Support for Computer Forensics Examination Planning with Domain Modeling: A Report of One Experiment Trial

Alfred C. Bogen
United States Army Corps of Engineers, Engineering Research & Development Center
Chris.bogen@erdc.usace.army.mil

David A. Dampier and Jeffrey C. Carver
Mississippi State University Department of Computer Science and Engineering
dampier@cse.msstate.edu,
carver@cse.msstate.edu

Abstract

In any forensic investigation, planning and analysis activities are required in order to determine what digital media will be seized, what types of information will be sought in the examination, and how the examination will be conducted. Existing literature and suggested practices indicate that such planning should occur, but few tools provide support for such activities. Planning an examination may be an essential activity when investigators and technicians are faced with unfamiliar case types or unusually complex, large-scale cases.

This paper presents the results of an empirical study that evaluates two planning methods for computer forensics examination: a methodology that includes domain modeling and a more typical, ad hoc planning approach. This paper briefly describes the case domain modeling and planning methodology, describes the empirical study, and presents preliminary results of and conclusions drawn from the empirical study.

1. Introduction

Existing modeling approaches in computer forensics each provide a different view of a computer forensics investigation: Digital Investigation Process Language (DIPL) [10] provides a chain-of-events view, attack trees [9] and adversary models [8] offer adversary (or suspect) strategy views, and forensic graphs [6] offer a hypothesis test view. The authors of this article have also contributed to modeling research by suggesting that domain modeling should be used as a method for scoping the relevant information in a computer forensics examination [2-5]. The motivation for such modeling approaches is to increase the level of formalism and rigor in computer forensics practice, represent forensics knowledge, and improve practitioner performance.

Current best practices for computer forensics examination imply that the products of examination planning are keyword lists, checklists, and other documents [1, 11, 12]. Ad hoc methods for producing these documents may be insufficient when investigators and technicians encounter large-scale cases, unusually complex cases, or unfamiliar case types. These products are developed based on assumptions regarding the information domain of the case. The planning method described in this article provides a framework for analyzing this information domain and developing examination plans. This paper also presents the results of an experiment trial on examination planning methods.

Established ontology and domain modeling methods and representations in artificial intelligence and software engineering provide a suitable framework for a forensic case domain modeling methodology and representation. Both communities have produced an abundance of information on 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.

Furthermore, non-formal software engineering domain modeling methods are suitable for modeling computer forensics case domains because:

- Representations such as UML (Unified Modeling Language) and entity relationship diagrams are designed such that a layperson

Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)
0-7695-2755-8/07 $20.00 © 2007 IEEE

customer or software system stakeholder may 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 may 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.

Section 2 briefly describes a forensics case domain modeling preparation method that the authors derived from UML's conceptual modeling component.

2. Examination Planning Method with Domain Modeling

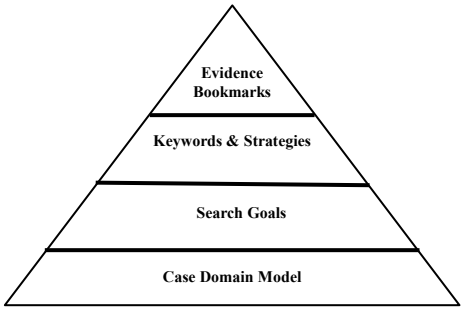
The activities in this planning methodology include:

1. Modeling the information domain of the case,
2. Defining search goals,
3. Allocating search methods to each search goal, and
4. Conducting the examination

Figure 1 illustrates the relationship between the products of the methodology. Starting with the 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 target users of this methodology are teams of forensics analysts, intelligence analysts, forensics technicians, investigators, and attorneys that routinely conduct large-scale computer forensics examinations. Such examinations are typically conducted by federal law enforcement, regulatory, and defense organizations such as the following organizations in the U.S.: the Federal Bureau of Investigation (F.B.I.), the Internal Revenue Service (I.R.S.), and the Central Intelligence Agency (C.I.A.). Such agencies have the abundant personnel and financial resources required to conduct large-scale computer forensics examinations. Members of such teams are likely to hold degrees in accounting, law, or criminal justice while being trained in computer forensics and other duty-specific areas.

Figure1: Relationship of Methodology Products



2.1 Modeling the Case Domain

The case domain represents the known and unknown information that is relevant to the forensics examination. The domain modeling method adopted in this methodology is derived from the UML conceptual modeling method presented by Larman [7]. This method consists of four phases: 1. identify concepts, 2. identify relationships, 3. identify attributes, and 4. instantiate the model.

Though the fundamental techniques of domain modeling are applied in this methodology, the modeler must consider heuristics and guidelines that are specific to the computer forensics domain.

- Tables that list common types of concepts and relationships can be invaluable domain modeling brainstorming tools. Such tables should be tailored to contain computer forensics-specific examples. Table 1 provides an example concept category list.
- Checklists in guides such as the U.S. Department of Justice's *Electronic Crime Scene Investigation: a Guide for First Responders* list evidence items by common case types [11]. Many of these evidence items are suitable concepts to include in a domain model.
- The attributes in a concept 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* and *birth date* is

Table 1: Common Concept Categories

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

sufficient information to distinguish between two distinct instances of *Suspect*.

- Instantiating the model is more important in the computer forensics context than it is in the software development context. Known attribute values will be used to seed the examination and unknown attribute values will be sought by the examination. It is important to flag the known and unknown attributes of each concept.

Figure 2 provides a UML class diagram representation of an email death threat case domain model. Boxes represent concepts with attributes listed inside the boxes. Bold-face attributes (e.g. Network Log Entry) indicate unknown attribute values. Lines drawn between concepts indicate relationships. A line with an arrow indicates a generalization-specialization relationship – e.g. a Faculty Member is a specialized type of University Personnel.

2.2 Defining 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 2 provides an example search goal.

Table 2: Example Search Goal

Goal ID:	1
Goal Statement:	Find file items that reference the victim
Purpose:	Find evidence of victim background research.
Involved Concepts and Attributes	Faculty Member {all attributes}
Known Attribute Values:	Office Number = 101 Office Hours = 1-3pm M W F Class Names = English Composition Full Name = Henry Silver Doe SSN = 123 – 45 – 6789 DOB = 1/1/1965 Phone Numbers = 555-555-1234 Email Addresses = hdoe@univeristy.edu Nicknames = Pizza Dough
Unknown Attribute Values Sought:	None

2.3 Specifying Search Methods

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.

Figure 2: Email Death Threat Case Domain Model

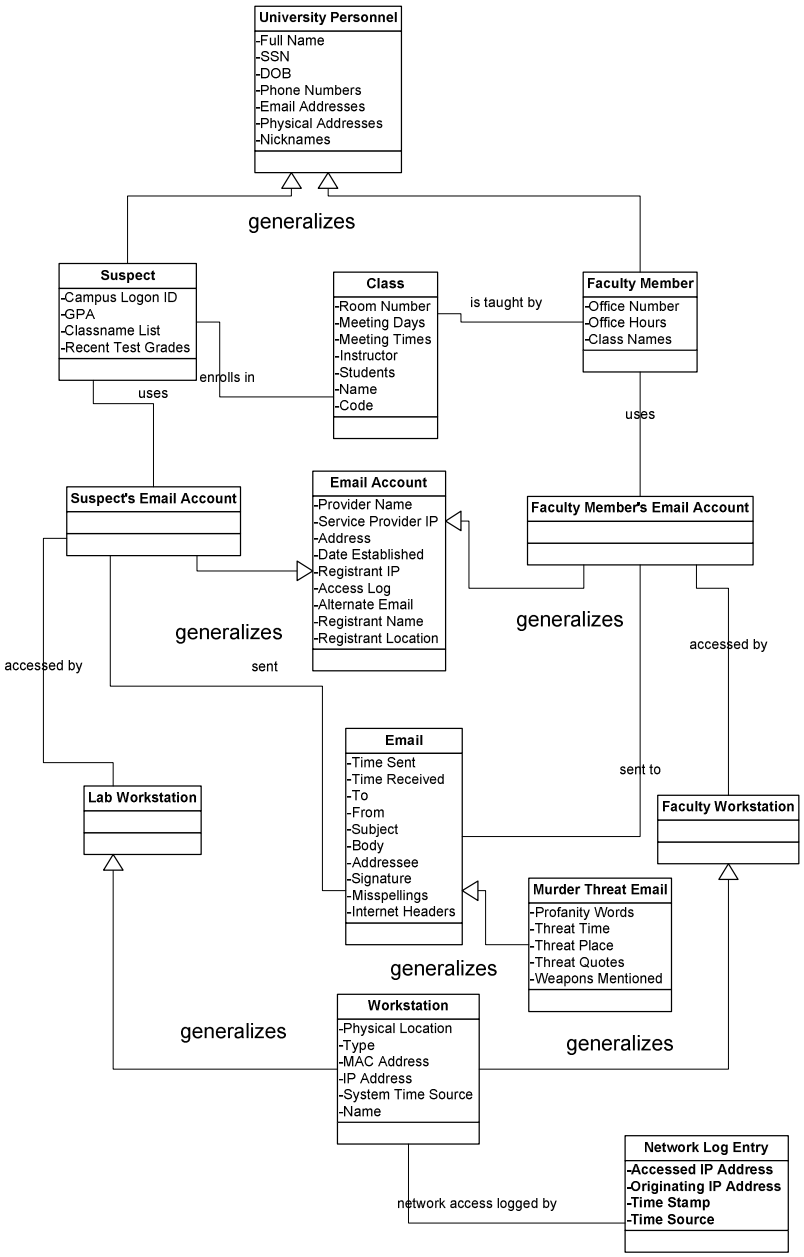


Table 3 presents an example keyword search list for the phone number attribute of the *Faculty Member* concept.

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.

Table 3: Example Keyword List

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

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.

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 4 presents an example table of search strategies.

2.4 Tagging the Evidence

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. When using 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 which 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 4: 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. Experiment Design

This section provides details regarding one of the first-round experiments that were performed to evaluate the effectiveness of the case domain modeling methodology. Section 3.1 describes the experiment design while Section 3.2 presents the results of the experiment.

3.1 Experiment Design and Procedure

The experiment population consisted of an experimental group that used the preparation method described in Section 2 and a control group that used an ad hoc planning approach. The subjects were undergraduate and graduate students in an introduction to computer forensics course. The experimental and control group subjects were balanced according to skill level determined by their overall course grade. Each group was given a 45 minute training session prior to the experiment which consisted of a preparation and examination session.

The control group was instructed to prepare for the examination by performing a sequence of 4 activities:

1. Summarize the Case Facts and Information Relevant to Forensics Activities
2. Classify the Case Type & Relevant Evidence Sources
3. Develop a Keyword Search List
4. State Plans for Other Forensics Activities

The end goal of the control group method is generally the same as 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 were instructed to complete the activities by writing lists, notes, and/or narratives.

During an examination session the subjects used a laptop with the Forensics Toolkit software (FTK) to execute keyword searches and bookmark evidence items. Subjects were instructed to use bookmark naming conventions that revealed whether they found the evidence using a planned keyword search (i.e. a search term developed in the planning session), an un-planned keyword search (i.e. a search term developed in the examination session), or a planned/unplanned non-keyword search. Planned activities were specified during the planning session and unplanned activities were improvised during the examination. The subjects performed these activities on a prepared fictitious case scenario and an evidence hard drive.

The case scenario involved a group of suspects that had allegedly committed bank robbery, burglary, and money laundering activities. The scenario materials included 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 evidence hard drive has a 40 GB advertised capacity and it contains two logical partitions: an 18 GB partition and a 19.2 GB partition (the remaining space is unallocated). A total of 58,459 file items (counts determined by Forensics Toolkit's count of file items) are present on the evidence disk and are distributed as follows:

Documents: 64
Spreadsheets: 0
Databases: 0
Graphics: 1,908
E-mail Messages: 178
Executables: 2
Archives: 785
Folders: 118
Slack/Free Space: 27,853
Other Known Type: 9
Unknown Type: 27,542

The set of evidence consisted of 29 file items. The ratio of evidence to non-evidence files is 0.0496%. The 29 evidence files are distributed as follows:

- 9 document and free space items 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 relevant landmarks
- 9 html files that provided tourist information about the area of the robbed bank, the jewelry store, and the burglarized locations

3.2 Experiment Data Collection

The data collected during the experiment is categorized as time and performance data. The time data represent the amount of time the subjects spent preparing and executing their examination.

The performance data 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 performance data also include evaluations of how the subjects found evidence: planned keyword searches, non-planned keyword searches, and non-keyword search methods.

Qualitative data was also collected using post-experiment surveys, but these data items are omitted from this section and will be briefly discussed in the conclusions section.

Table 5 presents the time data collected during the planning session and the examination session. Time is expressed in terms of minutes. The upper half of the table provides time data points for the control group while the bottom half of the table provides time data points for the Bravo Charlie experimental group – this scheme is also used in the other tables in this section.

Table 6 provides a summary of the amount of evidence located by the subject groups. The amount of evidence is expressed in terms of percentages. The evidence is also categorized into three groups: Emails, Images/Photos, and crime scene area information. The overall or total percent of evidence found is also provided in the right-most column. Table 7 presents data regarding the effectiveness of

the search methods used by the subjects. Values are expressed in terms of the percentage of overall evidence that was successfully located according to

Table 5: Time Data Items

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

the searching method used for locating the data. Searching methods are categorized as planned keyword searches (PK), unplanned keyword searches (UK), all keyword searches (PK+UK = AK), and non-keyword searches (NK). Non-keyword searches include any method other than keyword searching that the subjects used to find evidence.

3.3 Statistical Analysis of Data Points

Statistical tests were performed on the data points to determine whether or not differences in the means between the experimental and control group were statistically significant. In this study, a statistically significant difference is observed within a 90% confidence interval. Student's *t*-test for differences between means was applied when appropriate. When the data points did not meet the normal distribution and uniform variance assumptions a non-parametric Mann-Whitney test for differences between means was applied.

Table 8 presents the results of the statistical *t*-tests and Mann-Whitney tests on the collected data items. When the t-test was used a t-value is provided in the *t* column, and when a Mann-Whitney test was used an N/A is provided in the *t*-column.

Table 6: Evidence Found Data Items

Control Group	% Emails	% Photos	% Crime Area	% Overall
1	11.1	45.45	88.89	48.28
2	100	36.36	22.22	51.72
3	0	0	0	0
4	0	63.64	55.56	41.38
5	0	9.09	22.22	10.34
6	0	45.45	11.11	20.69
7	11.11	45.45	0	20.69
AVG.	17.459	35.06	28.571	27.59
Exp. Group				
1	0	27.27	11.11	13.79
2	77.78	18.18	22.22	37.93
3	0	18.18	0	6.90
4	100	27.27	11.11	44.83
5	100	45.45	22.22	55.17
6	100	45.45	22.22	55.17
7	11.11	72.73	11.11	34.48
AVG.	55.56	36.36	14.28	35.47

Table 7: Search Method Data Items

Control Group	% PK	% UK	% AK	% NK
1	0	0	0	48.28
2	6.90	13.79	20.69	13.79
3	0	0	0	0
4	0	0	0	41.38
5	3.45	3.45	6.9	34.48
6	0	0	0	20.69
7	0	10.34	10.35	10.35
AVG.	1.48	3.94	5.42	24.139
Exp. Group				
1	10.35	0	10.35	3.45
2	0	20.69	20.69	3.45
3	3.45	0	3.45	3.45
4	0	20.69	20.69	6.90
5	0	13.79	13.79	24.14
6	0	10.35	10.35	27.59
7	10.35	24.14	34.48	0
AVG.	3.45	12.81	16.26	9.85

Legend (% Evidence Found by Technique)
PK = Planned Keyword Searches
UK = un-planned Keyword Searches
AK = PK + UK
NK = Evidence Found w/o keyword searches

Table 8: Tests for Statistically Significant Differences on 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}**
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}
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_{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.					
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					
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					

In h_{b1}-h_{b4} the mean units are minutes and all other units are percentages of evidence located.

Based on the results of the statistical analysis, the following statistically significant differences were observed:

- The experimental group spent a statistically significantly greater amount of time in the planning and execution sessions (and hence more overall time)
- The experimental group located a significantly greater amount of evidence than the control group using unplanned and combined keyword searches (planned + unplanned)

4. Discussion and Conclusions

Though the statistical analysis revealed no statistically significant differences between the experimental and control groups with respect to the amount of evidence found, the experimental group

did find more overall evidence than the control group and in two out of the three evidence type categories.

A potential cause for the lack of significant difference in the amount of evidence found is the lack of vivid details in the case information. The effectiveness of the prescribed preparation activities and methods are highly dependent upon 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." Though such circumstances are not ideal for domain modeling, it is encouraging that the experimental group found more, albeit not statistically significant, evidence.

Analysis of the search method data points reveal statistically significant differences in the effectiveness of keyword searching activities between the experimental and control groups. The experimental group found a significantly greater amount of evidence files using un-planned keyword searches and combined keyword searching activities. These significant differences imply that case domain modeling will improve the effectiveness of keyword searching activities. However, the overall amount of evidence found between these groups was not significantly different. 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. This analysis suggests that the case domain modeling approach would be most useful in situations where the examiner must rely more heavily on keyword searching methods than browsing; the control and experimental group subjects found an average of 24.35% and 9.85% (respectively) of the overall evidence using file browsing techniques.

5. Ongoing and Future Work

This work presents the design and analysis of one experiment trial that is part of a larger research effort. Two other experiment trials have been conducted, and the analysis of these experiments is pending at the time of this publication. These two experiment trials will vary from the reported experiment trial in the following ways:

- Each trial offers a different evidence drive with varying distribution of total file items and file item types.
- Each trial has a different scenario. One scenario is an identity theft case and the other is a death threat email case. The level of background details provided to the subjects in each of these scenarios varies.
- In one trial the case domain modeling method was streamlined to exclude diagramming

Future publications will attempt to offer more substantial analysis and conclusions by presenting the results of all experiment trials and the entire research work. Future research will focus on refining the preparation method, elaborating on various ad hoc preparation methods, and experimenting on a larger and more diverse subject population.

6. References

[1] 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).

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

[3] 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.

[4] 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.

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

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

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

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

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

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

[11] 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.

[12] 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.