Cyber Security Understanding Cyber Crimes Computer Forensics And Legal Perspectives

Scene of the Cybercrime
Understanding and Managing Cybercrime
The Transnational Dimension of Cyber Crime and Terrorism
Transformational Dimensions of Cyber Crime
The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices
Prevention and Detection of Cyber Crimes
Cyber Crime Investigations
Cyber Crime, Security and Digital Intelligence
A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats
Cyber security mastery training guide
A Simple Plant to Protect You and Your Family from Cybercrimes
Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors
The Transformation of Crime in the Information Age
CyberForensics
Computer Networking and Cybersecurity
Cyber Security in Tanzania
Placing the Suspect Behind the Keyboard
Modern Principles, Practices, and Algorithms
Cyber Crime and Cyber Terrorism Investigator's Handbook
Understand the Role of Cybersecurity, Its Importance and Modern Techniques Used by Cybersecurity Professionals (English Edition)
Cyber Security
An Introduction
The Cybersecurity Self-Help Guide
Understanding Cybercrime
Introduction To Cyber Forensic Psychology: Understanding The Mind Of The Cyber Deviant Perpetrators
Applications and Perspectives
Crime, Conflict and Security in Cyberspace
Cyber Security Policy Guidebook
How to Avoid and Recover from Cybercrime
Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives
Cybercrimes: A Multidisciplinary Analysis
Cyber crime strategy
Cybercrime and Society
International and Transnational Crime and Justice
Cybercrime

Understanding Information Security Investigations
Cybercrime Investigations
Phenomena, Challenges and Legal Response
Computer Forensics and Cyber Crime

POWERS HAROLD

Scene of the Cybercrime Routledge
Cyberspace, Cybersecurity, and CybercrimeSAGE Publications
Understanding and Managing Cybercrime IGI Global
Written by a former NYPD cyber cop, this is the only book available that discusses the hard questions cyber crime investigators are asking. The book begins with the chapter “What is Cyber Crime? This introductory chapter describes the most common challenges faced by cyber investigators today. The following chapters discuss the methodologies behind cyber investigations; and frequently encountered pitfalls. Issues relating to cyber crime definitions, the electronic crime scene, computer forensics, and preparing and presenting a cyber crime investigation in court will be examined. Not only will these topics be generally be discussed and explained for the novice, but the hard questions —the questions that have the power to divide this community— will also be examined in a comprehensive and thoughtful manner. This book will serve as a foundational text for the cyber crime community to begin to move past current difficulties into its next evolution. This book has been written by a retired NYPD cyber cop, who has worked many high-profile computer crime cases Discusses the complex relationship between the public and private sector with regards to cyber crime Provides essential information for IT security professionals and first responders on maintaining chain of evidence
Forefront Books
Technological advancement saves time, ease of mobility, providing better communication means, cost efficiency, improved banking, better learning techniques, though safety and security are still questionable in aspects mentioned above. Cyber-attacks, crime, fraudulent are still increasing in recent years. Today, cyber security is widely viewed as a matter of pressing national importance. Many elements of cyberspace are notoriously vulnerable to an expanding range of attacks by a spectrum of hackers, criminals and terrorists. This book aims to collect the information both thematic as well as research-oriented from various personnel working in the various fields having different experiences to provide the essentials regarding what Cyber security is really about and not the perception of it being related purely to hacking activity. It will provide the fundamental considerations for those who are interested in or thinking of changing career into the field of Cyber Security. It will also improve a reader’s understanding of key terminology commonly used, nowadays, surrounding internet issues as they arise. The focus of the authors of various chapters in this book is on cyber security, cyber attacks, cyber crime, cloud security, cyber law, protection of women and children in cyber world & cyber space, analysis of cyber feminist campaign, data privacy and security issues in cloud computing, Mobile or Media addiction, Ransomewares, social networking, threats and impacts of cyber security.
The Transnational Dimension of Cyber Crime and Terrorism Syngress
Provides a key textbook on the nature of international and transnational crimes and the delivery of justice for crime control and prevention.
Transformational Dimensions of Cyber Crime Estalontech
The leading introduction to computer crime and forensicsis now fully updated to reflect today's newest attacks, laws, and investigatory best practices. Packed with new case studies, examples, and statistics, Computer Forensics and Cyber Crime, Third Edition adds up-to-the-minute coverage of smartphones, cloud computing, GPS, Mac OS X, Linux, Stuxnet, cyberbullying, cyberterrorism, search and seizure, online gambling, and much more. Covers all forms of modern and traditional computer crime, defines all relevant terms, and explains all technical and legal concepts in plain English, so students can succeed even if they have no technical, legal, or investigatory background.
The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices CRC Press
Cybersecurity for Beginners KEY FEATURES ● In-depth coverage of cybersecurity concepts, vulnerabilities and detection mechanism. ● Cutting-edge coverage on frameworks, Intrusion detection methodologies and how to design cybersecurity infrastructure. ● Access to new tools, methodologies, frameworks and countermeasures developed for cybersecurity. DESCRIPTION Cybersecurity Fundamentals starts from the basics of data and information, includes detailed concepts of Information Security and Network Security, and shows the development of ‘Cybersecurity’ as an international problem. This book talks about how people started to explore the capabilities of Internet technologies to conduct crimes globally. It covers the framework for analyzing cyber costs that enables us to have an idea about the financial damages. It also covers various forms of cybercrime which people face in their day-to-day lives and feel cheated either financially or blackmailed emotionally. The book also demonstrates Intrusion Detection Systems and its various types and characteristics for the quick detection of intrusions in our digital infrastructure. This book elaborates on various traceback schemes and their classification as per the utility. Criminals use stepping stones to mislead tracebacking and to evade their detection. This book covers stepping-stones detection algorithms with active and passive monitoring. It also covers various shortfalls in the Internet structure and the possible DDoS flooding attacks that take place nowadays. WHAT YOU WILL LEARN ● Get to know Cybersecurity in Depth along with Information Security and Network Security. ● Build Intrusion Detection Systems from scratch for your enterprise protection. ● Explore Stepping Stone Detection Algorithms and put into real implementation. ● Learn to identify and monitor Flooding-based DDoS Attacks. WHO THIS BOOK IS FOR This book is useful for students pursuing B.Tech.(CS)/M.Tech.(CS),B.Tech.(IT)/M.Tech.(IT), B.Sc (CS)/M.Sc (CS), B.Sc (IT)/M.Sc (IT), and B.C.A/M.C.A. The content of this book

is important for novices who are interested to pursue their careers in cybersecurity. Anyone who is curious about Internet security and cybercrime can read this book too to enhance their knowledge. TABLE OF CONTENTS 1. Introduction to Cybersecurity 2. Cybersecurity Landscape and its Challenges 3. Information Security and Intrusion Detection System 4. Cybercrime Source Identification Techniques 5. Stepping-stone Detection and Tracing System 6. Infrastructural Vulnerabilities and DDoS Flooding Attacks

Prevention and Detection of Cyber Crimes K. Jaishankar
The reason as to why I decided to write this book is the fact that many of us lives with a belief that we have only four common domains in this world, which are land, sea, air and outer space. But currently due to the development of science and technology a fifth common domain has been created, and that is cyberspace. This new common domain creates a new environment for the commission of crimes known as cyber crimes. And because of its nature, it became difficult to deal with these natures of crimes. The widespread digital accessibility creates new opportunities for the unprincipled because the manners in which offenders commit crimes changed from traditional to digital means. A lot of currencies are lost by both businesses and consumers to computer-criminals. Fair enough, computers and networks can be used to harass victims or set them up for violent attacks such as to coordinate and carry out terrorist activities that threaten us all. Coming back to our country Tanzania, regrettably in many cases law enforcement institutions have insulated behind these criminals, deficient in the technology and the trained recruits to address this fresh and rising risk. To make things worse, old laws did not fairly prevent the crimes from being committed. Furthermore, new laws had not quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. It is from this book whereby the position of cyber security, prevention and detection in Tanzania against cyber crimes, is determined. Actually, by looking at the Cyber Crime Act No.14 of 2015 on how the concepts above have been provided and implemented. Magalla Jr.Note de l'éditeur (FRENCH):Cet essai juridique en anglais traite du droit des nouvelles technologies de l'information et de la communication (NTIC) en Tanzanie, en particulier de la cybercriminalité, de sa définition, de sa prévention et de sa répression en fonction des formes multiples qu'elle prend dans le cyber espace. Après avoir dépeint le cadre général et international du droit des NTIC, l'auteur va décrire la situation tanzanienne. L'approche se veut à la fois doctrinale et pratique. Les principales sources du droit des NTIC sont décrites et l'ouvrage se termine sur des cas pratiques rencontrés dans des tribunaux tanzaniens.

Cyber Crime Investigations Prentice Hall
The history of cyber security is as old as the concept of the Internet. The internet is the web of networks and not all connected networks are capable of offering full secure communication and connectivity. Thus, arises the idea of cyber security through which both organisation data could be saved from lost or damaged. Therefore cyber security could be defined as the combination of the processes which are involved in saving an individual or organisation data both online and offline. Offline though does not seem to be connected with the term cyber. However, cyber-attacks that are launched even on a single computer connected with the Internet which otherwise might be connected with several other offline computers through the Intranet could damage the data on offline systems too.

Cyber Crime, Security and Digital Intelligence Newnes
Cyber attacks are on the rise. The media constantly report about data breaches and increasingly sophisticated cybercrime. Even governments are affected. At the same time, it is obvious that technology alone cannot solve the problem. What can countries do? Which issues can be addressed by policies and legislation? How to draft a good law? The report assists countries in understanding what cybercrime is about, what the challenges are in fighting such crime and supports them in drafting policies and laws.

A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats Elsevier
Since 2017 ,the global cyber arena has been occasionally hit by unprecedented cyber-crimes, with many data breaches, ransomware attacks, and even sophisticated state-sponsored cyber-attacks. The pace of cybersecurity growth is likely to continue in the upcoming years as industries invest heavily in security solutions to meet the ever-expanding range of threats and requirements. Nearly 68 per cent of business leaders agree global cybersecurity threats are on the rise. Cybercrimes are now an everyday concern for businesses. Cybersecurity statistics indicate a significant rise in data breaches and hacking, most of which involve workplace devices. Many organizations have poor security practices, making them vulnerable to cyber threats. And this is exacerbated by the presence of a global pandemic. Look at some cybersecurity industry statistics, so you'll know the state of today's cybersecurity and why you need to gear up your efforts to protect your systems: The global cybersecurity market is expected to be worth $352.25 billion, with an annual growth rate of 14.5%, by 2026 (Mordor Intelligence, 2020). Losses from cybercrime damages are expected to reach $6 trillion by 2021 (Cybercrime Magazine, 2020). Cybercrimes cost the world nearly $600 billion each year, equivalent to 0.8% of the global GDP (Mordor Intelligence, 2020). Ransomware damage worldwide is expected to reach $21 billion by 2021 (Cybersecurity Ventures, 2021). The Cisco Cyber Security Reports show that 50 percent of large organizations with a workforce of more than 10,000 spend at least $1 million on security every year. The report also found that 43 percent spend between $250,000 and $999,999, while 7 percent spend less than $250,000. The volume of cybersecurity data involving cybercrimes worldwide will continue to grow exponentially. Cybercriminals will continue with their shadowy ways of coming up with novel and more sophisticated ways of attacking the vulnerabilities of digital systems, including typical business software applications. Everyone should proactively always protect his or her information. So, here we are with our Awesome course - Cyber Security Mastery Training Guide This guide will educate you about the system and data security in the COVID era, the different types of hacking, phishing attacks, malware, ransomware, and tips to prevent them. Further, it also educates on creating the perfect Cyber Security budget post-pandemic and how to deal with the increasing scope of threats and a lot more tips and tricks. Using the strategy and information provided in our Mastery Guide, you will ensure fool-proof protection and create a culture of safety and cyber security excellence in your organization. This guide is jampacked with intelligent information you can implement to help you improve your cyber security efforts against common threats allowing you to set up a robust protection system

Cyber security mastery training guide Humayun Bakht
Written by experts on the frontlines, Investigating Internet Crimes

provides seasoned and new investigators with the background and tools they need to investigate crime occurring in the online world. This invaluable guide provides step-by-step instructions for investigating Internet crimes, including locating, interpreting, understanding, collecting, and documenting online electronic evidence to benefit investigations. Cybercrime is the fastest growing area of crime as more criminals seek to exploit the speed, convenience and anonymity that the Internet provides to commit a diverse range of criminal activities. Today's online crime includes attacks against computer data and systems, identity theft, distribution of child pornography, penetration of online financial services, using social networks to commit crimes, and the deployment of viruses, botnets, and email scams such as phishing. Symantec's 2012 Norton Cybercrime Report stated that the world spent an estimated $110 billion to combat cybercrime, an average of nearly $200 per victim. Law enforcement agencies and corporate security officers around the world with the responsibility for enforcing, investigating and prosecuting cybercrime are overwhelmed, not only by the sheer number of crimes being committed but by a lack of adequate training material. This book provides that fundamental knowledge, including how to properly collect and document online evidence, trace IP addresses, and work undercover. Provides step-by-step instructions on how to investigate crimes online Covers how new software tools can assist in online investigations Discusses how to track down, interpret, and understand online electronic evidence to benefit investigations Details guidelines for collecting and documenting online evidence that can be presented in court

A Simple Plant to Protect You and Your Family from Cybercrimes Springer Science & Business Media

If you want to learn the basics of computer networking and how to protect yourself from cyber attacks, then keep reading... Two manuscripts in one book: Computer Networking: An All-in-One Beginner's Guide to Understanding Communications Systems, Network Security, Internet Connections, Cybersecurity and Hacking Cybersecurity: A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering This book delivers a variety of computer networking-related topics to be easily understood by beginners. It focuses on enabling you to create a strong foundation of concepts of some of the most popular topics in this area. We have provided the reader with a one-stop highway to learning about the fundamentals of computer networking, Internet connectivity, cybersecurity, and hacking. This book will have the following advantages: A formal yet informative tone, meaning it won't feel like a lecture. Straight-to-the-point presentation of ideas. Focus on key areas to help achieve optimized learning. Networking is a very important field of knowledge to which the average person may be oblivious, but it's something that is everywhere nowadays. In part 2 of this book, you will take a journey into the world of cybercrimes and cybersecurity. The information is designed to help you understand the different forms of hacking and what you can do to prevent being hacked. By the end of this part, you may decide to pursue a career in the domain of information security. In part 2, you will discover the following: The importance of cybersecurity. A brief history of cybercrime, the different types, and its evolution over the years. The various types of cyber-attacks executed over the Internet. 10 Types of Cyber hackers-the masterminds behind attacks. The secrets of phishing attacks and how you can protect yourself against them. The different kinds of malware that exist in the digital world. The fascinating tools to identify and tackle malware. Ransomware and how attackers leverage technology to make money. 9 security testing methods you can learn to do. Social engineering and how to identify a social engineering attack. Network Security, Web Application Security, and Smartphone security. Examples of different types of hacks and past incidents to emphasize the need for cybersecurity. The topics outlined in this book are delivered in a reader-friendly manner and in a language easy to understand, constantly piquing your interest so you will want to explore the topics presented even more. So if you want to learn about computer networking and cyber security in an efficient way, then scroll up and click the "add to cart" button!

Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors The Stationery Office

When it comes to computer crimes, the criminals got a big head start. But the law enforcement and IT security communities are now working diligently to develop the knowledge, skills, and tools to successfully investigate and prosecute Cybercrime cases. When the first edition of "Scene of the Cybercrime" published in 2002, it was one of the first books that educated IT security professionals and law enforcement how to fight Cybercrime. Over the past 5 years a great deal has changed in how computer crimes are perpetrated and subsequently investigated. Also, the IT security and law enforcement communities have dramatically improved their ability to deal with Cybercrime, largely as a result of increased spending and training. According to the 2006 Computer Security Institute's and FBI's joint Cybercrime report: 52% of companies reported unauthorized use of computer systems in the prior 12 months. Each of these incidents is a Cybecrime requiring a certain level of investigation and remediation. And in many cases, an investigation is mandates by federal compliance regulations such as Sarbanes-Oxley, HIPAA, or the Payment Card Industry (PCI) Data Security Standard. Scene of the Cybercrime, Second Edition is a completely revised and updated book which covers all of the technological, legal, and regulatory changes, which have occurred since the first edition. The book is written for dual audience; IT security professionals and members of law enforcement. It gives the technical experts a little peek into the law enforcement world, a highly structured environment where the "letter of the law" is paramount and procedures must be followed closely lest an investigation be contaminated and all the evidence collected rendered useless. It also provides law enforcement officers with an idea of some of the technical aspects of how cyber crimes are committed, and how technology can be used to track down and build a case against the criminals who commit them. Scene of the Cybercrime, Second Editions provides a roadmap that those on both sides of the table can use to navigate the legal and technical landscape to understand, prevent, detect, and successfully prosecute the criminal behavior that is as much a threat to the online community as "traditional" crime is to the neighborhoods in which we live. Also included is an all new chapter on Worldwide Forensics Acts and Laws. * Companion Web site provides custom tools and scripts, which readers can download for conducting digital, forensic investigations. * Special chapters outline how Cybercrime investigations must be reported and investigated by corporate IT staff to meet federal mandates from Sarbanes Oxley, and the Payment Card Industry (PCI) Data Security Standard * Details forensic investigative techniques for the most common operating systems (Windows, Linux and UNIX) as well as cutting edge devices including iPods, Blackberries, and cell phones.

The Transformation of Crime in the Information Age Elsevier
In order to enable general understanding and to foster the implementation of necessary support measures in organizations, this book describes the fundamental and conceptual aspects of cyberspace abuse. These aspects are logically and reasonably discussed in the fields related to cybercrime and cyberwarfare. The book illustrates differences between the two fields, perpetrators' activities, as well as the methods of investigating and fighting against attacks committed by perpetrators operating in cyberspace. The first chapter focuses on the understanding of cybercrime, i.e. the perpetrators, their motives and their organizations. Tools for implementing attacks are also briefly mentioned, however this book is not technical and does not intend to instruct readers about the technical aspects of cybercrime, but rather focuses on managerial views of cybercrime. Other sections of this chapter deal with the protection against attacks, fear, investigation and the cost of cybercrime. Relevant legislation and legal bodies, which are used in cybercrime, are briefly described at the end of the chapter. The second chapter deals with cyberwarfare and explains the difference between classic cybercrime and operations taking place in the modern inter-connected world. It tackles the following questions: who is committing cyberwarfare; who are the victims and who are the perpetrators? Countries which have an important role in cyberwarfare around the world, and the significant efforts being made to combat cyberwarfare on national and international levels, are mentioned. The common points of cybercrime and cyberwarfare, the methods used to protect against them and the vision of the future of cybercrime and cyberwarfare are briefly described at the end of the book. Contents 1. Cybercrime. 2. Cyberwarfare. About the Authors Igor Bernik is Vice Dean for Academic Affairs and Head of the Information Security Lab at the University of Maribor, Slovenia. He has written and contributed towards over 150 scientific articles and conference papers, and co-authored 4 books. His current research interests concern information/cybersecurity, cybercrime, cyberwarfare and cyberterrorism.

CyberForensics John Wiley & Sons
Recent developments in cyber security, crime, and forensics have attracted researcher and practitioner interests from technological, organizational and policy-making perspectives. Technological advances address challenges in information sharing, surveillance and analysis, but organizational advances are needed to foster collaboration between federal, state and local agencies as well as the private sector. Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives provides broad coverage of technical and socio-economic perspectives for utilizing information and communication technologies and developing practical solutions in cyber security, cyber crime and cyber forensics.

Computer Networking and Cybersecurity SAGE
Most books on cybercrime are written by national security or political experts, and rarely propose an integrated and comprehensive approach to cybercrime, cyber-terrorism, cyber-war and cyber-security. This work develops approaches to crucial cyber-security issues that are non-political, non-partisan, and non-governmental. It informs readers throug

Cyber Security in Tanzania Hoover Institution Press
The federal computer fraud and abuse statute, 18 U.S.C. 1030, outlaws conduct that victimizes computer systems. It is a cyber security law which protects federal computers, bank computers, and computers connected to the Internet. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision, but instead it fills cracks and gaps in the protection afforded by other federal criminal laws. This report provides a brief sketch of Section 1030 and some of its federal statutory companions, including the amendments found in the Identity Theft Enforcement and Restitution Act, P.L. 110-326. Extensive appendices. This is a print on demand publication.

Placing the Suspect Behind the Keyboard Springer Science & Business Media
Cybercrime is a complex and ever-changing phenomenon. This book offers a clear and engaging introduction to this fascinating subject by situating it in the wider context of social, political, cultural and economic change. Taking into account recent developments in social networking and mobile communications, this new edition tackles a range of themes spanning criminology, sociology, law, politics and cultural studies, including: - computer hacking - cyber-terrorism - piracy and intellectual property theft - financial fraud and identity theft - hate speech - internet pornography - online stalking - policing the internet - surveillance and censorship Complete with useful recommendations for further reading, incisive discussion questions and an updated glossary of key terms, Cybercrime and Society is an essential resource for all students and academics interested in cybercrime and the future of the Internet.

Modern Principles, Practices, and Algorithms BPB Publications
This edited book, Introduction to Cyber Forensic Psychology: Understanding the Mind of the Cyber Deviant Perpetrators, is the first of its kind in Singapore, which explores emerging cybercrimes and cyber enabled crimes.Utilising a forensic psychology perspective to examine the mind of the cyber deviant perpetrators as well as strategies for assessment, prevention, and interventions, this book seeks to tap on the valuable experiences and knowledge of leading forensic psychologists and behavioural scientists in Singapore.Some of the interesting trends discussed in this book include digital self-harm, stalkerware usage, livestreaming of crimes, online expression of hate and rebellion, attacks via smart devices, COVID-19 related scams and cyber vigilantism. Such insights would enhance our awareness about growing pervasiveness of cyber threats and showcase how behavioural sciences is a force-multiplier in complementing the existing technological solutions.

Cyber Crime and Cyber Terrorism Investigator's Handbook Vij Books India Pvt Ltd
This book presents a comprehensive study of different tools and techniques available to perform network forensics. Also, various aspects of network forensics are reviewed as well as related technologies and their limitations. This helps security practitioners and researchers in better understanding of the problem, current solution space, and future research scope to detect and investigate various network intrusions against such attacks efficiently. Forensic computing is rapidly gaining importance since the amount of crime involving digital systems is steadily increasing. Furthermore, the area is still underdeveloped and poses many technical and legal challenges. The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of online attacks. There are many reasons which are motivating the attackers to be fearless in carrying out the attacks. For example, the speed with which an attack can be carried out, the anonymity provided by the medium, nature of medium where digital information is stolen

without actually removing it, increased availability of potential victims and the global impact of the attacks are some of the aspects. Forensic analysis is performed at two different levels: Computer Forensics and Network Forensics. Computer forensics deals with the collection and analysis of data from computer systems, networks, communication streams and storage media in a manner admissible in a court of law. Network forensics deals with the capture, recording or analysis of network events in order to discover evidential information about the source of security attacks in a court of law. Network forensics is not another term for network security. It is an extended phase of network security as the data for forensic analysis are collected from security products like firewalls and intrusion detection systems. The results of this data analysis are utilized for investigating the attacks. Network forensics generally refers to the collection and analysis of network data such as network traffic, firewall logs, IDS logs, etc. Technically, it is a member of the already-existing and expanding the field of digital forensics. Analogously, network forensics is defined as "The use of scientifically proved techniques to collect, fuses, identifies, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities." Network forensics plays a significant role in the security of today's organizations. On the one hand, it helps to learn the details of external attacks ensuring similar future attacks are thwarted. Additionally, network forensics is essential for investigating insiders' abuses that constitute the second costliest type of attack within organizations. Finally, law enforcement requires network forensics for crimes in which a computer or digital system is either being the target of a crime or being used as a tool in carrying a crime. Network security protects the system against attack while network forensics focuses on recording evidence of the attack. Network security products are generalized and look for possible harmful behaviors. This monitoring is a continuous process and is performed all through the day. However, network forensics involves post mortem investigation of the attack and is initiated after crime notification. There are many tools which assist in capturing data transferred over the networks so that an attack or the malicious intent of the intrusions may be investigated. Similarly, various network forensic frameworks are proposed in the literature.