ATHABASCA UNIVERSITY

COMMON BODY OF KNOWLEDGE
FOR NETWORK FORENSIC SCIENCE

BY

LORAN DOUGLAS MACKOWETZKY

A project submitted in partial fulfillment

Of the requirements for the degree of

MASTER OF SCIENCE in INFORMATION SYSTEMS

Athabasca, Alberta

January, 2010

DEDICATION

I dedicate this to my loving wife, Barbara. Without your patience and support, I would have given up on a life long dream. Thank you Babs. I would like to thank my parents: Evelyn and John. They made sacrifices in their lives so my brother, Bryan, and I could follow our dreams. They were right. Dreams do come true.

ABSTRACT

The network forensic specialist's role is to preserve, identify, extract, and document computer evidence from disparate systems and to provide expert testimony in a court of law. The growing need for Network Forensic Specialists is outpacing the availability of university-trained graduates and, to meet the demand, universities are developing, and offering new computer-related forensic programs based on loosely defined skills. Without industry standards for qualifications, the current curriculum provides a hit-and-miss approach to producing qualified specialists. This paper proposes a different way to develop a university's curriculum by developing and implementing a Common Body of Knowledge (CBOK) for Network Forensic Science. The CBOK approach provides a common lexicon within the profession to discuss Network Forensic Science and to develop certification standards, which can become the foundation for curriculum development. The study has identified seven categories of knowledge for Network Forensics: Information Technology, Network Security, Law, Digital Forensics, Network Management, Network Forensics, and Information Assurance. The study discovers a relationship between digital forensics, network forensics, and information assurance that promotes a shareable common body of knowledge. The study concludes that the Network Forensics CBOK could be a starting point for a national or international standard for computer-related forensics certification and accreditation.

ACKNOWLEDGENTS

I would like to acknowledge the Canadian Information Professional Society and the Athabasca University for the agreement to allow those with the Canadian Information System Professional designation entrance into the MSIS program. It has given me an opportunity to complete a life-long dream. I would like to thank Dr. Harris Wang, to whom I am indebted, for the topic that he suggested for this study. I have found Network Forensics to be a new and exciting field of science to explore.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

In July 2009, hackers attacked multiple sites in the United States of America and South Korea in an attempt to steal information (Chang, 2009). By taking control of over tens of thousands of computers, the hacker performed a denial-of-service attack. Police Network Forensic Examiners reviewed the network forensic logs and were able to locate two dozen of the attacking computers. The police seized those computers and examined the malicious code for evidence.

The examiners discovered the purpose of this attack was to hide the true intent of the hacker. The hacker accessed specific computers and could have easily stolen or destroyed the files. Instead, the hacker produced a file containing a list of the computers' content and then sent the list to 416 computers in 59 countries.

Subsequently, the Police have been able to acquire twelve of those 416 computers. Unfortunately, the police suspect that the hacker used the computers to hold the file until it could be retrieved. The case is still under investigation.

E. Larry Lidz, a Senior Network Security Officer at the University of Chicago, reported the following incident in 2003 on the Educause website (www.educause.edu). The University of Chicago's network consists of 15,000 network devices. Concerned about the threat to security, the university formed the Network Security Center and began logging traffic through their Cisco routers. By using a distributive detection system, they were able to monitor network flows and successfully track down a person responsible for a denial-of-service attack. Even though they had insufficient evidence to act upon, they contacted the Secret Police and the Alaska State Police where the suspect lived. A

teenager denied the allegations but when presented with the evidence of the system logs, he confessed to the crime.

In use since 2003, Skype is a peer-to-peer voice (and video) over Internet protocol popular for connecting distant users over the Internet and is a considerable threat to the corporate network. Skype can bypass firewalls and pass through the network addressable translation unmonitored and, with the use of encryption, can avoid detection and blocking. Two Network Forensic Researchers took a forensic approach to these security risks and developed a set of socket-based detection and control policies for Skype traffic (Leung & Chan, 2007).

These are just a few examples of the work that Network Forensics Specialists do to track intruders and to keep networks operational. The field of Network Forensic Science is relatively new as compared to other forensic science fields. In 2007, Wyles and Reyes (p 3) provides a brief summary of forensic milestones: (a) Francis Galton (1822-1911) discovered finger printing, (b) Leone Lattes (1887 -1994) discovered blood groups, (c) Calvin Goddard (1891-1955) allowed firearms and bullet comparison as evidence, (d) Albert Osborn (1858- 1946) developed document examinations, and (e) Hans Gross (1847) – 1915) developed scientific study to conduct criminal investigations. Digital Forensics, the sibling of Network Forensics, has been around almost since the beginning of computers while Network Forensics emerged as the result of the last ten years of evolution in communication systems, which enabled the interconnecting of disparate computers (McGuire & Murff, 2006).

Research Question

Network Forensics Specialist is an emerging profession where the individual has to be multi-skilled to be effective. Network forensics originated within the police force for use in criminal investigations. At that time, the police had to train their specialists in-house primarily by on-the-job training because computer related forensic programs did not exist. With the proliferation of criminal activities dealing with computers, the police could not keep up with the demand for forensics specialists forcing them to outsource network forensics to civilian experts (Wassenaar & Woo & Wu, 2009).

Network Forensics is not only used for criminal investigations. Companies around the world are constantly under attack by amateur and professional hackers, and need trained specialists whose role is to monitor and prevent attacks. With training on network forensics software tools, they can incorporate the company's security policies on monitoring and prevention into the applications. The tools can alert the specialist of unusual activities that could indicate an attack is occurring. If an attacker is successful in infiltrating the company's security, network forensics plays an important role in the restoration of lost, damaged or destroyed data. Because of the new role for network forensics, there is a shift in training programs to expand beyond police forensic investigations to include training in real-time protection of companies against criminal behaviour (Qian, Joshi & Tipper & Krishanamurthy, 2007; Stahl, Carroll-Mayer & Norris, 2006).

What skills does a Network Forensic Specialist need to perform their role in investigations or for network security? Firstly, the person must be educated in forensic science (Malinowski, 2006). Forensic science is the application of science to law.

Forensics science deals with the physical evidence and the irrefutable proof gained by the application of known principles of science.

Secondly, the specialist must be proficient in digital forensics (McGuire & Murff, 2006). The steps in investigating digital forensics are preservation, identification, extraction, and documentation of computer evidence. It is critical for the specialist to have detailed working knowledge of computers, data storage mediums, and the network. With the widespread use of computers and networks, evidence has taken on a new form of electronically stored information. Digital evidence needs special procedures not typical of traditional forensics because the accessing of information can trigger a sequence of events that can alter or delete the information, corrupt the storage medium, or damage the device. The specialist has to replicate the source of the data, proving without a doubt the copy is the same as the original source, and that no one had the opportunity to tamper with the evidence.

What makes network forensic so different from digital forensics is the scope of the investigation which is no longer one computer and the collecting and preserving of evidence spans across a business network or globally through the Internet (Sitaraman & Venkatesan, 2006). The specialist needs training on network forensic tools to help investigate the system logs, and recreate the sequence of activities leading to, during and after the incident.

The specialists must be proficient in all aspects of information technology security (McGuire & Murff, 2006). Security is concerned about understanding the types of attacks, how attacks affect computers and networks, and how to prevent the attacks. Information security means protecting the information so that only authorized users have

access (Bogolea & Wijekumara, 2004). By understanding how security can protect the electronic data, forensic tools can be used for prevention and not just for investigation. By configuring the tools with the security policies, any deviation of the policies will cause an alert. The specialist must be able to protect, detect, and recover from external attacks.

The network forensics specialist must be knowledgeable in the law (Stahl et al, 2006). The law has strict procedures for acquiring, authenticating, and analysing digital evidence. While investigating computer crimes, the specialist needs to know what laws apply to what crime. Network forensics plays an important role in the presenting of evidence in court, and so, the understanding of the process and procedures for presenting evidence in court is critical.

The scope of knowledge for network forensics covers a wide spectrum of different skills and the legal perspective that binds them together: (a) software companies provide training on the tools, (b) police and security companies provide on-the-job-training, and (c) several universities offer courses in network forensics within a post-graduate degree. However, the degree is not a Network Forensic Science degree. The emergence of an accredited network forensics post-graduate degree is emerging at a few universities but research is still required to find the right spectrum and perspective of network forensics to align with the skill set (Malinowski, 2006).

The layers of specialists (Yasinsac, Erbacher, Marks, Pollit & Sommer, 2003) compound this issue. The entry-level examiner is trained only in operating the software tools while the professional level is trained in acquiring, authenticating, and analysing digital evidence. The policy maker's role is to manage the security policy and ensure the organization is in compliance. At the top are the network forensics researchers. Their

needs are advanced education that allows them to develop their research goals and to increase their knowledge of network forensics.

Network forensics is a part of forensic science and therefore the individual must be a scientist to perform forensics (Anderson, 2007). As such, universities should be the prime source of education. With a strong foundation on theories behind network forensics, the individual can be trained on-the-job with the software tools and fill any position within the network forensics specialist trade.

The growing need for Network Forensic Specialists is outpacing the availability of university-trained graduates. To meet the demand, universities are developing new computer related forensic programs based on loosely defined goals typically focused on the local target market such as police agencies or network security firms. Some universities are using case studies to look at existing programs for common requirements. This paper researches existing literature on Network Forensics to determine if a standard exists. The research question attempts to answer the following:

- Can a common body of knowledge be created for Network Forensic Science to establish a national or internal standard that can be used for Network Forensic Specialist certification and university curriculum accreditation;
- Can the common body of knowledge be validated against existing university curriculum; and
- Can an existing curriculum be modified or new curriculum be created using the common body of knowledge?

Research Goal

The research goal is to produce a Network Forensic Science's common body of knowledge for establishing certification and accreditation standards. To this date, no known certification exists for Network Forensics therefore the CBOK validation is against existing computer forensic related universities' curriculum. Once validated, the CBOK could be the foundation for development of an accredited post-graduate Forensic Science Degree.

The paper will explore network forensics from an analytical perspective to ascertain the skills needed by a network forensic specialist. The negative aspect of this paper is that network forensics is an evolving and expanding science. The time constraint of the paper restricts the development of the CBOK and, as a result, cannot be considered complete or authoritative.

Problem Statement

Today's world takes network forensics to a global scale and the demand for certified specialists exceeds the supply. Universities cannot keep up with the demand for network forensics since the requirements now go beyond criminal investigation and include corporate protect of information and government's national security.

Network Forensic Science is a field best performed by forensic scientists. However, because there is a lack of network forensic science programs, many Network forensics specialists are self-taught. They learn their trade by relying on initial training on network forensics software and hardware equipment and eventually become proficient through on-

the-job work experience. However, they lack the full academic understanding of network forensic science.

To ensure that there will a sufficient number of scientists to meet the growth expect in Network Forensics, universities must start offering accredited network forensics science programs (Wassenaar et al, 2009).

CHAPTER II

LITERARY REVIEW

Background

Many years ago, computer systems could only be stand-alone devices. Owners of the proprietary software would not share information that would create a common standard and the few existing standards did not allow disparate systems to communicate. The advent of the Internet has resolved these issues and any home computer can connect to any other computer system in the world.

However, this ease of access to the Internet has placed the world under the threat of an electronic attack. The illegal use of digital devices occurred because of the increased communication capabilities over the last 10 years (McGuire & Murff, 2006). The first recorded instances of criminal use of computers or hacking, as it is now known, were in the 1960s when inside workers sabotaged or manipulated mainframe computers. In the 1950s, the term “hacker” originated at the Masacheusetts Institute of Technology Artificial Intelligence Laboratory (Brenner, 2007). The term was used to denote a person who performed activities that were “for pure creativity and intellectual excitement” (Brenner, 2007, p 706). It was not until 1981 that network forensics played a key role in police investigations, which enabled them to arrest the first hacker. Ian Murphy, also known as “Captain Zap”, was charged and prosecuted for theft for altering the system time clocks so that the billing rate on an AT&T system would charge the lower evening rate during business hours (Brenner, 2007).

Rapidly, the attacks became more sophisticated and targeted larger groups or organizations. The first virus to affect personal computers was released in 1982 by a

ninth-grader (Brenner, 2007). In 1988, Robert Tappan Morris was the first person to release a worm (Brenner, 2007). The best-known case of computer theft occurred in 1994 when Vladimir Levin, a Russian hacker, stole millions of dollars from a bank account in New York. The International Council of Electronic Commerce Consultants (EC Council) states that a security breach will occur in eighty-five percent of all companies (Kleiman et al, 2007). As the threats continue to grow, so does the need for network forensic specialists.

Due to the financial impact of these threats, the police needed to be skilled in network forensics to find evidence to arrest the criminals. These were the first forensic examiners and they were highly trained to present evidence in a criminal case. Their focus was on a single computer, searching for evidence in the digital media. This is no longer the case. Network forensics includes detection and recovery from intruder attacks. The Internet and networks have given the attacker larger targets to focus their attention on. The attackers are using the Internet to attack a company's networks and they are often going without detection. When the intrusion is detected, the company's focus is the recovery of lost data and not prosecution of the culprit.

The information systems managers and administrators have a stake in discovering intrusions and minimizing damage (Endicott-Popovsky, Frincke & Taylor, 2007; Thomas & Forcht, 2004). The need for network forensics is no longer limited to the realm of law enforcement but now includes the corporate business.

The potential threat of terrorists using cyber crime has prompted a U.S. President in 2003 to state,"The cornerstone of American's cyberspace security strategy is and will remain a public-private partnership" (Mcguire & Murff, 2006, p 274). The universities

have to develop educational programs to provide digital and network forensics specialists to meet the demand in law enforcement agencies, corporations, and the government.

The Common Body of Knowledge

For the purpose of this study, the definition of a Network Forensics Specialist is an investigator who uses knowledge in forensics, law, computer and network systems, and network security to monitor, detect and trace intrusions on the network. When an intrusion occurs, the network forensic specialist can preserve, identify, extract and document computer evidence and is able to provide expert testimony in a court of law.

This study will consist of research covering the spectrum and perspective of network forensics. The information is broken down into modules to formulate a common body of knowledge (CBOK) in a format that is useful to develop a network forensics science certification and accreditation process. The common body of knowledge is a collection of knowledge and practices that are generally accepted (Duncan, 1996). Generally accepted infers that the knowledge and practices have widespread consensus about their value and usefulness.

The CBOK approach was chosen for the research study to provide a common lexicon within the profession to discuss Network Forensic Science. Many associations use a CBOK approach to identify the knowledge required to obtain certification in a given profession. The following are just a few of the many organizations that have a CBOK for certification purposes:

- Canadian Information Processing Society (www.cips.ca)
- Project Management Institute (www.pmi.org)
- International Council on System Engineering (http://g2sebok.incose.org/)

- International Institute of Business Analysis (http://www.theiiba.org/am/)

The remaining portion of the study will be broken down into the seven categories. Each category will consist of three parts (a) the rationale describes the research and the reasons for the category, (b) a brief description of the CBOK for the category, and (c) the skills in point form. This acts as a summary of the information.

The proposed Network Forensic Science CBOK consists of the following seven categories:

- Information Technology
- Network Security
- Law
- Digital Forensics
- Network Forensics
- Security Management
- Information Assurance

Information Technology

Rationale. The cornerstone for network forensics science is that the evidence must be irrefutable. In court, the legal defence will attempt to challenge (a) the authenticity of the evidence, (b) the reliability of the evidence, and (c) the creditability of the investigator. The Network Forensic Specialist must never provide opinions on evidence that exceeds his knowledge base (Wiles & Reyes, 2007). By doing so, his testimony may be tainted, the evidence may be thrown out, and suspicion may be placed on all of his other evidence. As a result, specialists must be well versed in the computer world to ensure they can provide irrefutable evidence.

In this study, all universities reviewed had all the computer, digital, and network forensic courses offered within a computer degree program (Bogolea & Wijekumara, 2004). Academia understands the importance of information technology in forensics. This alone implies that information technology (IT) is a crucial skill for the IT related forensic specialist and, for this reason, the first proposed category in the CBOK is Information Technology.

Information technology has been around for a long time and there are countless number of relating jobs and job descriptions. Finding information on skills is not difficult. The challenge is to understand what information technology skills are desirable to a network forensic scientist. There are many organizations in the world with IT standards. For the purpose of this study, the Canadian Information Systems Professionals Body of Knowledge (CIPS BOK) is used to lay out the basic information technology knowledge category with the computer architecture and network skills. The benefit is two-fold: the industry approved CIPS BOK, and the effort in summarizing the skill set has been reduced.

However, the skill set for forensics goes beyond the IT components. Network forensics specialists, as expert witnesses, must prove they have strong knowledge in storage media and operating systems (Wiles & Reyes, 2007). In-depth knowledge of the different operating systems provides the understanding of files types, directory structures, and system logs. The specialist examines the files to see if they are altered, destroyed, or hidden. By knowing the type of operating system under attack, the specialist can (a) begin the investigation on the storage media, the file, and data structures and (b) search for the signs of attacks and hidden information.

Overview. Information Technology covers the background knowledge that enables the network forensic specialist to develop an understanding of computer architecture, digital media, operating systems, and networks components. The specialist will apply the information technology knowledge for the purpose of performing digital and network forensics in the business, government, or police arenas.

Skills.

- Computer Architecture
    - Data Representation
    - Digital Logic
    - Input/Output Interfacing
    - Memory Systems
    - Process Organization
- Digital Media
    - Files
    - Hidden partitions
    - Slack Space
    - Swap File
    - Unallocated partitions
- Operation Systems
    - Linux
    - Windows
- Network
    - Digital Communications

- Errors
- Inter Networks
- Local Area Networks
- Network Security
- Wide Area Networks

Network Security

Rationale. Information was once store primarily on paper and physical security played the primary role in its protection from unauthorized access. The widespread use of computers has resulted in an unprecedented amount of information being stored electronically. A university study in 2001 indicates that over 93% of new information resides on digital media (Sitaraman & Venkatesan, 2006).

The combination of digital media and the electronic connecting of computers through the Internet provide attackers easier access. In 2004 alone, over 73% of organizations identified at least one attack on their computer systems while the remainder cannot detect that an attack occurred (Chen & Davis, 2006). With potential electronic access internally and externally, no longer can physical security protect information (Wiles & Reyes, 2007; Chen & Davis, 2006). Network Security is the next level of protection organizations must implement to ensure the confidentiality, integrity, and availability of their systems (Sitaraman & Venkatesan, 2006; Figg & Zhou, 2007)

There are four principles that are critical to Network Security and to Network Forensics that a specialist should know: (a) the risks, (b) the type of attacks, (c) how to detect an attack, and (d) how to prevent an attack.

Risks. It is imperative for an organization to understand that it is always at risk for

an attack and to be prepared to prevent or mitigate the risk. At one time, spies primarily existed to steal secrets from other countries. Today, spies steal intellectual property for profit (Wiles & Reyes, 2007). In many industries, stiff competition will tempt organizations to acquire stolen information that would give them a competitive advantage. In today's market, companies must protect their intellectual property and their infrastructure if they are to remain solvent and productive.

The attacker's target may not be specific to one computer. In fact, the impact can be global. Viruses, Worms and Trojans implant themselves onto unprotected computers and continue spreading and infecting other computers. A virus is computer code that makes copies of itself (Hansman & Hunt, 2005). When the virus encounters another system, it will copy itself onto that system. File sharing is a common and effective way to spread a virus.

A worm is different from a virus in that the worm will exploit security vulnerabilities and spread itself onto other computers. Worms do not need to transfer as part of a host (Hansman & Hunt, 2005). The Trojan is a program that the user mistakenly downloads and executes thinking it serves a useful function. The Trojan can lay dormant waiting for a trigger to perform its destructive behavior.

The network infrastructure and services provided can also be at risk. Attackers can force network equipment to fail or work incorrectly. By damaging the company's service networks, the outage interrupts the business's ability to do work. In this case, the goal of the attacker would be to cause a loss of business revenue.

Many companies do business via the Internet where the client must provide financial information to complete a transaction. These companies usually have a large

client base and are at risk to attackers who commit financial fraud. It is necessary for the company to provide a secure network by ensuring that every precaution was used to prevent an attack.

Not all attackers appear to have a malicious intent. However, an attacker's intrusion into the company's network obviously implies the system is not secure. If an attack is successful and becomes public knowledge, the company's reputation and financial security is compromised. Risk analysis is critical to the success of any security policies as it identifies and quantifies the risk. Understanding the risk will enable the specialist to ensure contingency and disaster recovery plans are developed and ready for use (Bogolea and Wijekumara, 2004).

Attacks. Chen and Davis describe in summary the different types of attacks. They indicate that the attackers are equally from internal and external sources. This implies that some attacks are coming from trusted and knowledgeable employees and the specialist needs to search for all types of attacks from all sources. Attacks can be summarized into four main categories:

- Probing: surveillance of a group of computers looking for vulnerabilities;
- DOS: denial of service by keeping the memory busy with activity; preventing legitimate users access to the resources;
- U2Su: Unauthorized access to super user (root) privileges; and
- R2L: Unauthorized access from a remote machine

Detection. Chen and Davis describe how the attackers will progress through these three steps within their attacks:

- Reconnaissance: Reconnaissance is the process of finding a target by using methods such as footprinting, active scanning, and war dialing to find public information on potential targets;
- Gaining Access: The intruders will attempt to gain access by using methods such as password cracking, session highjacking and sniffing. They attempt to gain illegal access to existing users accounts; and
- Cover-up: The intruders will evade detection by erasing evidence of their presence. Intruders use various methods such as rootkits, modifying logs and tunnelling.

Network Forensics specialists should be aware that illegal activity detected in any one of the steps would indicate the worst potential threat may have already occurred and they must investigate all unauthorized activities.

Protection. The goal of network security is to allow access to those that need the information and to deny access to those who do not. Therefore, the operating systems must be able to verify the identity of the user. Authentication is the process by which the user has a secret that only the operating system knows. The sharing of a secret is the method used to authenticate that the person is who they say they are.

Kaufman & Perlman & Speciner describes three types of authentication. Password- based authentication is the method where the shared secret is transmitted between the user and the system in clear text. This type of authentication is highly risky. An eavesdropper can capture the password and log in impersonating the other person.

Another type of protection is addressed-based authentication. The user does not share a secret with the operating system and access is granted based only on the IP address of the user. However, the intruder can fake an IP address. The strongest of the authentication methods is the cryptographic authentication. The system through secure means is given the hash value of the password. Every time the user tries to log in, the computer computes the hash and sends it to the server to compare it against the hash value on file. If the match occurs, the user logs in.

As implied in the cryptographic authentication, Network Forensics specialists need to understand cryptography and its value. “Cryptography is the ability to send and receive messages between participants in a way that prevents others from reading” (Kaufman & Perlman & Speciner, 2002, p 41). Cryptography also provides additional services such as integrity checking and authentication. There are many different types of encryption and decryption methods. The specialist needs to know the strength and weaknesses of each of the encryption methods.

Standards refer to the steps and the associated cryptographic algorithms used to share the secret. The steps are broken down into the actual messages transmitted and the role each message performs. The system in conjunction with the user’s computer will select from a list of available encryption/decryption algorithms to share the user’s secret including the generating of the hash value.

Logging in and authentication is a slow process. Standards include a method of identifying a user by a certificate that is stored with a trusted third party. By validating the certificate, the access will continue until the certificate expires.

Emails are sent in a readable format called plain text. Anyone intercepting the email can read its content. Several different methods exist that will encrypt a message that can only be shared with someone that has the key to decrypt the message. There is a need for repudiation: an electronic signature can be added to the email that can only be attached by the owner of the encryption key called the private key. The receiver opens and verifies the hash value using the public key. The public key only works with the originator's private key.

The network forensics specialist needs to understand how network security protection functions and how to apply policies to prevent attacks from occurring. The second proposed category of the common body of knowledge is Network Security.

Overview. Network Security covers the background knowledge to enable the specialist to ensure (a) a user is who they say they are, (b) the user has the need to access the information, and (c) the information is protected to prevent others from gaining access (Kaufman et al, 2002).

Skills.

- Risks
    - Identify the risks (e.g. viruses, worms, Trojans)
    - Identify probability and impact of the risk
    - Establish contingency plan
    - Establish disaster recovery plan
- Attacks
    - Know the types of attacks
        - Probing

        - Denial of Service
        - U2Su: Unauthorized access to super user (root) privileges
        - R2L: Unauthorized access from a remote machine
- Detection
    - Know the phases of attack and the methods used in each
        - Reconnaissance
            - Footprinting
            - Active scanning
            - Vulnerability scanning
        - Gaining Access
            - Sniffing
            - Session hijacking
            - Password attacks
            - Vulnerability exploits
            - Social Engineering
            - Malicious Code
        - Cover Up
            - Evading IDS
            - Modifying logs
            - Rootkits
            - Covert channels
- Protection
    - Authentication

- Cryptography
- Standards
  - Encryption algorithms
  - Real time session security
  - Certificates
- Electronic Mail
  - Encryption
  - Digital signature

Law.

Rationale. Computer crime involves the use of a computer, its systems, and its applications to perform an illegal act. In most other crime scenes, evidence is usually a physical object but digital evidence is logical not physical. It is a series of bits turned on and off. At first, digital evidence was considered hearsay because the evidence is indirectly conveyed. Comments made in emails are hearsay whereas data generated from computer applications is not. If the information is part of normal work then it is admissible.

Since the first evidence gathering is related to the execution of a criminal act, police forensics experts had to develop the skills to preserve, identify, extract, and document the digital evidence. Their knowledge of criminal law is crucial because they must present evidence according to the law related to the crime.

A second type of law is civil law. If a hacker attacks a computer, they are performing a civil violation. Unfortunately, organizations prefer not to pursue legal action because they are more concerned about the corporate reputation that affects the balance

sheet and the stock value. Implications of poor security can cause a loss of revenue. Another reason is the civil law process is a long drawn out process and corporations do not want to lock up computer equipment (evidence) and resources during the court proceedings (Endicott-Popovsky et al, 2007).

Criminal. "That body of the law that deals with conduct considered so harmful to society as a whole that it is prohibited by statute, prosecuted and punished by the government" (Duhaime, 2009). There are two fundamental principles of criminal law: actus reus also known as the guilty act and mens rea, the guilty mind. The physical act of carrying out the crime is the actus reus. The intent of the action is the mens rea (Kleiman et al, 2007). Both the physical act and the intent must be present to be considered a crime.

Network Forensics Specialists are required to understand the laws as they pertain to digital media and networks. Digital Forensics and Network Forensics have one distinctive difference: The crime scene for digital forensics is a single computer while the network forensics' crime scene evolves until all the targeted computers are known and the source is discovered. International attacks means that laws that apply may not be local and jurisdiction now becomes a difficult to resolve because the court needs both subject matter and personal matter jurisdiction. Subject matter jurisdiction is the court's power to hear the particular type of dispute. Personal jurisdiction is the ability to enforce a judgment over a defendant.

International. Network forensics has a borderless nature to it. Understanding international law and treaty conventions will make the work challenging because the specialist will have to know the law that covers the crime in that jurisdiction (Sitaraman

& Venkatesan, 2006). The intruder's jurisdiction may not consider the intruder's act to be criminal and may not allow prosecution.

Civil. Civil law deals with contracts and tort actions between persons. A contract is an agreement that went through the standard process of offer, acceptance, and considerations (Kleiman et al, 2007). A tort is when the actions of a person causes a violation of personal, business or property interest when they, as a reasonable person, should have foreseen their actions would cause harm. These issues are resolved in civil court.

Not all attacks are criminal and the only avenue left for the company is to pursue a civil case. Unfortunately, corporations rarely take civil action because the time, cost, and effort needed would not usually recover damages. There are gray areas in civil law that include what constitutes illegal use of a computer, what you can and can't detect or monitor, and the status of the evidence and the exposure to a liability suit in case of a security problem.

Procedural. The Network Forensic Specialist can present evidence in court. Specialists working within the justice system present evidence on a frequent basis. Corporations that prosecute internal and external attackers will have a specialist prepare their evidence and appear in court. The handling of the investigation, collecting, tracking, and presenting evidence has to adhere to procedural law. Court systems have specific procedures to ensure the rights of the individual are not violated by evidence that is inadmissible in court. The U.S. Department of Justice provides guides to law enforcement agencies and prosecutors to ensure digital forensic evidence meets procedural law

requirements. The document covers all aspects of the procedures and covers the following topics (Gonzales, Schofield & Hagy, 2007):

- Search and Seizure
- Integrity, Discovery, and Disclosure of Digital Evidence
- Courtroom Preparation and Evidence Rules
- Presentation of Digital Evidence Rules
- Presentation of Digital Evidence

The key principles involved in procedural law are:

- Authorization: Permission is required to access devices for evidence (Sitaraman & Venkatesan, 2006). Police can use warrants or subpoenas to gain access to evidence.
- Handling of Evidence: To preserve the admissibility of the evidence, the forensics specialist must adhere to forensic procedures.
- Expert Opinion: The forensic expert must be qualified to provide an opinion based on an admissible method. The two methods are the Frye test and the Daubert test. Most courts use the Daubert test but a few still use the Frye test. Daubert test suggests scientific evidence is admissible if:
    - The scientific technique can be and has been tested
    - The technique has been subjected to peer review and publication
    - There is a known or potential rate of error; and
    - The relevant scientific community has generally accepted the technique.

- Disclosure to the defence: The defence is entitled to a duplicate of the digital evidence. The prosecution must identify, preserve and present evidence to the defence and show the forensic specialists searched for and reported all relevant evidence even if it is in the defence's favor. If the defence's forensic specialist is able to find evidence not found by the prosecution it would affect the credibility of the prosecutor's forensics specialist testimony.

Ethics. The disclosure to the defence exemplifies why ethical behavior must be part of the specialists' everyday activity and their personal integrity. All exculpatory evidence must be disclosed. Exculpatory evidence is any evidence that may exonerate or diminish the liability of the defendant. The lack of disclosure and the discovery of the omission could result in the court accusing the specialist of evidence tampering or withholding (Thomas & Forscht, 2004). The role of the specialist is not to assign guilt or innocence of the accused but is to present evidence in an objective way to allow others to determine the guilt or innocence.

The network forensics specialist has an even more challenging issue with ethics. To defeat an attacker or to be thorough in their investigation, the specialists must be equally or better skilled at the methods used by the attackers. In other words, the specialists have the skills to become an attacker. Their ethical behavior has to be held to a higher standard to ensure they do not engage in their own criminal activity or use their skills for personal gain (Stahl et al, 2006). Any training that the specialist receives has to emphasis the professional ethical standard they must live by to perform their duties. The academic institution needs to stress the student must demonstrate ethical and moral responsibilities to themselves, and others including the University, and their future

employer. One approach to the ethical issue is for the specialists to study historical forensics cases and discuss the moral and ethical issues pertinent in those cases. The forensic cases can be hypothetical in nature or actual cases known in the public domain as long as the following is taken into account: (a) confidentiality, (b) anonymity and (c) other ethical considerations.

Overview. Law covers the background knowledge to enable the network forensic specialist to adhere to the legal and professional ethics standard of the profession. The legal implications can cross multiple jurisdictions and can be criminal or civil or both. Presenting of evidence must be complete, impartial, and with full disclosure to the defence. At all times, the network forensic specialist must demonstrate strong professional ethic and moral responsibility to themselves, to others, the School, and their employer.

Skills.

- Criminal Law – *actus reus* and *mens rea*: The act and the intent
- International Law
    - Jurisdiction
    - International Treaty
- Civil Law
    - Contract
        - Offer
        - Acceptance
        - Consideration

    - Torts
        - Tort of conversion – use as not intended
- Procedural Law
    - Process
        - Search and Seizure
        - Integrity, Discovery, and Disclosure of Digital Evidence
        - Courtroom Preparation and Evidence Rules
        - Presentation of Digital Evidence Rules
        - Presentation of Digital Evidence
    - Principles
        - Authorization
        - Handling of Evidence
        - Expert Opinion
        - Disclosure to Defence
- Ethics
    - present evidence in a subjective way to allow others to determine the guilt or innocence
    - exculpatory evidence must be disclosed
    - professional ethical standards
    - not to use for criminal activity or personal gain

Digital Forensics

Rationale. A Network Forensics specialist also needs to needs to know and understand digital forensics. As mentioned in the section about Information Technology,

the specialist must know all forms of digital media and the means by which information is stored. Network Security knowledge provides the specialist the understanding of the types of attacks and what digital media is affected when an attack occurs. Digital Forensics knowledge provides the specialist with the skills to extract the information whether it is normal media format or hidden within the media structure such as dead or empty sectors (Kruse & Heiser, 2001).

There are several different methods describing ways of performing digital forensics. By many definitions, digital forensics is the preservation, identification, extraction and documentation of computer evidence (Thomas & Forcht, 2004). Sitaraman and Venkatesan suggest the three "A"s investigation process: Acquire, Authenticate, and Analyze. The investigation process will vary slightly depending on the jurisdiction. For this essay, the investigation process consists of the following categories: Collect, Authenticate, Analyze, and Report.

Collect. The forensic specialist needs to acquire the evidence by a method that preserves the evidence in its original format. Unfortunately, turning a computer on or off will immediately alter the logs, hard drive space, and destroy valuable evidence. On entering the crime scene, the specialist will do an assessment and collect evidence in the order of volatility. It makes sense to collect information that has the shortest lifespan first to ensure it is captured and preserved. (Wile & Reyes, 2007). When the specialist is ready to remove and transport, the evidence is sealed to prevent tampering.

Instead of using the original media for evidence and causing the destruction of information, the data has to be captured onto another media where the analysis can occur.

The specialist must ensure the replication media is sterilized before any use. Any contamination from previous use will void the authentication.

Whenever possible, the information is gathered and copied each time in a true bit map stream of the original and the original is kept under documented control to ensure its integrity and value are admissible in court (Sitarman & Venkatesan, 2006). As with any evidence, the specialist will create a chain of custody which is a documented record representing the chronological history of the investigation, and all contact and activities of the evidence. The record includes information such as (a) who handled the evidence, (b) what procedures were performed, (c) date and time, and (d) when the evidence was collected. The records can also include information such as where the evidence was found, and why it is considered evidence (Sitaraman & Venkatesan, 2006).

Authenticate. The specialist has to be able to persuade a court of law that the evidence originated from the computer in the crime scene. This may sound easy but remember the analysis is done on an exact replica of the digital evidence. How can you confirm the copy is identical to the original? The answer is authentication.

Authentication is a digital fingerprint. The technique using either a hashing or a message digest algorithm calculates a unique fixed length value from the input length. In the case of the evidence, the length of the data stored on the media is the input value that is used. The hash value is not reversible in that someone cannot take the hash value and reverse engineer the algorithm to find out the input length of the source. A simple change alters the length of the data and generates a different hash value. To authenticate the replica and prove that no tampering has occurred, the specialists would recalculate the hash value and demonstrate that it matches the value of the original. (Sitaraman &

Venkatesan, 2006). The specialist will need to know how to use MD5 or SHA encryption algorithms to calculate the hash value.

Examine. Today, digital evidence can be found in many storage medias: random access memory, flash drives, floppy drives and hard drives. The information can be found in many places: network logs, e-mails, word documents and could be hidden in picture files or free space on the hard drive. (Sitaraman & Venkatesan, 2006). Some of the other hiding places include:

- Slack space;
- Unallocated space;
- Registries;
- Hidden files;
- Encrypted files;
- Password-protected files; and
- System logs.

Analyze. The analysis of the data is the most extensive and most critical process of the forensic specialist. The process must be well documented and kept in the chain of custody records. The defence will have the same access to the evidence and will use its own forensic specialist to attempt to discredit the findings. Once the media replica is examined as described above, the information is analyzed to determine if there is evidence on the system. The analysis phase deals with the recovery of deleted, hidden, password-protected, and encrypted files. Some of the approaches used in analyzing the data are:

- reading the partition table;

- searching existing files for relevant information such as keywords, system state changes, text strings;
- retrieving information from deleted files;
- checking for data hidden in boot record, unallocated space, slack space or bad blocks in the disk; and
- Cracking passwords.

The process can be extremely slow. The size of the media is growing leaps and bounds, and it is nearly impossible to explore every possible location and method of concealing information. The specialist has to follow a methodical approach and try to think as the accused would and look in the most probable locations. When the locations are found, the specialist performs visualization that is the process of generating a timeline of computer activity using the information found in the log files.

The goal is not just to convict the accused but also to understand the attack and discover ways to prevent it. The forensic specialist needs to do a root-cause analysis of the attack to develop policies that will prevent a reoccurrence of the problem. The information can also be used for statistical purposes in determining the full extent of the problem (Sitaraman & Venkatesan, 2006)

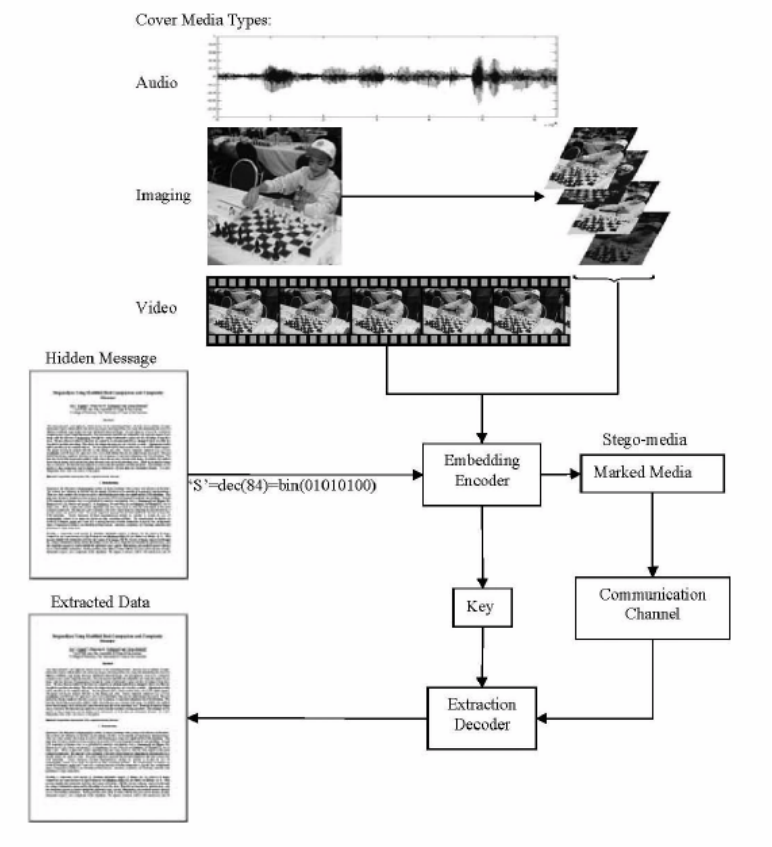
Report. Identifying the impact of the attack relies heavily on the ability to write efficient reports. Interpreting the results of the analysis depends on the knowledge and experience of the specialist (Sitarman & Venkatesan, 2006). As they go through each step of the preservation, identification, extraction, and documentation of computer evidence and carefully document the process in the chain of custody, they must be able to take their technical knowledge and translate it into simple terms that can be used in a

court of law. There can be no ambiguity as to the meaning and the significance of the results obtained. As they go through the process, there are a few rules that apply (Wiles & Reyes, 2007):

- Examine the original evidence as little as possible. Copy the original and test on the copy;
- Follow the rule of evidence and do not tamper with the evidence;
- Prepare a chain of custody and keep it accurate;
- Document any change to the evidence; and
- Do not make opinions or comments that are outside the knowledge base of the specialist.

Some times, the information is hidden within files. This process is called steganography. For example, if the criminal wants to hide a text document; they can use the steganography software to append the file to a photo. The photo software will read the photo up to the end marker of the image and then display the image. To a viewer, there is nothing attached but the criminal can use the steganography software to extract the appended file at any time. Due to the amount of photos that exist on a computer, the specialist cannot check every single file. Fortunately, the presence of the steganography software on the computer will imply it is being used to hide information and that is sufficient evidence to warrant further analysis of the files (Agaian & Rodriguez, 2006; Sitaraman & Venkatesan, 2006)

Figure 1. Basic Model of Steganography



Reprint from Agaian, S.S., Rodriguez, B.M. Basic steganalysis techniques for the digital media Forensics Examiner. Page 178. Copyright (2006). with permission of the publisher IGI Publishing

Today, network forensic software tools can quickly search the media for evidence and can be used to create reports, which simplify the whole process. Since there is a tendency to depend solely on the accuracy of the software, the software itself can be called into question as to its ability to be accurate. All software must meet the Daubert Criteria:

- The tool must be tested against a known data set for accuracy, reliability, and is repeatable in identifying the attacks;
- The software has gone through peer-review; and

- The forensic community has accepted the methodology.

There are many tools available for performing specific forensic tests. It is noteworthy to state that not one single software toolkit exists that encompasses all the forensic testing that a specialist performs.

Overview. Digital Forensics covers the background knowledge to enable the network forensic specialist to preserve, identify, extract, and document computer evidence. The specialist must demonstrate an understanding of the importance to follow procedural law in the management of digital evidence and be able to provide expert testimony in a court of law.

Skills.

Preserve

- Order of Volatility
- Chain of Custody
- Preservation of original
- Authentication
    - MD5
    - SHA
- Identify
    - Media
        - random access memory
        - flash drives
        - floppy drives
        - hard drives

        - portable devices
    - Locations
        - Slack space
        - Unallocated space
        - Registries
        - Hidden files
        - Encrypted files
        - Password-protected files
        - System logs.
- Extract
    - Methods
        - reading the partition table
        - searching existing files for relevant information such as keywords, system state changes, text strings
        - retrieving information from deleted files
        - checking for data hidden in boot record, unallocated space slack space or bad blocks in the disk
        - Cracking passwords
    - Steganography
- Document computer evidence
    - Protocol
        - Examine the original evidence as little as possible. Copy the original and test on the copy

        - Follow the rule of evidence and do not tamper with the evidence
        - Prepare a chain of custody and keep it accurate
        - Document any change to the evidence
        - Do not make opinions or comments that are outside the knowledge base of the specialist.
    - Daubert Criteria for software
        - The tool must be tested against a known data set for accuracy reliability, and is repeatable in identifying the attacks
        - The software has gone through peer review
        - The forensic community accepts the methodology as valid

Network Forensics

Rationale. Computer forensics deals with the preservation, identification, extraction, and documentation of computer evidence of a single computer while the network forensics' investigation is on multiple computers across network systems.

Network Monitoring and Logging. When the attacked and attacking system can be anywhere in the world, it makes the job of authenticity and reliability difficult. Authenticity and reliability are two tests used on evidence and are composed of digital and physical evidence. (Wiles & Reyes, 2007). The digital proof is easier to obtain than the physical proof since the device used to perform the attack could be out of the jurisdiction of the forensic specialist.

Since the two tests will be difficult to apply to network forensics, the network forensic specialist's goal must be proactive and not reactive like in digital forensics

(Endicott-Popovsky et al, 2007). The best way to detect and stop intrusion is to monitor the network for suspicious data streams or processes that are occurring in real time. Network forensics uses software and artificial intelligence analysis engines to capture and correlate data from the streams of bits flowing in and out of the network across the Internet (Sitaraman & Venkatesan, 2006).

The algorithms can establish the normal flow of traffic and identify certain anomalies. By the characteristics of the anomalies or signature, the software can identify when an attack is in progress. When the software detects the attack, the software will then collect data in the order of volatility. For example, the software will capture the current state of the computer memory, the cache, and then the swap file on the hard drive. Then system logs are read to create the historical trail of events.

The final stage to the order of volatility is to make a copy of the media and use digital forensics to locate the evidence. Regretfully, the algorithms are not sophisticated enough to be able to interpret attacks patterns in network traffic that are encrypted. More research is required to solve the many ways attackers can defeat the software protective functions.

E-Mail Tracing. E-mail can be an important piece of evidence for several reasons. If it was used in the commission of a crime, the email becomes evidence. Since emails track the originator and destination accounts, the e-mail header can be useful to track suspects (Sitaraman & Venkatesan, 2006). E-mail spoofing is an attempt to hide the identity of the originator. This will fool the recipient into believing that the email comes from a trusted source. Some parts of the e-mail header cannot be altered. The specialist can, by tracing the e-mail path through routers and the firewall logs, find the true source

device of the e-mail. A deleted email can be restored from one of the e-mail servers that retain a copy even after a successful delivery. Understanding the hidden value of information obtained from emails can assist the specialist in tracking down the source of most e-mails.

IP Trackback. One of the attacks used is the denial-of-service attack. The intruder will send a stream of requests to the company's servers denying legitimate users access to them. The attacker will forward the request through unsuspecting computers fooling the attacked system into believing the attacks are from valid IP addresses. The forensic specialist can trace the attacker to the source by selectively monitoring packets of flow using the router's logging mechanism. The path can be reconstructed by marking and tracing the packets along the path to the origin. The approach is not always successful because it depends on finding the packets to track (Sitaraman & Venkatesan, 2006).

Attack Traceback and Reconstruction. Not all of the attacks need to be spread by human intervention. Viruses and worms can spread quickly from computer to computer and the ability to track this self-contained, self-propagating code has gained importance in network forensic monitoring. When a malicious virus or worm is detected in the router traffic, the specialist is able to detect the source node by using an approach called query-response. The specialist can query each router for the source and destination of the packets to determine the path the virus or worm took from its origin.

There are several benefits in establishing network forensics on the corporate networks. Intrusions will occur and some will succeed even against the best-protected networks. Corporations are aware of this and use network forensics as a way to minimize the damage by the attacker. When an intrusion occurs, the system logs can track the

changes in the environment. With a log of altered files readily available, the system administrators can restore lost or damaged files from the backup. The recovery time is reduced substantially because massive restores are not required.

The second benefit is the support of digital forensics. The forensic software is tracking the changes to the computer systems while the log is listing the files that were altered. When an intrusion is detected, the digital forensic work begins and the software can indicate where to find the evidence. Since the logs are on the network servers, the information is accessible without doing an invasive search of the computer system. The computer can be isolated and the media removed. However, the specialist should be aware that the logs may be tampered with to hide the trail of the intrusion and more traditional methods may have to be used.

The third use of network forensics is the detection of the attack in progress and proactively identifying the source of the act. This is useful for several reasons: (a) the attack can be interrupted preventing further damage and (b) the intrusion can be monitored to trace back to the source of the attack.

The monitoring of the network is not as easy as it sounds. Not one single software application tool can do everything needed and the specialist has to use numerous tools to monitor the different boundaries. Examples are early detection software such as virus-scanning tool that runs on a single computer and distributive detection systems designed to work at the network level. However, the two types of detection systems are not inter-connected. Alerts that occur at the workstations are not actively forwarded to the distributive detection system. The specialist must know that an alert in one system

requires intervention to begin forensic network analysis with the distributive tools to track the activity to the source (Kahai & Namuduri & Pendse, 2006).

Overview. Network Forensics covers the background knowledge that enables the network forensic specialist to monitor, detect, and trace intrusions on the network. By using basic and distributive detection systems, the specialist will set up security policies that will initiate alerts when an intrusion occurs. When an alert does occur, the specialist will be able to identify the affected systems, perform recoveries, trace the intruder to the source, and commence an investigation by collecting digital forensics.

Skills.

- Identify real-time attacks
- Perform backup recovery
- Initiate IP Tracing
- Perform attack trace back and reconstruction
- Commence Forensic Investigation
- Use Forensic Software
    - Early Detection Systems
    - Distributive Detection Systems
    - Forensic Toolkits

Security Management

Rationale. In 2006, Von Solms and Louwren suggested there is a relationship between policy making and forensics. The policy making establishes the network security to prevent intrusions. Network Forensics is the ability to detect the intrusion and Digital Forensics is the pursuing of legal actions against the intruder. The Network Forensics

Specialist is required to understand how to make policies, how to implement policies and how to audit to ensure the policies are complied with.

There has to be a real balance between monitoring and tracking all network activity while enabling the users to do business. Excess security hinders business productivity while insufficient security invites attacks that can also hinder or stop business activities. Security and the corporate management have to establish well-balanced policies on network security protection (Yeager, 2006).

Network security protection is provided by establishing controls on the network systems. By establishing controls, security can set the boundaries and limits of operations. The principles of security control are (Tipton & Krause, 2007):

- Proprietary of information – ensuring the information has not been inappropriately altered;
- Compliance of established rules – defining the limits and boundaries that systems and people work within;
- Safeguarding of assets – the concern of management, security, and auditors. Assets are defined as tangible and intangible objects that the organization value;
- Efficient use of resources – controlling resources in a way that protection is provided but not to the level that severely impedes resources: cash, people, time; and
- Accomplishment of established goals and objectives – organization has set goals to be achieved and security should not interfere with the achievement of the goals.

The implementation of the principles is achieved by the following methods (Tipton & Krause, 2007):

- The control environment – establishes an organizational structure wherein decision-making authority is well defined and responsibilities are allocated as part of the control environment;
- Risk Assessment – defines the threats and exposures. The organization can apply controls to reduce the risk of the threat and the impact;
- Control activities – establishes role-based authority of access and permissions to ensure no unauthorized activity can occur;
- Information and communication – communicating data so everyone has the information to do their jobs. It is critical to understand (a) what is communicated and how it is communicated and (b) to be sensitive to the importance and distribution of the information. Efforts are needed to protect confidential information; and
- Monitoring – ensuring that the controlled environment is established and performing as planned. Often controls are not normalized and as a result not working to the best intentions of security. Monitoring can identify opportunities for improvement that would have otherwise gone unnoticed.

The relationship between security management, network forensics and digital forensics are intertwined. If the security management and network forensics are poorly implemented, attacks can occur and a large portion of the specialist's effort will be reactive in nature by performing data recovery and digital forensics. If an organization develops strong policies and implements them using the software tools in network

forensics, it can be network forensics ready and proactively prevent attacks and reduce the use of digital forensics (Endicott-Popovsky et al, 2007).

Endicott-Popovsky et al proposes that the intruder and security management play a continuous game of escalation. The intruder finds a way to defeat the network policies forcing Security to implement new policies. The intruder is highly adaptive and continues to attack and defeat the newest policies. As a result, security is constantly fixing current problems but not addressing the root cause: the intruder. Until organizations are willing to pursue legal action, the escalation will continue.

Network Forensics Response is the proactive monitoring and tracking of attacks. The goal is to recover from the attack as quickly as possible and to implement new policies to reduce the possibility of a re-occurrence. The traditional approach to network forensic response is (Endicott-Popovsky et al, 2007):

- Resistance: implement policies that will reduce security threats and risks;
- Recognition: monitor and detect threats as they occur; and
- Recovery: determine the extent of infiltration and perform recovery of affected files

Network forensics Response is the proactive capturing of system data to enable digital forensics. The intent is to be prepared to pursue a criminal/civil investigation in any attacks on the networks. Endicott-Popovsky et al proposes an additional “R”: Redress. Redress is retaliating against the intruder by making them accountable in a court of law. The goal should not be recovering from an incident but to maximizing the organization’s ability to collect creditable evidence in the pursuit of conviction.

Security Management must include the implementation of tools, practices, techniques, and security awareness programs to protect the network and to prevent intrusions. The inclusion of redress in the network forensic response will send a much-needed message to intruders that the corporate networks are restricted areas and illegal access will result in legal action.

Overview. Security Management covers the background knowledge that enables the network forensic specialist to create, implement, and monitor security policies as defined in the corporation's security governance. The specialist will be able to apply the principle of security management to safeguard the assets and to establish a network forensic response team to manage incidents.

Skills.

- Principles of Security Control
    - Proprietary of information
    - Compliance of established rules
    - Safeguarding of assets
    - Efficient use of resources
    - Accomplishment of established goals and objectives
- Methods of Security Control
    - Control environment
    - Risk assessment
    - Control activities
    - Information and Communication
    - Monitoring

- Network Forensic Response
    - Resist
    - Recognize
    - Recovery
    - Redress

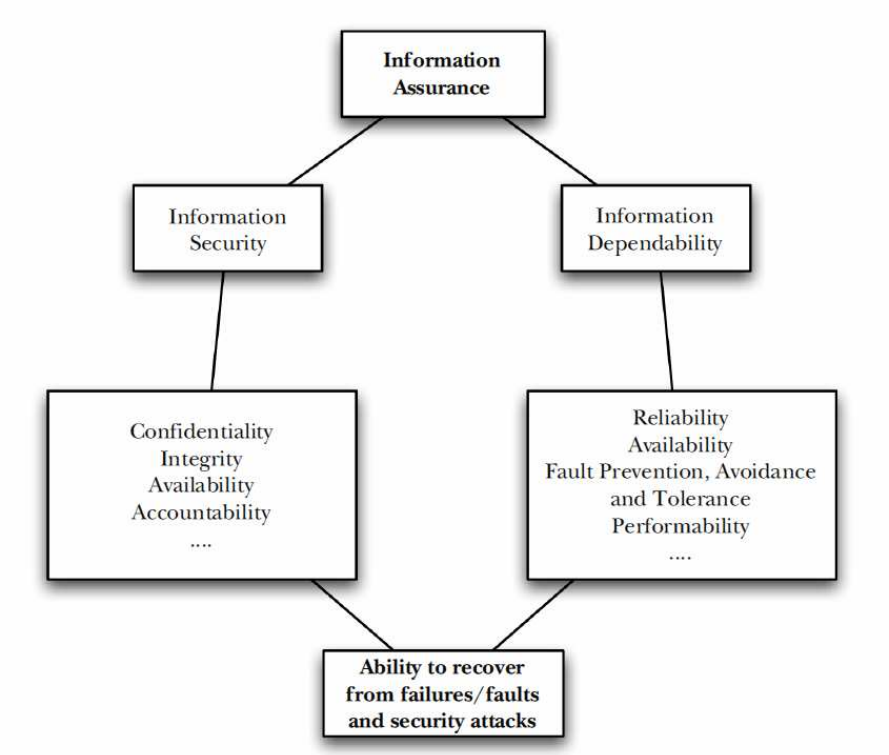
Information Assurance

Rationale. The interconnectivity and interoperability of network systems are recognized as a critical infrastructure of society (Qian et al, 2007). Corporations depend on their network information systems to be available twenty-four hours a day and seven days a week. Society as a whole has become dependent on the Internet and the social community it provides and has concerns about the security and dependability of the network systems.

The security aspects of the interconnectivity and interoperability is well managed by security management through the creation, implementation and monitoring of security policies. Security Management is concerned about the confidentiality, integrity and availability (CIA) of information (Qian et al, 2007) and not the dependability.

The dependability of interconnectivity and interoperability deals with the ability of the systems to provide specific services in the event of a failure. The difference between security and dependability is that dependability focuses on faults and errors in the systems and security deals with protecting the systems against malicious attacks. Often, the effects of either can have the same result on systems and networks. As a result, both are consider a sub-process under a more global concept of Information Assurance.

Figure 2. Information Assurance: Interaction between security and dependability



Reprinted from Publication Yi Qian, James Joshi, David Tipper and Prashant Krishnamurthy, Information Assurance/ Information Assurance, Pages No 5., Copyright (2008), with permission from Elsevier

Information Assurance (IA) refers to the trustworthiness and reliability of the networks and systems. IA ensures the systems are available to the users, the information is accurate and complete as possible, and the security and dependability is maintained (Hamil, Deckro & Kloeber, 2004). The U.S. Department of Defence doctrine on Information Operations defines IA as:

- Protect and defend information and information systems by
    - Availability
    - Integrity
    - Identification and authentication
    - Confidentiality, and

    - Non-repudiation
- Provide restoration by
    - Protection
    - Detection
    - Restoration
- Using technologies and processes such as
    - Multilevel security
    - Access controls
    - Secure network servers
    - Intrusion detection software

Information Assurance is safeguarding information. The user is assured that there is a process in place to protect information from unauthorized disclosure. An organization consists of groups with different needs and protection, which creates boundary issues. An information assurance technical framework can resolves the issues. Within an organization, the framework applies a common set of principles and processes for each of the four categories of boundaries (Rittinghouse & Hancock, 2007):

- Local computing environments – applications are installed on the client and server side;
- enclave boundaries – collection of local computers on a local area network are covered under one security policy;
- network and infrastructure – hardware that connects the enclaves together; and
- Supporting infrastructures - the mechanism on which the Information Assurance is used in the network, enclave, and computing environment. The

supporting infrastructure provides the functions to manage the system in a secure manner and to provide security-enabled services such as public keys (PKI).

The threat of intrusions will continue to escalate. To be able to defend against the threat, the specialist needs to know the different classes of attacks (Rittinghouse & Hancock, 2007):

- Passive – The intruder is intercepting traffic reading the unprotected communications, decrypting weak passwords, and capturing authentication information. The intruder's goal includes disclosure of personal information;
- Active – The intruder attempts to circumvent the system security. The goal is denial of service, disclosure of data files, or modification of files;
- Close-in – The intruder is an unauthorized person in the physical location of networks, systems or facilities with the intent to surreptitiously enter facilities or gain access;
- Insider – The intruder is internal with the intent to bypass security to more easily do their job or to perform malicious acts to obtain unauthorized information; and
- Distribution – The intruder attempts to alter hardware or software at the factory or during distribution with the goal to insert malicious code.

The prescribed method to manage these types of attacks is known as defence-in-depth. Defence-in-depth concentrates on the technology to defend the three principle aspects of Information Assurance: people, operations and technology (Rittinghouse &

Hancock, 2007). The defences are applied to each of the three principles to ensure the entire organization is not at risk when one of the three principles is successfully attacked.

The protection, detection, and restoration of Information Assurance are three of the functions of network forensics and the network forensic specialist therefore plays a major role in Information Assurance.

Overview. Information Assurance covers the background knowledge that enables the network forensic specialist to protect, detect, and restore the systems against all threats be it intrusions or system errors. To make the systems trustworthy and reliable, the specialist should apply the principles of information assurance technical framework.

Skills.

- Protect and defend Information and Information systems by
    - Availability
    - Integrity
    - Identification and authentication
    - Confidentiality
    - Non-repudiation
- Provide restoration by
    - Protection
    - Detection
    - Restoration
- Use technologies and processes such as
    - Multilevel security
    - Access controls

    - Secure network servers
    - Intrusion detection software
- Know the four categories of environments
    - Local computing environments
    - Enclave boundaries
    - Network and infrastructure
    - Supporting infrastructures
- Understand the source of attacks
    - Passive
    - Active
    - Close-in
    - Insider
    - Distribution
- Understand the principles of Information Assurance
    - People
    - Operations
    - Technology

Conclusion

The proposed seven categories for Common Body of Knowledge are Information Technology, Network Security, Law, Digital Forensics, Network Forensics, Security Management, and Information Assurance. They represent a sub-set of the skills Network Forensics Specialists should have to perform their duties.

The normal process to create a CBOK includes a peer review, certification creation, and accreditation. An organization consisting of Network Forensics Specialists could work together to make the CBOK their certification standard. The organization could then work with universities to accredit their education programs for the designation. Based on that criterion, my proposed common body of knowledge is just a framework and start point to enable others to develop Network Forensics Specialist certification and post-graduate curriculum accreditation.

CHAPTER III

RESEARCH METHODOLOGY

The goal of the study is to discover and research the CBOK appropriate for accrediting curriculum of a Network Forensics Science program.

Research Methods

The qualitative approach was used because quantitative research has proven to be less effective for the following reasons: There are no empirical values to state that if the network forensic skill *x* appears *y* number of times that it can be considered to be true and the key-word definitions are inconsistent producing information open to misinterpretation resulting in incorrect quantifications. For example, in literature the term "cyber-forensics" can describe digital, computer and network forensics depending on the author.

Study Conduct

The approach to research consists of an analytical qualitative method utilizing a blend of analytic induction and grounded theory approaches (Ritchie & Lewis, 2003). The analytic induction consists of multiple iterative cycles that are completed when the CBOK model is reformulated to the point where the skills fit into a category. Within each iterative cycle, the approach uses grounded theory to categorize the skills and adjusts their relationship with the other skills until the relationships are saturated. Each iterative cycle consists of four steps: gathering, organizing, categorizing, and filtering.

Gathering. The taxonomy structure is undefined at the beginning of the process. The first iteration of skills fit under no categories. The categories were formed only when the interrelationship with other skills became apparent. In addition, the skills' relationship under a category and the interrelationship with other skills can be fluid. Only after many

iterative cycles are the final associations developed. A mind map tool was used to capture the information and to provide a way to alter the relationships as necessary. The mind map is a non-linear, graphical representation of words and ideas related to one single idea. The branches on the mind map represented the categories and the sub-branches represented the skills within the categories.

A mind map is a useful approach in that after each iterative cycle the information can be better categorized as new taxonomy groups are postulated. Another benefit of the mind map approach is that the repetition of the same information in the research papers confirms the CBOK structure is sound.

The gathering of quality literature is an important aspect of the research. Reviewing an article, book, or paper includes determining if it is refereed or not refereed. Refereed literature is reviewed by the author's peers in the same field, and the intent is for the peers to comment and make recommendations on whether the literature is accepted and authoritative. To avoid possibilities that the chosen literature is not refereed, the literature is selected from the digital library databases available through the Athabasca University's library. A web-based search tool is available that provides cross reference searches in Google Scholar. For this study, Google Scholar provides another source of research.

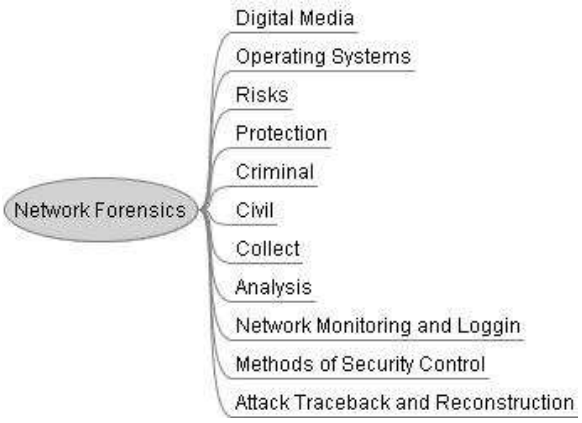
The research gathering commences with searching for literature in reference databases such as ACM, IEEE and Science Direct using key words like network forensics or law and forensics. These sites provided articles, research papers, and books related to the topic. When keyword searches did not find a match, the Google Scholar was used to search a larger database of material. If that search was successful, new keywords were

applied in the digital libraries to find the same article. The reason for repeating the library search is that the Google Scholar will identify books or papers but not necessarily give permission to these documents whereas the university's library provides full access.

Once the literature was determined to be authoritative, its content was evaluated for relevancy to the topic and the date of publishing. Due to the fast changing field of forensics, any article more than six years old is automatically excluded unless the information is for historical purposes.

Organizing. From the literature, the skills are extracted and grouped together in preparation for categorization (figure 3). Not all literature was deemed satisfactory for inclusion in the essay and the cyclical approach provided opportunities to perform additional searches in literature to expand on categories requiring further development.

Figure 3. Mindmap - Organizing by characteristics



Categorizing. The approach to categorization includes analytic induction and grounded theory approaches (Ritchie & Lewis, 2003). Analytic induction provides the iterative cycling of the categorization process as each literature's content is organized by the inter-relationship. The grounded theory approach is the network forensics specialist's taxonomy of the skills. Taxonomy is from the Greek taxis [order] and nomia [law]

meaning the categorization of objects by their relationships. As the skills are known and the relationships are associated, a pattern forms.

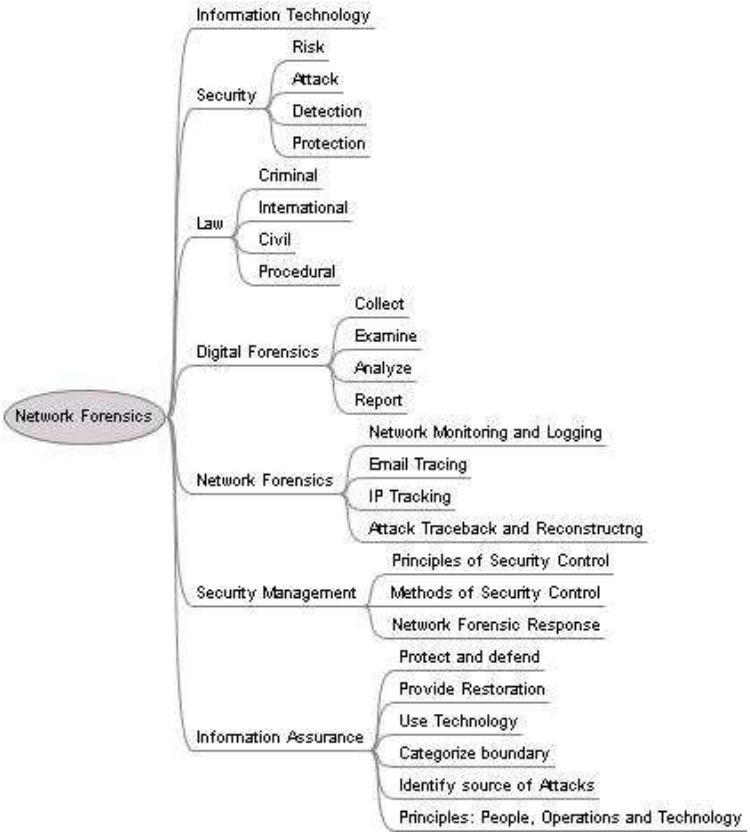
If new information is discovered, the key words particular to the new information is used to find additional relevant literature on the topic. The skill's taxonomy characteristic forms the basis for categorization. For example, firewall protection falls into the taxonomy group of Network Security. By the time the process was completed, there were seven different categories of Network Forensics Specialist's Skills: Information Technology, Network Security, Law, Digital Forensics, Network Forensics, Security Management, and Information Assurance (figure 4).

Filtering. Filtering plays two roles in the essay. The first is to remove knowledge that does not meet the criteria of any of the categories or provides more detail than required. This does not mean the information is not of value but that it is a sub-set of an existing category and inclusion would mean expanding the CBOK to include all the similar skills at that level. The second role of filtering is to separate the research literature into the three premises for the essay: Network Forensics Specialist taxonomy to build a common body of knowledge, the CBOK validation based on existing post-graduate curriculum programs, and the application of the CBOK to produce a post-graduate curriculum.

The research methodology used in this essay is an analytic qualitative research method using analytic induction and grounded theory approaches. The process was cyclical involving four steps: Gathering, Organizing, Categorizing, and Filtering. The knowledge or skills identified were categorized into a taxonomy structure using a mind-

mapping tool. To ensure the CBOK is accurate, the taxonomy is validated against existing university curriculum.

Figure 4. Mindmap - Categorized by taxonomy



The validation of a CBOK is not included in the iterative cycle but is a part of the research findings and research conclusion in Chapter 4. The application of the CBOK and implementation of a CBOK-base curriculum is included in the research implication in Chapter 5.

CHAPTER IV

RESEARCH STUDY RESULTS

Introduction

The purpose of this study was to build the Common Body of Knowledge (CBOK) for Network Forensic Science by reviewing material relating to this field and applying a taxonomy approach of categorization. The first phase of this study involved selecting and reviewing literature that were refereed papers or books on topics specifically on computer-related forensics. It was in this phase that the CBOK took form as the study identified seven categories of knowledge: Information Technology, Network Security, Law, Digital Forensics, Network Management, Network Forensics, and Information Assurance.

The second phase involved selecting and reviewing several papers, books, and university's websites dedicated to computer-related forensics' curriculum that validated the concept of CBOK as a potential foundation of certification and accreditation in Network Forensic Science.

The goal was to compare the seven categories of knowledge to the course contents to establish a relationship between the categories and the curriculum. The reasonable assumption is that the curriculum would have gone through some form of peer review before obtaining accreditation. The theory is that although different approaches are used to develop the curriculum (Bogolea & Wijekumara, 2004), the CBOK could have been one of the approaches used. Therefore, the CBOK should be easily identified within the course curriculum and similar programs should have the same pattern of associated categories.

Study Findings

The study produced the following findings:

- Today's specialists are not well prepared;
- Network Forensics Science programs are not offered;
- Similar Programs exist; and
- Interrelationship exists between disparate forensic programs

Today's Specialists are not well prepared. The findings indicate two problems with the role of today's specialists. Firstly, that the number of available network forensics specialists cannot meet the demand of an ever-expanding proliferation of criminal activities involving computers. Secondly, that those same specialists are not generally well prepared to appropriately identify, handle, manage, and present digital evidence to the legal community (McGuire, Murff, 2006). The law enforcement system is forced to outsource network forensics to non-police experts (Wassenaar et al, 2009). Because of the new role of network forensics, there is a shift in training programs to expand beyond police forensic investigations to include training in real-time protection of companies against criminal behaviour (Qian et al, 2007; Stahl et al, 2006). Unfortunately, there are not enough university network forensic programs to meet the demand and those available do not adequately prepare a specialist to perform all forms of forensic work.

Network Forensics Science programs are not offered. The Science of Network Forensics is a new field of study. The problem of inadequately trained network forensic specialists is exacerbated by the fact that there are few if any universities offering network forensic programs. In fact, outside of law enforcement, there are very few programs offered at all in relation to computer-based forensics (Figg & Zhou, 2007).

Universities need to offer accredited Network Forensics Science programs to ensure there will be a sufficient number of scientists graduating to meet the growth expected in Network Forensics (Wassenaar et al, 2009).

A common thread in all the research in computer related forensics science is that the curriculum is offered at inter-disciplinary universities with a criminal justice and computer science program (McGuire, Murff, 2006). The computer science program as the host department could offer forensic law courses taught by qualified criminal justice instructors.

University courses should have two basic attributes: they possess scholarly rigor, and are unique enough to offer a comparative advantage to existing programs (Figg, Zhou, 2007). Network Forensic Science possesses both attributes and yet there is reluctance by universities to offer this program. Studies indicate that the reasons for this reluctance are the special and expensive requirements of such a program.

The training lab is an extraordinary expense to a university program and this deters universities from developing a network forensic program. The costly and key components of this program are a fully functional separate network consisting of servers, firewalls, routing and switching equipment (McGuire & Murff, 2006; Yasinsac et al, 2003). The student needs to be as knowledgeable in hacking techniques and the test lab provides a safe and secure environment for training. This environment is closely monitored to ensure there is no threat of unethical behaviour by students (Stahl et al, 2006).

Many experts consider that learning on software tools is not education but training and, therefore, should not be part of the university's curriculum. Training relates to

learning the tools of the trade and education to learning the theory behind the science. The use of training is best suited for entry-level positions in network forensics where the specialist must first understand the software tools to operate them. Hands-on training is best if offered in a test lab. This implies software training is better if offered at technical schools.

However, the focus of those in positions that are more senior is not on the use of the tools, but what the tools reveal about the data and the structure (Yasinsac et al, 2003). Therefore, the training will be a simulation of an attack where by the software is the means by which the students can access and interpret the software logs to discover the simulated attacks. In either case, the training lab is essential for all levels of network forensic specialists' learning even though the roles in which they function are different. For these reasons, universities should offer software training to provide students with realistic experiences in assessments.

Similar Programs Exist. The CBOK validation cannot be validated against any existing network forensic program. The closet to a full program is at universities that offer either a course in computer-related forensics or a minor in its computer science degree. Unfortunately, they offer insufficient material to justify qualifying as a program to validate the CBOK.

The validation of the CBOK had to be discovered and researched by indirect association with computer related forensic programs that are well established at universities in U.S, United Kingdom, and Australia. The research shows digital forensic and information assurance programs are prevalent at the university Bachelor and Master

level. The process reviews course content for skills that is compared to the CBOK to identify the related category.

The validation is the review of the course material of similar programs. The search for existing university programs was expanded to include BSc in Digital Forensics, MSc in Digital Forensics, MSc in Information Security, and MSc in Information Assurance. The universities are divided into their respective degrees and are shown in appendix C. At first view, a common thread between the degrees does not exist with the exception of BSc in Digital Forensics.

Table 1. CBOK Categories Relationship between different degree programs

Degree	IT	NS	Law	DF	SM	NF	IA
BSc in Digital Forensics	R	R	R	R	R		
MSc in Digital Forensics	*	*	R	R	R		o
BSc in Network Forensics (Proposed)	R	R	R	R	R	R	
MSc in Network Forensics (Proposed)	*	*	R	R	R	R	R
Msc in Information Assurance	R	R	o	R	R	o	R

Abbreviations IT = Information Technology, NS = Network Security, DF = Digital Forensics, SM = Security Management, NF = Network Forensics, IA = Information Assurance, *= Foundation, R = Required, o = Optional

The EC University is offering a Master of Security Science (MSS) program that is very similar to the Network Forensic Science's CBOK. It is a new university and program is licensed through the New Mexico Higher Education Department. The Master of Security Science offered by the EC Council has been included in the list although it has not yet received accreditation. A search on the U.S. Department of Education –

Accreditation Web site (http://www.ope.ed.gov/accreditation/Search.aspx) confirms the program is not listed as an accredited program. However, it is the only computer-forensic program found that has similar specifications of the Network Forensic CBOK.

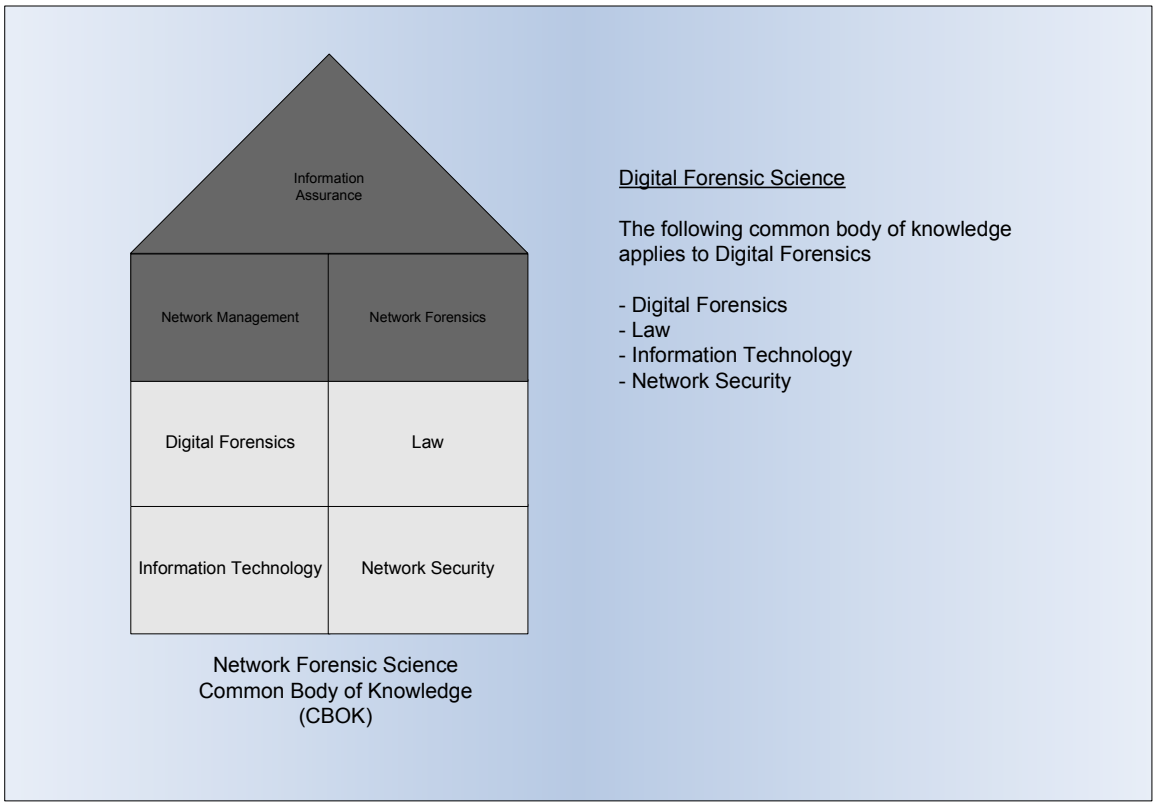
In Table 1, the common categories of each of the different programs are summarized for easier viewing. Information Technology and Network Security are listed as Foundation (F) because they are considered prerequisites for the post-graduate program. Information Assurance curriculum, Law and Network Forensics are optional courses as the research indicates the focus of the program is policies and standards in protecting information.

There is a direct relationship between digital forensics and network forensics in that they share the same core CBOK categories, excepting that Network Forensics Science includes Network Management and Network Forensics. Table 1 shows that Network Forensic Science includes Information Technology, Network Security, Digital Forensic, and Law. Through the research, it was confirmed that Network Forensic Science requires network management for development of network monitoring policy and network forensics to implement the monitoring policies.

EC Council's Master of Security Science is the most similar to a Network Forensic Science program with the exception that it does not include the Information Assurance category. Based on the research, network forensics has an important role in Information Assurance for the detection and protection of information (Qian et al, 2007). Based on that theory, BSc and MSc in Network Forensic Science are proposed programs with the Information Assurance category included.

Inter-relationships exist between disparate programs. As of today, there is no core curriculum for Network Forensic Science. The reality of the current situation has forced the study to widen the search into curriculum of similar computer-forensic programs. The study also has found some common categories and relationships between disparate programs. An inter-relationship between these programs and the CBOK is proposed:

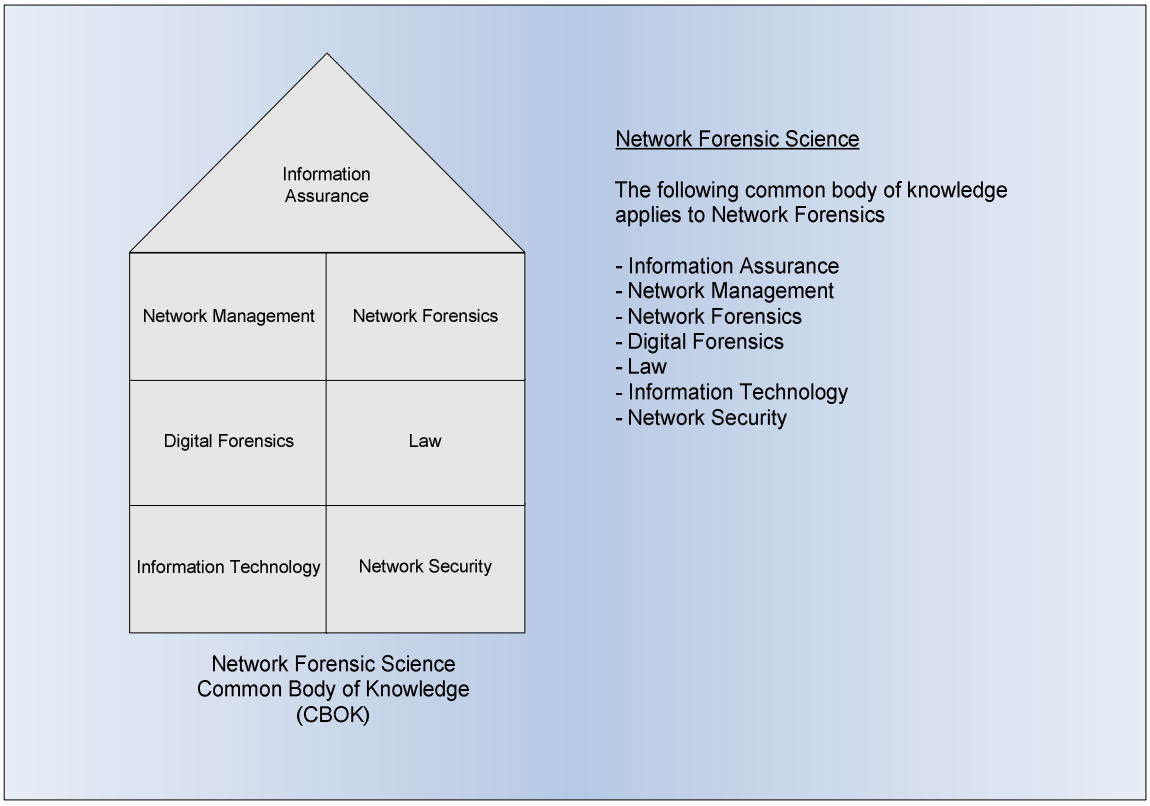
Figure 5. Digital Forensic Science



- Digital Forensics – investigate criminal activities on a single computer and present evidence in a court of law.
- Network Forensics – monitor, detect and trace intrusions on the network and investigate criminal activities on network devices by performing digital forensics.

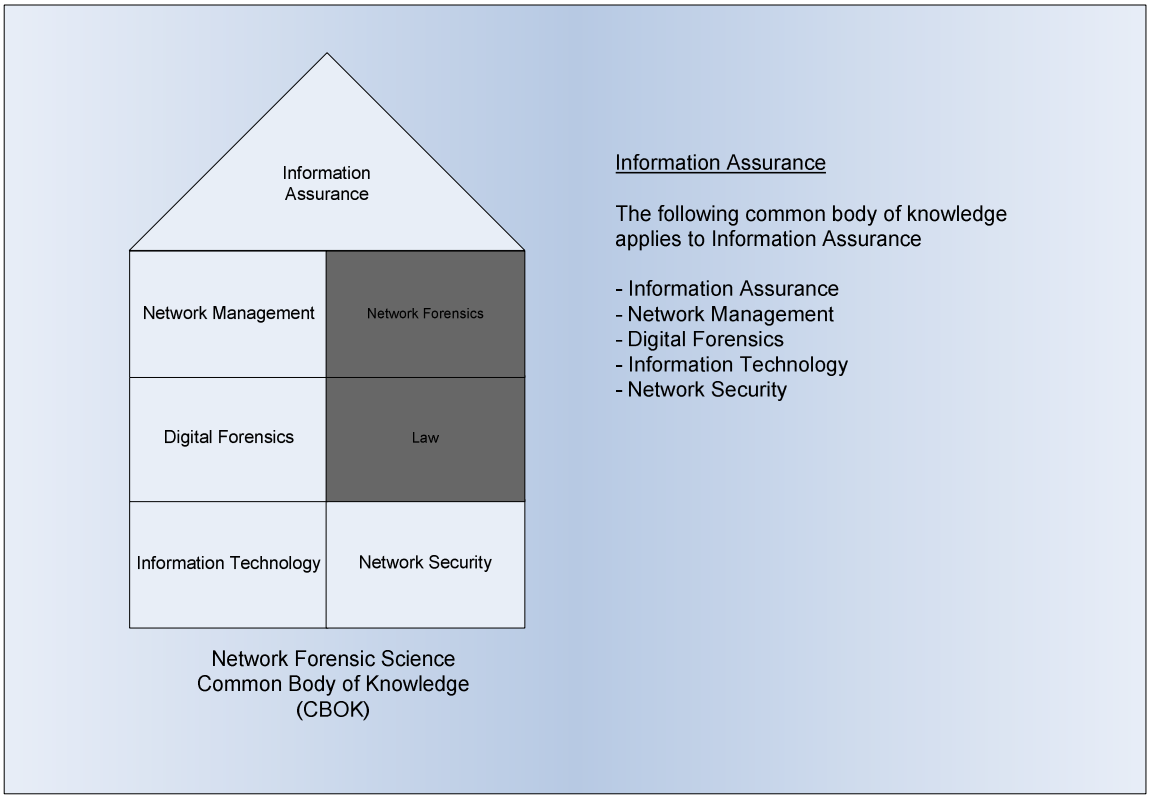
- Information Assurance – develop a security program utilizing security management and distributive detection systems to protect the information on a corporate network.

Figure 6. Network Forensic Science



Network forensic category is a key component for Information Dependency within Information Assurance (Qian et al, 2007). Information Assurance CBOK category is an important component for Network Forensics Specialists to be effective at planning, establishing and administering security and information assurance systems in commercial settings and in law enforcement" (McGuire, Murff, 2006). However, the Information Assurance program is not the same as a Network Forensic Science program as it does not include a law component.

Figure 7. Information Assurance



Study Conclusions

The intent of computer related forensic science programs is to prepare students for service in a variety of business, military and government arenas in digital forensics or as network security professionals (McGuire, Murff, 2006). Network Forensic Science is a new field of study and universities have little or no standards to follow in the development of their course content. Universities are reluctant to offer Network Forensic Science degree for the following reasons:

- The expense involved in building and maintaining expensive computer training labs;

- The difficulty in acquiring and retaining qualified instructors in law and computer forensic science when there are no inter-discipline law and computer science programs offered; and
- The lack of existing standards to develop their course curriculum.

Bogolea and Wijekumar have found in their research that different approaches are used to develop a computer-related forensics program at a university. These approaches include:

- Take an existing computer science program and implement a security specialty;
- Survey of security training and educational programs to develop the curriculum;
- Modify an existing computer science program so that it is a computer-related forensic program;
- Develop a framework via workshops and working groups of education experts to use in the development of the curriculum; and
- Survey and interview Information Technology professionals, and study workforce needs in Information Security to develop the curriculum.

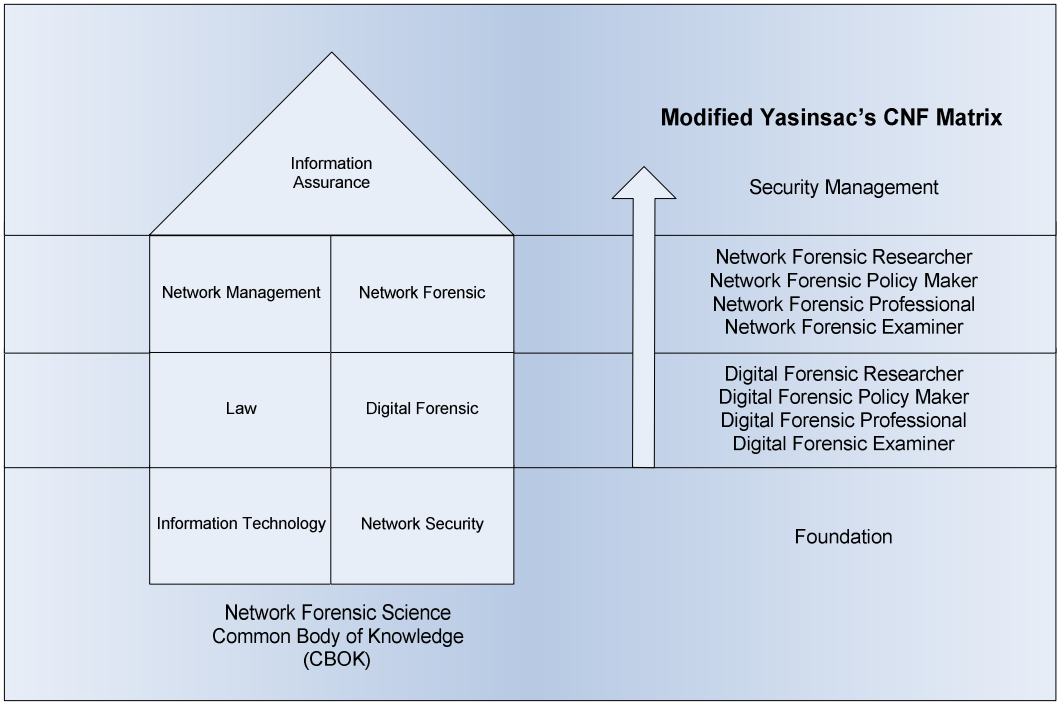
None of these approaches uses a CBOK methodology and the programs are very specific to their local requirements such as an association with a local police force. The study concludes that there is no international or national standards set specifically for Network Forensic Science.

The CBOK can be used as a building block for multiple computer-related forensic programs. By creating a four tier-level of knowledge, the skill set has an association to

the desired career path (Figure 8). The career paths used for this study are the Certified Network Forensic positions (Yasinsac at al, 2003) and are divided into the following positions:

- Technician – exercise the skills required to perform evidence gathering;
- Professional – exercise the technical skills required to perform evidence presentation with broad understanding of legal procedures and requirements;
- Policy Maker – make decisions on the balance of privacy and the forensic data gathering for early and distributive detection systems; and
- Researcher – contribute to knowledge in the advancement of network forensics science.

Figure 8. CBOK Relationship to Careers



The Common Body of Knowledge is presented with Yasinsac's Certified Network Forensics (CNF) Matrix (Yasinsac et al, 2003) and a proposed Certified Digital

Forensics Matrix (CDF) to show a hierarchical relationship between the seven categories and potential careers (figure 8).

Study Recommendations

The demand for security related Information Technology workers, digital forensics personnel, and incident response specialists is higher than for other IT and knowledge workers (McGuire, Murff, 2006). The development of curriculum in digital forensics and information assurance are far more developed than in network forensics. As a result, the network forensic programs are just beginning to appear at universities. The study recommends that:

- The field of network forensics and other computer-related forensics be recognized as a branch of forensic science;
- The Network Forensics Common Body of Knowledge be further developed in association with a forensic science organization ;
- The Forensic Science organization creates the certification standard for Network Forensic Science using the Common Body of Knowledge as a foundation.
- Universities use the Forensic Science organization's certification standard for Network Forensics Specialists to build an accredited Network Forensic Science program.

CHAPTER V

CONCLUSION AND RECOMMENDATIONS

The success of this study depends on adequately answering the three research questions.

Question 1

Can a common body of knowledge be created for Network Forensic Science to establish a national or international standard that can be used for Network Forensic Specialist certification and university curriculum accreditation? Yes. The study clearly indicates the skills required in Network Forensic Science fits into the seven proposed categories to form a common body of knowledge. I believe that this example of CBOK could establish a national or international standard to be used for certification or curriculum accreditation based on the precedent set by organizations such as the Canadian Information Processing Society and Project Management Institute. These organizations could use the CBOK approach for certification and accreditation.

Question 2

Can a common body of knowledge be validated against existing university curriculum? Yes. The study reviewed existing university curriculum and the findings are included in Chapter IV's Table 1. These findings clearly demonstrate that each of the seven categories of CBOK are used in existing curriculum and all seven categories are used within the curriculum's of Carnegie Mellon University, Norwich University and EC Council University, validating the use of CBOK.

Question 3

Can an existing curriculum be modified or new curriculum created by using the common body of knowledge approach? Yes. To demonstrate the creation of new curriculum in Network Forensic Science, the following example is proposed. The curriculum is composed of two elements: structure and content. The structure of the program is modeled on the Athabasca University's Master of Science in Information Systems framework (www.athabascau.ca). The original framework is based on the MSIS 2000 Model Curriculum which is sponsored by the Association for Computing Machinery (www.acm.org) and the Association for Information Systems (http://home.aisnet.org). The structure divides the courses into three categories:

- Foundation (minimum 3 credits) – to ensure that the students are prepared for the Core courses. The Survey course (Table 2) is mandatory for all students. Depending on the students' credentials and experience, the other foundation courses can be exempted on review of the program admission committee;
- Core (minimum 9 credits) – to advance the students' existing knowledge and skills in the basics of network forensics; and
- Specialization (minimum 12 credits) - to allow the student to choose a project approach or a specialization to complete the program.

The requirements are a minimum of 24 credits (eight 3-credit course or five 3-credit courses and the Project Specialization). Those with less academic credentials may be required to complete 39 credits (thirteen 3-credit courses or ten 3-credit courses and the Project Specialization).

The following table will demonstrate a Network Forensic Curriculum based on a MSIS model framework but using content based on the CBOK.

Table 2. Proposed Network Curriculum based on the CBOK

Network Forensic Science Curriculum		
Course Id	**Course Name**	**CBOK Category**
NF FOUNDATIONS		
NF 501	Systems Development with Emerging Technology	Information Technology
NF 502	IT Hardware and Software	Information Technology
NF 503	Operating Systems and Logs	Information Technology
NF 504	Network Security	Network Security
NF 601	Survey of Computing and Information Forensics	Network Forensics
NF CORE		
NF 602	Law and Expert Witness	Law
NF 603	Digital Forensics	Digital Forensics
NF 604	Network Forensics	Network Forensics
NF 605	Network Management	Network Management
NF 695	Research Methods in Network Forensics	Network Forensics
NF 696	Research Project/Essay	Network Forensics
SPECIALTIES		
Project Specialization		
NF 697,698,699	Network Forensic Application	Network Forensics
Examiner Specialization		
NF 610	Digital Forensics Investigation	Digital Forensics
NF 611	Ethical/Legal/Social Issues in Forensics	Law
NF 612	Network Forensics Lab	Network Forensics
Network Management Specialization		
NF 613	Data Mining	Information Technology
NF 614	Information Assurance	Information Assurance
Research Specialization		
NF 615	Artificial Intelligence	Network Forensics
NF 616	Advanced Network Forensics Lab	Network Forensics

At first glance, it is not apparent that the program is composed of all seven categories of the Network Forensic's CBOK. However, Table 3 presents the courses grouped by the CBOK's category. The right column lists the associated courses for each category. Each category has at least one course associated with it. Based on the CBOK, the new curriculum meets the requirements for accreditation.

Table 3. Grouping Courses by CBOK Category

Common Body of Knowledge Category	Course IDs
Information Technology	NF 501, NF 502, NF 503, NF 613
Network Security	NF 504
Law	NF 602, NF 611
Digital Forensics	NF 603, NF 610
Network Management	NF 605
Network Forensics	NF 601, NF 604, NF 695, NF 696, NF 697, NF 698, NF 699, NF 612, NF 615, NF 616
Information Assurance	NF 614

Although the course content itself meets the requirements based on the CBOK approach, the university must meet two other criteria to meet the requirements. The first criterion is the program should be offered at an inter-disciplinary university that operates a Criminal Justice program (McGuire, Murff, 2006). The second criterion is the requirement of a network laboratory (McGuire & Murff, 2006; Yasinsac et al, 2003; Stahl & Carroll-Mayer & Norris, 2006).

An existing curriculum can be modified or a new curriculum can be created based on the CBOK approach if the curriculum's content covers the seven categories of the CBOK, the university can provide the inter-disciplinary instructors, and the university has a fully functional independent network laboratory.

Further Research.

The common body of knowledge encompasses the skills and knowledge required in the network forensics' field. The application of the seven categories will work whether the principle owner of the certification is in the discipline of forensic science, security, or information systems. The common body of knowledge is scalable allowing for the level of concentration in the category to be adjusted to these roles: examiner, professional,

policy maker, and researcher (Yasinsac et al, 2003). Further research is required to develop the relationship of the CBOK to the applicable role.

Software tools were not discussed in the research study because the tools are constantly redesigned and created (Sitaraman & Venkatesan, 2006). The development of a university's forensic lab will depend on the most common applications used by the market most likely to be hiring the graduates.

One of the problems in forensic software development is that there is no complete single application tool used for digital and network forensics (Sitaraman, Venkatesan, 2006). Further study is required to develop a holistic tool for forensic monitoring and analysis. Any new software developed must pass the Daubert Test (Sitaraman & Venkatesan, 2006) which is administered through the National Institute of Justice (U.S) (www.ojp.usdoj.gov/nij/) and the National Institute of Standards and Technology (www.nist.gob/index.html).

The research and discovery of the CBOK for Network Forensics Science is an exploration of current literature on the topic. The research findings represent well founded but unfortunately quickly out-dated papers on forensic information. Anyone attempting to develop a Network Forensic Science program will need to maintain close working relationships with commercial and government agencies because these are the leaders concerned with infrastructure security, cybercrime, and digital forensics examination (McGuire & Murff, 2006). Working with them will enhance the curriculum by providing access to experts with practical experience and ensuring the content is adjusted annually to reflect current and relevant issues in Network Forensic Science.

Network Forensics Science is a multi-disciplinary program consisting of three disciplines: Forensics, Security, and Information Technology. The research study proposes that certification and accreditation should be controlled by the Forensic Science community. An important United States (U.S.) agency to be considered for the accreditation process is the Forensic Science Education Programs Accreditation Commission (FEPAC). FEPAC's (www.aafs.org) mission is to maintain and to enhance the quality of forensic science education through a formal evaluation and recognition of college-level academic programs. The Commission's function is to develop and maintain standards, and to administer an accreditation program that recognizes and distinguishes high quality undergraduate and graduate forensic science programs. These standards are used by many U.S. and Canadian universities offering Forensic Science programs. The accredited universities are listed on the website.

FEPAC is a committee within the American Academy of Forensic Sciences (Academy). The Academy (www.aafs.org) practices, teaches, and conducts research in forensic science. The Academy consists of eleven sections that maintain their own certification standards. The Academy has recently formed a new Digital and Multimedia Section that includes network forensics and the establishment of the certification could be developed in conjunction with this new section.

Further study is required for the development of certification and accreditation for those choosing an Information Systems or Security career track. In Information Systems, the approach could include creating a course or specialization within an existing program and working with similar organizations to develop an Information Systems model for Network Forensics.

Another approach would be to develop the certification and accreditation by the security community. There are several security organizations that offer certification that identify network forensic skills and there are opportunities to associate the CBOK to one of these certifications. Several Information Services and Security discipline organizations offer certifications that can be researched in respect to the CBOK (Appendix B).

Accreditation through a forensic organization will substantiate the Network Forensic Science certification while going through Information Systems or Security organizations will only certify the individual in Network Forensics. If the university's curriculum targets students interested in a career with the police force or government agency, the Network Forensic Science designation is critical. For those students interested in the protection of information and network assets, the path of network forensics is suitable. It is imperative that the university or college build the curriculum for accreditation based on the applicable disciplinary-organization's certification.

The recognition and acceptance is some form of the Network Forensic Science CBOK can provide a starting place for advancement and standards for network forensics. With the interrelationship between the three fields: Digital Forensics, Network Forensics and Information Assurance, the Network Forensic Science CBOK could be adopted as a national or international standard for all computer-related forensics and be used in university curriculum accrediation.

REFERENCES

Agaian, S.S., Rodriguez, B.M., (2006). Basic steganalysis techniques for the digital media Forensics Examiner. Appears in *Digital Crime and Forensics Science in Cyberspace, pp. 175-216* edited by Panagiotis Kenellis, Evangelos Kiountouzis,Nicholas Kolokotronis, and Drakoulis Martakos. 2006. Hershey, PA, USA. IGI Publishing

Anderson, G. Editor (2007). All you ever wanted to know about Forensic Science in Canada but didn't know who to ask! Canadian Society of Forensic Sciences. Retrieved from http://www.csfs.ca/

Bem, D., Huebner, E. (2008).Computer forensics workshop for undergraduate students, In *Proceedings of Tenth Australasian Computer Education Conference*. 2008, *Wollongong, Australia*

Brenner, S.W. (2007). History of computer crime, In Karl De Leeuw and Jan Bergstra, Editor(s), *The History of Information Security*, Elsevier Science B.V., Amsterdam, 2007, Pages 705-721, DOI: 10.1016/B978-044451608-4/50026-2.

Bogolea, B., Wijekumara, K.(2004).Information security curriculum creation: A case study. In *Proceedings of the 1st annual conference on Information security curriculum development.* Kennesaw, GA. pp55-69

Chang, J. (2009, July 14).S. Korean police: Hacker extracted data in attacks. *ABC News Technology & Science*. Retrieved from http://www.abcnews.go.com/

Chen, T.M., Davis, C. (2006). Overview of an electronic attack. Appears in *Digital Crime and Forensic Science in Cyberspace*. pp. 1 -26. Edited by Panagiotis Kenellis,

Evangelos Kiountouzis,Nicholas Kolokotronis, and Drakoulis Martakos. 2006. Hershey, PA, USA. IGI Publishing

Dardick, G.S., Lau, L.K.(2005). Interdisciplinary minor in digital forensics, security and law. In *Proceedings of the 6th conference on Information technology education.* pp 371-371. Newark, New Jersey. USA

Duhaime, L. (2009) Re: Criminal Law [Online Legal Dictionary] Retrieved from http://duhaime.org/LegalDictionary/C/CriminalLaw.aspx

Duncan, William R. (1996). *A Guide to the Project Management Body of Knowledge*. Upper Darby, PA USA: Project Management Institute. Retrieved from www.pmi.org

Endicott-Popovsky, B., Frincke, D.A., Taylor, C.A. (2007). A Theoretical Framework for Organizational Network Forensic Readiness. *Journal of Computers, Vol 2, No 3, May 2007.* Retrieved from http://www.academypublisher.net

Figg, W., Zhou, Z.(2007, April). A Computer Forensics Minor Curriculum Proposal. *In Journal of Computing Sciences Vol 22 Issue 4. pp 32-38* Consortium for Computing Sciences in Colleges, USA

Gonzales, A.R., Schofield, R.B., Hagy, D.W. (2007). Digital evidence in the courtroom: A Guide for Law Enforcement and Prosecutors. U.S. Department of Justice. Retrieved from http://www.ncjrs.gov/pdffiles1/nij/211314.pdf

Hamill, J.T., Deckro, R.F, Kloeber Jr, J.M.(2004). Evaluating Information Assurance Strategies. *Decision Support Systems 39Issue 3 (2004, May) pp 463-484*. Department of Operational Sciences, Air Force Institute of Technology, USA

Hansman S., Hunt R. (2005, February). A taxonomy of network and computer attacks, *Appears in Computers & Security, Volume 24, Issue 1, February 2005, Pages 31-43.* DOI: 10.1016/j.cose.2004.06.011.

Kahai, P., Namuduri, K., Pendse, R. (2006).Tracing cyber crimes with a privacy-enabling forensic profiling system. *Digital Crime and Forensics Science in Cyberspace, pp. 138-154.* Eedited by Panagiotis Kenellis, Evangelos Kiountouzis,Nicholas Kolokotronis, and Drakoulis Martakos. 2006. Hershey, PA, USA. IGI Publishing

Kaufman, C., Perlman, R., Speciner, M. (2002). *Second Edition Network Security Private Communication in a Public World*. 2002 Upper Saddle River, NJ, USA. Prentice Hall Press

Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., Wright, C. (2007). In Dave Kleiman, Kevin Cardwell, Timothy Clinton, Michael Cross, Michael Gregg, Jesse Varsalone and Craig Wright, Editor(s), *The Official CHFI Study Guide (Exam 312-49*), Syngress, Rockland, 2007, Pages iii-vi, DOI: 10.1016/B978-159749197-6.50001-8.

Kruse, W., Heiser, J. (2002). Computer forensics: Incident response essentials. Addison Wesley.

Leung, C-M., Chan, Y-Y.(2007). "Network Forensics on Encrypted Peer-to-Peer VoIP Traffics and the Detection, Blocking, and Prioritization of Skype Traffics. Iin Proceedings of 16th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. June 2007

Malinowski, C.,(2006). Training the Cyber Investigator. *Digital Crime and Forensics Science in Cyberspace, pp. 311-333.* Edited by Panagiotis Kenellis, Evangelos

Kiountouzis,Nicholas Kolokotronis, and Drakoulis Martakos. 2006. Hershey, PA, USA. IGI Publishing

McGuire, T.J., Murff, K. N. (2006, December). Issues in the development of a digital forensics curriculum. *Journal of Computing Sciences in Colleges Vol 22, Issue 2. pp 274-280.* Consortium for Computer Sciences in Colleges.

Mukkamala, S., Sung, A.H.(2003). Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques. In *International Journal of Digital Evidence. Winter 2003, Volume 1, Issue 4, pp. 1-17.* Retrieved from http://www.utica.edu/academic/institutes/ecii/publications/articles/A04CCCB9-D778-B3D4-3C9A98DB4B0F99D1.pdf

Qian, Y., Joshi, J., Tipper, D., Krishnamurthy, p.(2008), Information Assurance, Information Assurance, Morgan Kaufmann, Burlington, 2008, Pages 1-15, DOI: 10.1016/B978-012373566-9.50003-3.

Ritchie, J., Lewis, J. (2003). *Qualitative Research Practice: A Guide for Social Science Students and Researchers.* 2003. London: Sage Publications

Rittinghouse, J.W., Hancock, W.M.(2004). Network Security Management Basics. In *Cybersecurity Operations Handbook*, Digital Press, Burlington, 2004, Pages 25-61. DOI: 10.1016/B978-155558306-4/50007-X.

Sitaraman, S., Venkatesan S.(2006). Computer and network forensics. Appears in *Digital Crime and Forensics Science in Cyberspace, pp. 56-74* edited by Panagiotis Kenellis, Evangelos Kiountouzis,Nicholas Kolokotronis, and Drakoulis Martakos. 2006. Hershey, PA, USA. IGI Publishing

Soe, L.L., Manson, D., Wright, M.(2004).Establishing network computer forensics classes. In *proceedings of the 1th conference on Information security curriculum development.* Kennesaw, GA, U.S.A

Stahl, B.C., Carroll-Mayer, M., Norris, P. (2006). Forensic computing: The problem of developing a multidisciplinary university course. Appears in *Digital Crime and Forensics Science in Cyberspace, pp. 291- 310* edited by Panagiotis Kenellis, Evangelos Kiountouzis,Nicholas Kolokotronis, and Drakoulis Martakos. 2006. Hershey, PA, USA. IGI Publishing

Tipton, H.F., Krause, M. (2007). *Information Security Management Handbook, Sixth Edition*. Boston, MA, USA. Auerbach Publications.

Thomas, D.S., Forcht, K.A.(2004). Legal Methods of Using Computer Forensics Techniques for Computer Crime Analysis and Investigation, *Information Systems, Volume V, No 2, 2004, pp. 692-698.* Retrieved from http://www.iacis.org/iis/2004_iis/PDFfiles/ThomasForcht.pdf

Troell, L., Pan, Y., Stackpole, B. (2004).Forensic course development – one year later. In *proceedings of the 5th conference on Information technology education.* Pages 50-55. Salt Lake City, Utah, U.S.A.

Von Solms, S.H., Louwrens, C.P. (2006).The relationship between digital forensics, corporate governance, IT governance and IS governance. Appears in *Digital Crime and Forensics Science in Cyberspace, pp. 243-265* edited by Panagiotis Kenellis, Evangelos Kiountouzis,Nicholas Kolokotronis, and Drakoulis Martakos. 2006. Hershey, PA, USA. IGI Publishing

Wassenaar, D., Woo, D., Wu, P.(2009).A Certificate program in computer forensics. Paper presented at the Second Annual CCSC Southwestern Conference, Pages 158-167. Consortium for Computing Science in Colleges, USA.

Wiles, J., Reyes, A., (2007) Contributing Authors, The Best Damn Cybercrime and Digital Forensics Book Period, Syngress Burlington, 2007

Yasinsac, A., Erbacher, R.F.., Marks, D.G., Pollit, M.M., Sommer, P.M. (2003). Computer forensics education. *Security & Privacy Magazine, IEEE*, I(4), 15-23. doi: 10.1109/MSECP.2003.1219052

Yeager, R (2006, September). Criminal computer forensics management. *Proceedings of the 3rd annual conference on Information security curriculum development*. Kennesaw, GA USA. Pp 168 – 174. doi: 10.1145/1231047.1231085

APPENDIX A

PROPOSED

COMMON BODY OF KNOWLEDGE

FOR NETWORK FORENSIC SCIENCE

1. INFORMATION TECHNOLOGY

1.1. Overview

Information Technology covers the background knowledge that enables the network forensic specialist to develop an understanding of computer architecture, digital media, operating systems, and networks components. The specialist will apply the information technology knowledge for the purpose of performing digital and network forensics in the business, government, or police arenas.

1.2. Skills

1.2.1. Computer Architecture

- 1.2.1.1. Data Representation
- 1.2.1.2. Digital Logic
- 1.2.1.3. Process Organization
- 1.2.1.4. Memory Systems
- 1.2.1.5. Input/Output Interfacing

1.2.2. Digital Media

- 1.2.2.1. Files
- 1.2.2.2. Slack Space
- 1.2.2.3. Swap File
- 1.2.2.4. Unallocated partitions
- 1.2.2.5. Hidden partitions

1.2.3. Operation Systems

- 1.2.3.1. Windows
- 1.2.3.2. Linux

1.2.4. Networking

- 1.2.4.1. Digital Communications
- 1.2.4.2. Local Area Networks
- 1.2.4.3. Wide Area Networks
- 1.2.4.4. Inter Networks
- 1.2.4.5. Errors
- 1.2.4.6. Network Security

2. NETWORK SECURITY

2.1. Overview

Network Security covers the background knowledge that enables the specialist to ensure (a) a user is who they say they are, (b) the user has the need to access the information, and (c) the information is protected to prevent others from gaining access.

2.2. Skills

2.2.1. Risks

- 2.2.1.1. Identify the risks (e.g. viruses, worms, trojans)
- 2.2.1.2. Identify probability and impact of the risk
- 2.2.1.3. Establish contingency plan
- 2.2.1.4. Establish disaster recovery plans

2.2.2. Attacks

- 2.2.2.1. Know the types of attacks
  - 2.2.2.1.1. Probing
  - 2.2.2.1.2. Denial of Service
  - 2.2.2.1.3. U2Su: Unauthorized access to super user (root) privileges
  - 2.2.2.1.4. R2L: Unauthorized access from a remote machine

2.2.3. Detection

- 2.2.3.1. Know the phases of attack and the methods used in each
  - 2.2.3.1.1. Reconnaissance
    - 2.2.3.1.1.1. Footprinting
    - 2.2.3.1.1.2. Active scanning
    - 2.2.3.1.1.3. Vulnerability scanning
  - 2.2.3.1.2. Gaining Access
    - 2.2.3.1.2.1. Sniffing
    - 2.2.3.1.2.2. Session hijacking
    - 2.2.3.1.2.3. Password attacks
    - 2.2.3.1.2.4. Vulnerability exploits
    - 2.2.3.1.2.5. Social Engineering
    - 2.2.3.1.2.6. Malicious Code
  - 2.2.3.1.3. Cover Up
    - 2.2.3.1.3.1. Evading IDS
    - 2.2.3.1.3.2. Modifying logs
    - 2.2.3.1.3.3. Rootkits
    - 2.2.3.1.3.4. Covert channels

2.2.4. Protection

- 2.2.4.1. Authentication
- 2.2.4.2. Cryptography
- 2.2.4.3. Standards

2.2.4.3.1. Encryption algorithms
2.2.4.3.2. Real time session security
2.2.4.3.3. Certificates
2.2.4.4. Electronic Mail
2.2.4.4.1. Encryption
2.2.4.4.2. Electronic signature

3. LAW

3.1. Overview

Law covers the background knowledge that enables the network forensic specialist to adhere to the legal and professional ethics standard of the profession. The legal implications can cross multiple jurisdictions and can be criminal or civil or both. Presenting of evidence must be complete, impartial, and with full disclosure to the defence. At all times, the network forensic specialist must demonstrate strong professional ethics and moral responsibility to themselves, to others, the School, and their employer

3.2. Skills

- 3.2.1. Criminal Law – *actus reus* and *mens rea*: The act and the intent

- 3.2.2. International Law
  - 3.2.2.1. Jurisdiction
  - 3.2.2.2. International Treaty

- 3.2.3. Civil Law
  - 3.2.3.1. Contract
    - 3.2.3.1.1. Offer
    - 3.2.3.1.2. Acceptance
    - 3.2.3.1.3. Consideration
  - 3.2.3.2. Torts
    - 3.2.3.2.1. Tort of conversion – use as not intended

- 3.2.4. Procedural Law
  - 3.2.4.1. Process
    - 3.2.4.1.1. Search and Seizure
    - 3.2.4.1.2. Integrity, Discovery, and Disclosure of Digital Evidence
    - 3.2.4.1.3. Courtroom Preparation and Evidence Rules
    - 3.2.4.1.4. Presentation of Digital Evidence Rules
    - 3.2.4.1.5. Presentation of Digital Evidence
  - 3.2.4.2. Principles
    - 3.2.4.2.1. Authorization
    - 3.2.4.2.2. Handling of Evidence
    - 3.2.4.2.3. Expert Opinion
    - 3.2.4.2.4. Disclosure to Defence

- 3.2.5. Ethics
    - 3.2.5.1.1. present evidence in a subjective way to allow others to determine the guilt or innocence
    - 3.2.5.1.2. exculpatory evidence must be disclosed
    - 3.2.5.1.3. professional ethical standards

3.2.5.1.4. not to use for criminal activity or personal gain

4. DIGITAL FORENSICS

4.1. Overview

Digital Forensics covers the background knowledge that enables the network forensic specialist to preserve, identify, extract, and document computer evidence. The specialist must demonstrate an understanding of the importance to follow procedural law in the management of digital evidence and be able to provide expert testimony in a court of law.

4.2. Skills

- 4.2.1. Preserve
  - 4.2.1.1. Order of Volatility
  - 4.2.1.2. Chain of Custody
  - 4.2.1.3. Preservation of original
  - 4.2.1.4. Authentication
    - 4.2.1.4.1. MD5
    - 4.2.1.4.2. SHA

- 4.2.2. Identify
  - 4.2.2.1. Media
    - 4.2.2.1.1. random access memory
    - 4.2.2.1.2. flash drives
    - 4.2.2.1.3. floppy drives
    - 4.2.2.1.4. hard drives
    - 4.2.2.1.5. portable devices
  - 4.2.2.2. Locations
    - 4.2.2.2.1. Slack space
    - 4.2.2.2.2. Unallocated space
    - 4.2.2.2.3. Registries
    - 4.2.2.2.4. Hidden files
    - 4.2.2.2.5. Encrypted files
    - 4.2.2.2.6. Password-protected files
    - 4.2.2.2.7. System logs.

- 4.2.3. Extract
  - 4.2.3.1. Methods
    - 4.2.3.1.1. reading the partition table,
    - 4.2.3.1.2. searching existing files for relevant information such as keywords, system state changes, text strings
    - 4.2.3.1.3. retrieving information from deleted files,
    - 4.2.3.1.4. checking for data hidden in boot record, unallocated space, slack space or bad blocks in the disk

4.2.3.1.5. Cracking passwords

4.2.3.2. Steganography

4.2.4. Document computer evidence

4.2.4.1. Protocol

4.2.4.1.1. Examine the original evidence as little as possible. Copy the original and test on the copy

4.2.4.1.2. Follow the rule of evidence and do not tamper with the evidence

4.2.4.1.3. Prepare a chain of custody and keep it accurate

4.2.4.1.4. Document any change to the evidence

4.2.4.1.5. Do not make opinions or comments that are outside the knowledge base of the specialist

4.2.4.2. Daubert Criteria for software:

4.2.4.2.1. The tool must be tested against a known data set for accuracy, reliability, and repeatable of identifying the attacks

4.2.4.2.2. The software has gone through peer-review

4.2.4.2.3. The forensic community accepts the methodology as valid.

5. NETWORK FORENSICS

5.1. Overview

Network Forensics covers the background knowledge that enables the network forensic specialist to monitor, detect, and trace intrusions on the network. By using basic and distributive detection systems, the specialist will set up security policies that will initiate alerts when an intrusion occurs. When an alert does occur, the specialist will be able to identify the affected systems, perform recoveries, trace the intruder to the source, and commence an investigation by collecting digital forensics.

5.2. Skills

5.2.1. Identify real-time attacks

5.2.2. Perform backup recovery

5.2.3. Initiate IP Tracing

5.2.4. Perform attack trace back and reconstruction

5.2.5. Commence Forensic Investigation

5.2.6. Use Forensic Software

5.2.6.1.Early Detection Systems

5.2.6.2.Distributive Detection Systems

5.2.6.3.Forensics ToolKits

6. SECURITY MANAGEMENT

6.1. Overview

Security Management covers the background knowledge that enables the network forensic specialist to create, implement, and monitor security policies as defined in the corporation's security governance. The specialist will be able to apply the principle of security management to safeguard the assets and to establish a network forensic response team to manage incidents.

6.2. Skills

6.2.1. Principles of Security Control

- 6.2.1.1. Proprietary of information
- 6.2.1.2. Compliance of established rules
- 6.2.1.3. Safeguarding of assets
- 6.2.1.4. Efficient use of resources
- 6.2.1.5. Accomplishment of established goals and objectives.

6.2.2. Methods of Security Control

- 6.2.2.1. Control environment
- 6.2.2.2. Risk assessment
- 6.2.2.3. Control activities
- 6.2.2.4. Information and Communication
- 6.2.2.5. Monitoring

6.2.3. Network Forensic Response

- 6.2.3.1. Resist
- 6.2.3.2. Recognize
- 6.2.3.3. Recovery
- 6.2.3.4. Redress

7. INFORMATION ASSURANCE

7.1. Overview

Information Assurance covers the background knowledge that enables the network forensic specialist to protect, detect, and restore the systems against all threats be it intrusions or system errors. To make the systems trustworthy and reliable, the specialist should apply the principles of information assurance technical framework.

7.2. Skills

7.2.1. Protect and defend Information and Information systems by
- 7.2.1.1. Availability
- 7.2.1.2. Integrity
- 7.2.1.3. Identification and authentication
- 7.2.1.4. Confidentiality, and
- 7.2.1.5. Non-repudiation

7.2.2. Provide restoration by
- 7.2.2.1. Protection
- 7.2.2.2. Detection
- 7.2.2.3. Restoration

7.2.3. Use technologies and processes such as
- 7.2.3.1. Multilevel security
- 7.2.3.2. Access controls
- 7.2.3.3. Secure network servers
- 7.2.3.4. Intrusion detection software

7.2.4. Know the four categories of boundaries
- 7.2.4.1. Local computing environments
- 7.2.4.2. Enclave boundaries
- 7.2.4.3. Network and infrastructure
- 7.2.4.4. Supporting infrastructures

7.2.5. Understand the source of attacks
- 7.2.5.1. Passive
- 7.2.5.2. Active
- 7.2.5.3. Close-in
- 7.2.5.4. Insider
- 7.2.5.5. Distribution

7.2.6. Understand the principles of Information Assurance
- 7.2.6.1. People
- 7.2.6.2. Operations
- 7.2.6.3. Technology

APPENDIX B

COMPUTER FORENSIC ORGANIZATIONS

The following table consists of a few organizations that have an interest in network forensic.

Table B1. Organizations with Computer-Forensic interests

Organization	Certification	Discipline	Website
International Association of Computer Investigation Specialist		Forensic Science	www.iacis.com
High Technology Crime Investigation Association		Forensic Science	www.htcia.org
International Society Computer Examiners		Forensic Science	www.isfce.com
Institute of Electrical and Engineers		Forensic Science	www.ieee.org
GIAC	GIAC	Information Assurance	http://www.giac.org/
Information Systems Security Management Profession ISC^2	CISSP-ISSMP	Security	http://www.iscw.org
SCP	SCNA	Security	http://www.securitycertified.net/

APPENDIX C

CBOK ASSESSMENT OF CURRICULUM

Table C1. CBOK Categories Identified in Master of Security Science

University	IT	NS	Law	DF	SM	NF	IA
EC Council University	1	1	1	1	1	1	
Total	1	1	1	1	1	1	

Abbreviations IT = Information Technology, NS = Network Security, DF = Digital Forensics, SM = Security Management, NF = Network Forensics, IA = Information Assurance

Table C2. CBOK Categories Identified in Master of Science in Digital Forensics

University	IT	NS	Law	DF	SM	NF	IA
Charles Sturt University		1	1	1	1		1
Middlesex University		1	1	1	1		
UCF	1	1	1	1	1		
Sam Houston State University	1	1	1	1			1
De Montfort University		1	1	1	1		
Total	2	5	5	5	4		2

Abbreviations IT = Information Technology, NS = Network Security, DF = Digital Forensics, SM = Security Management, NF = Network Forensics, IA = Information Assurance

Table C3. CBOK Categories Identified in Master of Science in Information Assurance

University	IT	NS	Law	DF	SM	NF	IA
Carnegie Mellon University	1	1		1	1	1	1
Norwich University	1	1	1	1	1		1
Total	2	2	1	2	2	1	2

Abbreviations IT = Information Technology, NS = Network Security, DF = Digital Forensics, SM = Security Management, NF = Network Forensics, IA = Information Assurance

Table C4. CBOK Categories Identified in Bachelor of Science in Digital Forensic

University	IT	NS	Law	DF	SM	NF	IA
De Montfort University	1	1	1	1	1		
University of Portsmouth	1	1	1	1	1		
Total	2	2	2	2	2		

Abbreviations IT = Information Technology, NS = Network Security, DF = Digital Forensics, SM = Security Management, NF = Network Forensics, IA = Information Assurance

Table C5. Universities Website

University	Degree	Web Site
Charles Sturt University	MSc in Digital Forensics	http://www.itmasters.edu.au/
Middlesex University	Msc Electronic Security and Digital Forensics	http://www.mdx.ac.uk/
UCF	MSc in Digital Forensic	http://msdf.ucf.edu/
Sam Houston State University	MSc in Digital Forensics	http://www.df.shsu.edu/
De Montfort University	MSc Computer Security	http://www.dmu.ac.uk/
EC Council University	Master of Security Science	http://www.eccuni.us/
Carnegie Mellon University	Information Security Technology and Management	http://www.ini.cmu.edu/degrees/index.html
Norwich University	MSc in Information Assurance	http://infoassurance.norwich.edu/curriculum_overview.php
De Montfort University	BSc Honours Forensic Computing	http://www.dmu.ac.uk/Subjects/Db/coursePage2.php?courseID=1033
University of Portsmouth	BSc of Digital Forensics	http://www.port.ac.uk/courses/coursetypes/undergraduate/BScHonsDigitalForensics/whatwillistudy/