not properly investigated and prosecuted in Nigeria.
4. The cyber criminals have expert knowledge of how to manipulate and navigate through computer systems, networks and devices.

5. Hitherto to passage of the cyber-crime bill of 2015, the cyber criminals had a safe haven to operate as majority of their criminal activities were not considered criminal offences

6. The law enforcement agencies do not have the required expertise, technologies and techniques to thoroughly investigate and prosecute these cyber crimes

In other to catch a criminal, the best approach is to think like the criminal and be able to recreate the crime in other to better investigate the crime thoroughly and hence prosecute the criminal. Computer forensics investigators are trained to possess a high level of expertise and also ability to apply critical thinking in cyber-crime investigations. Computer forensics is still very new to the Nigerian landscape; it is still at its developmental stage. At the moment the burden of training computer forensics examiners is solely saddled by the Computer Forensics Institute of Nigeria. The result of this is that there is very little manpower in this field. The resultant effect of these pitfalls is that the Nigerian cyber space became very insecure. Cyber criminals from the world over now locate allies in Nigeria to aid and albeit them in their cyber-crimes. The increase in cyber insecurity has its negative impacts on the image of nation as a whole, even as it has its attaining financial loses as well.

According to Olayiwola (2012), in other to tackle cyber-crime and ensure national cyber security, organizational priorities should include creating awareness relating to security breaches, methods of combating them and training of more manpower in digital forensics and cyber security. Computer forensics is a tool for people who are interested in extending or perfecting their skills to defend against cyber-crimes, cyber threats and attacks and damaging acts. You cannot properly protect yourself from threats you do not understand. Computer forensics investigation ensures that vital evidences are not destroyed and evidences are not ruled out as inadmissible in court during prosecution of cyber criminals. Hence the need for capacity building and training of personnel in computer forensics, in other to advance the Nigerian national cyber security and the culture of security as a whole. Computer forensics is therefore the missing link between cyber-crime, its elimination and ensuring cyber security in Nigeria.

Conclusion

There is a widespread use of personal computers in businesses and homes. Government enterprises, agencies and companies are exchanging more information online than ever before, and high-tech crimes are increasing at a rapid rate. This creates more of a need for crime investigators to have access to computer based information. There is an increased awareness in the legal community of the need for computer forensic services to obtain successful prosecutions which could otherwise fail because of unsatisfactory equipment, procedures, or presentation in court. Computer forensics investigation therefore is the missing link between cyber-crimes, cyber criminals and achieving cyber security. The paper advocates greater attention to be focused on developing computer forensics practice and profession in Nigeria as this will help curb the excesses of cyber criminals. The resultant effect of this is increased national security.

References

Aaron, P., Cowen, D. & Davis. C. (2009). Hacking exposed: Computer forensics. Retrieved 27 August 2010 from http://www.mheducation.co.uk/9780071626774-emela-hacking-exposed-computer-forensics-secrets-solutions.

Bassette, R., Bass, L., & O'Brien, P. (2006). Computer forensics: An essential ingredient for cyber security. *Journal of Information Science and Technology, Vol 3,* No 1, ISSN 1545-0287.

Dunbar, B. (2001). A detailed look at Steganographic techniques and their use in an Open-Systems Environment. SANS Institute InfoSec Reading Room, retrieved on 12/9/16, from https://www.sans.org>covert>detailed.

Gallagher, Sean, (2014). Photos of an NSA "upgrade" factory show Cisco router getting implant. Ars Technica. Retrieved August 3, 2014, from https://arstechnica.com.

Garfinkel, S. (2006). Forensic Feature Extraction and Cross-Drive Analysis. Proceedings of the Digital Forensics Conference, 2006, Aug 14-16, Lafayette, Indiana, USA, Vol 3, pp 71-81.

Gasser, M. (1988). *Building a secure computer system.* New York, USA: Van Nostrand Reinhold.

Govil, J. (2007). Ramifications of cyber-crime and suggestive preventive measures. *IEEE, 43 (4),* pp. 610-615.

Federal Trade Commission (2006). Identity theft survey report, P2. Retrieved from www.ftc.gov>reports-federal-trade-report-prepared-commission-synovate. Retrieved on 7th may 2016.

Jaishankar K., Sankary, V. Uma (2006). Cyber Stalking: A Global Menace in the Information Super Highway. Retrieved 21, March, 2012 from http://www.erces.com/journal/articles/archives/volume2/v03/v02.htm.

Jefferey, C. (2016). What is cyberspace. Retrieved on 7th May 2016, from http://searchsoa.techtarget.com/definition/cyberspace.

Leigland, R. (2004). A formalization of digital forensics. International Journal of Digital Evidence, fall 2004, Volume, Issue 2, pp 1-32, Extracted from www.ijde.org, on 7/1/17.

Manali, O. (2012). Types of computer crimes. Retrieved 21, March, 2012 from –http://www.buzzle.com/articles/types-of-computer-crimes.html.

Matusitz, J. (2005). Cyber terrorism. *American Foreign Policy Interests 2*: 137-147.

Moore, R. (2005). *Cybercrime: Investigating high-technology computer crime*. Cleveland, Mississippi: Anderson Publishing.

Noblett, M. G., Pollitt, M. M. & Presley, L. A. (2000). Recovering and examining computer forensic evidence. Retrieved 26 July 2010' from https://www.merlot.org>view material.

Olayiwola, P. O. (2012). Information security and framework and national cyber security. Paper presented at the conference on regulatory imperatives for cyber-crime and cyber security in Nigeria. 5th march 2012.

Pierluigi, P. (2014). *Preventing and recovering from cyber-crime. The state of security*. Nov 4 2014 edition. Tripwire, Inc, Portland, Oregun, USA.

Rotich, E. K., Metto, S. K., Siele, L., & Muketha, G. M. (2014). A survey of cyber-crime perpetration and prevention: A review and model for cyber-crime prevention. Murarga's University of Technology Institutional Repository, retrieved on 12th June 2016, from http://help.handle.net123456789/264.

Rouse, M. (2015). Social engineering definition. TechTarget. Retrieved 6 September 2015, from www.whatis.techtarget.com/definition/social engineering.

Scannell, K. (24 Feb, 2016). CEO email scam costs companies $2bn. *Financial Times*. Retrieved 7 May 2016, from https://www.ft.com>content.

Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication. Vol 63* No 3, pp382-412.

Warren, G. Kruse, J., & Heiser, G. (2002). *Computer forensics: Incident response essentials.* Boston, Massachusetts, USA: Addison-Wesley, Pearson Education, Pearson Inc, p. 392.

Woodie, A. (2016). Why ONI may be our best hope for cyber security now. Retrieved 13 July 2016, from www.datanami.com.

Yasinsac, A., Erbacher, R. F., Marks, D. G., & Pollitt, M. M. (2003). Computer forensics education. *IEEE Security & Privacy*. Retrieved on 12 May 2016, from cites every.ist.psu.edu>view doc>download.

Ziff, D. (2015). Definition of computer security. *Encyclopedia. PCMag.* Retrieved 6 September 2015 from www.pcmag.com