1-1-2006

Selecting Keyword Search Terms in Computer Forensics Examinations Using Domain Analysis and Modeling

Alfred Christopher Bogen

SELECTING KEYWORD SEARCH TERMS IN COMPUTER FORENSICS EXAMINATIONS USING DOMAIN ANALYSIS AND MODELING

By

Alfred Christopher Bogen

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 2006

SELECTING KEYWORD SEARCH TERMS IN COMPUTER FORENSICS

EXAMINATION USING DOMAIN ANALYSIS AND MODELING

By

Alfred Christopher Bogen

Approved:

David A. Dampier Associate Professor of Computer Science and Engineering (Major Professor and Director of Dissertation)	Rayford Vaughn Billie J. Ball Professor of Computer Science and Engineering (Committee Member)
Susan M. Bridges Professor of Computer Science and Engineering (Committee Member)	Donna S. Reese Professor of Computer Science and Engineering, Associate Dean of Bagley College of Engineering (Committee Member)
Jeffrey C. Carver Assistant Professor of Computer Science and Engineering (Committee Member)	Edward B. Allen Associate Professor of Computer Science and Engineering and Graduate Coordinator (Committee Member)
Roger King Associate Dean of Research and Graduate Studies	

Name: Alfred Christopher Bogen

Date of Degree: December 8, 2006

Institution: Mississippi State University

Major Field: Computer Science

Major Professor: Dr. David A. Dampier

Title of Study: SELECTING KEYWORD SEARCH TERMS IN COMPUTER FORENSICS EXAMINATION USING DOMAIN ANALYSIS AND MODELING

Pages in Study: 217

Candidate for Degree of Doctor of Philosophy

The motivation for computer forensics research includes the increase in crimes that involve the use of computers, the increasing capacity of digital storage media, a shortage of trained computer forensics technicians, and a lack of computer forensics standard practices. The hypothesis of this dissertation is that domain modeling of the computer forensics case environment can serve as a methodology for selecting keyword search terms and planning forensics examinations. This methodology can increase the quality of forensics examinations without significantly increasing the combined effort of planning and executing keyword searches. The contributions of this dissertation include:

- A computer forensics examination planning method that utilizes the analytical strengths and knowledge sharing abilities of domain modeling in artificial intelligence and software engineering,
- A computer forensics examination planning method that provides investigators and analysts with a tool for deriving keyword search terms from a case domain model, and

- The design and execution of experiments that illustrate the utility of the case domain modeling method.

Three experiment trials were conducted to evaluate the effectiveness of case domain modeling, and each experiment trial used a distinct computer forensics case scenario: an identity theft case, a burglary and money laundering case, and a threatening email case. Analysis of the experiments supports the hypothesis that case domain modeling results in more evidence found during an examination with more effective keyword searching. Additionally, experimental data indicates that case domain modeling is most useful when the evidence disk has a relatively high occurrence of text-based documents and when vivid case background details are available.

A pilot study and a case study were also performed to evaluate the utility of case domain modeling for typical law enforcement investigators. In these studies the subjects used case domain models in a computer forensics service solicitation activity. The results of these studies indicate that typical law enforcement officers have a moderate comprehension of the case domain modeling method and that they recognize a moderate amount of utility in the method. Case study subjects also indicated that the method would be more useful if supported by a semi-automated tool.

DEDICATION

This research is dedicated to the memory and legacy of Dr. Brad Carter, who was the author's first computer science and software engineering instructor at Mississippi State University's Computer Science and Engineering Department. Not only did Dr. Carter make many significant contributions to the CSE department, but his excellent work in the classroom helped countless students (such as the author) become more mature and disciplined programmers and engineers. The author submits this dedication to Dr. Carter as an expression of respect and gratitude.

ACKNOWLEDGMENTS

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

- The author's entire family,
- The author's PhD advisor, academic mentor, and constant source of moral support and solace,
- The author's PhD committee and all of MSU's CSE instructors who contributed to the author's education,
- The Mississippi State Attorney General's Office (MSAGO) Cyber Crime Unit,
- USACE ERDC supervisors and colleagues, and
- Countless friends, acquaintances, mentors, and musical collaborators.

TABLE OF CONTENTS

CHAPTER Page

CHAPTER Page

LIST OF TABLES

TABLE Page

TABLE Page

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Computer forensics is a discipline that has been practiced for many years by computer administrators, law enforcement officers, and other practitioners. A computer forensics investigation typically involves the generic activities of incident identification, media collection, media examination, evidence analysis, and evidence presentation. The topic has more recently emerged as a popular subject of computer security and information assurance research. The motivation for computer forensics research includes the increase in crimes that involve the use of computers, the increasing capacity of digital storage media, a shortage of trained computer forensics investigators and technicians, and a lack of computer forensics standard practices.

The hypothesis of this dissertation is that domain modeling of the computer forensics case environment (known as case domain modeling) can serve as a methodology for selecting keyword search terms and planning forensics examinations. This methodology can increase the quality of forensics examinations without significantly increasing the combined effort of planning and executing keyword searches. The hypothesis is discussed in more detail in Section 1.4.

Case domain modeling supports computer forensics examination planning by providing a structured approach to analyzing, filtering, and specifying the case information that will be required for conducting an examination. The case domain model

is an organized representation of information about the case domain that will be required for a computer forensics examination. This document describes a methodology for planning a computer forensics examination and deriving appropriate keyword search terms using domain modeling.

The remainder of this chapter is organized as follows: Sections 1.1 and 1.2 summarize the scope of computer forensics research and practice, Section 1.3 discusses the motivations for this dissertation, Section 1.4 presents the hypothesis of this dissertation, Section 1.5 highlights the contributions of this dissertation, Section 1.6 discusses practical applications of this dissertation research, and Section 1.7 provides an overview of the remainder of this document.

1.1 Digital Forensics Defined

Digital forensic science is an emerging scientific discipline defined by the First Annual Digital Forensics Research Workshop in 2001 as:

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purposes of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations [52].

Digital forensic science is not yet a mature scientific discipline because it has not yet exhibited the required characteristics of a scientific discipline: theory, abstractions and models, elements of practice, corpus of literature and professional practice, and confidence/trust in results [52].

Digital forensics can be further divided into three major areas:

- Computer forensics: Collecting, analyzing, and preserving evidence from digital storage media,
- Network forensics: Collecting, analyzing, and preserving evidence that is spread throughout a network of computers, and
- Software forensics: Determining the identity of the original author of a piece of software, malware, virus, malicious code, etc.

This dissertation focuses exclusively on computer forensics, with a primary emphasis on the *examination* activity in a generic computer forensics process. Support is also provided for the *preservation*, *analysis*, and *presentation* activities that occur in a generic computer forensics process.

1.2 The General Computer Forensics Process

Although there is no widely adopted standard process model for computer forensics [49, 57, 74], a variety of process models have been proposed [4, 6, 19, 22, 31, 48, 52, 57, 64, 66, 70]. These process models generally include the abstract phases of identification, collection, examination, analysis, and presentation. This dissertation adopts the Digital Forensics Research Workshop (DFRWS) model of the investigative process [52] illustrated in Figure 1.1 (an adaptation of the original figure) as a framework for the specific model of the examination activity. This model of the complete process was chosen because it was developed by a group of workshop members from academia, law enforcement, and private industry. Sections 1.2.1–1.2.6 describe each phase of the DFRWS model of the computer forensics investigation process.

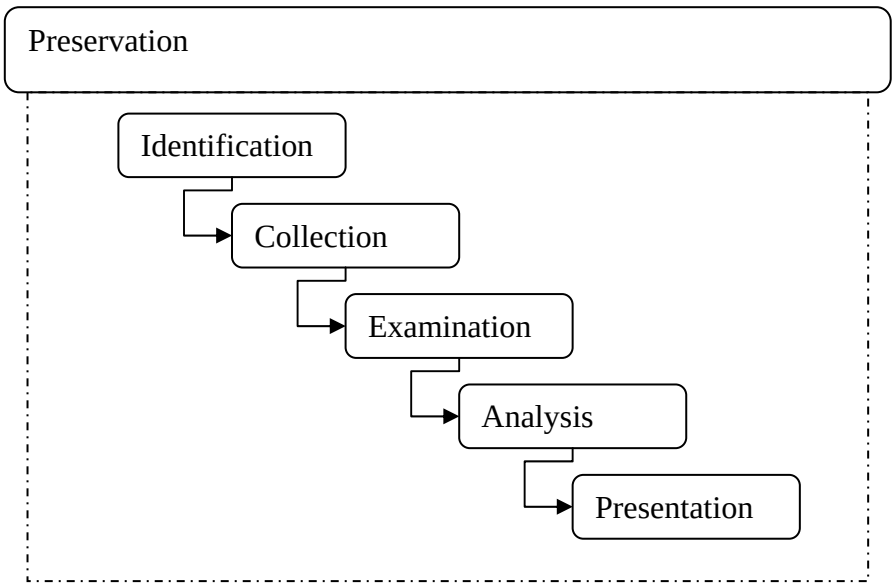


Figure 1.1 The DFRWS Digital Investigation Process

1.2.1 Preservation

The preservation phase can be regarded as an umbrella activity because it is not really a stand-alone phase. The preservation "phase" is actually a set of activities that are continually practiced during the identification, collection, examination, analysis, and presentation phases. Hence, the rounded rectangle in Figure 1.1 that is labeled "preservation" encloses all other process activities (illustrated with a dotted rectangle). Preservation activities are concerned with ensuring that the evidence is handled properly to guarantee validity in a court of law. For example, the chain of custody must be documented and maintained throughout the entire investigation. In cases that do not involve legal proceedings, many preservation practices can be omitted. Computer forensics cases that

may not involve legal proceedings include data recovery, time-critical combat zone military intelligence gathering, and network security incident root cause analysis.

1.2.2 Identification

In the identification phase, a crime or incident is detected or reported to the relevant authorities, who may be law enforcement officers, chief information officers, security officers, corporate managers, or incident response centers. The crime may fall into one or more of the following categories: a crime committed against a computer system, a crime where a computer or other digital device is an instrument, or a non-computer-related crime where the suspect is assumed to have information of evidentiary value stored on computers, disks, or other digital devices [42]. At the end of the identification phase, the relevant authorities determine whether or not it is appropriate to proceed with a computer forensics investigation.

1.2.3 Collection

The activities of the collection phase are twofold: 1) physically seizing the involved computers or digital devices, and 2) digitally copying (imaging) the data from the seized computers or digital devices. “Computers or digital devices” may include but are not limited to: digital cameras, digital video recorders, personal digital assistant devices (e.g. Palm Pilots), hard drives, floppy disks, cell phones, answering machines, laptop computers, desktop computers, large computers (e.g. servers), memory cards, and pagers [70]. Investigators generally prefer not to confiscate entire computing configurations unless they contain contraband materials (e.g. child pornography and

pirated software) or will enable the suspect to continue conducting malicious activities (e.g. phishing scams). Instead, they prefer to seize only the storage media contained in the devices, and in minimal threat situations, investigators may image the media onsite without confiscating any computing devices or media.

The investigators may be required to obtain a search warrant or an official consent to search in order to legally seize digital evidence. Assuming that the proper legal procedures have been followed, handling electronic evidence at the crime scene typically involves:

- Recognition and identification of the evidence,
- Documentation of the crime scene,
- Collection and preservation of the evidence, and
- Packaging and transportation of the evidence [1, 6, 19, 22, 31, 42, 48, 70].

One of the most important rules in criminal computer forensics cases is that analysis or examinations are not performed on the original media [25, 31, 42, 52]. Instead, technicians perform examination on bit-stream images of the original evidence. In most cases, two images of the original evidence are obtained: one image is for working with tools and software that do not necessarily preserve the disk's integrity, and the other image is maintained as an unaltered copy and is for previewing using only tools that preserve the disk's integrity [42].

A bit-stream image not only contains all of the files on the digital media or hard drive, but also contains data that is hidden in free space and slack space. This topic is discussed in more detail in Section 1.2.4. In criminal cases, once bit-stream images are

obtained, the original evidence is securely stored and is only digitally accessed in very special circumstances (e.g. if the images are lost or destroyed).

1.2.4 Examination

The examination phase typically accounts for the greatest amount of effort in a digital investigation. Likewise, examination is the primary focus of this dissertation. During the examination phase, forensic technicians explore bit-stream images and sometimes original source storage devices in order to find interesting or relevant digital evidence. The Alameda County District Attorney's Office in California claims that it can take approximately four hours to exhaustively examine a single 1.4-MB (megabyte) removable disk, and it can take about three days to exhaustively examine an 8-GB (gigabyte) hard drive [1]. At the present time, a computer forensics technician will likely be required to examine a suspect's personal computer that often contains over 100 GB of storage capacity.

Most digital evidence is recovered by examining and searching files that are "stored in plain sight"; that is, they are accessible via a logical directory structure and are not obscured by advanced data-hiding methods. The type of investigation will determine what files may be most useful: text files, video files, image files, audio files, etc. Because it is very time consuming to manually examine all files on a hard disk, keyword searches and other data filters are applied to efficiently locate evidence [1, 5, 16, 26, 48, 49]. Files may contain interesting keywords, or they may have interesting or suspicious names.

If the suspect is clever, then he/she may have attempted to hide evidence in "plain sight" using a variety of methods:

- Steganography: This technique allows the user to hide data (e.g. text messages or other graphics) inside a graphics file. Special software must be used to detect the presence of steganography and extract the hidden data. Such detection is exceptionally difficult with current technology.

- Encryption: Encrypted files are password protected, and the original contents are obscured by the encryption algorithm. The password must be recovered or cracked in order to decrypt and view the hidden data.

- Changes in the file extension: An incorrect file extension will render the file unreadable. For example, if a suspect is attempting to hide a .pdf file *plan.pdf*, he/she may change the file extension so that the file is named *plan.exe*. To view the original file, a user must be change the file name back to *plan.pdf*.

- Use of non-suspect file names: It is unlikely that a clever suspect will use obvious filenames such as *terroristplan.txt* or *HowIMurderedMyWife.pdf*. Instead the clever suspect may use seemingly innocent file names such as *cakeRecipe.txt, MobyDick.pdf,* or *MyCar.jpg*.

Examination activities are not only directed towards visible files but may also be directed towards free space and slack space. Free space consists of areas, known as clusters, on storage media where new data may be recorded. The size of a cluster is a fixed characteristic of the media and the file system. A file occupies one or more clusters, and the number of clusters is determined by the file size divided by the cluster size. Since only whole clusters may be used, the number of required clusters must be rounded up if the file size is not evenly divisible by the cluster size. For example, if the cluster size is set to 64 kilobytes and the file size is 363 kilobytes, then the file will occupy 6 clusters (363/64 = 5.671875, rounded up to 6). When a file is "deleted," it remains in one or more clusters until portions of other files are written to the same clusters. The unused portion of the final cluster is usually not overwritten and is known as slack space. Commercial computer forensics tools allow investigators to easily view data left in free space and

slack space. Useful data is usually more difficult to recover from slack space because only a portion of one cluster of the file is recovered.

1.2.5 Analysis

Once evidence is identified, it must be analyzed in order to establish the chain of events, relationships between physical and digital evidence, and criminal intent. A collaborative team consisting of lawyers, investigators, and forensics technicians may analyze the evidence. In some cases information extracted from the analysis phase may cause the investigator to revisit previous phases of the investigation process to obtain more evidence. Establishing a chain of events may be challenging if the evidence was obtained from a variety of sources. The systems that originally contained the evidence may be from different time zones, they may have unsynchronized system times, and the suspect may have intentionally tampered with the system time to create misleading file creation times.

1.2.6 Presentation

At the end of the computer forensics process the investigators review and revise their notes and, if necessary, write reports describing their investigative efforts. In legal cases the digital forensics investigator will likely testify as an expert witness. To serve as effective expert witnesses, computer forensic technicians document their work. A legal proceeding may take place a year or several years after the forensic examination, and in such cases detailed documentation is invaluable to expert witnesses and to the legal case [3]. Computer forensics documentation must not only provide a complete and consistent

representation of the computer forensics process, but it must also support a presentation that is clear and comprehensible to a layperson. To some extent the procedures that investigators follow and document must also be comprehensible to a layperson.

1.3 Motivation

While violent crimes such as armed robbery are decreasing in the U.S., computer crime[1] is becoming more prevalent worldwide [4, 36, 49, 75]. The growth of the Internet has contributed to an increase in cyber-crimes such as child pornography, gambling, money laundering, financial scams, extortion, and sabotage [8, 40, 75]. From teenage network hackers and corporate executives to child pornographers and terrorists, the computer has attracted a potpourri of offenders with various skills, motives, experiences, and nationalities [29, 33, 56].

Besides using a computer in the commission of a crime, computer criminals share another similarity: the chances of being detected, reported, caught, and/or prosecuted are relatively small [36]. In an extreme case of misfortune, a sheriff's department investigator working exclusively on computer crimes full-time for five years only made five arrests, none of which led to convictions [69]. Though the FBI has attempted to encourage reports of computer crimes against business infrastructures, law enforcement sometimes seems to respond apathetically towards small-business victims [29, 60]. These small-business victims may be ignored because of a heavy backlog of computer forensics cases. Additionally, large-business victims may be reluctant to report computer crimes for fear

[1] Computer crime is generally defined as either a crime involving the use of a computer to commit the crime or a crime in which a computer is the victim of the crime.

that it would result in a lack of confidence among stockholders. Many businesses are more interested in getting their systems running again than in prosecuting the criminals responsible for the incident [45].

While computer crime is increasing, computer forensics technicians are scarce [40]. This shortage of certified personnel is an obvious cause of computer forensics case backlogs. Civilian computer forensics firms are only beginning to emerge as profitable solutions to the need for more personnel. There are also secondary contributing factors: the constant growth of digital storage media capacity and the lack of standard technical methodologies for computer forensics [1, 5, 18, 52, 62]. When searching for textual evidence on an aggregation of media that may exceed a terabyte (1000 GB), it may be insufficient to rely on ad hoc examination planning techniques and best-guess keyword search techniques for finding evidence [5]. In cases that involve corporate or organizational scandals, the aggregation of digital media may easily exceed several terabytes of data. In a panel presentation at the 2006 National Colloquium on Information Systems Security Education, an FBI agent working on the Enron case claimed that there was in excess of 3 terabytes of digital media that had to be examined. Documented policies and procedures for digital investigation emphasize the importance of planning a forensic examination (including keyword searches) but do not offer detailed guidelines for producing this plan using a structured process or methodology. Instead, organizations adopt “home-grown” techniques for planning their examinations. Such non-standardization has gained the attention of researchers and practitioners of computer forensics [52].

The inexperience of local law enforcement agencies (with respect to computer forensics), the lack of standard computer forensics methodologies, the constantly increasing digital storage capacity, the growing prevalence of digital devices, and the "hidden"[2] nature of computer crimes all contribute to the need for advancements in computer forensics research and practice. As a first step in addressing these problems, a group of researchers and practitioners of digital forensics attending the first Digital Forensics Research Workshop (DFRWS) in 2001 outlined a roadmap for digital forensic research [52]. DFRWS developed several research goals, including developing standard methodologies and techniques, creating tools that are aligned with the DFRWS computer forensics process definition, and building computer forensics expertise.

1.4 Hypothesis

The hypothesis of this dissertation is that domain modeling of the computer forensics case environment (known as case domain modeling) can serve as a methodology for selecting keyword search terms and planning forensics examinations. This methodology can increase the quality of forensics examinations without significantly increasing the combined effort of planning and executing keyword searches.

Case domain models represent the information domain of the computer forensics case, and the goal of developing the case domain model is to define the scope of case information that will be required during a computer forensics examination. Case domain models are generalized ontology/domain models that may be reused in similar cases.

[2] Computer crime is hidden because a law enforcement officer is less likely to intercept a computer crime in progress, unlike more visible crimes such as traffic violations, robbery, and assault.

These generalized ontology models are instantiated when they are "filled-in" with information from a specific case. For example, a case domain model may include a generalized *Suspect* concept that has the *name* and *birthday* descriptive attributes. These *name* and *birthday* attributes of the generalized *Suspect* concept may be instantiated with values such as *John Doe* and *January 1, 1970*.

A methodology for selecting keyword search terms describes how a comprehensive list of keyword search terms may be derived from selected elements of the case domain model. The case domain modeling approach to planning is an improvement over current, established approaches to keyword search planning and examination planning. Those established approaches to examination planning and forensics keyword search planning are discussed in Chapter II of this document. Evaluation of the hypothesis is based on the research questions in the following three paragraphs.

Does the case domain modeling methodology result in an increased amount of evidence found in an examination? Generally speaking, the amount of evidence found in an investigation determines the quality of the case. Evidence is the foundation upon which legal cases are built, and the amount of evidence can determine the strength of the prosecution or defense. In computer forensics, an item of evidence is typically a single file that the examiner has tagged because of its relevance to the underlying facts and circumstances of the case. Experiments were performed to measure the amount of evidence found in the established approach and the case domain modeling methodology for planning forensics keyword searches. Students from the fall 2005 Introduction to

Cybercrime and Computer Forensics (CSE 4273/6273) class and the summer 2006 Special Topics in Computer Forensics (CSE 8990) class were recruited for these experiments.

Does the case domain modeling methodology require a significant amount of additional effort when compared to a typical approach? It is assumed that the methodology may require investigators and forensics technicians to spend more time planning the keyword search examination than is required by established planning approaches. Ideally, the methodology will not require a significant amount of additional effort in order to improve keyword search results. It may also be the case that the increased time investment during the planning stages may decrease the typical amount of time spent executing keyword searches; the time taken to conduct an ad hoc, trial-and-error keyword search may exceed the amount of time that could have been spent building a structured keyword search plan. Analysis of the experiments compares the amount of effort spent planning and conducting keyword searches using an ad hoc approach and using the case domain modeling methodology.

Is the case domain modeling method useful for typical law enforcement investigators who participate in cases involving computer forensics? Traditionally, computer forensics practitioners have come from careers in criminal justice and law enforcement with limited previous computer or information technology experience. The increase in the occurrence of cyber-crimes and the growing demand for digital forensics technicians is extending recruitment to persons who originate from careers in computer science, software engineering, and information technology with limited previous criminal

justice or law enforcement experience. It is expected that practitioners with the latter, more computer-science-intensive background would have fewer difficulties understanding the ontology modeling foundations of the case domain modeling methodology than those practitioners with the former, more law-enforcement-intensive background. However, it is important to determine whether or not typical investigators and practitioners from a non-technical background can effectively understand and apply the fundamental ontology modeling concepts in the methodology. Though typical practitioners may be unfamiliar with the theoretical foundations of the methodology, it is likely that they could understand its purpose and populate an abstract case domain model. Two law enforcement practitioner case studies were performed to address this research question. In these studies the case domain model supported the investigators in a digital forensics service solicitation activity. After the activity the subjects were surveyed regarding their experience and opinion of case domain modeling. These subjects were recruited from the law enforcement computer forensics training courses offered at the Mississippi State University Department of Computer Science and Engineering Computer Forensics and Cybercrime Training Center.

1.5 Contributions

This dissertation provides evidence that case domain modeling is a useful framework for planning and executing computer forensics examinations. The general contributions provided by this dissertation are listed below.

- *A method for applying ontology modeling to computer forensic examinations.* Thus far, the potential utility of ontology modeling has been largely unrealized in the domain of computer forensics. This dissertation applies

ontology and domain modeling to computer forensics examination planning. In this dissertation, a case domain modeling approach is applied to the task of keyword search selection and other examination planning tasks. As ontology or domain modeling is shown to be useful for extracting useful keyword search terms, other related computer forensics applications of ontology/domain modeling may be explored. Case domain models can also be useful for learning how general forensics case types are distinct from one another. Finally, the structured characteristics of the case domain modeling framework can also enable the establishment of a knowledge base for semi-automated tools.

- *A methodology for deriving computer examination keyword search terms from a case ontology*. Though many tools exist for executing and logging the results of keyword searches, such tools are not supported by a structured methodology for selecting keyword search terms. The methodology for keyword search term selection offers an improvement over the typical, ad hoc method for planning forensics keyword searches. Experimental results evaluate the claims that this methodology can improve the quality of keyword searches.

- *Experimental evidence that indicates utility for modeling language methodologies in computer forensics*. Existing and current research in computer forensics modeling has not yet offered substantial experimental data indicating a utility for the prescribed approach. This dissertation describes a case domain modeling methodology that support examination planning and offers conclusions based on experiments using quantitative and qualitative measures. This dissertation's experimental design may be replicated and reused by other computer forensics modeling and tool researchers. Finally, positive experimental results produced by this dissertation may provide the motivation for the refinement and ultimately the establishment of related ready-to-use computer forensics modeling approaches.

Thus far, the evolution of this research topic has been chronicled in one journal article and three conference papers authored by Bogen and Dampier [9-12]. Two of those conference papers were exclusive to the digital forensics community: the Digital Forensics Research Workshop (online proceedings) and the First International Workshop on Systematic Approaches to Digital Forensic Engineering (IEEE sponsored with published conference proceedings) [9, 10]. Results of this research work will be

submitted to computer forensics journals such as *Digital Investigation* and the *International Journal of Digital Evidence*. Conferences in the domain modeling and ontology modeling communities may also be suitable targets for additional publications.

1.6 Practical Applications

A computer forensics modeling process may be beneficial to both law enforcement and civilian computer forensics firms. In a law enforcement organization a cyber-crime investigator handles the case before a computer forensics technician extracts the digital evidence. The investigator is a law enforcement officer who assumes the role of an information expert of case details, while the computer forensics technician is a technology expert who offers an independent examination and analysis of digital media. In such situations the responsibilities of the cyber-crime investigator include obtaining subpoenas and warrants, executing arrest and search warrants, interviewing suspects and victims, documenting the underlying facts and circumstances of a case, collaborating with other law enforcement officers, and providing the computer forensics technician with necessary case details. The forensics technician schedules an examination of the digital media based on current case backlog and case priority. The amount of digital evidence recovered is highly dependent on the investigator's ability to analyze the case and offer the most relevant details to the forensics technician.

A cyber-crime investigator could use a computer forensics case domain modeling methodology to assist in analyzing the case, forming hypotheses, defining the scope of the investigation, identifying evidence sources, and deriving keyword search terms. The modeling artifacts may provide the forensics technician with sufficient information to

perform the media examination. Once a case model is constructed, it may be generalized and reused on similar cases. Reuse of modeled case knowledge can improve the productivity of the investigator and provide the forensics examiner with a standardized representation of case facts. This generalized format can help facilitate information sharing between agencies and provide protection against leaking confidential or sensitive case-specific data; agencies may share generalized search strategies and forensics knowledge with partner organizations without providing the confidential details of a case. The case domain modeling methodology can also contribute to the training of novice or beginner investigators who are adapting their analytical skills to cyber-crime cases. A case domain modeling methodology can provide a structured approach to case analysis and provide investigative tips. Expert investigators may also benefit from using this structured approach when they encounter unfamiliar crimes or unusually complex cases that involve an abundance of digital media and a network of suspects. The modeling methodology is designed such that an investigator with intermediate computer skills and little or no background in engineering can model his/her investigative knowledge.

Like law enforcement agencies, private or civilian agencies can reap similar benefits from the application of a modeling methodology. The characteristics of civilian computer forensics firms that distinguish them from law enforcement agencies include the absence of personnel exclusively allocated to investigative work, the necessity for marketing strategies and profit delivery, an increased diversity of cases that may or may not involve legal proceedings, and the increased likelihood that personnel will not originate from a legal or law enforcement background. It is likely that many computer

science, software engineering, and information technology practitioners will attempt to establish computer forensics firms to profit from the demand for computer forensics services. Such individuals will likely serve dual roles as investigator and computer forensics technician. An examination planning methodology has the potential to be highly beneficial to these technology-oriented personnel who have little experience conducting any criminal or private investigations; the methodology provides a familiar, structured framework that serves as an analytical investigative tool. Computer scientists and software engineers should have little difficulty using a computer forensics modeling methodology if they are already familiar with software modeling methodologies.

The emergence of the computer forensics discipline has created a new demand for intelligent computer forensics software tools. Like other software developers, computer forensics tool vendors must understand the application domain in order to deliver quality software. Case models created by computer forensics investigators can be useful sources of domain knowledge for developers of computer forensics tools. Such domain models can be formalized as components of data-mining applications, knowledge-based applications, and other intelligent software applications.

1.7 Organization

The remainder of this document provides the background and details of this dissertation research work. Chapter II provides a review of related work in the areas of computer forensics, artificial intelligence, and software engineering. Chapter III describes the case domain modeling method. Chapter IV presents the results of the first two experimental trials of case domain modeling for examination planning and execution. An

additional case domain modeling experiment was planned based on the analysis of the first two experiments. Chapter V presents the results of this third and final trial of case domain modeling applied to examination planning and execution. Chapter VI presents the results of two case studies that evaluate the utility of case domain modeling to forensics service solicitation by law enforcement investigators. Finally, Chapter VII presents conclusions and identifies potential areas for future research.

CHAPTER II

RELATED WORK

This chapter presents a survey of literature and research work related to this dissertation. The following topics are explored in this chapter: computer forensics modeling, computer forensics standard practices, ontology modeling in artificial intelligence, and domain analysis and modeling in software engineering.

2.1 Modeling Approaches in Computer Forensics

Modeling languages present opportunities for improving computer forensics practices, but practitioners are not using them. Most computer forensics investigators appear to rely on home-built methods using commercial software packages such as *Encase*[3] or *Forensics Toolkit*[4]. Furthermore, only a limited amount of research on the use of modeling approaches in computer forensics has been published. This section of the literature review documents the existing and current work of researchers and practitioners who have contributed to modeling languages and modeling concepts in computer forensics.

[3] Encase is a registered trademark of Guidance Software, Inc.
[4] Forensics Toolkit is a registered trademark of Access Data, Inc.

2.1.1 Process Modeling Approaches

A number of process modeling approaches for computer forensics have been developed. The term “process” may refer to a process of events that occur in a network incident, or it may refer to a prescribed general investigative process.

2.1.1.1 The Digital Investigation Process Language

Peter Stephenson’s proposal for a Digital Investigation Process Language (DIPL) offers the first research in the application of a modeling language to computer forensics process modeling. DIPL is a component of Stephenson’s larger concept for an End-to-End Digital Investigation (EEDI) Process [63, 66]. Practitioners may specify the chain of events that occur in an incident that requires digital forensics using DIPL. DIPL was adapted from the LISP (LISt Processor) language, and it can be used to specify template investigative processes and document the process followed in an investigation [67]. Stephenson has illustrated how DIPL may be applied to conducting digital incident postmortems on network systems. DIPL and EEDI focus primarily on network forensics investigations [65].

Figure 2.1 provides a simple example of DIPL applied to a digital incident postmortem investigation. A postmortem investigation attempts to discover the cause of a network or computer system failure. The example provides a specification of the process followed for identifying a network incident. DIPL provides a more formal specification of events than the corresponding natural language event description in Figure 2.1.

DIPL Code Listing

```
(And
  (Report
        (When
          (Time [19:23:00 GMT 04 05 2004])
        )
          (Observer
                (RealName 'John Smith')
        )
        (Change State
          (OldState 'Normal network operation'
                (ArchitectureName 'CSE Network')
          )
          (CurrentState 'Web server crashed – network overloaded'
                (ArchitectureName 'CSENetwork')
          )
          (When
                (Time [10:30:00 GMT 02 05 2004])
          )
  )
  (ByMeansOf
        (Attack
          (AttackSpecifics
                (AttackNickName 'Unknown Denial of Service Attack')
                      (Comment 'Probably Zombie Attack')
                      (BeginTime [10:20:35 02 05 2004])
                      (EndTime [10:24:28 02 05 2004])
                (Target
                      (Host Name 'WEBServer-1')
                      (UDPPort 1444)
                )
         )
   )
 )
)
```

Corresponding Natural Language Description

A web server on the CSE network crashed at 10:30 GMT on May 2, 2004. This incident was observed at 19:23 GMT on May 4, 2004 by John Smith. The attack is assumed to be caused by a zombie-style denial of service attack that occurred at the web server on UDP port 1444 between 10:20 and 10:24 GMT on May 2, 2004.

Figure 2.1 DIPL Example

2.1.1.2 Investigative Process Models

Investigative process models (sometimes simply referred to as process models) define a sequence of generic activities or phases that characterize general approaches to computer forensics investigations. A variety of computer forensics process models have

been proposed in the literature, and the topic remains popular in current computer forensics research literature [4, 6, 19, 22, 31, 48, 52, 57, 64, 66, 70].

This dissertation assumes that investigators follow a process model similar to the DFRWS investigative model [52]. This process model was described in Section 1.2 of this document. The DFRWS process model has been selected because members of the academic, law enforcement, and software development communities collaborated to develop it. Other process models provide enhancements to the relatively simple DFRWS process model. Reith et al. proposed a DFRWS abstract process model that enhances the DFRWS model by inserting two phases between the identification and preservation phases of the DFRWS model: preparation and approach strategy [57]. Carrier and Spafford proposed a more radical enhancement to the DFRWS model by integrating physical crime scene investigation activities into the model [19]. Carrier and Spafford's process model contains 17 phases that are grouped into 5 categories: readiness phases, deployment phases, physical crime scene investigation phases, digital crime scene investigation phases, and review phases. This model also allows investigators to revisit some of the physical and digital crime scene investigation phases. Baryamureeba and Tushabe enhanced Carrier and Spafford's model by allowing the investigators to revisit any of the five categories[5] of process phases [7]. Revisiting phases may be necessary if new evidence is found or if investigators determine that an alternative investigative strategy must be developed and implemented.

[5] Baryamureeba and Tushabe also reorganized Carrier and Spafford's phase categories by replacing the digital and physical crime scene investigation phases with the trace back and dynamite phases. However, Baryamureeba and Tushabe's model places physical and digital crime scene activities in all five of their phase categories.

A more detailed comparison of computer forensics process models is omitted from this literature review because this dissertation presents a modeling approach that is not highly dependent upon the chosen process model. The methodology described in this dissertation may occur in any computer forensics process model that includes activities similar to the examination phase of the DFRWS model.

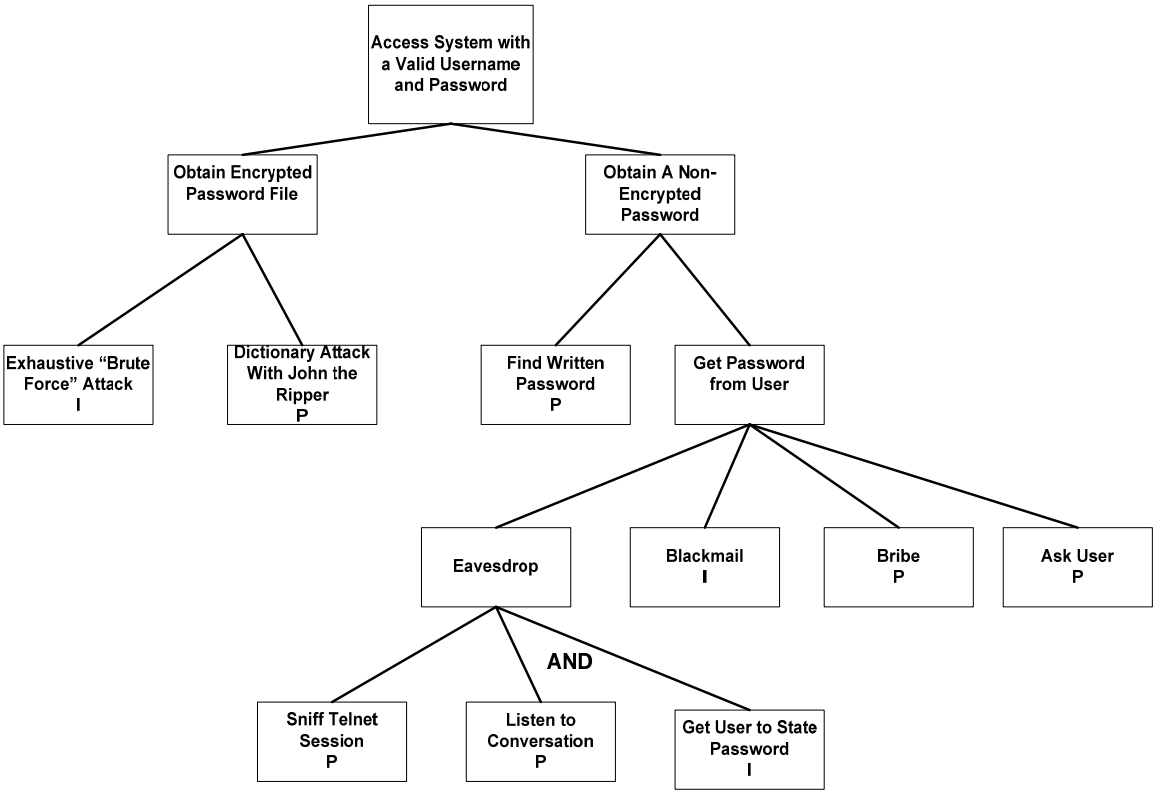
2.1.2 Hypothesis Modeling Approaches

Hypothesis modeling approaches to computer forensics provide expressive tools for representing a general hypothesis of an incident and decomposing this hypothesis into a collection of supporting hypotheses. The goals of hypothesis modeling approaches include understanding adversary tactics, identifying the state of an attack, classifying adversarial resources, or representing and reusing investigative knowledge.

2.1.2.1 Attack Trees

In 1999 Schneier introduced the concept of attack trees for modeling threats against computer systems [59]. Schneier claimed that "if we can understand all the different ways in which a system can be attacked, we can likely design countermeasures to thwart those attacks" (page 21). Though Schneier did not mention the term "forensics" in his work, his attack trees are applicable to digital forensics.

In an attack tree structure, the root node represents the goal of the attack, and the leaf nodes represent various ways to achieve the goal. Figure 2.2 presents an example attack tree for gaining unauthorized access via a password. The leaf nodes in the example are labeled as possible (P) or impossible (I), indicating the feasibility of the corresponding



(Key: I = Impossible, P = Possible)

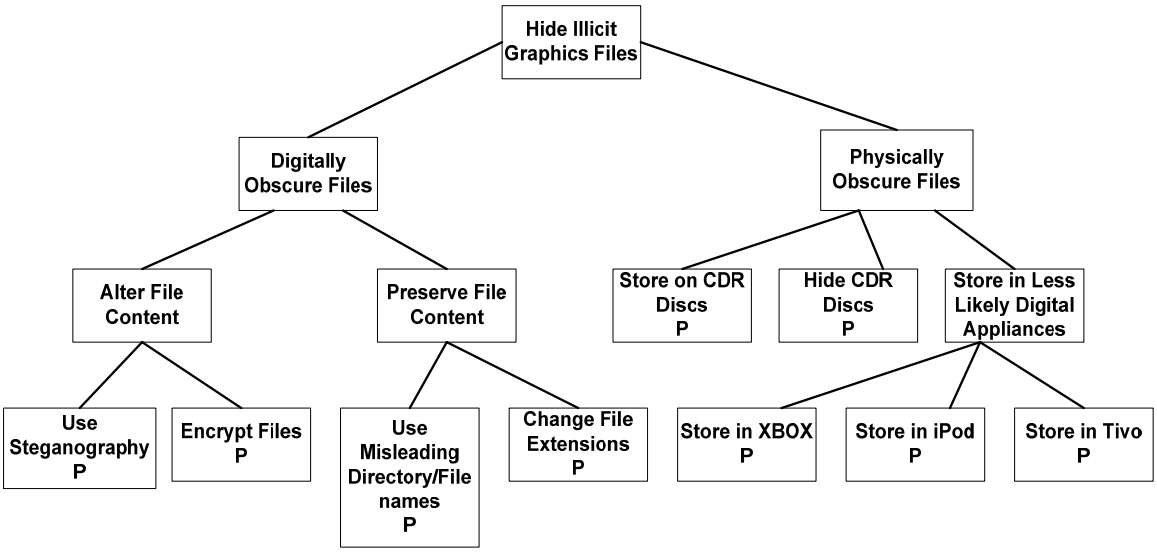
Figure 2.2 Attack Tree Example

action. The leaf nodes may be labeled using other schemes, such as monetary cost, amount of time, and amount of special equipment required.

Attack trees may be especially helpful when conducting network forensics postmortems. In postmortem investigations it is important for the investigator to consider all attack options and form a hypothesis that specifies the most likely attack. Attack trees offer a structured method for considering attack options and may result in a more complete analysis of possible attacks. Attack trees also document an investigator's analysis using a relatively easy-to-comprehend illustration. The investigator may quickly

refer to an attack tree to maintain focus during a tiresome investigation that involves examining hundreds of network log entries.

Attack trees may also be applied to computer forensics media analysis (Figure 2.3) if the investigator wishes to form hypotheses regarding how a clever suspect may have hidden data. Such an application of attack trees has not been discussed in existing



(Key: P = Possible)

Figure 2.3 Computer Forensics Attack Tree Example

literature. However, computer forensics hypothesis modeling approaches such as adversary modeling and forensics graphs are similar in several respects to attack trees [17, 44].

2.1.2.2 Adversary Modeling

Lowry et al. indicated the need for an adversary modeling technique for developing forensic observables that indicate the state of a malicious network attack [44]. The goal of adversary modeling is to "hypothesize potential adversaries or malicious acts, identify threats and adversary missions, identify the means that would have to be used or have a high probability of being used, and develop observables for those means" [22, 44]. Their adversary modeling approach is similar to the attack tree method, but adversary modeling is more specialized. Lowry et al. identified the need for a modeling approach that attempts to classify potential network system adversaries and identify their skills, resources, motivations, and attack processes. Table 2.1 presents a classification of potential adversary actors as presented by Lowry et al. [44]. Actors in Classes III and IV typically possess more resources and more devastating goals than actors in Class I. Furthermore, "an adversary will not use his most valuable or sophisticated techniques or methods unless there is sufficient payoff" [44].

Lowry et al. claimed that existing computer forensics tools and methods have been insufficient for delivering "observables" related to Class III and Class IV adversaries. Lowry et al. assumed that all attackers follow a generic attack process that includes the following phases: intelligence gathering, system discovery, detailed preparations, testing/practice, and attack execution. Assuming that a known adversary is conducting or planning an attack, the defenders of a system may identify forensic observables such as the current state of the attack and transitions between states in an

attack. Lowry et al. suggested that an attack graph representation similar to the attack tree may be used to represent the states and transitions of an attack.

Table 2.1 Adversary Classes

Class	Named Actors
IV	First-world and certain second-world countries, including military and intelligence agencies. Future terrorist organizations. Future organized criminal groups. Some types of insiders.
III	Almost every country not in the Class IV category. Some terrorist organizations. Some organized criminal groups. Some types of insider. Some types of radical organizations.
II	Very few countries. Many terrorist organizations. Many organized criminal groups. Many types of insiders. Many types of radical groups. Very expert hackers and hacker coalitions.
I	Some terrorist organizations. Some organized criminal groups. Many types of insiders. Many types of radical groups. Beginner to journeyman hackers.

The nodes of an attack graph represent states (pre- and post-conditions), and the edges represent attack activities that cause state transitions. This approach complements attack trees because adversary modeling focuses on *if* a goal state has been achieved, while attack trees focus on *how* an adversary may achieve a goal or certain state.

Lowry et al. emphasized that adversaries spend the majority of their time gathering intelligence, making detailed preparations, and testing and practicing. Class III and Class IV adversaries typically execute more sophisticated attacks and hence spend more time planning and gathering intelligence. Defenders must find evidence left behind from an attacker's intelligence gathering and preparation activities in order to observe the current state or a state transition of the attack. Lowry et al. concluded that future forensic

methods and tools must be based on an understanding of adversary characteristics, behavior, goals, and techniques. Analyzing evidence without the context offered by adversary modeling may fail to produce the forensic "observables" described by Lowry et al.

2.1.2.3 Forensic Graphs

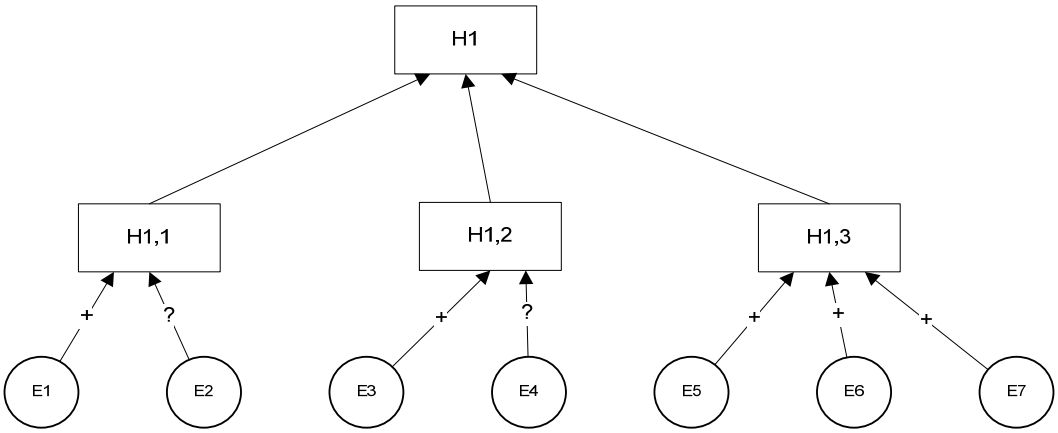
Bruschi and Monga proposed a methodology for "archiving, retrieving, and reasoning about computer forensics knowledge." Bruschi and Monga's work is based on the assumption that common patterns exist in crimes that can be exploited to ease the work of investigators [17]. They proposed a hypothesis framework that accompanies the following investigative process followed by detectives: "formulate a hypothesis on the state of the world that caused the case, collect evidence on the basis of these hypotheses, correlate actual evidence with hypotheses, and adjust hypotheses, and repeat the process until the consistency state of the knowledge about the case is sensibly high" [17] .

Bruschi and Monga formalized their modeling approach by defining a forensic graph. The forensic graph, FG, is a tuple that is defined as follows:

$$FG = < H, E, F_h, F_e, w >$$

where H is the set of hypotheses, E is the set of evidence-collecting tests, F_h is a decomposition relation $(F_h \subseteq H \times H)$, w is the weight of evidence, $w \in \{?,+,-\}$, and F_e is an association relation $(F_e \subseteq H \times E \times w)$.

The weight of evidence indicates if the evidence has been analyzed (w = ? when not analyzed), if the evidence corroborates the hypothesis (+), or if the evidence contradicts the hypothesis (–). Figure 2.4 illustrates a graphical and textual specification of a forensic graph that decomposes this hypotheses: Suspect *I* on date *D* possessed a copy of the file *F*.



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 2.4 Example Forensic Graph

Bruschi and Monga's graph structure is beneficial for knowledge reuse because subgraphs can be selected from several forensic graph instances and combined into new forensic graphs. Thus, the knowledge from several past investigations may be aggregated on a new investigation. Providing clear arguments and objectives using the forensic graph is also beneficial to prosecutors who need to form legal arguments based on the evidence; the forensic graph illustrates how evidence relates to investigative hypotheses. Bruschi and Monga expressed interest in formalizing their hypothesis formulation approach because of difficulty in reusing natural language hypotheses in investigations with varying degrees of scope and circumstances.

2.2 Adopted Planning Procedures in Computer Forensics Examination

Before suggesting improvements to computer forensics investigations, it is necessary to discuss the existing planning practices and procedures of computer forensics examinations. This section of the literature review is intended to outline planning procedures that have been adopted by investigators. These procedures are typically documented by the law enforcement community and in some instances are confidential. This section focuses on adopted planning procedures that are relevant to planning and executing an examination. The remainder of this section is organized as follows: Section 2.2.1 discusses the typical structure of an organization that conducts computer forensics investigations, Section 2.2.2 discusses how investigators identify relevant case information, Section 2.2.3 discusses planning keyword searches, Section 2.2.4 discusses documenting the examination, and 2.2.5 provides an analysis of adopted procedures for computer forensics investigations.

2.2.1 Organizational Structure

In legal organizations the case investigator and the computer forensics examiner are roles that are typically played by two separate parties. According to the United States Department of Justice, "in most computer searches, the case agent organizes and directs the search, learns as much as possible about the computers to be searched, and writes the affidavit establishing probable cause. The technical specialist explains the technical limitations that govern the search to the case agent and prosecutor, creates the plan for executing the search, and in many cases takes the lead role in executing the search itself…. Of course, each member of the team should collaborate with the others to help ensure an effective search" [70].

In private or commercial data recovery and computer forensics firms, such role distinctions are less likely to occur, as one person may have both investigative and forensic responsibilities. Regardless of who plays the roles, the investigative and forensic tasks must be performed to recover evidence; the investigation activities uncover information about the circumstances or case, while the forensic activities extract evidence using technological methods based on investigative information. The methodology presented in this document recognizes this distinction between investigative activities and forensic activities and provides support for both roles.

2.2.2 Defining the Scope of an Examination

Before passing a case to a forensics examiner, the investigator must narrow the scope of the forensics examination by identifying information that is relevant to the case. The United States Department of Justice (USDOJ) suggested that an investigator should

at least provide the forensics examiner with the following information: “case summary, IP addresses, keyword lists, nicknames, passwords, points of contact, supporting documents, and type of crime” [70]. Preparing this background information and additional required information requires the investigator to act as an information filter who supplies the forensics technician with data useful in an examination. Experienced investigators instinctively identify the relevant information when dealing with familiar case types, while less experienced investigators require guidance. In this same USDOJ computer forensics manual, the authors provided brief outlines of information that is relevant to specific case types [70]. Table 2.2 lists two case types and relevant information items as they appear in the computer forensics manual.

Table 2.2 Case Types and Relevant Information

Case Type	Relevant Information Items
Email Threats / Harassment / Stalking	Address books, diaries, e-mail/notes/letters, Internet activity logs, legal documents, telephone records, financial/asset records, victim background research, images
Extortion	Date and time stamps, e-mail/notes/letters, history log, Internet activity log, temporary Internet files, user names

Such checklists may provide valuable introductory information to beginner investigators but may be too general for novice or advanced investigators. For example, Table 2.2 lists diaries as an item of interest but does not provide additional information about the attributes of a diary in the context of an email threat case. Identifying attributes of a diary entity is an activity that investigators may perform instinctively or through an

analytical process; the investigators must perform this activity to narrow the scope of the examination and present the forensics technician with a search plan to find the relevant artifacts contained in a diary. The USDOJ indicates that such case domain information must be collected and organized by the investigator before a successful forensics examination occurs. As indicated in Section 2.1, there is no previous computer forensics research that addresses the need for modeling these case domain concepts. Section 2.4 will describe software engineering technologies that may be applicable for modeling relevant information attributes in a case domain.

2.2.3 Keyword Search Planning

Keyword searches are a common technique for locating data during examinations, and sources suggest that keyword searches should be carefully planned [1, 5, 48, 49, 70, 71]. As discussed previously, the investigator and the forensics examiner are likely not the same person. In such situations it is essential that the investigator provide the forensics examiner with a list of keyword search terms; the investigator is the information expert regarding the case details, and the forensics examiner is a technology expert who requires case information in order to deliver forensics evidence. Only two brief sources provide further guidance for developing a list of effective keyword search terms for a computer forensics case [16, 26]. Depending on the complexity of the case the investigator may require a more structured approach to preparing a list of keyword search terms.

Brown claimed that “keyword searching in computer forensics can make or break an investigation [16]. Choosing the wrong search terms may cause you to miss vital

evidence, or may return so many hits that you spend hours looking for a needle in a haystack to find any real evidence." Brown claimed that too often computer forensics practitioners take GREP[6] (or other tools) training courses, which may cause them to become too tool-centric. Instead, the investigators should keep their primary focus on what they are looking for and where they need to look. Brown did not discount the use of GREP or other tools; rather he expressed the need for a search effort that is driven by fundamental investigation concepts where tools provide support instead of motivation. Brown later offered some elementary tips that include the use of search phrases, case sensitive searches, unique misspellings, Boolean logic, and nested searches. He cited a case where a bank robber gave tellers demand notes that contained misspelled words. The investigators found an electronic copy of the ransom note by including the misspelled words in a keyword search. Brown claimed that a computer forensics examiner can usually find what he/she is looking for by selecting appropriate keywords and applying only a few simple Boolean logic operators. Brown's search tips are less significant than his general statement: effective computer forensics data searching is achieved by maintaining focus on what the examiner is looking for and where he/she thinks it is, not by becoming an expert in forming complex keyword expressions.

Feldman, like Brown, specified the need to focus on maintaining a fundamental strategy and plan [16]. Feldman, of Computer Forensics Inc. (CFI), offered these brief tips for planning computer forensics data searches:

---

[6] GREP (global regular expression print) is a highly expressive search utility that originated in the UNIX operating system. GREP provides the power to search for regular expressions in one or more files.

1. Identify the type of data you want.
2. Determine whether or not you want information regarding system events such as the date and time files where opened, accessed, and/or deleted.
3. Specify relevant time periods.
4. Obtain a list of users, their log-on names, and other network aliases.
5. Use good search terms; avoid “noise” words that bloat search results.
6. Group search terms together; prioritize your search.
7. Be flexible [26].

Once again, the search tips are rather simple, but they reinforce the previous point regarding the importance of planning a data search.

In criminal cases it is even more important to maintain a focus on the legal constraints of the search. For example, the United States Department of Justice identified several federal laws that are relevant to computer forensics cases. State and local governments may place further legal constraints on electronic search and seizure [71]. A major concern during examination is to remain consistent with the scope of the search warrant. The search warrant identifies a set of electronic devices to be seized, along with the nature of the evidence that will be sought. The examiner may violate the terms of the search warrant if he/she excessively searches for evidence of crimes not specified in the search warrant. During legal proceedings the forensics examiner may be challenged regarding the scope of his/her search and the motivation behind that search.

2.2.4 Documenting the Examination

Among other legal-oriented suggestions, computer forensics manuals in law enforcement instruct the forensics examiner to maintain detailed documentation in anticipation of legal proceedings [70, 71]. However, these manuals do not provide guidelines for producing this documentation, and it is assumed that such guidelines are defined within investigative organizations/branches. It is also likely that examination notes are produced by forensics technicians who adopt their own documentation styles, which are not officially defined. Private companies, such as New Technologies Incorporated (NTI), offer training courses in case documentation and how to use this documentation in expert witness testimony [3].

2.3 Ontology Modeling in Artificial Intelligence

Domain analysis and modeling, as adopted in this dissertation, originated from ontology and knowledge representation research in the artificial intelligence community. The terms “domain model” and “ontology” are often used interchangeably and involve the same fundamental principles. In this chapter the term “ontology” will be used in the context of artificial intelligence and knowledge representation, while domain analysis and modeling will be limited to the context of software engineering research and practice. This subsection presents an overview of ontology methodologies and representation languages as identified by sources in the artificial intelligence and knowledge representation domains. The goals of this ontology literature review are to establish the background of ontology modeling in computer science and to contribute to a survey of

candidate methods and representations for computer forensics domain modeling and analysis.

2.3.1 Ontology Definition and Background

Ontology theory originated from Plato and Aristotle's classical philosophical frameworks, and it emerged as a popular artificial intelligence, knowledge representation research topic in the 1990s [21, 34]. Artificial intelligence theories may be categorized as content theories or mechanism theories, and ontology research fits into the former category. Chandrasekaran et al. distinguished between content and mechanism theories and offered general commentary on the alternating popularity of them in AI research: "…Sometimes, the AI community gets excited by some mechanism such as rule systems, frame languages, neural nets, fuzzy logic, constraint propagation, or unification. The mechanisms are proposed as the secret of making intelligent machines. At other times, we realize that, however wonderful the mechanism, it cannot do much without a good content theory of the domain on which it is to work. Moreover, we often recognize that once a good content theory is available, many different mechanisms might be used equally well to implement effective systems, all using essentially the same content" [21]. Chandrasekaran also provided an interesting discussion of the alternation of content and mechanism theories in an article in the final issue of *IEEE Expert* in 1994[7] [20].

McCarthy is acknowledged as the first to use ontology as a term to refer to "the things that exist" in a common-sense knowledge base of logical facts [46]. According to

[7] Chandrasekaran was the Editor in Chief of *IEEE Expert* during its last five years. As a reflection of AI's movement away from the expert systems trend, in January 1995 *IEEE Expert* was renamed to *IEEE Intelligent Systems and their Applications*.

Welty, in 1986, Alexander et al. were the first to bring ontology from its classical philosophical meaning into a new computer science meaning [2, 73]. Alexander et al. explained their use of ontologies as follows: "To philosophers, ontology is the branch of metaphysics concerned with the nature of existence, and the cataloging of existent entities…We use the term to emphasize that a knowledge-based system is best designed by careful attention to the step-by-step composition of knowledge structures. An ontology is a collection of abstract objects, relationships and transformations that represent the physical and cognitive entities necessary for accomplishing some task" [2].

Currently, there are two dominant, conflicting definitions for ontology in the context of artificial intelligence and knowledge representation:

> a. According to Gruber, "an ontology is an explicit specification of a conceptualization. The term is borrowed from philosophy, where an Ontology is a systematic account of Existence" [34]. Welty indicated that this definition is probably the most commonly cited definition of ontology in artificial intelligence and that researchers commonly make incorrect claims that Gruber's article was the start of ontology research in computer science [73].
>
> b. According to Uschold and Gruninger, an ontology is "a shared understanding in a given subject area" [72].

The distinction between the previous definitions is subtle and somewhat elusive. Chandrasekran et al. elaborated further on the distinction between the two major uses of the term ontology in artificial intelligence: "…the term ontology has largely come to mean one of two related things. First of all [definition a], ontology is a representation vocabulary, often specialized to some domain or subject matter. More precisely, it is not the vocabulary as such that qualifies as an ontology, but the conceptualizations that the terms in the vocabulary are intended to capture…. In its second sense [definition b], the

term ontology is sometimes used to refer to a body of knowledge describing some domain, typically a commonsense knowledge domain, using a representation vocabulary…. In other words, the representation vocabulary provides a set of terms with which to describe the facts in some domain, while the body of knowledge using that vocabulary is a collection of facts about a domain…. The distinction is that the former emphasizes the use of ontology as a set of terms for representing specific facts in an instance of the domain, while the latter emphasizes the view of ontology as a general set of facts to be shared" [21].

Noy and McGuiness also recognized the inconsistent use of the term ontology and proposed yet another definition: "…the Artificial-Intelligence literature contains many definitions of an ontology; many of these contradict one another…[for the purposes of their paper] an ontology is a formal explicit description of concepts in a domain of discourse (classes (sometimes called concepts)), properties of each concept describing various features and attributes of the concept (slots (sometimes called roles or properties)), and restrictions on slots (facets (sometimes called role restrictions)). An ontology together with a set of individual instances of classes constitutes a knowledge base. In reality, there is a fine line where the ontology ends and the knowledge base begins" [50]. Also, in 2003 Welty indicated in a guest editorial that the meaning of ontology "…is often argued back and forth by well-meaning people to clarify confusion, but often, the argument causes more confusion than it eliminates. Like many things, one must actually do ontology to understand what it is" [73]. Finally, in 2004, Musen added this commentary on the meaning of ontology: "although no simple predicate tells us

unambiguously whether a particular specification is an ontology, we can still agree on certain things. We can agree that ontologies enumerate the salient concepts in an application area" [15].

2.3.2 Methods and Principles for Ontology Design

Researchers and practitioners recognized that the successful deployment of large-scale shared ontologies and ontology libraries would be highly dependent on the establishment of quality-centric methods and principles for designing ontology products. This subsection presents an overview of influential literature on ontology design methods and principles.

In 1986, Alexander et al. proposed an ontological analysis methodology for developing artificial intelligence knowledge bases [2]. They suggested that ontology development follows a three-phase process that produces a new type of knowledge at each stage: static knowledge, dynamic operations, and epistemic knowledge. Static knowledge describes physical objects that exist in the world, and dynamic operations can alter the state of the physical objects. Epistemic knowledge provides guidance for when to apply dynamic operations based on the state of the static objects. They also proposed the following principles to guide users of the methodology:

> 1) Begin with physical entities, proceed to their properties and relationships from there…2) The static, dynamic, and epistemic ontologies are not strict boundaries, use them loosely…3) Clearly establish the distinction between objects and what they are intended to represent…4) Understand and separate intensional and extensional entities…5) Build relevant abstractions through the use of generalization and aggregation…6) Encode rules as simple associations, and heuristic steps as mappings between domains…7) Ensure the compositionality of elements [2].

In 1993, Gruber presented design criteria for reusable ontologies [34]. He proposed that disciplined engineering methods akin to software engineering methods were required in order to achieve the long-term goal of establishing a shared library of reusable knowledge components or ontologies. Additionally, ontology design criteria are important because all intelligent software agents commit to the ontology if their actions are to be consistent with the ontology, and "a common ontology defines the vocabulary with which queries and assertions are exchanged among agents" [34]. With these usages of ontologies in mind, Gruber proposed five design criteria for ontologies: clarity, coherence, extensibility, minimal encoding bias, and minimal ontological commitment. Because of their significance in the body of ontology design research, Gruber's descriptions of these design criteria are presented in Table 2.3 as they appeared in his paper [34]. Readers should consult Gruber's paper for detailed illustrations of and case studies involving the five ontology design criteria.

Gomez-Perez contributed guidelines for the evaluation of ontologies, and he suggested the following steps in an ontology definition evaluation:

1. "Check the structure or architecture of the ontology," 2. "check the syntax of the definitions," and 3. "check the content in the definitions" [32]. In step one, the structure of the ontology is evaluated according to the selected design criteria (e.g. Gruber's five design criteria). In step two, syntactically incorrect structures and definitions are defined independent of their semantics. Finally, in step three, the consistency, completeness, and conciseness of the ontology is evaluated.

Table 2.3 Gruber's Ontology Design Criteria (directly quoted from [34])

Design Criteria	Description
Clarity	An ontology should effectively communicate the intended meaning of defined terms. Definitions should be objective. While the motivation for defining concept might arise from social situations or computational requirements, the definition should be independent of social or computational context. Formalism is a means to this end. When a definition can be stated in logical axioms, it should be. Where possible, a complete definition (a predicate defined by necessary and sufficient conditions) is preferred over a partial definition (defined by only necessary or sufficient conditions). All definitions should be documented with natural language.
Coherence	An ontology should be coherent: that is, it should sanction inferences that are consistent with the definitions. At the least, the defining axioms should be logically consistent. Coherence should also apply to the concepts that are defined informally, such as those described in natural language documentation and examples. If a sentence that can be inferred from the axioms contradicts a definition or example given informally, then the ontology is incoherent.
Extensibility	An ontology should be designed to anticipate the uses of the shared vocabulary. It should offer a conceptual foundation for a range of anticipated tasks, and the representation should be crafted so that one can extend and specialize the ontology monotonically. In other words, one should be able to define new terms for special uses based on the existing vocabulary, in a way that does not require the revision of the existing definitions.
Minimal encoding bias	The conceptualization should be specified at the knowledge level without depending on a particular symbol-level encoding. An encoding bias results when representation choices are made purely for the convenience of notation or implementation. Encoding bias should be minimized, because knowledge-sharing agents may be implemented in different representation systems and style of representation.
Minimal ontological commitment	An ontology should require the minimal ontological commitment sufficient to support the intended knowledge sharing activities. An ontology should make as few claims as possible about the world being modeled, allowing the parties committed to the ontology freedom to specialize and instantiate the ontology as needed. Since ontological commitment is based on consistent use of vocabulary, ontological commitment can be minimized by specifying the weakest theory (allowing the most models) and defining only those terms that are essential to the communication of knowledge consistent with that theory.

Uschold and Gruninger are also primary contributors of preliminary principles and methods for ontology design [72]. They recognized a lack of standard methodologies and research literature for producing quality ontology designs and products. They proposed a methodology for building ontologies that are developed for communication, interoperability, and systems engineering (specification, reliability, and reusability). In the context of communication, an ontology "reduces conceptual and terminological confusion by providing a unifying framework within an organization" [72]. In the context of interoperability, ontologies address the problem "in which we have different users that need to exchange data or who are using different software tools. A major theme for the use of ontologies in domains such as enterprise modeling and multiagent architectures is the creation of an integrating environment for different software tools" [72]. Finally, in the systems engineering context, ontologies serve as specification and design products of the software system.

Uschold and Gruninger's methodology includes the following items: identification of the purpose and scope, building of the ontology, evaluation, documentation, and development of guidelines for each phase. This methodology is a refinement of Gruninger and Fox's previous methodology for the design and evaluation of ontologies that included the following components: identification of the motivating scenario, mapping of informal competency questions to the scenario, specification using first-order logic, and evaluation of the first-order logic according to formal competency questions (axioms and completeness theorems) [35]. Further discussion of Gruninger and Fox's methodology is omitted because Uschold and Gruninger's model contains the same

ideas, and it is not specific to first-order logic specifications. Table 2.4 presents a description for each component of Uschold and Gruninger's ontology design methodology.

Uschold and Gruninger's ontology development methodology serves as the basis for contemporary literature on ontology development. For example, in 2001 Noy and McGuiness, from Stanford University's Knowledge Systems Laboratory, published a technical report entitled, "Ontology Development 101: A Guide to Creating Your First Ontology" [50]. Noy and McGuiness presented an ontology development process that is very similar to Uschold and Gruninger's methodology. Noy and McGuiness's methodology includes the following steps: 1. Determine the domain scope of the ontology, 2. Consider reusing existing ontologies, 3. Enumerate important terms in the ontology, 4. Define classes and the class hierarchy, 5. Define the properties of classes, 6. Define the facets of the slots (cardinalities, attribute types, etc.), and 7. Create instances. They also offered three general guidelines within the context of Uschold and Gruninger's methodology: "There is no one correct way to model a domain—there are always viable alternatives. The best solution almost always depends on the application that you have in mind and the extensions that you anticipate…. Ontology development is necessarily an iterative process…. Concepts in the ontology should be close to objects (physical or logical) and relationships in your domain of interest. These are most likely to be nouns (objects) or verbs (relationships) in sentences that describe your domain" [50].

Based on this review of ontology development methodologies and principles, there seems to be a general agreement in the artificial intelligence community that

Table 2.4 Uschold and Gruninger's [72] Ontology Design Methodology

Methodology Component	Description
Identify Purpose and Scope	Define the usage scenarios and application domain of the ontology
Building the Ontology	Consists of three activities: ontology capture, ontology coding, and integration of existing ontologies
Ontology Capture	Identify the concepts and relationships, produce precise unambiguous textual descriptions of them, and identify terms for referring to concepts and relationships
Ontology Coding	Choose the meta-ontology or terms used to specify the ontology (classes, entities, relations, slots, attributes, etc.), select a representation language that supports the meta-ontology, code the ontology in the representation language
Integrating Existing Ontologies	During the capture and coding phases, evaluate the potential for reuse of existing ontologies.
Evaluation	Apply ontology design evaluation criteria such as those proposed by Gruninger and Fox [35] and Gomez-Perez [32]
Documentation	Clearly define the assumptions and important decisions that were made with regards to the ontology design and representation
Guidelines for Each Phase	Include guidelines for each of the above phases as well as indication of relationships between the phases. Gruber [34] provides preliminary guidelines that may be applied in the above phases.

developing quality ontology knowledge bases demands a systematic, engineering approach. Also, there seems to be a consensus that methodologies for ontology development should include a process framework for ontology development, principles for following the process, and criteria for evaluating the resulting product. Choosing a methodology may be dependent on the project characteristics and the chosen ontology representation language.

2.3.3 Ontology Representations

To conclude this survey of work on ontology modeling in artificial intelligence, this subsection presents an overview of four general categories of ontology representations as identified by Russell and Norvig: logic programming languages, production systems, description logic systems, and frame systems and semantic networks [58]. Logic programming languages and production systems will be described together because they both represent the ontology in terms of first-order logic.

2.3.3.1 Logic Programming Languages and Production Systems

Logic programming languages represent ontologies as a consistent collection of first-order logic implications and predicates. For example, parenthood may be represented by two functions, *Mother* and *Father*, where one's mother is one's female parent, and one's father is one's male parent. *Female* and *Male* may be represented as unary predicates, and *Parent* may be represented as a binary predicate. Formally stated:

$$\forall m, cMother(c) = m \Leftrightarrow Female(m) \wedge Parent(m, c)$$
$$\forall f, cFather(c) = f \Leftrightarrow Male(f) \wedge Parent(f, c)$$

According to Russell and Norvig, “logic programming views the program and inputs as logical statements about the world, and the process of making consequences explicit as a process of inference” [58]. An inference engine is an essential part of a logic programming language, and it may be used to respond to queries via backward-chaining. For example, based on the following positive literals and the definitions of *Mother* and *Father*, backward-chaining may be applied to determine the mother and father of *Chris*: *Male*(*Al*), *Female*(*Charlotte*), *Parent*(*Charlotte*, *Chris*), *Parent*(*Al*, *Chris*). Based on the ontology, it may be inferred that *Charlotte* is the mother of *Chris* and *Al* is the father of *Chris*. Details of the backward-chaining algorithm are beyond the scope of this chapter, and readers are advised to consult Russell and Norvig for further details [58]. PROLOG, the most popular logic programming language, has been used as a tool for building compilers, parsing natural language, and building expert systems. All inference calculations in PROLOG are performed using a backwards-chaining, depth-first search algorithm.

Like logic programming languages, production systems represent the ontology in first-order logic terms. However, the application of logic programming languages and production systems differ: logic programming languages evaluate queries using backward-chaining, and production systems use forward-chaining to infer new information about the world. However, in production systems the consequence of the implications (rule memory) is an action to add or delete information from the collection of positive literals (working memory). CLIPS is an example of a production system.

Some of the most heavily debated issues in logical knowledge representation have revolved around what is known as the frame problem [58, 61]. The frame problem, described by McCarthy and Hayes in 1969, details a significant disadvantage of declarative logical knowledge representation: "Using mathematical logic, how is it possible to write formulae that describe the effects of actions without having to write a large number of accompanying formulae that describe the mundane, obvious non-effects of those actions" [61]? The frame problem is commonly illustrated in terms of an example that involves a specification on the effects of moving an object and painting an object: "1. *Colour*(*x*, c) *holds after Paint*(*x*,*c*), 2. *Position*(*x*, *p*) *holds after Move*(*x*,*p*)" [61]. For example, an object is green after it is painted green, and an object is in the yard after it is moved into the yard. Though it is intuitive to assume that the color of an object does not change after it is moved, the former two rules do not allow one to draw this rather commonsense conclusion. To address this problem, a knowledge-based system must contain frame axioms that state how the ontology is unchanged by each action. The challenge of the frame problem is in representing these commonsense rules in a clear and concise manner while avoiding the burden of explicitly specifying $M \times N$ frame axioms, where M is the number of single-property-modifying actions and N is the number of properties. The issue has been, for the most part, resolved by solutions such as circumscription, situation calculus, and successor-state axioms [58, 61]. Further discussion of the frame problem, its variants, and solution approaches are beyond the scope of this chapter.

2.3.3.2 Description Logic Systems

According to Russell and Norvig, "the syntax of first-order logic is designed to make it easy to say things about objects. Description logics are designed to focus on categories and their definitions" [58]. In general, the description logic representation is more straightforward and concise than first-order logic. For example, in CLASSIC, a description logic system, $\forall x, Mother(x) \Leftrightarrow Female(x) \wedge HasChild(x)$ may be represented as *Mother* = *And*(*Female*, *HasChild*). Description logics such as CLASSIC and KL-ONE also improve on the tractability of inference by guaranteeing a polynomial response time to all inference queries. Because of inference tractability and more user-friendly, concise syntax, practitioners adopted CLASSIC and other description logic systems for applications such as financial management, database interfaces, and software information systems [58]. However, due to restrictions on the description logic syntax, namely the lack of disjunction and negation, it is difficult and sometimes impossible to represent complex problems and queries.

2.3.3.3 Frame Systems

Frame systems offer a significant syntactical departure from logic programming languages, production systems, and description logic systems. Frame-based systems represent ontologies as collections of objects that are related by subset and membership relations. Objects also have slots with allowable values, and subset objects may inherit these slots from superset objects. Figure 2.5 illustrates a frame-based knowledge base. A rectangle represents an object, and it contains the object name and the slots of the object.

Arrows drawn between objects represent subset or membership relationships. Though the syntax is more user-friendly than first-order logic, the frame-based or semantic network may be translated into first-order logic. For example, the *Stringed Instruments* and *Guitars* objects may be translated into the following first-order logic sentences:

$$\forall x, StringedInstrument(x) \Rightarrow HasStrings(x) \wedge HasTuners(x)$$
$$\forall x, Guitars(x) \Rightarrow StringedInstrument(x) \wedge HasNeck(x) \wedge HasBridge(x)$$

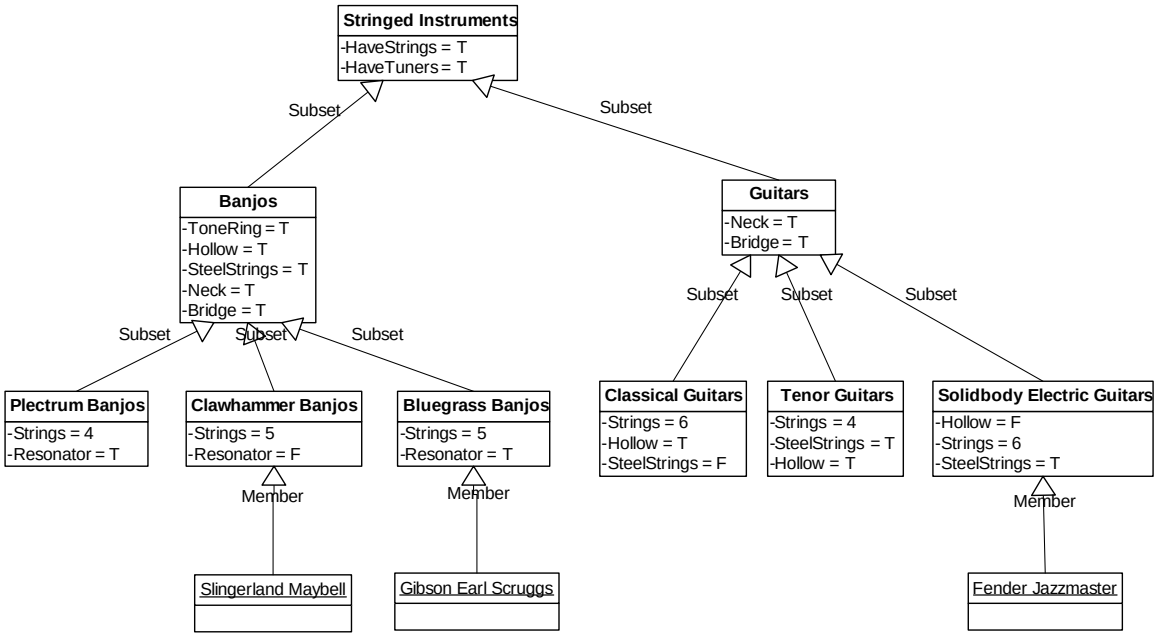


Figure 2.5 Frame-Based Knowledge Base Example

Given a large knowledge base with many objects, the frame-based ontology illustration (as illustrated in Figure 2.5) is not scalable. Typically, frame-based ontology languages provide syntax for graphical representation and for textual representation; in large knowledge bases the graphical representation may be applied to a subset of the most widely used object hierarchies. The frame-based approach is significantly less expressive

than logic programming languages, production systems, and description logics; frame-based knowledge bases do not allow negation, disjunction, or quantification. However, according to Russell and Norvig, the frame-based approach offers the following advantages: “they are able to capture inheritance information in a modular way, and their simplicity makes them easy to understand” [58].

Currently, frame-based ontology representations are very popular in literature regarding the Semantic Web. The Semantic Web is an initiative led by the World Wide Web Consortium (W3C) to enhance the metadata standards for Web documents and services. Currently, access to documents on the World Wide Web is highly dependent on ambiguous keyword matches and website rankings, and there is little machine-interpretable data present in World Wide Web documents. XML (Extensible Markup Language), RDF (Resource Description Framework), and OWL (Web Ontology Language) are the standard languages of the Semantic Web. OWL is a frame-based language that is used for publishing ontologies on the World Wide Web, and its standard is specified by the W3C [76]. In the Semantic Web, ontologies will be published, shared, and referenced in Web content and Web services; the ontologies will provide a machine-readable, shared understanding of concepts present in documents. Table 2.5 provides an OWL representation for the class of *Solidbody Electric Guitars* as specified in the frame-based knowledge base illustrated in Figure 2.5.

Several tools are available for supporting frame-based ontology development in OWL and other languages. In 2002, OntoWeb, a European-Union-funded ontology

Table 2.5 OWL Ontology Example

```
<owl:Class rdf:ID="Solidbody_Electric_Guitars">
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:onProperty>
        <owl:DatatypeProperty rdf:ID="Strings"/>
      </owl:onProperty>
      <owl:hasValue rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >6</owl:hasValue>
    </owl:Restriction>
  </rdfs:subClassOf>
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:onProperty>
        <owl:DatatypeProperty rdf:about="#SteelStrings"/>
      </owl:onProperty>
      <owl:hasValue rdf:datatype="http://www.w3.org/2001/XMLSchema#boolean"
      >true</owl:hasValue>
    </owl:Restriction>
  </rdfs:subClassOf>
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:onProperty>
        <owl:DatatypeProperty rdf:about="#Hollow"/>
      </owl:onProperty>
      <owl:hasValue rdf:datatype="http://www.w3.org/2001/XMLSchema#boolean"
      >false</owl:hasValue>
    </owl:Restriction>
  </rdfs:subClassOf>
  <rdfs:subClassOf rdf:resource="#Guitars"/>
</owl:Class>
```

project, published a comprehensive evaluation of tools for ontology development, ontology merge and integration, ontology evaluation, ontology storage and querying, and ontology-based annotation [51]. Their evaluation criteria included factors such as software architecture, interoperability, underlying knowledge representation language, available inference services, and usability. All of the evaluated tools were relevant to Semantic Web development, and many of the ontology development tools, such as Apollo, Link Factory, OntoEdit, Ontolingua, Protégé, WebODE, and WebOnto, support frame-based ontology development.

2.4 Domain Modeling in Software Engineering

In the 1980s and 1990s, while artificial intelligence researchers were busy exploiting the reasoning capabilities of ontologies, software engineers began placing an increasing amount of emphasis on developing reusable components and providing support for requirements engineering tasks. During this period, software engineering researchers began applying methods and principles similar to ontology design methods to the problem of analyzing and modeling the application domain for which a software product is built; in the context of this chapter, this will be known as domain analysis and modeling. This section defines domain modeling in the context of software engineering, describes methods and principles of domain modeling, and presents an overview of prevalent domain modeling representations. This topic is discussed in sufficient detail such that candidate methods and representations for computer forensics domain modeling may be identified and evaluated later in this document.

2.4.1 Domain Modeling Definition and Background

The term "domain analysis" was first defined by Neighbors in 1980 as "the activity of identifying objects and operations of a class of similar systems in a particular problem domain" [47]. Neighbors proposed that domain analysis was essential for developing reusable software components, and he stated that "the key to reusable software is to reuse analysis and design; not code" [47]. Neighbors's early domain analysis research was part of a trend of application-domain focus in software engineering, where, "by application domain, we mean a collection of problems that have something in common, usually (but not always) the nature of the problem" [30]. The trend began because researchers recognized a shortfall in general, weak problem-solving methods to system development; analyzing and modeling the application domain provided a focused, strong problem-solving method for systems development. In the context of problem-solving methods, "strong methods are those designed to address a specific type of problem, while weak methods are those general approaches that may be applied to many types of problems" [30]. Though Neighbors originally proposed domain analysis in the context of reusable components, the operational goals of domain analysis and modeling were later expanded to include:

- "Requirements & Specifications: Eliciting, verifying, and formalizing software requirements and specifications.
- Automated Program Generation: Generating code from a system specification.
- Reverse Engineering: Identifying the semantics of existing code.
- Explanation & Communication: Capturing and communicating system content as with an executive information system.

- Decision Modeling: Understanding and resolving design decisions and rationales.
- Education & Training: Training analysts and end users.
- Testing: Automating the testing procedure" [37, 38].

The result of domain analysis activities is a model that represents entities, attributes, and operations native to the application domain. During design and coding, developers make decisions about which elements of the domain model will be transformed into software components. In some circumstances, the model's validity is based on the agreement and common understanding between all system stakeholders; stakeholder feedback and negotiation is an essential approach to requirements verification and validation [41, 53]. In this sense, domain models are consistent with Uschold and Gruninger's definition that an ontology is a "a shared understanding in a given subject area" [72].

2.4.2 Domain Modeling Methods and Principles

When Neighbors proposed domain analysis, he did not specify a method or process for constructing a domain model; rather, he focused on the more encompassing method for transforming a domain model into reusable software components. Neighbors called this the "Draco Approach," and it included the following activities: "the analysis of a complete problem area or domain (domain analysis), the formulation of a model of the domain into a special-purpose, high level language (domain language), the use of software components to implement the domain languages, and the use of source-to-source program transformations to specialize the components for their use in a specific

system" [47]. However, as the trend toward application domain methods began, specific methods for domain analysis followed.

Prieto-Diaz described the domain analysis process in the following narrative: "Information is collected from existing systems in the form of source code, documentation, designs, user manuals, and test plans, together with domain knowledge and requirements for current and future systems. Domain experts and domain analysts extract relevant information and knowledge. They analyze and abstract it. With the support of a domain engineer, knowledge and abstractions are organized and encapsulated in the form of domain models, standards, and collections of reusable components. The process is guided by domain analysis methods and techniques as well as management procedures" [54]. Table 2.6 summarizes the inputs, roles, support mechanisms, and output of Prieto-Diaz's domain analysis process.

Table 2.6 Domain Analysis Process Inputs, Roles, Support, and Output

Inputs/Sources of Domain Knowledge	Technical literature, existing implementations, customer surveys, expert advice, and current and future requirements
Roles	Problem domain expert, domain analyst, and domain engineer
Supporting Mechanisms	Domain analysis methods, management procedures
Domain Analysis Output	Taxonomies, standards, functional models, and domain languages

The object-oriented development methodology has become the standard solution for software reuse and, to a large extent, domain modeling in software engineering. The object-oriented paradigm views the application domain as a collection of related entities

that encapsulate attributes and operations [43, 53]. This domain representation is similar to the frame-based ontologies in artificial intelligence. The object-oriented development methodology begins with object-oriented analysis. The goal of object-oriented analysis is to identify the classes relevant to the problem domain and to identify the relationships, attributes, and behavior of these classes. A typical object-oriented analysis process includes the following sequence of tasks:

1. "Basic user requirements must be communicated between the customer and the software engineer.
2. Classes must be identified.
3. A class hierarchy is defined.
4. Object-to-object relationships should be represented.
5. Object behavior must be modeled.
6. Tasks 1 through 5 are reapplied iteratively until the model is complete" [53].

Alternatively, if few requirements have been developed, the first representation of an object-oriented domain model may exclude the behavior and operations of classes and focus only on class hierarchies, class attributes, and class relationships (information domain). This is sometimes known as the Shalaer-Mellor method of object-oriented analysis, and it is also present in the Unified Modeling Language (UML) approach to object-oriented analysis [41, 43]. As the requirements are refined and design activities are performed, domain concepts are transformed into system classes with delegated responsibilities and operations. Larman specified the following sequence of tasks for this approach to object-oriented domain modeling: 1. identify domain concepts, 2. identify relationships between domain concepts, and 3. identify the attributes or properties of the

domain concepts [43]. The following three paragraphs discuss this approach to object-oriented domain analysis in more detail.

Domain concepts may be any ideas, things, or objects that are relevant to the development project. Concept category lists and noun extraction are common tools and techniques for identifying candidate concepts in a problem domain [43, 53]. Table 2.7 provides an example concept category list with example concepts. In noun extraction, text passages relevant to the project are grammatically parsed, and all nouns are listed as candidate concepts. However, noun extraction may provide an overwhelming list of candidate concepts that contains redundant and irrelevant entries.

Coad and Yourden[8] suggested six selection characteristics that a class or concept should exhibit to be included in the domain model:

1. Retained information: The potential class will be useful during analysis only if information about it must be remembered so that the system can function.
2. Needed services: The potential class must have a set of identifiable operations that can change the value of its attributes in some way.
3. Multiple attributes: During requirements analysis, the focus should be on 'major' information; a class with a single attribute may, in fact, be useful during design, but is probably better represented as an attribute of another class during the analysis activity.
4. Common attributes: A set of attributes can be defined for the potential class, and these attributes apply to all instances of the class.
5. Common operations: A set of operations can be defined for the potential class, and these operations apply to all instances of the class.
6. Essential requirements: External entities that appear in the problem space and produce or consume information essential to the operation of any solution for the system will almost always be defined as classes in the requirements model [53].

[8] The original source of the six criteria is P. Coad and E. Yourden, *Object-Oriented Analysis*, 2nd ed., Prentice-Hall, 1991.

Table 2.7 Concept Category List

Concept Category	Examples
Physical or tangible objects	Cell phone, hard drive, CDR disk
Descriptions of things	Marketing report, Technical Report
Places	Home, street
Transactions	Payment, sale, money deposit, email transmission
Roles of people	User, Systems Administrator
Containers of things	Databases, hard drives
Things in a container	Files, transactions
Computer or electro-mechanical systems	Internet store, credit card authorization system
Organizations	Sales Department, Savings and Loan Department
Events	Sale, Class Registration
Rules and policies	Tax Laws, Security Policies
Records of finance, work, contracts, legal matters	Bank Account Log, Work Contract
Services	Internet service provider, telephone service, cell phone service
Manuals, Books	Embedded System Specifications, Scientific Theories

Relationships between objects identify some meaningful or interesting association. As was the case in identifying concepts, relationships may also be identified by using a relationship category list such as the one in Table 2.8. The goal of identifying these relationships is to enhance the understanding of the application domain, but the concepts themselves are more important than the relationships between the concepts [43]. Larman provided the following guidelines for selection relationships (he referred to them as associations):

- "Focus on those associations for which knowledge of the relationship needs to be preserved for some duration ("need-to-know" associations).
- It is more important to identify concepts than to identify associations.
- Too many associations tend to confuse a conceptual [domain] model rather than illuminate it. Their discovery can be time-consuming, with marginal benefit.
- Avoid showing [selecting] redundant or derivable associations" [43].

Finally, a set of attributes is selected that enumerate the important information held by a concept. Example attributes include descriptive data such as phone number, zip code, date, name, social security number, etc. When selecting attributes, Pressman [53] advised the developer to answer the following question for each concept: "What data items (composite and/or elementary) fully define this class [concept] in the context of the problem at hand?" This process of selecting concepts, relationships, and attributes may be performed iteratively such that previous phases are revisited when required; for example, during the attribute identification phase, it may be necessary to introduce new concepts or remove unnecessary concepts.

Table 2.8 Concept Relationship Categories

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	Employee – Car
A is a member of B	Employee – Company
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	Tech Support - Users
A is known/logged/recorded/reported in B	Email registration – Network logs

Domain models and ontologies are similar (this will be discussed further in Section 2.4.3), and in some instances, researchers directly prescribe ontology development methods for requirements domain analysis [14, 55]. Prieto-Diaz adapted Uschold and Gruninger's ontology development method, and Breitman and Leite devised their own method based on previous ontology methods and on application language methods [14, 55, 72]. As ontology is a contemporary "buzzword" in computer science literature, more ontology-based requirements modeling and software engineering methods are likely to follow.

2.4.3 Domain Modeling Representations

Domain models are generally more focused and less formal than the ontology and knowledge models used in artificial intelligence applications. Table 2.9 provides a comparison of ontology knowledge models and domain models as presented by Prieto-Diaz [55]. Typically, reasoning and inference algorithms are not applied to domain models, so formality is not required. However, domain models may be extended to include the formal features and notation of ontologies [23, 28]. Additionally, some requirements domain modeling languages do provide the formality provided by knowledge-based ontology languages. This formality may be required in order to support automated component validation or automated code generation

Table 2.9 Comparison of Domain Model and Ontology

Feature	Domain Model	Ontology
Controlled vocabulary	Yes	Yes
Taxonomy	Yes	Yes
Thesaurus	Yes	Yes
Abstract concept definitions	Informal	Formal
Semantic relationships	Yes	Yes
Multiple viewpoint models	Yes	Yes
Axioms	Yes	Yes
Cross-domain association	Implicit (via thesaurus)	Explicit
Formal notation	No	Yes

.

The remainder of this section presents three example representations of requirements domain models: the Unified Modeling Language, the Entity Relationship Diagram, and Formal Specification Languages.

2.4.3.1 Conceptual Diagrams in the Unified Modeling Language

UML conceptual diagrams are typically constructed during the early requirements phase of software projects in order to help the developers understand the application domain of the project [43]. The foundational element of the UML conceptual diagram is the concept. A concept represents a "real-world" entity that may contain zero or more attributes that describe the concept. The conceptual diagram serves as a reference during requirements engineering design and as the basis for later UML models such as system contracts and class diagrams.

The UML conceptual model notation is relatively simple, as the model is intended to be reviewed by a layperson. Figure 2.6 provides an example of a UML conceptual model applied to the domain of a retail point-of-sale system [43]. Concepts are represented by boxes, with the concept name appearing in the top of the box. If attributes exist, they are listed in the field below the concept name. Lines drawn between concepts indicate a named relationship with a specified cardinality. For example, one Product Catalog contains one or more Product Specification concepts.

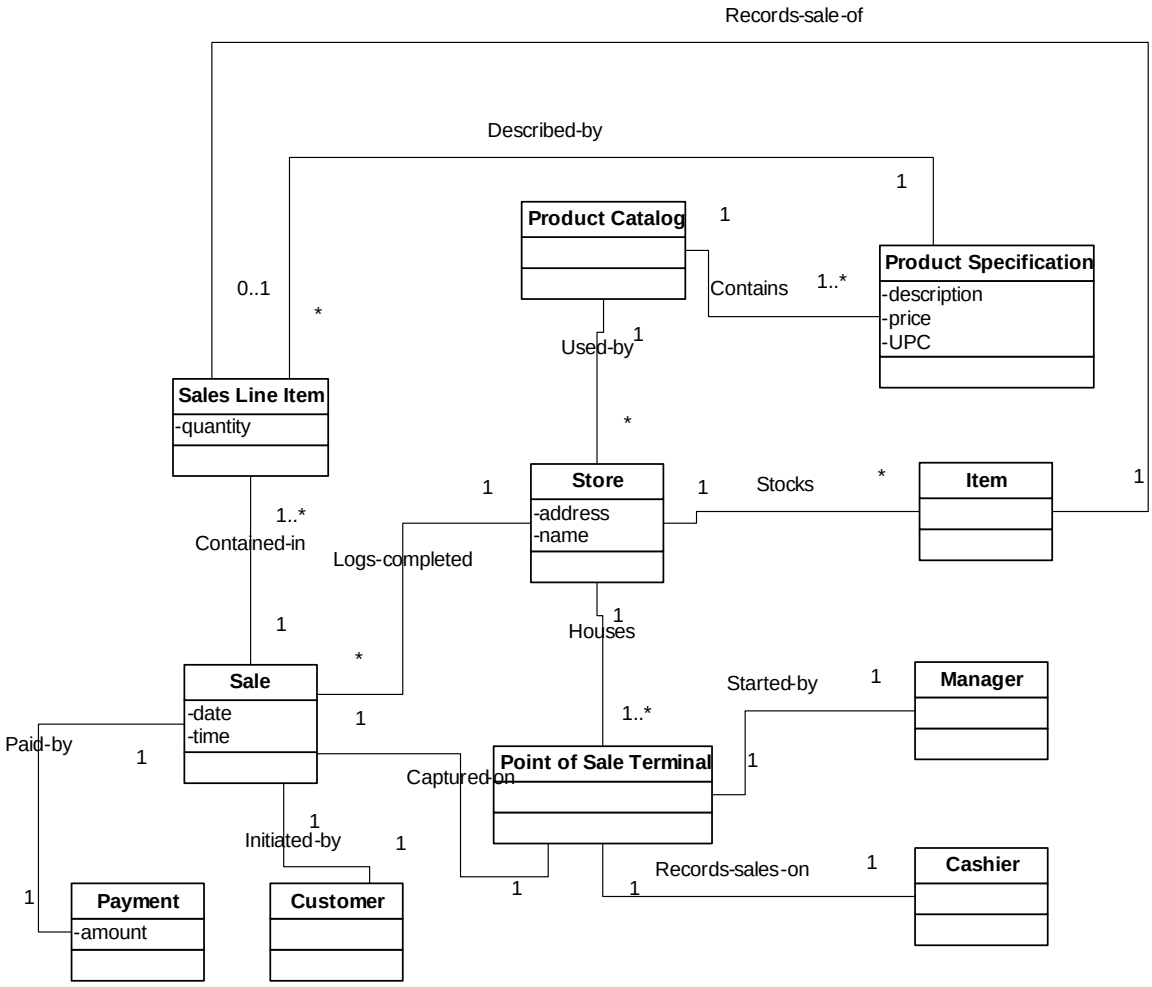


Figure 2.6 UML Conceptual Diagram for Point-of-Sale System

As the UML representation is very popular, researchers have developed extensions to UML such as UMLSEC for security applications, and methods for translating a UML conceptual diagram into a formal ontology [23, 28, 39]. These extensions to UML illustrate the popularity and flexibility of UML and the dominance of the object-oriented development methodology.

2.4.3.2 Entity Relationship Diagrams

Entity relationship diagrams are primarily used for designing relational database schemas, but they may also be used for representing the information domain of a non-database application. The entity relationship diagram was proposed by Chen in 1976 and is known as a semantic data model [41]. There are three fundamental components of the entity relationship diagram: entities, attributes, and relationships. The meanings of these terms are synonymous to the concepts, attributes, and relationship elements of the UML conceptual diagram, and in fact, the entity relationship diagram is a precursor to object-oriented models [41].

Figure 2.7 illustrates an entity relationship diagram for an Internet shopping system.[9] Rectangles represent entities, ovals represent entity attributes, and diamonds represent relationships. A line drawn between an entity and a relationship indicates the entity's participation in the relationship. There are two additional components to the entity relationship diagram notation: cardinality and modality. Cardinality indicates the number of entities participating in a relationship, and modality indicates whether or not

[9] Figure 2.7 is a reproduction of an entity relationship diagram that was provided with an evaluation version of *Smart Draw* software by Hemera Technologies Incorporated.

the relationship is required or optional. A “crow’s foot” indicates a multiple cardinality, and a vertical line indicates a singular cardinality. For example, in Figure 2.7, one *Order* entity *Contains* many *Item* entities. Modality is indicated by a vertical line (mandatory relationship) or a circle (optional relationship), and modality is only specified when the cardinality is also specified. When modality is specified, its indicators occur beside the cardinality indicator and nearest to the relationship diamond. For example, in Figure 2.7, a *Customer* entity is an optional element of an *Orders* relationship, but an *Item* entity is a required element of an *Orders* relationship. If cardinality and modality are not specified, then the relationship is understood to have a one-to-one cardinality with a mandatory modality.

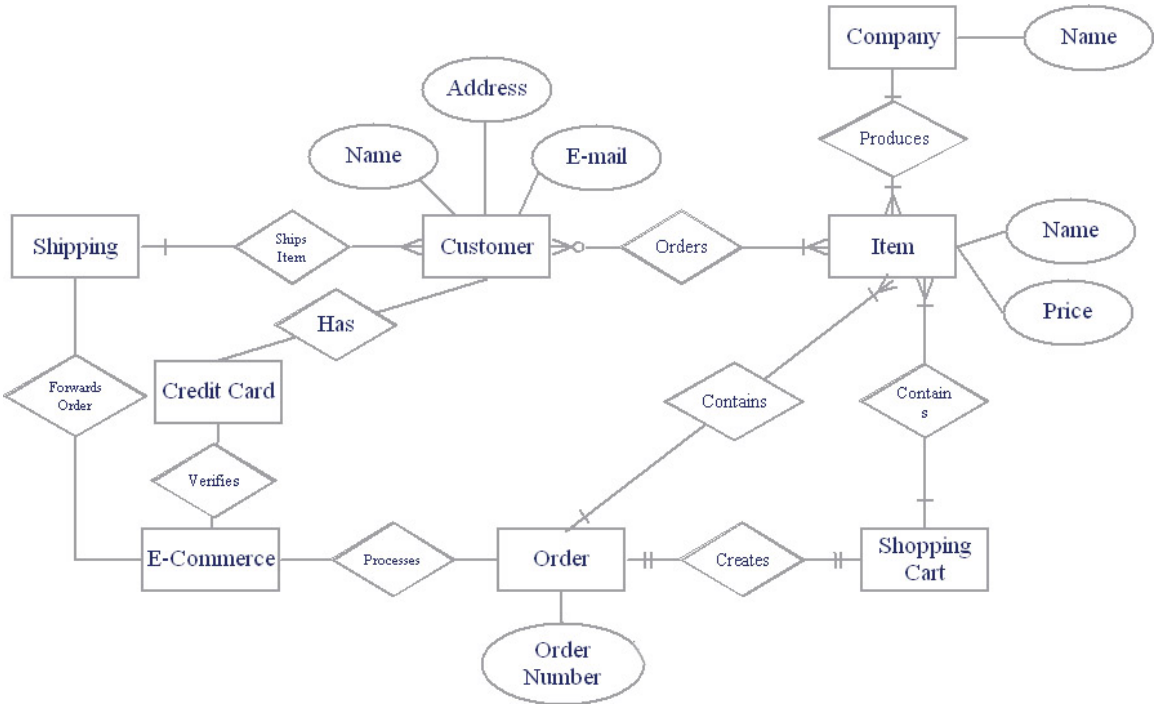


Figure 2.7 Entity Relationship Diagram for Internet Shopping System

2.4.3.3 Formal Requirements Specification

Formal software specification languages such as Z (pronounced Zed) and the requirements modeling language allow users to represent system requirements using rigid mathematical terms. The mathematical representation of system requirements eliminates problems with ambiguity and allows software engineers to mathematically prove that the coded system behaves according to the formal specifications. The use of formal methods requires skills in Boolean algebra and set theory, requiring users to attend extensive training. Figure 2.8 provides an example Z specification for an order invoices data schema [27]. Z also allows states and operations to be defined. This type of domain model specification contains the same level of formality present in knowledge-based ontology models.

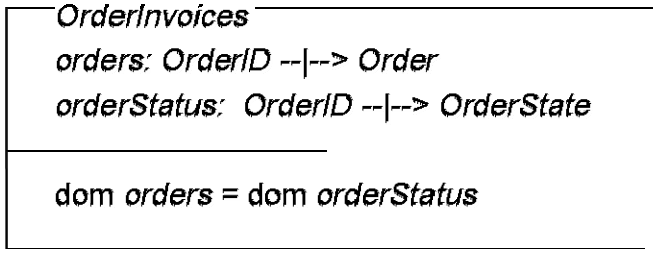


Figure 2.8 Z Data Schema Specification for Order Invoices

The schema in Figure 2.8 specifies that "…*orders* and *orderStatus* are partial functions from the set *OrderID*. The functions are partial (i.e., their domains do not necessarily cover the whole of the *OrderID* set in this case) since only valid orders are mapped in this way. All orders have a status associated with them. This type of general

information that must apply at all times (whatever the specific state of the system at any given time) is presented as a stat *invariant* predicate in most Z specifications (e.g., dom *orders* = dom *orderStatus*, constraining the domains of both functions to always be the same)" [27].

The practicality of formal methods in software engineering has been an ongoing debate for the past two decades. Critics claim that formal methods have not gained widespread acceptance in software engineering practice because the learning curve is too steep, it takes too much time to write formal specifications for a large system, and formal methods are only appropriate for safety critical systems. Researchers have responded to the critics by proposing the use of lightweight approaches to formal methods. This lightweight formalism has characteristics such as:

- Placing more emphasis on creating an abstract representation than on formal notational details.
- Employing formal methods as an analysis tool, and not using formal methods for theorem proving on the mapping of specifications to design/code.
- Using theorem proving on a small subset of the system (optional).
- Using formal specifications on a selected subset of confusing or risky system requirements.
- Using formal methods in response to problems encountered during requirements analysis (e.g. misunderstood requirements, volatile requirements).
- Improving the quality of natural language baselined requirements [13, 24].

2.5 Summary

This chapter has provided a survey of work related to this dissertation. With respect to each of the topic areas, this chapter has:

- Established the current state of the art in computer forensics modeling approaches.
- Established the current state of practice in computer forensics investigations.
- Described common methods and representations of knowledge-based ontologies.
- Described common methods and representations for software engineering domain analysis and modeling.

Chapter 3 will synthesize the research presented in this chapter by introducing a method for planning a forensics examination that includes domain modeling. The case domain modeling approach utilizes the fundamental theories of domain and ontology modeling discussed in this chapter. The case domain modeling method described in Chapter 3 was used in the experiments that are described in Chapter 4 and Chapter 5.

CHAPTER III

CASE DOMAIN MODELING KEYWORD SEARCH PLANNING METHODOLOGY

This chapter describes the case domain modeling and keyword search derivation methodologies. These topics are discussed in sufficient detail to characterize how the methodology may be applied in practical circumstances. However, these methodologies were customized to suit the needs of each experiment or case study.

3.1 Analysis of Related Work

Current best practices for computer forensics examination imply that the information domain of a case is defined by keyword lists, checklists, and other documents [6, 70, 71]. Ad hoc methods for scoping the information domain of an examination may be insufficient when investigators and technicians encounter large-scale cases, unusually complex cases, or unfamiliar case types. Existing modeling approaches in computer forensics each provide a different view of the investigation: DIPL provides a chain-of-events view, attack trees and adversary models offer adversary (or suspect) strategy views, and forensic graphs offer a hypothesis test view [17, 44, 59, 67, 68]. No previous forensic modeling approaches provide a method for exclusively analyzing and modeling the information domain of the forensics case. This dissertation research

addresses this shortcoming of existing modeling approaches by offering a more structured domain modeling approach for defining the information domain of a forensics examination.

Established ontology and domain modeling methods and representations in artificial intelligence and software engineering provide a suitable framework for establishing a forensic case domain modeling methodology and representation. Both communities have produced an abundance of information on the topic of information domain modeling. In general, the software engineering methods for domain analysis and model representation seem to be more appropriate for case domain modeling adaptation than the knowledge-based ontology methods and representations.

First-order-logic-based ontology representations (logic programming languages, description logics, and production systems) provide more expressive power than is necessary for defining the information domain of a forensics examination. Additionally, these languages are likely to be too technical for users who do not have extensive background in philosophy, computer science, or computer engineering. The frame-based ontology representation is the least expressive and the most user friendly. Though the frame-based ontology representation is based on first-order logic and set theory, it does not contain formal notations and syntax; entities are defined by boxes, lists, and link-lines instead of first-order logic sentences.

Software engineering domain model representations are derivatives of the frame-based ontology representations. Though they are restricted to software engineering applications, this restriction does not discount their utility for computer forensics

applications. The products of software engineering and computer forensics differ significantly. The former delivers a practical software configuration that consists of documentation, computer-executable code, and data structures, while the latter delivers digital evidence and documentation that indicates the occurrence of a digital event [53]. However, there are significant similarities between the approaches and underlying philosophies of software engineering and computer forensics: a focus on delivering a quality product, the importance of structured and scientific methods, the application of repeatable processes, the application of computer science concepts, the reuse of knowledge and components, and the application of software tools for supporting methods and processes. Furthermore, non-formal software engineering domain modeling methods are suitable for modeling computer forensics case domains because:

- Representations such as UML and entity relationship diagrams are designed such that a layperson customer or software system stakeholder can review and validate the model. It is likely that computer forensics case stakeholders (investigators, lawyers, juries, etc.) will also be capable of reviewing and validating the model.

- The UML and entity relationship diagram representations provide sufficient power to model the information domain of a computer forensics case. Computer forensics case domains are populated with related concepts that can be described by attributes.

- The purpose of domain modeling in software engineering is aligned with the purpose of case domain modeling. In both instances, the information domain is defined in order to define the scope of development or investigative activities.

3.2 Characteristics of Target Users

The target users of the methodology described in Section 3.3 are teams of forensics analysts, intelligence analysts, forensics technicians, investigators, and

attorneys who routinely conduct large-scale computer forensics examinations. Complex and large-scale computer forensics examinations are mostly conducted by federal law enforcement, regulatory, and defense organizations such as the Federal Bureau of Investigation (FBI), the Internal Revenue Service (IRS), and the Central Intelligence Agency (CIA). These agencies have the abundant personnel and financial resources required to conduct large-scale computer forensics examinations. The computer forensics examination team members are more likely to have college degrees in accounting or criminal justice than in computer science, and they are trained in computer forensics by their employers.

In such large-scale computer forensics examinations, there may be an abundance of diverse case information often related to an unfamiliar case domain. Consequently, there is a high degree of uncertainty regarding the goals of a large-scale examination. For example, a computer forensics team may be tasked with imaging and examining more than 30 workstations and a few servers if they conduct white collar crime investigations of corporations or large organizations. In such circumstances it can be difficult to characterize the evidence of a crime and clearly outline the scope and goals of the forensics examination. This methodology for examination planning manages case complexity by providing a structured approach for analyzing the case information, developing planning products, and identifying evidence.

3.3 Case Domain Modeling Examination Planning Method

Table 3.1 defines the four activities of the methodology and specifies the products of each activity. Figure 3.1 illustrates the relationship between the products of the

methodology. Starting with the case domain model, each subsequent product is built upon its predecessor. Thus all products can be traced back to elements in the case domain model. The remainder of this section provides details for each activity in the methodology.

Table 3.1 Examination Methodology Activities and Products

Activity	Products
1. Model the information domain of the case	Case domain model
2. Define search goals	Statement of search goals
3. Specify search methods for each goal	Keyword search lists and statements of search strategies
4. Conduct the examination	Evidence bookmarks and traceability matrices
Revisit activities and products when necessary: Domain modeling is an iterative process, and when new information is discovered, the model must be changed to reflect the new information. Also, new goals may be developed based on the findings of an examination.	

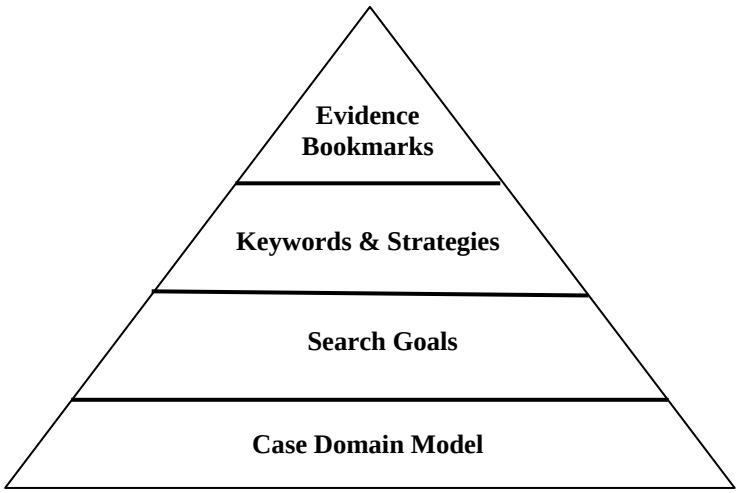


Figure 3.1 The Traceable Relationship of the Examination Methodology Products

3.3.1 Case Domain Modeling

The goals of case domain modeling are to analyze and organize the information domain of the forensics case. This case domain represents the known and unknown information that is relevant to the forensics examination. The case domain modeling method is derived from the UML conceptual modeling method presented by Larman [43]. This method consists of four phases, and each phase may be repeated during the modeling activity (it is a non-linear process):

1. Identify concepts,
2. Identify relationships,
3. Identify attributes, and
4. Instantiate the model.

The fundamentals of domain modeling are adapted from software development to computer forensics. However, specific heuristics and methods are required for domain modeling in the context of computer forensics examination. The remainder of this section describes how each of the generic domain modeling steps should be executed in the examination planning methodology.

3.3.1.1 Identifying Concepts

The concept is the foundational element of the case domain model. Concepts are entities that are relevant to the computer forensics portion of the investigation. A concept is described by zero or more attributes and is related to at least one other concept. These concepts should include information required to conduct the examination and information that will be sought by the examination. It is important to begin with an extensive list of

concepts and gradually eliminate concepts that are irrelevant. Reusability is another important factor to consider when selecting concepts; reusing concepts can save time when developing future case domain models. A concept name that is more abstract is easier to reuse than a concept name that is more specific. For example, S*uspect* is more general than *John Smith* and thus is easier to reuse in a later case. An attribute such as *Name* may be included in the S*uspect* concept in order to distinguish between actual instances of the concept. Some of the eliminated concepts can be modeled as attributes instead of concepts, so it is useful to preserve the candidate list of concepts for later use.

Identifying concepts in a case domain is a brainstorming activity that is supported by concept category checklists and noun–verb extraction. The USDOJ's *Electronic Crime Scene Investigation: A Guide for First Responders* provides checklists (pp. 42-44) of common evidence entities that should be sought in certain types of investigations [70]. Tables 3.2, 3.3, and 3.4 provide a complete reproduction of the USDOJ checklist as it appeared in their guide [70]. The evidence entities in these checklists can be directly mapped to case concepts.

Table 3.2 USDOJ Evidence Targets by Case Type (Part 1)

	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											✓			

Table 3.3 USDOJ Evidence Targets by Case Type (Part 2)

	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):														
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"						✓								

Table 3.4 USDOJ Evidence Targets by Case Type (Part 3)

	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		✓												

A more general concept category checklist should also be used to enumerate the common types of concepts with examples relevant to the computer forensics domain. Table 3.5 provides a concept category table that is tailored to the computer forensics application domain. The modeler must brainstorm on each concept category and determine if there are relevant case concepts that fit the category.

Table 3.5 General Concept Category Checklist

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

Finally, if the concept checklists do not provide a sufficient list of concepts, then a list of candidate concepts is identified by extracting nouns and verbs (known as noun–verb extraction) from case documents such as underlying facts and circumstances, warrants, subpoenas, arrest reports, incident reports, etc. [43].

3.3.1.2 Identifying Relationships

For the purposes of planning a forensics investigation, the concept names and attributes are the most important items of information; concepts and attributes are the relevant pieces of information that the technician will use to seed the examination plan. However, relating the concepts adds an additional layer of information that can help an outsider understand the background and circumstances of a case. Larman's relationship category table (see Table 2.8) can be adapted to identify typical relationships that may occur between case domain concepts [43]. Table 3.6 provides a concept relationship category table with some examples common to computer forensics examinations.

When too many relationships are selected, then the complexity of the case domain model becomes unmanageable. Larman states that "…it is undesirable to overwhelm the conceptual [domain] model with associations [relationships] that are not strongly required and which do not illuminate our understanding. Too many un-compelling associations obscure rather than clarify" [43]. Thus, redundant and derivable relationships should be avoided in favor of essential relationships that foster an understanding of the case domain. Multiplicity (also called cardinality) constraints may be added to the relationships to specify how many items are involved in the relationship: A *Suspect owns*

0 or more *Vehicle*s. Such constraints may enhance case domain understanding, but they are not essential for deriving and identifying important case information.

Table 3.6 Case Domain Modeling Relationship Category Table

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

3.3.1.3 Identifying Attributes

Attributes are the defining characteristics of a concept, and they represent the information that is essential to the computer forensics examination. These attributes may be referred to when constructing keyword searches, examining text documents, examining network logs, etc. For example, when looking for documents that refer to the

suspect, the *name* attribute of concept *Suspect* can be elaborated to form a short keyword list that includes initials, nicknames, first name, last name, middle name, etc.

Concepts and relationships are very similar, and it is up to the modeler to determine if something should be modeled as an attribute or a concept. Because of this inherent similarity, the concept category tables are also used as brainstorming tools to identify attributes. As a minimum, the list of attributes should be exhaustive enough to uniquely distinguish between instances of a concept. For example, the *name* attribute is insufficient for distinguishing between unique instances of a *Suspect* concept. Appending this attribute list with *social security number* is sufficient information to distinguish between two distinct instances of *Suspect*. As was the case with other phases of the methodology, it is important to maintain a moderate approach between providing a comprehensive attribute list and providing a minimal attribute list.

3.3.1.4 Instantiate the Model

To instantiate the model, the attributes must be assigned actual values. The attributes for each concept should be categorized as known or unknown. Known values are assigned values, and attributes with unknown values should be flagged as "unknown." When appropriate, the forensic examination activities will attempt to find the values of the unknown attributes, and the known attribute values will be developed into keyword search lists. Alternatively the occurrence of too many unknown attribute values may indicate to the modeler that additional case information must be collected before proceeding with the examination. It is also important to flag any attribute values that are misspelled words in documents written or referenced by the suspects, witnesses, or

victims involved in the case. Because people commonly misspell the same words, known misspellings are powerful keyword searches that can help find documents authored by an individual.

3.3.1.5 Representing the Model

The UML conceptual diagram is used as the graphical syntax for case domain models. Figure 3.2 provides an illustration of a case domain model for an email death threat case at a university. Tools such as Microsoft Visio and ArgoUML can be used to create a graphical case domain model. Attributes with unknown values are flagged with boldface and underlined font. Known attribute values must be excluded from the diagram to conserve page space. Instead of including them in the diagram, known concept attribute values should be included in a separate table.

Alternatively, the case domain model can be represented without using graphical notations. A case concept can be described in a text form that has blanks for concept name, attribute names, attribute values, and related concepts. In the tabular representation, the emphasis is placed on the case concepts and attributes instead of the relationships. A graphical representation of a case domain model is most useful when the investigation involves a large team of analysts and investigators, the expected investigation time is relatively long, and the investigators are accustomed to the use of visual aids as analytical tools. The tabular representation is more appropriate when there is a small team (possibly even one person) involved in the forensics investigation and the expected investigation time is short.

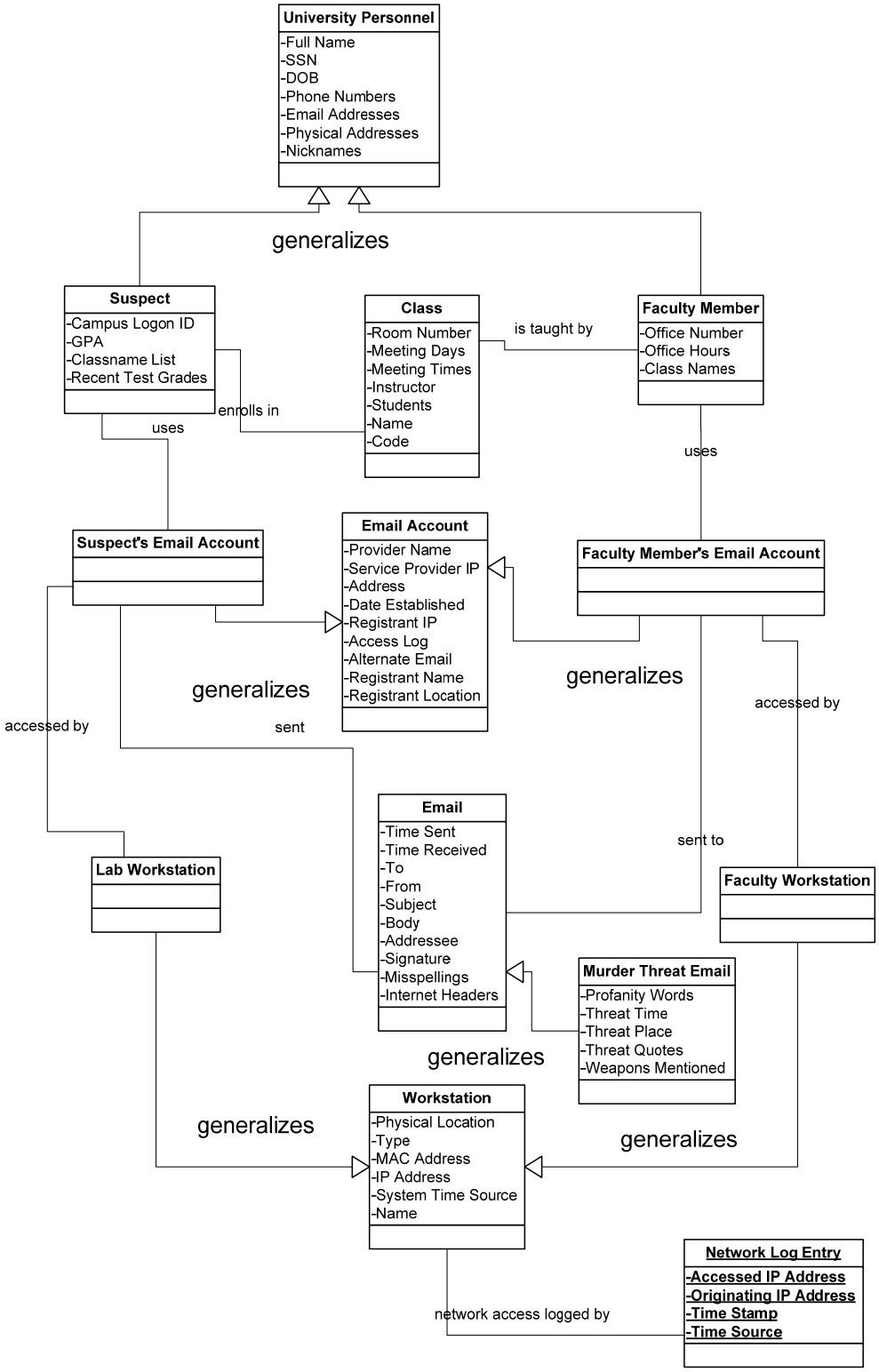


Figure 3.2 University Death Threat Email Case Domain Model Diagram

3.3.2 Developing Search Goals

Search goals identify a concise search requirement for the examination and reference the relevant items in the case domain model. Search goals may be represented in a table that includes the following items of information: an ID tag that is unique to the case, a concise goal statement that references one or more concepts in the domain model, the purpose for the search goal, a list of all relevant concepts and attributes, a list of known attribute values, and a list of unknown attribute values that should be sought. Table 3.7 presents a search goal table for the email death threat case scenario.

Table 3.7 Example Search Goal Table

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

3.3.3 Developing Keyword Lists and Search Strategies

Keyword lists are often an important artifact for defining the scope of a search warrant and an examination. A keyword list should be developed for each known attribute value referenced in a search goal table. The keyword list should reference one or more goal IDs, identify the concept and attribute, specify a location(s) for the search, and uniquely identify each element in the keyword search list. Table 3.8 provides an example keyword list for the home phone number attribute referenced by the search goal in Table 3.7. The example enumerates common string representations of a phone number.

Attribute values can be elaborated into keyword lists by identifying synonyms, abbreviations, and other alternative representations. For example, a keyword list for the date value of October 31, 2005 may contain the following items: 10/31/2005, 10/31, 10/31/05, Halloween 2005, 10-31-2005, 31 October, October 31st, etc. As was the case with identifying case domain concepts and relationships, it is important to maintain a balance between providing a comprehensive list and providing a concise list. Apply logical operators to combine and/or exclude terms. Depending on the search tool used, various logical operators can be added to a search string (e.g. OR, AND, NOT, CONTAINS, NEAR). These logical operators can be used to represent the relationships that exist between concepts in the case domain model. For example, to find documents that establish a relationship between John Smith (suspect) and Jane Doe (victim), the search string can specify a logical-AND combination of the two persons' last names: Smith AND Doe.

Table 3.8 Keyword Search List Example

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

Keyword search terms should be prioritized in each list according to their likelihood of finding the search target. Best practices for keyword searching in computer forensics cases can provide additional support for the keyword search term selection methodology [16, 26].

Finally, general search strategies must be developed to support the search goals. These search strategies are techniques that may be used to supplement or as an alternative to keyword searching. Each search strategy statement should reference a goal ID, be uniquely identified, describe the prescribed strategy or heuristic, and reference relevant concepts in the case domain model. Table 3.9 presents an example collection of search strategies for the search goal in Table 3.7.

Table 3.9 Example Search Strategies

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

3.3.4 Conducting the Examination

Examinations are conducted using forensics software that allows users to bookmark file items that are of interest to the technician. Most commonly these bookmarks indicate an item that will be entered into evidence in the final report. Computer forensics tools such as Forensics Toolkit allow the user to enter metadata about the bookmark that includes a name and a description. For this methodology, bookmark metadata must contain a reference to the search strategy or keyword search term ID that was used to locate the file item. If the file item was found using a technique other than one identified in the plan, then a description of this search method should also be indicated in the bookmark metadata. Making such a reference indicates how the file item was found and allows the file item to be traced back to elements of the examination plan. After the examination is finished, a report should be generated that indicates which activities were conducted and which ones produced bookmarked results. Reviewing this report provides a way to check the completeness of the results with respect to the plan. If

it is determined that some critical elements of the plan were not executed, then the examination may be revisited. Table 3.10 presents an example of such a report.

Table 3.10 Example Examination Results Table

Keyword ID	**Performed? (Y/N)**	**Evidence Bookmark Names**
K-1.1.1	Y	Victim Digdirt Report
K-1.1.2	Y	None
K-1.1.3	Y	None
Strategy ID	**Performed? (Y/N)**	**Evidence Bookmark Names**
S-1.1	N	None
S-1.2	Y	Victim's photograph, Directions to Victim's Home
Other Activities	**Performed? (Y/N)**	**Evidence Bookmark Names**
Keyword Search String "Doeman"	Y	None
Keyword Search String on misspelled word "exert"	Y	Suspect Correspondence

Analysis of the results will likely reveal new information about the case domain than was unknown during the planning activities, and analysis of the results may also necessitate further planning and examining. In such circumstances it is necessary to revise the domain model and revisit previous phases of the planning methodology.

3.4 Summary

This chapter described the examination planning method that was used in the experiments described in Chapter 4 and Chapter 5. The purpose of case domain modeling is to provide a rigorous analytical method for analyzing case details, filtering important

forensic-relevant case information, and providing the foundation for an organized and focused forensics examination plan. Chapter 4 and Chapter 5 evaluate this case domain modeling method by presenting the results of three experiment trials. These experiments compare the effectiveness of case domain modeling versus a more ad hoc examination planning approach.

CHAPTER IV

CASE DOMAIN MODELING APPLICATIONS FOR FORENSICS PRACTITIONERS: PLANNING AND EXECUTING FORENSICS EXAMINATIONS: PART I

This chapter describes how the case domain modeling planning method in Chapter III was evaluated using two experiment trials. These experiment trials required a control group and an experimental group to plan and execute a computer forensics examination. The experimental groups used the case domain modeling method and the control groups used an ad hoc planning approach. The performance of these groups is compared with respect to the amount of evidence found and the amount of time spent in the examination. The remainder of this chapter is organized as follow: Section 4.1 describes the experiment design, Section 4.2 includes the raw data that was collected in the experiment trials, Section 4.3 presents a statistical analysis of the experiment data items, and Section 4.4 concludes this chapter by providing discussion of the results.

4.1 Experiment Design

The experiment population consists of an experimental group, which used the case domain modeling and keyword search derivation methodology, and a control group, which did not use the case domain modeling approach. Each group used their respective methods to plan an examination, conduct keyword searches, and record the results. Table 4.1 provides the design details of the experiment.

Table 4.1 Experiment 1 Design

Experiment ID	E1
Research Questions Addressed	1. Does the case domain modeling methodology result in an increased amount of evidence found in an examination? 2. Does the case domain modeling methodology require a significant amount of additional effort when compared to a typical approach?
Hypotheses	• The experimental group will identify more evidence than the control group. • The experimental group will spend more time planning their keyword searches than the control group. • The experimental group will spend less time executing their keyword searches than the control group. • Overall, the experimental group will spend more time in the experiment than the control group.
Experimental Group	Subjects who were provided training in how to use the case domain modeling approach to forensics keyword search planning.
Control Group	Subjects who were provided training in how to use a typical approach to forensics keyword search planning.
Independent Variable	Presence or absence of the case domain modeling approach in the task of computer forensics keyword search planning and execution.
Dependent Variables	• The amount of evidence recovered from the provided media • The amount of effort required for planning keyword searches • The amount of time spent executing keyword searches
Confounding Variables	• The variability of subjects' forensics skills o This was controlled by asking subjects to voluntarily tell the grade they received or currently hold in the CS 4273/6273 course
Experiment Subject Population	• MSU CSE students who were enrolled in CSE 4273/6273 (Introduction to Cyber Crime and Computer Forensics) during the fall 2005 semester.
Number of Subjects	31
Experiment Site	Mississippi State Department of Computer Science and Engineering
Incentives	None

Table 4.1 (continued)

Experiment Method	• Subjects volunteered for the experiment and signed a consent form. • Subjects committed to participate on a specific time, date, and place. • Prior to the experiment, the control group and the experimental group were given a separate 60-minute lectures on how to plan and execute a keyword search. The control group was given instructions that are characteristic of a typical approach to keyword search planning/execution, and the experimental group was given instructions on how to plan/execute a keyword search using the case domain modeling method. • When the experiment was conducted, the control group and the experimental group were placed in separate rooms. They were given the following materials: a case file, one evidence hard drive, experiment instructions, pens, 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 hard drives. o Each group was given a four-hour time limit to complete this task, but they were allowed to quit when they felt they had found all of the evidence. o The groups were instructed to take detailed notes on their keyword search plan, the results of their search, and the time that planning/execution events occurred. Details on how this documentation was to be recorded were provided in the experiment instructions. When appropriate, forms were provided as documentation tools. • At the conclusion of the experiment, each group submitted their notes and results to the principal investigator or the faculty advisor (Dr. Dampier). They also completed an exit survey that evaluated the qualitative factors of their keyword searching method.

Table 4.1 (continued)

Experiment Preparations	• A case scenario, a case file, and evidence hard drives were developed prior to the experiment.
	  o As a class project, student teams in the fall 2005 CSE 4273/6273 course prepared these materials. The class was divided into four teams, and each team developed a unique case scenario and case file and hid evidence on a hard drive. For the final class project, each team attempted to find the evidence hidden by another team.
	  o When recruiting subjects, the principal investigator ensured that participants from the fall 2005 CSE 4273/6273 course were not given an evidence disk that they have seen before; they did not have developed the hard drive or examined it prior to the experiment.
	• Instructional materials were developed for keyword search planning with case domain modeling and with the typical approach. The participants were given the training lecture Power Point slides for use in their search planning and execution.
	• Instructional materials were developed for directing the experimental and control groups' participation in the experiment, including instructions on how to complete the experiments.
	• A domain modeling software, Visio, was installed on the experimental group computers.
	• A qualitative exit survey was drafted.
	• 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 were reserved by contacting Dr. Dampier and Keri Chisolm (Systems Administrator).

Required Resources	• 24 hard drives (20–80 GB) • 24 Forensics Workstations with Forensics Toolkit software • 12 Forensics Workstations with the case domain modeling tool, Microsoft Visio. • Hard copies of all written materials: a case file, instructional materials, and an exit survey • 2-4 rooms/labs in the CSE department (depending on the size of the rooms)

4.1.1 The Control Group Preparation Method

Chapter III outlined the case domain modeling method that is prescribed for the experimental groups in Experiment 1. This sub-section outlines the preparation method prescribed for the control groups in Experiment 1. The control group preparation method is a sequence of four activities:

1. Summarize the case facts and information relevant to forensics activities,
2. Classify the case type and relevant evidence sources,
3. Develop a keyword search list, and
4. State plans for other forensics activities.

The goal of the control group method is generally the same as for the experimental group method: identify the relevant facts, develop a keyword search list, and plan non-keyword searching activities. However, the control group method is ad hoc in the sense that there is no rigorous analytical process to follow for each of these activities. Instead, the purpose of each activity is briefly described and the subjects are instructed to complete the activities by writing lists and notes.

4.1.2 Organization of Subject Population

As identified in Table 4.1, the experiments' case scenarios, case information, and evidence files were prepared by Mississippi State University (MSU) students enrolled in the fall 2005 Introduction to Cybercrime and Computer Forensics CSE 4273/6273 course. There were forty-nine students attending the course at MSU. Additionally there were twenty distance learning students at Jackson State University (JSU), and two distance learning students at the United States Army Corps of Engineers Engineering Research

and Development Center (USACE-ERDC) in Vicksburg, MS. The distance learning students did not participate in the experiments. As a class assignment, Dr. Dampier required all MSU students (this excludes the JSU and USACE-ERDC students) to participate in a group that must prepare a case scenario, a case file, and an evidence hard drive. Later in the semester, each group exchanged their work with another group and attempted to find the hidden evidence. There were four groups with eleven or twelve students in each group. Figure 4.1 illustrates the organization of groups with respect to evidence files according to the CSE 4273/6273 course assignment. Dr. Dampier also required that these groups keep their evidence preparation and examination work secret

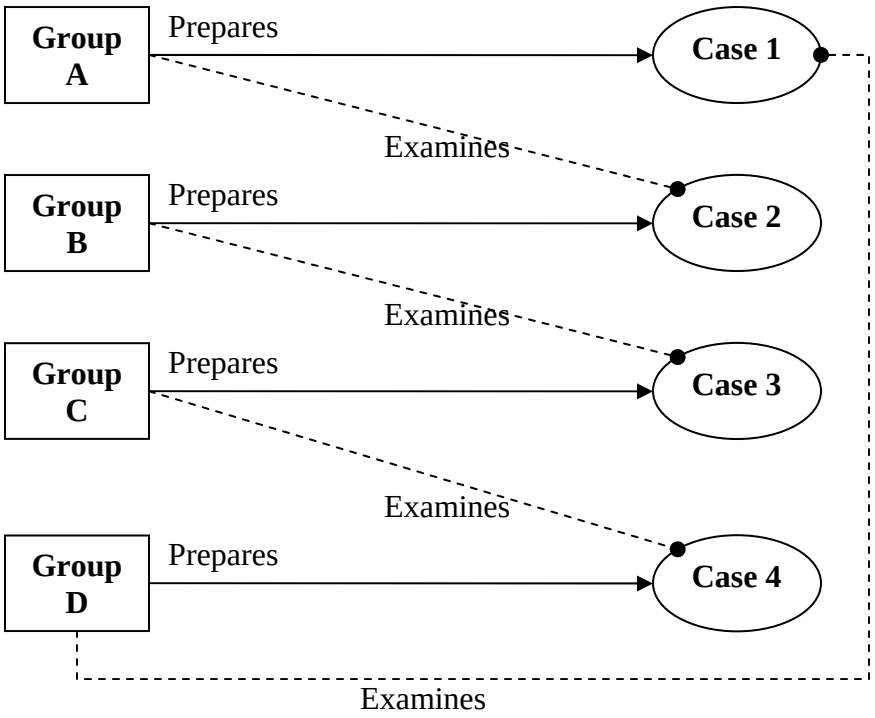


Figure 4.1 CSE 4273/6273 Group Assignment Organization

from other groups or other individuals outside of the course. Assuming that this confidentiality was maintained and that the group assignments were successfully completed, then there are exactly two cases unfamiliar to each group. Figure 4.2 illustrates the relationships between the groups and their unknown cases.

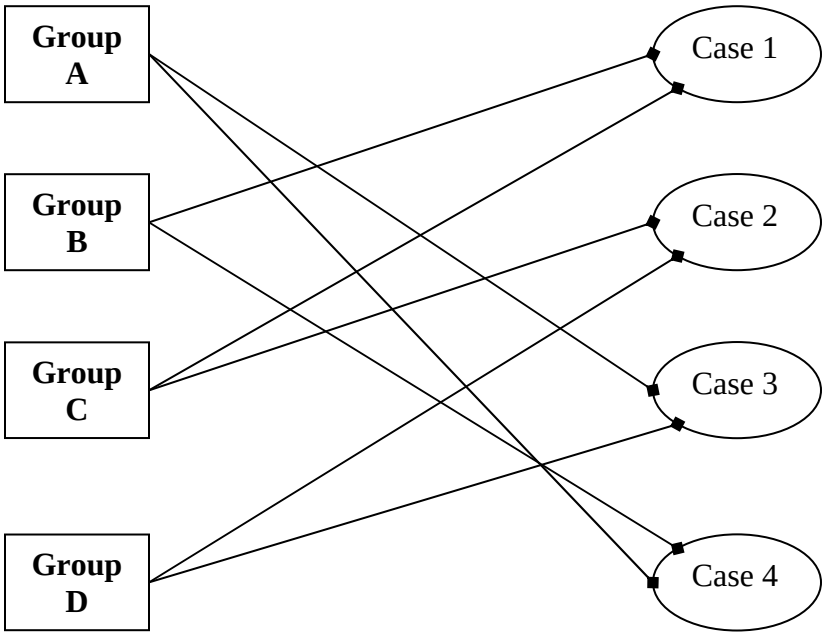


Figure 4.2 CSE 4273/6273 Groups Linked to Their Respective Unknown Cases

Additional constraints were placed on the organization of the experimental and control group subjects in Experiment 1. These constraints were imposed in an attempt to make the population uniform and balanced with respect to forensics expertise. First, in both experiments the experimental and control groups were balanced according to skill level. The students were categorized into three skill groups according to their CSE

4273/6273 grade average rankings. To the highest extent possible, equal numbers of subjects from each skill group were placed in the experimental and control groups. Furthermore, in Experiment 1, the experimental groups and control groups were balanced according to which evidence materials they had been exposed. Figure 4.3 illustrates the final organization of the experimental groups and control groups for Experiment 1. This approach to evidence preparation included the following disadvantages:

- Planning and coordination effort was required in order to ensure that fall 2005 CSE 4273/6273 students did not work on cases that they have developed or examined prior to the experiment.
- Additional time was spent configuring hardware resources to accommodate two different sets of evidence.
- The subject population was distributed across two pairs of experimental and control groups. This made it more difficult to draw statistical conclusions regarding the difference of means in the data.

However, the benefits of using the student-prepared evidence outweighed the disadvantages. The benefits of the adopted evidence preparation approach included:

- The principal investigator focused his initial experiment efforts on preparing instructional materials for the experiment instead of preparing case scenarios, case files, and evidence hard drives.
- The principal investigator was restricted from consciously or subconsciously producing a case scenario and evidence that is biased in favor of the case domain modeling methodology.
- The case domain methodology was evaluated on two case types that were prepared by two independent groups. This provides additional insight regarding the applicability of case domain modeling to specific case types.

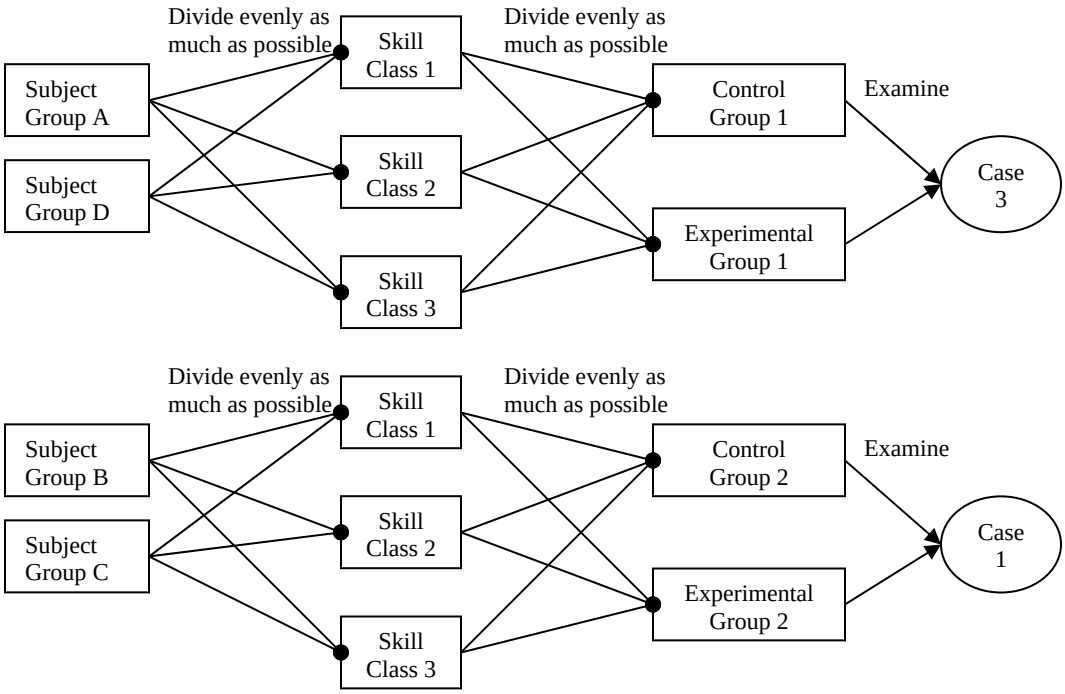


Figure 4.3 Experiment 1 Subject Division and Organization

4.1.3 The Prepared Evidence Drives and Scenarios

As described in Section 4.1.2, the subject population was divided into four major groups: A, D, B, and C. Groups A and D were combined, separated into an experimental group and a control group, and assigned to work on the evidence and scenario known as Case 3. Likewise Groups B and C were combined and partitioned into experimental and a control groups, and they worked on the evidence and scenario known as Case 1.

Case 3, known as Alpha Delta, was an identity theft and hacking scenario. The scenario stated that twelve bank statements of allegedly stolen identities were found in a public place in proximity to a suspect. A half-page description of the scenario and the

twelve bank statements were prepared as background information to distribute to the examiners. The Alpha Delta evidence drive has an advertised capacity of 40 gigabytes (GB), and its allocated space was divided among three logical partitions: an 18.4-GB partition, a 17.6-GB partition, a 1.02-GB partition (the remaining space is unallocated). A total of 2,981 file items were present on the disk, including 99 evidence files. Figure 4.4 illustrates the distribution of file item types on the evidence drive.

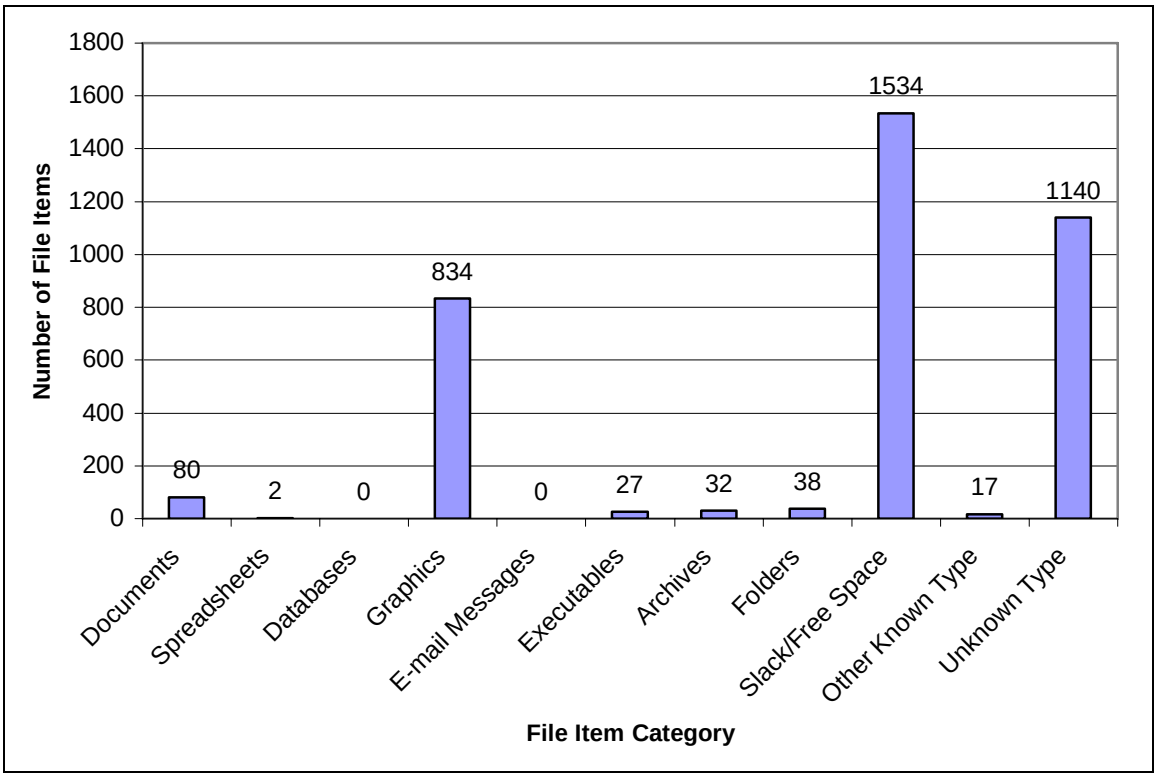


Figure 4.4 Distribution of File Item Types on the Alpha Delta Evidence Disk

The ratio of evidence files to non-evidence files was 3.32%. The 99 evidence files were distributed as follows:

- 43 files contained mass lists of stolen identity information such as social security numbers and credit card numbers,
- 44 files contained instructional materials for hacking and other illicit activities,
- 1 file contained an archive of pictures that were modified using steganography to contain stolen identity information,
- 1 file contained a text passage where the suspects indicated their use of steganography to hide information, and
- 10 files were executables or archive files that contained what may be considered as hacker software tools.

Case 1, known as Bravo Charlie, was a bank robbery, burglary, and money laundering scenario. Figure 4.5 illustrates the distribution of file types on the Bravo Charlie evidence disk.

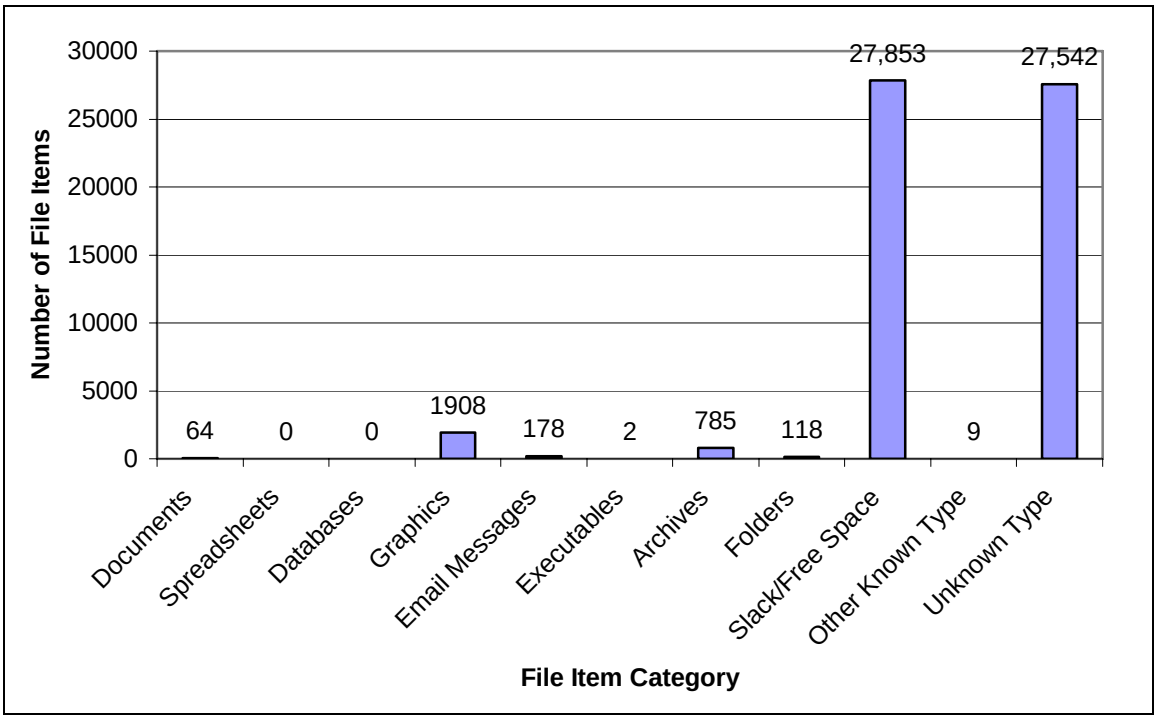


Figure 4.5 Distribution of File Item Types on the Bravo Charlie Evidence Disk

No scenario statement was prepared, but the hard copies of 12 bank statements, 3 Dallas, TX, news headlines (describing robberies), and 3 map images of a bank were prepared as artifacts that were found near the suspect computer. The Bravo Charlie evidence hard drive also had a 40-GB advertised capacity, and it contained two logical partitions: an 18-GB partition and a 19.2-GB partition (the remaining space was unallocated). A total of 58,459 files were present on the Case 1 disk, including 29 evidence files. The ratio of evidence to non-evidence files was 0.0496%. The 29 evidence files were distributed as follows:

- 9 files containing email messages written to and by the suspects; these messages contained references to their illegal activities,
- 11 image files that illustrated things such as the architectural layout of the robbed bank and various Dallas, TX, landmarks, and
- 9 html files that provided tourist information about the Dallas, TX, area of the robbed bank and the jewelry store.

4.1.4 Experiment Logistics

All of the facilities, software, and hardware used in this experiment were owned and maintained by the MSU Department of Computer Science and Engineering. The following resources were used in the experiments:

- Three classrooms,
- 20 PC workstations with the Forensic Toolkit software package, and
- 20 40-GB hard drives.

4.2 Data items Collected

The same data items were collected for both the Alpha Delta and the Bravo Charlie experiment populations. These data items may be categorized as time, performance, and survey data. The time data items represent the amount of time the subjects spent preparing and executing their examination. A cell phone clock was used as the official time, and the starting and finishing times for each subject were recorded by the principal investigator and his assistants. The performance data items represent how much of the scenario evidence the subjects located and bookmarked in their examination.

The subjects' Forensic Toolkit case files were reviewed against a "solution" file that indicated where the scenario evidence was located on the evidence drive. The survey data was collected from a post-experiment evaluation survey that included multiple choice and short answer questions. The data items collected from the multiple choice portions of the surveys provide insight into the practicality and effectiveness of the subjects' preparation and examination methods. The following subsections present the data items that were collected in the Alpha Delta and Bravo Charlie experiment trials.

4.2.1 Data items Collected: Alpha Delta Trial

Table 4.2 presents the time data items collected on the Alpha Delta group during the planning session and the examination session. Time is expressed in minutes. The upper half of the table provides time data items for the control group (ad hoc planning approach), while the bottom half of the table provides time data items for the experimental group (case domain modeling planning approach). This scheme is also used in the other tables in this section.

Table 4.3 provides a summary of the amount of evidence located by the Alpha Delta groups. The amount of evidence is expressed in percentages. The evidence is also categorized into four groups: Stolen Identity (ID) files, Hacker References, Steganography (Steg) Evidence, and Hacking Tools. The overall or total percent of evidence found is also provided in the right-most column.

Table 4.4 presents data regarding the amount of evidence found using specific search methods. Values are expressed in terms of the percentage of overall evidence that was successfully located using the specified search method.

Table 4.2 Alpha Delta Planning and Execution Effort

Control Group Subjects	**Planning Session Time (min.)**	**Examination Session Time (min.)**	**Total Time (min.)**
AD1-1	92	160	252
AD1-2	92	141	233
AD1-3	92	161	253
AD1-4	92	154	246
AD1-5	103	135	238
AD1-6	116	120	236
MEAN →	97.83	145.17	243
Experimental Group Subjects			
AD2-1	137	129	266
AD2-2	137	146	283
AD2-3	169	194	363
AD2-4	174	185	359
AD2-5	171	184	355
AD2-6	189	164	353
MEAN→	162.83	167	329.83

Table 4.3 Alpha Delta Amount of Evidence Found Data Items

Control Group	% Stolen ID Files	% Hacker References	% Steg Evidence	% Hacking Tools	Overall %
AD1-1	100	56.82	50	80	77.78
AD1-2	2.26	29.55	0	20	16.16
AD1-3	100	36.36	50	20	62.63
AD1-4	11.63	43.18	50	20	27.27
AD1-5	6.98	13.64	50	50	15.15
AD1-6	100	70.46	0	10	75.76
MEAN→	53.48	41.67	33.33	33.33	45.79
Experimental Group	**% Stolen ID Files**	**% Hacker References**	**% Steg Evidence**	**% Hacking Tools**	**Overall %**
AD2-1	100	59.09	0	20	71.72
AD2-2	97.67	84.09	50	50	85.86
AD2-3	97.67	45.46	100	60	70.71
AD2-4	97.67	11.36	0	10	48.48
AD2-5	2.33	15.91	0	0	8.1
AD2-6	4.65	18.18	0	10	11.11
MEAN→	66.67	39.02	25	25	49.33

Table 4.4 Alpha Delta Amount of Evidence Found by Searching Methods

Control Group	% Evidence Found with Planned Keyword Searches	%Evidence Found with Unplanned Keyword Searches	% Evidence Found with Keyword Searches	% Evidence Found Using Non-Keyword Searches
AD1-1	40.40	2.02	42.42	71.71
AD1-2	40.40	0	40.40	12.12
AD1-3	10.10	17.17	27.27	35.35
AD1-4	23.23	0	23.23	4.04
AD1-5	13.13	1.01	14.14	1.01
AD1-6	45.45	10.10	55.55	20.20
AVERAGE	28.79	5.05	33.84	24.07
Experimental Group				
AD2-1	1.01	47.47	48.48	23.23
AD2-2	2.02	44.44	46.46	39.39
AD2-3	3.03	5.05	8.08	62.62
AD2-4	46.46	2.02	48.48	0
AD2-5	8.08	0	8.08	0
AD2-6	2.02	6.06	8.08	3.03
AVERAGE	10.44	17.51	27.94	21.38

Searching methods are categorized as planned keyword searches, unplanned keyword searches, all keyword searches, and non-keyword searches. Planned keyword searches were identified during the planning session, while unplanned keyword searches were specified during the examination session; these two categories are aggregated to represent all keyword searches. Non-keyword searches include any method other than keyword searching that the subjects used to find evidence.

Table 4.5 presents the post-experiment multiple choice survey questions. Table 4.6 presents the multiple responses of the Alpha Delta group. The alphabetic multiple choice identifiers (a-e) were replaced with numerical identifiers (1-5). Questions Q1, Q2, and Q3 have a range of 1–5, while questions Q4 and Q5 have a range of 1–4. A listing of the responses from the two survey discussion questions is omitted, but insightful survey responses will be cited when appropriate.

Table 4.5 Alpha Delta Multiple Choice Post-Experiment Survey Questions

Q1	Was the time you spent preparing appropriate for the examination task? a. My preparation time was extremely short considering the difficulty of the examination: I should have spent at least 2 additional hours preparing b. My preparation time was somewhat short considering the difficulty of the examination: I should have spent an additional 30 minutes – 1 hour preparing. c. I spent just the right amount of time preparing for the examination task d. I spent a little too much time preparing: I over-prepared by approximately 30 minutes – 1 hour e. I spent way too much time preparing: I over-prepared by at least 2 hours
Q2	Did your preparation efforts contribute to a clear and complete understanding of the case? a. The preparation effort contributed to confusion regarding case concepts and case facts b. The preparation effort was not helpful for understanding or identifying important case concepts c. The preparation effort was somewhat helpful for understanding or identifying important case concepts. d. The preparation effort was helpful in understanding and identifying important case concepts e. The preparation effort was very helpful in understanding and identifying important case concepts.
Q3	Estimate your level of confidence in the results of your examination? a. I found less than 20% of the evidence b. I found between 20-40% of the evidence c. I found between 41-60% of the evidence d. I found between 61-80% of the evidence e. I found between 81-100% of the evidence
Q4	Were you given a sufficient amount of time to execute the examination? a. I needed a significant amount of additional time to execute the examination (> 2 hours) b. I needed additional time to execute the examination (1-2 hours) c. I needed a little bit of additional time to execute the examination (30 minutes – 1 hour) d. I executed all planned activities and was given a sufficient amount of time to execute the examination.
Q5	Did you spend additional time developing or brainstorming keyword searches after the preparation sessions/during the examination? a. I developed several keyword searches during the examination session (> 20) b. I developed some keyword searches during the examination session (10-20) c. I developed very few keyword searches during the examination session (1-10) d. I developed no keyword searches during the examination session

Table 4.6 Alpha Delta Multiple Choice Survey Data Items

Control Group	Q1	Q2	Q3	Q4	Q5
AD1-1	3	4	4	4	1
AD1-2	3	3	2	4	3
AD1-3	4	2	4	4	3
AD1-4	3	4	3	4	3
AD1-5	3	4	2	4	3
AD1-6	3	4	4	4	3
MEDIAN	3	4	3.5	4	3
Experimental Group					
AD2-1	4	4	4	4	3
AD2-2	1	3	3	4	2
AD2-3	3	3	2	4	1
AD2-4	2	4	5	4	3
AD2-5	3	3	2	4	3
AD2-6	3	4	1	4	2
MEDIAN	3	4	2.5	4	3

4.2.2 Data Items Collected: Bravo Charlie Trial

Table 4.7 presents the time data items collected on the Bravo Charlie group during the planning session and the examination session. Time is expressed in minutes. The upper half of the table provides time data items for the Bravo Charlie control group, while the bottom half of the table provides time data items for the Bravo Charlie experimental group. This scheme is also used in the other tables in this section.

Table 4.8 provides a summary of the amount of evidence located by the Bravo Charlie groups. The amount of evidence is expressed in percentages. The evidence is also

Table 4.7 Bravo Charlie Planning and Execution Effort

Control Group	Planning Session Time (min.)	Examination Session Time (min.)	Total Time (min.)
BC1-1	85	120	205
BC1-2	89	119	208
BC1-3	104	74	178
BC1-4	62	99	161
BC1-5	114	79	193
BC1-6	99	122	221
BC1-7	72	114	186
AVERAGE	89.29	103.86	193.14
Experimental Group			
BC2-1	124	141	265
BC2-2	142	108	250
BC2-3	98	131	229
BC2-4	130	131	261
BC2-5	217	174	391
BC2-6	161	142	303
BC2-7	67	137	204
AVERAGE	134.14	137.71	271.86

categorized into three groups: Emails, Images/Photos, and Dallas, TX area information. The overall or total percent of evidence found is also provided in the right-most column.

Table 4.9 presents data regarding the effectiveness of keyword searching in the Bravo Charlie group. Values are expressed in terms of the percentage of overall evidence that was successfully located using the specified searching method. Searching methods are categorized as planned keyword searches, unplanned keyword searches, keyword searches, and non-keyword searches. Planned keyword searches were identified during the planning session, while unplanned keyword searches were specified during the examination session; these two categories are aggregated to represent all keyword searches. Non-keyword searches include any method other than keyword searching that the subjects used to find evidence.

Table 4.10 presents the post-experiment multiple choice survey questions (this is a repeat of Table 4.5). Table 4.11 presents the multiple responses of the Bravo Charlie group, and the alphabetic multiple choice identifiers (a–e) were replaced with numerical identifiers (1–5). Questions Q1, Q2, and Q3 have a range of 1–5, while questions Q4 and Q5 have a range of 1–4. A listing of the responses from the two survey discussion questions is omitted, but insightful survey responses will be cited in the analysis/discussion sections.

Table 4.8 Bravo Charlie Amount of Evidence Found Data Items

Control Group	% Emails	% Images/Photos	% Dallas, TX Area Information	Overall %
BC1-1	11.1	45.45	88.89	48.28
BC1-2	100	36.36	22.22	51.72
BC1-3	0	0	0	0
BC1-4	0	63.64	55.56	41.38
BC1-5	0	9.09	22.22	10.34
BC1-6	0	45.45	11.11	20.69
BC1-7	11.11	45.45	0	20.69
AVERAGE	17.459	35.06	28.571	27.59
Experimental Group	**% Emails**	**% Images/Photos**	**% Dallas, TX Area Information**	**Overall %**
BC2-1	0	27.27	11.11	13.79
BC2-2	77.78	18.18	22.22	37.93
BC2-3	0	18.18	0	6.90
BC2-4	100	27.27	11.11	44.83
BC2-5	100	45.45	22.22	55.17
BC2-6	100	45.45	22.22	55.17
BC2-7	11.11	72.73	11.11	34.48
AVERAGE	55.56	36.36	14.28	35.47

Table 4.9 Bravo Charlie Amount of Evidence Found with Searching Methods

Control Group	% Evidence Found with Planned Keyword Searches	%Evidence Found with Unplanned Keyword Searches	% Evidence Found with Keyword Searches	% Evidence Found Using Non-Keyword Searches
BC1-1	0	0	0	48.28
BC1-2	6.90	13.79	20.69	13.79
BC1-3	0	0	0	0
BC1-4	0	0	0	41.38
BC1-5	3.45	3.45	6.9	34.48
BC1-6	0	0	0	20.69
BC1-7	0	10.34	10.35	10.35
AVERAGE	1.48	3.94	5.42	24.139
Experimental Group				
BC2-1	10.35	0	10.35	3.45
BC2-2	0	20.69	20.69	3.45
BC2-3	3.45	0	3.45	3.45
BC2-4	0	20.69	20.69	6.90
BC2-5	0	13.79	13.79	24.14
BC2-6	0	10.35	10.35	27.59
BC2-7	10.35	24.14	34.48	0
AVERAGE	3.45	12.81	16.26	9.85

Table 4.10 Multiple Choice Survey Questions

Q1	Was the time you spent preparing appropriate for the examination task? a. My preparation time was extremely short considering the difficulty of the examination: I should have spent at least 2 additional hours preparing b. My preparation time was somewhat short considering the difficulty of the examination: I should have spent an additional 30 minutes – 1 hour preparing. c. I spent just the right amount of time preparing for the examination task d. I spent a little too much time preparing: I over-prepared by approximately 30 minutes – 1 hour e. I spent way too much time preparing: I over-prepared by at least 2 hours
Q2	Did your preparation efforts contribute to a clear and complete understanding of the case? a. The preparation effort contributed to confusion regarding case concepts and case facts b. The preparation effort was not helpful for understanding or identifying important case concepts c. The preparation effort was somewhat helpful for understanding or identifying important case concepts. d. The preparation effort was helpful in understanding and identifying important case concepts e. The preparation effort was very helpful in understanding and identifying important case concepts.
Q3	Estimate your level of confidence in the results of your examination? a. I found less than 20% of the evidence b. I found between 20-40% of the evidence c. I found between 41-60% of the evidence d. I found between 61-80% of the evidence e. I found between 81-100% of the evidence
Q4	Were you given a sufficient amount of time to execute the examination? a. I needed a significant amount of additional time to execute the examination (> 2 hours) b. I needed additional time to execute the examination (1-2 hours) c. I needed a little bit of additional time to execute the examination (30 minutes – 1 hour) d. I executed all planned activities and was given a sufficient amount of time to execute the examination.
Q5	Did you spend additional time developing or brainstorming keyword searches after the preparation sessions/during the examination? a. I developed several keyword searches during the examination session (> 20) b. I developed some keyword searches during the examination session (10-20) c. I developed very few keyword searches during the examination session (1-10) d. I developed no keyword searches during the examination session

Table 4.11 Bravo Charlie Multiple Choice Survey Data Items

Control Group	Q1	Q2	Q3	Q4	Q5
BC1-1	3	3	2	4	3
BC1-2	2	3	3	4	2
BC1-3	3	3	1	4	2
BC1-4	3	2	3	4	2
BC1-5	2	3	1	4	3
BC1-6	5	5	1	1	3
BC1-7	4	4	3	4	2
MEDIAN	3	3	2.5	4	3
Experimental Group					
BC2-1	3	5	4	4	5
BC2-2	2	4	3	4	3
BC2-3	2	4	3	4	1
BC2-4	3	4	4	4	3
BC2-5	2	3	2	4	2
BC2-6	2	4	2	4	3
BC2-7	3	3	1	4	3
MEDIAN	2	4	3	4	3

4.3 Statistical Analysis of Data Items

The preferred method of statistical analysis of the data items is the paired, one-sided *Student's paired t*-test for significant differences between two independent means. The one-sided *t*-test is used to determine if the mean of one population is significantly greater than the mean of another population; with a 90% confidence interval there is only a 10% chance that the difference was caused by chance. The probability of the null hypothesis, *p*, is the probability that the difference between two means is caused by chance, and 1 – *p* is the probability of assuming the alternative hypothesis that one mean is greater than the other. There are four critical assumptions that must be true in order to use the *t*-test: 1) observations must be independent of one another, 2) the dependent variable must be measured using an interval or ratio scale, 3) the dependent variable from each group must be normally distributed, and 4) the distribution of the dependent variable for each group must have the same variance.

The first two assumptions of the *t*-test—independent observations and interval/ratio scale measurements—are satisfied by the design of the experiment. Assumptions 3 and 4 must be evaluated based on the results of the data collected. When the assumptions for the *t*-test are not satisfied, an alternative Mann-Whitney test is used to evaluate differences between means. The Mann-Whitney test is a non-parametric test used for comparing two independent groups of sampled data. The Mann-Whitney test makes no assumptions about the distribution or the equality of variance in the sample data. Non-parametric tests use the ranks of data (instead of raw values) to calculate statistical differences. It is preferable to compare the differences between the raw data,

and thus the *t*-test is preferred when its critical assumptions are met. The Mann-Whitney test is a two-sided, non-directional test whose alternative hypothesis is that the two means are significantly different; unlike the one-sided, paired *t*-test, the Mann-Whitney test cannot test whether the mean of one population is significantly greater than the mean of another population.

Sub-sections 4.3.1 and 4.3.2 present the results of the statistical tests for the Alpha Delta and Bravo Charlie experiment trials, respectively. The alternative hypotheses for the *t*-tests are based on pre-experiment research questions and hypotheses. All hypotheses in Sub-sections 4.3.1 and 4.3.2 are evaluated based on a 90% confidence interval. Thus, if the probability of assuming the null hypothesis is less than or equal to 10%, then the alternative hypothesis is accepted and a statistically significant difference is observed.

4.3.1 Statistical Analysis of Alpha Delta Trial

According to the sample size, five degrees of freedom are applied on all of the one-tailed Alpha Delta *t*-tests. Table 4.12 presents the results of the normality and equality of variance tests for the Alpha Delta group. Table 4.12 also provides the final conclusion for whether or not the data item is eligible for statistical comparison with the *t*-test.

Table 4.13 presents the results of the *t*-tests and Mann-Whitney tests (applied when appropriate) on the collected time/effort data items for the Alpha Delta groups. If the Mann-Whitney test was conducted, then the field for *t*-values is marked "N/A." Time values are expressed in minutes. Based on the results of these statistical tests, the following statement can be made: The case domain modeling method contributed to an increase in time spent during the planning and execution phases.

Table 4.12 Alpha Delta Data Items *t*-test Eligibility

Data Item	Shapiro-Wilk Normality Test, p	Normal?	2 Variance Equality Test, p	Variance Equal?	*t*-Test Eligible?
Planning Time Con. Group	0.005594	No	0.121	Yes	No
Planning Time Exp. Group	0.191886	Yes			
Execution Time Con. Group	0.470179	Yes	0.341	Yes	Yes
Execution Time Exp. Group	0.491627	Yes			
Total Time Con. Group	0.349366	Yes	0.003	No	No
Total Time Exp. Group	0.019637	No			
%Stolen ID Con. Group	0.009624	No	0.929	Yes	No
%Stolen ID Exp. Group	0.002270	No			
%Hacker References Con. Group	0.994311	Yes	0.440	Yes	Yes
%Hacker References Exp. Group	0.331678	Yes			
%Steganography Con. Group	0.001351	No	0.313	Yes	No
%Steganography Exp. Group	0.006373	No			
%Hacking Tool Con. Group	0.069188	No	0.848	Yes	No
%Hacking Tool Exp. Group	0.230158	Yes			
%Overall Con. Group	0.103523	Yes	0.813	Yes	Yes
%Overall Exp. Group	0.235196	Yes			
%Found w/ Planned Keywords Con. Group	0.217518	Yes	0.747	Yes	No
%Found w/ Planned Keywords Exp. Group	0.000533	No			
%Found w/ unplanned Keywords Con. Group	0.041475	No	0.025	No	No
%Found with unplanned Keywords Exp. Group	0.014540	No			
%Found w/ all Keywords Con. Group	0.302029	Yes	0.437	Yes	Yes
%Found w/ all Keywords Exp. Group	0.906800	Yes			
%Found w/o Keywords Con. Group	0.211162	Yes	0.948	Yes	Yes
%Found w/o Keywords Exp. Group	0.188729	Yes			

Table 4.13 Alpha Delta Mean Differences of Time Data Items

Hypothesis	Control Mean ($\bar{x}$)	Experimental Mean ($\bar{y}$)	*t*	*p*	Outcome
h_{a1}	$\bar{x}$ = 97.83	$\bar{y}$ = 162.83	N/A	0.003	Accept h_{a1}
h_{a2}	$\bar{x}$ = 145.17	$\bar{y}$ = 167	*t* = 1.78	0.932	Reject h_{a2}
h_{a3}	$\bar{x}$ = 243	$\bar{y}$ = 329.83	N/A	0.004	Accept h_{a3}
Hypothesis Legend					
h_{a1} = The experimental group dedicated a significantly different amount of time on the planning session than the control group.					
h_{a2} = The experimental group spent a significantly less amount of time on the execution session than the control group.					
h_{a3} = The experimental group spent a significantly different amount of total time on the experiment exercise than the control group.					

Table 4.14 provides the results of the *t*-tests and Mann-Whitney tests performed on the percent of evidence found by the Alpha Delta experimental and control groups. The means are expressed in percentages. None of these statistical tests on these data items revealed any statistical difference between the amounts of evidence found by the experimental and control groups. However, the experimental group found more overall evidence than the control group and more evidence related to stolen identities (the second largest category of evidence files).

Table 4.15 presents the results of the *t*-tests and Mann-Whitney tests that were performed on the data items related to the amount of evidence found by searching methods. The control group located a statistically significantly greater amount of evidence using planned-keyword searching than the experimental group. The experimental group found a greater amount (non-significant) of evidence using unplanned keyword searches than the control group.

Table 4.14 Alpha Delta Mean Differences of Percentage of Evidence Found Data Items

Hypothesis	**Control Mean ($\bar{x}$)**	**Experimental Mean ($\bar{y}$)**	***t***	***p***	**Outcome**
h_{a4}	53.48	66.67	N/A	0.681	Reject h_{a4}
h_{a5}	41.67	39.02	0.177	0.567	Reject h_{a5}
h_{a6}	33.33	25	N/A	0.476	Reject h_{a6}
h_{a7}	33.33	25	N/A	0.411	Reject h_{a7}
h_{a8}	45.79	49.33	0.198	0.425	Reject h_{a8}
Hypothesis Legend					
h_{a4} = The experimental group located a significantly different amount of evidence files containing victim stolen identities than the control group					
h_{a5} = The experimental group located a significantly greater amount of evidence files containing hacker reference materials than the control group					
h_{a6} = The experimental group located a significantly different amount of evidence files related to the suspect's use of steganography than the control group					
h_{a7} = The experimental group located a significantly different amount of evidence files containing hacking software tools than the control group					
h_{a8} = The experimental group located a significantly greater overall amount of evidence files than the control group					

Table 4.15 Alpha Delta Mean Differences of Search Method Data Items

Hypothesis	Control Mean ($\bar{x}$)	Experimental Mean ($\bar{y}$)	*t*	*p*	Outcome
h_{a9}	28.79	10.44	N/A	0.054	Accept h_{a9}
h_{a10}	5.05	17.51	N/A	0.294	Reject h_{a10}
h_{a11}	33.84	27.94	-0.574	0.705	Reject h_{a11}
h_{a12}	24.07	21.38	0.230	0.414	Reject h_{a12}
Hypothesis Legend					
h_{a9} = The experimental group located a significantly different amount of evidence files using planned keyword searches than the control group					
h_{a10} = The experimental group located a significantly different amount of evidence files using unplanned keyword searches than the control group					
h_{a11} = The experimental group located a significantly different amount of evidence files using planned or unplanned keyword searches than the control group					
h_{a12} = The experimental group located a significantly different amount of evidence files using non-keyword searches than the control group					

Basic frequency distribution statistics are provided for the post-experiment survey data items. Table 4.16 presents the distribution of responses for survey question 1: *Was the time you spent preparing appropriate for the examination task?* All but one of the control group subjects indicated that they felt they spent the appropriate amount of preparation time. Only half of the experimental group subjects indicated that they spent an appropriate amount of time preparing, one subject indicated that they spent a little too much time preparing, and two subjects indicated that they felt that additional preparation time was required considering the difficulty of the examination. It is unexpected that approximately 33% of the experimental group would indicate a short preparation time, considering that the experimental group mean preparation time was almost twice as long

Table 4.16 Alpha Delta Survey Q1 Response Distributions

Q1: Was the time you spent preparing appropriate for the examination task?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. My preparation time was extremely short considering the difficulty of the examination: I should have spent at least 2 additional hours preparing	0 / 0%	1 / 16.667%
2. My preparation time was somewhat short considering the difficulty of the examination: I should have spent an additional 30 minutes – 1 hour preparing	0 / 0%	1 / 16.667%
3. I spent just the right amount of time preparing for the examination task	5 / 83.333%	3 / 50.000%
4. I spent a little too much time preparing: I over-prepared by approximately 30 minutes – 1 hour	1 / 16.667%	1 / 16.667%
5. I spent way too much time preparing: I over-prepared by at least 2 hours	0 / 0%	0 / 0%
Reference Data: Control/Experimental Group Q1 Median Response = 3 / 3 Control/Experimental Group Mean Preparation Time = 97.83 min. / 162.83 min. Control/Experimental Group Mean Execution Time = 145.17 min. / 167 min. Control/Experimental Group Mean % Evidence Found = 45.79% / 49.333%		

as the control group. Incidentally, the control group subjects who indicated the need for more preparation time spent 137 and 174 minutes in the preparation session.

Table 4.17 presents the distribution of responses to survey question 2: *Did your preparation efforts contribute to a clear and complete understanding of the case?* No subjects in the control or experiment group indicated that the preparation effort was extremely helpful in understanding the case, but at least half of each group indicated that the preparation effort was helpful in understanding the case concepts. The control group provided the only negative response (one subject) to question 2, indicating that the preparation effort was not helpful for understanding case concepts.

Table 4.18 presents the response distributions for survey question 3: *Estimate your level of confidence in the results of your examination?* Though the experimental group found more overall evidence than the control group, the confidence in their results was somewhat lower than the control group.

Table 4.19 presents the response distributions for survey question 4: *Were you given a sufficient amount of time to execute the examination?* Both subject groups unanimously indicated that they were given a sufficient amount of time to conduct their planned activities and conduct a thorough examination.

Table 4.17 Alpha Delta Survey Q2 Response Distributions

Q2: Did your preparation efforts contribute to a clear and complete understanding of the case?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. The preparation effort contributed to confusion regarding case concepts and case facts	0 / 0%	0 / 0%
2. The preparation effort was not helpful for understanding or identifying important case concepts	1 / 16.667%	0 / 0%
3. The preparation effort was somewhat helpful for understanding or identifying important case concepts	1 / 16.667%	3 / 50.000%
4. The preparation effort was helpful in understanding and identifying important case concepts	4 / 66.667%	3 / 50.000%
5. The preparation effort was very helpful in understanding and identifying important case concepts	0 / 0%	0 / 0%
Reference Data: Control/Experimental Group Q2 Median Response = 4 / 4 Control/Experimental Group Mean Preparation Time = 97.83 min. / 162.83 min. Control/Experimental Group Mean Execution Time = 145.17 min. / 167 min. Control/Experimental Group Mean % Evidence Found = 45.79% / 49.333%		

Table 4.18 Alpha Delta Survey Q3 Response Distributions

Q3: Estimate your level of confidence in the results of your examination?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. I found less than 20% of the evidence	0 / 0%	1 / 16.667%
2. I found 20–40% of the evidence	2 / 33.333%	2 / 33.333%
3. I found 41–60% of the evidence	1 / 16.667%	1 / 16.667%
4. I found 61–80% of the evidence	3 / 50.000%	1 / 16.667%
5. I found 81–100% of the evidence	0 / 0%	1 / 16.667%
Reference Data: Control/Experimental Group Q3 Median Response = 3.5 / 2.5 Control/Experimental Group Mean % Evidence Found = 45.79% / 49.333%		

Table 4.19 Alpha Delta Survey Q4 Response Distributions

Q4: Were you given a sufficient amount of time to execute the examination?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. I needed a significant amount of additional time to execute the examination (> 2 hours)	0 / 0%	0 / 0%
2. I needed additional time to execute the examination (1–2 hours)	0 / 0%	0 / 0%
3. I needed a little bit of additional time to execute the examination (30 minutes – 1 hour)	0 / 0%	0 / 0%
4. I executed all planned activities and was given a sufficient amount of time to execute the examination	6 / 100.000%	6 / 100.000%
Reference Data: Control/Experimental Group Q4 Median Response = 4 / 4 Control/Experimental Group Mean Preparation Time = 97.83 min. / 162.83 min. Control/Experimental Group Mean Execution Time = 145.17 min. / 167 min. Control/Experimental Group Mean % Evidence Found = 45.79% / 49.333%		

Table 4.20 presents the response distributions for survey question 5: *Did you spend additional time developing or brainstorming keyword searches after the preparation sessions/during the examination?* Overall, the control group indicated that they spent more time developing unplanned keyword searches than the experimental group. Though there was no significant difference in the amount of evidence found with unplanned keyword searches, on average, the experimental group did find more evidence with unplanned keyword searching than the control group (17.51% vs. 5.05%).

Table 4.20 Alpha Delta Survey Q5 Response Distributions

Q5: Did you spend additional time developing or brainstorming keyword searches after the preparation sessions/during the examination?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. I developed several keyword searches during the examination session (> 20)	1 / 16.667%	1 / 16.667%
2. I developed some keyword searches during the examination session (10–20)	0 / 0%	2 / 33.333%
3. I developed very few keyword searches during the examination session (1–10)	5 / 83.333%	3 / 50.000%
4. I developed no keyword searches during the examination session	0 / 0%	0 / 0%
Reference Data: Control/Experimental Group Q5 Median Response = 3 / 3 Control/Experimental Group Mean Preparation Time = 97.83 min. / 162.83 min. Control/Experimental Group Mean Execution Time = 145.17 min. / 167 min. Control/Experimental Group Mean % Evidence Found = 45.79% / 49.333% Control/Experimental Group Mean % Evidence Found with Unplanned Keyword Searches = 5.05% / 17.51%		

4.3.2 Statistical Analysis of Bravo Charlie Trial

Table 4.21 presents the results of the normality and equality of variance tests for the Bravo Charlie group. Table 4.21 also provides the final conclusion for whether or not the data item is eligible for statistical comparison with the *t*-test. According to the sample size of the Bravo Charlie group, six degrees of freedom were used in the statistical *t*-tests. Hypotheses are evaluated based on a 90% confidence interval.

Table 4.22 presents the results of the Mann-Whitney tests (none of these data items were *t*-test-eligible) performed on the collected time/effort data items for the Bravo Charlie groups. Time values are expressed in minutes. Based on the results of these tests, the following statement may be made with a high degree of certainty: the case domain modeling method contributed to a significant increase in the amount of time spent in planning and executing the forensics examination.

Table 4.23 provides the results of the *t*-tests performed on the data items that measured the amount of evidence found by the experimental and control groups. The means are expressed in percentages. None of the *t*-tests performed on these data items revealed any statistical difference between the amounts of evidence found by the experimental and control groups. However, the experimental group found more evidence than the control group in two out of the three evidence categories, and the experimental group once again found more overall evidence than the control group.

Table 4.21 Bravo Charlie Data Items *t*-test Eligibility

Data Item	Shapiro-Wilk Normality Test, p	Normal?	2 Variance Equality Test, p	Variance Equal?	*t*-Test Eligible?
Planning Time Con. Group	0.956439	Yes	0.034	No	No
Planning Time Exp. Group	0.933707	Yes			
Execution Time Con. Group	0.081085	No	0.947	Yes	No
Execution Time Exp. Group	0.376322	Yes			
Total Time Con. Group	0.983399	Yes	0.017	No	No
Total Time Exp. Group	0.298139	Yes			
%Email Con. Group	0.000084	No	0.494	Yes	No
%Email Exp. Group	0.015764	Yes			
%Images Con. Group	0.255372	Yes	0.747	Yes	Yes
%Images Exp. Group	0.178225	Yes			
%AreaInfo Con. Group	0.130402	Yes	0.004	No	No
%AreaInfo Exp. Group	0.086137	Yes			
%Overall Con. Group	0.501375	Yes	0.918	Yes	Yes
%Overall Exp. Group	0.334944	Yes			
%Found w/ Planned Keywords Con. Group	0.000931	No	0.179	Yes	No
%Found w/ Planned Keywords Exp. Group	0.004797	No			
%Found w/ unplanned Keywords Con. Group	0.011132	Yes	0.216	Yes	Yes
%Found w/ unplanned Keywords Exp. Group	0.236194	Yes			
%Found w/ all Keywords Con. Group	0.018772	Yes	0.572	Yes	Yes
%Found w/ all Keywords Exp. Group	0.608417	Yes			
%Found w/o Keywords Con. Group	0.793916	Yes	0.287	No	No
%Found w/o Keywords Exp. Group	0.019128	No			

Table 4.22 Bravo Charlie Mean Differences of Time Data Items

Hypothesis	Control Mean ($\bar{x}$)	Experimental Mean ($\bar{y}$)	*t*	*p*	Outcome
h_{b1}	89.29	134.14	N/A	0.048	Accept h_{b1}
h_{b2}	103.86	137.71	N/A	0.009	Accept h_{b2}
h_{b3}	193.143	271.86	N/A	0.006	Accept h_{b3}
Hypothesis Legend					
h_{b1} = The experimental group dedicated a significantly different amount of time on the planning session than the control group.					
h_{b2} = The experimental group spent a significantly different amount of time on the execution session than the control group.					
h_{b3} = The experimental group spent a significantly different amount of total time on the experiment exercise than the control group.					

Table 4.24 presents the results of the *t*-tests performed on the Bravo Charlie search method data items. Values are expressed in terms of the percentage of overall evidence found by using the specified search method. The results of these *t*-tests indicate that the experimental group's unplanned and overall keyword searching activities were significantly more effective than the control group's keyword searching activities. Thus, it is highly likely that the case domain modeling method contributed to a more thorough use of keyword searching methods. Though there is a significant difference in how the groups found data, as indicated in Table 4.23, there was no statistically significant difference between the amounts of evidence found by the experimental and control groups.

Table 4.23 Bravo Charlie Mean Differences of Amount of Evidence Found Data Items

Hypothesis	Control Mean ($\bar{x}$)	Experimental Mean ($\bar{y}$)	*t*	*p*	Outcome
h_{b4}	17.46	55.56	N/A	0.157	Reject h_{b4}
h_{b5}	35.06	36.36	0.127	0.235	Reject h_{b5}
h_{b6}	28.57	14.28	N/A	0.595	Reject h_{b6}
h_{b7}	27.59	35.47	0.771	0.235	Reject h_{b7}
Hypothesis Legend					
h_{b4} = The experimental group located a significantly different amount of evidence files containing suspect emails than the control group					
h_{b5} = The experimental group located a significantly greater amount of evidence files containing suspect images than the control group					
h_{b6} = The experimental group located a significantly different amount of evidence files related to the Dallas, TX area than the control group					
h_{b7} = The experimental group located a significantly greater amount of overall evidence files than the control group					

Table 4.24 Bravo Charlie Mean Differences of Search Method Data Items

Hypothesis	Control Mean ($\bar{x}$)	Experimental Mean ($\bar{y}$)	*t*	*p*	Outcome
h_{b8}	1.48	3.45	N/A	0.455	Reject h_{b8}
h_{b9}	3.94	12.81	3.166	0.01	Accept h_{b9}
h_{b10}	5.42	16.26	3.268	0.009	Accept h_{b10}
h_{b11}	24.139	9.85	N/A	0.123	Reject h_{b11}
Hypothesis Legend					
h_{b8} = The experimental group located a significantly different amount of evidence files using planned keyword searches than the control group					
h_{b9} = The experimental group located a significantly greater amount of evidence files using unplanned keyword searches than the control group					
h_{b10} = The experimental group located a significantly greater amount of evidence files using planned or unplanned keyword searches than the control group					
h_{b11} = The experimental group located a significantly different amount of evidence files using non-keyword searches than the control group					

Basic frequency distribution statistics are provided for the post-experiment survey data items. Table 4.25 presents the response distribution to survey question 1: *Was the time you spent preparing appropriate for the examination task?* Though the experimental group spent a greater amount of time planning than the control group, the experimental group had a higher occurrence of individuals who indicated the need for more planning time.

Table 4.26 presents the response distributions for survey question 2: *Did your preparation efforts contribute to a clear and complete understanding of the case?* The experimental group had a higher occurrence of individuals who indicated that the preparation effort was helpful or very helpful (options 4 and 5) in understanding case concepts: five responses versus two responses.

Table 4.27 presents the response distributions for survey question 3: *Estimate your level of confidence in the results of your examination?* On average, the experimental group was somewhat more confident in their results than the control group, with a median response of 3 versus 2; this is consistent with the experimental group's somewhat greater mean percentage of overall evidence found.

Table 4.28 presents the response distributions for survey question 4: *Were you given a sufficient amount of time to execute the examination?* The response to this question was nearly identical to the Alpha Delta trial: all but one of the experiment subjects indicated that they were given a sufficient amount of time to execute their planned activities and conduct a thorough examination.

Table 4.25 Bravo Charlie Survey Q1 Response Distributions

Q1: Was the time you spent preparing appropriate for the examination task?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. My preparation time was extremely short considering the difficulty of the examination: I should have spent at least 2 additional hours preparing	0 / 0%	0 / 0%
2. My preparation time was somewhat short considering the difficulty of the examination: I should have spent an additional 30 minutes – 1 hour preparing	2 / 28.571%	4 / 57.143%
3. I spent just the right amount of time preparing for the examination task	3 / 42.857%	3 / 42.857%
4. I spent a little too much time preparing: I over-prepared by approximately 30 minutes – 1 hour	1 / 14.286%	0 / 0%
5. I spent way too much time preparing: I over-prepared by at least 2 hours	1 / 14.286%	0 / 0%
Reference Data: Control/Experimental Group Q1 Median Response = 3 / 2 Control/Experimental Group Mean Preparation Time = 89.29 min. / 134.14 min. Control/Experimental Group Mean Execution Time = 103.86 min. / 137.71 min. Control/Experimental Group Mean % Evidence Found = 27.59% / 35.47%		

Table 4.26 Bravo Charlie Survey Q2 Response Distributions

Q2: Did your preparation efforts contribute to a clear and complete understanding of the case?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. The preparation effort contributed to confusion regarding case concepts and case facts	0 / 0%	0 / 0%
2. The preparation effort was not helpful for understanding or identifying important case concepts	1 / 14.286	0 / 0%
3. The preparation effort was somewhat helpful for understanding or identifying important case concepts	4 / 57.143	2 / 28.571
4. The preparation effort was helpful in understanding and identifying important case concepts	1 / 14.286	4 / 57.143
5. The preparation effort was very helpful in understanding and identifying important case concepts	1 / 14.286	1 / 14.286
Reference Data: Control/Experimental Group Q2 Median Response = 3 / 4 Control/Experimental Group Mean Preparation Time = 89.29 min. / 134.14 min. Control/Experimental Group Mean Execution Time = 103.86 min. / 137.71 min. Control/Experimental Group Mean % Evidence Found = 27.59% / 35.47%		

Table 4.27 Bravo Charlie Survey Q3 Response Distributions

Q3: Estimate your level of confidence in the results of your examination?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. I found less than 20% of the evidence	3 /42.857	1 / 14.286%
2. I found 20–40% of the evidence	1 / 14.286	2 / 28.571%
3. I found 41–60% of the evidence	3 / 42.857	2 / 28.571%
4. I found 61–80% of the evidence	0 / 0%	2 / 28.571%
5. I found 81–100% of the evidence	0 / 0%	0 / 0%
Reference Data: Control/Experimental Group Q3 Mean Response = 2 / 3 Control/Experimental Group Mean % Evidence Found = 27.59% / 35.47%		

Table 4.28 Bravo Charlie Survey Q4 Response Distributions

Q4: Were you given a sufficient amount of time to execute the examination?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. I needed a significant amount of additional time to execute the examination (> 2 hours)	1 / 14.286%	0 / 0%
2. I needed additional time to execute the examination (1–2 hours)	0 / 0%	0 / 0%
3. I needed a little bit of additional time to execute the examination (30 minutes – 1 hour)	0 / 0%	0 / 0%
4. I executed all planned activities and was given a sufficient amount of time to execute the examination	6 / 85.714%	7 / 100%
Reference Data: Control/Experimental Group Q4 Median Response = 4 / 4 Control/Experimental Group Mean Preparation Time = 89.29 min. / 134.14 min. Control/Experimental Group Mean Execution Time = 103.86 min. / 137.71 min. Control/Experimental Group Mean % Evidence Found = 27.59% / 35.47%		

Table 4.29 presents the response distributions for survey question 5: *Did you spend additional time developing or brainstorming keyword searches after the preparation sessions/during the examination?* The survey results indicate that the experimental group developed more unplanned keyword searches than the control group. This result is consistent with the significantly greater amount of evidence that the experimental group found with unplanned keyword searches when compared with the control group.

Table 4.29 Bravo Charlie Survey Q5 Response Distributions

Q5: Did you spend additional time developing or brainstorming keyword searches after the preparation sessions/during the examination?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. I developed several keyword searches during the examination session (> 20)	0 / 0%	1 / 14.286%
2. I developed some keyword searches during the examination session (10–20)	4 / 57.143	1 / 14.286%
3. I developed very few keyword searches during the examination session (1–10)	3 / 42.857	4 / 57.143%
4. I developed no keyword searches during the examination session	0 / 0%	1 / 14.286%
Reference Data: Control/Experimental Group Q5 Median Response = 3 / 3 Control/Experimental Group Mean Preparation Time = 89.29 min. / 134.14 min. Control/Experimental Group Mean Execution Time = 103.86 min. / 137.71 min. Control/Experimental Group Mean % Evidence Found = 27.59% / 35.47% Control/Experimental Group Mean % Evidence Found with Unplanned Keyword Searches = 3.94% / 12.81%		

4.3.3 Statistical Analysis on the Aggregate of Alpha Delta and Bravo Charlie Trials

All time data items, the total percentage of evidence found, and all search method data items were aggregated from the Alpha Delta and Bravo Charlie groups. Table 4.30 provides the results of the normality and variance equality tests that determine the data items' eligibilities for the *t*-test.

Table 4.30 Aggregate Data Items *t*-test Eligibility

Data Item	SW, p	Normal?	2 Variance Equality Test, p	Variance Equal?	*t*-Test Eligible?
Planning Time Con. Group	0.533818	Yes	0.002	No	No
Planning Time Exp. Group	0.971364	Yes			
Execution Time Con. Group	0.440974	Yes	0.855	Yes	Yes
Execution Time Exp. Group	0.355692	Yes			
Total Time Con. Group	0.420793	Yes	0.025	No	No
Total Time Exp. Group	0.338347	Yes			
%Overall Evidence Con. Group	0.338203	Yes	0.925	Yes	Yes
%Overall Evidence Exp. Group	0.398338	Yes			
%Found w/ Planned Keywords Con. Group	0.004360	No	0.273	Yes	No
%Found w/ Planned Keywords Exp. Group	0.000030	No			
%Found w/ unplanned Keywords Con. Group	0.002067	No	0.002	No	No
%Found w/ unplanned Keywords Exp. Group	0.026030	No			
%Found w/ all Keywords Con. Group	0.007397	No	0.836	Yes	No
%Found w/ all Keywords Exp. Group	0.012356	No			
%Found w/o Keywords Con. Group	0.247465	Yes	0.753	Yes	No
%Found w/o Keywords Exp. Group	0.004219	No			

The time data items from the Alpha Delta and Bravo Charlie groups were combined, and *t*-tests were performed on this aggregate data set. Table 4.31 presents the

results of the *t*-tests and Mann-Whitney test performed on the aggregate of the time data items in the Alpha Delta and Bravo Charlie groups. All three *t*-tests indicate within a 99% confidence interval that the experimental groups spent more time in the exercise than the control groups.

Table 4.31 Aggregate of Alpha Delta and Bravo Charlie Groups Mean Differences of Time Data Items

Hypothesis	**Control Mean ($\bar{x}$)**	**Experimental Mean ($\bar{y}$)**	***t***	***p***	**Outcome**
h_{ab1}	93.23	147.39	N/A	0.001	Accept h_{ab1}
h_{ab2}	122.92	151.23	$t = 3.262$	0.003	Accept h_{ab2}
h_{ab3}	216.15	298.62	N/A	0.001	Accept h_{ab3}
Hypothesis Legend					
h_{ab1} = The experimental groups dedicated a significantly different amount of time on the planning session than the control groups.					
h_{ab2} = The experimental groups spent a significantly less amount of time on the execution session than the control groups.					
h_{ab3} = The experimental groups spent a significantly different amount of total time on the experiment exercise than the control groups.					

Table 4.32 presents the *t*-test and Mann-Whitney results on the aggregate data items of the Alpha Delta and Bravo Charlie overall amount of evidence found. The *t*-test indicates that there is no significant difference between the overall amounts of evidence found between the aggregated control and experimental groups.

Table 4.33 presents the Mann-Whitney tests performed on the aggregate of the Alpha Delta and Bravo Charlie groups' search method data items. The results of these

tests indicate that the experimental group found a significantly greater amount of evidence than the control group using unplanned keyword searches.

Table 4.32 Aggregate of Alpha Delta and Bravo Charlie Groups Mean Difference of Overall Percentage of Evidence Found

Hypothesis	**Control Mean ($\bar{x}$)**	**Experimental Mean ($\bar{y}$)**	***t*, St. Dev.(s_t)**	***p***	**Outcome**
h_{ab4}	$\bar{x}$ = 35.99	$\bar{y}$ = 41.87	t = 0.620	0.273	Reject h_{b4}
Hypothesis Legend					
h_{ab4} = The experimental groups located a significantly greater amount of evidence files than the control groups					

Table 4.33 Aggregate of the Alpha Delta and Bravo Charlie Groups Mean Difference of Keyword Search Method Data Items

Hypothesis	**Control Mean ($\bar{x}$)**	**Experimental Mean ($\bar{y}$)**	***t*, St. Dev.(s_t)**	***p***	**Outcome**
h_{ab5}	14.08	6.68	N/A	0.495	Reject h_{ab5}
h_{ab6}	4.45	14.98	N/A	0.049	Accept h_{ab6}
h_{ab7}	12.94	21.65	N/A	0.116	Reject h_{ab7}
h_{ab8}	24.11	15.17	N/A	0.181	Reject h_{ab8}
Hypothesis Legend					
h_{ab5} = The control groups located a significantly different amount of evidence files using planned keyword searches than the experimental groups					
h_{ab6} = The experimental groups located a significantly different amount of evidence files using unplanned keyword searches than the control groups					
h_{ab7} = The experimental groups located a significantly different amount of evidence files using planned or unplanned keyword searches than the control groups					
h_{ab8} = The control groups located a significantly different amount of evidence files using non-keyword searches than the experimental groups					

Table 4.34 presents the question 1 survey response distributions of the combined Alpha Delta and Bravo Charlie trials. Table 4.35 presents the question 2 survey response distributions of the combined Alpha Delta and Bravo Charlie trials.

Table 4.34 Experiment 1 Aggregate Q1 Survey Response Distributions

Q1: Was the time you spent preparing appropriate for the examination task?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. My preparation time was extremely short considering the difficulty of the examination: I should have spent at least 2 additional hours preparing	0 / 0%	1 / 7.692%
2. My preparation time was somewhat short considering the difficulty of the examination: I should have spent an additional 30 minutes – 1 hour preparing	2 / 15.385%	5 / 38.462%
3. I spent just the right amount of time preparing for the examination task	8 / 61.538%	6 / 46.154%
4. I spent a little too much time preparing: I over-prepared by approximately 30 minutes – 1 hour	2 / 15.385%	1 / 7.692%
5. I spent way too much time preparing: I over-prepared by at least 2 hours	1 / 7.692%	0 / 0%
Reference Data: Control/Experimental Group Q1 Median Response = 3 / 3 Control/Experimental Group Mean Preparation Time = 93.23 min. / 147.39 min. Control/Experimental Group Mean Execution Time = 133.92 min. / 141.23 min. Control/Experimental Group Mean % Evidence Found = 35.99% / 41.87%		

Table 4.35 Experiment 1 Aggregate Q2 Survey Response Distributions

Q2: Did your preparation efforts contribute to a clear and complete understanding of the case?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. The preparation effort contributed to confusion regarding case concepts and case facts	0 / 0%	0 / 0%
2. The preparation effort was not helpful for understanding or identifying important case concepts	2 / 15.385%	0 / 0%
3. The preparation effort was somewhat helpful for understanding or identifying important case concepts	5 / 38.462%	5 / 38.462%
4. The preparation effort was helpful in understanding and identifying important case concepts	5 / 38.462%	7 / 53.846%
5. The preparation effort was very helpful in understanding and identifying important case concepts	1 / 7.692%	1 / 7.692%
Reference Data: Control/Experimental Group Q2 Median Response = 3 / 4 Control/Experimental Group Mean Preparation Time = 93.23 min. / 147.39 min. Control/Experimental Group Mean Execution Time = 133.92 min. / 141.23 min. Control/Experimental Group Mean % Evidence Found = 35.99% / 41.87%		

Table 4.36 presents the question 3 survey response distributions of the combined Alpha Delta and Bravo Charlie trials. Table 4.37 presents the question 4 survey response distributions of the combined Alpha Delta and Bravo Charlie trials.

Table 4.38 presents the question 5 survey response distributions of the combined Alpha Delta and Bravo Charlie trials.

Table 4.36 Experiment 1 Aggregate Q3 Survey Response Distributions

Q3: Estimate your level of confidence in the results of your examination?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. I found less than 20% of the evidence	3 / 23.077%	2 / 15.385%
2. I found 20–40% of the evidence	3 / 23.077%	4 / 30.769%
3. I found 41–60% of the evidence	4 / 30.769%	3 / 23.077%
4. I found 61–80% of the evidence	3 / 23.077%	3 / 23.077%
5. I found 81–100% of the evidence	0 / 0%	1 / 7.692%
Reference Data: Control/Experimental Group Q3 Median Response = 3 / 3 Control/Experimental Group Mean % Evidence Found = 35.99% / 41.87%		

Table 4.37 Experiment 1 Aggregate Q4 Survey Response Distributions

Q4: Were you given a sufficient amount of time to execute the examination?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
1. I needed a significant amount of additional time to execute the examination (> 2 hours)	1 / 7.692%	0 / 0%
2. I needed additional time to execute the examination (1–2 hours)	0 / 0%	0 / 0%
3. I needed a little bit of additional time to execute the examination (30 minutes – 1 hour)	0 / 0%	0 / 0%
4. I executed all planned activities and was given a sufficient amount of time to execute the examination	12 / 92.308%	13 / 100%
Reference Data: Control/Experimental Group Q4 Median Response = 4 / 4 Control/Experimental Group Mean Preparation Time = 93.23 min. / 147.39 min. Control/Experimental Group Mean Execution Time = 133.92 min. / 141.23 min. Control/Experimental Group Mean % Evidence Found = 35.99% / 41.87%		

Table 4.38 Experiment 1 Aggregate Q5 Survey Response Distributions

Q5: Did you spend additional time developing or brainstorming keyword searches after the preparation sessions/during the examination?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
I developed several keyword searches during the examination session (> 20)	1 / 7.692%	2 / 15.385%
I developed some keyword searches during the examination session (10–20)	4 / 30.769%	3 / 23.077%
I developed very few keyword searches during the examination session (1–10)	8 / 61.538%	7 / 53.846%
I developed no keyword searches during the examination session	0 / 0%	1 / 7.692%
Reference Data: Control/Experimental Group Q5 Median Response = 3 / 3 Control/Experimental Group Mean Preparation Time = 93.23 min. / 147.39 min. Control/Experimental Group Mean Execution Time = 133.92 min. / 141.23 min. Control/Experimental Group Mean % Evidence Found = 35.99% / 41.87% Control/Experimental Group Mean % Evidence Found with Unplanned Keyword Searches = 4.452 / 14.977		

4.4 Discussion of Experiment 1 Results and Conclusions

The statistical analysis of the Alpha Delta, Bravo Charlie, and aggregate data sets will be discussed with respect to two research questions:

1. Does the case domain modeling methodology result in an increased amount of evidence found in an examination?

2. Does the case domain modeling methodology require a significant amount of additional effort when compared to a typical approach?

Sections 4.4.1 and 4.4.2 discuss the experiment results with respect to research question 1, and Section 4.4.3 discusses the results with respect to research question 2. Finally, Section 4.4.4 provides conclusions and discusses implications relevant to further evaluation of the dissertation hypothesis.

4.4.1 Amount of Evidence

There were no statistically significant differences in the amount of evidence found by the case domain modeling subjects versus the ad hoc method subjects. However, the case domain modeling subjects did find a greater overall amount of evidence in each of the experiment trials. In the Alpha Delta trial the experimental group found an average of 49.33% of the overall evidence, while the control group found an average of 45.79% of the overall evidence. In the Bravo Charlie trial the experimental group found 35.47% of the overall evidence, while the control group found an average of 27.59% of the overall evidence. These differences, though not significant, do support the claim that the case domain modeling method can provide an improvement in the amount of evidence found in an examination.

The effectiveness of the prescribed preparation activities and methods depend on the level of detail in the available case information. One subject commented on their post-experiment survey that "…there should be more case information. It seems like when the complete forensics team is brought in, the case should be fairly well developed already." In each trial the case materials provided subjects with a brief, one-paragraph description of a scenario and several printouts of bank statements or Internet news reports. There was very little information provided to place these materials in the context

of a scenario, and no victims or subjects were identified. Though the subjects were not provided with an abundance of background information, the experimental group's performance (with respect to evidence found) suggests that case domain modeling can still be applicable and useful in less than ideal circumstances.

Additionally, the Alpha Delta evidence disk had a total of 2,981 file items, while the Bravo Charlie evidence disk had a total of 58,459 file items. To some extent, the number of files on a disk can determine the complexity of the case, and if there are too many files, then it becomes difficult and perhaps impossible to exhaustively browse the files. When it is impractical to browse the files, then preparing keyword searches and search strategies may be more important. In the Alpha Delta trial there was a difference of 3.54 percentage points in the average overall amount of evidence found, while in the Bravo Charlie trial there was a difference of 7.88 percentage points in the average overall amount of evidence found (each difference was in favor of the experimental group), and the Bravo Charlie evidence disk contained nearly twenty times more files than the Alpha Delta evidence disk. These comparisons imply that the case domain modeling approach may be more effective for relatively large evidence disks and less effective for smaller evidence disks. It is expected that a more rigorous preparation method will have more value when it is applied to a relatively complex task.

4.4.2 Keyword Searching

Analysis of the Bravo Charlie and aggregate data sets revealed statistically significant differences in the effectiveness of keyword searching activities between the experimental and control groups. In the Bravo Charlie trial the experimental group found

a significantly greater amount of evidence files using unplanned keyword searches and in all overall keyword searching activities. Analysis of the aggregate data set revealed that the experimental group found a significantly greater amount of evidence files using unplanned keyword searches than did the control group. These significant differences support the portion of the hypothesis that claims that case domain modeling will improve the effectiveness of keyword searching activities. Therefore, the case domain modeling approach likely directed the subjects to spend more time attempting and exhausting keyword search efforts instead of simply browsing the hard drive for files.

4.4.3 Time and Effort

The most significant differences between the experimental and control groups occurred with respect to the amount of time spent in the experiment. This was an expected difference in the preparation session, as the experimental groups were directed to follow a more rigorous approach to preparation than the control groups. Ideally the case domain modeling approach would contribute to more evidence collected and less overall time spent. However, the experimental group spent significantly greater time in the examination session and in the overall experiment. Though these differences were significant, the total time limit of the experiment was 8 hours. Thus, the time differences observed are less than one regular work day. Additionally, the experimental group's greater time investment yielded a greater amount of overall evidence, although the difference was not statistically significant.

4.4.4 Conclusions and Implications for a Follow-up Experiment

On average the experimental groups found a greater percentage of overall evidence than the control groups. However, this difference was not statistically significant. It is assumed that the vagueness of the case scenario materials contributed to this lack of significant difference between the control and experimental groups. Based on the results of Experiment 1, an additional experiment was planned. Experiment 2 was almost identical to Experiment 1 with the following exceptions:

- The number of document file items was increased by at least an order of 10 in order to make it less feasible for subjects to browse through all of the text-based files.
- The case scenario, an email threat in a university environment, was vividly populated with an underlying facts and circumstances report, suspect and victim interviews, email subpoena results, and threatening emails.
- To improve the experimental group's time performance, the case domain modeling method was streamlined to exclude the diagramming activity.

Chapter 5 presents the results of the follow-up experiment that was designed and executed based on the results presented in this chapter.

CHAPTER V

CASE DOMAIN MODELING APPLICATIONS FOR FORENSICS PRACTITIONERS: PLANNING AND EXECUTING FORENSICS EXAMINATIONS: PART II

This experiment was planned and conducted based on the analysis of the Alpha Delta and Bravo Charlie student-subject experiment trials. This experiment was designed not only to evaluate the same research questions as in Experiment 1, but also to observe the influence of evidence disk characteristics and case file material. Section 5.1 describes the experiment design, Section 5.2 describes the evidence preparation procedure, Section 5.3 provides the raw data collected during the experiment, Section 5.4 presents the statistical analysis of the data, the discussion of the results, and conclusions, and Section 5.5 discusses threats to validity applicable to the experiments.

5.1 Experiment Design

This experiment is known as the Phi Gamma experiment trial. The design of the Phi Gamma experiment is nearly identical to the Alpha Delta and Bravo Charlie experiment trials described in Chapter III. However, there are some notable differences between the two experiment designs:

- The subjects were all graduate students enrolled in Dr. Dampier's summer 2006 Advanced Topics in Digital Forensics course.

- The subjects did not participate in preparing any of the evidence or scenario materials. The scenario materials were prepared by the principal investigator, and the evidence drive was prepared by Dr. Dampier's research assistants and, to a limited extent, the principal investigator.

5.1.1 The Control Group and Experimental Group Phi Gamma Preparation Methods

The control group preparation method used in this experiment was identical to the control group preparation method prescribed for Experiment 1 in Section 4.1.1. A few modifications were made to the experimental group preparation method described in Chapter III. During the training session the experimental group was exposed to the UML class diagram representation of the case domain model. However, the preparation method did not require the experimental group subjects to create the case domain model diagram. Instead they were instructed to represent their case domain model in a tabular format as illustrated in Table 5.1. Identifying concept relationships was also excluded from this revised case domain modeling method. This change was implemented in an attempt to streamline the method, place more emphasis on the analytical method than the diagramming syntax, and reduce the amount of effort required to apply the case domain modeling method.

Table 5.1 Case Domain Concept Representation for Experiment 2

Concept Name: →	**Suspect**
Attribute Name	**Attribute Value**
Name	*Jane Doe*
Address	*100 Last House Dr.*
Phone	*(555)-555-6667*
Birthday	*Unknown*

5.1.2 Organization of Phi Gamma Subject Population

The subject population consisted of students enrolled in Dr. Dampier's summer 2006 Advanced Topics in Digital Forensics graduate course. Fifteen subjects participated in the experiment: eight of the subjects were in the experimental group, and seven were in the control group. Two subjects in the experimental group and one subject in the control group had previously participated in the Bravo Charlie or Alpha Delta experiment trials. To balance the two subject populations, one of the experimental group subjects who had previously participated in the experiment was randomly excluded from the data items. A second subject was excluded from the data items because of the subject's relatively extensive exposure to the case domain modeling method and the experiment design. The data collected for one of the control group subjects was excluded because the subject participated in preparing the evidence disk; this subject performed the experiment for the value of the experience. The data items that are presented in this chapter were collected from the remaining twelve subjects, with six subjects in each group. Exactly one subject from the control group and one from the experimental group had participated in the previous Bravo Charlie or Alpha Delta trials. These subjects were also placed in the same groups to which they had previously been assigned.

5.1.3 The Prepared Phi Gamma Evidence Drive and Scenario

The principal investigator prepared all of the background materials and evidence files used in this experiment. The scenario was an email death threat case in a university environment. In the scenario, the victim, Dr. Henry Doe (English professor), received anonymous death threats from a Microsoft Hotmail account. Prior to receiving the death

threats the professor had had an unpleasant conflict with a former student, Jane Bateman, who had cheated on an assignment. The originating IP addresses of the messages all came from a university library's anonymous-login public-use computer. Also, a university librarian had observed the suspect and her friends behaving suspiciously in the library computer lab. The investigating agents seized the suspected library computer, subpoenaed the records of the Hotmail account, and interviewed the involved parties. The case file included the threatening emails, a summary of underlying facts and circumstances, interview transcripts, and the results of the Hotmail subpoena. The names of the involved parties were selected from popular horror films, and any similarities to persons alive or deceased are coincidental.

The evidence files and non-evidence files were distributed on the computer by Dr. Dampier's research assistants. The principal investigator also spent a limited amount of time distributing additional non-evidence files on the evidence disk. The evidence disk has an advertised capacity of 10 GB and contained one partition. Figure 5.1 illustrates the distribution of file item types on the evidence disk. The disk had a total of 56,894 file items, with thirty-three evidence files. The evidence files were categorized and distributed as follows:

- Eight file items were text documents left by the primary suspect, Jane Bateman. These file items contained messages related to the cheating incident and the threatening emails.
- Fifteen file items were documents left by Victor Linoge, the primary suspect's boyfriend. These files contained victim research information and homework assignment files that were authored during the same time period that one of the threatening emails was sent.

- Ten file items were documents and graphics left by Frank Booth, a friend of the primary suspect's boyfriend. These files contained plans for attacking the suspect and references to the threatening emails.

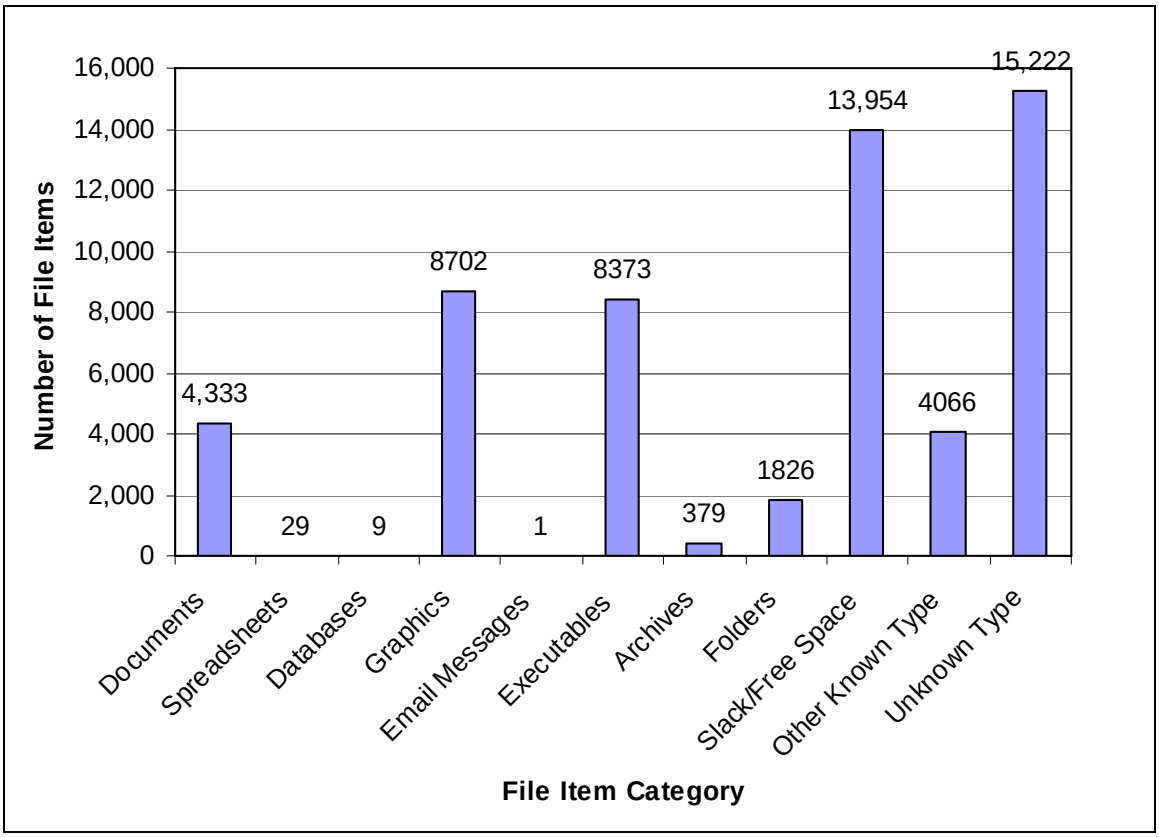


Figure 5.1 Distribution of File Item Types on the Phi Gamma Evidence Disk

5.1.4 Phi Gamma Experiment Logistics

All of the facilities, software, and hardware used in this experiment were owned and maintained by the MSU Department of Computer Science and Engineering. Conducting the Phi Gamma experiment trial required the use of the following resources:

- 2 MSU computer science and engineering classrooms,

- 15 laptop computers with the Forensics Toolkit software,
- 1 10-GB hard drive, and
- 2 of Dr. Dampier's computer forensics research assistants.

5.2 Phi Gamma Data Items Collected

Table 5.2 presents the time data items collected on the Phi Gamma experiment trial during the planning session and the examination session. Time is expressed in minutes. The upper half of the table provides time data items for the control group, while the bottom half of the table provides time data items for the experimental group. This scheme is also used in the other tables in this section.

Table 5.3 provides a summary of the amount of evidence located by the experimental and control groups. The amount of evidence is expressed in percentages. The evidence is also categorized into three groups: Jane, Victor, and Frank. The names of the evidence categories represent the first names of the suspects who left behind the evidence file items. The overall or total percentages of evidence found are also provided in the right-most column.

Table 5.2 Phi Gamma Planning and Execution Effort

Control Group	Planning Session Time (min.)	Examination Session Time (min.)	Total Time (min.)
PG1-1	62	114	176
PG1-2	68	85	153
PG1-3	56	87	143
PG1-4	55	84	139
PG1-5	48	92	140
PG1-6	62	86	148
AVERAGE	58.50	91.33	149.83
Experimental Group			
PG2-1	76	103	179
PG2-2	54	60	114
PG2-3	76	85	161
PG2-4	85	76	161
PG2-5	95	126	221
PG2-6	86	85	117
AVERAGE	78.67	89.17	167.83

Table 5.3 Phi Gamma Amount of Evidence Found Data Items

Control Group	% Jane	% Victor	% Frank	Overall %
PG1-1	62.5	0.0	27.3	23.5
PG1-2	12.5	0.0	18.2	8.8
PG1-3	0.0	0.0	0.0	0.0
PG1-4	62.5	13.3	18.2	26.5
PG1-5	62.5	0.0	0.0	14.7
PG1-6	25.0	6.7	9.1	11.8
AVERAGE	37.5	3.3	12.1	14.2
Experimental Group				
PG2-1	62.5	6.7	27.3	26.5
PG2-2	50.0	40.0	36.4	41.2
PG2-3	25.0	0.0	9.1	8.8
PG2-4	12.5	0.0	27.3	11.8
PG2-5	87.5	6.7	54.5	41.2
PG2-6	62.5	6.7	18.2	23.5
AVERAGE	50.0	10.0	28.8	25.5

Table 5.4 presents data regarding the amount of evidence found using specific search methods. Values are expressed in terms of the percentage of overall evidence that was located using the specified search method. Searching methods are categorized as planned keyword searches, unplanned keyword searches, keyword searches, and non-keyword searches. Planned keyword searches were identified during the planning session, while unplanned keyword searches were specified during the examination session. These two categories are aggregated to represent all keyword searches. Non-keyword searches include any method other than keyword searching that the subjects used to find evidence.

Table 5.4 Phi Gamma Amount of Evidence Found by Searching Methods

Control Group	% Evidence Found with Planned Keyword Searches	%Evidence Found with Unplanned Keyword Searches	% Evidence Found with Keyword Searches	% Evidence Found Using Non-Keyword Searches
PG1-1	23.5	0.0	23.5	0.0
PG1-2	8.8	0.0	8.8	0.0
PG1-3	0.0	0.0	0.0	0.0
PG1-4	14.7	11.8	26.5	0.0
PG1-5	14.7	0.0	14.7	0.0
PG1-6	8.8	2.9	11.8	0.0
AVERAGE	11.8	2.5	14.2	0.0
Experimental Group				
PG2-1	17.6	8.8	26.5	0.0
PG2-2	41.2	0.0	41.2	0.0
PG2-3	0.0	8.8	8.8	0.0
PG2-4	2.9	8.8	11.8	0.0
PG2-5	26.5	14.7	41.2	0.0
PG2-6	17.6	5.9	23.5	0.0
AVERAGE	17.6	7.8	25.5	0.0

Table 5.5 presents the post-experiment multiple-choice survey questions. Table 5.6 presents the multiple responses of the Phi Gamma groups. The alphabetic multiple choice identifiers (a–e) were replaced with numerical identifiers (1–5). A listing of the responses from the two survey discussion questions is omitted, but insightful survey responses will be cited in the analysis/discussion sections.

Table 5.5 Phi Gamma Multiple Choice Post-Experiment Survey Questions

Q1	Was the time you spent preparing appropriate for the examination task? a. My preparation time was extremely short considering the difficulty of the examination: I should have spent at least 2 additional hours preparing b. My preparation time was somewhat short considering the difficulty of the examination: I should have spent an additional 30 minutes – 1 hour preparing. c. I spent just the right amount of time preparing for the examination task d. I spent a little too much time preparing: I over-prepared by approximately 30 minutes – 1 hour e. I spent way too much time preparing: I over-prepared by at least 2 hours
Q2	Did your preparation efforts contribute to a clear and complete understanding of the case? a. The preparation effort contributed to confusion regarding case concepts and case facts b. The preparation effort was not helpful for understanding or identifying important case concepts c. The preparation effort was somewhat helpful for understanding or identifying important case concepts. d. The preparation effort was helpful in understanding and identifying important case concepts e. The preparation effort was very helpful in understanding and identifying important case concepts.
Q3	Estimate your level of confidence in the results of your examination? a. I found less than 20% of the evidence b. I found between 20–40% of the evidence c. I found between 41–60% of the evidence d. I found between 61–80% of the evidence e. I found between 81–100% of the evidence
Q4	Were you given a sufficient amount of time to execute the examination? a. I needed a significant amount of additional time to execute the examination (> 2 hours) b. I needed additional time to execute the examination (1–2 hours) c. I needed a little bit of additional time to execute the examination (30 minutes – 1 hour) d. I executed all planned activities and was given a sufficient amount of time to execute the examination.

Table 5.6 Phi Gamma Multiple Choice Survey Data Items

Control Group	Q1	Q2	Q3	Q4
P1	3	5	5	3
P2	1	4	2	4
P3	2	3	5	3
P4	2	3	4	2
P5	3	4	3	4
P6	2	4	2	4
MEDIAN	2	4	3.5	3.5
Experimental Group				
G1	3	3	2	4
G2	2	5	5	4
G3	1	3	2	4
G4	3	4	5	4
G5	Did not reply			
G6	3	4	5	4
MEDIAN	3	4	5	4

5.3 Statistical Analysis of Phi Gamma Data Items

As with the Alpha Delta and Bravo Charlie experiment trials, the preferred method for observing significant differences between means is the one-sided *t*-test. When the critical assumptions of the *t*-test are not satisfied, then the non-parametric Mann-Whitney test is used to observe significant differences between means. All statistical tests are observed with a 90% confidence interval. Table 5.7 presents the results of the normality and variance tests that determine *t*-test eligibility for each pair of data items.

Table 5.7 Phi Gamma Data Items *t*-test Eligibility

Data Item	SW, p	Normal?	2 Variance Equality Test, p	Variance Equal?	*t*-Test Eligible?
Planning Time Con. Group	0.879743	Yes	0.152	Yes	Yes
Planning Time Exp. Group	0.456501	Yes			
Execution Time Con. Group	0.695062	Yes	0.156	Yes	Yes
Execution Time Exp. Group	0.816702	Yes			
Total Time Con. Group	0.073187	No	0.067	No	No
Total Time Exp. Group	0.644884	Yes			
%Jane Con. Group	0.079391	No	0.932	Yes	No
%Jane Exp. Group	0.782827	Yes			
%Victor Con. Group	0.006373	No	0.048	No	No
%Victor Exp. Group	0.003066	No			
%Frank Con. Group	0.415044	Yes	0.458	Yes	Yes
%Frank Exp. Group	0.830223	Yes			
%Overall Con. Group	0.865666	Yes	0.456	Yes	Yes
%Overall Exp. Group	0.331360	Yes			
%Found w/ Planned Keywords Con. Group	0.827072	Yes	0.176	Yes	Yes
%Found w/ Planned Keywords Exp. Group	0.691910	Yes			
%Found w/ unplanned Keywords Con. Group	0.001158	No	0.968	Yes	No
%Found w/ unplanned Keywords Exp. Group	0.479993	Yes			
%Found w/ all Keywords Con. Group	0.865666	Yes	0.456	Yes	Yes
%Found w/ all Keywords Exp. Group	0.331360	Yes			

Table 5.8 presents the results of the Mann-Whitney tests and *t*-tests performed on the collected time/effort data items for the experimental and control groups. The *t*-value column is marked "N/A" when a Mann-Whitney test was performed. Time values are expressed in minutes. Based on the results of these tests, the following statement may be made with a high degree of certainty: the case domain modeling method contributed to a significant increase in the amount of time spent in planning the examination, but there was no significant differences in the overall time and execution time. In contrast to the Alpha Delta and Bravo Charlie trials, the experimental group's mean execution time was slightly lower than the control group's mean execution time.

Table 5.8 Phi Gamma Mean Differences of Time Data Items

Hypothesis	**Control Mean ($\bar{x}$)**	**Experimental Mean ($\bar{y}$)**	***t***	***p***	**Outcome**
h_{c1}	58.500	78.667	2.447	0.029	Accept h_{c1}
h_{c2}	91.333	89.167	0.269	0.399	Reject h_{c2}
h_{c3}	149.833	167.833	N/A	0.149	Reject h_{c3}
Hypothesis Legend					
h_{c1} = The experimental group dedicated a significantly greater amount of time on the planning session than the control group.					
h_{c2} = The experimental group spent a significantly less amount of time on the execution session than the control group.					
h_{c3} = The experimental group spent a significantly different amount of total time on the experiment exercise than the control group.					

Table 5.9 provides the results of the *t*-tests performed on the data items that measured the amount of evidence found by the experimental and control groups. The

means are expressed in percentages. Based on the results of these tests, the experimental group found a significantly greater amount of evidence left by suspect Frank, and they also found a significantly greater amount of overall evidence. Additionally, the experimental group's mean amount of evidence found was slightly higher than the control group's mean amount of evidence found in the remaining two categories: Jane and Victor.

Table 5.9 Phi Gamma Mean Differences of Amount of Evidence Found Data Items

Hypothesis	**Control Mean ($\bar{x}$) in %**	**Experimental Mean ($\bar{y}$) in %**	***t***	***p***	**Outcome**
h_{c4}	37.5	50.0	N/A	0.505	Reject h_{c4}
h_{c5}	3.3	10.0	N/A	0.337	Reject h_{c5}
h_{c6}	12.1	28.8	2.101	0.045	Accept h_{c6}
h_{c7}	14.2	25.5	1.635	0.081	Accept h_{c7}
Hypothesis Legend					
h_{c4} = The experimental group located a significantly different amount of evidence files left by Jane Doe than the control group					
h_{c5} = The experimental group located a significantly different amount of evidence files left by Victor Linoge than the control group					
h_{c6} = The experimental group located a significantly greater amount of evidence files left by Frank Booth than the control group					
h_{c7} = The experimental group located a significantly greater amount of overall evidence files than the control group					

Table 5.10 presents the results of the *t*-tests performed on the search method data items. Values are expressed in terms of the percentage of overall evidence found by using the specified search method. The non-keyword search category was not tested because no subjects reported the use of any non-keyword searching methods. The results of these

tests indicate that the experimental group found a significantly greater amount of evidence using unplanned keyword searches and overall keyword searches. The experimental group's mean amount of evidence found using planned keyword searches was also slightly higher than the control group's mean.

Table 5.10 Phi Gamma Mean Differences of Search Method Data Items

Hypothesis	**Control Mean ($\bar{x}$) in %**	**Experimental Mean ($\bar{y}$) in %**	***t***	***p***	**Outcome**
h_{c8}	11.8	17.6	0.919	0.20	Reject h_{c8}
h_{c9}	2.5	7.8	N/A	0.094	Accept h_{c9}
h_{c10}	14.2	25.5	1.635	0.081	Accept h_{c10}
Hypothesis Legend					
h_{c8} = The experimental group located a significantly greater amount of evidence files using planned keyword searches than the control group					
h_{c9} = The experimental group located a significantly different amount of evidence files using unplanned keyword searches than the control group					
h_{c10} = The experimental group located a significantly greater amount of evidence files using planned or unplanned keyword searches than the control group					

Basic frequency distribution statistics are provided for the post-experiment survey data items. Table 5.11 presents the response distribution to survey question 1: *Was the time you spent preparing appropriate for the examination task?* The experimental group and control group means are both below three, which indicates that the subjects likely felt that they should have spent more time preparing for the examination. However, the experimental group's median is slightly higher, indicating that they felt slightly more prepared than the control group.

Table 5.11 Phi Gamma Survey Q1 Response Distributions

Q1: Was the time you spent preparing appropriate for the examination task?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
My preparation time was extremely short considering the difficulty of the examination: I should have spent at least 2 additional hours preparing	1 / 16.67%	1 / 20.00%
My preparation time was somewhat short considering the difficulty of the examination: I should have spent an additional 30 minutes – 1 hour preparing	3 / 50.00%	1 / 20.00%
I spent just the right amount of time preparing for the examination task	2 / 33.33%	3 / 60.00%
I spent a little too much time preparing: I over-prepared by approximately 30 minutes – 1 hour	0 / 0.00%	0 / 0.00%
I spent way too much time preparing: I over-prepared by at least 2 hours	0 / 0.00%	0 / 0.00%
Reference Data: Control/Experimental Group Q1 Median Response = 2 / 3 Control/Experimental Group Mean Preparation Time = 58.500 min. / 78.667 min. Control/Experimental Group Mean Execution Time = 91.333 min. / 89.167 min. Control/Experimental Group Mean % Evidence Found = 14.20% / 25.5%		

Table 5.12 presents the response distributions for survey question 2: *Did your preparation efforts contribute to a clear and complete understanding of the case?* The experimental group and control group medians are identical (4), and both indicate that the subjects felt that their respective preparation methods were helpful.

Table 5.12 Phi Gamma Survey Q2 Response Distributions

Q2: Did your preparation efforts contribute to a clear and complete understanding of the case?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
The preparation effort contributed to confusion regarding case concepts and case facts	0 / 0.00%	0 / 0.00%
The preparation effort was not helpful for understanding or identifying important case concepts	0 / 0.00%	0 / 0.00%
The preparation effort was somewhat helpful for understanding or identifying important case concepts	2 / 33.33%	2 / 40.00%
The preparation effort was helpful in understanding and identifying important case concepts	3 / 50.00%	2 / 40.00%
The preparation effort was very helpful in understanding and identifying important case concepts	1 / 16.67%	1 / 20.00%
Reference Data: Control/Experimental Group Q2 Median Response = 4 / 4 Control/Experimental Group Mean Preparation Time = 58.500 min. / 78.667 min. Control/Experimental Group Mean Execution Time = 91.333 min. / 89.167 min. Control/Experimental Group Mean % Evidence Found = 14.20% / 25.5%		

Table 5.13 presents the response distributions for survey question 3: *Estimate your level of confidence in the results of your examination?* The experimental group's response median was higher than that of the control group, and this is consistent with the results of the overall amount of evidence found by the experimental group.

Table 5.13 Phi Gamma Survey Q3 Response Distributions

Q3: Estimate your level of confidence in the results of your examination?		
Choice	**Control Group DistributionFrequency / Percent**	**Experimental Group DistributionFrequency / Percent**
I found less than 20% of the evidence	0 / 0.00%	0 / 0.00%
I found 20–40% of the evidence	2 / 33.33%	0 / 0.00%
I found 41–60% of the evidence	1 / 16.67%	2 / 40.00%
I found 61–80% of the evidence	1 / 16.67%	0 / 0.00%
I found 81–100% of the evidence	2 / 33.33%	3 / 60.00%
Reference Data: Control/Experimental Group Q3 Median Response = 3.5 / 5 Control/Experimental Group Mean % Evidence Found = 14.20% / 25.5%		

Table 5.14 presents the response distributions for survey question 4: *Were you given a sufficient amount of time to execute the examination?* The experimental group unanimously indicated that they had a sufficient amount of time to execute their search, while only 50% of the control group indicated that they had a sufficient amount of time to execute their search. This response is somewhat unexpected because the control group spent slightly less time (on average) than the experimental group during the examination session.

Table 5.14 Phi Gamma Survey Q4 Response Distributions

Q4: Were you given a sufficient amount of time to execute the examination?		
Choice	**Control Group Distribution Frequency / Percent**	**Experimental Group Distribution Frequency / Percent**
I needed a significant amount of additional time to execute the examination (> 2 hours)	0 / 0.00%	0 / 0.00%
I needed additional time to execute the examination (1–2 hours)	1 / 16.67%	0 / 0.00%
I needed a little bit of additional time to execute the examination (30 minutes – 1 hour)	2 / 33.33%	0 / 0.00%
I executed all planned activities and was given a sufficient amount of time to execute the examination	3 / 50.00%	5 / 100.00%
Reference Data: Control/Experimental Group Q4 Median Response = 3.5 / 4 Control/Experimental Group Mean Preparation Time = 58.500 min. / 78.667 min. Control/Experimental Group Mean Execution Time = 91.333 min. / 89.167 min. Control/Experimental Group Mean % Evidence Found = 14.20% / 25.5%		

5.4 Discussion of Phi Gamma Results and Conclusions

The results of the Phi Gamma experiment and its relation to the previous Alpha Delta/Bravo Charlie experiment trials are presented with respect to two research questions:

1. Does the case domain modeling methodology result in an increased amount of evidence found in an examination?

2. Does the case domain modeling methodology require a significant amount of additional effort when compared to a typical approach?

Sections 5.4.1 and 5.4.2 discuss the results with respect to research question 1, and Section 5.4.3 discusses the results with respect to research question 2. Finally, Section 5.4.4 provides conclusions and discusses implications that are relevant to the Alpha Delta, Bravo Charlie, and Phi Gamma experiment trials.

5.4.1 Amount of Evidence

Unlike the Alpha Delta and Bravo Charlie experiment trials, the Phi Gamma experiment trial yielded significant differences with respect to the amount of evidence found between the two groups. The experimental group found more evidence in all categories than the control group, and this difference was statistically significant in the Frank category and in the overall category. This result provides a strong affirmative response to research question 1. However, in order to observe this result, the case domain modeling approach was streamlined, a more document-seeded evidence drive was prepared, and a vivid case file was provided to the groups. It is assumed that the high occurrence of document file items on the disk contributed to the success of the case domain modeling method. The rationale behind this assumption involves the subjects' exclusive use of keyword searching methods; this rationale is discussed in Section 5.4.2.

5.4.2 Keyword Searching

The experimental group found more evidence than the control group using planned keyword searching, unplanned keyword searching, and overall keyword searching. These differences were significant in the non-keyword searching and overall keyword searching categories. These results provide a strong affirmative response for

research question 2. Unlike the subject in the Alpha Delta and Bravo Charlie experiments, the subject in the Phi Gamma experiment reported no evidence files located with non-keyword searching techniques.

Though the case domain modeling method was slightly modified in the Phi Gamma trial, the prescribed control group method remained unchanged from the Alpha Delta and Bravo Charlie trials. Therefore, the characteristics of the evidence disk, the case scenario, and the case scenario materials contributed heavily to the subjects' reliance on planned and unplanned keyword searching methods. The Alpha Delta and Bravo Charlie results, like the Phi Gamma results, implied that case domain modeling improved the effectiveness of keyword searches. It is likely that this reliance on keyword search methods contributed heavily to the experimental group subjects' ability to locate a significantly greater amount of evidence.

5.4.3 Time and Effort

The experimental group spent more time in the preparation session than the control group, less time in the examination session than the control group, and more overall time in the experiment than the control group. Of these three differences, only the differences in the preparation session are statistically significant. These results support an affirmative response to research question 2, indicating that the case domain modeling approach does require an additional amount of time when compared to more ad hoc approaches. However, the Phi Gamma experiment yields the first observance of the experimental group spending slightly less in any time category than the control group.

5.4.4 Overall Conclusions for the Three Practitioner Case Domain Modeling Experiments

The Alpha Delta, Bravo Charlie, and Phi Gamma experiments were planned based on the three research questions outlined in the introduction to Section 5.4. Based on those research questions, hypotheses were constructed to be evaluated by statistical tests for differences between means. These hypotheses include:

1. The experimental group will find a greater amount of evidence than the control group.
2. The experimental group will spend more time in the preparation session than the control group.
3. The experimental group will spend less time in the examination session than the control group.
4. The experimental group will spend less overall time in the combined experiment activities than the control group.
5. The experimental group will find more evidence using keyword searches than the control group.
6. The experimental group will find more evidence using non-keyword searches than the control group.

Table 5.15 presents a summary of the experiment results that relate to hypothesis 1. For each experiment trial the following information is presented: the ratio of evidence categories where the experiment group found more evidence than the control group, the ratio of evidence categories where the experimental group located a significantly greater amount of evidence than the control group, and whether or not the experimental group located a greater amount of overall evidence than the control group (* indicates a statistically significant difference). Hypothesis 1 is supported because the experimental

group consistently located a greater overall amount of evidence than the control group, and this difference is significant in the Phi Gamma trial.

Table 5.15 Summary of Evidence Found in Alpha Delta, Bravo Charlie, and Phi Gamma Experiments

Experiment Trial	Ratio of Evidence Categories where Experimental > Control	Ratio of Evidence Categories where Experimental > Control (statistically significant)	Overall Evidence: Experimental > Control?
Alpha Delta	1 / 4	0 / 4	Yes
Bravo Charlie	2 / 3	0 / 3	Yes
Phi Gamma	3 / 3	1 / 3	Yes*
* indicates a statistically significant difference			

Table 5.16 presents a summary of the experiment results that relate to hypotheses 2–4. For each experiment trial the following information is provided: whether or not the experimental group spent a greater amount of time in the preparation session, whether or not the experimental group spent a greater amount of time in the execution session, and whether or not the experimental group spent a less overall amount of time in the examination. Table entries that contain an asterisk (*) represent a statistically significant difference. Hypothesis 2 is strongly supported because all three experiment trials revealed that the experimental group spent a significantly greater amount of time planning than the control group. This difference was expected because of the more rigorous nature of the case domain modeling preparation method. Hypothesis 3 is weakly supported by the fact that in the Phi Gamma trial, the experimental group spent slightly less time in the

examination than the control group. In contrast, in the Alpha Delta and Bravo Charlie experiment trials, the control group spent a significantly less amount of time in the examination session than the experimental group. Likewise, the control group consistently spent less overall time in the experiment than the experimental group, and these differences were significant in the Alpha Delta and Bravo Charlie trials.

Table 5.16 Summary of Time Data in Alpha Delta, Bravo Charlie, and Phi Gamma Experiments

Experiment Trial	Preparation Time: Experimental > Control?	Execution Time: Experimental < Control?	Overall: Experimental < Control?
Alpha Delta	Yes*	No*	No*
Bravo Charlie	Yes*	No*	No*
Phi Gamma	Yes*	Yes	No
* indicates a statistically significant difference			

Table 5.17 summarizes the experiment results that relate to hypothesis 5 and hypothesis 6. For each experiment trial the following information is presented: whether or not the experimental group found a greater amount of evidence than the control group using unplanned keyword searches, planned keyword searches, all keyword searches, and non-keyword searches. Table entries that contain an asterisk (*) represent a statistically significant difference.. In all three experiment trials the experimental group found more evidence using overall keyword methods than the control group, and these differences were significant in the Bravo Charlie and Phi Gamma trials. The consistent trend and the significant differences strongly support hypothesis 5. The control group found more

evidence using non-keyword searches in the Alpha Delta and Bravo Charlie trials, and none of these differences were significant. In the Phi Gamma experiment no subjects reported any evidence files found using non-keyword searching methods. Though it would be ideal for case domain modeling to contribute to more evidence found using keyword and non-keyword searching methods, case domain modeling was specifically tailored for keyword searching methods. The failure of the experiments to support hypothesis 6 is not necessarily a negative outcome when considering the positive evidence supporting hypothesis 5. The control group generally found less evidence using keyword searches than the experimental group. It follows that the control group would find more evidence using non-keyword searches than the experimental group.

Table 5.17 Summary of Search Method Data in Alpha Delta, Bravo Charlie, and Phi Gamma Experiments

Experiment Trial	**Planned Keywords: Experimental > Control?**	**Unplanned Keywords: Experimental > Control?**	**Overall Keywords: Experimental > Control?**	**Non-keywords: Experimental > Control?**
Alpha Delta	No*	Yes	No	No
Bravo Charlie	Yes	Yes*	Yes*	No
Phi Gamma	Yes	Yes*	Yes*	Equivalent
* indicates statistically significant difference				

With the exception of the Alpha Delta trial, the case domain modeling preparation method consistently and significantly increased the effectiveness of keyword searching in the experiment trials. The case domain modeling method also consistently yielded more

located evidence file items than the ad hoc method. In the Phi Gamma trial this difference was significant, and the utility of the case domain modeling approach was likely impacted by the characteristics of the evidence disk that contained significantly greater document file items than the Alpha Delta and Bravo Charlie trials; the Phi Gamma evidence disk contained more than 4,000 document file items, while the Alpha Delta and Bravo Charlie disks contained fewer than 100 document file items. Thus, when a practitioner feels that keyword searching will be heavily used in an examination, then the case domain modeling method would be an appropriate tool for deriving search goals and keyword search terms.

The use of the case domain modeling approach requires an investment of additional time. In the Alpha Delta and Bravo Charlie trials this overall investment of time was significantly greater than in the Phi Gamma trial. Though these differences were statistically significant, they represent a relatively negligible amount of time due to the brief nature of the experiments: a maximum of 3 or 4 hours was allowed in each of the experiment sessions. When the amount of document file items and case file information was significantly increased, the case domain modeling method contributed to a slightly lower examination time than the ad hoc method. This result implies that the case domain modeling method may contribute to lower examination times and perhaps a lower overall amount of time when a sufficiently large, complex case is encountered.

5.5 Threats to Validity of the Experiments

Threats to validity in this section are discussed with respect to three categories: internal validity, construct validity, and external validity. Internal validity refers to

whether or not there is a causal relationship between the case domain modeling planning method and the observed improvements in evidence collection and keyword searching. The results of the experiments established a strong relationship between the case domain modeling method and an increase in effort. It is possible that this additional effort caused the observed improvements in evidence collection and keyword searching.

Construct validity refers to whether or not the data collected in the experiments accurately represents the quality of a computer forensics examination and the effectiveness of its search activities. One limitation of the study is that each evidence item is weighed equally and the quality of an examination is determined by how many evidence items are recovered. Though some items of evidence can be more valuable in a presentation, during the examination it is appropriate for the technician to find as much relevant evidence as possible. The experiments also do not evaluate qualitative factors such as the quality of the examination report or the repeatability of the examination procedure.

External validity refers to whether or not the conclusions of these studies may be generalized to other practitioners of computer forensics now and in the future. The following factors should be considered before generalizing the results of these experiments: the duration of the examination activities, the size of the population, and the characteristics of the population. The planning methodology is designed for large-scale examinations and investigations that could require weeks or months of effort. Due to time constraints and the availability of subjects, the experiments provided a total of eight hours for the examination activity. Though the size of the subject population was sufficient to

observe statistically significant differences, the population size was not large enough to reject outliers in the results. Finally, the subjects were graduate and undergraduate computer science and engineering students taking an introductory computer forensics course. Though the target users of the methodology would have practical computer expertise, they would likely hold college degrees in criminal justice and accounting. Thus, the target user group would, at first, be less familiar with the theoretical concepts of domain modeling than the experiment subjects.

Chapter 6 concludes the evaluation of case domain modeling by presenting the results of two case studies involving traditional law enforcement investigators. While the experiments in Chapter 4 and this chapter evaluated the utility of case domain modeling as a forensics examiner's tool, Chapter 6 will evaluate the utility of case domain modeling as an investigator's forensics service solicitation tool.

CHAPTER VI

CASE DOMAIN MODELING APPLICATIONS FOR LAW ENFORCEMENT INVESTIGATORS: PREPARING FOR AND SOLICITING COMPUTER FORENSICS SERVICES

Case studies were conducted in order to elicit feedback from law enforcement investigators regarding the practicality and applicability of case domain modeling in soliciting the services of a forensics technician. The following two case studies correspond to the following dissertation research question: *Is the case domain modeling method useful for typical law enforcement investigators who participate in cases involving computer forensics?*

Section 6.1 presents the design and results of Case Study 1, Section 6.2 presents the design and results of Case Study 2, Section 6.3 presents conclusions drawn from the two law enforcement case studies, and Section 6.4 presents the threats to validity of the case studies.

6.1 Case Study 1: Pilot Study

This case study involved two law enforcement investigators attending the CF101, Computer Forensics Tools and Techniques course at the Mississippi State University Computer Forensics Training Center. This case study was designed as a pilot study that

was run in order to prepare for the Case Study 2, which involved a larger group of subjects. Section 6.1.1 discusses the design of the case study, Section 6.1.2 presents the data that was collected from the subjects, and Section 6.1.3 presents a discussion of the results of the case study and conclusions.

6.1.1 Case Study 1: Method

The general purpose and design philosophy of Case Study 1 and Case Study 2 were the same. Unlike the practitioner experiments, the subjects in these case studies were not distributed between a control group and an experimental group. Instead, all of the subjects in each case study were given the same instructional lecture, the same activity to complete, and the same post-study evaluation survey. Also, the subjects were not using case domain modeling in the same manner as the practitioner subjects used case domain modeling: In the Chapter IV & V experiments, the subjects created a case domain model and derived keyword search terms, and in these case studies the subjects were provided with a forensics service solicitation form supplemented with a generalized case domain model. The purpose of the case domain model in these case studies was to communicate to the investigator the hypothetical forensic technician's assumptions regarding what information is most important with respect to a general type of case. The hypothesis is that communicating these assumptions will help solicit the most relevant information from the investigator while also giving them room to challenge these assumptions. Though the two case studies were somewhat different, in both instances the subjects were given a case scenario and tasked with filling out a forensics service solicitation form that featured the case domain model.

All subjects voluntarily participated in the experiment after all the planned coursework was completed. There was a total of three hours allocated for conducting the case study. The first 30–40 minutes was allocated to a training lecture that described the case study policies, research goals, and case domain modeling approach. The remaining 2.5–2.67 hours were allocated to the subjects' execution of a forensics service solicitation task.

At the beginning of the forensics solicitation task the subjects were given the same email death threat case file materials that were provided to the subjects in the Phi Gamma practitioner experiment. The subjects were instructed to read the case file materials and complete a forensics service solicitation form that was prepared by a fictitious digital forensics service provider. They were also given a hard copy of the case domain model illustrated in Figure 6.1. The form solicited information as follows:

1. *Based on the Case Domain Model please identify all known attribute values by filling out the table below* [Table 6.1 provides an excerpt of the table]. *If attribute values are unknown, then mark "Unknown" in the attribute value fields. If you are unsure of attribute values based on your knowledge of the case, then mark "Unsure" in the attribute value field. If the attribute value is a very long text excerpt, mark "see attachment."*

2. *Are there any Missing Concepts or Attributes in the Case Domain Model? If so then list them in the space provided below. Be sure you identify a concept name for the missing attribute(s), and be sure to distinguish between concepts and attributes when identifying new concepts.*

3. *Summarize the goals of your requested forensics service. Each goal statement should clearly and concisely state a single goal of the forensics examination. If possible, use concept and attribute names in your goal descriptions. If additional space is needed, then use the back of the page.*

4. *Is there anyone else we should contact regarding the case? Please provide the contact information if possible.*

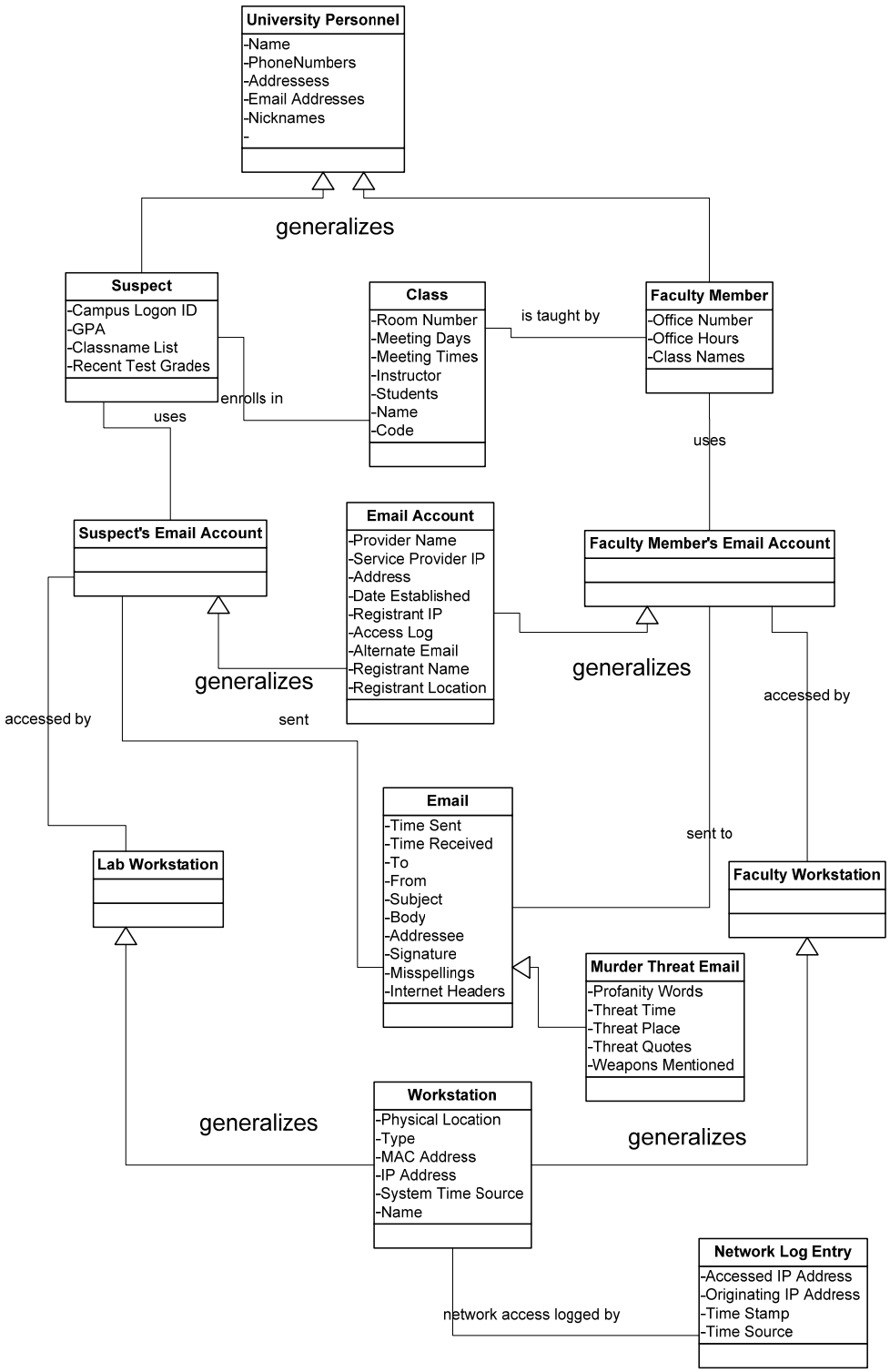


Figure 6.1 Email Death Threat Case Domain Model

Table 6.1 Partial Concept Attribute Value Table for Form Step 1

Concept Name	**Attribute Name**	**Attribute Value**
Suspect	Name	
Suspect	Phone Numbers	
Suspect	Email Addresses	
Suspect	Campus Logon ID	
Suspect	GPA	
Suspect	Classname List	
Suspect	Recent Test Grades	
Suspect's Email Account	Provider Name	
Suspect's Email Account	Service Provider IP	
Suspect's Email Account	Address	
Suspect's Email Account	Date Established	
Suspect's Email Account	Registration IP	

When the subjects finished conducting this forensics service solicitation task, the time that it took them to perform the task was recorded and they completed a survey that solicited information regarding their background and opinions regarding their case study experience. The survey contains five multiple choice questions and six discussion/short answer questions. Table 6.2 presents the multiple choice questions and Table 6.3 presents the discussion/short answer questions.

Table 6.2 Case Study 1 Multiple Choice Survey Questions

Question ID	Question Statement and Response Choices
MQ1	Rate your level of expertise and confidence with respect to computers and software technology. a. Little to No Computer Experience b. Beginner Computer User c. Novice Computer User d. Advanced Computer User e. Expert Computer User
MQ2	On a 1-5 scale, rate your understanding of the content and purpose of the case domain model. 1 indicates the lowest level of understanding and 5 indicates the highest level of understanding. (Circle the appropriate number) 1 2 3 4 5
MQ3	On a 1-5 scale, do you think that building (from scratch) a case domain model or a similar type of model would be a practical tool for use in actual investigations and forensics examinations? 1 indicates the lowest level of utility/practicality, and 5 indicates the highest level of utility/practicality. (Circle the appropriate number) 1 2 3 4 5
MQ4	On a 1-5 scale, would requesting forensics services using the method outlined in the exercise be helpful to you? 1 indicates the lowest level of utility and 5 indicates the highest level of utility. (Circle the appropriate number) 1 2 3 4 5
MQ5	Did the modeling contribute to a clear and complete understanding of the case? a. The preparation effort contributed to confusion regarding case concepts and case facts b. The preparation effort was not helpful for understanding or identifying important case concepts c. The preparation effort was somewhat helpful for understanding or identifying important case concepts. d. The preparation effort was helpful in understanding and identifying important case concepts e. The preparation effort was very helpful in understanding and identifying important case concepts.

Table 6.3 Case Study 1 Discussion/Short Answer Survey Questions

Question ID	Question Statement
DQ1	How many years have you been a law enforcement agent?
DQ2	Approximately how many times have you requested computer forensics services?
DQ3	In the assignment scenario, would you perform any additional investigative activities before submitting your request for forensics services? If so, did the case domain model and request form help you arrive at this conclusion?
DQ4	Describe the strengths of the case domain model and the service request method.
DQ5	Describe the weaknesses of the case domain model and the service request method.
DQ6	Other comments and notes.

6.1.2 Case Study 1: Data Collected

This section reports the time spent by the subjects and their responses to the post-experiment survey. Table 6.4 presents the time data collected for the two subjects. Time is expressed in minutes, and the average time of the two subjects is presented in the last row of the table.

Table 6.4 Case Study 1
Time Data

Subject ID	Time (min.)
CS1	95
CS2	98
AVG	96

Table 6.5 reports the subjects' responses to the multiple choice post-experiment survey questions. The letter response values (a–e) for MQ1 and MQ5 were transposed to numbers (1–5). The median response values are provided on the last row of the table.

Table 6.6 reports the subjects' responses to the discussion/short answer questions. "No Response" indicates that the subject did not provide a response to the corresponding question.

Table 6.5 Case Study 1 Multiple Choice Survey Responses

SubjectID/QuestionID	MQ1	MQ2	MQ3	MQ4	MQ5
CS1	3	2	4	4	3
CS2	2	2	4	4	3
MEDIAN	2.5	2	4	4	3

Table 6.6 Case Study 1 Discussion/Short Answer Survey Responses

Question ID/SubjectID	CS1	CS2
DQ1 (yrs. in law enforcement)	27	6
DQ2 (number of digital forensics requests)	0	0
DQ3	Yes I would like other question added – (chat logs) The model (domain) did give me other ideas (history logs) (user names)	Yes the investigator should have checked up on the stories he got from Jane, it did not match the story of Palmer. In general the investigator should go more in depth.
DQ4	I think it could help a jury understand better if in layman terms.	It would be a good guideline for investigators to go by during the investigation.
DQ5	Maybe tough to explain to a jury	No Response
DQ6	Great job. Just not sure I was right person for survey.	No Response

6.1.3 Case Study 1: Discussion of Results and Conclusions

The two subjects in the experiment had 27 and 6 years of law enforcement investigative experience. Both subjects indicated that they had never requested computer forensics services. One subject indicated that he/she was a beginner computer user, while the other subject indicated that he/she was a novice computer user.

The responses to the multiple choice survey questions are inconsistent. On MQ2, both subjects indicated that they did not clearly understand the purpose of the case

domain modeling method; both subjects responded with a 2, where the range of responses was 1–5 (5 indicating the highest level of understanding). The subjects also responded somewhat moderately to MQ5, as each responded that "the preparation method was somewhat helpful in understanding and identifying important case concepts." However, on MQ3 and MQ4 the subjects responded more strongly and favorably to case domain modeling; they both responded with a 4 (1 indicates the most negative response and 5 indicates the most affirmative response) when asked, "Do you think that building (from scratch) a case domain model or a similar type of model would be a practical tool for use in actual investigations and forensics examinations?," and "Would requesting forensics services using the method outlined in the exercise be helpful to you?"

The subjects' comments in MQ3, MQ4, and MQ5 also provide some insight regarding the case domain modeling preparation method. Subject CS1 indicated in MQ3 that the model helped them consider alternative investigative ideas/possibilities. In MQ4 the subjects indicated the positive aspects of the case domain model by indicating that it could be helpful for presenting to a jury and helpful as an investigative guideline. However, the same subject indicated that the model may be difficult to explain to a jury.

Though the subjects provided positive indications that case domain modeling would be practical and useful for digital forensics solicitations, subjects also indicated that they did not clearly understand the case domain modeling method. It is assumed that the training session and the solicitation form may have presented too many theoretical concepts that confused the subjects. Based on these responses a revised training session and forensics request form was prepared for Case Study 2.

6.2 Case Study 2

This case study involved seven law enforcement investigators attending the CF102, Computer Forensics Tools and Techniques course at the Mississippi State University Computer Forensics Training Center. This case study was a repeat of Case Study 1, but with revised training, activity form, and survey materials. These revisions were made based on the results of Case Study 1 and were an attempt to present a less theoretical lecture on case domain modeling. Section 6.2.1 discusses the design of the case study, Section 6.2.2 presents the data that was collected from the subjects, and Section 6.2.3 presents a discussion of the results of the case study and conclusions.

6.2.1 Case Study 2: Method

As in Case Study 1, Case Study 2 involved a training session, a case domain modeling driven digital forensics service solicitation activity, and a post-case study survey. The training presentation was revised/extended to provide more concrete examples of case domain modeling. Also, the term, "case domain modeling" was replaced with a more user-friendly term, "search scope diagram." The forensics service solicitation form was also revised and extended to more explicitly include the case domain modeling and separately solicit case information from defined categories. Figure 6.2 presents a section of the forensics solicitation form that preceded a query for information regarding case suspects.

The Involved People and Their Relationships?

It is extremely important that you provide us with accurate and relevant information about the people involved in the case. Our search scope model includes what we consider to be the most important descriptive attributes about the people (and their relationships) relevant to email threat cases. The figure illustrates the scope of information that we will be requesting from you in this section. It may be helpful for you to review the diagram while jogging your memory and locating the required information in your case notes. If you feel we have missed anything important or have asked for things outside of the scope of the case, please tell us at the end of each subsection.

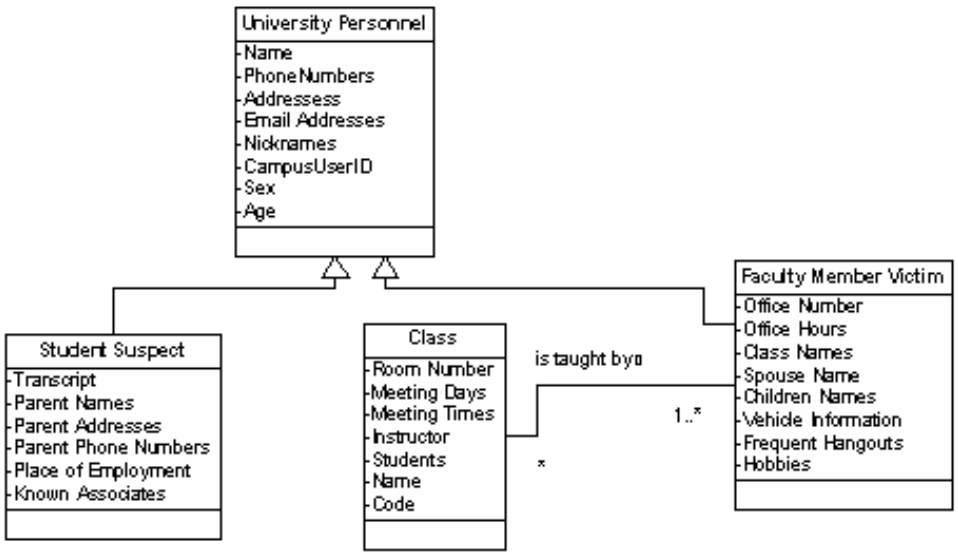


Figure 6.2 Case Study 2 Forensics Solicitation Form Excerpt 1

Figure 6.3 presents a portion of the solicitation form fields that preceded the appearance of Figure 6.2 in the distributed case study solicitation materials.

The Suspect(s)

For each suspect involved in the case please fill out the following forms. If you need additional space please use the back of the page. We will use this information to look for documents and files that were likely authored by the suspect(s).

----------Student Suspect 1----------

Name:_____
Age:_____ Sex: M F

Nicknames/Aliases:_____

Known
Associates:_____

Address:
Street:_____ City:_____
State:____Zip:_____

Phone Numbers:
Home:_____ Cell:_____ Work:_____
Other:_____

Email
Addresses:_____

Campus UserID:_____Major: _____
Minor:_____
Place of
Employment:_____
Mother's
Name:_____
Address:
Street:_____ City:_____
State:____Zip:_____
Other:_____

Figure 6.3 Case Study 2 Forensics Solicitation Form Excerpt 2

Table 6.7 Case Study 2 Short Answer/Discussion Survey Questions

Question ID	Question Statement
DQ1	How many years have you been a law enforcement agent?
DQ2	Approximately how many times have you requested computer forensics services?
DQ3	Approximately how many times have you performed computer forensics services?
DQ4	Describe the strengths of the search scope model and the service request method.
DQ5	Describe the weaknesses of the search scope model and the service request method.
DQ6	Other comments and notes.

Most of the multiple choice questions in the Case Study 2 survey were different than those in the Case Study 1 survey. Table 6.8 presents the multiple choice questions included in the Case Study 2 survey. Note that the term “case domain model” is replaced with “search scope diagram.”

Table 6.8 Case Study 2 Multiple Choice Survey Questions

Question ID	Question Statement and Response Choices
MQ1	Rate your level of expertise and confidence with respect to computers and software technology. a. Little to No Computer Experience b. Beginner Computer User c. Novice Computer User d. Advanced Computer User e. Expert Computer User
MQ2	On a 1-5 scale, rate your understanding of the content and purpose of the search scope diagrams included in the forensics service request form. 1 indicates the lowest level of understanding and 5 indicates the highest level of understanding. (Circle the appropriate number) 1 2 3 4 5
MQ3	On a 1-5 scale, rate your ability and potential to learn how to effectively build a search scope model from scratch? 1 indicates the lowest level of competence, and 5 indicates the highest level of competence. (Circle the appropriate number) 1 2 3 4 5
MQ4	On a 1-5 scale, would requesting forensics services using the method outlined in the exercise be helpful to you? 1 indicates the lowest level of utility and 5 indicates the highest level of utility. (Circle the appropriate number) 1 2 3 4 5
MQ5	Do you feel that reviewing the search scope model (in the training session and in the forensics request forms) helped you to realize flaws in the investigation that occurred in the scenario? 1 indicates the lowest level of usefulness and 5 indicates the highest level of usefulness. (Circle the appropriate number) 1 2 3 4 5
MQ6	Do you think that the search scope diagrams would be a helpful visual aid for presenting computer forensics findings to a jury? 1 indicates the lowest level of usefulness and 5 indicates the highest level of usefulness. (Circle the appropriate number) 1 2 3 4 5
MQ7	If you had a large collection of search scope diagrams that outlined many common computer forensics cases, would they helpful reference tools for planning your pre-forensics investigation? 1 2 3 4 5

6.2.2 Case Study 2: Data Collected

Table 6.9 presents the demographic information collected for MQ1, DQ1, DQ2, and DQ3. The average response for MQ1 is 3, "Novice Computer User." The average number of years of investigative experience is 24.17, the average number of times the subjects requested and performed digital forensics services is 2.8 and 0, respectively. Subject CS5 did not respond to any of the survey questions, and subject CS3 did not provide quantifiable numbers for DQ2 and DQ3, so their responses are not included in the averages.

Table 6.9 Case Study 2 Demographic Information

Question	CS1	CS2	CS3	CS4	CS5	CS6	CS7	Average
MQ1 (Computer Expertise 1 – 5)	3	3	4	3	No Response	3	2	3*
DQ1 (yrs. Investigative Experience)	26	19	53	16	No Response	13	18	24.17*
DQ2 (# of times requested forensics)	1	10	Numerous	0	No Response	0	3	2.8**
DQ3 (# of times performed forensics)	0	0	Numerous	0	No Response	0	0	0**
*This average excludes CS5 because CS5 did not provide a response **This average excludes CS5 and CS3 because CS5 did not provide a response, and CS3 did not provide a quantifiable response.								

Table 6.10 presents the results to survey multiple choice questions MQ2–MQ7. The median responses for each question are provided in the right-most column. Subject

CS5 did not provide responses to any of these questions, so his/her responses are not included in the computed medians.

Table 6.10 Case Study 2 Multiple Choice Question Responses MQ2–MQ7

Question	CS1	CS2	CS3	CS4	CS5	CS6	CS7	Median
MQ2 (comprehension)	4	4	3	3	N/A	4	2	*3.5
MQ3 (potential to learn to develop models)	4	3	3	3	N/A	3	3	*3
MQ4 (utility)	4	2	3	3	N/A	4	3	*3
MQ5 (realizing flaws)	4	4	3	3	N/A	4	3	*3.5
MQ6 (visual aid)	4	3	2	3	N/A	4	3	*3
MQ7 (utility of collection)	4	4	2	3	N/A	3	3	*3
*This excludes CS5 because CS5 did not provide a response								

Only one subject provided a response to one of the discussion questions DQ4–DQ6. Subject CS3 responded to DQ4, which asked the subjects to comment on the strengths of the forensics service solicitation method with the search scope diagram: “Effective but a lot of lost time due to information and data transfer.”

6.2.3 Case Study 2: Discussion of Results and Conclusions

The subjects’ responses to the multiple choice questions MQ2–MQ7 may be characterized as moderate: the responses of these questions have a range of 1–5, and the

average responses for MQ2–MQ7 were between 3 and 3.5. This moderate characterization is also supported by the fact that only one subject responded to any of the discussion questions.

The average response to MQ2 indicate that the subjects had a moderate comprehension of the search scope method, and half of the responding subjects indicated a high comprehension of the search scope model (indicating 4 out of a possible 5). This is an improvement over Case Study 1, when both subjects indicated a low comprehension of the search scope method.

MQ5 asks, "Do you feel that reviewing the search scope model (in the training session and in the forensics request forms) helped you to realize flaws in the investigation that occurred in the scenario?" The subjects responded more positively to MQ5 (median response = 3.5) than to any of the other questions. Fifty percent of the subjects indicated 4 to MQ5, and the remaining 50% of the subjects indicated 3.

One subject responded to a discussion question by indicating that the case domain modeling service solicitation method was useful but that it duplicated case information and took time to transfer information. Other case study subjects indicated similar responses in discussions with the principal investigator after the case study. It is likely that many investigators do not want to perform any more "paperwork" than is necessary, and the subjects seemed to have viewed the activity as paperwork. This seems to imply that the subjects would respond more favorably to the case domain modeling method if it were supported by a semi-automated tool that reduced the form-filling/paperwork nature

of the method. It also was not explained to the subjects that the prescribed method was experimental and would involve a technology transfer phase before being adopted.

6.3 Case Study 1 and Case Study 2: Summary and Conclusions

These case studies were designed to form a response to the research question that states: *Is the case domain modeling method useful for typical law enforcement investigators who participate in cases involving computer forensics?* The purpose of the case domain modeling method in these case studies was to solicit important case information from the investigators and support communication and knowledge transfer between the investigators and the forensics technicians. The conclusions presented in this section are based on the subjects' responses to post-case-study surveys. The following two paragraphs will summarize the results of Case Study 1 and Case Study 2. When responses to multiple choice questions are discussed, the value of the subjects' responses may be provided to supplement the discussion. These multiple choice questions have a range of 1–5, where 1 is the most negative response and 5 is the most positive response.

In Case Study 1, both subjects indicated that the method was useful when they responded with a 4 to two survey questions regarding the utility of the method in practical investigations. However, both subjects indicated that they did not have a clear understanding of the case domain modeling method: both subjects indicated a 2 to the survey question regarding method comprehension. Based on the subjects' difficulty in understanding the method, the training materials and case domain modeling forensics solicitation exercise were modified for use in Case Study 2. The desired result of these modifications was to increase subjects' comprehension of the prescribed forensics service

solicitation method. Additionally, in the discussion questions one subject indicated that the method would be useful for presentation to a jury (but difficult to explain to a jury), while the other subject indicated that the method would be a useful guideline for investigators to follow during an investigation.

The modifications to the training materials and case domain modeling forensics service solicitation method yielded an increase in subject comprehension. The median response to the survey question regarding comprehension was 3.5: three subjects indicated a value of 4, two subjects indicated a value of 3, and only one subject indicated a value of 2. The overall practitioner response to the case domain modeling method for forensics service solicitation may be characterized as moderate; the subjects did not react overwhelmingly positively or negatively when queried about the benefits or drawbacks of the prescribed method. The subjects indicated the most positive response when asked if the method helped them realize flaws in the investigative activities outlined in the case file; the median response was 3.5. Subjects indicated in discussion questions and in post-case-study conversations that the method duplicated paperwork and required excessive time for information transfer.

Based on the results of the case study the law enforcement subjects indicated that case domain modeling was most useful for identifying flaws in the investigative effort. Their overall response was moderate; they did not provide an overwhelmingly positive or negative response to the utility of case domain modeling. They also indicated that case domain modeling was somewhat difficult to understand in the exercise. Since the service solicitation exercise was primarily a form-filling/information transfer task, many subjects

had the impression that case domain modeling meant more paperwork. Subjects would likely respond more favorably to the same exercise if a semi-automated software tool supported the information transfer.

6.4 Threats to Validity

The threats to validity in these case studies are discussed in this section with respect to three categories: internal validity, construct validity, and external validity. Internal validity refers to whether or not the occurrence of case domain modeling in the solicitation activity caused the subjects to indicate that the solicitation method was moderately useful. The subjects were taking a free training course, and they may have felt obligated to respond positively on the surveys. Though their responses were not overwhelmingly positive, the subjects may have been more inclined to react more negatively if the study were not conducted in association with a free training course.

Construct validity refers not only to how accurately the survey solicited qualitative factors such as utility, but it also refers to how well the case study activity applied case domain modeling. In the studies, the purpose and method of domain modeling were discussed, and case domain models were used as visual aids and supporting features of the service solicitation task. Since the subjects in the study were not required to build domain models their survey responses (see MQ3 in case study 1) regarding the utility, building domain models was based on speculation and their ability to understand the fundamental theories of domain modeling. Additionally, since the survey was relatively brief, it did not include a pool of questions regarding the utility of case domain modeling in specific scenarios.

External validity refers to whether or not the conclusions of these studies may be generalized to other practitioners of computer forensics now and in the future. Since the combined population of these studies is nine subjects, it would be inappropriate to apply the conclusions of these studies to a large general population of law enforcement practitioners involved in computer forensics examinations. Additionally, the population of the study was primarily veteran law enforcement investigators with limited information technology and computer forensics expertise. The target user group of the methodology described in Chapter III has a more extensive information technology background and is routinely involved in large-scale and complex computer forensics cases. Target users of the methodology are likely to be employed by federal agencies, while the subjects in the case studies were employed by state and county law enforcement agencies.

The next chapter, Chapter 7, will conclude this document by summarizing the results of all the experiments and case studies, providing responses to the research questions, and introducing the potential for future applications and research work.

CHAPTER VII

CONCLUSIONS AND FUTURE WORK

This chapter concludes the dissertation by summarizing the conclusions formed that correspond to the three research questions:

1. Does the case domain modeling methodology result in an increased amount of evidence found in an examination?
2. Does the case domain modeling methodology require a significant amount of additional effort when compared to a typical approach?
3. Is the case domain modeling method useful for typical law enforcement investigators who participate in cases involving computer forensics?

Section 7.1 discusses research question 1, Section 7.2 discusses research question 2, and Section 7.3 discusses research question 3. Finally, Section 7.4 presents a discussion of future research for case domain modeling in computer forensics.

7.1 Research Question 1: The Amount of Evidence Found in Examination

As indicated in Chapter 5 and Chapter 6, examination planning with case domain modeling consistently contributed to a greater amount of evidence found by experiment subjects. The experimental group used the case domain modeling method and the control group used a typical, ad hoc method. The experimental group subjects found a significantly greater amount of evidence in the Phi Gamma trial, where relatively vivid case details were provided and a relatively abundant amount of document file items were present on the evidence drive. These experimental group subjects also found a greater

amount of overall evidence, albeit not significantly greater, in two experiment trials (Alpha Delta and Bravo Charlie) where only vague case background details were provided. Table 7.1 reprises Table 5.15 and presents a summary of the results of the three experiments with respect to the amount of evidence found. Experiment 3 yielded the best performance by the case domain modeling group: the case domain modeling subjects found more evidence than the control group in all three evidence categories, the difference in one of these evidence categories was statistically significant, and the difference in overall evidence was statistically significant. When compared to other experiments, Experiment 3 had a relatively vivid case file/background and the evidence drive contained an abundance of document file item types. Based on the comparison of the amount of evidence found by the subject groups, the following statement applies to Research Question 1: *Examination planning with case domain modeling contributes to an*

Table 7.1 Summary of Evidence Found in Alpha Delta, Bravo Charlie, and Phi Gamma Experiments

Experiment Trial	**Ratio of Evidence Categories where Experimental > Control**	**Ratio of Evidence Categories where Experimental > Control (statistically significant)**	**Overall Evidence: Experimental > Control?**
Alpha Delta	1 / 4	0 / 4	Yes
Bravo Charlie	2 / 3	0 / 3	Yes
Phi Gamma	3 / 3	1 / 3	Yes*
* indicates a statistically significant difference			

increase in the amount of evidence found, and this improvement is significant when the forensics technician is provided with vivid case details and an evidence disk with a relatively high occurrence of document file items.

Data collected from Experiments 1–3 also includes information regarding the search methods that subjects used for locating evidence. These methods were categorized as planned keyword searches, unplanned keyword searches, overall keyword searches, and non-keyword searches. Table 7.2 provides a reprisal of Table 5.17 and a summary of the experiment results with respect to the amount of evidence found with search methods. With the exception of the Alpha Delta trial, case domain modeling consistently contributed to a greater amount of evidence located using unplanned and overall keyword searching. Additionally, in the majority of the experiment trials, case domain modeling subjects located more evidence using planned keyword searches than the control group

Table 7.2 Summary of Search Method Data in Alpha Delta, Bravo Charlie, and Phi Gamma Experiments

Experiment Trial	**Planned Keywords: Experimental > Control?**	**Unplanned Keywords: Experimental > Control?**	**Overall Keywords: Experimental > Control?**	**Non-keywords: Experimental > Control?**
Alpha Delta	No*	Yes	No	No
Bravo Charlie	Yes	Yes*	Yes*	No
Phi Gamma	Yes	Yes*	Yes*	Equivalent
* indicates statistically significant difference				

subjects. Based on the comparison of the amount of evidence found by the subject groups using particular search methods, the following statement applies to Research Question 1: *Examination planning with case domain modeling contributes to more effective keyword searches when compared to a typical, ad hoc planning approach.*

7.2 Research Question 2: The Effort Involved in Applying Case Domain Modeling

As indicated in Chapter 5 and Chapter 6, case domain modeling contributed to a consistent increase in the amount of planning effort and overall effort. Table 7.3 reprises Table 5.16 and presents a summary of the differences between the experimental (case domain modeling) and control (ad hoc) groups in Experiments 1–3. In all of the experiment trials the case domain modeling method contributed to a significant increase in preparation time. This difference was expected, and it was hypothesized that an up-front investment of case domain modeling effort would contribute to a lower examination time. The results of the experiments do not support that hypothesis, as in all but one trial (Phi Gamma), the experimental groups' examination times were significantly greater than the control groups' examination times. Based on these observations, the following statement applies to Research Question 2: *Generally, the case domain modeling method requires a significant increase in planning and examination time. However, in its most successful trial, case domain modeling contributed to a lower examination mean time.* It is also important to note that the experiment sessions were limited to four hours each, yielding a maximum of eight hours for the overall planning and examination effort.

Table 7.3 Summary of Time Data in Alpha Delta, Bravo Charlie, and Phi Gamma Experiments

Experiment Trial	Preparation Time: Experimental > Control?	Execution Time: Experimental < Control?	Overall: Experimental < Control?
Alpha Delta	Yes*	No*	No*
Bravo Charlie	Yes*	No*	No*
Phi Gamma	Yes*	Yes	No
* indicates a statistically significant difference			

7.3 Research Question 3: Utility for Traditional Investigators

In Case Study 1, both subjects indicated that the method was useful when they responded positively to two survey questions regarding the utility of the method in practical investigations. However, both subjects indicated that they did not have a clear understanding of the case domain modeling method. Based on the subjects' difficulty in understanding the method, the training materials and case domain modeling forensics solicitation exercise were modified for use in Case Study 2. The desired result of these modifications was to increase subject comprehension of the prescribed forensics service solicitation method. Additionally, in the discussion questions one subject indicated that the method would be useful for presentation to a jury (but difficult to explain to a jury), while the other subject indicated that the method would be a useful guideline for investigators to follow during an investigation.

The modifications to the training materials and case domain modeling forensics service solicitation method produced an increase in subject comprehension. The average

response to the survey question regarding comprehension increased from 2 to 3.33 (out of a possible 5). The overall practitioner response to the case domain modeling method for forensics service solicitation may be characterized as moderate; the subjects did not react overwhelmingly positively or negatively when queried about the benefits or drawbacks of the prescribed method. The subjects indicated the most positive response when asked if the method helped them realize flaws in the investigative activities outlined in the case file; the average response was 3.5 out of 5. Additionally, subjects indicated in discussion questions and in post-case-study conversations that the method duplicated paperwork and required excessive time for information transfer.

Since the service solicitation exercise was primarily a form-filling/information transfer task, many subjects had the impression that case domain modeling meant more paperwork. Subjects would likely respond more favorably to the same exercise if a semi-automated software tool supported the information transfer. Based on the results of the case studies, the following statement applies to Research Question 3: *Law enforcement investigators indicated that case domain modeling was moderately effective for soliciting computer forensics services. Additionally, the subjects indicated in conversation that the method would be more useful if supported by a semi-automated software tool*.

7.4 Future Work

This dissertation represents the first known research concerning the application of domain modeling to planning and executing computer forensics examinations. Thus, the adoption of case domain modeling is not likely to occur until further research has been

conducted, ready-to-use methodologies are refined, and semi-automated tools are implemented (i.e. technology transfer).

The results of this dissertation research suggest that case domain modeling would be more appropriate for cases involving vivid details with an abundance of document items on the evidence drive. Future experiments could more definitively evaluate this observation by further characterizing the attributes of an evidence disk and its underlying case scenario. Additionally, it would be beneficial to evaluate the performance of case domain modeling against other typical or ad hoc approaches. For example, the control group could be given a detailed lesson on Forensic Toolkit and instructed to begin the examination without a preparation session. Such variations would provide more definitive answers regarding the effectiveness of case domain modeling and other approaches to digital forensics examinations.

Finally, future research work should include case studies where investigators use case domain modeling as an analytical tool instead of an information transfer and fact checking tool. If possible, future research work should include experiments (similar to the student experiments in this dissertation) that involve law enforcement investigators and forensics practitioners. Criminal justice students could provide another alternative population of experiment subjects.

Based on the results of future research, a ready-to-use case domain modeling methodology could be defined and adopted by practicing organizations. Though the definition of the methodology may be fundamentally similar to the definition of case domain modeling in software engineering, the methodology should be tailored to a

diverse audience of forensics practitioners and law enforcement officers; it should be written such that law enforcement organizations could include it in their standard operating procedure documentation.

Finally, when a case domain modeling methodology is well defined, software tools may be designed and implemented to support the methodology. Such tools should be supportive of the end-to-end practice of computer forensics planning, execution, and documentation. Such tools should also include support for other widely adopted digital forensics methods and practices.

REFERENCES

[1] Alameda County District Attorney's Office, "Computer Searches," 2000; http://www.acgov.org/da/pov/documents/web.htm (current 2004 July 1).

[2] J. H. Alexandar, M. J. Freiling, S. J. Shulman, J. L. Staley, S. Rehfuss, and S. L. Messick, "Knowledge Level Engineering: Ontological Analysis," presented at National Conference on Artificial Intelligence, Philadelphia, Pennsylvania, 1986.

[3] M. Anderson, "Computer Evidence Processing Good Documentation is Essential," 1999; http://www.forensics-intl.com/art10.html (current 2004 July 1).

[4] M. Anderson, "Electronic Fingerprints Computer Evidence Comes of Age," 2000; http://www.forensics-intl.com/art2.html, (current 2004 July 1).

[5] M. Anderson, "Hard Disk Drives -- Bigger is Not Better, Increasing Storage Capacities, the Computer Forensics Dilemma," 2001; http://www.forensics-intl.com/art14.html (current 2004 July 1).

[6] Association of Chief Police Officers (AOPO), "Good Practice Guide for Computer Based Electronic Evidence," 2003; http://www.nhtcu.org/ACPO%20Guide%20v3.0.pdf (current 2004 May 31).

[7] V. Baryamureeba and F. Tushabe, "The Enhanced Digital Investigation Process Model," 2004; http://www.dfrws.org/ (current 2005 January 11).

[8] A. Bequai, "Syndicated Crime and International Terrorism," *Computers and Security*, vol. 21, no. 4, 2002, pp. 333-337.

[9] A. C. Bogen and D. Dampier, "Preparing for Large-Scale Investigations with Case Domain Modeling," presented at Digital Forensics Research Workshop, New Orleans, LA, 2005.

[10] A. C. Bogen and D. Dampier, "Unifying Computer Forensics Modeling Approaches: A Software Engineering Perspective," presented at First International Workshop on Systematic Approaches to Digital Forensic Engineering, Taipei, Taiwan, 2005.

[11] A. C. Bogen and D. A. Dampier, “Knowledge Discovery and Experience Modeling in Computer Forensics Media Analysis,” presented at International Symposium on Information and Communication Technologies, Las Vegas, Nevada, 2004.

[12] A. C. Bogen and D. A. Dampier, “Modeling Evidence Recovery from Digital Media,” *Naval Science and Engineering*, vol. 3, no. 1, January, 2005,

[13] J. Bowen, R. Butler, D. Dill, R. Glass, D. Gries, and A. Hall, “An Invitation to Formal Methods,” *Computer*, vol. 29, no. 4, April, 1996, pp. 16-30.

[14] K. K. Breitman and J. C. S. do Prado Leite, “Ontology as a requirements engineering product,” presented at Requirements Engineering Conference, 2003. Proceedings. 11th IEEE International, 2003.

[15] C. Brewster, K. O’Hara, S. Fuller, Y. Wilks, E. Franconi, M. Musen, J. Ellman, and S. Shum, “Knowledge Representation with Ontologies: The Present and Future,” *IEEE Intelligent Systems*, vol. 19, no. 1, January/February, 2004, pp. 72-81.

[16] C. Brown, “The Art of Keyword Searching,” 2003; http://www.techpathways.com/uploads/TheArtOfKeywordSearching.pdf (current 2004 July 1).

[17] D. Bruschi and M. Monga, “How to Reuse Knowledge About Forensic Investigations,” presented at Digital Forensics Research Workshop, Linthicum, Maryland, 2004.

[18] M. Carney and M. Rogers, “The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction,” *International Journal of Digital Evidence*, vol. 2, no. 4, Spring, 2004,

[19] B. Carrier and E. Spafford, “Getting Physical with the Digital Investigation Process,” *The International Journal of Digital Evidence*, vol. 2, no. 2, Fall, 2003,

[20] B. Chandrasekaran, “AI, knowledge, and the quest for smart systems,” *Expert, IEEE [see also IEEE Intelligent Systems and Their Applications]*, vol. 9, no. 6, 1994, pp. 2-5.

[21] B. Chandrasekaran, J. R. Josephson, and V. R. Benjamins, “What are ontologies, and why do we need them?,” *Intelligent Systems and Their Applications, IEEE [see also IEEE Intelligent Systems]*, vol. 14, no. 1, 1999, pp. 20-26.

[22] E. Christiansen, "Building Computer Forensics Blocks," *Information Forensics Journal*, vol. 1, no. 1, Winter, 2003, pp. 6-7.

[23] S. Cranefield and M. Purvis, "UML as an Ontology Modeling Language," presented at The 16th International Joint Conference on Artificial Intelligence Workshop on Intelligent Information Integration, Stockholm, Sweden, 1999.

[24] S. Easterbrook and R. Covington, "Experiences Using Lightweight Formal Methods for Requirements Modeling," *IEEE Transactions on Software Engineering*, vol. 24, no. 1, January, 1998, pp. 4-13.

[25] European Network of Forensics Science Institutes - Forensic Information Technology Working Group, "Guidelines for the Best Practice in the Forensic Examination of Digital Technology," FITWG-BPM-001, October 27 2003.

[26] J. Feldman, "Effective Data Searches," http://www.forensics.com/pdf/Effective_Data_Searches.pdf (current 2004 July 1).

[27] M. Frappier and H. Habrias, "Software Specification Methods an Overview Using a Case Study." London, England: Springer, 2001.

[28] D. Gasevic, D. Djuric, V. Devedzic, and V. Damjanovic, "From UML to ready-to-use OWL ontologies," presented at Intelligent Systems, 2004. Proceedings. 2004 2nd International IEEE Conference, 2004.

[29] S. Gibson, "The Strange Tale of the Denial of Service Attacks Against GRC.COM," 2002; http://grc.com/dos/grcdos.htm (current 2004 May 31).

[30] R. L. Glass and I. Vessey, "Focusing on the application domain: Everyone agrees it's vital, but who's doing anything about it?," presented at Proceedings of the 1998 31st Annual Hawaii International Conference on System Sciences. Part 3 (of 7), Jan 6-9 1998, Big Island, HI, USA, 1998.

[31] T. Gluzinski and J. Kida, "Managing Your Evidence Problems Associated with Proper Collection Procedures," 2003; http://www.paladintek.com/WhitePaper/Managing_Your_Evidence.pdf (current 2004 July 9).

[32] A. Gomez-Perez, "Some ideas and examples to evaluate ontologies," presented at Artificial Intelligence for Applications, 1995. Proceedings., 11th Conference on, 1995.

[33] S. Gordon and R. Ford, "Cyberterrorism?," *Computers and Security*, vol. 21, no. 7, 2002, pp. 636-647.

[34] T. R. Gruber, "Toward Principles for the Design of Ontologies Used for Knowledge Sharing," in *Formal Ontology in Conceptual Analysis and Knowledge Representation*, N. Guarino and R. Poli, Eds. Deventer, The Netherlands: Kluwer Academic Publishers, 1993.

[35] M. Gruninger and M. S. Fox, "Methodology for the Design and Evaluation of Ontologies," presented at Workshop on Basic Ontological Issues in Knowledge Sharing, International Joint Conference on Artificial Intelligence, Montreal, Canada, 1995.

[36] A. Householder, K. Houle, and C. Dougherty, "Computer Attack Trends Challenge Internet Security," *Computer*, vol. 35, no. 4, April, 2002, pp. 5-7.

[37] N. Iscoe, "Domain Modeling - Evolving Research," presented at Knowledge-Based Software Engineering Conference, 1991. Proceedings., 6th Annual, 1991.

[38] N. Iscoe, G. B. Williams, and G. Arango, "Domain modeling for software engineering," presented at Software Engineering, 1991. Proceedings., 13th International Conference on, 1991.

[39] J. Jurjens, "Using UMLsec and Goal Trees for Secure Systems Development," presented at ACM Symposium on Applied Computing, Madrid, Spain, 2002.

[40] G. Kessler and M. Schirling, "Computer Forensics: Cracking the Books, Cracking the Case," *Information Security*, no., April, 2002, pp. 68-81.

[41] G. Kotonya and I. Sommerville, *Requirements Engineering Process and Techniques*. West Sussex, England: Wiley, 1997.

[42] W. Kruse and J. Heiser, *Computer Forensics*. Boston, Massachusetts: Addison Wesley, 2002.

[43] C. Larman, *Applying UML and Patterns An Introduction to Object-Oriented Analysis and Design*. Upper Saddle River, New Jersey: Prentice Hall, 1998.

[44] J. Lowry, V. Rico, and B. Wood, "Adversary Modeling to Develop Forensic Observables," presented at Digital Forensics Research Workshop, Linthicum, Maryland, 2004.

[45] C. May, "Computer Forensics--the Morse or Clouseau Approach," *Computer Fraud and Security*, vol. 2002, no. 11, November, 2002, pp. 14-17.

[46] J. McCarthy, "Circumscription - A Form of Non-Monotonic Reasoning," *Artificial Intelligence*, vol. 13, no., 1980, pp. 27-39.

[47] J. M. Neighbors, "Software Construction Using Components," in *Computer Science*: University of California at Irvine, 1980.

[48] New Technologies Incorporated, "Computer Evidence Processing Steps," 2004; http://www.forensics-intl.com/evidguid.html (current 2004 July 1).

[49] M. Noblett, M. Pollit, and L. Presley, "Recovering and Examining computer Forensic Evidence," *Forensic Science Communications*, vol. 2, no. 4, October, 2000,

[50] N. Noy and D. McGuiness, "Ontology Development 101: A Guide to Creating Your First Ontology," Stanford Knowledge Systems Laboratory Technical Report KSL-01-05, March 2001.

[51] OntoWeb Consortium: IST-2000-29243, "Deliverable 1.3: A Survey on Ontology Tools," 2002; http://ontoweb.org/About/Deliverables/D13_v1-0.zip (current 2005 September 9).

[52] G. Palmer, "A Road Map for Digital Forensic Research," Utica, New York, technical report DTR-T001-0, 2001.

[53] R. Pressman, *Software Engineering A Practitioner's Approach*, 6th ed. New York, New York: McGraw Hill, 2005.

[54] R. Prieto-Diaz, "Domain analysis: an introduction," *SIGSOFT Softw. Eng. Notes*, vol. 15, no. 2, 1990, pp. 47-54.

[55] R. Prieto-Diaz, "A Faceted Approach to Building Ontologies," presented at Information Reuse and Integration, 2003. IRI 2003. IEEE International Conference on, 2003.

[56] E. Quayle and M. Taylor, "Child Pornography and the Internet: Perpetuating a Cycle of Abuse," *Deviant Behavior: An Interdisciplinary Journal*, vol. 23, no. 4, 2002, pp. 331-361.

[57] M. Reith, C. Carr, and G. Gunsch, "An Examination of Digital Forensics Models," *International Journal of Digital Evidence*, vol. 1, no. 3, Fall, 2002,

[58] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 1 ed. Upper Saddle River, New Jersey: Prentice Hall, 1995.

[59] B. Schneier, "Attack Trees," *Dr. Dobb's Journal*, vol. 24, no. 12, December, 1999, pp. 21-29.

[60] E. Schultz, "The Sorry State of Law Enforcement," *Computers and Security*, vol. 24, no. 4, August, 2002, pp. 290-292.

[61] M. Shannahan, "The Frame Problem," 2004; http://plato.stanford.edu/archives/spr2004/entries/frame-problem/ (current 2005 September 7).

[62] M. Shannon, "Forensic Relative Strength Scoring: ASCII and Entropy Scoring," *International Journal of Digital Evidence*, vol. 2, no. 4, Spring, 2004,

[63] P. Stephenson, "End-to-End Digital Forensics," *Computer Fraud and Security*, vol. 2002, no. 9, 2002, pp. 17-19.

[64] P. Stephenson, "The Forensic Investigation Steps," *Computer Fraud and Security*, vol. 2002, no. 10, October, 2002, pp. 17-19.

[65] P. Stephenson, "Applying DIPL to an Incident Post Mortem," *Computer Fraud and Security*, vol. 2003, no. 8, August, 2003, pp. 17-20.

[66] P. Stephenson, "EEDI: A Structured Method for Digital Investigation," *Information Forensics Journal*, vol. 1, no. 2, Winter, 2003, pp. 1-3.

[67] P. Stephenson, "Using a Formalized Approach to Digital Investigation," *Computer Fraud and Security*, vol. 2003, no. 7, 2003, pp. 17-20.

[68] P. Stephenson, "Using a Formalized Approach to Digital Investigation," in *Getting the Whole Picture, A Series of 12 Columns on End-to-End Digital Investigation (EEDI) Appearing in Elsevier Advanced Technology's, "Computer Fraud and Security" Publication in 2002 and 2003*, vol. 1: International Institute for Digital Forensic Studies & Elsevier Advanced Technology, 2003, pp. 7.

[69] R. Thompson, "Chasing After 'Petty' Computer Crime," *IEEE Potentials*, vol. 18, no. 1, Feb./Mar., 1999, pp. 20-22.

[70] United States Department of Justice Office of Justice Programs, "Electronic Crime Scene Investigation a Guide for First Responders," United States Department of Justice, Washington, DC July 2001.

[71] United States Department of Justice Office of Justice Programs Computer Crime and Intellectual Property Section, *Search and Seizure Manual: Searching and*

Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, 1.0 ed. Washington, DC, 2002.

[72] M. Uschold and M. Gruninger, "Ontologies: Principles, Methods, and Applications," *The Knowledge Engineering Review*, vol. 11, no. 2, 1996, pp. 93-136.

[73] C. Welty, "Ontology Research," *AI Magazine*, vol. 24, no. 3, March, 2003, pp. 11-12.

[74] C. Whitcomb, "An Historical Perspective of Digital Evidence: A Forensic Scientist's View," *International Journal of Digital Evidence*, vol. 1, no. 1, Spring, 2002,

[75] H. Wolfe, "Computer Forensics," *Computers and Security*, vol. 22, no. 1, Jan., 2003, pp. 26-28.

[76] World Wide Web Consortium, "OWL Web Ontology Language Guide," 2004; http://www.w3.org/TR/owl-guide/ (current 2005 September 6).