Mississippi State University
Scholars Junction

Theses and Dissertations | Theses and Dissertations

1-1-2010

A concept mapping case domain modeling approach for digital forensic investigations

April L. Tanner

Follow this and additional works at: https://scholarsjunction.msstate.edu/td

Recommended Citation
Tanner, April L., "A concept mapping case domain modeling approach for digital forensic investigations" (2010). *Theses and Dissertations*. 83.
https://scholarsjunction.msstate.edu/td/83

This Dissertation - Open Access is brought to you for free and open access by the Theses and Dissertations at Scholars Junction. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of Scholars Junction. For more information, please contact scholcomm@msstate.libanswers.com.

www.manaraa.com

A CONCEPT MAPPING CASE DOMAIN MODELING APPROACH

FOR DIGITAL FORENSIC INVESTIGATIONS

By

April LaShai Tanner

A Dissertation
Submitted to the Faculty of
Mississippi State University
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy
in Computer Science
in the Department of Computer Science and Engineering

Mississippi State, Mississippi

December 2010

www.manaraa.com

Copyright by

April LaShai Tanner

2010

www.manaraa.com

A CONCEPT MAPPING CASE DOMAIN MODELING APPROACH

FOR DIGITAL FORENSIC INVESTIGATIONS

By

April LaShai Tanner

Approved:

David A. Dampier Associate Professor of Computer Science and Engineering (Major Professor and Director of Dissertation)	Rayford Vaughn Bill and Carolyn Cobb Professor of Computer Science and Engineering and Associate Vice President for Research (Committee Member)
Yoginder Dandass Associate Professor of Computer Science and Engineering (Committee Member)	Mahalingam Ramkumar Associate Professor of Computer Science and Engineering (Committee Member)
Edward Allen Associate Professor and Graduate Coordinator of Computer Science and Engineering	Sarah A. Rajala Dean of James Worth Bagley College of Engineering

www.manaraa.com

Name: April LaShai Tanner

Date of Degree: December 10, 2010

Institution: Mississippi State University

Major Field: Computer Science and Engineering

Major Professor: Dr. David A. Dampier

Title of Study: A CONCEPT MAPPING CASE DOMAIN MODELING APPROACH FOR DIGITAL FORENSIC INVESTIGATIONS

Pages in Study: 168

Candidate for Degree of Doctor of Philosophy

Over the decades, computer forensics has expanded from primarily examining computer evidence found on hard drives into the examination of digital devices with increasing storage capacity, to the identification of crimes and illegal activities involving the use of computers, to addressing standards and practices deficiencies, and to addressing the need to educate and train law enforcement, computer forensic technicians, and investigators.

This dissertation presents the concept mapping case domain modeling approach to aid examiners/investigators in searching and identifying digital evidence and analyzing the case domain during the examination and analysis phase of the computer forensic investigation. The examination and analysis phases of a computer forensic process are two of the most important phases of the investigative process because the search for and identification of evidence data is crucial to a case; any data uncovered will help determine the guilt or innocence of a suspect. In addition, these phases can become very

www.manaraa.com

time consuming and cumbersome. Therefore, finding a method to reduce the amount of time spent searching and identifying potential evidence and analyzing the case domain would greatly enhance the efficiency of the computer forensic process.

The hypothesis of this dissertation is that the concept mapping case domain modeling approach can serve as a method for organizing, examining, and analyzing digital forensic evidence and can enhance the quality of forensic examinations without increasing the time required to examine and analyze forensic evidence by more than 5%. Four experiments were conducted to evaluate the effectiveness of the concept mapping case domain modeling approach. Analysis of the experiments supports the hypothesis that the concept mapping case domain modeling approach can be used to organize, search, identify, and analyze digital evidence in an examination.

www.manaraa.com

DEDICATION

I would like to dedicate this research to my husband, Wade Tanner Jr., my children, Wade III and Anye', my parents Willie F. Butler and Anna and Dan McGrew, and Gennette and Wade Tanner Sr.

www.manaraa.com

ACKNOWLEDGMENTS

The author expresses her sincere gratitude to the following individuals and groups for providing support throughout this research work:

- The author's entire family for their constant support and encouragement throughout my journey,
- The author's PhD advisor, Dr. David Dampier, for his constant encouragement, guidance, and support throughout the doctoral program and the dissertation process,
- The author's PhD committee,
- The Mississippi State Attorney General's Office (MSAGO) Cyber Crime Unit,
- Gary Cantrell and Kendall Blaylock for their assistance with planning and creating seminar classes,
- Attendees of the CF 510: Investigative and Examination Planning class, and
- Countless friends and acquaintances.

www.manaraa.com

TABLE OF CONTENTS

www.manaraa.com

www.manaraa.com

www.manaraa.com

LIST OF TABLES

TABLE

www.manaraa.com

www.manaraa.com

www.manaraa.com

LIST OF FIGURES

FIGURE

www.manaraa.com

www.manaraa.com

CHAPTER I

INTRODUCTION

This dissertation explores the use of the concept mapping case domain modeling approach as a method for organizing the search and identification of digital forensics evidence during a computer forensics examination. This is important because cases are getting larger and more complex, and investigators need a way to help organize and sort data. The remaining sections of this chapter are organized as follows: Sections 1.1 discusses computer forensics procedure and research, Section 1.2 discusses the motivations for this dissertation, Section 1.3 presents the hypothesis of this dissertation, Section 1.4 highlights the expected contributions of this dissertation, and Section 1.5 provides an overview of the remainder of this document.

1.1 Computer Forensics

With the development of every new type of technology, criminals find ways to get around security mechanisms and commit crimes in some fashion. In computer forensics, crimes can be committed against the computer and crimes can be committed using the computer. Computer forensics requires that computer data be preserved, identified, extracted, documented, and interpreted [33, 41]. A few of the many crimes associated with computer forensics are child pornography, cyberstalking, economic espionage, online fraud, threatening letters or emails, identity theft, and hacking. These criminal

www.manaraa.com

activities are on the rise each year [70]. In 1984, the FBI and other law enforcement agencies began developing programs to examine computer evidence.

The FBI soon developed the Computer Analysis and Response Team (CART) to handle the growing need for computer evidence examinations. One of the main problems encountered by law enforcement was identifying resources within the organization that could be used to examine evidence. In May 1998, a Technical Working Group was established to address the forensic issues related to digital evidence. This led to the development of definitions, standards, and principles by the Scientific Working Group on Digital Evidence (SWGDE) later that year in August.

As a result of the continual advancements in technology, forensic criminal investigations have moved beyond computers to include digital technologies such as PDAs, cell phones, CDs, DVDs, mp3 players, IPods, thumb drives, external hard drives, and many other digital devices. The investigation of these devices including computers is better known as digital forensics. Digital forensics includes the forensics of all digital technology, including network forensics, software forensics, and computer forensics [7, 45, 49]. Network forensics requires that evidence from a network of computers is collected, analyzed, and preserved. Software forensics involves identifying the original author of a piece of software, malware, malicious code, virus, etc. [7]. At the first annual Digital Forensics Research Workshop (DFRWS) in 2001, digital forensic science was defined as [45]:

> "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence sources for the purposes of facilitating or

www.manaraa.com

> furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."

This dissertation focuses on the concept mapping case domain modeling approach for searching and identifying digital evidence and for analyzing the case domain during the examination and analysis phases of a digital forensic investigation.

1.1.1 Basic Forensic Methodology

Although technology continues to change, basic forensic methodology remains constant. The basic forensic methodology consists of the three A's which are acquiring the evidence without damaging or altering the original, authenticating that the recovered evidence and the originally seized data are the same, and analyzing the data without modifications [33]. Authentication ensures that evidence has not been altered in any way during the investigation. Evidence can be authenticated both physically and logically. Physical authentication requires a thorough chain of custody, detailed documentation, photographs of the computer setup and computer screen, and a secure storage location with limited access to the evidence. Logical authentication requires tasks such as working with copies of the original evidence, minimizing access to the original evidence, utilizing a write blocking mechanism during the imaging process, and the usage of hash algorithms to prove that working copies of the original evidence are identical to the original. This is also known as proof of integrity. Additionally, timestamping is an important element of authentication because it is used to show the existence of evidence at a specific point in time. Analyzing evidence involves combining all the evidential findings to determine what occurred. Analyzing the evidence is important during the

www.manaraa.com

examination of the evidence and for presentation of the evidence findings in court [33]. The proper application of these three basic methodologies is crucial during a digital investigation. Although, general steps were discussed, a more in depth and structured process is needed to properly guide the investigation of a digital crime.

1.1.2 The Digital Forensic Process

There is currently no universally adopted model for the forensic investigative process; however, the DFRWS investigative process model was created by a group of experts in the field composed of university researchers, computer forensic examiners, and analysts. This model was intended to determine any shortfalls that were occurring in the process and to determine areas where research was needed most. According to [45], the major categories or classes of the digital forensics process consist of identification, preservation, collection, examination, analysis, and presentation. Issues for each category were provided for each step in the investigative process. This dissertation used the DFRWS investigative process model shown in Table 1.1 as a basis for developing the concept mapping case domain model. Sections 1.1.2.1-1.1.2.7 briefly discuss the major phases of the DFRWS digital forensic investigative process. More details about the investigative process can be found in [2, 10, 22, 27, 38-42, 44, 46, 53, 58, 59, 65, 66, 71-75].

www.manaraa.com

Table 1.1 The DFRWS Investigative Process for Digital Forensic Investigations

Identification	Preservation	Collection	Examination	Analysis	Presentation
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation
Resolve Signature	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation
Audit Analysis		Sampling		Link	
		Data Reduction		Spatial	
		Recovery Techniques			

1.2.1.1 Identification

Event or crime detection is one of the first tasks listed in the DFRWS model. Once this occurs, one of the main goals is to determine what items, components, and data are associated with the digital crime. For instance, the crime scene should be photographed and documented in detail. Additional tasks associated with identifying evidence include taking 360 degree photos of the room with all the possible connections to and from the evidence, properly identifying and labeling of every piece of evidence taken from the suspect's location, and taking several photographs of the area surrounding the evidence. By photographing connections, the crime scene can be reconstructed and questions can be answered about the evidence environment in court. According to Kruse [33], pictures of the screen including any open files, the complete computer system, any identifying features on the evidence, and all other potential evidence items should be photographed. Potential evidence items include laptops, desktops, external hard drives,

www.manaraa.com

CDs, DVDs, floppy disks, thumb drives, cell phones, PDAs, gaming consoles, mp3 players, IPods, printers, fax machines, etc. In addition, written reports should contain extensive details about the evidence taken from the crime scene. Information such as software and version numbers, collection tools used, methods used to collect the evidence, and explanations detailing why evidence was collected in a specific way are all important aspects of the identification process that should be documented and included in the investigator's report [33].

1.2.1.2 Preservation

The chain of custody procedures are one of the most important tasks associated with this phase [10, 33]. Thorough documentation of the chain of custody helps to ensure the authenticity of the evidence and aids in refuting claims of evidence tampering. It also provides complete details pertaining to the possession of the evidence during the life of a case. These details decrease the likelihood that evidence will not be admitted in court. During this phase, the entire journey of the evidence must be accounted for from the crime scene to the courtroom. For instance, the chain of custody establishes who collected the evidence, how and where the evidence was collected, who took possession of the evidence, how the evidence was protected and stored, who removed it from storage and the reason for its removal [33]. Other tasks associated with this phase include properly shutting down the computer or evidence item, transporting the evidence to a secure location, and limiting access to the original evidence.

www.manaraa.com

1.2.1.3 Collection

Collection involves using approved methods, software, hardware, and recovery techniques to collect the evidence. In addition, documentation should be as detailed as possible. Any items of evidentiary value, such as those items mentioned in the identification phase, should be legally taken from the crime scene and properly documented following the chain of custody procedures. Imaging software and tools, data recovery software, and approved evidence collection methods are utilized in this phase of the investigation. Five properties of collecting evidence are that it must be admissible, authentic, complete, reliable, and believable [67]. For instance, admissible evidence is evidence that is used in court. Evidence must be authentic, which means that the evidence must be linked to the incident in some way. The completeness property specifies that all evidence should be collected to show the suspect's guilt or innocence. The reliability property signifies that the collection procedures should be authentic and correctly used. Lastly, the evidence should be believable, which means that it must be clearly understandable and believable to a jury.

1.2.1.4 Examination

Examination involves using specific tools and techniques to search, identify, and examine evidence relative to the suspected crime [49]. In this phase, evidence is searched in files, emails, images, folders, hidden spaces on the disk such as slack space, swap space, free space, registry and other areas. Computer forensic tools, such as the Forensic Toolkit (FTK)® and Encase®, are also used to examine these areas more effectively, and these tools also reduce the amount of time spent searching for evidence.

www.manaraa.com

Procedures and tools should also be documented during the examination. Technical skills are required to use these tools because evidence authenticity is of the utmost importance to digital forensic cases.

1.2.1.5 Analysis

The analysis phase involves reconstructing all the evidential findings in order to theorize what occurred by using graphical tools, diagrams, and spreadsheets [67]. In this phase, conclusions are drawn from the evidence collected during the examination phase. A timeline of events, relationships between the evidence found and physical items, and criminal intent can be reconstructed from the evidence found. This can often be a difficult and time consuming task. Beebe and Clark [4] stated that "data analysis is often the most complex and time consuming phase in the digital forensic process and few researchers and practitioners have focused on it when developing frameworks." Furthermore, the data analysis phase referred to by [4] consists of both the examination and analysis phases. Research has been proposed for creating analysis frameworks [7, 8, 15, 41, 54]. According to Stephenson [61], "valid techniques used in evidence analysis directly impacts the validity of the conclusions derived from the evidence and the credibility of the chain of custody." If invalid techniques are used, the resulting conclusions and the information documented in the chain of custody would also be assumed to be fallible.

1.2.1.6 Presentation

Every task completed prior to this phase plays a part in the presentation of the evidence in court. Often times, investigators and forensic examiners use tools and

www.manaraa.com

techniques to present case findings to the court in an organized, clear, and objective way [10]. Presentation is important to the investigative process because this is where the legal ramifications of the suspect's actions are determined. For instance, the forensic examiner must be able to present exactly what occurred during the identification, collection, preservation, examination, and analysis phases of an investigation.

1.2 Motivation

Computers and digital devices are continuing to evolve in the areas of storage, processing power, memory, and features. Due to these continual changes, further computer forensic research is greatly needed in these areas. Computer forensic research aims to address the lack of standards and practices in computer forensics, the examination of digital media devices with increasing storage capacity, crimes and illegal activities involving computers, and the need for educating and training law enforcement and computer forensic technicians. "The continuing maturity of this field will invariably bring some stabilization in best practices, training, certification, and toolsets, but new challenges will always emerge because of the dynamic structure of the technology at its root" [38]. Although progress is being made in addressing these issues, technological advancements will continue to make the digital forensic examination process even more complex.

The complexity of cases is continuing to grow due to the size of digital storage reaching gigabytes and terabytes [50]. With each new development, cheaper models with larger amounts of storage space and functionality are becoming more accessible to more people, even criminals. The creation and enhancements of digital devices directly

www.manaraa.com

affects the law enforcement community. According to Harrison et al. [25], with every new digital device that is developed, law enforcement officials are left with trying to find ways to extract the evidence without altering or damaging it, so that they can develop their criminal cases. Computer forensic specialists and state and local investigators are also confronting constraints such as time, budget, and capacity when handling computer forensic cases on a daily basis [35, 38]. With the growth in disk storage volume, the procedures and techniques used for data acquisition and imaging, and for the analysis of data must all be modified [36]. Furthermore, we must also consider the effects that increased storage has on forensic tools as well.

Computer forensic tools are most often used for examining and analyzing digital evidence. According to Berghel [5], several tools that have been designed to work on single workstations have been shown to work reasonably well for target systems 40 GB or less; in addition, manual examination of hard drives is becoming more and more obsolete given that some workstations are RAID five stacks and contain terabytes of disk space. To optimize time, a forensic examiner should not use just one tool but should have multiple tools in his/her toolkit. These tools may be designated to carefully collect, examine, and analyze the digital evidence [23]. These tools must also allow detailed information about the procedures and tools to be recorded.

Not only does digital investigation require chain of custody documentation, access management, diligence, and attention to detail; it also requires specialized knowledge of computer technology (both hardware and software), including various operating systems, file storage techniques, and file recovery techniques [23]. Some

www.manaraa.com

experts feel that law enforcement has become too dependent on tools. In the past few years, computer forensics has been primarily driven by vendors and applied technologies and very little consideration has been given to establishing a sound theoretical foundation [16, 49, 52]; consequently, requests for proof of theoretical foundations for valid ad hoc procedures and methodologies are continuing to rise [60]. Computer forensic tools such as Encase and the Forensic Toolkit (FTK) were designed specifically to assist forensic examiners with their examinations. On the contrary, one must be aware of the anti-forensic techniques and tools that have been and are being developed as countermeasures to computer forensic tools.

Anti-forensic techniques are being used to exploit weaknesses in current computer forensic tools. At the DFRWS workshop in August 2007, a definition for anti-forensics was stated as "any attempts to compromise the availability of or usefulness of evidence to the forensics process" [1]. According to Sartin [55], the information black market is continually growing and is leading to the growth of compromised data occurrences. In addition, the information black market has lead to the creation of anti-forensics, one of computer forensics most significant challenges. While digital forensics deals with log data, the authentication of information, date and timestamps, and file system contents, anti-forensics refers to the practice of negatively affecting the integrity of quality and quantity of digital evidence in a case. Anti-forensics techniques can make or break a case depending upon how successful these techniques are at making the evidence data difficult or impossible to examine. Anti-forensic techniques can prevent a forensic examiner from "accurately identifying the source of a security breach, preventing containment, and

www.manaraa.com

extending exposure" [61]. Sartin [55] stated that anti-forensic techniques are used in two-thirds of data compromise cases.

A security research group, known as Metasploit, is finding ways to exploit the weak spots in digital forensic programs in the following ways:

- by creating programs that acquires hashes from the NT Security Access Manager (SAM) file without accessing the hard drive,
- by hiding files within the slack space of the NTFS file,
- by defeating file signature detectors by allowing the user to mask and unmask files as any type, and
- by altering the four NT File System (NTFS) file times (modified, access, creation, and entry update)

These findings are only adding to the anti-forensics problem and interfering in investigations. Three anti-forensic strategies that can be used against computer forensics are attacks on data, attacks on tools, and attacks on the analyst. Attacks on data occur when the potential evidence is deleted or modified to make it useless or inadmissible in court; attacks on tools occur when weaknesses in forensic tools are altered to produce false investigation results; attacks on the analyst occur when a huge amount of information is generated which creates problems for the examiner by causing doubt in the validity of the evidence results [24]. One such exploit, the Timestomp exploit, interferes with forensic tool's timestamping abilities. This exploit has been reported to work in Guidance Software's Encase program and AccessData's FTK program and could potentially ruin the evidence collecting process [1].

The motivation behind the creation of the Metasploit group was to expose the weaknesses in forensic programs. The group's website states that "its goal is to provide

www.manaraa.com

useful information to people who perform penetration testing, IDS signature development, and exploit research. This site was created to fill in the gaps of the publicly available information on various exploitation techniques and to create a useful resource for exploit developers" [1]. One of the group's members stated that the reason the group chose to expose faults in digital forensic software was because the forensics community did not feel pressured to become innovative and users of the tools have become too dependent upon forensic tools. Many investigators feel that publicizing such information will only welcome hackers; however, many of these anti-forensic principles have been used for years.

To combat these problems, research communities are continually finding ways to enhance traditional methods. Features are currently being developed to counter anti-forensic tools. It is believed that very few people are using the Metasploit tools and that only a small amount of people are using advanced forensic techniques. However, determining who is using them is difficult because practitioners are hesitant to discuss this information [1]. The Timestomp anti-forensic tool is the most damaging to a case because the suspect's ability to alter the timestamp of the evidence could potentially free him of charges; in addition, commercial tools should also be capable of alerting investigators to the presence of anti-forensic tools since these tools tend to leave trace information behind. Furthermore, peer reviews and commercial pressure are needed to encourage better products [1]. Multiple forensic tools are useful for reducing the risk and interference of exploits in a case. Metasploit intends to work on additional exploits such as NTFS change journal modification, secure deletion, browser log manipulation, and file

www.manaraa.com

modification. On the contrary, methods and tools are available for aiding in discovering whether anti-forensic tools have been used. A hexadecimal editor is suggested for use when data anomaly detection is used. The hexadecimal editor can be used to analyze the disk contents for anomalies. The registry would be a good place to look when trying to determine whether anti-forensic tools were used as well. It was also suggested that a hash database be used to determine if wiping tools had been used [1].

Another problem encountered by forensic examiners is that they have to seek out their own training on an ongoing basis. "Both the law enforcement community and the private sector/academia are concerned with the lack of a standardized, or even a consensus approach to training computer forensic practitioners [52]. According to [38, 63], "today's technological advancements occur with such frequency that keeping up to date on the latest electronic-based systems and their associated technologies poses a daunting task for state and local law enforcement agencies with limited resources and personnel, [and] criminals operating in cyberspace continuously employ new techniques and methods, thereby making it more difficult for law enforcement to keep pace." In addition, Mohay [36] and Bhaskar [6] stated that "it is difficult to implement a response with computer forensics as the main focus because knowledge of computer forensics within the law enforcement community is very limited and there is limited legal support trained in computer forensics law." Furthermore, semantically strong representational models and automated methods of comparing data are necessary for forensic investigators to effectively investigate the ever increasing amounts of data [36].

www.manaraa.com

Security breaches and data compromise are becoming more visible because of consumer and/or identity related information and the victimization of companies, bringing computer forensics into the focus. Through training, law enforcement is becoming more effective at identifying computer crimes and apprehending individuals. In addition, companies are offering more courses in computer forensic investigations and colleges and universities are establishing computer forensic courses and workshops to provide students and law enforcement officials with the fundamentals of computer forensics [55]. With this new knowledge of how to properly investigate computer related crimes, a way to share this knowledge would greatly benefit the law enforcement community. There is no specified way to share digital forensic knowledge and this limitation results in the same problems and mistakes occurring and the same solutions being presented over and over again [25]. A digital forensic lessons learned repository could provide a way to disseminate knowledge gained from investigations. This repository could ultimately lead to a standardized methodology for digital forensic investigations.

In this dissertation, the concept mapping case domain methodology aims to provide a way to organize and structure knowledge gained through examining and analyzing evidence so that this knowledge can be shared with the law enforcement community and researchers as well.

1.3 Hypothesis

The hypothesis of this dissertation is that the concept mapping case domain modeling approach can serve as a method for organizing, examining, and analyzing

www.manaraa.com

digital forensic evidence and can enhance the quality of forensic examinations without increasing the time required to examine and analyze forensic evidence by more than 5%.

The concept mapping case domain model is a variation of the case domain model proposed by Bogen [7]. The case domain model represented the information domain of the computer forensics case by defining the scope of the case information that was required during a computer forensics examination. The case domain models are generalized and can be reused with similar cases, and they are also instantiated when they are "filled-in" with specific case information. The concept mapping case domain model is similar to the case domain model because concept maps or concept models can be created to represent general and specific case information, these general concept models can be reused with similar cases, and the concept models are instantiated when specific information is included on the map. The difference in the two models is the way in which the case information is represented and the availability of a semi-automated tool. Concept maps, instead of the UML modeling, are used in this approach. Concept maps are simpler to understand and easier to construct than UML conceptual diagrams. Unlike with concept maps, characteristics such as generalization, inheritance, composition, attributes, and methods have to be considered when creating UML models. Concept maps allow the representation and combination of information obtained from multiple case domains, and concept maps can be drawn manually and/or can be generated using computer software such as CmapTools. The CmapTools software allows the user to link resources such as photos, images, graphs, videos, charts, tables, texts, web pages and/or other concept maps located anywhere on the Internet to concepts or linking words using

www.manaraa.com

drag and drop operations [43]. For instance, photos and images specific to a case can be applied to the appropriate concept in the concept map and referenced during and after an investigation. The methodology used in the case domain approach for selecting keyword search terms will also be used to create a comprehensive list of keyword search terms to be used in the concept mapping case domain model. Additionally, this keyword selection method will also be combined with the concept mapping concept selection method discussed in Chapter II of this document. To evaluate this hypothesis, we designed our experiments to answer three research questions.

Research Question 1: Does the concept mapping case domain modeling approach result in an increased amount of evidence found during a digital forensic investigation? Checklists are generally used to search for and identify evidence in computer forensics examinations. These checklists however, do not provide the added benefit of incorporating the case details into the search as well. In addition, since there is no standard method to follow for examining digital evidence, the concept mapping case domain modeling approach (CMCDMA) could result in an increased amount of evidence in an investigation. The concept mapping case domain modeling approach provides the following advantages in a computer/digital forensics examination: it provides a quick and easy way to access the web-based, visual concept map containing evidential target categories and case types with each of their associated tasks shown in [65] relative to the case domain, it provides a structured, organized visual diagram that can be used to review the case-specific details which are represented in concept map form, and allows for the documentation of related and unrelated information relative to the case domain including

www.manaraa.com

the "actual" evidence items of the case. These items can be linked to particular concepts within the case-specific concept map as icons. Items may include photos, images, videos, documents, evidence reports, subpoenas, etc. Including these icons could potentially lead to additional searches and evidence findings and could provide a quick way to reference the evidence items for a specific case or cases. Experiments were performed to determine how much evidence was identified using a typical ad hoc approach and the concept mapping case domain modeling approach. Students attending the CF 510 Seminar Course on Investigative and Examination Planning participated in the experiments.

Research Question 2 asks the following: Does the concept mapping case domain modeling approach require a significant amount of additional effort when compared to a typical approach? In Bogen's [7] case domain model, it was assumed that investigators and forensic technicians would spend more time planning the keyword examination than when using established planning, methods, and the experimental results found that more time was spent planning the keyword examination. Therefore, given that the concept mapping case domain model is a variation of the case domain model, the same will be assumed here. In addition to planning keyword search terms, a keyword specific case concept map will be created and will contain case-specific information from the case scenario. According to [43], the amount of effort required to construct and use concept maps depends on one's prior knowledge of the area. If the person creating the map has limited knowledge of the case domain, then more effort may be required. This effort will be reduced because the general concept maps will be created prior to the experiment and

www.manaraa.com

will be used as guides to aid in the search and identification of evidence in the examination. The effort required by the subjects to create more specific concepts in the keyword case specific concept map should be alleviated due to the lecture given before the experiment. This lecture discusses concept mapping and keyword searching, provides several hands-on activities using concept maps, and demonstrates the application of the concept mapping software, CmapTools to several case scenarios. Use of the tool is optional in the experiment. If the subjects choose to use the CmapTools software, they will have the ability to link digital resources/evidence, to construct more specific sub-maps relative to the case domain by adding more inclusive case domain information to the concepts and/or creating additional concepts and relationships, and to save a digital copy of their case-specific concept map. Experimental analysis compares the amount of effort spent planning or identifying keywords from the case domain and the USDOJ crime category target list and executing searches with these keywords using the ad hoc approach and the concept mapping case domain modeling approach.

Research Question 3 asks the following: Is the concept mapping case domain modeling approach useful for typical law enforcement investigators involved in computer forensic cases? Computer Forensics has become an important part of law enforcement due to the increasing growth of digital crimes. Technological crimes do not only relate to computers anymore, but encompass all digital media. In addition to limited personnel and resources, law enforcement officers must seek out training not only in computer forensics techniques, but many times, in computer technology as well. Computer forensic examinations have expanded beyond federal law enforcement to include state

www.manaraa.com

and local law enforcement as well. Having knowledge of computer forensic procedures is essential to successfully identifying, collecting, examining, and analyzing evidence in an investigation. It is expected that subjects, with computer forensic examination experience would have fewer difficulties understanding and utilizing the concept mapping case domain modeling approach than those with little or no knowledge of computer forensic examinations. Those with experience have some experience with computers and examination software and also have had to at least follow some type of method for properly searching for and identifying evidence, which gives them the advantage of following computer forensic procedures in an examination. Four experiments were performed, and the data collected from those subjects using the concept mapping case domain modeling approach was analyzed with regards to experience level. In the experiments, law enforcement officers using the concept mapping case domain modeling approach were asked to disclose their level of experience in regards to computer forensic examinations so that comparisons could later be made about their performance in the experiments and the applicability of the proposed approach in real world cases. After completing the experiment, each subject provided survey responses about their experiences using the concept mapping case domain modeling approach.

1.4 Expected Contributions

This dissertation will provide evidence that the concept mapping case domain modeling is useful for organizing, examining, and analyzing digital forensic evidence in computer forensic examinations. The general contributions of this dissertation are listed below.

www.manaraa.com

- *A method for applying concept mapping to computer forensic examinations.* Concept maps have largely been used for educational purposes; however, they have also been used in business, governmental, and military settings for reasons such as eliciting expert knowledge, to support the design of new technologies, for knowledge management, and for training and support. So far, concept mapping has not been utilized in the domain of computer forensics. This dissertation will apply the concept mapping case domain modeling approach to computer forensics examination planning tasks such as keyword selection and case domain representation. The availability of free semi-automated concept mapping software will also help to foster knowledge sharing in the law enforcement community because concept maps can be saved in html format and accessed over the Internet.

- *An approach for sharing, reusing, and managing knowledge acquired in a computer forensics investigation.* Computer forensic examiners and/or forensic technicians generally use standard search techniques and computer and digital forensic tools to examine and analyze forensic evidence. Many times, they incorporate their own special techniques to help them uncover evidence. Currently, a standard method does not exist that allows these special techniques to be shared with others and to be reused by others within the law enforcement community. Finding a method for effectively reusing and managing knowledge could improve the digital forensic process. A digital forensic repository was proposed that would allow members of the law enforcement community to share their digital forensic knowledge. Furthermore, this repository would aid in the elimination of reoccurring problems, mistakes, and the same solutions being presented repeatedly. This digital forensic repository or lessons learned repository would allow any knowledge gained through forensic examinations to be disseminated throughout the law enforcement community; however, the development of this repository has yet to be undertaken. The concept mapping case domain model could be used as a scaffold for a digital forensics repository. In addition, it could be used to create knowledge management strategies specific to criminal investigations. Utilizing both the concept mapping software tool and the proposed approach could potentially improve the skills and work of novice and expert forensic investigators for the following reasons: a structured method would be provided for examining evidence, new knowledge could easily be added to the concept map, the concept map could be modified to show how an expert examines evidence, new information could be incorporated into the map easily, concept maps pertaining to specific cases could be stored on a server and shared with other law enforcement officials, misunderstandings in the examination process could be uncovered, concept maps could be easily retrieved for review, and knowledge gained from investigations can be shared across the law enforcement community and potentially lead to a digital forensic knowledge repository.

www.manaraa.com

- *Experimental evidence that will show the utility of concept mapping case domain modeling in computer forensics.* Although research exists in computer forensic modeling, there is yet to be a significant amount of experimental data in computer forensic case modeling. This dissertation presents a concept mapping case domain modeling approach that utilizes concept mapping for planning, searching for, and identifying evidence during an examination. The goal of this dissertation is to provide a replicable and reusable approach that can be utilized with other computer forensic modeling approaches and by researchers and the law enforcement community.

The remainder of this research work is as follows: Chapter II provides a review of the related work in the areas of computer forensics, conceptual modeling, and knowledge management. Chapter III discusses the concept mapping case domain modeling approach. Chapter IV presents the results of the four experiment trials of the concept mapping case domain modeling approach applied to examination planning and execution. Chapter V presents conclusions and discusses potential areas for future research.

www.manaraa.com

CHAPTER II

LITERATURE REVIEW

A survey of literature and research work related to this dissertation is presented in this chapter. The following topics were explored in this chapter: computer forensics modeling approaches, domain modeling in computer forensics, conceptual modeling, and knowledge management.

2.1 Computer Forensic Modeling Approaches

Computer forensic modeling approaches provide a planned way of executing computer forensic investigations. Several approaches have been developed, yet no specific, universal methodology has been standardized. Many of these approaches lack much needed empirical evidence of their application and usage. In addition, one of the many reasons is that these approaches are not being used. Instead, forensic examiners rely on their own knowledge of the investigative process and most often use commercial software such as Encase and Forensic Toolkit (FTK) to search and identify evidence during the examination and analysis phases of the investigation. Another reason is that research has not been conducted to find out if computer forensic examiners are aware of computer forensic modeling methodologies. For those examiners who are familiar with one or more of these modeling approaches, research is necessary to find out if these approaches are being applied by forensic examiners in "real" digital forensic

www.manaraa.com

investigations. In lieu of constant technological advances, knowledge and usage of computer forensic modeling approaches are one of many choices available to address the increasing storage capacities of digital devices, crimes and activities involving digital devices, and the education and the training of law enforcement and computer forensic examiners. The Digital Forensic Research Workshop (DFRWS) addressed the need for such a modeling methodology and provided a simple structured method for modeling the digital forensic investigative process called the DFRWS model.

2.1.1 Investigative Process Models

The DFRWS model was developed by a research panel consisting of the academic, operational, and commercial areas of government. This model presented a general framework of actions that should take place during a computer forensic investigation, which were identification, preservation, collection, examination, analysis, and presentation. Furthermore, this model offered a basis for future work, which has resulted in the development of additional modeling methodologies. Extensions of the DFRWS models were presented in [3, 4, 15, 19, 49, 54, 69]. Although some models only added additional steps to the process, other models focused more on the problems that addressed the complexity of an investigation and the features and functionality of devices. For instance, Reith [49] presented a model that integrated both digital and non-digital technologies, that provided for more detailed subcategories for specific investigations, and that introduced the possibility of iterating between the investigative process phases. Ciardhuáin [19] proposed a model that would represent the flow of information during and after an investigation. This model provided the scope of the

www.manaraa.com

investigation, a basis for sharing expertise, and a foundation for investigative tool requirements analysis and capture. He also suggested that regulation, legislation, and organizational policies be linked to the model along with the ability to capture detailed characteristics of various investigation types. Unlike the previous models, which presented a linear, abstract process model, Beebe and Clark [4] proposed a hierarchical framework that focused on the concrete principles of an investigation. At a higher level, their model provided a simplified or generalized view of objectives to accomplish, and at lower levels for each phase in the tier, it provided more detailed information by including sub phases. Since, the steps in the model are outlined in an objectives-based fashion instead of task based fashion, the model was suggested for use as a decision support tool. The inclusion of sub phases in this model made it practical for actual investigations; in addition, the model was presented as being more flexible, amendable, and applicable in different user environments. Other suggested advantages of this model were that it could be used to determine where research was needed, and it could be used to track tools that had been used during the examination. Each of these models addressed each of the phases of the DFRWS model; however, none focused primarily on a particular phase. However, Bogen [7] and Venter [69] proposed models that addressed the specifics of phase tasks within the investigative process.

2.1.2 Hypothesis Modeling Approaches

Hypothesis modeling is discussed in this dissertation because the concept mapping technique utilizes hypothesis development in the creation of concept maps. The hypothesis helps to focus the development of the map and the creation of relative

www.manaraa.com

concepts and relationships. In this section, models utilizing non-expressive and expressive tools are discussed. In addition, characteristics of these models were used in the development of the concept mapping case domain modeling approach.

2.1.2.1 Event-Based Digital Forensic Framework

In 2004, Carrier and Spafford [15] presented an event-based framework for digital forensics investigation, which included preserving the system, searching for digital evidence, and reconstructing digital events. In addition, this framework supported hypothesis development that aided in crime or incident questions being answered. The framework also included the investigation process model, which was based on physical crime scene procedures as shown in Figure 2.1.

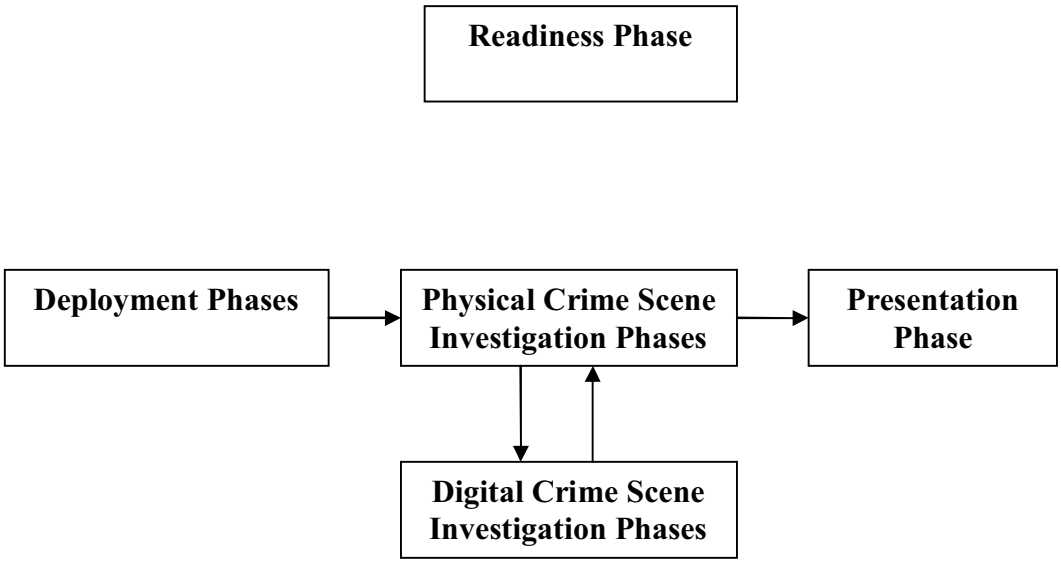


Figure 2.1 Graphical Representation of the Major Phase Categories Framework [15]

www.manaraa.com

Clear goals were provided for each phase, however, specific requirements for each phase had not been developed. According to Carrier and Spafford [15], a digital forensics framework should be flexible enough to support future technologies and various incident types, and should be simple and abstract enough where tool requirements and test procedures can be created for each phase. The digital crime scene investigation phase was discussed in detail and included system preservation, evidence searching, and event reconstruction additional phases and sub-phases relative to the examination and analysis phases of an investigation. Documentation was included in each of the phases of the digital crime scene investigation phase shown in Figure 2.2. Documentation is important because it helps with proving integrity and is an important part of the chain of custody procedures, which pinpoint who did what, when, and where in an investigation.

The main objective of the system preservation phase is to preserve the crime scene and all of the objects it contains. In this phase, the preservation of the evidence is not the goal because, at this point, the evidence has not yet been discovered. In the evidence searching phase, digital objects that contain information about the incident are chosen and evidence information would then be located. Carrier and Spafford [15] stated that an investigator's experience at determining what types of evidence should exist is beneficial when defining targets or evidence that has already been found. After identifying an object as evidence, it has to be properly documented and preserved. In the

www.manaraa.com

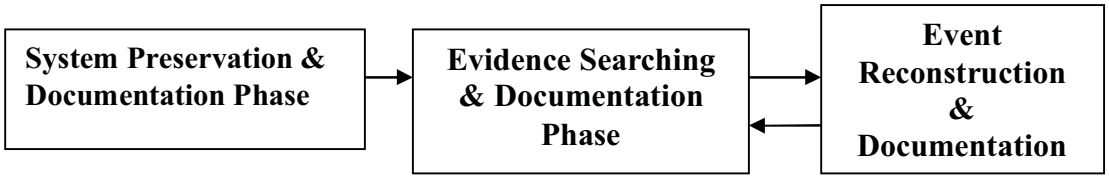


Figure 2.2 Graphical Representations of the Digital Crime Scene Investigation Phases [15]

event reconstruction phase, the hypotheses are developed according to the events that occurred and conclusions are developed about what actually took place. Carrier and Spafford stated that digital event reconstruction has not been focused upon in digital forensics; they also stated that event reconstruction may be useful in determining the source and events that created a file instead of just identifying the existence of a file.

According to [15], choosing a model to use during an investigation is subjective or dependent on the person searching for evidence. The best model choice is one that can incorporate future technologies and be used in different investigations. In this framework and other methodologies, incorporating future technologies into models is very important. In order for a model to be utilized, it should be able to be modified with new information without changing the basic framework principles of the model.

This paper is relative to this dissertation because it addressed hypothesis development. Concept mapping encourages the development of hypotheses in order to guide the creation of the concept map. The basic principles of the framework are common in the event-based digital forensic framework such as incorporating future technologies, scalability, use with different cases, simplicity, and abstractness; however, it doesn't, provide an expressive tool for recording case information.

www.manaraa.com

2.1.2.2 Attack Trees

Schneier [57] discussed how to model security threats against computer systems using attack trees. The goal was to create a model that can be used to understand different ways in which the system can be attacked and to develop countermeasures to stop those attacks. According to Schneier, attack trees provide a formal, methodical way of representing attacks against a computer system using a tree structure where the root node is the goal, and the leaf nodes are different ways of achieving that goal. Although this model was developed for computer security purposes, a model was created to show that this model could also be applied to computer forensics. In Figure 2.3, Bogen [7] developed a computer forensics related attack tree for gaining unauthorized access using a password. This figure helped show the representational flexibility of an attack tree.

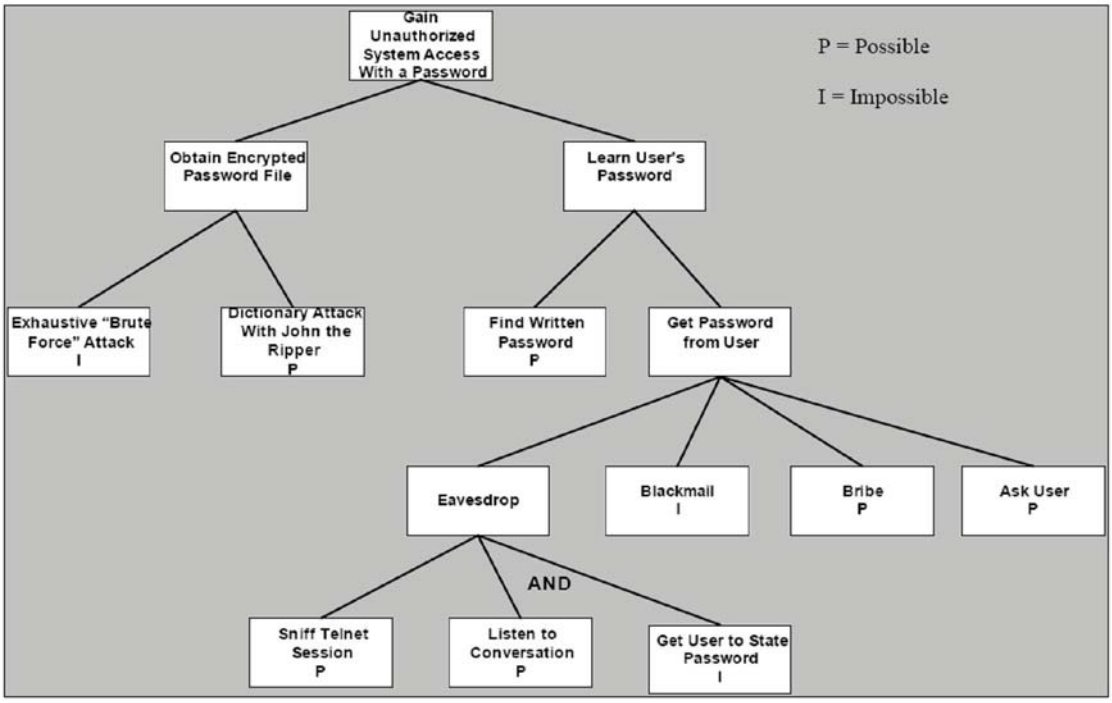


Figure 2.3 Computer Forensic Attack Tree Example [7]

www.manaraa.com

Furthermore, this flexibility makes it more adaptable to the computer forensics context since very few modifications were needed.

In order to create an attack tree, first, possible attack goals must be identified. Each goal is represented as a separate tree and may share sub-trees and nodes. Secondly, all attacks against the goal must be determined and added to the tree; this process is repeated as necessary. Next, the node values are researched and assigned according to the difficulty of the attack. Node values play an important role in an attack tree. The assignment of these node values, which are Boolean or continuous numbers, are used to determine the low and high risk factors, cheapest attack methods, and the probability of success of an attack occurring. The nodes and goal node are calculated based upon the system modification and/or new vulnerability discoveries. Attacks could be ranked according to which is cheaper, more likely to succeed, succeeded, and so on. From these values one would be able to learn about the system's vulnerabilities and level of security [57].

Schneier stated that "attack trees provide a formal methodology for analyzing the security of systems and subsystems. They provide a way to think about security, to capture and reuse expertise about security, and to respond to changes in security. Attack trees form the basis of understanding that process." This statement is also applicable to computer forensics because attack trees can provide a formal methodology for analyzing the digital forensics of systems and subsystems, and it can provide for thinking about, analyzing, capturing, and reusing expertise and knowledge about computer forensics. Attack trees are applicable to this dissertation since, like concept mapping, attack trees

www.manaraa.com

can be used to make decisions, to develop hypotheses, to capture knowledge in a reusable form, to list assumptions about a system, to create a visual representation of the evidential path for narrowing the scope, and it also provides simple and easy to understand notation. It was also stated that the attack model is scalable and, therefore, doesn't require the user of the model to be an expert to use it; however, some expert knowledge is required for implementing certain processes listed in nodes of the model.

Although attack trees would be useful, some disadvantages of the model do exist if used in computer forensics. One way in which concept maps are better than attack trees for usage is that attack trees cannot represent more than one goal in one tree. A separate tree must be created. Therefore, if there are several attack goals for a particular attack, the relationships between the attack goals could not be depicted in the attack tree. When creating concept maps, each goal can be represented in one map and their relationships to one another would be known. Separate concept maps with attack methods for each goal can be created for the goal concept map. Furthermore, attack trees would not be useful in large and/or complex cases because a large number of attack tree representations and goals would have to be constructed. According to Bogen [7], an attack tree that is too deep would become difficult to comprehend and represent, especially on a piece of paper; however, several attack trees can be created for a single security incident, which is also true for concept mapping. Additional concept maps or "sub-maps" can be created for a single investigation. Attack trees present a more general representation of an attack goal and the ways to reach that goal. Attack trees are also more structured and have a step-by-step relationship whereas evidence may not. The

www.manaraa.com

only detailed information provided in an attack tree is whether the attack type is possible or impossible. In concept maps, specific information, such as an actual password, can be included on the map with specific steps/details as to how the password was obtained. An additional advantage that the concept map has over the attack tree is the availability of a tool. With concept mapping software, specific details for an attack type node can be included as an icon(s) within the node or concept.

2.1.3 Process Flow Diagrams for Training and Operations

Venter [69] proposed a general process flow framework that assisted cyber forensic first responders in the identification and collection phases of the investigative digital forensic process. The process flow framework was created to make the search and seizure practices, at the electronic crime scene, easier to understand and implement for those individuals without formal qualifications, such as first responders. This framework provided a centralized way to record information at the crime scene, design principles and layout characteristics for the different process flows, and flowchart design principles for seizing particular types of evidence such as desktops computer hard disks, CDs, DVDs, and other evidence items. During the experiment, generalized checklists of items to assess were made available during an investigation to accommodate those first responders, who lacked the expertise needed to make decisions at the scene of the crime. The framework was based on four principles, which were to ensure ease of use for non-IT professionals, to be applicable in the most likely cases, to not interfere with expert testimony or possibly assist with it, and to be used for not only training, but operations as well. Layout characteristics of the process flow framework were designed so that those

www.manaraa.com

individuals utilizing this framework could have a place to document their findings and to use the framework as a guide for naming evidence. The first characteristic was that the process flows must fit on a single A4 page. This requirement made it easier for storage and placement of the process flow diagram in a normal A4 record book; also, it could be reproduced and used for future investigations. The second characteristic of the framework was that the process flow diagram could be used to record information about specific evidence during the evidence collection process, since all the information recorded is case or domain specific. The third characteristic of the framework was that the first responders were provided with simple naming conventions for evidence. These naming conventions would remind the first responders of the correct naming conventions for a specific piece of evidence. Venter also provided process flow diagrams for inspecting and preparing the scene, collecting evidence and evidence information, and for debriefing the scene and recording seizure information as shown in Figure 2.4.

Venter provided generic framework elements and elements of specific process flows that showed actions or tasks that the first responder should follow. Figure 2.4 shows the generic framework element present in each process flow, which were "Inspect & Prepare Scene", "Collect Evidence & Evidence Information", and "Debrief Scene & Record Seizure Information." Figure 2.5 provides a process flow for an electronic crime

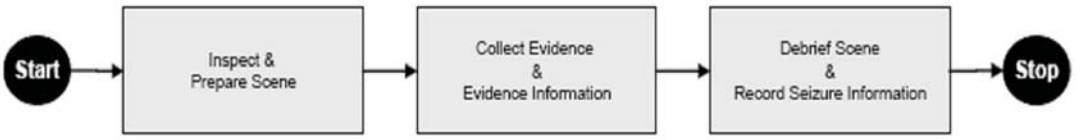


Figure 2.4 Generic Framework Elements [69]

www.manaraa.com

scene, and Figure 2.6 provides a process flow diagram for seizing desktop computer hard disks. In this figure, each of the generic process flow elements can be seen. For instance, determining the LAN/Modem connection would apply to the "Inspect & Prepare Scene." The "Collect Evidence & Evidence Information" element is used for recording specific information about the computer evidence. The "Debriefing Scene & Record Seizure Information" element information would be recorded to show how the evidence was collected, by choosing if packaging or bubble wrap was used for storing the evidence. Other process flow frameworks were presented that addressed other types of evidence such as cell phones and PDAs, CDs/DVDs, flash drives, and floppy disks.

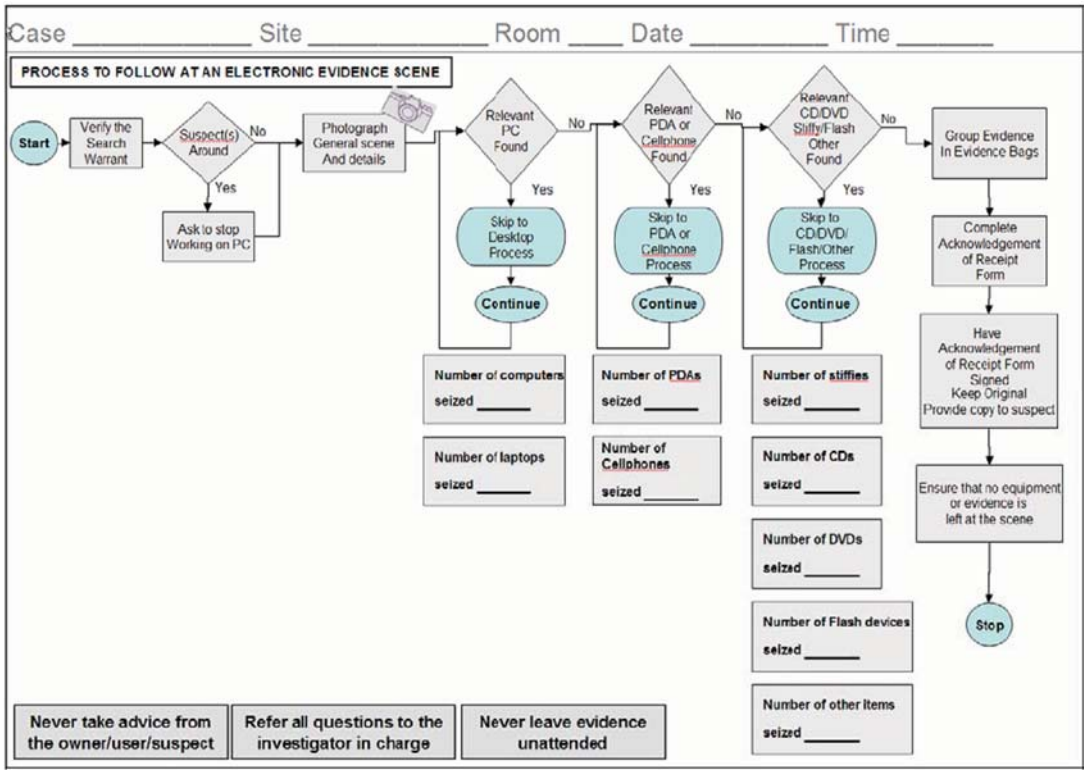


Figure 2.5 Process Flow for Electronic Crime Scene [69]

www.manaraa.com

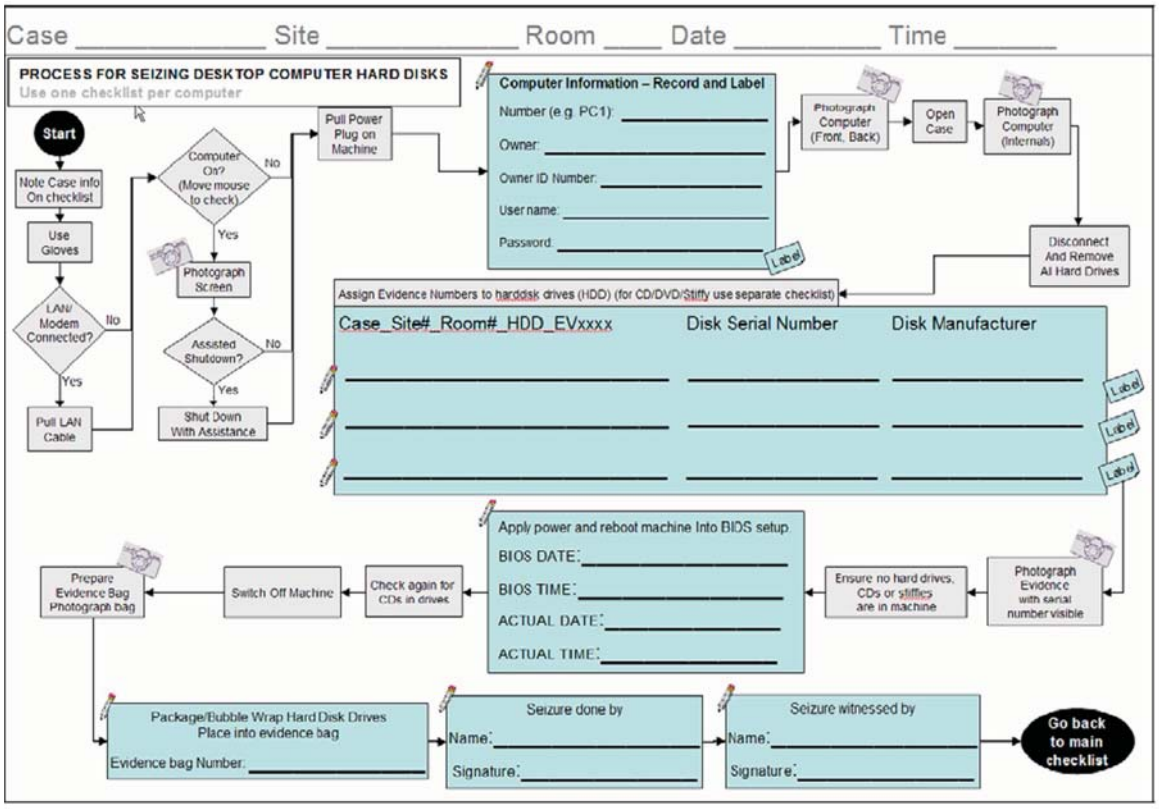


Figure 2.6 Process Flow for Seizing Desktop Computer Hard Disks [69]

Venter's research is related to my dissertation because this framework provided a visual checklist for case-specific activities, and it also provided a simple expressive tool for documenting this case-specific information. Additionally, it provided a framework that gave a simple format that non-technical individuals could easily use and understand. In an experiment conducted using this framework, it was found that the study participants preferred using the process flows to checklists, and the participants stated they would prefer to use them in operational activities. The study also found that this tool increased the first responders' confidence in identifying, seizing, and recording the evidence items and it also decreased their seizure times.

www.manaraa.com

2.1.4 Case Domain Modeling

Bogen's [7] case domain model provided a framework for analyzing case details by filtering important forensic-relevant case information; in addition, it provided a foundation for organizing and focusing a forensics examination plan. According to Bogen, "no previous forensic modeling approaches provided for exclusively analyzing and modeling the information domain of the forensics case." Existing modeling approaches only provided investigative views such as the chain of events view, attack trees and adversary modeling strategy views, and hypothesis test view. Bogen's case domain modeling approach addressed these shortcomings by offering a more structured domain modeling approach. His model utilized established ontology and domain modeling methods to develop the framework of the model, and artificial intelligence and software engineering concepts were used to represent the model. Furthermore, domain analysis and model representation characteristics of software engineering were adapted to the case domain model.

Bogen indicated that a different approach was needed to provide the scope of information, for examining large scale cases, complex cases, and unfamiliar cases. With large, complex cases, Bogen stated that "it can be difficult to characterize the evidence of a crime and clearly outline the scope and goals of the forensics examination." He proposed a structured approach for analyzing case information, for developing planning products, and for identifying evidence. Bogen presented the four activities of the case domain modeling methodology and specified the products for each activity. The activities consisted of modeling the information domain of the case, developing search

www.manaraa.com

goals, specifying search methods for each goal, and conducting the examination. The following products delivered from the activities would be in a case domain model: a statement of search goals, keyword search lists and statements of search strategies, and evidence bookmarks and traceability matrices, respectively.

In order to model the information domain and create the case domain model, a four phase process is required. This four phase process consists of identifying concepts, identifying relationships between the concepts, identifying attributes of the concepts, and instantiating the model by adding case specific information. The United States Department of Justice (USDOJ) checklist was used to map evidence entities to case concepts in the case domain model [7, 65]. In case domain modeling, the case domain represents known and unknown information or concepts relevant to the digital forensics examination. These concepts are modeled using UML conceptual diagrams, as shown in Figure 2.7 For each concept, known attribute values for concepts are not shown on the diagram in order to conserve page space; however, these attributes are instead included in a separate table. Flagged unknown attribute values are indicated with boldface and underlined font. Bogen stated that the UML model is not required because the case domain modeling method is independent and can be represented without using graphical notations. He stated that graphical representations are most useful with large teams, relatively long investigations, and for investigations that usually use visual aids and analytical tools. He also stated that a tabular representation would be more useful with smaller teams with shorter investigation times.

www.manaraa.com

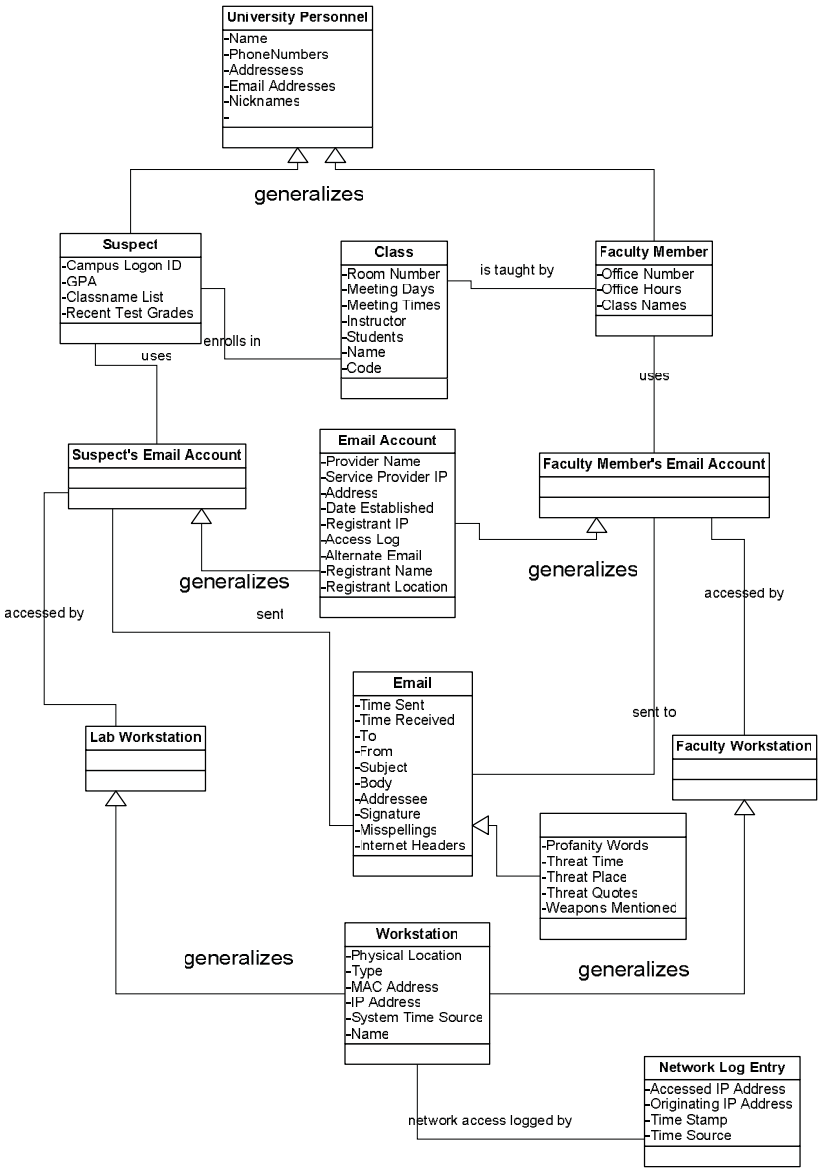


Figure 2.7 Conceptual Case Diagram [7]

In Bogen's methodology, as shown in Table 2.1, search goal tables are used to list the keywords of each attribute, which would be used to search for evidence. Keyword search tables are useful for providing different tactics for searching for a keyword, as shown in Table 2.2. Search goal strategies, shown in Table 2.3, were also suggested as

www.manaraa.com

an alternative or supplement for keyword searching. Forensics software was also used to conduct the examination, and it was used for book marking file items. In his methodology, bookmarked metadata containing search strategy references or keyword search terms would be used to locate file items, which allows one to trace how the evidence was found, also known as traceback.

Table 2.1 Search Goal Table [7]

Goal ID:	1
Goal Statement:	Find file items that reference the victim
Purpose:	Attempt to find evidence that the suspect(s) conducted background research on the victim
Involved Concepts and Attributes:	Faculty Member {Office Number, Office Hours, Class Names, Full Name, SSN, DOB, Phone Numbers, Email Addresses, Physical Addresses, Nicknames}
Known Attribute Values:	Office Number = 101 Office Hours = 1-3pm M W F Class Names = English Composition 101, Creative Writing 102 Full Name = Henry Silver Doe SSN = 123 – 45 – 6789 DOB = 1/1/1965 Phone Numbers = 555-555-1234 (home) 555-555-5432 (office) Email Addresses = hdoe@university.edu Nicknames = Pizza Dough
Unknown Attribute Values Sought:	None

Table 2.2 Keyword Search Table [7]

Goal ID:	1
Concept Attributes:	Faculty Member {Phone Number = 555-555-1234 (home}
Search Locations:	All files and folders on all evidence disks
Keyword ID:	Keyword String
K-1.1.1	555-555-1234
K-1.1.2	(555)555-1234
K-1.1.3	5555551234

www.manaraa.com

Table 2.3 Example of Search Strategies [7]

Goal ID	Strategy ID	Description	Relevant Concepts
1	S-1.1	Browse directory structure for filenames that seem to relate to the victim before conducting the keyword searches.	Faculty Member
1	S-1.2	Sort all of the files by date, filter the files that have modification or creation dates within the time frame of the email threats. If there are less than 100 files, attempt to browse these files for relevant information.	Faculty Member, Murder Threat Email

This research is related to this dissertation as a variation of the case domain model. Bogen's research offers the following: a way to focus on case specific information, a way to reuse knowledge, a systematic way to plan for an examination, and expressive tools for documenting the findings of an examination. Limitations of the case domain modeling approach include that it may be a little too intensive for examiners with large cases. Recording all the information in the search goal table, creating keyword search strategies, and developing search goal strategies on paper may become confusing in large cases when trying to link all the information together, especially when analyzing the evidence. Given that paperwork is a vital part of law enforcement investigations, this dissertation provides an approach that could organize this process and further aid in knowledge reuse and management within the law enforcement community. The aim of this dissertation is to further extend the case domain model by incorporating the concept mapping method and a semi-automated tool into the examination phase of a digital forensic investigation.

www.manaraa.com

2.2 Conceptual Modeling in the Computer Forensics Domain

Conceptual models are used to represent knowledge graphically or in a visual context. Conceptual modeling is a simplified representation of a real system, that is software independent, and it is a repetitive process that helps novices learn new information by visually representing previously known information with new information. According to [64], conceptual maps should meet three criteria, which are learnability, functionality, and usability. Learnability suggests that the model should be easy to learn, functionality suggests that the model should correspond to the target system, and usability means that the models should be easy to use. Conceptual models are iterative and repetitive, and are continually revised during modeling. They can also be used to represent small and large domains. These visual representations of conceptual models can provide novices with an easier way to relate information by comparing and contrasting known and unknown information [64]. Another characteristic of conceptual models is that they are models that show concepts and their relationships to one another. These concept relationships aid in improving a learner's conceptual retention, reduces verbatim recall, and improves problem-solving transfer. Several forms of conceptual models exist such as knowledge maps, semantic networks, cognitive maps, event diagrams, process flow diagrams, mental models, case diagrams, Petri nets, and concept maps.

Conceptual modeling is important to this dissertation because concept mapping, a type of conceptual modeling, will be used to map details of a forensic case in this dissertation. Generally, in digital forensics investigation, a list of tasks to complete is

www.manaraa.com

provided for examination. Visual representations of the examination and analysis of evidence have been graphically presented very rarely. Providing a new approach for examinations could ultimately reduce the search for evidence and force researchers to look at new methods for improving the search and seizure of evidence and ultimately improve the whole investigation technique; furthermore, this approach could possibly allow novice and expert forensic examiners to uncover things that they had not previously known and/or add to the knowledge of the investigative process. This section will discuss three conceptual modeling systems. These three models are similar in that they each use node-link structures to express relationships between concepts.

2.2.1 Semantic Networks

Semantic networks express the semantic similarity or frequency of words or concepts. Semantic networks are interconnected networks of nodes and links with labeled links between the nodes; these networks do not have to be hierarchical. Semantic networks are based on nodes (concepts) and the meaningful, unconstrained linking labels, which form the relationships between each concept. Semantic networks can become very large and complex, which, subsequently, only allows the user to view part of the network. In the Figure 2.8 below, a web-structured view is provided that shows concepts related to the central concept [67]. Semantic networks and pathfinder networks are in the class of networks that show the relatedness of data as it exists in mental models. Pathfinder networks preserve the shortest possible paths, given the data, so that links are eliminated when they are not on shortest paths. Pathfinder networks (PFNs) can be used in the

www.manaraa.com

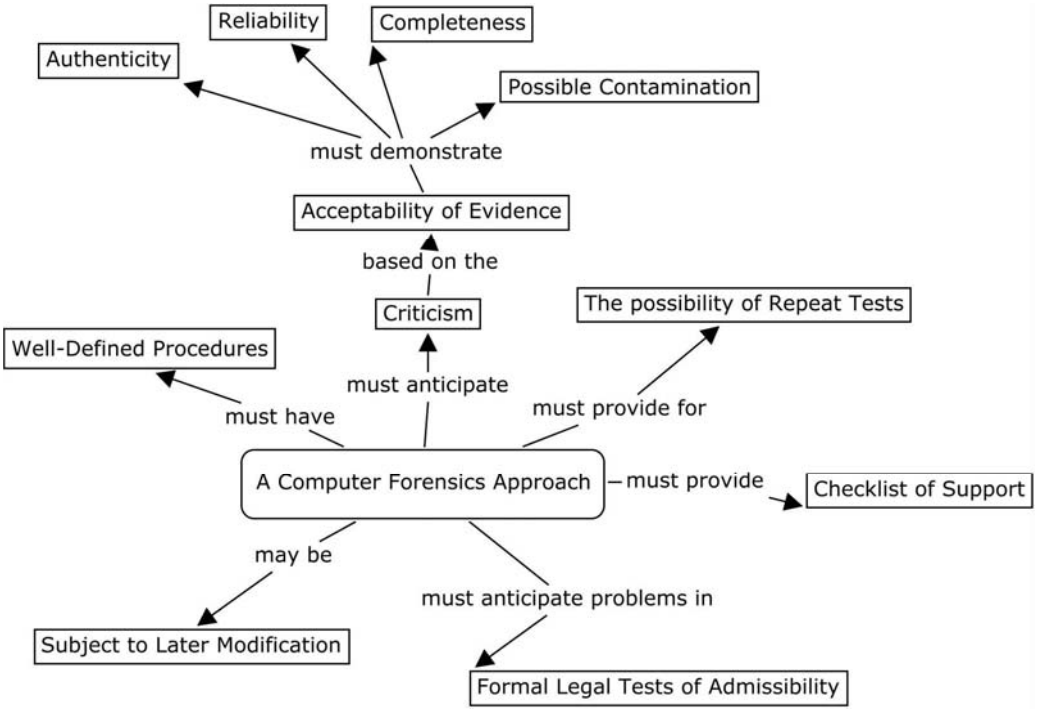


Figure 2.8 Elements of a Computer Forensics Approach [67]

forensics domain to provide a graphical view or representation of how concepts or keywords are interrelated within a particular concept domain [21]. PFNs can be used to "uncover networks for a particular content domain [, and these networks] can be generated by a variety of people representing different perspectives or points-of-view of a domain [and can be used] to analyze different perspectives within the domain" [21]. For instance, PFNs could be developed to represent the relatedness of concepts within the computer forensics domain by allowing experts within this area of forensics to present their expert knowledge relative to the relatedness of concepts within the computer forensics domain. Also, PFNs can be useful in computer forensic modeling for comparing existing models; concepts from each model could be developed and compared in order to come up with a unified domain modeling approach. Misunderstandings, inaccurate

www.manaraa.com

information, and missing information could each be addressed using this technique. Kudikyala [34] applied pathfinder network techniques to software engineering in order to determine their predictive ability to reduce misunderstandings found in software requirements among stakeholders by understanding the overall requirements, by understanding individual requirements, and by understanding the system. Hybrid PFNs, another type of PFN, would also be beneficial to the computer forensics domain.

Hybrid PFNs can be used for indexing purposes; in this way, similar documents are separated so that they can be searched for and found more easily [17, 18, 37]. This searching ability would be useful in large scale investigations within the computer forensic domain. Another type of PFN that could be useful in the computer forensics domain is pair-wise comparison PFNs. Pathfinder networks based on pair-wise comparison PFNs could be used in the computer forensics domain as a training tool. For instance, PFNs can be created during training sessions to determine how well novice forensic examiners understand the interrelatedness and organization of the concepts within the forensic domain. PFNs utilized before and after an investigation would aid in determining what knowledge was gained from the domain. Novice examiners in the forensic domain could develop their own maps using PFNs and then compare their maps to the expert's map to gain a better understanding of the relatedness of the concepts within the domain.

The ability of PFNs to reveal patterns in data that are in close proximity would be very useful in the computer forensics because these patterns could be used to plan an investigation. Given the details of a case, PFNs can be used to make predictions about

www.manaraa.com

the relatedness of the concepts and from these concepts, determine what actions a suspect possibly took to commit the crime or even what tools were possibly used. PFNs can be used to predict the pattern of events as well. PFNs can be depicted as graphs and can be used to determine the minimum number of choices with the best solution for uncovering potential areas where evidence may lie; also, the distance, which is the minimum number of links connecting the nodes or concepts between two nodes or concepts, can be used to predict how related concepts are to one another [56, 68]. PFNs may also be useful in extracting information from evidence during an investigation [56, 68]. Given a concept, all related concepts would be checked for useful information; for instance, if the evidence found is an intentionally misnamed file, then other files that are misnamed may exist, so through the use of PFNs an underlying pattern or relation may discovered.

2.2.2 Cognitive Mapping

Cognitive maps, also known as causal maps, are ideas or nodes represented as large interconnected networks typically containing sentences or paragraphs. The interconnections contain unlabeled, directional links which are causal or understood to mean "leads to." Cognitive maps are not hierarchical and are usually large, complex networks containing hundreds of ideas with one or more focal points as shown in Figure 2.9. Another important aspect of cognitive mapping is that it can be used to transform tacit knowledge into explicit knowledge. Rodhain [51] stated that tacit knowledge can be transformed, reorganized, or reconstructed during the process of constructing an external or visual representation of the particular domain; furthermore, the result is not a simple transformation of tacit knowledge into explicit knowledge, since the process goes through

www.manaraa.com

several modifications. This process helps clarify the domain information and structure the individual's thought [51]. Fuzzy cognitive maps (FCMs), another type of cognitive map, can be used to determine the relatedness of concepts using positive and negative correlations such as if A causes B, then increasing A increases B, and decreasing A decreases B [28, 31]. FCMs can be applied to the digital forensic investigations; for instance, FCMs can be used to represent knowledge bases in a case domain and can determine the relatedness of concepts to other concepts by using positive and minus signs. FCMs are useful when uncertainty in reasoning is necessary to classify objects. In computer security, Siraj [60] demonstrated how common attack patterns with the same or similar features were identified using fuzzy cognitive modeling in order to cluster alerts in a system. Furthermore, FCMs can be used to reason about uncertainty and classify objects in a computer forensics examination. Some objects/concepts may not be a part of the computer forensics domain, however, FCMs would still allow those concepts to be classified, and a possible pattern could still be determined [20, 26]. FCMs can be used with other conceptual models to manage information using fuzzy logic rules, which have the if-then hypothesis format. Fuzzy cognitive maps could also assist with complexity; for instance, the probability that concepts are related can be determined using positive and negative correlations such as if A causes B, then increasing A increases B, and decreasing A decreases B and so on [28]. By integrating the conceptual models and FCMs, patterns could result in additional extraction of data from the map. According to [29, 30, 31], the fuzziness of FCMs plays an important role in knowledge acquisition and provides a way for experts to graphically represent their knowledge.

www.manaraa.com

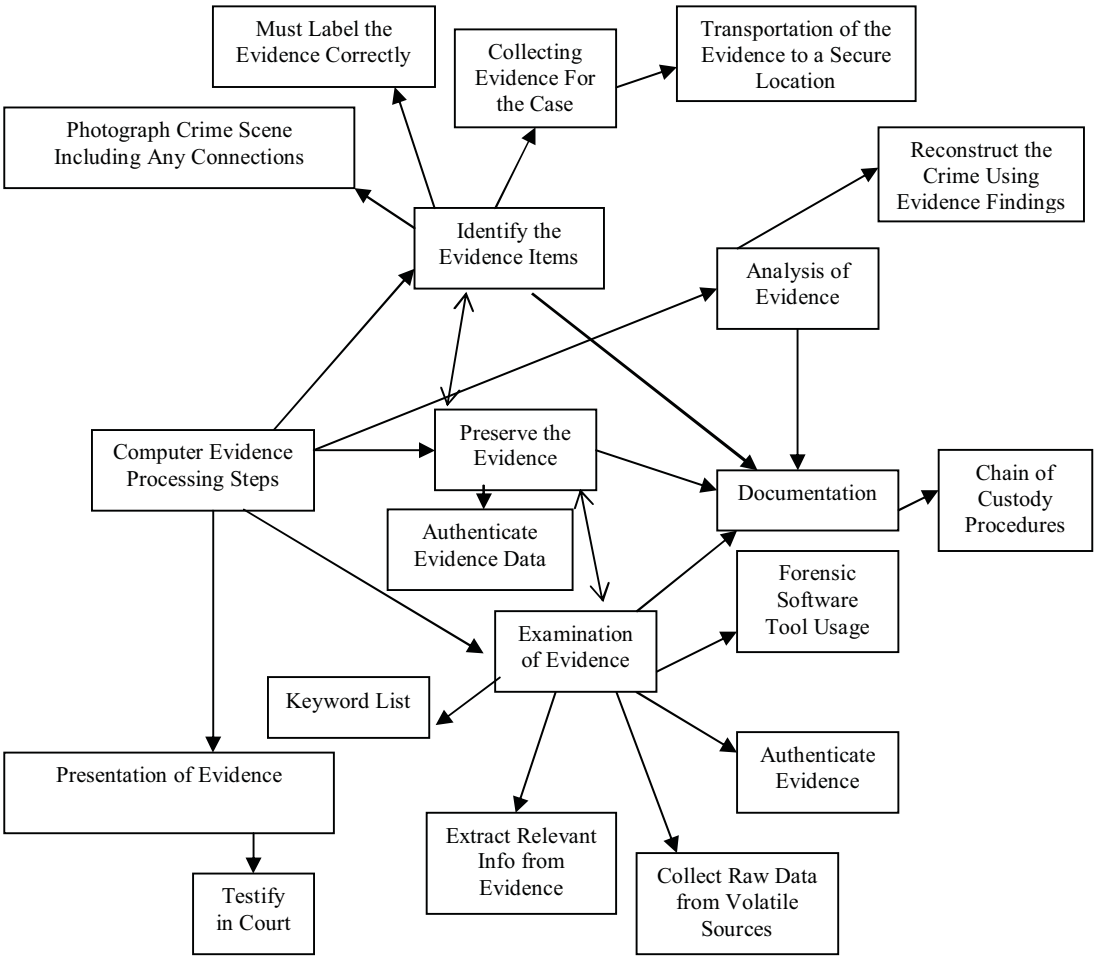


Figure 2.9 An Example Computer Forensic Investigative Process Cognitive Map

Kosko stated that "the fuzzier the knowledge representation, the easier the knowledge acquisition." More ways to represent knowledge can lead to additional information. With fuzzy cognitive maps, the dis-concepts or negations have to be accounted for as well, and mapped weights are applied to the edges or the relationships of concept maps. These negations could also be useful for developing hypotheses as well. Figure 2.10 represents a FCM of a causal, fuzzy relationship affecting learning a user's password and shows both positive and negative causality [7, 28].

www.manaraa.com

Fuzzy cognitive maps would be useful to this dissertation for determining knowledge/concept combination strategies by first applying positive and negative signs to concepts [28, 29, 30]. Fuzziness measures the degree to which something occurs or some condition exists, and it can be used to determine the probability that an event happened or could have happened. Furthermore, FCMs would be useful for reconstructing crimes and modeling past cases by applying causality to the concepts. This dissertation work shares many similarities to FCMs. Like concept mapping, FCMs can provide a quick "first approximation to an expert's state or printed casual knowledge" [31]; a quick overview

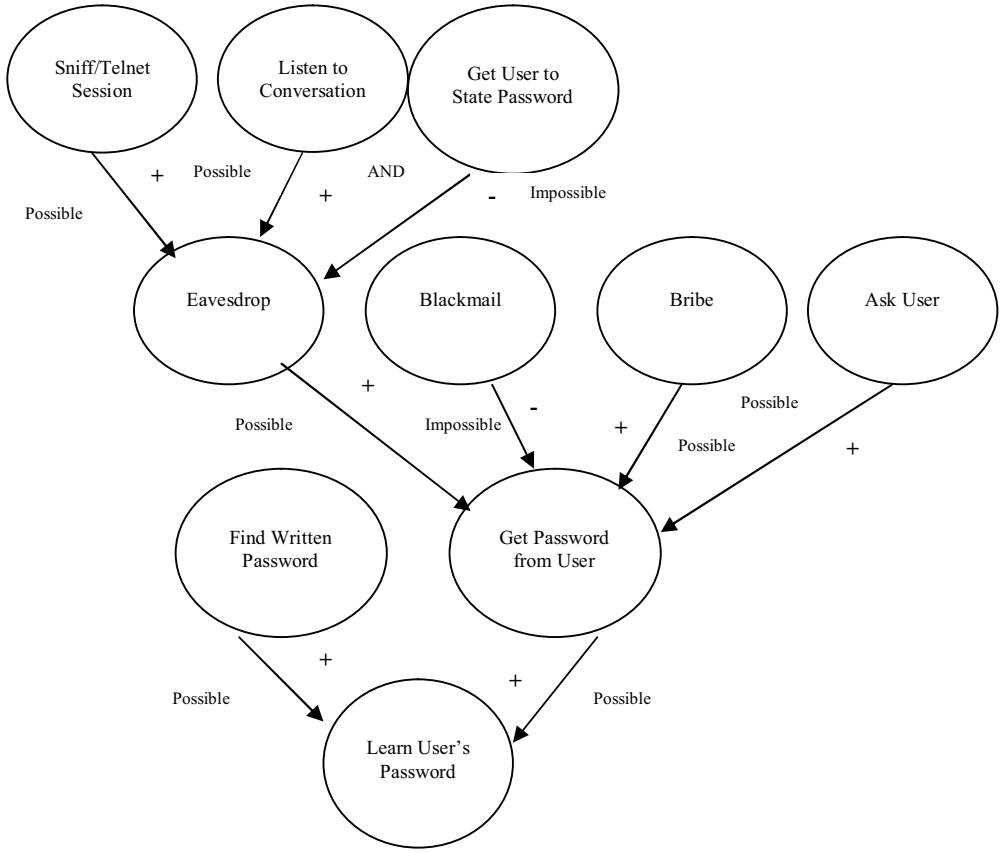


Figure 2.10 The Causal Relationships of Learning a User's Password FCM

www.manaraa.com

of an expert's knowledge can be determined by referring to his or her concept map. Similar to concept mapping, FCM feedback allows experts to address their problems by drawing causal pictures of the problem; in addition, two or more FCMs could be added to produce new FCMs [31]. FCMs could also be useful when experts are developing the concept maps. The experts could apply positive and negative signs to each of the arcs/links and then use the FCM technique to sum the weights and combine the experts' maps into one map and show a complete map of the experts' knowledge. This knowledge would represent concept relations that would most likely occur. In addition, the weights on the arcs could be changed or adapted to reflect the learned information from the training data. Different weights given by each expert could lead to "hidden patterns" that were not originally known. In large investigations where concept maps can get very large, it would be useful to use FCMs to identify patterns of events. FCMs could be used to identify possible attack sequences and could be used to plan investigations by following a given pattern.

2.2.3 Concept Maps

Concept maps are another type of conceptual model that organizes and represents knowledge hierarchically by showing the relationships between concepts. Concepts are usually represented as enclosed circles or boxes, while cross-links are represented as lines as shown in Figure 2.11. The most inclusive, general concepts are located at the top of the map, and the less general, more specific concepts are located hierarchically below. Specific events objects, which are not required to be included in ovals or boxes, help clarify the meaning of a concept and are featured in these maps. Unlike the previous

www.manaraa.com

models, cross-links are included on the line connecting concepts. Cross-links show how concepts are related to one another.

Concept maps were first used in 1972 to track and better understand children's knowledge of science [43]. Since then, researchers and practitioners from various fields have used them as evaluation tools, to plan curriculums, to capture and archive expert knowledge, and to map domain information [32, 43]. Novak and Cañas stated that "concept mapping has been shown to help learners learn, researchers create new knowledge, administrators to better manage organizations, writers to write, and evaluators assess learning." Furthermore, a concept map can be viewed as a "simple tool [that] facilitates meaningful learning and the creation of powerful knowledge frameworks that not only permit utilization of the knowledge in new contexts, but also

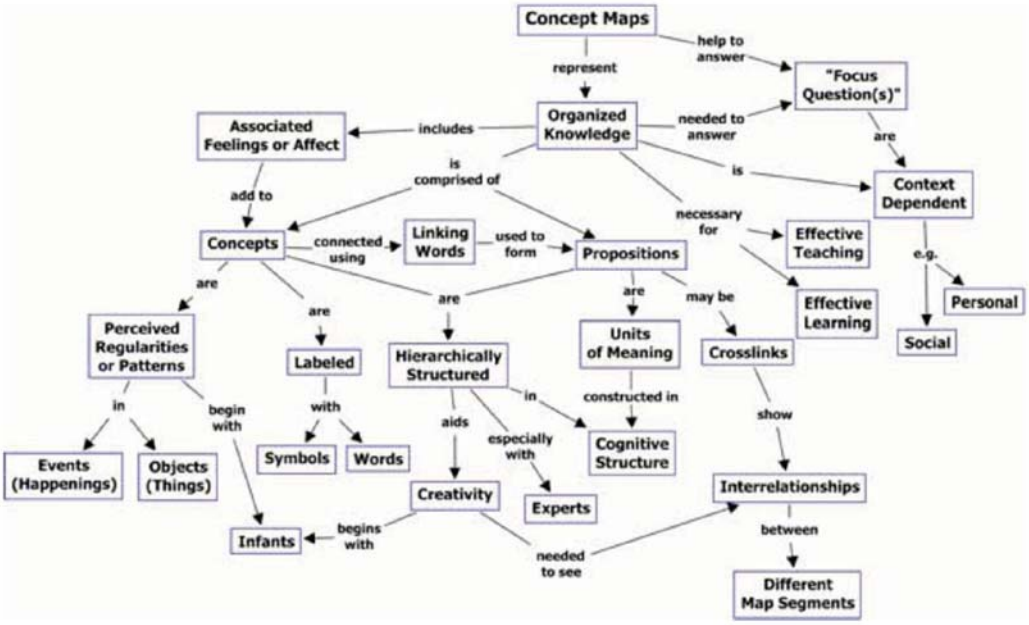


Figure 2.11 A Concept Map Showing Key Features of Concept Maps [43]

www.manaraa.com

the retention of knowledge for long periods of time"[43]. In other words, information that is learned through the use of concept maps allows one to relate this information to previous and potentially new information and retain this information longer.

In order to construct good concept maps, the person constructing the map or maps should be familiar with that particular domain of knowledge [43]. Prior knowledge of the domain is necessary in order to effectively use these models. Novak and Cañas suggested that the following steps be followed in order to build good concept maps. First, a focus question should be developed to help define the context of the concept map. This question helps specify what problem or issue the concept map will resolve. This aspect would be useful in computer forensic investigations, because it would ultimately help in the creation of hypothesis to be used in forensic analysis. Next, key concepts that apply to the domain should be identified. It is suggested that the concepts, first, be listed. From that list, the concepts should be ranked and listed according to the most general concepts to the more specific concepts. This procedure helps to start the map creation process. Next, a preliminary concept map should be constructed from the concepts. Novak and Cañas also suggested that concepts be written on Post-It notes, and the Post-Its should be arranged correctly before writing them down on paper. They also suggested that computer software, one such as IHMC CmapTools, be used. Both options allow the user to move concepts around easily. Post-It notes were suggested for use with larger groups and CmapTools was suggested for use with two or more individuals. CmapTools allows the user to move concepts around with the cross-links as well. It also allows for collaboration on maps between individuals in the same room or on the Internet. Next,

www.manaraa.com

after the preliminary map has been constructed, the map should be revised. Several revisions of the map may result; in this case, computer software would be more appropriate. After revisions have been made, cross-links should be created and placed between the concepts to show how they are related to one another. The last step in concept map creation involves revising the map and repositioning concepts for better understanding, clarity, and structure. Once all of these steps have taken place, a final map should be created. Concept maps can be manually sketched on paper or can be generated using concept mapping software. It is suggested that software be used, because future changes could be made to the concept map much easier.

The concept mapping software also provides many additional features that enhance important details of concept maps for a specific domain. For instance, the CmapTools software allows the user to link resources such as photos, images, graphs, videos, charts, tables, texts, web pages or other concept maps [13, 43]. This software is free to use, allows collaboration from a distance, allows concept maps to be published and shared with others via server, and allows searching within the concept map and/or searching of the Internet for information relative to the map such as articles or other digital information. These resources can be shown as icons, which are located as an image or images at the bottom of the concepts like in Figure 2.12.

When the icon is clicked, the icon will display a list of links that the user can choose from to open the linked resource. Evidence reports created using forensics software could even be included on a concept map. This would provide the examiner or investigator with a quick view of the case; furthermore, the software can export the map

www.manaraa.com

as a PDF file, html file, or image file. The software also creates a "web page" version of the concept map so an Internet ready version can be viewed and used. Another important component of the Institute for Human and Machine Cognition's (IHMC) software toolkit is the CmapServer. The CmapServer can be used to store the concept maps. It promotes collaboration among users and ultimately between law enforcement units. It also provides "discussion threads" and "annotations" so that comments can be made about the maps during construction. According to [43], "the high degree of explicitness of concept maps makes them an ideal vehicle for exchange of ideas or for the collaborative

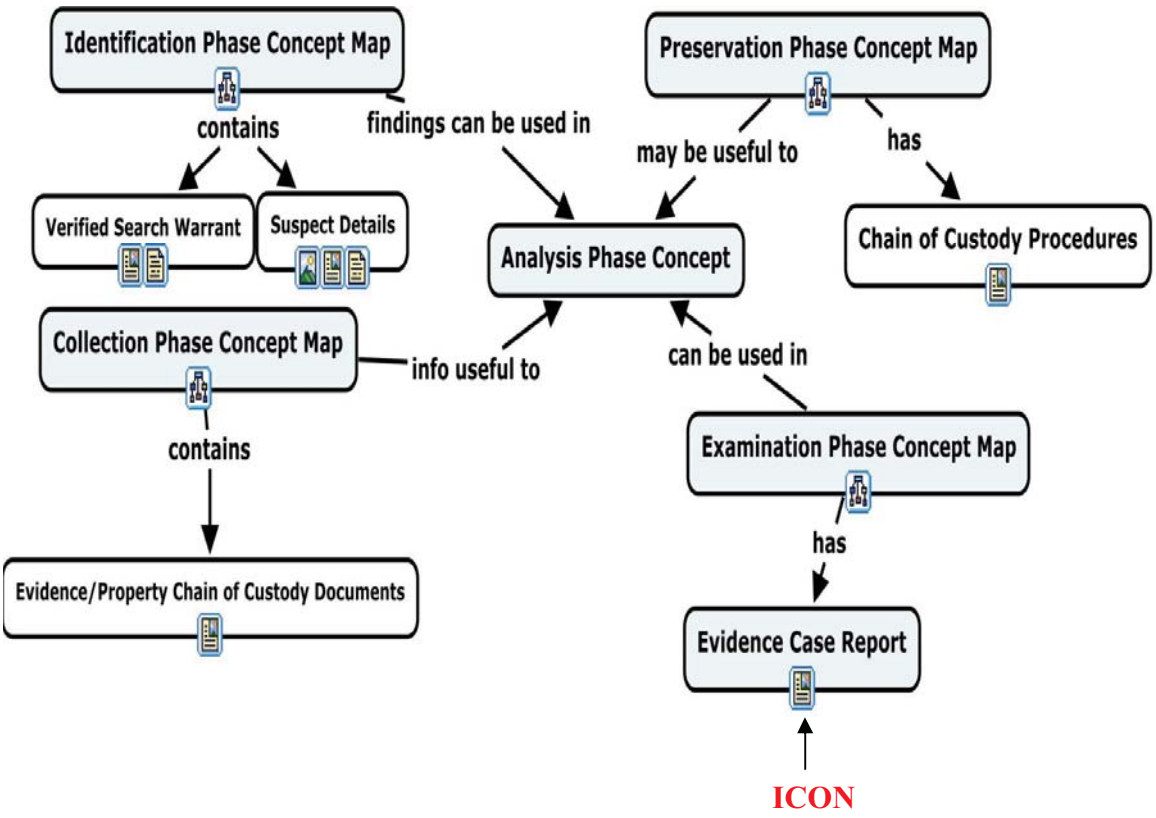


Figure 2.12 A CmapTools Generated Computer Forensics Analysis Phase Concept Map

www.manaraa.com

construction of new knowledge." In other words, when people work in groups someone may think of something that the other did know or hadn't realized and in this case, that person will have learned something new and will add to his existing knowledge from what he has just learned [13]. By sharing digital forensic information over the Internet, the digital forensic community could be brought closer together. This could aid in the development of a lessons learned digital forensic repository.

Figures 2.12 and 2.13 show concept maps generated using the CmapTools software. Figure 2.12 is a computer forensic analysis phase concept map. In this figure, it shows how each concept is linked and also shows the icons of each concept. Some concepts are not connected to the other concepts; however, they still contain information relative to the computer forensic analysis phase and are still displayed in the map.

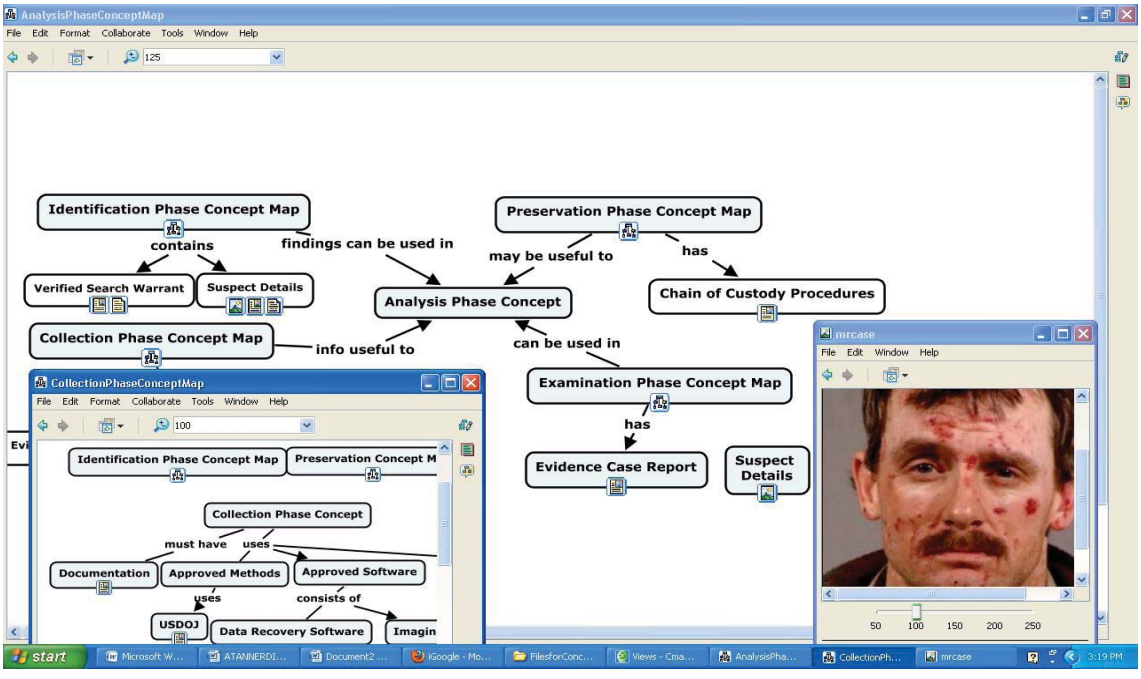


Figure 2.13 A CmapTools Generated Analysis Phase Concept Map with Icons Displayed

www.manaraa.com

Figure 2.13 is a concept map generated by the concept mapping software that shows how a concept map can be represented within another concept map. On the Collection Phase Concept Map concept found in the Analysis Phase concept map, an icon for the collection phase concept map has been created and stored within that concept. The concept mapping tool can reduce the complexity associated with large scale investigations in digital forensics by creating an overall view of the case, and most importantly include additional details within sub-maps.

Concept mapping would enhance the case domain modeling approach in the following ways: by adding a visual sequence of steps rather than a detailed list of steps; by minimizing the level of knowledge needed to understand the maps for individuals with or without experience; by providing an additional way of documenting the evidence; by assisting with reporting information confidently; and by utilizing the maps during official examinations as well as during training. Novak and Cañas [43] stated that a concept map "may first look like a simple arrangement of words into a hierarchy, but when care is used in organizing the concepts represented by the words, and the propositions or ideas are formed with well-chosen linking words, one begins to see the good concept map is at once simple, but also elegantly complex with profound meanings." This dissertation used concept mapping during the examination and analysis phases of a computer forensics investigation. The concept map was chosen as the graphical representation for the computer forensics model because it is relatively easy to understand, easy to learn, and has free software that is easy to use.

www.manaraa.com

2.3 Knowledge Management in Computer Forensics

Of the many issues associated with computer forensics, knowledge management strategies are also important to the future of not only computer forensics, but digital forensics as well. According to [14], "Effective knowledge management maintains the knowledge assests of an organization by identifying and capturing useful information in a usable form, and by supporting refinement and reuse of that information in service of the organization's goals. A particularly important asset is the internal knowledge embodied in the experience of task experts that may be lost with shifts in projects and personnel." There is a need for knowledge management in digital forensics due to the increased usage of the Internet, the increase in digital crimes using different types of digital media, and the constant advances in technology. A standardized method for capturing and reusing digital crime knowledge could prove to be invaluable to the law enforcement community. This section will discuss the importance and the need for knowledge management in digital forensics.

2.3.1 Need for Expert Knowledge in Computer Forensics

Tacit knowledge or expert knowledge is basically an internal knowing of what needs to be done and how it should be done [14]. Computer crimes are increasing, and there is a great need for knowledge sharing amongst the local, state, and federal authorities to further combat these crimes. When computer forensic examiners perform examinations, their specialized skills may not be recorded. These specialized skills could be very useful for external reviews and training. Skilled and experienced personnel know what to look for, where to look, and how to look without compromising the evidence.

www.manaraa.com

Externalizing this knowledge could assist novice examiners in investigations and could potentially lead to the creation of a knowledge repository. In most cases, digital forensic examiners must search through large amounts of data to find evidence. With digital storage capacities becoming increasingly larger, this task is becoming even more complex and time consuming. Knowledge management methodologies in the computer forensics domain have been addressed in [12, 48, 54]. Bruschi, Monga, and Martignoni [12] proposed a model that organizes forensic knowledge in a reusable way. This model uses past experiences to train new personnel, to enable knowledge sharing among detective communities, and to allow third parties to assess the quality of collected information. They also suggested that disciplined methodologies should be created that provide the possibility of archiving digital forensic knowledge that would aid in training and best practice guidelines.

2.3.2 Knowledge Capture and Reuse

A method for effectively reusing and managing knowledge could greatly improve the digital forensic process. According to [48], the practice of digital forensics could be enhanced by developing "knowledge management strategies specific to law enforcement that will operate within the specific context of criminal investigations" [48]. A possibility exists for incorporating concept maps into every phase of a digital investigation; however, in this research, concept mapping will be applied only to the examination phase of an investigation. In [12], their approach aims to provide a "methodology for archiving, retrieving, and reasoning about forensic knowledge, in order to incrementally improve the skills and the work of a team of detectives." Their proposed

www.manaraa.com

software tool and approach will produce reusable forensic knowledge as support during investigations, will organize past experience to encourage knowledge sharing among forensic experts, and will record collected information in a way that eases quality assessment. In order to demonstrate the importance of capturing and reusing knowledge, Kramer utilized concept maps to provide a method for capturing the tacit knowledge of design process experts.

Kramer's [32] research project attempted to collect, understand, and reuse the knowledge of multiple domain experts on design processes that drive initial design decisions associated with translating "Requirements on Orbit" to "Design Requirements." Concept maps were utilized as a knowledge acquisition and representation tool among multiple domain experts in the translation from a statement of requirements to design requirement specifications. Three specific goals for this research were as follows: demonstrating how concept maps can be used for knowledge acquisition among multiple domain experts; developing a prototype knowledge representation model from the concept maps for guiding the development of design requirements from "Statements of Requirements on Orbit"; and assessing the utility of that prototype knowledge acquisition and representation model by examination of a limited problem set. This research is related to my dissertation because it provided a way to acquire and represent expert knowledge in the concept maps. Kramer was able to effectively show the usefulness of concept maps in eliciting and representing expert knowledge; consequently, this dissertation explores the possibility of utilizing concept maps in the computer forensics domain.

www.manaraa.com

2.3.2.1 A Knowledge Reuse Framework

The goal of Bruschi, Monga, and Martignoni's [12] research was to develop a model that would use forensic graphs to organize forensic knowledge that could be used in future investigations. These graphs could be altered to represent unrelated information, to structure the graphical representation of the hypothesis and evidence in order to provide a quick overview of the case, and also to guide less skilled detectives during evidence collection by recording the information in a structured fashion. Their framework contains an acyclic directed graph whose nodes are hypotheses, the evidence collecting tests are attached leaf hypotheses, and the edges represent decomposition links and the first application of the synthesis rule (i.e. link between evidence and hypotheses), which is defined as follows:

$$FG=<H, E, F_h, F_e, w> \quad (2\text{-}1)$$

where H is the set of hypotheses, E is the set of evidence collecting tests, F_h is a decomposition relation ($F_h \subseteq H \times H$), and w, or $w \in \{?,+,-\}$, is the weight of evidence that is used to determine if the evidence has been analyzed, if the evidence test was performed, and if the results corroborate or contradict a hypotheses. F_e is an association relation or the application of the synthesis rule ($F_e \subseteq H \times E \times w$).

www.manaraa.com

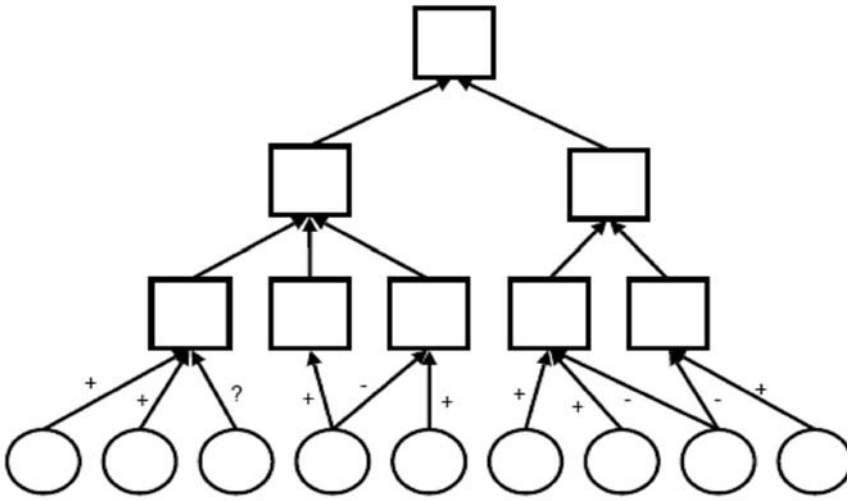


Figure 2.14 Graphical Formalism Adopted to Represent Case Graph [12]

The forensic graph, shown in Figure 2.14, is used to represent all the knowledge acquired over time. The weight of evidence becomes meaningful when the model is instantiated or when data is applied to it. When the model is instantiated, a new graph or case graph is created that will use only a subset of the whole set of elements. As shown in Figure 2.14, hypotheses are represented by squares, evidence collecting tests are represented as circles, and the weight of evidence is represented by a label on the edge linking evidence to hypotheses. The input of the decomposition rule is the root node of the graph and its output is the whole graph composed only by square nodes. The synthesis rule accepts in input, which is the output of the previous phase, and outputs the graph made by both square nodes and circle nodes. From this graph, the detective would then test each piece of evidence and record how they modified his/her belief in the hypotheses he/she is linked to by using the following symbols: the "+" symbol means

www.manaraa.com

corroboration, "-" means contradiction, and "?" signifies that evidence was not collected or not applicable" [12].

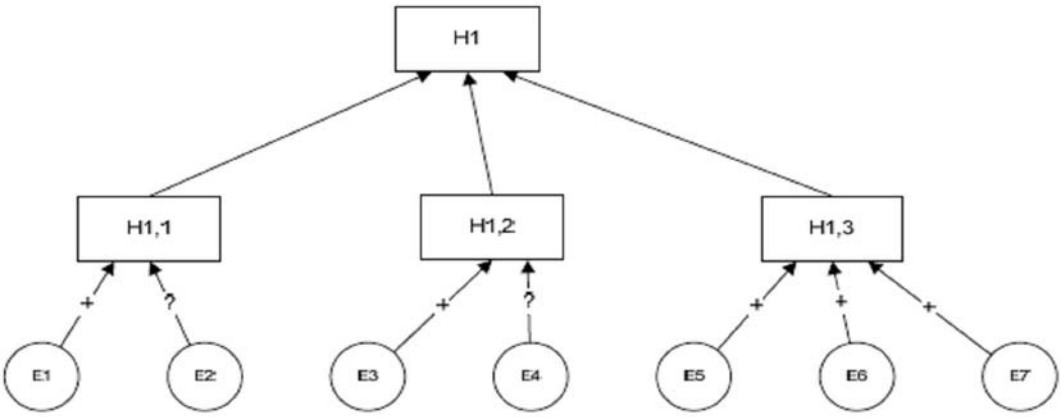
Figure 2.15 provides a textual and graphical representation of a forensic graph that decomposes the hypothesis: Suspect *I* on date *D* possessed a copy of file *F* [7]. Figure 2.15 is an instantiated forensic graph relative to the computer forensic domain.

This framework is related to this dissertation because the goals of both [12] and this research are very similar. The goals are to find a way to reuse knowledge by using an alterable visual graph that represents hypothesis and evidence information in a structured fashion; in addition, a quick overview of the case can be used to guide novice investigators thorough the evidence examination process. Also, both provide a structured way to record evidential findings. In conclusion, [12] and the concept mapping case domain modeling approach both address the need for creating a model that promotes knowledge reuse in the law enforcement community.

2.3.2.2 Case-Relevant Framework

Rubin, Yun, and Gaertner [54] proposed a method to effectively bind computer intelligence into the current framework. This binding would benefit the current investigation procedure with higher automation, effectiveness, and better knowledge reuse. The data analysis phase, which consists of both the examination and analysis phases, is tedious, time-consuming, and requires investigator expertise according to [54]. The objectives of the data analysis phase are to "examine, search, and extract relevant data collected in the data collection phase and to supply sufficient information for the

www.manaraa.com



H_1 I on date D, possessed a copy of the file F.
- $H_{1,1}$ I's system contained a file that corresponds exactly to the incriminated one (both metadata and content match).
  - E_1 F is found on I's system(both metadata and content match).
  - E_2 F was on I's system but it has been deleted (metadata matches, the recovered content corresponds to the original).
- $H_{1,2}$ I's system contained a file that corresponds only in part to the F (only metadata matches).
  - E_3 F is found on I's system (metadata matches but content does not).
  - E_4 F was on I's system but it has been deleted (metadata matches, the recovered content does not correspond to the original).
- $H_{1,3}$ I's system contained only reference to F.
  - E_5 references to F are found in user's history.
  - E_6 references to F are found in user's documents.
  - E_7 references to F are found in the application's history.

Figure 2.15 Example Forensic Graph [7]

crime scenario reconstruction and suspected activity confirmation." Experienced investigators usually maintain a collection of search lists from previous cases to be reused in future cases during data analysis. [54] stated that a systematic mechanism for knowledge collection, management, sharing, and reuse, and decision support is needed. In addition, this framework should be simple to understand and utilize. For this reason, it was believed that a formal and repeatable test dataset and evaluation environment for the data analysis phase was needed. Although many computer forensic tools offer an integrated environment for data capturing, imaging, searching, filtering, and analyzing,

www.manaraa.com

[62] stated that "the major part of the information searching, extraction, and analysis work is still left to the human." For instance, the investigator still has to examine the evidence to determine whether the discovered evidence is relevant to the case or not.

Case-Relevance is described as "the property of any piece of information, which is used to measure its ability to answer the investigative who, what, when, why, and how questions in a criminal investigation" [54]. Case-relevance is defined to measure the importance of any information given in a case, and can be useful for searching, filtering, and organizing data effectively. The six degrees of Case-Relevance, shown in Figure 2.16, represent a continuous spectrum from absolutely irrelevant to provably case-relevant. Possible and probable are used to distinguish the increasing level of Case-Relevance or irrelevance. The spectrum helps establish an effective framework for analyzing cost versus completeness because time is limited in computer forensic investigations. By binding computer intelligence into the computer forensic framework based on Case-Relevance, the current system becomes a target-oriented framework that requires no redesign of the framework itself.

Law enforcement agencies have the best-maintained document system, but for reasons of security and privacy protection, these documents are not accessible to the

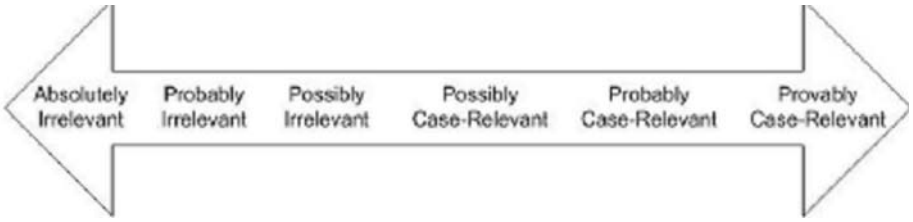


Figure 2.16 Degrees of Case-Relevance [54]

www.manaraa.com

research community [54]. The author's suggest adopting law enforcement methods to build and publish a standard dataset for computer forensics investigations. The dataset should be created from re-organized and filtered raw data of selected cases. This research is useful to this dissertation because integrating case relevance into the examination phase of the digital forensics investigations could assist an examiner in determining if evidence is relevant to the case. By using the case-relevance spectrum, the investigator would know what evidence information is most relevant to the case and should be included and presented in his/her findings.

2.4 Analysis of Related Work

Several modeling approaches have been proposed for use during a digital forensics investigation. However, little or no empirical data exists that shows the practicability and applicability of these approaches to digital forensic cases. More qualitative and quantitative data is greatly needed in the digital forensics domain, which could lead to a consensus for a standardized investigative approach for digital forensics investigations. Modeling approaches are not being used by forensic examiners to carry out examinations. Reasons for this could be that examiners do not fully understand the models, use of the models would only increase the time required to examine and analyze an already large backlog of evidence, and/or there would be no additional benefit of using these models. Currently, keyword searches, checklists, other documents, and computer forensic software tools are used to aid in the discovery of evidence during an examination. Utilizing digital forensic models, especially case specific models, could lead to better ways of developing experimental data. This data could then be shared with

www.manaraa.com

the law enforcement community and researchers as well. The DFRWS model lead to the creation of several different models; however, experimental data is still very limited.

Investigative, hypothesis, process flow, and case domain modeling approaches all resulted from the DFRWS model. Investigative process models focus more on the phases of the digital investigation. These models provide a plan for conducting a forensic investigation, and they address the basic phases of the DFRWS model; however, this type of modeling provides only a general pattern of activities with no artifacts. Experiments have not been performed using these models, so there is no way to determine their effectiveness as a better modeling approach as compared to other approaches. The hypothesis modeling approaches use hypotheses for analyzing all the possibilities of the case details. These modeling approaches could possibly be useful to expert computer forensic investigators, but would not be as useful to novice investigators because more details would be needed for them to carry out an examination. Modeling approaches that focused on the information domain of the case were also proposed in [7, 69]. Venter [69] discussed the proper collection of evidence relative to a case while Bogen [7] focused on the planning of an examination for a case. In both instances, expressive tools were used. Venter provided a process flow diagram to show what items should be collected and Bogen utilized UML models and tables to represent the case domain information. The process flow diagrams only addressed the collection of evidence, but none were created for the examination and analysis of the evidence. The case domain modeling approach was created "to address the shortcomings of existing modeling approaches by offering a structured domain modeling approach for defining the information domain of a forensics

www.manaraa.com

examination" [7]. Although Bogen's work did show that the case domain modeling approach improved the search for and identification of evidence, there was not a significant improvement in the results. It was also found that the case domain modeling approach did not significantly improve the subjects' understanding of the case and the case concepts.

This dissertation research is an extended version of Bogen's case domain model, and it will use the concept mapping technique to organize, structure, and represent the information domain of a forensics examination. The concept mapping case domain modeling approach was developed to determine its viability and applicability as a general reference framework for use during examinations and analysis; in addition, this work will focus more on the concept mapping technique when applied to the case domain modeling approach.

The first way in which this dissertation work differs from the case domain model is that a different conceptual diagram (concept maps) was used to determine its applicability to the search and identification of evidence and the analysis of the case domain. Secondly, evidence items identified and extracted such as photos, images, text documents, web pages, and etc. could be added to the final concept map using concept mapping software. Thirdly, semi-automated computer software (concept mapping software) was made available for use by the subjects to search for, identify, and extract evidence using concept maps for a particular case. A general computer forensic examination guide concept map was created from government guidelines and peer-reviewed journal papers and combined into one map. This map was used by the subjects

www.manaraa.com

in the experiments. Lastly, this research evaluated whether the use of concept maps led to a better retention of knowledge and a better understanding of the forensic examination and analysis of a particular case.

Conceptual models are suitable for representing the information domain of a computer forensics examination. The concept mapping method is most suitable for modeling the case domain because concept maps are easy to understand, can be used to organize information, has a semi-automated tool available, can be shared, has the ability to create new knowledge and uncover gaps in a person's knowledge. Unlike concept mapping, semantic networks and cognitive mapping would not be useful for large scale investigations because the size of the maps would increase drastically, and it would also be difficult to represent the domain information in a way that would be beneficial to law enforcement. Concept maps can become quite large as well. Given that complexity is an issue with many domain methodologies, [11] stated that the ability of concept maps to provide a total and limited, synthetic and descriptive view of a knowledge domain can be very beneficial in complex domains. Similar to other domain modeling approaches, concept maps are used to identify domain concepts, to identify relationships between those domain concepts, and to identify attributes or properties of those concepts [7]. In digital forensics, the information domain of a case has been defined by using keyword lists, checklists, and other documents; however, to overcome complexity in the forensics domain, concept maps can also be used as guides to navigate through large amounts of data.

www.manaraa.com

One advantage that the concept mapping technique provides is the placement of concept maps within other concept maps; this feature could greatly reduce the complexity of the forensics domain. Within each concept, additional concepts and concept maps can be developed and each concept could contain information regarding the investigative procedure for that particular phase of the investigation. For instance, in the examination phase concept, a concept map could be developed from the evidence items and crime categories provided in [2, 44, 65, 66]. These evidence items and crime categories can be directly mapped as case concepts. A keyword selection methodology could be adapted from the case domain modeling approach and relationships could be determined by using the case domain modeling relationship category table also provided in [7]. As the forensics domain expands, concept maps can be easily modified to represent additional concepts, relationships, and concept maps. The individual using concept maps could visually see what activities have been accomplished and have not been accomplished as well. According to Tergan [62], concept maps take advantage of "the human visual perception system and the benefits of visual information representation." The benefits of using concept maps include ease of recognition, finding differences or keywords by possibly scanning a picture or some object, the compactness of the concept maps representation, and the ease of keeping an overview of the domain [62].

Given how complex domains can become, concept maps would be useful as an indexing and navigational tool [13, 43]. According to [68], a deficiency in visual representation of concept maps occurs when there are overlapping concepts in concept maps; this overlap inhibits an individual from obtaining a quick overview of the domain.

www.manaraa.com

However, quick overviews of the specified domain are one of the advantages of using the concept mapping technique; it was also insisted that concept maps be created within other concept maps as a way to reduce overlapping concepts [68]. Zaff and McNeese [76] discussed how concept mapping can be used to organize one's thoughts and can serve as an external memory aid when navigating complex domains; however, they also stated that too many concepts and relationships can result in the visual complexities as well. To remedy this problem, it was suggested that the concept map either be parsed into subsections or by hierarchical structure. Parsing the map into subsections based on related concepts could make the concept map more visually stimulating, however, one of the main advantages of using the concept mapping technique is that it allows one to view all of the relationships between the concepts; however, this characteristic would not be fulfilled when the concept map is parsed into subsections, because some concepts and relationships may be hidden. Parsing by hierarchical structure was also suggested for solving the concept map complexity problem. Instead of grouping concepts into subsections, it was suggested that the more global, general, or key concepts be represented within concept maps and the more detailed concepts be represented within the more general concepts [12].

Concept mapping has been utilized for managing knowledge for training, for knowledge sharing, for evaluating of tools, for capturing and reusing expert knowledge, for preserving knowledge, and as decision aids in areas such as education, business, military, and government. Implementing a modeling approach that could effectively manage and reuse knowledge would greatly enhance the digital forensic investigative

www.manaraa.com

process. Knowledge management strategies were incorporated into the concept mapping case domain modeling approach in an attempt to exploit tacit knowledge that experienced subjects may have had and ultimately transform it into a reusable form using concept maps.

www.manaraa.com

CHAPTER III

CONCEPT MAPPING CASE DOMAIN MODELING APPROACH

This chapter describes the concept mapping case domain modeling approach and discusses how the approach may be useful in real criminal cases.

3.1 Concept Mapping Case Domain Modeling

The goals of the concept mapping case domain model are to organize, examine, and analyze the known and unknown domain information of the forensics case. The concept mapping case domain model is derived from Bogen's [7] case domain model and concept mapping method developed by Novak and Cañas [43]. Elements of both the UML conceptual modeling and concept mapping approaches are used to develop this process consisting of a five phase, non-linear process for modeling the information domain:

1. Identifying a focus question,
2. Identifying the case concepts,
3. Identifying the attributes,
4. Identifying the relationships, and
5. Instantiating the model.

The remainder of these sections describes how each of the domain modeling steps should be executed for planning the examination.

www.manaraa.com

3.1.1 Identifying a Focus Question

Concept maps can be constructed to answer a question by developing a focus question. Focus questions help provide the context for the map. It also helps the creator to stay focused on the task and can lead to a richer concept map [43]. A focus question may also be useful during the analysis phase of the investigation; for instance, this question can assist the examiner in developing hypotheses to aid in solving the case or lead to the search for additional evidence.

3.1.2 Identifying the Case Concepts

Concepts are the key components of both the concept map and case domain model because they are used to represent events or objects, are related to other concepts, and include information relative to the case domain that is needed for the examination. In the concept mapping case domain modeling approach, concepts can have zero or more attributes and can have zero or more concepts. This would be useful in cases where unknown information is found because it can be represented on the concept map as a concept as well. Like the case domain modeling approach, a list of concepts relative to the information domain would be selected in the concept mapping case domain modeling approach (CMCDMA). The concepts will be organized according to rank. This ranking starts from the most general, most inclusive concepts, to the most specific, least general concepts. Furthermore, this list ranking helps begin the map construction process. Instead of eliminating concepts, Novak and Cañas [42], refer to the list as a "parking lot" since concepts are moved from the parking lot into the appropriate place in the concept map. Concepts that are not used would remain in the parking lot for potential later use.

www.manaraa.com

Reusability is very important when selecting concepts because the reuse of concepts from previous cases/models can save time when developing future cases/models. This is one of the main reasons that general concepts are developed first when selecting concepts in the concept mapping case domain modeling approach. In the CMCDMA, unused concepts can remain as concepts in the concept map and even though these concepts do not have a place in the map, they can still be added as a concept, if needed.

Concepts in the case domain modeling approach were identified using noun-verb extraction and the USDOJ's checklist of common evidence items that should be looked for in different types of investigations as shown in Table 3.1, Table 3.2, Table 3.3 and Table 3.4 [7, 65].

The CMCDMA used the examples in Table 3.1 to identify, create, and/or suggest additional concepts for the concept maps. Table 3.2 provides a general concept category checklist that links the common types of concepts with relevant computer forensic examples in the domain [7]. This checklist would be useful for determining if the concepts in each category were relevant to the case domain. Furthermore, the evidence categories and activities shown in the Tables 3.3, 3.4, and 3.5 were used to map case concepts in the CMCDMA.

Novak and Cañas [43] suggested that a preliminary concept map be created after the concepts have been identified using either post-it notes or a concept mapping software, CmapTools. In smaller investigations, concepts could be represented as each

www.manaraa.com

Table 3.1 Case Domain Model Concept Category Table with Examples [7]

Concept Category	Examples
Physical or tangible objects	Cell phone, Hard Drive, CDR disk
Descriptions of things	Marketing Report, Incident Report
Places	Home, Street
Transactions	Payment, Sale, Money Deposit, Email Transmission
Roles of people	Victim, Suspect, Witness
Containers of things	Databases, Hard Drives
Things in a container	Files, Transactions
Computer or Electro-mechanical systems	Internet Store, Credit Card Authorization System
Abstract noun concepts	Motive, Alibi, Insanity, Poverty
Organizations	Mafia, Corporate Department, Government Organization
Events	Robbery, Meeting, Phone Call, File Access
Rules and policies	Laws, Procedures
Records of finance, work, contracts, legal matters	Employment Contract, Lease, Receipt, Subpoena
Services	Internet Service Provider, Telephone Service, Cell Phone Service
Manuals, Books	Flight Manual, Explosives Manual

www.manaraa.com

Table 3.2 USDOJ Evidence Targets by Case Category (Part I) [65]

	Sex Crimes					Crimes Against Persons				Fraud/Other Financial Crime				
	Child Exploitation/Abuse	Prostitution	Death Investigation	Domestic Violence	E-Mail Threats/ Harassment/Stalking	Auction Fraud	Computer Intrusion	Economic Fraud	Extortion	Gambling	Identity Theft	Narcotics	Software Piracy	Telecommunications Fraud
General Information:														
Databases		✓				✓		✓		✓		✓		
E-Mail/notes/letters	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Financial/asset records		✓	✓	✓	✓	✓		✓		✓		✓		✓
Medical records		✓	✓	✓										
Telephone records			✓	✓	✓	✓								✓
Specific Information:														
Account data						✓								
Accounting/bookkeeping software						✓								
Address books		✓	✓	✓	✓	✓	✓	✓		✓		✓		
Backdrops											✓			
Biographies			✓											
Birth certificates											✓			
Calendar		✓				✓		✓		✓		✓		
Chat logs	✓					✓							✓	
Check, currency, and money order images								✓			✓			
Check cashing cards											✓			
Cloning software														✓
Configuration files							✓							
Counterfeit money											✓			
Credit card generators											✓			
Credit card numbers											✓			
Credit card reader/writer											✓			
Credit card skimmers								✓						
Customer database/ records		✓								✓				✓
Customer information/ credit card data						✓		✓		✓				
Date and time stamps	✓								✓					
Diaries			✓	✓	✓									
Digital cameras/software/ images	✓					✓					✓			
Driver's license											✓			
Drug recipes												✓		
Electronic money										✓				
Electronic signatures											✓			

www.manaraa.com

Table 3.3 USDOJ Evidence Targets by Case Category (Part II) [65]

	Sex Crimes		Crimes Against Persons			Fraud/Other Financial Crime							
	Child Exploitation/Abuse	Prostitution	Death Investigation	Domestic Violence	E-Mail Threats/ Harassment/Stalking	Auction Fraud	Computer Intrusion	Economic Fraud	Extortion	Gambling	Identity Theft	Narcotics	Software Piracy	Telecommunication Fraud
Specific Information (Cont):														
Erased Internet documents										✓				
ESN/MIN pair records														✓
Executable programs							✓							
False financial transaction forms								✓						
False identification		✓						✓				✓		
Fictitious court documents										✓				
Fictitious gift certificates										✓				
Fictitious loan documents										✓				
Fictitious sales receipts										✓				
Fictitious vehicle registrations										✓				
Games		✓												
Graphic editing and viewing software	✓													
History log									✓					
"How to phreak" manuals														✓
Images	✓		✓		✓	✓								
Images of signatures							✓							
Image files of software certificates												✓		
Image players									✓					
Internet activity logs	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓		✓
Internet browser history/cache files						✓								
IP address and user name							✓							
IRC chat logs							✓							
Legal documents and wills			✓		✓									
Movie files	✓													
Online financial institution access software						✓		✓						
Online orders and trading information										✓				
Prescription form images											✓			
Records/documents of "testimonials"						✓								

www.manaraa.com

Table 3.4 USDOJ Evidence Targets by Case Category (Part III) [65]

	Sex Crimes		Crimes Against Persons					Fraud/Other Financial Crime						
	Child Exploitation/Abuse	Prostitution	Death Investigation	Domestic Violence	E-Mail Threats/ Harassment/Stalking	Auction Fraud	Computer Intrusion	Economic Fraud	Extortion	Gambling	Identity Theft	Narcotics	Software Piracy	Telecommunications Fraud
Specific Information (Cont):														
Scanners/scanned signatures										✓				
Serial numbers												✓		
Social security cards										✓				
Software cracking information and utilities												✓		
Source code							✓							
Sports betting statistics									✓					
Stock transfer documents										✓				
System files and file slack										✓				
Temporary Internet files								✓						
User names							✓		✓					
User-created directory and file names that classify copyrighted software												✓		
User-created directory and file names that classify images	✓													
Vehicle insurance and transfer documentation										✓				
Victim background research					✓									
Web activity at forgery sites										✓				
Web page advertising		✓												

post-it. Post-its or concepts could be moved around more easily than compared to illustrating the concepts on paper and erasing, drawing, and redrawing. Post-its are best for use in groups also. Novak and Cañas also highly suggest using software, because like Post-its, it allows one to easily restructure the map by moving the concepts or groups of

www.manaraa.com

concepts around with their linking statements. After the preliminary map is created, the attributes should be established.

3.1.3 Identifying the Attributes

In the concept mapping case domain model, attributes are identified after the concepts are specified. They will not be represented as ovals or boxes because they represent specific examples of events or objects and help clarify the concepts meaning. Attributes can be used for constructing keyword searches, examining documents, examining network logs, linking other concepts, and etc [7]. For instance, the attribute information can be placed in a file and represented as an icon within a particular concept. Attributes represented as a sub-map or concept map within a concept could also be placed within the concept containing the file attributes or the attributes can be included as notes on the concept. The concepts in Table 3.1 may also be used to identify attributes as well.

3.1.4 Identifying the Relationships

Concept maps use cross-links or linking words to represent relationships between the concepts by showing how they are related to one another. According to Novak and Cañas [43], "cross-links are key to show that the learner understands the relationships between the sub-domains in the map[, and] it is necessary to be selective in identifying cross-links and to be as precise as possible in identifying linking words that connect concepts". Bogen [7] stated that "relating the concepts adds an additional layer of information that can help an outsider understand the background and circumstances of a case." This would be very beneficial when training forensic examiners or anyone who

www.manaraa.com

examines forensic cases. Table 3.5 shows a concept relationship category table that provides examples common in computer forensic examinations. Poorly developed cross-links often lead to redundancy and should be avoided; for this reason, more prominent, useful cross-links should be created.

3.1.5 Instantiating the Model

Instantiating the model requires the addition of the attributes to the map. In the concept mapping case domain model, the model will be instantiated throughout the construction of the model. Attributes can be categorized as known or unknown, and the known values of the attributes will be used to develop keyword search lists. Misspelled words should also be used in the keyword search list because they can be useful in finding documents authored by a person [7, 57]. Any unknown attributes can be noted

Table 3.5 Relationship Category Table with Examples [7]

Relationship Category	Examples
A is a physical part of B	DVD Drive – Workstation
A is a logical part of B	Network Mapping – Network Intrusion
A is physically contained in/on B	Used CDR Media – CD Case
A is a description for B	Readme file – Executable Program
A owns B	Suspect – Vehicle
A is a member of B	Suspect – Gang
A is an organizational subunit of B	Information Technology Division – Company
A uses or manages B	Systems Administrator – Company Network
A is a specialized version of the generalized B	Systems Administrator – Company Employee
A communicates with B	Suspect – Associates
A is known, logged, recorded, or reported in B	Email Registration – Network Logs

www.manaraa.com

on the concept map or placed in a file and saved as an icon for a concept relative to the unknown attributes that have been found. Any attributes found after the model has been created can be added to the map as well.

3.1.6 Representing the Model

The concept map will be used to graphically represent the concept mapping case domain model. Figure 3.1 provides a representation of the concept mapping case domain model for a narcotics case. Tools such as CmapTools, SmartDraw, Inspiration, and VUE can be used to create graphical concept mapping case domain models. Additional attribute information such as files, pictures, images, video, audio, and other digital items can also become icons for a concept also. For instance, the backpack concept's attribute is the Hannah Montana concept, which displays a photo of the actual backpack in the case in Figure 3.2.

The graphical representations can be used in both large and small scale investigations. The CmapTools software would be very useful in larger investigations because if an investigation needs to be reviewed it would be easy to take a quick glance at the investigation to get an idea about the case. Manually creating concept maps using post-it notes or paper would be useful in smaller investigations. Once the map is finished, a digital version of the map can then be created using the CmapTools software. The digital copy will allow the addition of evidential items and eliminate the need to refer back to paper copies because they will be attached to the appropriately labeled concepts in the concept map. With the concept mapping case domain model, concepts with attributes can be created and page space would still be conserved.

www.manaraa.com

The concept mapping case domain model is not reliant on the CmapTools software. This model can be constructed without the use of CmapTools. However, it would be very beneficial in the law enforcement community for including additional resources such as photos, subpoenas, search warrants, examination search procedures used, and etc. The subjects were encouraged to create additional sub-maps that are linked to the starting map; this may help the subjects develop a deeper understanding of the case. The most general, most inclusive ideas are given, and then the least inclusive more specific concepts can be created by the subjects similar to Figure 3.2.

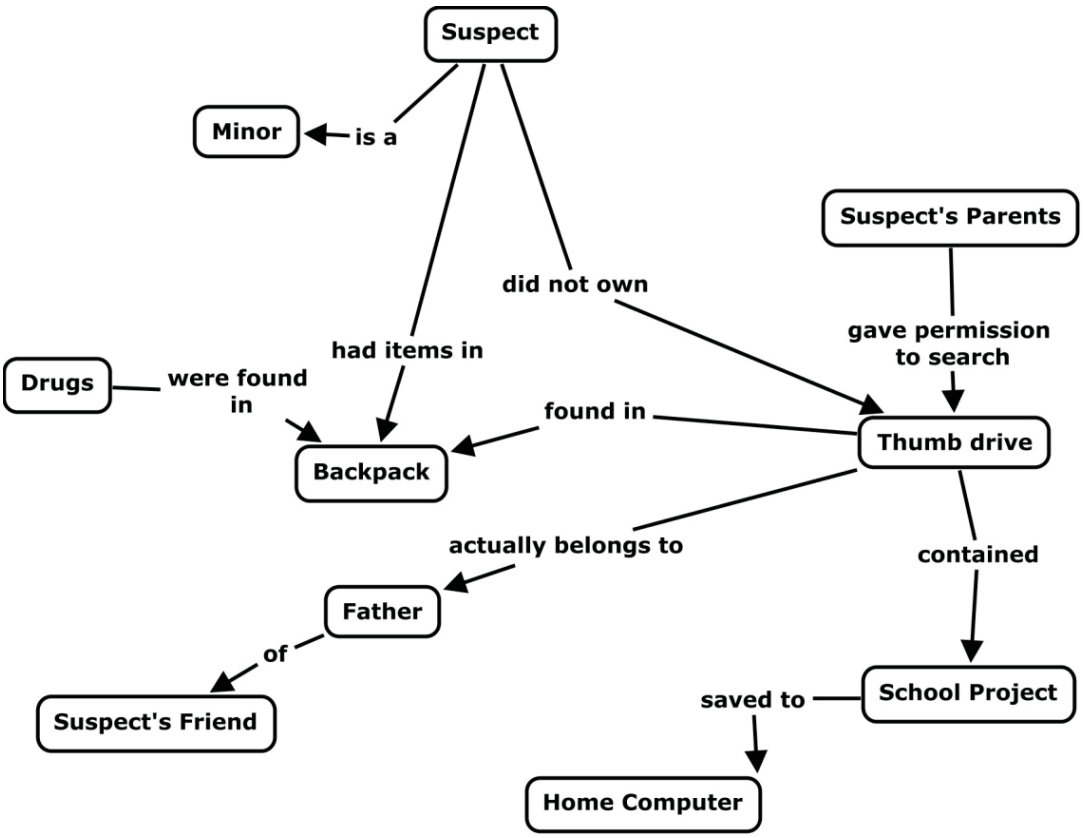


Figure 3.1 Keyword Concept Map for Narcotics Case Example

www.manaraa.com

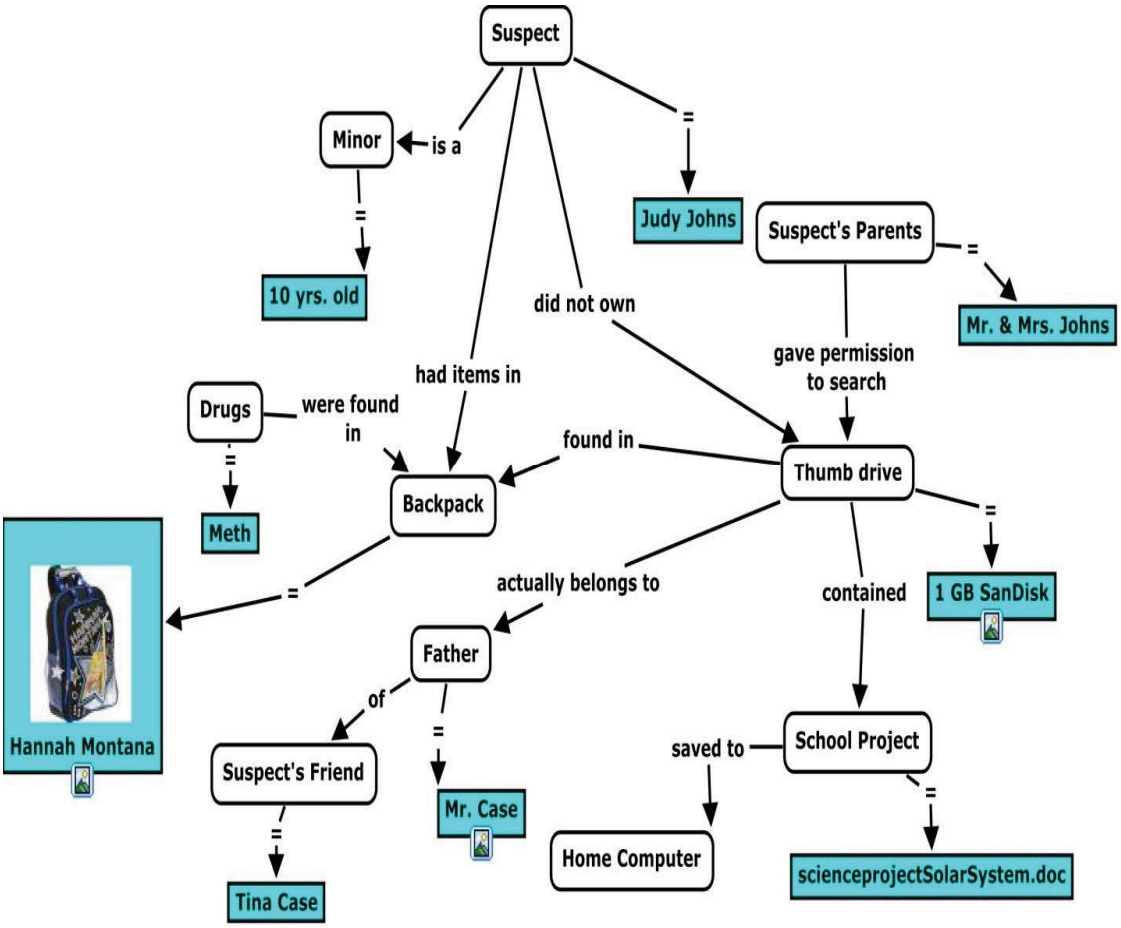


Figure 3.2 Narcotics Case Keyword Concept Map with Case Specific Details

3.2 The Keyword Concept Map

When applying the concept mapping case domain modeling approach, a list of keywords are created from the case details or case scenario. These keywords are modeled and are represented in a concept map, also known as the keyword concept map as shown in Figure 3.1. The keyword concept map is useful for defining the scope of the search during the examination. This map can also be used to search for evidence because the examiner can check off the keywords that were used to search for evidence during the

www.manaraa.com

examination. Furthermore, the graphical keyword model can also include case specific details or attributes as shown in Figure 3.2. These case specific details will also serve as keyword search terms as well. The CmapTools software enables evidence found during an investigation to be stored as an icon on the keyword concept map. The keyword concept map can provide the examiner with a quick way to view the evidence that was collected based on specific keywords or can be used to store documents associated with the case within the case concept map as well. These items can include things such as search warrants, subpoenas, reports, organizational procedures, surveillance videos, etc. and are represented as accessible items on the concepts as icons at the top of Figure 3.3.

In addition, Figure 3.3 would be useful for the investigator in the event that a case goes to trial much later. By then, the investigator may have investigated several cases and may have forgotten the details relevant to this particular case. Instead of searching for hard copies of the case details contained in a file, the investigator could access the concept map of the case and view the keywords and case information contained in the map. If case file information has been added to the map as icons, then those case files can be accessed from the concept map as well.

Additional keywords to search for can be obtained from the USDOJ tables. In Figure 3.4, a generalized USDOJ's evidence targets by case type concept map is shown. This concept map represents the crime categories and case types tables shown in Tables 3.2, 3.3, 3.4.

Each concept can be further expanded to include general and specific information relative to each case type as shown in Figure 3.5. In this figure, the evidence target

www.manaraa.com

information for the narcotics investigation case type is represented in the concept map. The narcotics keyword concept from Figure 3.4 presents general and specific concepts to show what items should be searched and identified to uncover evidence in Figure 3.5.

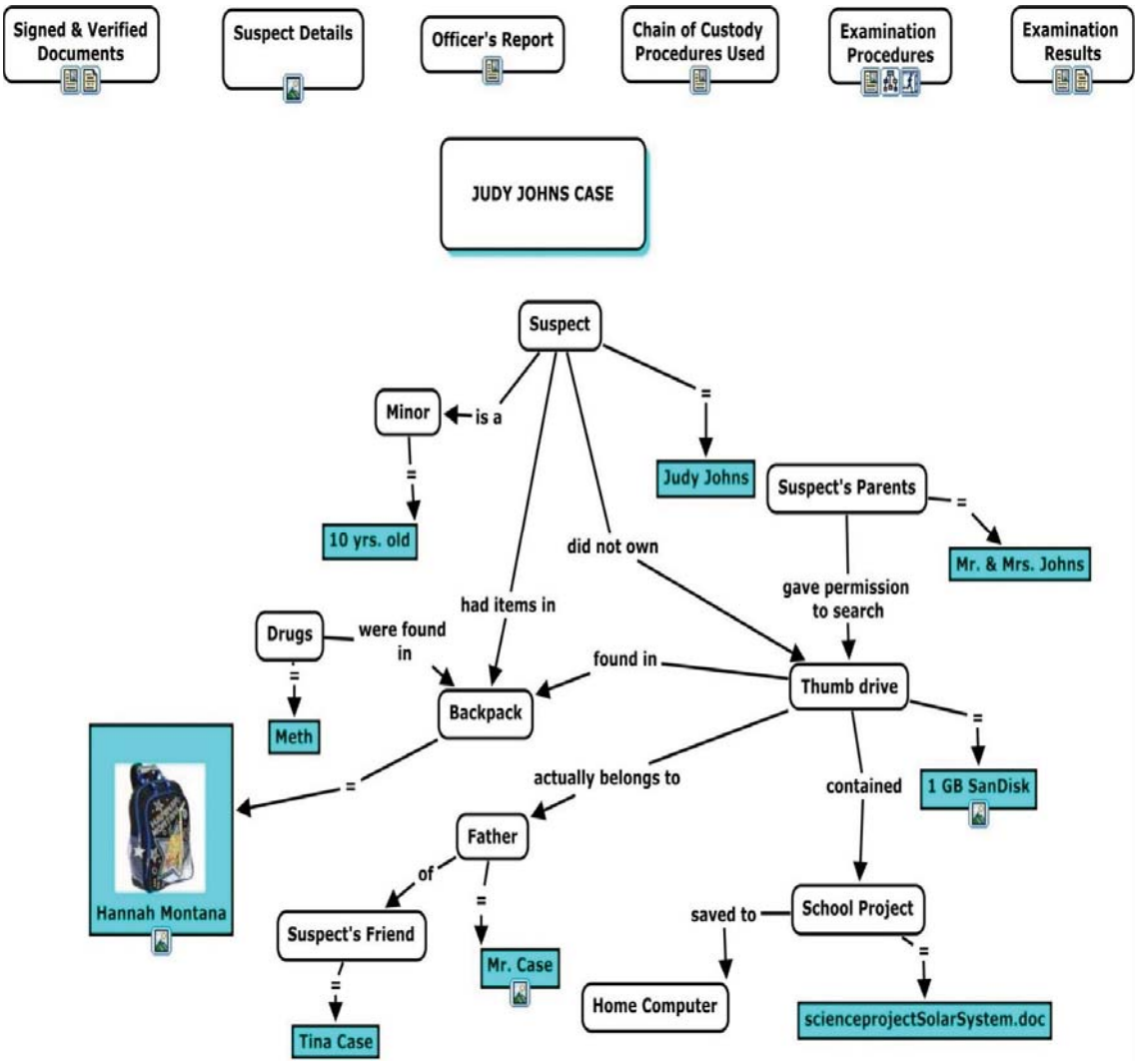


Figure 3.3 Narcotics Case Concept Map with Case Specific Information

www.manaraa.com

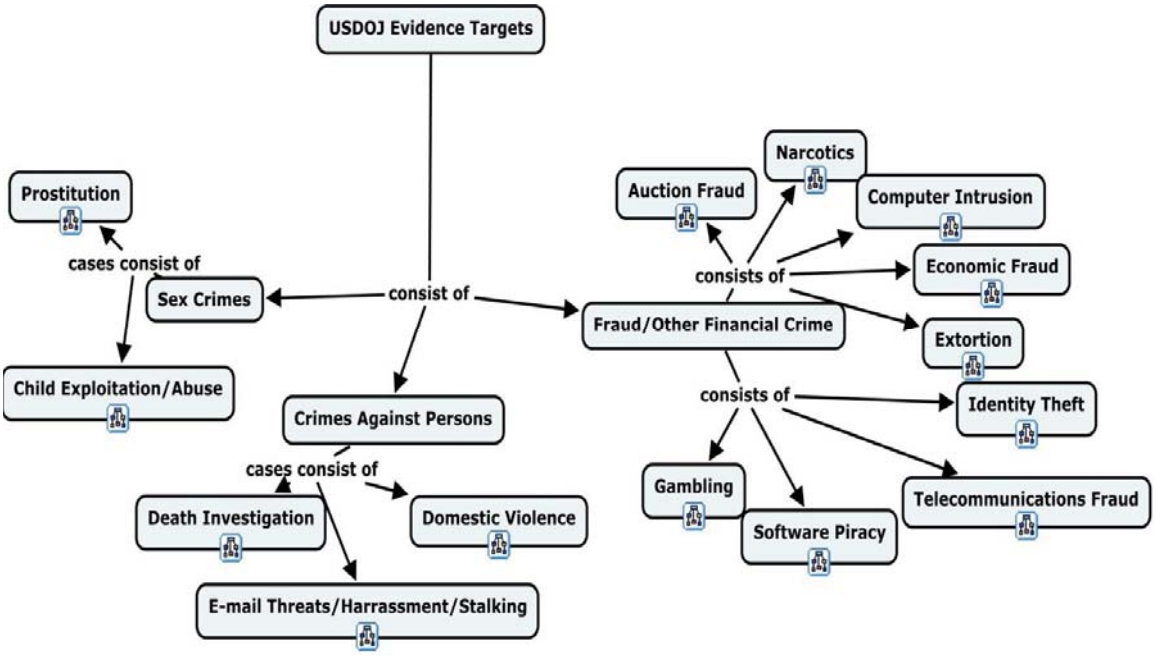


Figure 3.4 USDOJ Evidence Target Case Type Concept Map

3.3 The Examination Search Concept Map

The Examination Search concept map provides the descriptive instructions for examiners to follow to search for evidence using the relevant concepts shown in Figure 3.6. This concept map was created based on checklists and guidelines provided in [67]. The procedures are numerically labeled and can be used to guide the search and identification of evidence as well. This map would be useful for guiding the examiner during an examination and for allowing the examiner to add any special techniques he/she uses to the concept map. Special techniques suggested by the examiner could easily be added to the map and used in future examinations as well. The number of search procedures for an examination could contain more or less steps than those shown

www.manaraa.com

in Figure 3.6. Given that each case is different, a different set of tasks may be required to search for and identify evidence in an investigation as shown in Figure 3.7.

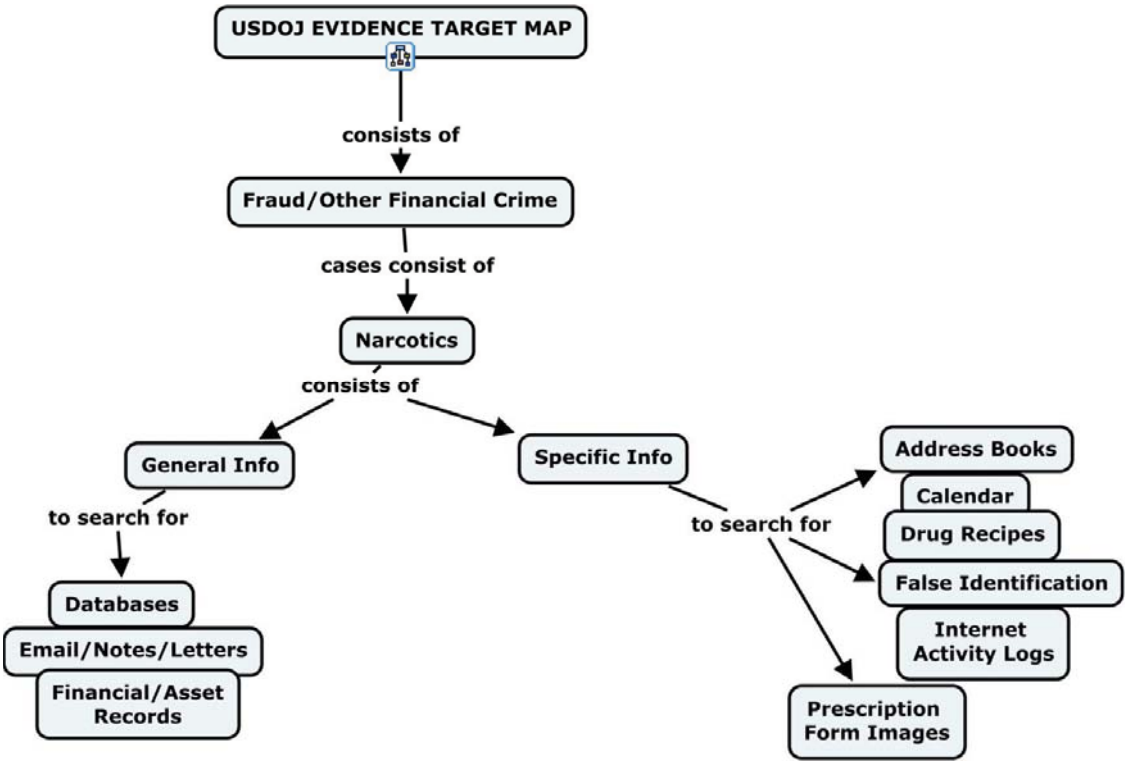


Figure 3.5 USDOJ Narcotics Keyword Concept Map

www.manaraa.com

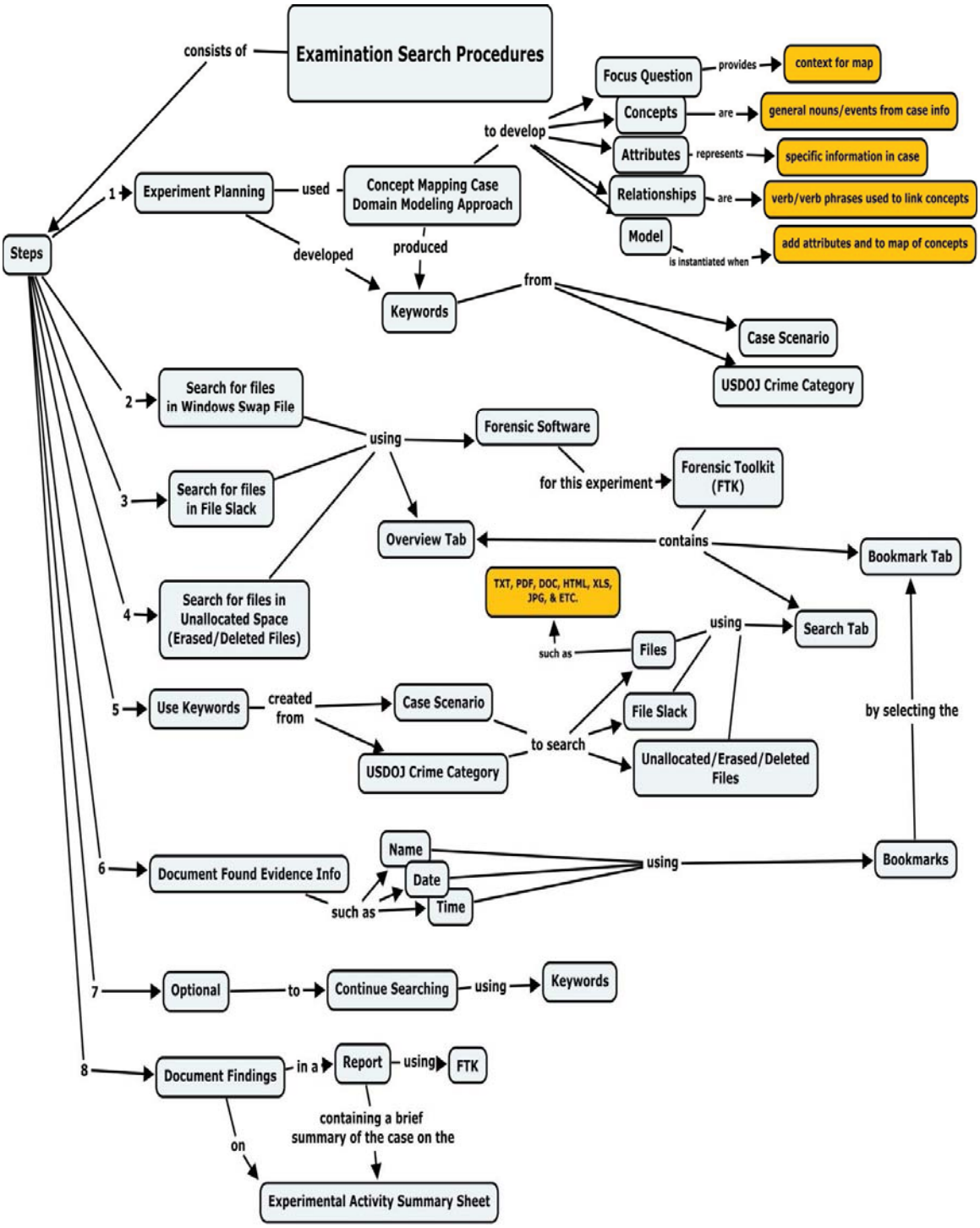


Figure 3.6 An Examination Search Concept Map for a Case Scenario

www.manaraa.com

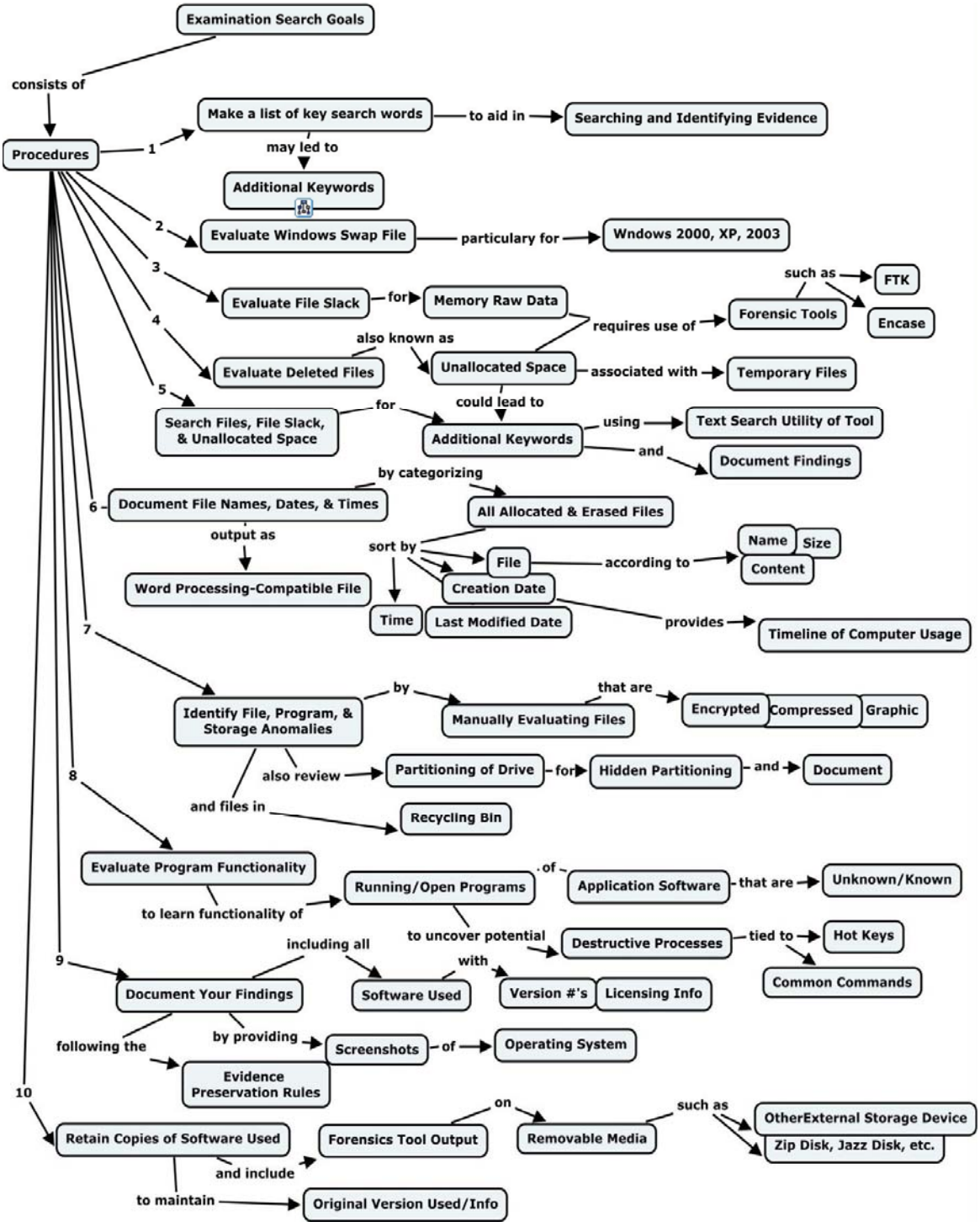


Figure 3.7 A General Examination Concept Map

www.manaraa.com

This map could easily be altered to include additional tasks as needed. To make the map less cluttered and more readable, it could be broken into two or more concept maps; for instance, one map could include tasks 1-5, and the other map could contain tasks 6-10.

3.4 Conducting the Examination

In order to conduct the examination, forensics software was used to search and identify evidence utilizing the keywords and concept maps created from the concept mapping case domain modeling approach and the examination concept map. This evidence was bookmarked and included in the final report. Computer forensic software, such as FTK and Encase, allowed the examiner to provide additional/important notes about the bookmarked evidence in addition to time and date information and the location of the evidence. For this approach, the bookmarked information was used to indicate what evidence was found and where the evidence was found. The forensic software also logged information regarding when the software was accessed, what was bookmarked, and the time the item or items were bookmarked. It also listed what keywords were searched. This log was useful for reporting what terms the examiner used for searching for the evidence and if the search led to the bookmarking of any items. In other words, it showed the success of the keyword search for uncovering evidence items. Once all the keywords had been searched and the examiner had completed his/her examination of the evidence drive, a report was generated including all of the bookmarked items created by the examiner. After the report had been created, a summary report was filled out to determine if prior questions the examiner may have had were proven to be correct. This summary included general types of evidence that were found, how the evidence related to

www.manaraa.com

the case or case scenario, and the conclusions about the case. The summary report aided in analyzing the evidence findings and was useful in presenting new information about the case that was unknown by the subject before the examination. The report could also lead to new questions and could result in a reexamination of the evidence to search for additional evidence. If this occurred, the phases of the concept mapping case domain modeling approach would need to be revisited so that one or more additional concept maps could be created or altered to aid in the new search effort.

3.5 Summary

This chapter presented the concept mapping case domain modeling approach, which was used in the experiments discussed in Chapter 4. The purpose of the concept mapping case domain modeling approach is to provide a simplified method for representing case details, for identifying relevant forensic case information from the case details, and for providing an organized, structured method for planning, examining, and analyzing a computer forensics case. Chapter 4 evaluates the concept mapping case domain modeling approach by presenting the results of four experiment trials.

www.manaraa.com

CHAPTER IV

EXPERIMENTAL DESIGN

This chapter describes how the concept mapping case domain modeling approach in Chapter III was evaluated using four experimental trials. These experimental trials required a control group and an experimental group to plan and execute the digital forensics examination. The experimental group used the concept mapping case domain modeling approach and the control group used the ad hoc approach. The groups were evaluated based on their performance with respect to the amount of evidence found and the amount of time spent in the examination. Section 4.1 presents the experimental design, Section 4.2 includes the data that was collected from each of the experimental trials, Section 4.3 presents the statistical analysis of the experiment data items, and Section 4.4 concludes this chapter with a discussion of the results.

4.1 Experimental Design

The experiment population consisted of law enforcement officers taking an investigation planning class offered through the National Forensics Training Center. They were divided into a control group and experimental group. The experimental group used the concept mapping case domain modeling approach. The control group did not

www.manaraa.com

use the concept mapping case domain modeling approach but used the generally used, ad hoc method. Each group used their respective methods to develop keywords, plan and execute the examination, and record the results. The design details of the experiment are provided in Table 4.1.

www.manaraa.com

Table 4.1 Concept Mapping Case Domain Modeling Approach Experiment Design

Experiment ID	CMCDMA_ED1
Research Questions Addressed	1. Does the concept mapping case domain modeling approach result in an increased amount of evidence found in an examination as compared to a typical approach? 2. Does the concept mapping case domain modeling approach require a significant amount of additional effort when compared to a typical approach? 3. Is the concept mapping case domain modeling approach useful for typical law enforcement investigators involved in computer forensic cases?
Hypotheses	• The experimental group will identify more evidence than the control group. • The experimental group will spend less time searching for evidence than the control group. • Overall, the experimental group will spend more time in the experiment than the control group. • The experimental group will spend less time in the examination than the control group due to a greater amount of time spent planning. • Investigators with little or no experience will identify at least the same amount of evidence as those investigators with experience. • Investigators with little or no experience will spend at least the same amount of time executing the examination as those investigators with experience.
Experimental Group	Subjects who were provided training in how to use the concept mapping case domain modeling approach to search and identify evidence and analyze the case domain.
Control Group	Subjects who were provided training in how to use a typical approach to search and identify evidence and analyze the case domain.
Independent Variable	Presence or absence of the concept mapping technique in the task of searching and identifying evidence and analyzing the case domain.
Dependent Variables	• The amount of evidence retrieved from the provided media • The amount of effort required to use the assigned technique
Confounding Variables	• The variability of subjects' forensic skills ○ This was controlled by asking subjects to voluntarily tell the number of hours of training they have had in the area of computer forensics

www.manaraa.com

Table 4.1 (continued)

Experiment Subject Population	• Members of law enforcement attending the CF 510 Seminar (Investigative and Examination Planning) offered by the National Forensics Training Center
Number of Subjects	19
Experiment Site	National Forensics Training Center (Cyber Crime Fusion Center) in Jackson, MS
Incentives	Five additional credit hours

Experiment Method	• Subjects who have volunteered to participate in the experiment and signed a consent form.
	• Subjects who have committed to participate on a specific date, time, and place.
	• Prior to the experiment, the control group and the experimental group were given an hour lecture on planning and executing a digital forensic examination.
	• Prior to the experiment, the experimental group were given an hour lecture on the concept mapping case domain modeling approach.
	• Prior to the experiment, two 30-minute exercises were given to the experimental group to supplement the understandability of the concept mapping domain modeling method and to familiarize the subjects with the concept mapping tool, CmapTools.
	• When the experiment was conducted, the control group and experimental groups were placed in the same room at the same time. They were given the following materials: a case file, an evidence thumb drive, experiment instructions, pens, pencils, and paper.
	• The participants were instructed (via the experiment instruction hand-out) to use their respective methods to analyze the case file and to find evidence on the evidence drives.
	  ○ Each group was given up to 2.5 hours to complete this task, but they were allowed to quit when they felt they had found all the evidence.
	  ○ The groups were instructed to record keywords that were used and the time the planning/execution of the events occurred. The experiment instructions provided the details about how the documentation was to be recorded.
	• At the conclusion of the experiment, each group submitted their notes and results to the principal investigator. They completed an exit survey that would evaluate the qualitative factors of their particular method of use.

www.manaraa.com

Table 4.1 (continued)

Experiment Preparations	• A case scenario, a case file, and an evidence thumb drive were developed prior to the experiment.
	  ○ Evidence pertaining to the case file and case scenario was hidden on the thumb drive. An authenticated image of the evidence thumb drive was placed on the computers.
	  ○ When recruiting subjects, the principal investigator made sure that participants in the CF 510 Seminar had not been a part of any of the previous CF 510 Seminar classes that had been held previously. Participants in the course were allowed to take the seminar class only once.
	• Instructional materials were developed for the concept mapping domain modeling approach and for the typical approach. The participants were given a training folder for use in their investigations.
	• Instructional materials were developed for directing the experimental and control groups' participation in the experiment, including instructions on how to complete the experiments.
	• CmapTools, a domain modeling concept mapping software, was installed on the experimental group's computers.
	• A qualitative exit survey was created.
	• In accordance with the Institutional Review Board for the Protection of Humans in Research (IRB), the appropriate subject consent forms were drafted and approved.
	• The forensics lab and required resources was reserved by contacting Denise Whitehead (MS Attorney General's Office Administrative Secretary).

Required Resources	• 1 USB Thumb drive (2 GB) • 15 Forensic Workstations with a Preloaded Image of the Evidence Thumb drive • 15 Forensic Workstations with Forensics Toolkit software • 8 Forensic Workstations with concept mapping domain modeling tool, CmapTools • Hard copies of all written materials: a case file, instructional materials, concept maps, and an exit survey • Digital copies of concept maps: the examination search concept map and case concept map • The Computer Forensics lab in the Cyber Crime Fusion Center

www.manaraa.com

4.1.1 The Control Group Preparation Method

This section discusses the preparation method for the control groups in the experiments. The concept mapping case domain modeling approach was the preparation method used by the experimental groups, which was discussed previously in Chapter III. The control group's preparation method consisted of the following activities:

1. Reviewing the case facts and information regarding forensics activities to follow,
2. Developing a keyword search list from the case facts,
3. Classifying the case type and evidence items to search for,
4. Developing a keyword search list from the case type and evidence items, and
5. Searching for evidence by following the forensic activities for the approach.

The goals of both the control and experimental groups were generally the same. Both groups were required to identify the significant case facts, to develop keywords from the case details, to classify case type or types, and to search for evidence using forensic procedures relative to the approach. The difference in the control and experimental groups' approaches was that the control group used an ad hoc approach, which required no step-by-step process to follow the forensic activities. For the experiment, ad hoc procedures were concisely presented to the subjects who were given a general evidence processing checklist to follow as a guide. Any additional information they wished to provide was recorded on the instruction guide.

4.1.2 Organization of the Subject Population

The experiments, case scenario, case information, and evidence drive were prepared for subjects attending the CF 510 Seminar on Investigative and Examination

www.manaraa.com

Planning. Given that this was a special class that had not been held before, none of the subjects had prior knowledge of the details of the experiments, case scenario, case information, and evidence drive. Four seminar classes were held. Within each class, four to six subjects participated in the experiments. In cases where the number of subjects was uneven, the experimental group contained one more subject than the ad hoc group.

Constraints were placed on each class participating in the experiments to make the population balanced and uniform based on their computer forensics examination expertise. A survey was given to each subject to determine their level of expertise. In order to balance the level of expertise in each group for each seminar class where subjects had 4 or more years of experience, each subject chose a piece of paper marked either " A" (ad hoc) or "E" (experimental). This helped to ensure that all of the most experienced subjects did not end up in one group. In addition, the remaining subjects also chose from a piece of paper appropriately marked "A" (ad hoc) or "E" (experimental) which determined what group each belonged to. Since each subject chose from the marked pieces of paper, this prevented the groups from being biased by the principal investigator. Figure 4.1 represents how a class of five subjects could be grouped, where two are experienced and the others have 0-4 years experience.

www.manaraa.com

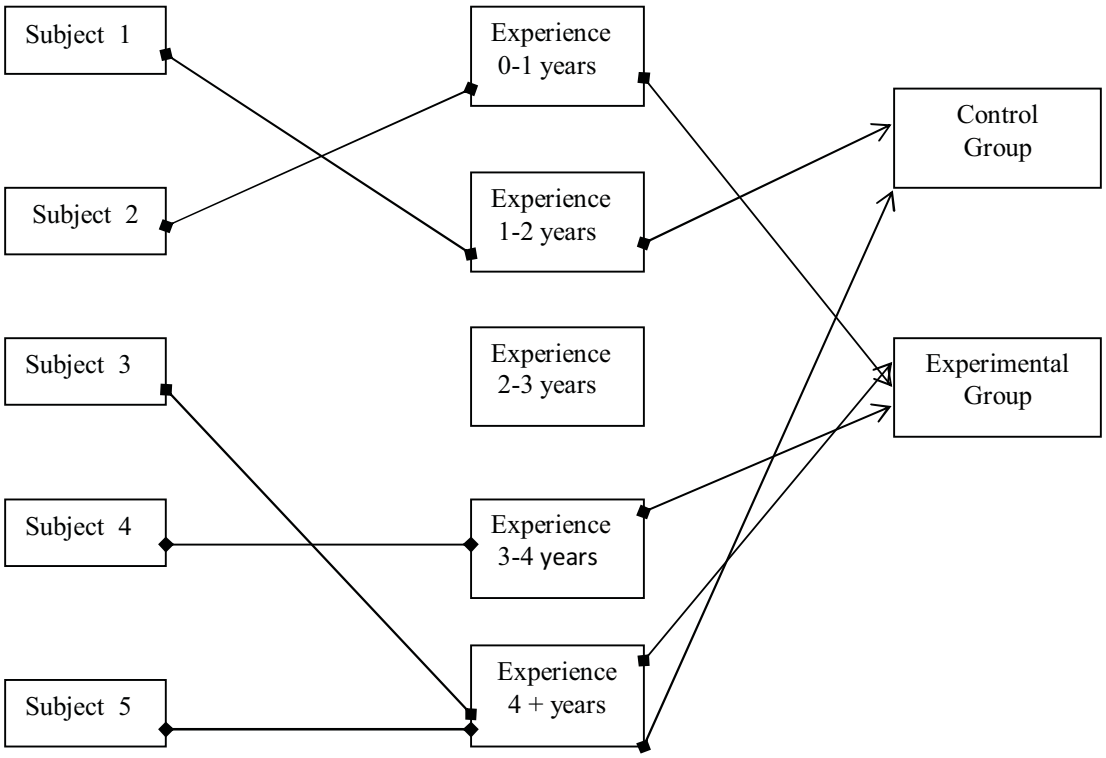


Figure 4.1 Experiment Subject Organization and Division

4.1.3 The Prepared Evidence Drive and Scenario

The principal investigator prepared all of the background information and evidence files used in the experiment and in the seminar class. As discussed previously, each subject was separated into an ad hoc group and experimental group. Each group was assigned to work on the evidence using the murder-gambling case scenario. The scenario stated that May Doe was involved in a fatal car accident that was initially labeled an accident. After further examination of the vehicle, it was found that the brakes had been tampered with. A thumb drive was also retrieved from the armrest of the vehicle at the crime scene. A more detailed description of the case was prepared and given to the subjects. The evidence drive consisted of a 2 gigabyte (GB) thumb drive that

www.manaraa.com

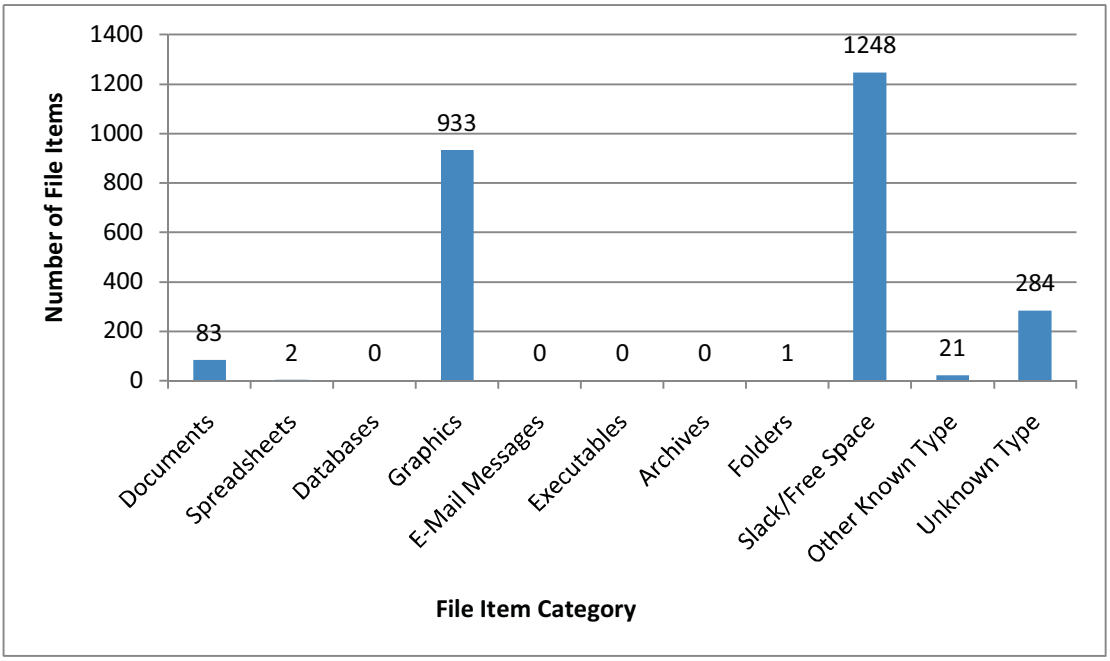


Figure 4.2 File Item Type Distribution on the Evidence Thumb Drive

contained a total of 2572 files, including 59 evidence files. Figure 4.2 provides the distribution of the file item types on the evidence drive. The ratio of the 59 evidence files to non-evidence files was 2.29% and was distributed as follows:

- 12 files contained various emails between the victim, her husband (Jim Doe), the husband's mistress (Pam Dean), and the life insurance agent,
- 11 files contained Google searches for things such as home selling tips, sleeping pills, how to get a divorce, and engagement rings,
- 12 files contained information about gambling and searches related to gambling,
- 10 files contained information regarding vehicle manuals, searches for vehicles, and brakes, and brake service information,
- 7 files contained photos of the victim's husband and mistress as well as letters shared between them,

www.manaraa.com

- 5 files contained life insurance information such as applications and searches,
- 2 files contained letters written by the victim to her husband.

4.1.4 Experiment Logistics

The facilities, software, and hardware used in the experiment belonged to and were maintained by the MSU Department of Computer Science and Engineering. The resources used in the experiment were as follows:

- one classroom,
- 6 laptops with the Forensic Toolkit software package, and
- 1 2-GB thumb drive.

4.2 Data Items Collected

The data items collected in each of the experiments were categorized according to time, performance, and as survey data. The official time was recorded from a cell phone clock; in addition, the principal investigator recorded the beginning and ending times for each subject. Prior to the experiments, each computer's clock was adjusted to match the time of the cell phone clock. The amount of time each subject spent preparing for and executing their examination represented the time data items. The amount of evidence each subject found and bookmarked in their examination represented the performance data items. This data was found in the subjects' Forensic Toolkit case file folders. A solution document was prepared prior to the examination. This document indicated where all the evidence files were located on the evidence drive. The subjects' findings

www.manaraa.com

were matched against the solution document. The survey data, which included a combination of multiple choice and short answer questions, was collected at the end of the experiment. The data items collected from this survey provided invaluable insight about the applicability, practicality, usefulness, and effectiveness of the subjects' methods. The data items collected from the four class experiments are presented in the following subsections. The time and performance data items collected in each experiment were used to answer and evaluate the research questions and hypotheses, respectively.

4.2.1 Data Items Collected: Experiments 1-4

Table 4.2 represents the data collected during the planning and examination efforts in Experiments 1-4, where time is expressed in minutes. Time data information was provided for the control group (ad hoc approach), which was reflected in the top portion of the table. The experimental group's (concept mapping case domain modeling approach) time data information was provided in the bottom portion of the table. This diagram was used for other tables in this section as well. The data represented in this table was used to answer the research question and hypotheses.

Research Question: *Does the concept mapping case domain modeling approach require a significant amount of additional effort to perform a digital forensic examination when compared to an ad hoc approach?*

The hypotheses are as follows:

- *The experimental group will spend more time in the planning phase than the control group.*

www.manaraa.com

- *The experimental group will spend less time in the examination phase than the control group.*

- *Overall, the experimental group will spend less time in the total experiment than the control group*.

To address this research question, the time/effort taken for each subject to plan, to examine the evidence, and to complete the examination was collected between each group. In addition, the amount of time taken for the subjects to plan and to execute the examination was compared between the control and experimental groups. This data was used to determine if the required planning phase in the concept mapping case domain modeling approach resulted in a smaller amount of time taken to examine the evidence when compared to the planning time of the control group. This data was used to prove or disprove the hypotheses. Effort was measured by the following:

- A greater amount of time required more effort, and

- A smaller amount of time required less effort.

Table 4.3 represents the amount of evidence, which is expressed as percentages, found by the control and experimental groups. The evidence was classified as seven groups: Emails, May, Jim, Life Insurance, Gambling, Vehicle, and Other. The group names of the evidence represent the types of evidence and the names of the victim and suspect who had files on the evidence drive. In addition, the overall or total percentage of the evidence found by each subject was provided in the last column. In addition to Table 4.2, these percentages were used to answer the following research question and hypothesis:

www.manaraa.com

Research Question: *Does the concept mapping case domain modeling approach result in an increased amount of evidence found during a digital forensic investigation?*

The hypothesis is as follows: *The experimental group will identify more evidence than the control group.*

To address this research question, the mean percentages of evidence found by each of the groups for each category and the overall mean percentages for all categories for each group was be analyzed. This data ascertained whether the use of the concept mapping case domain modeling approach resulted in a greater number of evidence items being identified by the experimental group than the control group. The data provided in Table 4.3 was used to prove or disprove the hypothesis.

www.manaraa.com

Table 4.2 Experiments 1-4 Planning and Examination Effort

Control Group	**Planning Time (minutes)**	**Examination Time (minutes)**	**Total Time (minutes)**
E1A-1	17	176	193
E1A-2	5	184	189
E2A-1	14	57	71
E2A-2	10	54	64
E3A-1	13	109	122
E3A-2	19	103	122
E4A-1	29	109	138
E4A-2	11	122	133
AVERAGE	14.75	111.75	126.50
Experimental Group			
E1E-1	10	140	150
E1E-2	44	131	175
E1E-3	30	123	153
E2E-1	13	114	127
E2E-2	40	80	120
E2E-3	40	87	127
E3E-1	27	65	92
E3E-2	38	33	71
E3E-3	5	87	92
E4E-1	7	104	111
E4E-2	55	72	127
AVERAGE	28.09	94.18	122.28

www.manaraa.com

Table 4.3 Experiments 1-4 Amount of Evidence Found Data

Control Group	% of Emails	% of May	% of Jim	% of Life Insurance	% of Gambling	% of Vehicle	% of Other	Overall %
E1A-1	58.33	50.00	57.14	100.00	50.00	70.00	54.55	62.71
E1A-2	75.00	100.00	71.43	100.00	91.67	80.00	100.00	91.53
E2A-1	58.33	100.00	14.29	100.00	91.67	80.00	100.00	74.58
E2A-2	58.33	100.00	14.29	100.00	83.33	70.00	27.27	61.02
E3A-1	91.67	100.00	71.43	100.00	66.67	70.00	72.73	77.97
E3A-2	50.00	100.00	28.57	100.00	83.33	60.00	81.82	67.80
E4A-1	25.00	0.00	14.29	0.00	8.33	30.00	0.00	13.56
E4A-2	66.67	100.00	71.43	80.00	83.33	70.00	72.73	74.58
AVERAGE	60.42	81.25	42.86	85.00	69.79	66.25	63.64	65.47
Experimental Group								
E1E-1	91.67	100.00	28.57	80.00	83.33	70.00	63.64	79.66
E1E-2	50.00	100.00	42.86	80.00	33.33	40.00	54.55	52.54
E1E-3	58.33	100.00	28.57	100.00	50.00	40.00	63.64	57.63
E2E-1	58.33	100.00	14.29	100.00	75.00	40.00	45.45	55.93
E2E-2	50.00	100.00	42.86	80.00	83.33	50.00	54.55	62.71
E2E-3	58.33	50.00	14.29	80.00	25.00	50.00	45.45	42.37
E3E-1	58.33	100.00	57.14	80.00	58.33	30.00	36.36	52.54
E3E-2	33.33	100.00	14.29	100.00	91.67	50.00	45.45	54.24
E3E-3	58.33	100.00	14.29	80.00	16.67	70.00	63.64	47.46
E4E-1	58.33	50.00	14.29	60.00	58.33	50.00	81.82	55.93
E4E-2	75.00	100.00	28.57	100.00	83.33	70.00	90.91	76.27
AVERAGE	59.09	90.91	27.28	85.46	59.85	50.91	58.68	57.94

www.manaraa.com

4.2.2 Data Items Collected: Experimental Groups

Unlike the previous sections, this section focused primarily on the data provided by the experimental groups from each of the four experiments. In this section, the focus was to determine what affect the subjects' experience with computer forensic examinations had on their abilities to use the concept mapping case domain modeling approach to plan, search, and identify evidence in the digital forensic examination. The goal was to compare the overall amount of evidence found and time spent in the phases, as well as a complete examination of those with little or no experience to those with experience. The data collected from each of the experiments for each experimental group was used to answer the research question and hypotheses.

Research Question: *Is the concept mapping case domain modeling approach useful for typical law enforcement investigators involved in computer forensic cases?*

The hypotheses are as follows:

- *Investigators with little or no experience will identify more evidence than those investigators with experience.*
- *Investigators with little or no experience will spend more time executing the examination than those investigators with experience.*

Table 4.4 provides the level of experience for subjects in the experimental groups for each of the four experiments based on the answers that the subjects provided voluntarily. At the beginning of the seminar course, the subjects were asked to rate their level of expertise with respect to computer forensic examinations. The experience levels were as follows:

- No Experience (0-1 years) consists of knowledge of the computer forensic investigation process.

www.manaraa.com

- Little Experience (1-2 years) which consists of the previous experience level and attended seminars/courses/workshops in computer forensics.

- Some Experience (2-3 years) consists of the previous experience levels, securing the computer/digital evidence, and notifying forensics lab, knowledge of computer forensic software and hardware.

- More experience (3-4 years) consists of the previous experience levels, used digital forensic software and hardware tools to authenticate or copy evidence in an actual digital forensic investigation.

- Expert/Experienced (4-5+ years) consists of the previous experience levels, performed digital forensic examinations, created reports using digital forensics software.

Table 4.4 Experience Level of Subjects in Experimental Groups for Experiments 1-4

Experiment	No Experience (0-1 years)	Little Experience (1-2 years)	Some Experience (2-3 years)	More Experience (3-4 years)	Expert/ Experienced (4-5+ years)
Experiment 1					
E1E-1			X		
E1E-2					X
E1E-3			X		
Experiment 2					
E2E-1			X		
E2E-2				X	
E2E-3					X
Experiment 3					
E3E-1			X		
E3E-2		X			
E3E-3		X			
Experiment 4					
E4E-1		X			
E4E-2		X			

www.manaraa.com

Similar to the previous subsection, the planning and examination time data and amount of evidence data provided by the experimental groups from the experiments was be combined into one table as shown in Table 4.5.

Table 4.5 represents the data collected during the planning and examination efforts in Experiments 1-4, where time is expressed in minutes. Time data information was provided for each subject in the experimental groups (concept mapping case domain modeling approach) for each experiment. In this research, subjects with little or no experience had 0-2 years experience in computer forensic examinations; in addition, those subjects with more than 2 years experience in computer forensics examinations were considered experienced.

Table 4.5 Planning and Examination Effort for Experimental Groups in Experiments 1-4

Little or No Experience	**Planning Time (minutes)**	**Examination Time (minutes)**	**Total Time (minutes)**
E3E-2	38	33	71
E3E-3	5	87	92
E4E-1	7	104	111
E4E-2	55	72	127
AVERAGE	26.25	74.00	100.25
Experience			
E1E-1	10	140	150
E1E-2	44	131	175
E1E-3	30	123	153
E2E-1	13	114	127
E2E-2	40	80	120
E2E-3	40	87	127
E3E-1	27	65	92
AVERAGE	29.14	105.71	134.86

www.manaraa.com

Table 4.6 Amount of Evidence Found in Experiments 1-4 by Experimental Groups

Little or No Experience	% of Emails	% of May	% of Jim	% of Life Insurance	% of Gambling	% of Vehicle	% of Other	Overall %
E3E-2	33.33	100.00	14.29	100.00	91.67	50.00	45.45	54.24
E3E-3	58.33	100.00	14.29	80.00	16.67	70.00	63.64	47.46
E4E-1	58.33	50.00	14.29	60.00	58.33	50.00	81.82	55.93
E4E-2	75.00	100.00	28.57	100.00	83.33	70.00	90.91	76.27
AVERAGE	56.25	87.50	17.86	85.00	62.50	60.00	70.46	58.48
Experience								
E1E-1	91.67	100.00	28.57	80.00	83.33	70.00	63.64	79.66
E1E-2	50.00	100.00	42.86	80.00	33.33	40.00	54.55	52.54
E1E-3	58.33	100.00	28.57	100.00	50.00	40.00	63.64	57.63
E2E-1	58.33	100.00	14.29	100.00	75.00	40.00	45.45	55.93
E2E-2	50.00	100.00	42.86	80.00	83.33	50.00	54.55	62.71
E2E-3	58.33	50.00	14.29	80.00	25.00	50.00	45.45	42.37
E3E-1	58.33	100.00	57.14	80.00	58.33	30.00	36.36	52.54
AVERAGE	60.71	92.86	32.66	85.71	58.33	45.71	51.95	57.63

Table 4.6 represents the amount of evidence, which is expressed as percentages, found by each subject in the experimental groups in each experiment. The evidence was classified into seven groups: Emails, May, Jim, Life Insurance, Gambling, Vehicle, and Other. The group names of the evidence represented the types of evidence and the names of the victim and suspect who had files on the evidence drive. In addition, the overall or total percentage of the evidence found by each subject and each group were provided in

www.manaraa.com

the last column. The data items collected in this experiment were be used to address the research questions and hypotheses provided in this subsection.

Table 4.7 presents the post-experiment multiple-choice survey questions for the experimental group. The responses for the little or no experience and experienced group were also provided. Table 4.8 provides the multiple-choice survey responses given by the LNE and E groups.

Table 4.7 Experimental Group Post-Experiment Survey Questions

Q1	Do you think the concept mapping model contributed to a clear and complete understanding of the case and examination tasks? a. I think the model contributed to confusion regarding the case concepts and case facts and examination tasks b. I think the model was not helpful for understanding the case concepts and examination tasks c. The model was somewhat helpful for understanding the case concepts and examination tasks d. The model was helpful in understanding the case concepts and examination tasks e. The model was very helpful in understanding the case concepts and examination tasks
Q2	Rate how difficult the approach was to understand? a. The approach was not difficult to understand. b. The approach was slightly difficult to understand. c. The approach was moderately difficult to understand. d. The approach was very difficult to understand. e. The approach was extremely difficult to understand.
Q3	Rate your understanding of the content and purpose of the concept mapping case domain modeling approach for use during an examination. a. The content and purpose of the approach was extremely difficult understand. b. The content and purpose of the approach was very difficult to understand.

www.manaraa.com

Table 4.7 (continued)

	c. The content and purpose of the approach was moderately difficult to understand. d. The content and purpose of the approach was slightly difficult to understand. e. The content and purpose of the approach was not difficult to understand.
Q4	Rate your confidence in your ability and potential to learn how to effectively build a concept mapping model from scratch during an examination. a. I am extremely not confident in my ability to learn to build a model from scratch. b. I am not confident in my ability to learn to build a model from scratch. c. I am not confident or confident in my ability to build a model from scratch. d. I am confident in my ability to learn to build a model from scratch. e. I am extremely confident in my ability to learn to build a model from scratch.
Q5	Rate your confidence level in applying the concept mapping case domain model approach during a computer forensics examination. a. I am extremely not confident in my ability to apply the approach during an examination. b. I am not confident in my ability apply the approach during an examination. c. I am not confident or confident in my ability to apply the approach during an examination. d. I am confident in my ability to learn to apply the approach during an examination. e. I am extremely confident in my ability to apply the approach during an examination.
Q6	How difficult was it to follow the Examination Search Procedures concept map to search and identify evidence? a. The concept map was not difficult to follow. b. The concept map was slightly difficult to follow. c. The concept map was moderately difficult to follow. d. The concept map was very difficult to follow. e. The concept map was extremely difficult to follow.
Q7	How likely would you be to use this approach for forensic investigations? a. I am extremely likely to use this approach in forensic investigations. b. I am likely to use this approach in forensic investigations. c. I am neither likely nor unlikely to use this approach in forensic investigations. d. I am unlikely to use this approach in forensic investigations. e. I am extremely unlikely to use this approach in forensic investigations.

www.manaraa.com

Table 4.8 LNE and E Group Post-Experiment Multiple Choice Survey Responses

LNE Group	Q1	Q2	Q3	Q4	Q5	Q6	Q7
LNE1	4	2	4	4	4	3	4
LNE2	3	2	3	3	3	3	2
LNE3	3	3	3	3	3	3	2
LNE4	3	4	5	5	2	2	4
MEDIAN	3	3.5	3.5	3.5	3	3	3
E Group							
E1	4	2	3	3	4	2	4
E2	5	1	5	5	5	2	5
E3	5	1	5	5	5	2	4
E4	4	2	2	2	2	3	4
E5	3	1	5	5	5	2	3
E6	5	2	4	4	4	2	5
E7	4	2	4	4	4	3	4
MEDIAN	4	2	4	4	4	2	4

Numerical identifiers (1-5) were used in the place of the alphabetic multiple choice identifiers (a-e) in Table 4.8. Table 4.9 presents the post-experiment discussion survey questions for the experimental group. The experimental group was given survey questions in an effort to obtain both qualitative and quantitative data about the concept mapping case domain modeling approach. Although the responses for the discussion questions have been omitted, the analysis sections include insightful discussion responses given by the group.

To further evaluate this research question, an Internet Crimes Against Children (ICAC) investigator and three computer forensic examiners from the Mississippi Attorney General's Office were given a lecture and demonstration of the concept mapping case domain modeling approach. At the end of the demonstration, the investigator and examiners participated in a discussion survey, similar to Table 4.9, to

www.manaraa.com

evaluate the concept mapping case domain modeling approach. The multiple-choice questions and responses are given in Tables 4.10 and 4.11, respectively.

Table 4.9 Experimental Group Post-Experiment Survey Discussion Questions

Q1	Do you think the approach would be useful for analyzing the case details of a forensic examination? Explain.
Q2	Did you find it difficult to use the approach for this activity? Explain.
Q3	Do you think the concept map diagrams would be helpful visual aids for presenting computer forensics findings to a jury? Explain.
Q4	Do you think the modeling approach would be useful for training law enforcement about computer forensics procedures? Explain.
Q5	Describe any strengths of the concept mapping case domain model? Explain.
Q6	Describe any weaknesses of the concept mapping case domain model? Explain.

www.manaraa.com

Table 4.10 ICAC Investigator and Computer Forensic Examiner Survey Questions

Q1	How difficult was the approach was to understand? a. The approach was not difficult to understand. b. The approach was slightly difficult to understand. c. The approach was moderately difficult to understand. d. The approach was very difficult to understand. e. The approach was extremely difficult to understand.
Q2	How well did you understand the content and purpose of the concept mapping case domain modeling approach for use during an examination? a. The content and purpose of the approach was extremely difficult to understand. b. The content and purpose of the approach was very difficult to understand. c. The content and purpose of the approach was moderately difficult to understand. d. The content and purpose of the approach was slightly difficult to understand. e. The content and purpose of the approach was not difficult to understand.
Q3	Rate your confidence in your ability and potential to learn how to effectively build a concept mapping model from scratch during an examination. a. I am extremely not confident in my ability to learn to build a model from scratch. b. I am not confident in my ability to learn to build a model from scratch. c. I am neither confident nor not confident in my ability to build a model from scratch. d. I am confident in my ability to learn to build a model from scratch. e. I am extremely confident in my ability to learn to build a model from scratch.
Q4	Rate your confidence level in applying the concept mapping case domain model approach during/after an ICAC investigation/computer forensics examination. a. I am extremely not confident in my ability to apply the approach during an examination. b. I am not confident in my ability apply the approach during an examination. c. I am not confident or not confident in my ability to apply the approach during an examination. d. I am confident in my ability to learn to apply the approach during an examination. e. I am extremely confident in my ability to apply the approach during an examination.
Q5	How likely would you be to use this approach for ICAC/computer forensic investigations? a. I am extremely likely to use this approach in forensic investigations. b. I am likely to use this approach in forensic investigations. c. I am neither likely nor unlikely likely to use this approach in forensic investigations. d. I am unlikely to use this approach in forensic investigations. e. I am extremely unlikely to use this approach in forensic investigations.

www.manaraa.com

Table 4.11 ICAC Investigator and Computer Forensic Examiner Survey Responses

Question	Q1	Q2	Q3	Q4	Q5
AGO-1	2	4	5	4	4
AGO-2	2	5	5	4	3
AGO-3	2	4	5	5	2
AGO-4	2	2	4	4	4
MEDIAN	2	4	5	4	3.5

Survey discussion questions, similar to those in Table 4.8, were also given to the investigators and examiners. The questions and responses were not provided; however, the analysis sections includes their discussion responses.

4.3 Statistical Analysis Methods for Experiments

The chosen method of statistical analysis for testing the hypotheses in the experiment data was the independent, one-sided t-test. The t-test was used to compare the differences or means of the two independent groups. Furthermore, t-tests were used to show if the mean of one population is significantly different or greater than the mean of another population; a confidence interval of 95% means that there was only a 5% chance that the difference between the groups was caused by chance. The null hypothesis assumed that the experimental manipulation had no effect on the subjects; therefore, the control and experimental groups' data should be very similar. However, if a difference was observed, then one could infer that the difference between the two groups was a result of the experimental manipulation. For instance, if the probability

www.manaraa.com

value, p, was less than or equal to the significance level of 5% or .05, then the null hypothesis was rejected and the alternative hypothesis was accepted and the difference was recognized as a statistically significant; however, if the probability value, p, was greater than the significance level of 5% or .05, then the null hypothesis was accepted and the alternative hypothesis was rejected.

T-tests require that four criteria are met before it can be used, and they are as follows: 1) data should be measured at least at the interval level, 2) the data should be independent, 3) the data should be normally distributed, and 4) the variances should be the same or equal for the group. Criteria 1 was satisfied because all the data is measured using interval and numerical scales. Criteria 2 was satisfied because the performance of one subject was not influenced by another subject, which in turn did not affect the data. Criteria 3 and 4 were tested using the data obtained from the experiments. The Shapiro-Wilk (S-W) test was used to determine if the data was normally distributed. The S-W test is a nonparametric test that yields exact significance values and determines whether data is normally distributed. If the significance value, p, was less than or equal to .05, then the data was not normally distributed and violated the normality criteria of the t-test. Levene's test was used to test the homogeneity of variances or if the variances of the two groups were equal. If the p-value was less than or equal to .05, then the variances were significantly different; otherwise, the homogeneity of variances assumption had been verified.

When the t-test's criteria were not met, the non-parametric Kolmogorov-Smirnov (K-S) test was used to evaluate the difference between the means of the two groups.

www.manaraa.com

Unlike the independent t-test, the K-S test does not make assumptions about the distribution and variance of equality of the data. Instead, the ranks, not raw values, are used to calculate the statistical differences. The K-S test is a non-parametric test that determines if the differences in means are statistically different from the normal distribution. Although the Mann-Whitney test is the equivalent of the independent t-test, the K-S and Mann-Whitney tests are very similar in that both test whether two groups have been drawn from the same population. The Mann-Whitney tests works better with large group sizes, and the K-S test has better statistical power when the group sizes are less than 25, which is true for this case. Parametric tests, such as the independent t-test, are preferred to non-parametric because these tests can evaluate whether the mean of a population is statistically greater than the mean of another population, whereas the non-parametric test only evaluates whether there is a significant difference, but not if this significance is greater.

The results of the statistical tests for experiments 1-4 are presented in subsections 4.3.1-4.3.2. The research questions and hypotheses served as the alternative hypotheses for the t-tests. Each of the alternative hypotheses was evaluated based on the 95% confidence interval. The alternative hypotheses were accepted and recognized as having a statistically significant difference when the probability of the null hypothesis was less than or equal to 5% or .05. Otherwise the alternative hypotheses were rejected.

www.manaraa.com

4.3.1 Statistical Analysis of Experiment Data

Instead of analyzing the data for each individual experiment, the data for experiments 1-4 was combined and analyzed according to the groups. For instance, the control group had a total of eight subjects and the experimental group had a total of eleven subjects. The results of the normality and homogeneity of variance tests that determined t-test statistical comparison eligibility for each pair of data items from the experiments are provided in Table 4.12.

The results of the t-tests and K-S tests were appropriately applied to the effort/time data, expressed in minutes, for both the control and experimental groups as shown in Table 4.13. If t-tests were used to evaluate the data, then the field for t-values contained a value for the test; otherwise, the K-S tests were used and the fields were marked with "- -." The results of the statistical tests showed that no significant difference in effort was observed between the control and experimental groups. However, the results also showed that those subjects using the concept mapping case domain modeling approach (experimental group) spent less time in the examination phase and total experimental exercise than the control group. This decrease in examination time could have been a result of the greater amount of time spent in the planning phase by the experimental group.

www.manaraa.com

Table 4.12 t-test Eligibility for Experiment Data Items

Data Item	Shapiro-Wilk Normality Test, p	Normal?	Levene's Test for Equality of Variances	Variance Equal?	t-test Used?
% Emails Control Group	.698	Yes	.469	Yes	No
% Emails Exp. Group	.049	No			
% May Files Control Group	.000	No	.115	Yes	No
% May Files Exp. Group	.000	No			
% Jim Files Control Group	.017	No	.002	No	No
% Jim Files Exp. Group	.023	No			
% Life Insurance Con. Grp	.000	No	.153	Yes	No
% Life Insurance Exp. Grp	.008	No			
% Gambling Control Group	.017	No	.971	Yes	No
% Gambling Exp. Group	.249	Yes			
% Vehicles Control Group	.008	No	.963	Yes	No
% Vehicles Exp. Group	.077	Yes			
% Other Control Group	.332	Yes	.046	No	No
% Other Exp. Group	.340	Yes			
% Overall Control Group	.038	No	.257	Yes	No
% Overall Exp. Group	.151	Yes			
Planning Time Control Grp	.653	Yes	.011	No	No
Planning Time Exp. Group	.336	Yes			
Examination Time Con. Grp	.492	Yes	.356	Yes	Yes
Examination Time Exp. Grp	.903	Yes			
Total Time Control Group	.392	Yes	.249	Yes	Yes
Total Time Exp. Group	.911	Yes			

www.manaraa.com

Table 4.13 Statistical Results of Experiment Effort/Time Data

Hypothesis	Control Mean ($\bar{x}$)	Experimental Mean ($\bar{y}$)	t	p	Result
h_1	$\bar{x}$ = 14.75	$\bar{y}$ = 28.09	- -	0.127	Reject h_1
h_2	$\bar{x}$ = 111.75	$\bar{y}$ = 94.18	0.921	0.185	Reject h_2
h_3	$\bar{x}$ = 126.50	$\bar{y}$ = 122.27	0.227	0.412	Reject h_3
Hypothesis Legend					
h_1 = The experimental group spent a significantly different amount of time in the planning phase/session than the control group.					
h_2 = The experimental group spent a significantly less amount of time in the examination phase/session than the control group.					
h_3 = The experimental group spent a significantly less amount of time on the total experimental exercise than the control group.					

Table 4.14 provides the results of the K-S tests that evaluated whether the amount of evidence found by the control and experimental groups were statistically significant. The amount of evidence found data is expressed in percentages. The statistical tests did not reveal any significant differences between the amount of data found between the control and experimental groups. However, the experimental group's mean was somewhat higher for evidence related to May files and Life Insurance files than the control group.

4.3.2 Statistical Analysis of Experimental Group Data Based on Experience Level

The data for these statistical analysis tests were taken from the experimental groups of the four experiments. The experimental group data was grouped into two categories: Little or No Experience (LNE) and Experienced (E). The LNE group consisted of four subjects and the E group consisted of seven subjects. The results of the

www.manaraa.com

normality and homogeneity of variance tests that determined t-test statistical comparison eligibility for each pair of data items from the experiments are provided in Table 4.15.

The results of the *t*-tests and K-S tests were appropriately applied to the effort/time data, expressed in minutes, for both the LNE and E groups as shown in Table 4.16. If t-tests were used to evaluate the data, then the field for t-values contained a value for the test; otherwise, the K-S tests were used and the fields were marked with "- -." Based on the results of the statistical tests, the concept mapping case domain modeling approach resulted in the LNE group spending a significantly less amount of time in the total experimental activity than the E group. Although no significant difference was observed during the planning and examination phases, the LNE group did spend less time in the planning and examination phases than the E group.

Table 4.17 provides the results of the *t*-tests and K-S tests that evaluated whether the amount of evidence found by the LNE and E groups were statistically significant. The amount of evidence found data is expressed in percentages. Based on the statistical tests, the LNE group found a significantly greater amount of evidence containing Other files than the E group. Although no other significant differences were found between the groups, the LNE group's mean amount of evidence found was slightly higher for Gambling files, Vehicle files, and total overall evidence.

www.manaraa.com

Table 4.14 Statistical Results of Experiment Percent of Evidence Found Data

Hypothesis	Control Mean ($\bar{x}$)	Experimental Mean ($\bar{y}$)	t	p	Result
h_4	$\bar{x}$ = 60.42	$\bar{y}$ = 59.09	- -	0.995	Reject h_4
h_5	$\bar{x}$ = 81.25	$\bar{y}$ = 90.91	- -	1.000	Reject h_5
h_6	$\bar{x}$ = 42.86	$\bar{y}$ = 27.28	- -	0.420	Reject h_6
h_7	$\bar{x}$ = 85.00	$\bar{y}$ = 85.46	- -	0.494	Reject h_7
h_8	$\bar{x}$ = 69.79	$\bar{y}$ = 59.85	- -	0.814	Reject h_8
h_9	$\bar{x}$ = 66.25	$\bar{y}$ = 50.91	- -	0.069	Reject h_9
h_{10}	$\bar{x}$ = 63.64	$\bar{y}$ = 58.68	- -	0.323	Reject h_{10}
h_{11}	$\bar{x}$ = 65.47	$\bar{y}$ = 57.94	- -	0.069	Reject h_{11}

Hypothesis Legend
h_4 = The experimental group found a significantly different amount of evidence files containing Emails than the control group.
h_5 = The experimental group found a significantly different amount of evidence containing May files than the control group.
h_6 = The experimental group found a significantly different amount of evidence containing Jim files than the control group.
h_7 = The experimental group found a significantly different amount of evidence containing Life Insurance files than the control group.
h_8 = The experimental group found a significantly different amount of evidence containing Gambling files than the control group.
h_9= The experimental group found a significantly different amount of evidence containing Vehicle files than the control group.
h_{10} = The experimental group found a significantly different amount of evidence containing Other files than the control group.
h_{11} = The experimental group found a significantly different amount of overall evidence than the control group.

www.manaraa.com

Table 4.15 t-test Eligibility for Experimental Group Data based on Experience Level

Data Item	Shapiro-Wilk (S-W) Normality Test, p	Normal?	Levene's Test for Equality of Variances	Variance Equal?	t-test Used?
% Emails LNE Group	.572	Yes	.705	Yes	No
% Emails E Group	.002	No			
% May Files LNE Group	.001	No	.108	Yes	No
% May Files E Group	.000	No			
% Jim Files LNE Group	.001	No	.451	Yes	No
% Jim Files E Group	.482	Yes			
% Life Insurance LNE Grp	.272	Yes	.094	Yes	No
% Life Insurance E Group	.000	No			
% Gambling LNE Group	.493	Yes	.507	Yes	Yes
% Gambling E Group	.385	Yes			
% Vehicles LNE Group	.024	No	.880	Yes	No
% Vehicles E Group	.263	Yes			
% Other LNE Group	.798	Yes	.080	Yes	Yes
% Other E Group	.482	Yes			
% Overall LNE Group	.306	Yes	.816	Yes	Yes
% Overall E Group	.433	Yes			
Planning Time LNE Group	.314	Yes	.056	Yes	Yes
Planning Time E Group	.297	Yes			
Examination Time LNE Grp	.749	Yes	.744	Yes	Yes
Examination Time E Group	.574	Yes			
Total Time LNE Group	.949	Yes	.797	Yes	Yes
Total Time E Group	.898	Yes			

www.manaraa.com

Table 4.16 Statistical Results for Effort Based on Experimental Group Experience Level

Hypothesis	Little or No Experience Mean ($\bar{x}$)	Experienced Mean ($\bar{y}$)	t	p	Result
h_{e1}	$\bar{x}$ = 26.25	$\bar{y}$ = 29.14	-0.258	0.401	Reject h_1
h_{e2}	$\bar{x}$ = 74.00	$\bar{y}$ = 105.71	-1.741	0.058	Reject h_2
h_{e3}	$\bar{x}$ = 100.25	$\bar{y}$ = 134.86	-2.120	0.032	Accept h_3
Hypothesis Legend					
h_{e1} = The group having little or no experience spent a significantly less amount of time in the planning phase/session than the experienced group.					
h_{e2} = The group having little or no experience spent a significantly less amount of time in the examination phase/session than the experienced group.					
h_{e3} = The group having little or no experience spent a significantly less amount of time on the total experimental activity than the experienced group.					

Basic frequency distribution statistics for the experimental group's post-experiment survey data are provided in Tables 4.18-4.24. The response distribution to survey question 1 is given in Table 4.18 and was based on the responses of the LNE and E groups. Question 1 reads as follows: Do you think the concept mapping model contributed to a clear and complete understanding of the case and examination tasks? All the subjects from both groups indicated that the model was helpful in understanding the case concepts and examination tasks. Six out of seven subjects in the E Group indicated that the model was helpful or very helpful in understanding the case concepts and examination tasks. Although no subjects in the LNE Group felt that the model was very helpful, they did find slightly more evidence than the E Group.

Table 4.19 provides the distribution responses to question 2, which reads as follows: Rate how difficult the approach was to understand? Although the subjects in

www.manaraa.com

Table 4.17 Statistical Results for Amount of Data Found Based on Experience Level

Hypothesis	Little or No Experience Mean ($\bar{x}$)	Experienced Mean ($\bar{y}$)	t	p	Result
h_{e4}	$\bar{x} = 56.25$	$\bar{y} = 60.73$	- -	0.997	Reject h_4
h_{e5}	$\bar{x} = 17.86$	$\bar{y} = 32.66$	- -	1.000	Reject h_5
h_{e6}	$\bar{x} = 87.50$	$\bar{y} = 92.86$	- -	0.643	Reject h_6
h_{e7}	$\bar{x} = 85.00$	$\bar{y} = 85.71$	- -	0.997	Reject h_7
h_{e8}	$\bar{x} = 62.50$	$\bar{y} = 58.33$	0.243	0.407	Reject h_8
h_{e9}	$\bar{x} = 60.00$	$\bar{y} = 45.71$	- -	0.377	Reject h_9
h_{e10}	$\bar{x} = 70.46$	$\bar{y} = 51.95$	2.069	0.035	Accept h_{10}
h_{e11}	$\bar{x} = 58.48$	$\bar{y} = 57.62$	0.946	0.179	Reject h_{11}

Hypothesis Legend
h_{e4} = The group with little or no experience found a significantly different amount of evidence files containing Emails than the experienced group.
h_{e5} = The group with little or no experience found a significantly different amount of evidence containing May files than the experienced group.
h_{e6} = The group with little or no experience found a significantly different amount of evidence containing Jim files than the experienced group.
h_{e7} = The group with little or no experience found a significantly different amount of evidence containing Life Insurance files than the experienced group.
h_{e8} = The group with little or no experience found a significantly greater amount of evidence containing Gambling files than the experienced group.
h_{e9}= The group with little or no experience found a significantly different amount of evidence containing Vehicle files than the experienced group.
h_{e10} = The group with little or no experience found a significantly greater amount of evidence containing Other files than the experienced group.
h_{e11} = The group with little or no experience found a significantly greater amount of overall evidence than the experienced group.

www.manaraa.com

the LNE Group indicated that they had some difficulty with understanding the approach, their mean planning and examination times were less than the E Group, and they found slightly more evidence as well. Although 57.14% of the E Group experienced difficulty with understanding the approach, 42.86% felt that the approach was not difficult to understand.

In survey question 3, the subjects were asked to rate their understanding of the content and purpose of the concept mapping case domain modeling approach for use

Table 4.18 Experiment Post-Survey Response Distribution for Q1

Q1: Do you think the concept mapping model contributed to a clear and complete understanding of the case and examination tasks?		
Option	LNE Group Distribution Frequency/Percent	E Group Distribution Frequency/Percent
1. I think the model contributed to confusion regarding the case concepts and examination tasks	0 / 0%	0 / 0%
2. I think the model was not helpful for understanding the case concepts and examination tasks	0 / 0%	0 / 0%
3. The model was somewhat helpful for understanding the case concepts and examination tasks	3 / 75.00%	1 / 14.29%
4. The model was helpful in understanding the case concepts and examination tasks	1 / 25.00%	3 / 42.86%
5. The model was very helpful in understanding the case concepts and examination tasks	0 / 0%	3 / 42.86%
Experiment Reference Data: LNE/E Group Mean Planning Time = 26.25 min. / 29.14 min. LNE/E Group Mean Examination Time = 74.00 min. / 105.71 min. LNE/E Group Mean % of Overall Evidence Found = 58.48% / 57.63%		

www.manaraa.com

during an examination. The distributions for their responses are shown in Table 4.20. Although both groups experienced difficulty in understanding the content and purpose of the approach, none of the subjects experienced extreme difficulty. Fifty percent of the LNE subjects and 71 % of the E subjects felt that the content and purpose of the approach was not difficult or slightly difficult to understand.

Table 4.21 presents the response distribution for survey question 4, which states the following: Rate your confidence in your ability and potential to learn how to effectively build a concept mapping model from scratch during an examination. Although 50% of the subjects in the LNE Group were unsure of their abilities to build a model from scratch, none of the subjects indicated that they were not confident in their abilities to build a model. Five of the seven E Group subjects indicated that they were confident or extremely confident in their abilities to build a model from scratch.

Table 4.22 contains the responses to post-survey question 5, which states the following: Rate your confidence level in applying the concept mapping case domain model approach during a computer forensics examination. Six of the seven E Group subjects were confident or extremely confident in their abilities to apply the approach. Although 75 % of the subjects in the LNE Group indicated that they were not confident or unsure in their ability to apply the approach during an examination, experimental results showed that their mean planning and examination times were less than the E Groups mean times, and the mean amount of evidence found by the LNE Group was slightly more than the E Groups.

www.manaraa.com

Table 4.23 provides the distribution responses to question 6, which reads as follows: How difficult was it to follow the Examination Search Procedures concept map to search for and identify evidence? Although both groups felt that the maps were slightly or moderately difficult to follow, both groups found more than 50% of the evidence using the Examination Search Procedures concept map.

Table 4.19 Experiment Post-Survey Response Distribution for Q2

Q2: Rate how difficult the approach was to understand?		
Option	LNE Group Distribution Frequency/Percent	E Group Distribution Frequency/Percent
1. The approach was not difficult to understand.	0 / 0%	3 / 42.86%
2. The approach was slightly difficult to understand.	2 / 50.00%	4 / 57.14%
3. The approach was moderately difficult to understand.	1 / 25.00%	0 / 0%
4. The approach was very difficult to understand.	1 / 25.00%	0 / 0%
5. The approach was extremely difficult to understand.	0 / 0%	0 / 0%
Experiment Reference Data: LNE/E Group Mean Planning Time = 26.25 min. / 29.14 min. LNE/E Group Mean Examination Time = 74.00 min. / 105.71 min. LNE/E Group Mean % of Overall Evidence Found = 58.48% / 57.63%		

www.manaraa.com

Table 4.20 Experiment Post-Survey Response Distribution for Q3

Q3: Rate your understanding of the content and purpose of the concept mapping case domain modeling approach for use during an examination.		
Option	LNE Group Distribution Frequency/Percent	E Group Distribution Frequency/Percent
1. The content and purpose of the approach was extremely difficult to understand.	0 / 0%	0 / 0%
2. The content and purpose of the approach was very difficult to understand.	0 / 0%	1 / 14.29%
3. The content and purpose of the approach was moderately difficult to understand.	2 / 50.00%	1 / 14.29%
4. The content and purpose of the approach was slightly difficult to understand.	1 / 25.00%	2 / 28.57%
5. The content and purpose of the approach was not difficult to understand.	1 / 25.00%	3 / 42.86%
Experiment Reference Data: LNE/E Group Mean Planning Time = 26.25 min. / 29.14 min. LNE/E Group Mean Examination Time = 74.00 min. / 105.71 min. LNE/E Group Mean % of Overall Evidence Found = 58.48% / 57.63%		

Table 4.24 provides the distribution responses to question 7, which reads as follows: How likely would you be to use this approach for forensic investigations? Although none of the E Group subjects indicated that they were likely to use the approach for forensic investigations, 50% of the LNE Group indicated that they were likely to use the approach.

Table 4.25-4.29 provides the survey responses given by the ICAC investigator and Computer Forensic Examiners/Investigators from the Mississippi Attorney General's Office. Table 4.25 provides the distribution responses to question 1, which reads as

www.manaraa.com

follows: How difficult was the approach to understand? All of the investigators indicated that the approach was slightly difficult to understand.

Table 4.21 Experiment Post-Survey Response Distribution for Q4

Q4: Rate your confidence in your ability and potential to learn how to effectively build a concept mapping model from scratch during an examination.		
Option	LNE Group Distribution Frequency/Percent	E Group Distribution Frequency/Percent
1. I am extremely not confident in my ability to learn to build a model from scratch.	0 / 0%	0 / 0%
2. I am not confident in my ability to learn to build a model from scratch.	0 / 0%	1 / 14.29%
3. I am neither confident nor not confident in my ability to build a model from scratch.	2 / 50.00%	1 / 14.29%
4. I am confident in my ability to learn to build a model from scratch.	1 / 25.00%	2 / 28.57%
5. I am extremely confident in my ability to learn to build a model from scratch.	1 / 25.00%	3 / 42.86%
Experiment Reference Data: LNE/E Group Mean Planning Time = 26.25 min. / 29.14 min. LNE/E Group Mean Examination Time = 74.00 min. / 105.71 min. LNE/E Group Mean % of Overall Evidence Found = 58.48% / 57.63%		

www.manaraa.com

Table 4.22 Experiment Post-Survey Response Distribution for Q5

Q5: Rate your confidence level in applying the concept mapping case domain model approach during a computer forensics examination.		
Option	LNE Group Distribution Frequency/Percent	E Group Distribution Frequency/Percent
1. I am extremely not confident in my ability to apply the approach during an examination.	0 / 0%	0 / 0%
2. I am not confident in my ability to apply the approach during an examination	1 / 25.00%	1 / 14.29%
3. I am neither confident nor not confident in my ability to apply the approach during an examination.	2 / 50.00%	0 / 0%
4. I am confident in my ability to apply the approach during an examination.	1 / 25.00%	3 / 42.86%
5. I am extremely confident in my ability to apply the approach during an examination.	0 / 0%	3 / 42.86%
Experiment Reference Data: LNE/E Group Mean Planning Time = 26.25 min. / 29.14 min. LNE/E Group Mean Examination Time = 74.00 min. / 105.71 min. LNE/E Group Mean % of Overall Evidence Found = 58.48% / 57.63%		

In Table 4.26, when asked in question 2 to rate their understanding of the content and purpose of the concept mapping case domain modeling approach for use during an examination, three of the four investigators indicated that the approach was not difficult or slightly difficult to understand. Table 4.27 provides the distribution responses to question 3, which reads as follows: Rate your confidence in your ability and potential to learn how to effectively build a concept mapping model from scratch during an examination. All of the investigators indicated that they were confident or extremely confident in their abilities to build a model from scratch.

www.manaraa.com

Table 4.23 Experiment Post-Survey Response Distribution for Q6

Q6: How difficult was it to follow the Examination Search Procedures concept map to search and identify evidence?		
Option	LNE Group Distribution Frequency/Percent	E Group Distribution Frequency/Percent
1. The concept map was not difficult to follow.	0 / 0%	0 / 0%
2. The concept map was slightly difficult to follow.	1 / 25.00%	5 / 71.43%
3. The concept map was moderately difficult to follow.	3 / 75.00%	2 / 28.57%
4. The concept map was very difficult to follow.	0 / 0%	0 / 0%
5. The concept map was extremely difficult to follow.	0 / 0%	0 / 0%
Experiment Reference Data: LNE/E Group Mean Planning Time = 26.25 min. / 29.14 min. LNE/E Group Mean Examination Time = 74.00 min. / 105.71 min. LNE/E Group Mean % of Overall Evidence Found = 58.48% / 57.63%		

Table 4.28 asked the investigators the following in question 4: Rate your confidence in applying the concept mapping case domain modeling approach during/after an ICAC investigation/computer forensics examination. The investigators all indicated that they were confident or extremely confident in their abilities to apply the modeling approach during an investigation/examination. Table 4.29 provides the distribution responses to question 5, which reads as follows: How likely would you be to use this approach for ICAC/computer forensic investigations? Two of the four investigators indicated that they were unlikely to use the approach; although one investigator was undecided on whether he/she would use the approach, one investigator did indicate that he/she was likely to use the approach in investigations.

www.manaraa.com

Table 4.24 Experiment Post-Survey Response Distribution for Q7

Q7: How likely would you be to use this approach for forensic investigations?		
Option	LNE Group Distribution Frequency/Percent	E Group Distribution Frequency/Percent
1. I am extremely likely to use this approach in forensic investigations.	0 / 0%	0 / 0%
2. I am likely to use this approach in forensic investigations.	2 / 50.00%	0 / 0%
3. I am neither likely nor unlikely to use this approach in forensic investigations.	0 / 0%	1 / 14.29%
4. I am unlikely to use this approach in forensic investigations.	2 / 50.00%	4 / 57.14%
5. I am extremely unlikely to use this approach in forensic investigations.	0 / 0%	2 / 28.57%
Experiment Reference Data: LNE/E Group Mean Planning Time = 26.25 min. / 29.14 min. LNE/E Group Mean Examination Time = 74.00 min. / 105.71 min. LNE/E Group Mean % of Overall Evidence Found = 58.48% / 57.63%		

Table 4.25 ICAC Investigator and CF Examiner Survey Responses for Q1

Q1: How difficult was the approach to understand?	
Option	ICAC & CFE Distribution Frequency/Percent
1. The approach was not difficult to understand.	0 / 0%
2. The approach was slightly difficult to understand.	4 / 100.00%
3. The approach was moderately difficult to understand.	0 / 0%
4. The approach was very difficult to understand.	0 / 0%
5. The approach was extremely difficult to understand.	0 / 0%

www.manaraa.com

Table 4.26 ICAC Investigator and CF Examiner Survey Responses for Q2

Q2: Rate your understanding of the content and purpose of the concept mapping case domain modeling approach for use during an examination.	
Option	ICAC & CFE Distribution Frequency/Percent
1. The content and purpose of the approach was extremely difficult to understand.	0 / 0%
2. The content and purpose of the approach was very difficult to understand.	1 / 25.00%
3. The content and purpose of the approach was moderately difficult to understand.	0 / 0%
4. The content and purpose of the approach was slightly difficult to understand.	2 / 50.00%
5. The content and purpose of the approach was not difficult to understand.	1 / 25.00%

Table 4.27 ICAC Investigator and CF Examiner Survey Responses for Q3

Q3: Rate your confidence in your ability and potential to learn how to effectively build a concept mapping model from scratch during an examination.	
Option	ICAC & CFE Distribution Frequency/Percent
1. I am extremely not confident in my ability to learn to build a model from scratch.	0 / 0%
2. I am not confident in my ability to learn to build a model from scratch.	0 / 0%
3. I am neither confident nor not confident in my ability to build a model from scratch.	0 / 0%
4. I am confident in my ability to learn to build a model from scratch.	1 / 25.00%
5. I am extremely confident in my ability to learn to build a model from scratch.	3 / 75.00%

www.manaraa.com

Table 4.28 ICAC Investigator and CF Examiner Survey Responses for Q4

Q4: Rate your confidence in applying the concept mapping case domain model approach during/after an ICAC investigation/computer forensics examination.	
Option	ICAC & CFE Distribution Frequency/Percent
1. I am extremely not confident in my ability to apply the approach during an investigation/examination.	0 / 0%
2. I am not confident in my ability to apply the approach during an investigation/examination	0 / 0%
3. I am neither confident nor not confident in my ability to apply the approach during an investigation/examination.	0 / 0%
4. I am confident in my ability to apply the approach during an investigation/examination.	3 / 75.00%
5. I am extremely confident in my ability to apply the approach during an investigation/examination.	1 / 25.00%

Table 4.29 ICAC Investigator and CF Examiner Survey Responses for Q5

Q5: How likely would you be to use this approach for ICAC/computer forensic investigations?	
Option	ICAC & CFE Distribution Frequency/Percent
1. I am extremely likely to use this approach in investigations.	0 / 0%
2. I am likely to use this approach in investigations.	1 / 25.00%
3. I am neither likely nor unlikely to use this approach in investigations.	1 / 25.00%
4. I am unlikely to use this approach in investigations.	2 / 50.00%
5. I am extremely unlikely to use this approach in investigations.	0 / 0%

www.manaraa.com

4.4 Discussion of Experimental Results and Conclusions

The statistical analysis results of the combined experiments (1-4) will be discussed with respect to three research questions:

1. Does the concept mapping case domain modeling approach result in an increased amount of evidence found in an examination as compared to a typical approach?
2. Does the concept mapping case domain modeling approach require a considerable amount of additional effort when compared to a typical approach?
3. Is the concept mapping case domain modeling approach useful for typical law enforcement investigators involved in computer forensic cases?

Section 4.4.1 discusses the results with respect to research question 1, section 4.4.2 discusses the results with respect to research question 2, and section 4.4.3 discusses the results with research question 3. Section 4.4.4 provides relevant conclusions about the experiment.

4.4.1 Amount of Evidence

In relation to the amount of evidence found, no significant differences were found between those subjects using the concept mapping case domain modeling approach (experimental group) and the ad hoc approach (control group). Although the experimental group did not identify more overall evidence than the control group, the experimental group did find more evidence for May files and Life Insurance files than the control group, 90.91% vs. 81.25% and 85.46% vs. 85%, respectively. Since the results of

www.manaraa.com

the experiment show that the control group did not find more evidence than the experimental group in all categories, research question 1 cannot be completely refuted. Furthermore, post-survey discussion responses indicated that several of the experimental group subjects felt that the approach would be useful for analyzing the case details of a forensic examination. One subject stated, "I am presently working an actual case that I wish I now had this knowledge to use on." Another subject said that "it helps you think outside the box and develop information you may have missed by just writing." Other subjects indicated that the approach and the concept map made it easier for the average investigator/examiner to examine evidence, the approach helped with organization, helped to focus and keep a clear picture of the entire examination, and helped with recalling case information and making sure all of the basic examination tasks are performed.

4.4.2 Time and Effort

The statistical analysis results indicated that there was no significant difference in the effort/time data between the experimental and control groups. However, the experimental group spent less time in the examination and in the overall experimental exercise than the control group, 94.18 minutes vs. 115.75 minutes and 122.27 vs. 126.50 minutes, respectively. The experimental group spent more time in the planning phase of the exercise than the control group. This increase in time was expected since the experimental group had more detailed tasks to complete than the control group. Moreover, taking the additional time to plan the examination potentially reduced the amount of time needed to search for and identify evidence during the examination phase.

www.manaraa.com

According to the post-experiment survey responses, all of the subjects in the experimental group indicated that they did not find it difficult to use the approach for the activity/exercise.

Research question 2 questioned whether the concept mapping case domain modeling approach required a significant amount of additional effort to perform a digital forensic examination when compared to an ad hoc approach. In section 4.2.1, the following hypotheses were developed to answer research question 2: A.) The experimental group will spend more time in the planning phase than the control group; B.) The experimental group will spend less time in the examination than the control group; C.) Overall, the experimental group will spend less time in the total experiment than the control group. The results showed that A, B, and C were proven to be true, therefore, the data indicated that the concept mapping case domain modeling approach did not require a significant amount of additional effort to perform a digital forensic examination when compared to an ad hoc approach.

4.4.3 Usability for Law Enforcement

Research question 3 questioned whether the concept mapping case domain modeling approach was useful for typical law enforcement investigators involved in computer forensic cases. Two hypotheses were developed to answer the research question which are as follows: A) Investigators with little or no experience will spend less time executing the examination than those investigators with experience; B) Investigators with little or no experience will identify more evidence than those investigators with experience. To answer this research question, the data from the

www.manaraa.com

experimental groups was categorized into two groups, little or no experience (LNE) and experienced (E). The statistical results indicated that LNE group spent a significantly less amount of time on the total experimental activity than the E group. Although no significant difference was observed between the groups for the planning and examination times, the LNE group spent less time in the planning phase and examination phase than the E group. The statistical results also indicated that the LNE group found a significantly greater amount of evidence containing Other files than the E group. Although no other statistical differences were observed, the LNE group did find more evidence than the E group for Gambling files, Vehicle files, and total overall evidence. These results of the experiment indicated that the concept mapping case domain modeling approach was useful for typical law enforcement involved in computer forensic cases. Furthermore, this experiment showed that subjects with experience or little or no experience in computer forensic examinations were able to properly use the concept mapping case domain modeling approach to search for and identify evidence.

According to the post-experiment discussion survey responses, a majority of the subjects felt that the approach and the concept map diagrams would be beneficial to law enforcement during examinations, for training, and for presenting information to jurors. For instance, when asked if the concept map diagrams would be helpful visual aids for presenting computer forensics findings to a jury (Q3), 8 subjects answered yes, 2 answered no, and 1 answered maybe. Several subjects felt that visual aids were always helpful when explaining things to jurors. When the subjects were asked question 4, which asks if the modeling approach would be useful for training law enforcement about

www.manaraa.com

computer forensic procedures, nine of the subjects answered yes, 1 answered no, and 1 answered somewhat. The subjects were also asked to describe any strengths (Q5) and weaknesses (Q6) of the concept mapping case domain model. The subjects listed what they considered to be strengths of the approach below:

- Ease of organization
- Offers a graphical representation of what occurred and what was discovered
- Helps you to think outside of the box
- Helps to focus the investigator and limit the amount of data to search/analyze/review
- Very helpful in determining evidence

Weaknesses of the approach that the subjects gave were that it was time consuming, the map was cluttered and hard to follow, and the concept map duplicated the investigator's notes. Although one subject felt that it was time consuming, the experimental results showed that the approach and concept maps aided in the experimental group spending less time in the examination than the control group. One subject felt that the map was cluttered and hard to follow. The layout of the concept map can be modified to include several additional concept maps containing those same procedures. For this experiment, however, only one map was used in an effort to reduce the amount of paper so that the subjects would not have to search through several pages of concept map diagrams to find the procedures to follow. To further address this weakness, a web-based concept map of the search procedures could be created that would be less cluttered and easier to follow. Each search procedure concept could contain an

www.manaraa.com

icon that would link to another concept map containing the specific steps to follow for that particular search procedure.

The post-lecture survey responses given by the ICAC/AGO investigators were also helpful in determining the usefulness of the approach for typical law enforcement as well. The investigators experience with investigations range from 2.5 to 10 years. Each of the investigators thought that the approach would be useful in investigations; one investigator stated that having "everything in one spot is helpful." Another investigator stated that it would be a good application for a trial and would also be "a good tool to track several suspects involved in an operation." Another investigator stated that it would be good for preparing for a case and for "large scale white collar type crime[s]."

One disadvantage that was reported was that linking files for large cases could become very time consuming, and actually reading reports could give the investigator a better idea of what evidence to look for in a case. Even though the CmapTools software makes it easy to add and remove files, possibly automating the file uploading process could alleviate some of the time required to link the appropriate files to the case concept.

Another disadvantage given was that since they have to manage several cases and lengthy reports, this approach "would not be feasible on a single possession case." A way to approach this disadvantage would be to create general concept maps for the different types of crime categories including general characteristics associated with the crime. It would be the investigators responsibility to add specific details about the suspect including any and all information relative to the case, including a concept or concept map containing additional suspects involved in the case. This concept or concept

www.manaraa.com

map could be used to link to other crime category concept maps that the suspect(s) may have been a part of. Keyword searching within the concept map could also aid in the linking process because the search application would list each concept and/or concept map where the specific search term (such as the suspect's name) was found. This could also simplify the linking of information within the concept maps as well.

The investigators were also asked if they thought the concept map diagrams would be helpful as visual aids for presenting investigation results to a jury. Each of the investigators felt that the concept map diagrams would be useful because "it would help to convey evidence to a jury," according to one investigator. The investigators were asked if they thought the modeling approach would be useful for training future investigators about procedures. Each of the investigators thought that it would be helpful, but one of these investigators stated that it should be used "only as a training tool" and not as an actual guide since there are so many different ways to examine a case depending on what the case facts are. Another investigator made the statement that "unless the investigator already has a good knowledge and good analytical skills," the concept map diagrams would not be useful for training purposes.

The investigators were asked to describe how the approach would be beneficial to their investigations. One investigator commented that it would be "a good visual aid to quickly see where you were in an exam," while other investigators stated that it would beneficial for trial and "for everyday investigation[s] of a CP [child pornography] suspect, [for] linking large scale cases together, [to act as] a checklist of some sorts for all case types, [to encourage] the examiner to brainstorm the case, [and for organizing] the

www.manaraa.com

case for easy and quick review." The investigators were also asked if they thought the concept mapping case domain modeling approach (including concept maps) would be useful for new cases and revisiting old cases when preparing for court. Each of the investigators thought that the approach would be useful when preparing for or during court proceedings for the following reasons:

- It would save time since, there would be "no need to have to pull from several unlinked sources" since all the case information would be located in one place.
- To "explain how the case links together (the facts)…[for instance] to show how the suspect is linked to the evidence."
- Because "the CM [concept map] breaks the case down to its bare bones and makes it very easy for a jury to see" how the evidence is related to the suspect and important to the case.
- Although the approach would not "result in any [new] revelations about the case… depending on the complexity…it would better organize the information" of the case.

Based on the experimental results and responses from the participants in the experimental activity and the survey discussion responses from the Attorney General's Office investigators, it can be reasonably concluded that the concept mapping case domain modeling approach is useful to law enforcement investigators involved in computer forensic cases.

www.manaraa.com

4.5 Threats to Validity

Threats to the validity of the experiments include the following:

Small Sample Size: There were a total of four experiments conducted, and each experiment consisted of five to six participants. To get healthier statistical data, the data from both groups were aggregated from each of the experiments to represent one experiment. The group sizes were still small with 8 control subjects and 11 experimental subjects. It would be improper to apply the findings of the experiment to all law enforcement investigators and examiners involved in computer forensic investigations. Some of the subjects had limited computer skills and computer forensic knowledge. Intended users of this approach in computer forensic examinations are expected to have satisfactory experience with computer forensic examinations. These individuals could include divisions of local and state law enforcement that focus primarily on computer forensics and federal agencies as well.

Subject Responses to Surveys: The subjects using the concept mapping case domain modeling approach may have felt obligated to answer favorably to the surveys since they were attending a free workshop and were guaranteed to receive five additional training hours for completing the exercise. Not all of the subjects responded positively. Furthermore, they may have responded more negatively if the course was not free and if they were not receiving the five additional training hours.

Computer Problems: A computer problem (freezing up) was encountered during Experiment 1 but was corrected for the remaining experiments. These problems were experienced in the experiment by both groups. These problems may have led to a

www.manaraa.com

decrease in the motivation to continue searching for evidence due to having to reboot the computer one or more times.

Chapter 5 concludes the dissertation by providing a summary of the results, responses to the research questions, and discuss future research work.

www.manaraa.com

CHAPTER V

CONCLUSIONS AND FUTURE WORK

This chapter concludes this dissertation and addresses the hypothesis and the three research questions and conclusions of each. Section 1.3 presented the hypothesis of this dissertation which states that the concept mapping case domain modeling approach can serve as a method for organizing, examining, and analyzing digital forensic evidence and can enhance the quality of forensic examinations without increasing the time required to examine and analyze forensic evidence by more than 5%. Three research questions were developed to address this hypothesis and are as follows:

1. Does the concept mapping case domain modeling approach result in an increased amount of evidence found in an examination as compared to a typical approach?

2. Does the concept mapping case domain modeling approach require a considerable amount of additional effort when compared to a typical approach?

3. Is the concept mapping case domain modeling approach useful for typical law enforcement investigators involved in computer forensic cases?

Section 5.1 discusses research question 1, Section 5.2 discusses section 2, Section 5.3 discusses research question 3, and Section 5.4 discusses future research work with the concept mapping case domain modeling approach.

www.manaraa.com

5.1 Research Question 1: Comparison of the Amount of Evidence Found

To address research question 1, it was assumed that use of the concept mapping case domain modeling approach (CMCDMA) would result in the experimental group identifying more evidence than the control group. Although the CMCDMA did not result in an overall increase of evidence found in the examination than the ad hoc approach, the CMCDMA did result in more evidence being found in two evidence file categories, May files and Life Insurance files.

The experimental data was also broken down further into two categories, little or no experience (LNE) and experienced (E) based upon the subjects' years of experience with computer forensic examinations. The data showed that the group with little or no experience found more evidence in the Gambling file, Vehicle file, and Other file categories. A significant difference in the amount of evidence was observed in the Other file category as well. In addition, the LNE group found more overall evidence than the experienced group. This data demonstrated that the CMCDMA can be used by those with little or no experience to search for and identify evidence and by those with experience as well. It also demonstrated that the CMCDMA could be used as a guide and/or training mechanism for searching for and identifying evidence. Based on the amount of evidence found data for the experimental and control groups, the following can be stated about Research Question 1: The concept mapping case domain modeling approach contributes to an increase in the amount of evidence found when comparing the experience levels of those utilizing the approach. The use of the concept mapping case domain modeling approach resulted in a decreased overall amount of evidence found by

www.manaraa.com

the experimental group than the control group. However, only 11.5% more evidence was recovered by the control group than the experimental group. It is important to note that the total experiment was limited to two hours. Additional time may have resulted in the experimental group uncovering approximately the same or more evidence than the control group.

5.2 Research Question 2: The Effort Used to Apply the Concept Modeling Approach

To address research question 2, it was assumed that use of the concept mapping case domain modeling approach (CMCDMA) would result in the experimental group spending more time in the planning phase, less time in the examination phase, and less time in the total experiment than the control group. The experimental data verified that the experimental group spent more time in the planning phase, less time in the examination phase, and less time in the overall experiment. In Table 4.2, it was observed that the greater amount of time spent in the planning phase by the experimental group resulted in less time spent in the examination phase. Although the increase in the planning time did not result in more evidence being found by the experimental group during the examination, all of the subjects indicated in their post-experiment surveys that the approach was not difficult to apply and use in the examination. Based on the effort data for the experimental and control groups, the following can be stated about Research Question 2: Generally the concept mapping case domain modeling approach required an increase in planning time. However, this increase in planning time resulted in a decreased mean examination time and total examination time.

www.manaraa.com

The effort of the experimental group, consisting of the little or no experience (LNE) and experienced (E) groups, was compared to determine if more effort was needed by the LNE group to use the CMCDMA than by the E group. Although the E group's prior knowledge and experience with computer forensic procedures would seem to be advantageous to their uncovering more evidence and requiring less time to execute the examination, the data showed that the LNE group spent a significantly less amount of time in the overall experimental activity than the E group. The LNE group spent 25.66% less time in the overall experiment than the E group. Furthermore, the LNE group spent less time in the planning phase and examination phases than the E group. With regards to the experience level, the following can be stated about Research Question 2: Usage of the concept mapping case domain modeling approach resulted in less time spent in the planning, examination, and overall experiments by those with little or no computer forensic experience than those with experience.

5.3 Research Question 3: Utility for Law Enforcement Investigators

Data from the experiments and survey responses from the Mississippi Attorney General's Office investigators/examiners (CFE/ICAC) suggested that the concept mapping case domain modeling approach was useful for typical law enforcement investigators involved in computer forensic cases. The two hypotheses questions created to address this research question are as follows:

1. Investigators with little or no experience will identify more evidence than those investigators with experience.

www.manaraa.com

2. Investigators with little or no experience will spend less time executing the examination than those investigators with experience.

The experimental findings for the amount of evidence found and effort for the LNE and E groups was discussed previously in sections 5.1 and 5.2. The data indicated that hypothesis 1 was valid since investigators with little or no experience did identify more evidence than those investigators with experience; furthermore, hypothesis 2 was verified also because the data did show that the investigators with little or no experience spent less time executing the examination than those investigators with experience. Several of the investigators thought that the approach would be helpful as visual aids in court, for training, and for use during computer forensic examinations. Furthermore, they indicated that the approach was useful for organizing the case facts and materials, for focusing the investigation, for providing a graphical "quick view" of what occurred in the case and what was discovered, and for determining what evidence should be searched for and identified. Some investigators, however, felt that the approach was time consuming and the concept maps were cluttered. It is believed that taking the additional time to create the concept maps using the approach ultimately reduces the time needed to review the case when it goes to trial. All of the evidence, case facts and findings, documents, and so forth would be located on that concept map for that case which would eliminate the need to have to find and open several different software programs, folders, files, etc. Reviewing the concept map and referencing important documents would be simplified, and this information could be quickly accessed and shared with other law officers involved with the case including prosecutors.

www.manaraa.com

To further address the research question 3, the CF/ICAC investigators were lectured and given a survey to determine if the concept mapping case domain modeling approach would be useful in computer forensic investigations. The investigators all indicated that the approach would be useful in investigations for linking and tracking several suspects, for preparing for trial, for accessing all case documents in one location from the case concept map, for presenting investigation results to a jury, and for linking large scale cases together. Although none of the investigators indicated that they were likely to use the approach in their investigations, each indicated that they were confident in their abilities to learn how to build a concept map and apply the concept map and approach in computer forensic examinations/investigations. These investigators did not get the opportunity to apply the concept mapping case domain modeling approach in the hands-on activities. If they had hands-on experience using the approach, it is believed that the investigators would be more likely to use the approach in some aspect of their investigations whether it is to review cases or to create concept maps for new cases. Also, hand-on experience using the CmapTools software may have made them more likely to use the approach for ICAC/computer forensic investigations.

Based on the quantitative and qualitative data of this research, the following can be stated in regards to this research work: the concept mapping case domain modeling approach can serve as a method for organizing, examining, and analyzing digital forensic evidence and can enhance the quality of forensic examinations without increasing the effort required to examine and analyze forensic evidence by more than 5%. Not only did the data show that the approach was useful for organizing the case facts, examining and

www.manaraa.com

analyzing the evidence, it showed that the approach did not increase the effort, but reduced the effort required to examine and analyze forensic evidence by approximately 3.34%. Although the amount of evidence found by the experimental group (concept mapping case domain modeling approach) was less than the control group (ad hoc approach), additional research could potentially show an improvement in the amount of data found using the experimental approach.

5.4 Contributions

The contributions of this research are as follows:

- Developed a method that can be used to graphically organize the case facts and plan, search, identify, and analyze digital forensic evidence in a digital forensic investigation.
- Developed a method that can be used to easily share evidential findings and to reuse and manage knowledge acquired about the digital forensics process.
- Validated the usefulness and utility of the CMCDMA through four experiments. Empirical data was also created for computer forensic case domain modeling. A seminar class was created to focus on the CMCDMA resulting in the creation of activities and digital forensic related keyword concept maps.
- Developed a method that can be used for training and the support of expert and novice investigators/examiners involved in digital forensic investigations.
- Developed a method that provides a centralized location where evidential documents such as the examiner's case report, subpoenas, search warrants,

www.manaraa.com

chain of custody documents, images of actual evidence, and a quick overview of the case can be accessed.

5.5 Publications

The papers that have been published from this research work are as follows:

Referred Conference Paper

A. Tanner and D. Dampier, "Improving Digital Forensics Investigations with Concept Mapping," Proceedings of the Fifth International Conference on Digital Forensics, Jan. 25-28, 2009, Orlando, Florida.

Book Chapter

A. Tanner and D. Dampier, "Concept Mapping for Digital Forensics Investigations," Advances in Digital Forensics V, 2009.

5.6 Recommendations for Future Research

The purpose of this doctoral research was to provide the preliminary framework for the application of concept mapping to domain modeling for organizing, planning, examining, and graphically representing case information in computer forensic examinations. Additional experiments are needed to better determine the effectiveness of the approach on law enforcement. It is possible that additional activities using the approach could help the subjects better understand and use the approach during examinations and therefore aid in the experimental group recovering more evidence than the control group. Experiments could be conducted using expert computer forensic examiners only. In these experiments, the examiners could first search for evidence using an ad hoc method or their current techniques for searching for evidence. After that examination, they could use the concept mapping case domain approach to search for and

www.manaraa.com

identify evidence in another examination using a similar case. The data and survey results from this examination could provide valuable empirical data for modeling the computer forensic examination process using concept maps.

Additional research is needed to address concept map creation using automated methods. The CmapTools software has a feature that creates the concepts when entered by the user; however the tool does not position these newly created concepts. An automated process could be developed that creates and positions the concepts entered by the investigator. This feature could potentially reduce the time needed to manually create and position the concepts in the concept maps. The users would be able to edit the map, if needed. Furthermore, this feature could also simplify the file adding process to the concepts by simply entering the concept name and selecting the necessary file or files.

The concept mapping case domain modeling approach could be applied to other phases of digital forensic investigations also. Similar to Venter's process flow diagrams discussed in Section 2.1.3, process flow concept maps could be created to assist the cyber forensic first responders in the identification and collection phases of the investigative digital forensic process. A hard copy of the process flow concept maps could accompany the first responders at the scene. This would allow them to record information at the electronic crime scene, and when the investigator enters the findings electronically, this information can be included in the concept map along with photos taken of the crime scene including the suspect, the physical evidence, other digital media, and etc. Even the type of packing used and a photo of the investigator recording the evidence can be applied to the concept map.

www.manaraa.com

Additional research using the concept mapping case domain modeling approach can be conducted to determine the impact that the approach has on computer forensics when preparing for court and/or reviewing cases. The concept maps created for a particular case could be shared between the investigators and the prosecutors and used during the case review process. At the end of the case review, all involved could answer a survey about the usefulness of the digital forensic case concept maps and their advantages and disadvantages for reviewing case details or for preparing for upcoming court. Research work could also include the investigators' use of concept maps to present case facts to jurors.

Additional experimentation using the concept mapping case domain modeling approach is needed for this approach to become a clearly defined, simple method for investigating digital forensic crimes. The concept mapping case domain modeling approach combines domain modeling and digital forensic procedures that provides a unique, graphical view of the digital forensic case. This graphical view could be very useful in investigations for training novice digital forensic investigators and examiners. Law enforcement officers participating in this research work listed several qualities that the concept mapping case domain possessed. They stated that the approach helps to focus an investigation, it helps to organize the case facts of an investigation, it can be used for training, and it can be used to link suspects to several different cases in an investigation. Furthermore, automating the concept mapping case domain modeling approach could reduce the effort needed to manually create case specific concept maps. An automated tool could be created to assist examiners with quickly accessing and

www.manaraa.com

analyzing the case domain from the case facts and evidence provided in the concept map. Further research using the approach is required to determine the impact of the approach, not only on digital forensic examinations, but the entire investigation as well.

www.manaraa.com

REFERENCES

[1] "Antiforensics – Subverting Justice with Exploitation," *Computer Fraud & Security*, vol. 2007, no. 2, Feb. 2007, pp. 16—18.

[2] Association of Chief Police Officers, "Good Practice Guide for Computer based Electronic Evidence," http://cryptome.sabotage.org/acpo-guide.htm (current 20 Sep. 2006).

[3] V. Baryamureeba and F. Tushabe, "The Enhanced Digital Investigation Process Model," *Proceedings: 4th Annual Digital Forensic Research Workshop*, Baltimore, Maryland, August 2004, pp. 1—9, https://www.dfrws.org/2004/day1/Tushabe_EIDIP.pdf (current 8 Sep. 2006).

[4] N. Beebe and J. Clark, "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process," *Proceedings: 4th Annual Digital Forensic Research Workshop*, Baltimore, Maryland, August 2004, pp. 1—25, https://www.dfrws.org/2004/day1/Beebe_Obj_Framework_for_DI.pdf (current 8 Sep. 2006).

[5] H. Berghel, "Hiding Data, Forensics, and Anti-Forensics," *Communications of the ACM*, vol. 50, no. 4, Apr. 2007, pp. 15—20.

[6] R. Bhaskar, "State and Local Law Enforcement is not Ready for a Cyber Katrina," *Communications of the ACM*, vol. 49, no. 2, Feb. 2006, pp. 81—83.

[7] A. C. Bogen, *Selecting Keyword Search Terms in Computer Forensics Examinations using Domain Analysis and Modeling*, doctoral thesis, Department of Computer Science and Engineering, Mississippi State University, Mississippi State, Mississippi, 2006.

[8] A. C. Bogen, D. Dampier, and J. Carver, "Support for Computer Forensics Examination Planning with Domain Modeling: A Report of One Experiment Trial," *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, Waikoloa, Hawaii, Jan. 2007, IEEE, pp. 267b—267b.

www.manaraa.com

[9] A.C. Bogen and D. Dampier, "Unifying Computer Forensics Modeling Approaches: A Software Engineering Perspective," *Proceedings: First International Workshop on Systematic Approaches to Digital Forensic Engineering*, Taipei, Taiwan, Nov. 2005, IEEE, pp. 27—39.

[10] D. Brezinski and T. Killalea, "RFC3227: Guideline for Evidence Collection and Archiving," http://www.ietf.org/rfc/rfc3227.txt (current 8 Sep. 2006).

[11] E. Bruillard and G. L. Baron, "Computer-Based Concept Mapping: A Review of a Cognitive Tool for Students," *Proceedings: Conference on Educational Uses of Information and Communication Technologies*, Beijing, China, Aug. 2000, IFIP, pp. 331-338.

[12] D. Bruschi, M. Monga, and L. Martignoni, "How to Reuse Knowledge about Forensic Investigations," *Proceedings: 4th Annual Digital Forensic Research Workshop*, Baltimore, Maryland, August 2004, pp. 1—13, http://www.dfrws.org/2004/day3/D3-Martignoni_Knowledge_reuse.pdf (current 8 Sep. 2006).

[13] A. J. Cañas et al., "A Summary of Literature Pertaining to the Use of Concept Mapping Techniques and Technologies for Education and Performance Support," The Institute for Human and Machine Cognition, http://www.ihmc.us/users/acanas/Publications/ConceptMapLitReview/IHMC%20Literature%20Review%20on%20Concept%20Mapping.pdf (current 6 Jun. 2007).

[14] A. Cañas, D. Leake, and D. Wilson, "Managing, Mapping, and Manipulating Conceptual Knowledge," IHMC, http://www.ihmc.us/users/acanas/Publications/AAAI99CmapsCBR/AAAI99CmapsCBR.pdf (current 2 Feb. 2007).

[15] B. Carrier and E. Spafford, "An Event-Based Digital Forensic Investigation Framework," *Proceedings of the Fourth Annual Digital Forensic Research Workshop*, Baltimore, Maryland, August 2004, pp. 1—12, http://www.dfrws.org/2004/day1/Carrier-event.pdf (current 1 Nov. 2006).

[16] B. Carrier and E. Spafford, "Getting Physical with the Digital Investigation Process," *International Journal of Digital Evidence*, vol. 2, no. 2, Fall 2003, pp. 1—20.

[17] C. Chen, "Bridging the Gap: The Use of Pathfinder Networks in Visual Navigation," *Journal of Visual Languages and Computing*, vol. 9, no. 3, 1998, pp. 267—286, http://www.pages.drexel.edu/~cc345/papers/jvlc.pdf.

www.manaraa.com

[18] C. Chen and S. Morris, "Vizualizing Evolving Networks: Minimum Spanning Trees versus Pathfinder Networks," *Proceedings of the IEEE Symposium on Information Vizualization*, Seattle, Washington, Oct. 2003, IEEE, pp. 67—74.

[19] S. Ciardhuáin, "An Extended Model of Cybercrime Investigations," *International Journal of Digital Evidence*, vol. 3, no. 1, Summer 2004, pp.1—22.

[20] M. Dunham, *Data Mining: Introductory and Advanced Topics*, Prentice Hall, Upper Saddle River, New Jersey, 2003.

[21] J. Dunlap and S. Grabinger, "Using Pathfinder Networks to Examine Structural Knowledge," http://carbon.cudenver.edu/~jdunlap/sknowledge.pdf current (10 Jul. 2007).

[22] J. Feldman, "Top Ten Things To Do When Collecting Electronic Evidence," http://www.forensics.com/pdf/Top_Ten.pdf (current 26 Oct. 2006).

[23] J. Fernandez, S. Smith, M. Garcia, and D. Kar, "Computer Forensics- A Critical Need in Computer Science Programs," *Journal of Computing Sciences in Colleges*, vol. 20, no. 4, Apr. 2005, pp. 315—322.

[24] D. Forte and R. Power, "A Tour through the Realm of Anti-Forensics," *Computer Fraud & Security*, vol. 2007, no. 6, Jun. 2007, pp. 18—20.

[25] W. Harrison, D. Aucsmith, G. Heuston, S. Mocas, M. Morrissey, and S. Russelle, "A Lessons Learned Repository for Computer Forensics," *Proceedings: 2nd Annual Digital Forensics Research Workshop (DFRWS)*, Syracuse, New York, Aug. 2002, http://www.dfrws.org/2002/papers/Papers/Warren_Harrison.pdf (current 21 Mar. 2007).

[26] N. K. Kasabov, *Foundations of Neural Networks, Fuzzy Systems, and Knowledge Engineering*, MIT Press, Cambridge, Massachusetts, 1996.

[27] J. Kornblum, "Preservation of Fragile Digital Evidence by First Responders," http://www.dfrws.org/2002/papers/Papers/Jesse_Kornblum.pdf (current 20 Sep. 2006).

[28] B. Kosko, "Fuzzy Cognitive Maps," *International Journal of Man-Machine Studies,* vol. 24, 1986, pp. 65-75.

[29] B. Kosko, "Fuzzy Knowledge Combination," *International Journal of Intelligent Systems*, vol. 1, pp. 293-320, 1986.

www.manaraa.com

[30] B. Kosko and S. Isaka, "Fuzzy Logic," *Scientific American*, vol. 269, 76—81, July 1993.

[31] B. Kosko, *Neural Networks and Fuzzy Systems: A Dynamical Systems Approach to Machine Intelligence,* Prentice Hall, Englewood Cliffs, New Jersey, 1992.

[32] M. Kramer, *Using Concept Maps for Knowledge Acquisition in Satellite Design: Translating "Statement of Requirements on Orbit" to "Design Requirements"*, doctoral thesis, Graduate School of Computer and Information Sciences, Nova Southeastern University, Fort Lauderdale-Davie, Florida, 2005.

[33] W. Kruse and J. G. Heiser, *Computer Forensics: Incident Response Essentials*, Lucent, Boston, Massachusetts, 2002.

[34] U. K. Kudikyala, *Reducing Misunderstanding of Software Requirements by Conceptualization of Mental Models Using Pathfinder Networks*, doctoral thesis, Department of Computer Science and Engineering, Mississippi State University, Mississippi State, MS, 2004.

[35] R. Mercuri, "Challenges in Forensic Computing," *Communication of the ACM*, vol. 48, no. 12, Dec. 2005, pp. 17—21.

[36] G. Mohay, "Technical Challenges and Directions for Digital Forensics," *Proceedings: First International Workshop on Systematic Approaches to Digital Forensic Engineering*, Brisbane, Australia, Nov. 2005, IEEE, pp. 155—161.

[37] R. Mukhopadhyay, A. Ma, and I. K. Sethi, "Pathfinder Networks for Content Based Image Retrieval Based on Automated Shape Feature Discovery," *Proceedings of the Sixth International Symposium on Multimedia Software Engineering*, Miami, Florida, Dec. 2004, IEEE, pp. 522—528.

[38] National Institute of Justice, "Electronic Crime Scene Investigation: A Guide for First Responders 2001," http://www.iwar.org.uk/ecoespionage/resources/cybercrime/ecrimesceneinvestigation.pdf#search=%22electronic%20crime%20scene%20investigation %20a%20guide%20for%20first%20responders%202001%22 (current 8 Sep. 2006).

[39] National Institute of Justice, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement," http:// www.ncjrs.gov/pdffiles1/nij/199408.pdf (current 20 Sep. 2006).

www.manaraa.com

[40] National Institute of Justice, "Electronic Crime Needs Assessment for State and Local Law Enforcement," http://www.ncjrs.gov/pdffiles1/nij/186276.pdf (current 8 Sep. 2006).

[41] M. Noblett, M. Pollitt, L. Presley, "Recovering and Examining Computer Forensic Evidence," *Forensic Science Communications*, vol. 20, no. 4, Oct. 2000, http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm (current 20 Sep. 2006).

[42] R. Nolan, C. O'Sullivan, J. Branson, and C. Waits, "First Responders Guide to Computer Forensics," http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf (current 28 Sep. 2006).

[43] J. D. Novak and A. J. Cañas, "The Theory Underlying Concept Maps and How to Construct Them," Technical Report IHMC Cmap Tools 2006-01, Florida Institute for Human and Machine Cognition, 2006, http://cmap.ihmc.us/Publications/ResearchPapers/TheoryUnderlyingConceptMaps.pdf (current 7 Feb. 2007).

[44] NTI, "Computer Evidence Processing Steps," http://www.forensics-intl.com/evidguid.html (current 26 Oct. 2006).

[45] G. Palmer, *A Road Map for Digital Forensics Research*, technical report, Digital Forensic Research Workshop, Utica, New York, 2001.

[46] G. Palmer, "Forensic Analysis in the Digital World," *International Journal of Digital Evidence*, vol. 1, no. 1, Spring 2002, pp. 1—6.

[47] M. Pollitt, "An Ad Hoc Review of Digital Forensic Models," *Proceedings: Second International Workshop on Systematic Approaches to Digital Forensic Engineering*, Bell Harbor, Washington, Apr. 2007, IEEE, pp. 43—54.

[48] M. Pollitt and A. Whitledge, "Exploring Big Haystacks: Data Mining and Knowledge Management," M. Oliver and S. Shenoi, eds., *Advances in Digital Forensics II*, vol. 222, Springer, New York, pp. 67—76.

[49] M. Reith, C. Carr, and G. Gunsch, "An Examination of Digital Forensic Models," *International Journal of Digital Evidence*, vol. 1, no. 3, Fall 2002, pp. 1—20.

[50] G. Richard III and V. Roussev, "Next Generation Digital Forensics," *Communications of the ACM*, vol. 49, no. 2, Feb. 2006, pp. 76—80.

www.manaraa.com

[51] F. Rodhain, "Tacit to Explicit: Transforming Knowledge through Cognitive Mapping - An Experiment," *Proceedings: The 1999 ACM Special Interest Group on Computer Personnel Research (SIGCPR)*, New Orleans, Louisiana, 1999, pp. 51—56.

[52] M. Rogers and K. Seigfried, "The Future of Computer Forensics: A Needs Analysis Survey," *Computers & Security*, vol. 23, no. 1, Feb. 2004, pp.12—16.

[53] R. Rowlingson, "A Ten Step Process for Forensic Readiness," *International Journal of Digital Evidence*, vol. 2, no. 3, Winter 2004, pp. 1—28.

[54] G. Ruibin, T. Yun, and M. Gaertner, "Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework," *International Journal of Digital Evidence*, Spring 2005, vol. 4, no. 1, pp. 1—13, http://www.utica.edu/academic/institutes/ecii/publications/articles/B4A6A102-A93D-85B1-96C575D5E35F3764.pdf.

[55] B. Sartin, "Anti-Forensics – Distorting the Evidence," *Computer Fraud & Security*, vol. 2006, no. 5, May 2006, pp. 4—6.

[56] R. W. Schvaneveldt, F. T. Durso, and D. W. Dearholt, in G. Bower (Ed.), The P*sychology of Learning and Motivation: Advances in Research and Theory*, G. Bower ed., vol. 24, Academic Press, New York, pp. 249—284.

[57] B. Schneier, "Attack Trees," *Dr. Dobb's Journal*, vol. 24, no. 12, Dec. 1999, pp. 21—29.

[58] Scientific Working Group on Digital Evidence, "Best Practices for Computer Forensics," http://ncfs.org/swgde/documents/swgde2006/Best_Practices_for_ComputerForensics%20July06.pdf (current 5 Oct. 2006).

[59] T. Shipley and H. Reeve, "Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community," http://www.search.org/files/pdf/CollectEvidenceRunComputer.pdf (current 28 Sep. 2006).

[60] A. Siraj, *A Unified Alert Fusion Model for Intelligent Analysis of Sensor Data in an Intrusion Detection Environment*, doctoral thesis, Department of Computer Science and Engineering, Mississippi State University, Mississippi State, MS, 2006.

www.manaraa.com

[61] P. Stephenson, "Modeling of Post-Incident Root Cause Analysis," *International Journal of Digital Evidence*, Fall 2003, vol. 2, no. 2, pp. 1—16, http://www.utica.edu/academic/institutes/ecii/publications/articles/A0AE98D6-E1F6-1C9D-481CEE8C29401BFE.pdf (current 24 Mar. 2008).

[62] S.O. Tergan, "Digital Concept Maps for Managing Knowledge and Information: Searching for Synergies," *Knowledge and Information Visualization*, S.O. Tergan and T. Keller, eds., Springer, New York, pp. 185 – 204, http://ldt.stanford.edu/~educ39105/paul/articles_2005/digital %20concept%20maps.pdf (current 8 Mar. 2007).

[63] R. Thompson, "Chasing after 'petty' computer crime," *IEEE Potentials*, Feb/Mar. 1999, 20-22.

[64] L. Ulden, A. Alderson, and S. Tearne, "A Conceptual Model for Learning Internet Searching on the Internet," *Proceedings: The 34th Annual Hawaii International Conference on System Sciences*, Maui, Hawaii, Jan. 2001, IEEE, pp. 1—9.

[65] United States Department of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf (current 20 Sep. 2006).

[66] United States Secret Service, "Best Practices for Seizing Electronic Evidence," http://www.secretservice.gov/electronic_evidence.shtml (current 20 Sep. 2006).

[67] J. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, Second Edition, Charles River Media, Boston, Massachusetts, 2005.

[68] N. J. van Eck, F. Frasincar, J. van den Berg, "Visualizing Concept Associations Using Concept Density Maps," *Proceedings: 10th International Conference on Information* Visualization, London, United Kingdom, Jul. 2006, IEEE, pp. 270—275.

[69] J. Venter, "Process Flow Diagrams for Training and Operations," M. Oliver and S. Shenoi, eds., *Advances in Digital Forensics II*, vol. 222, Springer, New York, pp. 331—342.

[70] C. Whitcomb, "An Historical Perspective of Digital Evidence: A Forensic Scientist's View," International Journal of Digital Evidence, vol. 1, no. 1, Spring 2002, http://www.ijde.org/archives/carrie_article.html (current 11 Oct. 2007).

[71] H. Wolfe, "Computer Forensics," *Computers & Security*, vol. 22, no. 1, Jan. 2003, pp. 26—28.

www.manaraa.com

[72] H. Wolfe, "Evidence Acquisition," *Computers & Security*, vol. 22, no. 3, Apr. 2003, pp. 193—195.

[73] H. Wolfe, "Presenting the Evidence Report," *Computers & Security*, vol. 22, no. 6, Sep. 2003, pp. 479—481.

[74] H. Wolfe, "Setting Up an Electronic Evidence Forensics Laboratory," *Computers & Security*, vol. 22, no. 8, Dec. 2003, pp. 670—672.

[75] H. Wolfe, "The Circumstances of Seizure," *Computers & Security*, vol. 22, no. 2, Feb. 2003, pp. 96—98.

[76] B. Zaff and M. McNeese, "An Integrated Methodology for Knowledge and Design Acquisition," *Proceedings: National Aerospace and Electronics Conference*, Dayton, Ohio, May 1991, IEEE, pp. 779—785.

www.manaraa.com

APPENDIX A

IRB APPROVAL LETTER

www.manaraa.com

Mississippi State University
Office of Regulatory Compliance
Post Office Box 6223
Mississippi State, MS 39762

Compliance Division
Administrative Offices
Animal Care and Use (IACUC)
Human Research Protection
Program (IRB)
1207 Hwy 182 West
Starkville, MS 39759
(662) 325-3496 - fax

Safety Division
Biosafety (IBC)
Radiation Safety
Hazardous Waste
Chemical & Lab Safety
70 Morgan Avenue
Mississippi State, MS 39762
(662) 325-8776 - fax

http://www.orc.msstate.edu
compliance@research.msstate.edu
(662) 325-3294

April 15, 2009

April Tanner
336 Monticello Street
Hazlehurst, MS 39083

RE: IRB Study #09-023: A Concept Mapping Case Domain Modeling Approach for Digital Forensic Investigations

Dear Ms. Tanner:

The above referenced project was reviewed and approved via expedited review for a period of 4/15/2009 through 4/15/2010 in accordance with 45 CFR 46.110 #7. Please note the expiration date for approval of this project is 4/15/2010. If additional time is needed to complete the project, you will need to submit a Continuing Review Request form 30 days prior to the date of expiration. Any modifications made to this project must be submitted for approval prior to implementation. Forms for both Continuing Review and Modifications are located on our website at http://www.orc.msstate.edu.

Any failure to adhere to the approved protocol could result in suspension or termination of your project. Please note that the IRB reserves the right, at anytime, to observe you and any associated researchers as they conduct the project and audit research records associated with this project.

Please note that the MSU IRB is in the process of seeking accreditation for our human subjects protection program. As a result of these efforts, you will likely notice many changes in the IRB's policies and procedures in the coming months. These changes will be posted online at http://www.orc.msstate.edu/human/aahrpp.php. The first of these changes is the implementation of an approval stamp for consent forms. The approval stamp will assist in ensuring the IRB approved version of the consent form is used in the actual conduct of research. You must use copies of the stamped consent form for obtaining consent from participants.

Please refer to your docket number (#09-023) when contacting our office regarding this project.

We wish you the very best of luck in your research and look forward to working with you again. If you have questions or concerns, please contact me at jmiller@research.msstate.edu or call 662-325-2238.

Sincerely,

[For use with electronic submissions]

Jonathan Miller
IRB Officer

cc: David A. Dampier

المنارة للاستشارات
www.manaraa.com

APPENDIX B

IRB CONSENT FORM

www.manaraa.com

Consent Form

Title of Study: A Concept Mapping Case Domain Modeling Approach for Digital Forensic Investigations

Study Site: Mississippi State University's Forensic Training Center

Name of Researcher(s) & University affiliation: April L. Tanner and David A. Dampier

What is the purpose of this research project? The purpose of this project will be to understand whether the concept mapping case domain modeling approach will aid in searching and identifying digital evidence and in analyzing the case domain during a computer forensic investigation. The concept mapping case domain modeling approach is a type of computer forensic modeling approach that uses concept maps or visual maps or models to represent the case details and evidence findings in an investigation.

How will the research be conducted? The subject will examine and analyze case details using either an ad hoc approach or the concept mapping case domain modeling approach. The control group will be using the ad hoc or the more commonly used approach during the experiment. The experimental group will use the concept mapping case domain modeling approach to search and identify digital evidence during the experiment. First, the subjects will be given a 30-minute lecture on their respective modeling approaches. Next, the subjects will be presented with a fictitious case and will use their respective approaches to examine and analyze the case. Lastly, the subjects will be given a questionnaire to assess their experience with using the concept mapping case domain modeling approach. The experiment will take 2 to 2.5 hours to complete. An incentive of five additional training hours will be given to those subjects who complete the experiment.

Are there any risks or discomforts to me because of my participation? No. Procedures in the experiment are similar to and pose no more risk than those of the seminar or a real digital forensic examination.

Does participation in this research provide any benefits to others or myself? Yes. The potential benefits of this project will be seen in the ability to locate more digital forensic evidence with, in some circumstances, a less amount of effort and time. This study will not only provide a new method for examining and analyzing case information, but it will also increase the quality of digital forensics investigations.

Will this information be kept confidential? Yes. The participants' names will not be recorded with their responses and examination results. Also, please note that these records will be held by a state entity and therefore are subject to disclosure if required by law.

Who do I contact with research questions? If you should have any questions about this research project, please feel free to contact April Tanner at 601-576-4260. For additional information regarding your rights as a research subject, please feel free to contact the MSU Regulatory Compliance Office at 662-325-2238.

What if I do not want to participate? Please understand that your **participation is voluntary**, your **refusal to participate will involve no penalty or loss** of benefits to which you are otherwise entitled, and you **may discontinue your participation** at any time without penalty or loss of benefits.

You will be given a copy of this form for your records.

_____ _____

Participant Signature Date

_____ _____

Investigator Signature Date

MSU IRB
Approved: 04/15/09
Expires: 04/15/10

www.manaraa.com