FORENSIC ANALYSIS OF COMPUTER EVIDENCE

BY

IMANI NKECHINYERE PALMER

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Computer Science
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2018

Urbana, Illinois

Doctoral Committee:

Professor Roy Campbell, Chair
Professor Carl Gunter
Professor Adam Bates
Professor Jay Kesan
Dr. Boris Gelfand

ABSTRACT

Digital forensics is the science involved in the discovery, preservation, and analysis of evidence on digital devices. The end goal of digital forensics is to determine the events that occurred, who performed them, and how were they performed. In order for an investigation to lead to a sound conclusion, it must demonstrate that it is the product of sound scientific methodology.

Digital forensics is inundated with many problems. These problems include an insufficient number of capable examiners, without a standard for certification there is a lack of training for examiners and current tools are unable to deal with the more complex cases, and lack of intelligent automation. This work perpetuates the ability of computer science principles to digital forensics creates a basis of acceptance for digital forensics in both the legal and forensic science community.

This work focuses on three solutions. In terms of education, there is a lack of mandatory standardization, certification, and accreditation. Currently, there is a lack of standards in the interpretation of forensic evidence. The current techniques used by forensic investigators during analysis generally involve ad-hoc methods based on the vague and untested understanding of the system. These forensic techniques are the root of the significant differences in the testimony conducted by digital forensic expert witnesses. Lastly, digital forensic expert witness testimony is under great scrutiny because of the lack of standards in both education and investigative methods.

To remedy this situation, we developed multiple avenues to facilitate more effective investigations. To improve the availability and standardization of education, we developed a multidisciplinary digital forensics curriculum. To improve the standards of forensic evidence interpretation, we developed a methodology based on graph theory to develop a logical view of low-level forensic data. To improve the admissibility of evidence, we developed a methodology to assign a likelihood to the hypotheses determined by forensic investigators. Together, these methods significantly improve the effectiveness of digital forensic investigations. Overall, this work calls the computer science community to join forces with the digital forensics community in order to develop, test and implement established computer science methodology in the application of digital forensics.

Be Brave

Be Strong

Be Proud

And With That You Will Have The Mental Fortitude

To Face The Greatest Adversity

Life Has To Offer

~ Stephen Anthony Palmer

ACKNOWLEDGMENTS

I thank my advisor, Roy H. Campbell, for his encouragement during my years at graduate school. The biggest decision of my life was in choosing an advisor and I chose wisely. I also would like to thank Boris Gelfand for providing mentorship during my summer internships at Los Alamos National Laboratory, as well as, in the final years of my graduate studies. The other members of my Ph.D. committee: Carl Gunter, Adam Bates, and Jay Kesan provided valuable guidance and insight in fostering this work. Acknowledgements are also due to everyone in the Systems Research Group for their support and encouragement and the SURGE Fellowship for funding my graduate studies.
Eureka! ∼Eureka

I thank the many staff members in the Department of Computer Science and the College of Engineering who aided in my progress through the Ph.D. program. Rhonda McElroy, Chandra Chekuri, Mary Beth Kelley, Viveka Kudaligama, Kara Lynn MacGregor, and Kathleen Ann Runck helped me with many issues over the years.
Resistance is futile. ∼Star Trek: The Next Generation

To my mother Felecia Williams-Palmer, my father Stephen Palmer, my brother Stephen Palmer II and the rest of my family thank you for your love and support throughout my life. You were my first cheerleaders in life and in education. Thank you for your continued support and unconditional love.
Without education, you are not going anywhere in this world. ∼Malcolm X

My numerous friends, you have made each day a grand adventure. The constant love and support you each showed me throughout our time have been a joy. I owe you all a great deal of gratitude.
In a dark place we find ourselves, and a little more knowledge lights our way. ∼Star Wars Episode III: Revenge of the Sith

I would like to thank last those scholars who have gone before me who paved way for all my investigations and findings. I truly stand on the shoulder of giants.
Fortune favors the bold. ∼Star Trek: Deep Space Nine

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

Thesis Statement: *The application of computer science principles to digital forensics creates a basis of acceptance for digital forenscs in legal and foresnic science community.*

Forensic science is the term used to refer to a broad range of disciplines that use scientific techniques to analyze physical, chemical, biological, and digital data. It is more commonly known as the application of science to the enforcement of laws within both the criminal and civil justice system. There are many forensic science disciplines including anthropology, criminalistics, engineering sciences, odontology, pathology, psychiatry & behavioral science, questions documents, toxicology, and digital & multimedia sciences.

The role of a forensic scientist is ever-evolving. They are responsible for analyzing the evidence and presenting the results of the analysis in a court of law. The forensic scientist is beholden to the existence of legal standards for the admissibility of forensic tests and expert testimony. The admissibility of a forensic test is *Frye v United States*, which states that the forensic technique in question must have *general acceptance* by the scientific community. Rule 702 of the Federal Rules of Evidence regulates the admissibility of expert testimony in regard to a test or discipline. *Daubert v Merrell Dow Pharmaceutical*, Inc states that the decision about the admissibility of scientific evidence resides with the judge hearing the case.

Forensic science produces valuable evidence and contributes to the successful prosecution, conviction, and exoneration. Advances in serology have demonstrated that certain areas of forensic science have potential to aid law enforcement. However, substantive information and testimony based on faulty practices demonstrates the potential danger of evidence and testimony derived from imperfect testing and analysis. There are certain challenges facing the forensic science community. The shortage in the availability of skilled and well-trained personnel. This stems from a lack of standard education and accreditation process. This dearth in standardized knowledge, leads to the inability to generalize about current practices within the forensic community. This creates significant variations in the interpretation of forensic evidence. Lastly, the need to measure performance and limits in the accuracy of forensic analysis. As a result, the depth, reliability, and overall quality of substantive information arising from the forensic examination of evidence available to the legal system vary substantially across the country [1].

This work aims to solve the challenges in the forensic science subdiscipline digital forensics. In order to increase the number of skilled professionals, the development of a self-contain undergraduate digital forensic curriculum package. Next, in order to generalize current

practices and limit variations in the interpretation of forensic evidence, we present a survey of current digital forensic analysis techniques as well as build an extensible framework. Finally, we implement our framework with multiple case studies and discuss our results. This framework provides a likelihood of events from the provided evidence in order to demonstrate the reliability and quality of the methods.

The rest of this thesis is organized as follows: first, we introduce digital forensics and present a background in forensic science and digital forensics in Chapter 2. Chapter 3 shows the related work of the projects presented in this paper. In Chapter 5 on the Digital Forensic Education Initiative. Chapter 4 present a survey of current analysis techniques in digital forensic analysis. Chapter 6 describes the conceptual design of our analysis methodology. Chapter 8 evaluates the implementation of Sherlock with cause studies and discuss the effectiveness of Sherlock. We further support this thesis with a discussion defined in Chapter 7 and conclude with future work in Chapter 9.

CHAPTER 2: BACKGROUND

Forensic science is the application of science to criminal and civil investigations. The role of the forensic scientist is to collect, to preserve, and to analyze scientific evidence. The field of forensic science is a combination of many disciplines: anthropology, criminalistics, engineering sciences, odontology, and pathology.

2.1 THE DIGITAL FORENSIC PROCESS

The U.S National Institute of Justice (NIJ) in the Electronic Crime Scene Investigation Guide [2] published as workflow meant to guide to digital forensic examiners [3]. Their workflow consists of the following steps:

- Preparation: Prepare the equipment and tools to perform the tasks required during an investigation.
- Collection: Search, for document, and collect or make copies of the physical objects that contain electronic evidence.
- Examination: Make the electronic evidence visible and document contents of the system. Data reduction is performed to identify the evidence.
- Analysis: Analyze the evidence from the Examination phase to determine the significance and probative value.
- Reporting: Create examination notes after each case.

Digital forensics is able to solve crimes committed with computers (e.g. phishing and bank fraud), solve crimes against people where the evidence may reside digitally (e.g. money laundering and child exploitation) and reconstruct the evidence left by cyber attacks. In the beginning of digital forensics, many of the techniques were developed primarily for data recovery. There was not a great need for digital forensics because the evidence on systems could easily be recovered and with limited space on disks, most perpetrators relied on physical media such as printouts. In the late 1990s and early 2000s, digital forensics began to blossom. The widespread use of Microsoft Windows limited the scope of knowledge required of examiners. As well as the failure to implement encryption technology for data made it easy to develop and sell forensic tools. This was the start of digital forensics research and professionalization. In the last decade, progress in the field of digital forensics slowed and

the field was struck by many challenges. Today, examiners find it difficult to obtain data in a forensically sound manner and to process the data to provide results. The challenges only grow as the ubiquity of devices [4].

The increased public awareness of digital evidence says nothing about the state of digital forensics as a science. Indeed, the awareness of the need to collect and analyze digital evidence does not necessarily translate to scientific theory, scientific process and scientifically derived knowledge. The traditional forensic sciences (e.g., serology, toxicology, and ballistics) emerged out of academic research, enabling science to precede forensic science applications, as it should. Digital forensics, however, emerged out of the practitioner community - computer crime investigators and digital forensic tool developers seeking solutions to real-world problems. While these efforts have produced a great amount of factual knowledge and several commonly accepted processes and hardware and software tools, many experts concede that the scientific method did not underlie much of early digital forensic research [5].

2.2 THE HISTORY OF DIGITAL FORENSICS

The practice of digital forensics is relatively new. Digital forensics' history starts in the 1970s with the first noted description of using digital information to investigate a crime in Donn Parker's book, Crime by Computer [6]. As new devices develop and become more common, the practice of digital forensics continually expands. In the 1980s, there is a growth in computer crime leading law enforcement agencies to begin establishing specialized groups, i.e. FBI's Computer Analysis and Response Team [7]. Cliff Stoll writes of his pursuit of a hacker named Markus Hess, The Cuckooś Egg [8], one of the first forensic examinations. In the 1990s, computer forensics begins to join both the academic and forensic science world with the book, A Forensic Methodology for Countering Computer Crime [9]. As the commercialization of computers increased the number of people using computers more and more computer professionals who worked with law enforcement on a case-by-case basis. The 1990s marked the start of the *Golden Age* of digital forensics. Digital forensics became a magic window that could see into the past as well as into the criminal mind, with the dominance of the Windows platform it was easy to build forensic tools. Today digital forensics is facing a crisis as the capabilities of previous generations of digital forensic tools are diminished over the recent advances in digital devices [4].

Digital forensics faces many challenges:

- Growing size of storage devices is frequently insufficient time to create a forensic image

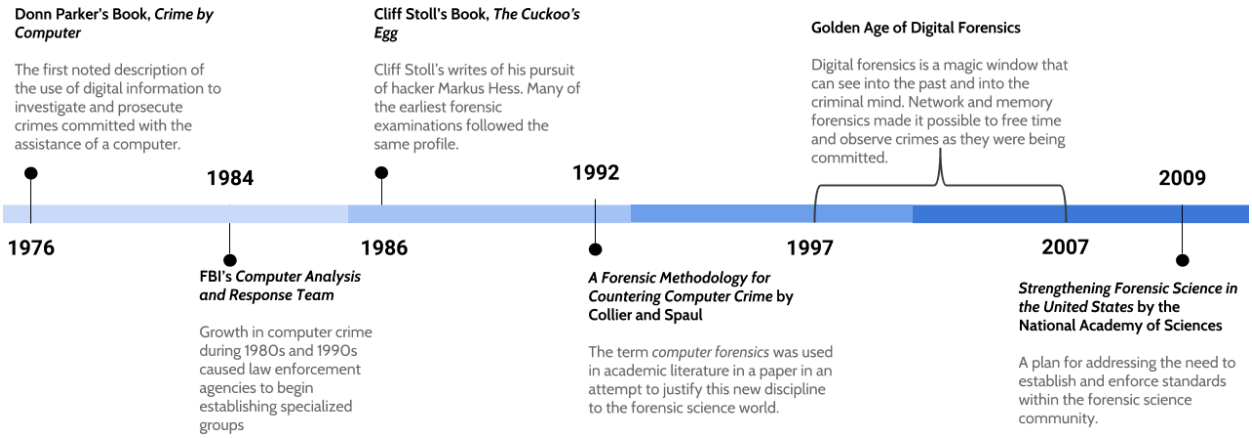

Figure 2.1: A graphical portrayal of the history of digital forensics.

- Increasing prevalence of embedded flash storage & the proliferation of hardware interfaces means storage devices can no longer be readily removed or imaged
- Proliferation of operating systems and file formats is dramatically increasing the requirements and complexity of data exploitation tools and the cost of tool development
- Cases require the analysis of multiple devices followed by the correlation of the found evidence
- Pervasive encryptions means that data frequently cannot be processed
- Use of the cloud for remote processing and storage, and to split a single data structure into elements, means that frequently data or code cannot be found
- Malware not written to persistent storage necessitates the need for expensive RAM forensics
- Legal challenges increasingly limit the scope of forensic investigations

2.3 DIGITAL FORENSICS AND SCIENTIFIC RIGOR

Digital forensics is an established field of forensic science, however, there is no formal theory on how to conduct an investigation. A digital forensic investigation is based on the abilities of its practitioner. Many believe that digital forensics does not require theory. Yet, many physical investigations rely on scientific rigor [10]. For example, DNA analysis is instrumental in forensic investigations. DNA evidence identifies matching DNA of an

individual or potential perpetrator with little probability of error. Currently, digital forensics has matured without the identification of scientific standards [11].

Many forensic science disciplines have theories that are published, accepted, and tested. However, digital forensics is directed by the technology investigated and the available tools [10]. The legal system fails to understand the significance of the digital evidence. Digital forensics remains far behind other forensic disciplines [11]. The legal system relies on the scientific method in order to ensure the admissibility of digital evidence in a court of law [12]. The Daubert standard determines the necessary factors for the admissibility of evidence in legal proceedings:

- Judge is the gatekeeper: The task of assuring the scientific expert testimony truly proceeds from scientific knowledge rests on the trial judge
- Relevance and reliability: The trial judge ensures that the expert's testimony is relevant to the task at hand and rests on a reliable foundation
- Scientific methodology: The proponent can demonstrate that it is the product of sound scientific methodology
- Illustrative factors: The process of formulating hypotheses and conducting experiments to prove or falsify the hypothesis is provided by a set of illustrative factors are met

This standard provides a clear and concise judgment on the digital evidence in court cases. In order to allow for the admissibility of digital evidence, we must be able to make well-reason and concrete claims about the accuracy and validity of conclusions presented in court [11].

Computer crime involves either a computer and/or a network [13]. Computer crimes encompass a range of activities. When an individual is the target of a computer crime, the computer is considered as a tool, these crimes include fraud and identity theft, information warfare, phishing scams, spam and the propagation of illegal obscene or offensive content. Computer crimes where the goal the computer is the target, the crimes include computer viruses, denial-of-service attacks, and malware. Cyberwarfare is the battlespace use and targeting of computers and networks in warfare and involves both offensive and defensive operations pertaining to a threat of cyber attacks, espionage, and sabotage. Computer crimes produce digital evidence that can be used to reconstruct events.

Digital evidence is ubiquitous and constantly evolving making it difficult to determine its admissibility. Digital forensics is in need of a deterministic approach to obtain the most judicious conclusions from evidence. To our knowledge, tools that aid in the scientific method

of reasoning about digital evidence are nonexistent. Current digital forensic tools mainly focus on evidence recovery. These tools have limited abilities to further analyze the data that is recovered [14]. There are multiple investigative frameworks, however, none have risen as a standard for the analysis phase. This framework will enable researchers and examiners to apply various reasoning models to their cases. The application of these reasoning methods would be automated in order to avoid discrepancies and provide reproducibility. As digital forensic science advances it is important to be able to rigorously determine conclusions are drawn from the electronic evidence. The ability to determine if these conclusions are drawn in the most judicious manner will also be of critical importance.

2.4 DIGITAL FORENSICS CHALLENGES

Digital forensics is undergoing a great change. This change is stimulated mainly by technological advancement has generated a reliance on digital forensics in legal system [15]. A digital forensic investigation occurs when digital evidence is collected and examined in accordance with the law [10]. Currently, the digital forensic investigative process has four main stages: collection, preservation, analysis, and visualization. Each of these phases must be performed in a judicious manner in order to allow the evidence found from the investigative process to be admissible in court [16]. However, the efficacy of the investigative phases and the extent to which the resultant evidence should be admissible is not clearly defined [11].

Presently, the analysis phase of the digital forensic investigative process is marred by bias and inaccuracy. The analysis phase lacks proper scientific analysis, which has severely impacted the reliability of investigative findings and the credibility of forensic analysts [17]. In order to overcome these obstacles, we must rely on the scientific method. Evidence reasoning is a fundamental part of investigative efficacy; however, the digital forensic process is currently deficient in the scientific rigor necessary to function in this capacity.

The examination of digital evidence requires a vast array knowledge. This knowledge encompasses various types of computers, models, programs, and etc. Analysts have varying educational backgrounds allowing for incompatible assumptions and differing conclusions from the examination of the same evidence. These problems have arisen in numerous court cases across the United States [11].

Starting in the 2000s, digital evidence has increasingly been used in court proceedings. In the case of the State of Connecticut v. Amero, a elementary school substitute teacher was convicted of contributing to the delinquency of minors because a school computer in her class displayed pop-ups from a pornographic website. It was found that the school computer was infected with spyware which contributed to the presentation of the pop-ups.

Julie Amero was able to get the conviction overturned but not before her previous life was in shambles [18].

In 2007, Michael Fiola returned his laptop to his employer. The laptop was passed to his boss after someone noticed Fiola used an exorbitant amount of data in comparison with his co-workers. After an investigation, child pornography was found in a folder that stores images viewed online Fiola was fired and charged with the possession of child pornography. The charges were eventually dropped after Fiola and his family spent thousands of dollars fighting the case. Fiola‘s defense attorney was able to find that the laptop contained a virus that was programmed to visit multiple children pornography websites [19].

More recently, Miller in the United States v. Miller [20], it was held held that even if it is found that malicious software was responsible for downloading or storing illegal content the defendant could still be convicted of knowingly possessing the illegal content. The legal system relied on the examiner and digital evidence in order to achieve these convictions and in many cases, the digital forensic tools were accurately being used however, the conclusions drawn from the evidence were incorrect [11].

2.5 DIGITAL FORENSIC RESEARCH

To date, research questions largely centered on the archaeology of digital artifacts. Digital forensic artifacts are the result of the physical media, operating system, file system and user-level applications. Each impacts what digital evidence is created and left behind. Like archaeologists who seek to understand past human behavior by studying artifacts, digital forensic investigators seek to understand past behavior in the digital realm by studying digital artifacts. Because digital forensic research during the past decade focused on the identification, excavation, and examination of digital artifacts, there is now a relatively solid understanding of what digital artifacts exist, where they exist, why they exist, and how to recover them. To its credit, the digital forensic research community shares this knowledge with other academic disciplines (e.g., computer science, information systems, engineering, and criminal justice) as well as with the practitioner community (law enforcement, private-sector practitioners, and e-discovery specialists) [5].

It is time to shift the focus towards developing methods towards retrieving understanding from these digital artifacts. Much of this work requires the manual skills of the investigator, given the minimal support from tools to allow the examiners to view the objects in the system. Evidence uncovered as part of the analysis phase may require the examiner to go back to the collection phase, and collect evidence, or to the examination phase in order to enumerate types of objects on the forensic target which were not previously examined [21].

There are several techniques that have been proposed to analyze programs to create higher-levels of abstraction. Many of these are designed as tools to assist a developer and are not fully automated. Some analyze the code and include lexical analysis to organize the source code into units and provide links between them. Syntactic analysis can create a parse tree, which allows control flow analysis to be performed to determine the order of instructions within a procedure and the order of procedures within a program. Data flow analysis can also be used to show dependence between instructions and variables or a program dependence graph can be created to show both the control and data flow. A variation of data flow analysis is slicing, which isolates the instructions that have an effect on a given variable.

Research is also exploring potential techniques to improve the analysis phase. The fidelity of the hypotheses formulated and conclusions reached based on the evidence provided from the examination phase. The current state of the Analysis phase is reliant on the ability of examiners to sift through vast amounts of data to determine the significance of each piece. There is a great need to research intelligent search, retrieval, and analytical algorithms to aid this search process. Research in intelligent analytical approaches is relatively scant. Smarter analytical algorithms would clearly reduce information retrieval overhead. They should help investigators get relevant data quickly, reduce the noise investigators must wade through, and help transform data into information and investigative knowledge [5].

In addition, to improving analytical efficiently, intelligent analytical approaches would enhance analytical effectiveness. Research has shown that data mining algorithms can reveal data trends and information otherwise undetectable by human observation and analysis. Indeed, the increased application of artificial intelligence, information science, data mining and information retrieval algorithms to digital forensics will enable investigators to obtain unprecedented investigative knowledge [5].

Many researchers also pursue the use of likelihood ratio to express the subjectivity and uncertainty associated with forensic science evidence. The likelihood ratio (LR) is a statement which conveys the probability of the observations given each of the stated propositions or hypotheses h. For example, the likelihood ratio communicates the probability of obtaining the observed similarities between a fingerprint from a known origin and the fingerprint of questioned origin under the hypothesis that the two samples have the same origin h_1 versus under the hypothesis that they have different origins h_2 [22].

The accused has a constitutional right to have the fact-finder apply a presumption of innocence to his case. The determination of the prior probability of a hypothesis in the face of ignorance of information bearing on the truth of the hypotheses. We can make a tentative assessment of how probable the hypothesis, however, we cannot be sure. A highly contested topic is whether forensic scientists should try to specify prior probabilities. It is suggested

that forensic scientists should assume equal prior probabilities based on the Principle of Indifference [23]. Principle (Principle of Indifference). If there is the unknown reason for predicting of our subject one rather than another of several alternatives, then relatively to such knowledge the assertions of each of these alternatives have an equal probability.

Three concerns arise from the use of subjective probabilities. Human beliefs concerning probabilities are vague, ambiguous, and inaccurate. The impact of this vagueness and ambiguity on the outcome of the probabilistic analysis is not fully understood. Lastly, outcome stemming from the use of subjective probabilities is difficult to explain and validate, which is crucial in legal applications. It is not unreasonable to question subjective probability values, the reasons for variability in such values and its magnitude. To facilitate such questioning by legal professionals, it is helpful to reduce subjective probability values and their variability to under stable propositions that can be validated [24].

The assignment of likelihood to the hypothesis of digital forensic cases is a just first step in the formalization of this field. It is impossible the implications of these likelihoods would have a great impact on the legal system. First, the advantages could impact phases outside analysis. We could test many hypotheses and if none of them rise above the acknowledge 50% this could mean we have not collected enough evidence and would need more evidence in order generate a higher likelihood for a certain set of hypothesis. However, do we state that for the preponderance of the evidence that a hypothesis with greater than 50% likelihood is fit, if not how do we define that number? Is reasonable doubt assumed with anything less than 50%? The application of probabilities to digital forensic analysis can provide great benefit however, there is a need to examine their place in the legal system. This includes how forensic reports would be written, and how to explain a greater knowledge of statistics to a lay jury when the requirement of knowledge for merely the digital evidence is vast.

The contributions of this work include:

1. Implementation and evaluation of a multidisciplinary digital forensic education program

2. An analysis of reasoning techniques to explore digital evidence

3. An extensible software framework for reasoning about digital evidence that conforms to the scientific method and the Daubert Standard

4. An indepth discussion on potential techniques that are able to improve the digital forensic process

CHAPTER 3: RELATED WORKS

Members of the digital forensics community are concerned by the relative absence of digital forensics practitioners training [25, 26, 27, 28]. There is a broad need for higher-education standards and curricula. To address the need for a standardized high-quality digital forensics education program, this project, in conjunction with the National Science Foundation (NSF), is developing and piloting a curriculum package in digital forensics suitable for adoption by other institutions. Research by Woods et al. [29], Ismand and Hamilton [30], Al Amro et al. [31], describe a technical foundation for the development of digital forensics education programs. Their scholarly findings provide a basis for this programs development, detailed below.

3.1 DIGITAL FORENSIC EDUCATION

Research investigators discuss different approaches to introduce digital forensics in higher education. Chi et al. [32] reported on the challenges of teaching computer forensics at Florida A&M University to students without a strong technical background. To supplement the students need for technical knowledge, Chi et al. created preparatory courses for students to bolster their prerequisite knowledge of computer forensics before introducing the more technical components of the field. In contrast, Srinivasan [33] described a course on computer forensics at the University of Louisville available only to computer information systems studets concentrating on information security. Bashir et al. [34] published research findings on a more multidisciplinary approach.

Other research investigations focus on building a curriculum around industry needs and fortifying the employability of their students in fields related to digital forensics. Lius baccalaureate program in digital forensics at Metropolitan State University adopted a practitioners model, aimed to prepare students for their target industries [35]. This approach failed to recruit the necessary qualified faculty for implementing the model. Wassenaar et al. [36] discusses an approach by Cypress College that prepares students for professional certification. The program required instructors that are digital forensics practitioners. The programs credibility relied on instructors abilities to communicate their industry experience. This projects design and development was influenced by challenges to digital forensics education already identified, discussed, and published by Bashir [34], Lang et al. [37], Woods [29], Walls et al. [38], Beebe [5], Kwan et al. [39], Bishop [40], Craiger et al. [41], Nance et al. [42], and Barnett —citebarnett1996computer. Further, this project identified challenges faced by

institutions involved with implementing digital forensics programs. These include: balancing training and education [43, 44], lack of an adequate textbook on digital forensics [35], finding qualified faculty [44, 35], lab setup [44, 35], selecting appropriate prerequisites [32, 35], and absence of widely accepted curriculum standards [45, 46, 47, 48].

3.2 DIGITAL FORENSIC TOOLS

The analysis of digital evidence is performed by evaluating the data to identify digital evidence that supports an existing theory, that which does not support an existing theory, and that which shows tampering. Analyzing every bit of data is a daunting task when confronted with the increasing size of storage systems. In digital forensics, the acquired data is typically at the lowest and most raw format, which is often too difficult for humans to understand. The skills required is great and is not efficient to require every forensic analyst to be able to do so. Currently, we have solved this problem by using tools to translate data through one or more layers of abstraction until it can be understood. For example, to view the contents of a directory from a file system image, the file system structures must be processed so that the appropriate data structures are displayed. The data that represents the directory contents exists the acquired file system image file, but in a format that is too low to identify. The directory is a layer of abstraction in the file system [49].

There are many tools that focus on the abstraction of evidence. Examples of these tools include EnCase [50], SleuthKit [51], Caine [52], Scalpel [53], Forensic Toolkit [54], Registry Recon [55], Libforensics [56], Cellebrite [57], XRY [58], PlainSight [59], P2 Explorer [60], Mandiant Redline [61], Xplico [62], Bulk Extractor [63], Oxygen Forensic Suite [64], The Coroner's Toolkit [65], Windows Scope [66] and Volatility [67]. However, as the growing size and proliferation of devices require not only analysis but a correlation of evidence. This has lead to the development of many tools focused on timeline reconstruction [68].

Zeitline is an open-sourced graphical tool that allows forensic investigators to import various events and then order and classify them into one or more timelines. Events may be grouped into super-events, creating a hierarchy of events [14]. FACE [69] expands on this work by adding automated analysis and correlation of disk images, memory images, network captures, and configuration files, in order to provide a more coherent view of the state of the target system and allowing investigators to quickly understand it. The reliance on time has shown to be a problem. A study that measures and compares the accuracy and effectiveness of various event reconstruction techniques show they have very high false-positive rates, up to 96% [70].

3.3 DIGITAL FORENSIC RESEARCH

A large amount of digital forensics research is being performed at universities and are funded by organizations suchas the National Science Foundation (NSF), the National Institute of Justice (NIJ) and the National Institute of Standards and Technology (NIST). However, there are relatively few cases of academic research being successfully transitioned to end users. The transition of technology from academia to end users is difficult but is essential given the scale of the digital forensics problem [4].

Digital forensics research is focused in a few directions, these directions are scalability, validity, and data abstraction. Most tools are developed and demonstrated on a relatively small data sets and fail when they are scaled up to real-world sizes. Researchers are failing to develop a range of techniques that perform well when running in a data-rich environment [4]. The application of establishing computer science performance paradigms such as distributed processing [71], datamining-based search process [72], file classification to aid analysis [73], self-organizing neural networks [74], evidence storage through network-based architecture and virtualization and threading via graphical processing units (GPUs) [75]. Validity pertains to the ability of research and tools to hold themselves to a level of scientific testing and reproducibility. New detection algorithms should be reported with a measurable error rate. The ability of researchers to move up the abstraction ladder, in order to create a new generation of forensic techniques, tools and procedures to help address the coming digital forensic crisis these areas focus on identity management, visualization, visual analytics, collaboration, and autonomous operation [4]. The digital forensic research community must challenge itself by raising the standards for rigor and relevance of research in digital forensics [5].

More recently, the literature has begun to explore other methods in order to analyze evidence. Self-Organizing Maps (SOM) is a type of artificial neural network which is used to visualize low-dimensional views of high-dimensional data. This visualization reveals interesting patterns from data. These patterns are able to aid in the investigator ‘s decision making. The output of SOM provides excellent visualizations of the evidence. However, input data to SOM requires data to be manually transformed, with a significant amount of human labor overhead [76]. The use of Self-Organizing Maps also hasnt been fully explored in investigator contexts and would need to be further examined.

There is work in automating the process of formulating predictions for hypotheses about specific types of events. A basic example is chkrootkit [77]. This tool formulates predictions for the hypothesis that a system has a rootkit installed. To test this hypothesis, the tool searches for file and system signatures of specific rootkits. It uses incident and system

characteristics and reconstruction to predict what evidence would exist if a rootkit were installed.

The DERBI system test hypotheses about different intrusion scenarios [78]. The system uses *evidence schemas* to describe what evidence may exist if a sequence of intrusion events occurred. For example, access times on certain files or modifications to log files. In the context of the process in this work, the DERBI system uses both system and incident characteristics to formulate and test hypotheses about a system intrusion. The formalization model proposed by Leigland and Krings is similar and it describes the components of a system and the expected evidence that would exist after a specific type of attack [79].

Elsasesser and Tanner developed a system that uses planning to reconstruct events [80]. A computer network is described to the analysis system based on which computers are connected to each other and what trust exists between them. Host configuration is also defined in the analysis system. Next, different attack plans are considered and evaluated to determine if they could have occurred. For example, the software or hardware is tested to ensure that a specific attack could occur. A simulator can also be used from a known state to determine if the events occurred. The logs and evidence from the simulated system are then compared to the logs and evidence from the suspect system. In the context of the process in this work, the Elsaesser and Tanner system requires that the investigator formulate and test the system configuration hypotheses. The system then formulates and test different event hypotheses.

Stallard and Levitt developed a program that formulates consistency-based predictions to test if the redundant information was inconsistent [81]. These would test a hypothesis that events occurred to remove evidence. For example, it could process the lastlog file on a Linux system and determine when each user was logged in. Based on this information, searches were conducted to identify files that were modified by users during times when, according to the log file, they were not logged in. A file modified by a user when he was not supposed to be logged in could be an indication that the lastlog file was modified.

Carney and Rogers used statistical tests to evaluate hypotheses about which program created a file [82]. The motivation for this approach was to determine if a file was downloaded by the user or planted there by an attacker. File creation times and references to the files in question were used as metrics.

To help with general predictions, the Autopsy Forensic Browser tool was modified to make suggestions for additional searches based on evidence that was found [83]. The investigator would identify evidence to the tool and it would make suggestions to search for files in the same directory, with similar temporal data, or similar file names. The goal of these searches was to find files that were related to the evidence, which is a basic form of reconstruction.

For example, searching for other files in the same directory or for files with the same creation time may find files that were installed at the same time.

Spatial outlier analysis has also been used to make predictions for hypotheses about the existence of files whose attributes were modified to hide the file [83]. The theory behind the procedure was that some attributes of a file would be statistically different from the other file attributes in the directory. For example, the times and name could be changed such that they are consistent with other files in the directory, but the starting block could be much larger. Predictions were made based on single and multiple attributes. Predictions were also made to find directories with hidden files.

As the use and complexity of digital devices continues to rise, the field of digital forensics remains in its infancy. The investigative process is currently faced with a variety of problems, ranging from the limited number of skilled practitioners, to the difficulty of interpreting different forms of evidence. Investigators are challenged with leveraging recovered evidence to find a deterministic cause and effect. Without reliable scientific analysis, judgments made by investigators can easily be biased, inaccurate and/or unprovable. Conclusions drawn from digital evidence can vary largely due to differences in their respective forensic systems, models, and terminology. This persistent incompatibility severely impacts the reliability of investigative findings as well as the credibility of the forensic analysts. Evidence reasoning is a fundamental part of investigative efficacy, however, the digital forensic process currently lacks the scientific rigor necessary to function in this capacity.

The standard for the admissibility of evidence stems from the Daubert trilogy, which establishes the requirements of relevancy and reliability [84]. NIST describes the general phases of the forensic process as collection, examination, analysis, and reporting [85]. Formalization is necessary to ensure consistent repeatability of all investigative scenarios. In recent years, literature has addressed the need for formalization of the digital forensic process, but primarily focused on evidence collection and preservation [81]. Ieong [86] highlights the need for an explicit, unambiguous representation of knowledge and observations. While a pedagogical investigative framework exists, there is yet to be a congruous system for digital evidence reasoning within the examination and analysis phases. Currently, digital forensic analysts use a variety of methods to develop conclusions about recovered evidence, yet the results are often marred by conflicting bias or are shrouded in a veil of uncertainty.

There have been numerous proposed reasoning frameworks, typically relying on applied mathematics, statistics & probabilities as well as, logic. However, before we can employ any particular methodology, there is a need to examine, review and explore all options in order to carry out the investigative process with the utmost precision.

CHAPTER 4: A SYSTEMATIC REVIEW ON REASONING ABOUT DIGITAL EVIDENCE

The forensic process relies on the scientific method to scrutinize recovered evidence that either supports or negates an investigative hypothesis. Currently, analysis of digital evidence remains highly subjective to the forensic practitioner. Digital forensics is in need of a deterministic approach to obtain the most judicious conclusions from evidence. The objective of this paper is to examine current methods of digital evidence analysis. It describes the mechanisms for which these processes may be carried out, and discusses the key obstacles presented by each. Lastly, it concludes with suggestions for further improvement of the digital forensic process as a whole.

4.1 DIFFERENTIAL ANALYSIS

Differential analysis is described as a method of data comparison used for reporting differences between two digital objects. Historically, it has been part of computer science for quite some time. Unix 's diff command was implemented in the early 1970 's, and is commonly used for fast comparison of binary and text files [87]. Continued advancements in hashing and metadata have since paved the way for more thorough differential analysis. It is flexible and adaptable to nearly all types of digital objects; Windows Registry hives, binary files, and disk images can all be compared for evidence of modification or tampering [88]. Nonforensic applications include security procedures of operating systems, such as Windows use of file signatures to verify integrity of downloaded driver packages [89].

Modern investigative tools such as EnCase [90], FTK [54] and SleuthKit [91] have incorporated modules for streamlining differential analysis of collected evidence, although each require significant training to become competent with the software features. Garfinkel et al. [87] formalize a model for differential analysis in the context of digital evidence; two collected objects a baseline object and a final object are compared for evidence of modification both before and after events of interest. Ideally, the process will highlight the most significant changes made from baseline A to final B, assuming those transformations resulted from actions taken by the suspect in question. In this context, differential analysis is often used to detect malware, file and registry modifications [87].

While the strategy of differential analysis is fundamentally the same regardless of which system level is being examined, each level possesses a certain degree of noise. In discussing differential analysis, will define noise as information resulting from comparison between baseline and final that is wholly irrelevant to the investigation.

A potential form of noise presents itself as benign modifications made to digital objects resulting from normal operation of a system. For example, an investigator may wish to examine the presence of a suspicious binary on a particular system apart of an enterprise network. The investigator selects a disk image of an identical, unmodified system from the same enterprise network to serve as the baseline for comparison. Differential analysis may reveal that the image of the system in question is incredibly anomalous compared to the baseline. This could potentially lead to the injudicious assumption that the most anomalous system is the most malicious [88], when in reality, it might have only been the result of benign modifications arising from differences in installed software. While files at the kernel level are generally protected from tampering, files in user directories are much more vulnerable to modification.

Although noise is often assumed to be unintentional, it is very possible that it could be inserted on purpose. When dealing with instances of steganography, differential analysis compares objects that are known to be hiding information with those that do not. Fiore [92] describes a framework by which selective redundancy removal can be used to prepare HTML files for carrying out linguistic steganography. Since the information is being hidden through the otherwise normal process of HTML file optimization, differential analysis will only appear to reveal benign occurrences, such as differences in HTML tag styling.

Future research is needed to expand metrics for identifying and accounting for different forms of noise in digital evidence. Mead [93] explains the National Software Reference Librarys effort to create a library of hashes of commercial software packages. Through combining hashing with differential analysis, investigators can drill-down the scope of inquiry by cross-referencing evidence with a database of known hash values. Eliminating evidence matching existing hashes can reduce the amount of noise arising from benign objects that is commonly problematic when dealing with larger systems, and better isolates the few remaining questionable objects. Further improvement of such databases, robust hashing algorithms, and perhaps a formal technique would be of benefit to investigators.

4.2 PROBABILISTIC MODELS

Conventional forensic analysis has long included models of statistical inference to assess the degree of certainty for which hypotheses and corresponding evidence can be causally linked [94]. This casual linkage is expressed by the following: if a cause is responsible for effect, and effect has been observed, then cause must have occurred [95]. For example, researchers know that the probability of two identical DNA fingerprints belonging to two different individuals is close to one in one billion [94]. If holding an item leaves finger-

prints on it, and fingerprints found on the weapon at a murder scene match the suspect 's own, then investigators can conclude there is over 99% certainty that the suspect held that weapon. Because criminal investigations are ultimately abductive, probabilistic techniques have become widely accepted in the forensic reasoning process [39] [95].

4.2.1 Classical Probability

Several recent criminal investigations have seen classical probability used to reason about contradicting scenarios regarding the presence of incriminating digital evidence. Examining two cases originating in Hong Kong, Overill et al. [96] reasoned the likelihood that the respective defendants intentionally downloaded various forms of child pornography versus accidentally downloading it among other benign content. In each case, the amount of child pornography seized was very small compared to the total amount of miscellaneous benign content, and in both instances were found to have been downloaded over a long period of time. In each case, it was determined that the probability of unintentionally downloading a small amount of child pornography is significantly below 10% [96].

While this method can indeed provide a quantitative assessment of the likelihood of guilt, it is limited to investigations where only few characteristics of the evidential traces are known. In both examples above, the defendants pleaded guilty, and thus metadata was disregarded [96]. It was assumed that the incriminating files had been downloaded over long periods of time, but had metadata been collected, the original hypothesis may have changed entirely. An example would be the offending content timestamped to a one-hour browsing period, thus invalidating the original hypothesis of accidental download. The growing importance of preserving metadata creates the need for probabilistic models that can integrate it into reasoning.

4.2.2 Bayesian Networks

In the last decade, Bayesian inference has gained popularity in the scientific community. Unlike frequentist inference that reasons with frequencies of past events, Bayesian inference reasons with *subjective beliefs estimates*, and allows room for new evidence to revise these beliefs [95]. Kwan et al. [39] introduced the idea of reasoning about digital evidence in the form of Bayesian networks: directed acyclic graphs whose leaf nodes represent observed evidence and interior nodes represent unobserved causes. The root node represents the central hypothesis to which all unobserved causes serve as sub-hypotheses. The model uses Bayes 'theorem to determine the conditional probability of evidence E resulting from

hypothesis H:

$$P(E|H) = P(E)P(H|E) \tag{4.1}$$

$P(E)$ is the prior probability of evidence E; $P(H)$ is the prior probability of H when no evidence exists; $P(H|E)$ is the posterior probability such that H has occurred when E is detected.

The construction of a Bayesian model begins with the defining of a root hypothesis. An example would be *The seized computer was used to send this malicious file.* The possible states of the hypothesis *Yes, No, and Uncertain* are assigned equal probabilities. As more evidence is discovered, sub-hypotheses and their corresponding probabilities are added beneath the root hypothesis. The process is repeated until refinement produces a most likely hypothesis.

However, Bayesian networks are dependent on the assignment of prior probabilities to posterior evidence [39]. In scenarios where uncertainty is present, fuzzy logic methodology is incorporated to quantify likelihood as a value between 1 (absolute truth) and 0 (false) [97]. The case study presented in [39] based its prior probabilities on results from questionnaires sent to several law enforcement agencies. Since human-computer interactions are non-deterministic, there is no systematic way to reason posterior evidential probabilities with complete certainty; conditional probabilities inferred from demonstrably normal behavior of one network might differ with those from another. Discrepancies in prior evidential probabilities can significantly impact the overall outcome of the Bayesian network, and thus, there is difficulty in soundly applying this method to digital forensic investigations.

4.2.3 Dempster-Shafer Theory

One of the limiting factors of using Bayesian analysis in security is that it requires the assignment of prior and conditional probabilities for the nodes in the reasoning model. Often times, the numbers are very hard to obtain. For example, how does one compute the prior probability for a particular registry key being modified? As another example, how does one compute the conditional probability of a particular registry key being modified given that the malware did not gain privileged access? Bayesian analysis works very well when the reasoning structure is well known and the probabilities are easy to obtain. In the real world, it is very hard to obtain those numbers and there is a high degree of uncertainty in the obtained evidence.

Dempster-Shafer theory (DST) is a reasoning technique that provides a way to encode

uncertainty more naturally [98]. Contrasting with Bayesian analysis, DST does not require one to provide a prior probability for the hypothesis of interest. DST also does not require the use of conditional probabilities thus addressing the other major limitation of Bayesian analysis techniques. The presence of certain evidence during forensic analysis does not necessarily indicate a malicious activity. For example, a change in registry key could be either due to a malware or by a benign application. There is always a degree of uncertainty in the obtained evidence at any given stage of the forensic analysis process. DST enables one to account for this uncertainty by assigning a number to a special state of the evidence *don 't know*. For example, a sequence of registry key modifications might indicate that a malware of specific family might have been downloaded. Based on empirical evidence, let us assume one believes that with 10% confidence. A probabilistic interpretation would then mean that one would believe that there is a 90% chance that the malware was not downloadedwhich is not intuitive. When using DST one would assign 10% to the hypothesis that the malware was downloaded and 90% to the hypothesis that I am not sure.

One can explain the difference between DST and probability theory using a coin toss example. When tossing a coin with unknown bias probability theory will assign a probability value of 0.5 to both the outcomes Head and Tail. This representation does not capture the inherent uncertainty in the outcome. DST, on the other hand, will assign 0 to the outcomes Head and Tail while assigning a value of 1 to the set Head, Tail. This exactly captures the reasoning process of a human in that when you toss a coin (with unknown bias) the only thing you are sure about the outcome is that it could be either Head or Tail. In general, when calculating the likelihood of a hypothesis DST allows admittance of ignorance on the confidence of evidence. DST provides rules for combining multiple evidences to calculate the overall belief in the hypothesis. The challenge of using DST is analogous to Bayesian analysis, though much better, in that no prior values have to be assigned to evidences.

4.3 EVENT RECONSTRUCTION MODELS

The ability to reconstruct events is of great importance to the digital forensic process. AlKuwari and Wolthusen [99] proposed a general framework to reconstruct missing parts of a target trace. This can be used for various areas of an investigation. This algorithm graphs a multi-modal scenario, determining all of possible routes connecting the gaps of a specific trace. Additional information may be included in the graph and marked appropriately. The broadcast algorithm used to determine all possible routes may require exponential time, suggesting that the search area should be bounded [99].

This approach relies on a specific target and would best be used to determine if an attack

on a system occurred. However, this approach poses problems for the algorithm if a specific target is not identified. Event reconstruction is not unique to digital forensics, and the ability to apply existing techniques could yield effective results.

4.3.1 Finite State Machines

Modern computer systems are often modeled as a series of finite states, graphically presented as a Finite State Machine (FSM). It is expressed as the quintuple $M = (Q, \Sigma, \delta, s^0, F)$, where:

- Q is the finite, non-empty set of machine states
- Σ is the finite, non-empty alphabet of event symbols
- δ: $Q \times \Sigma \leftarrow Q$ is the transition function mapping events between machine states in Q for each event symbol in Σ
- $s^0 \epsilon Q$ is the starting state of the machine
- $F \subseteq Q$ is the set of final machine states
- Nodes represent possible system states

- Arrows represent transitions between states [10] Gladyshev and Patel [100] introduced a formalization of this model into digital forensics. By back-tracing event states, investigators are presented with a reconstruction of events and can thus select the timeline most relevant to the available evidence.

  For finite state machine models to perform accurately comprehensive event reconstruction, investigators must be able to account for all possible system states. Complex events, such as those resulting from advanced persistent threats, are incredibly difficult to analyze. In addition, changing factors such as software updates may affect the resulting machine states. Carrier [10] proposes the development of a central repository for hosting information about machine events. Likening it to existing forensic databases on gun cartridges, an exhaustive, continuously updated library of system events would be of invaluable aide to investigators performing event reconstruction. However, an investigator may wish to explore other characteristics of events, such as the odds of a particular investigative hypothesis, or the real time distributions of reconstructed events. To compute answers to such questions, the formalization of event reconstruction must be extended with additional attributes that describe statistical and real-time properties of the system and incident [100].

4.4 COMBINING PROBABILITY WITH EVENT RECONSTRUCTION

Attack graphs are typically used for intrusion analysis, where each path represents a unique method of intrusion by a malicious actor. It is possible to use attack graph techniques in the event reconstruction process. Attack graphs are directed graphs where nodes represent pre and post conditions of machine events, and directed edges are conditions met between these nodes; the root node represents the singular event of interest to which all other nodes serve as precursors [101].

While attack graphs are helpful in identifying mechanisms of intrusion, their lacking of any probabilistic inference hinders their usefulness in quantitative evidential reasoning. Investigators presented with attack graphs must select the most probable attack scenarios, but there are currently no clear metrics for assessing likelihood. To address this, Xie et al. [102] combined attack graphs with Bayesian networks. By transferring attack graphs into acyclic Bayesian networks, this method utilizes conditional probability tables for nodes with parents, and prior probabilities for nodes without parents.

Like in regular Bayesian networks, this approach relies on the investigator supplying accurate conditional and prior probabilities for each event. Estimating prior probabilities has traditionally relied on feedback from the community in the form of surveys. This becomes incredibly difficult as scale increases; a large attack graph would require that the investigator survey and obtain probability information for every unique event, making analysis costly.

4.5 DISCUSSION

Evidence reasoning models are an important part of the forensic process. Unlike traditional forensic sciences, digital forensics deals almost exclusively with objects of nondeterministic nature; there is great difficulty in analyzing and scrutinizing digital evidence. Fundamental flaws hinder current evidence analysis models in their ability to assess accurately the likelihood of crime occurrence. Furthermore, conclusions based on probabilities complicate explanations in the courtroom, as demonstrated in the legal arguments surrounding Shonubi I-V [103]. These flaws must be identified and understood to avoid the possibility of injudicious assumptions resulting from the forensic process.

Differential analysis of digital evidence becomes difficult when the scope of investigation is widened; unintentional noise in the form of benign modifications may lead to dubious conclusions about system integrity. Furthermore, recent obfuscation techniques have successfully averted detection by traditional methods. Event reconstruction models are limited in their ability to provide investigators with clear attack scenarios, because they rely on the

exhaustive identification of possible machine states; there is yet to be a resource providing such information. Probabilistic reasoning models rely on prior probabilities known to the investigator, which have so far mainly been determined from surveying others in the field. Besides the obvious expenditure of time and effort in conducting such surveys, it is reckless to underestimate the potential for entropy and reason that small samples of observed probabilities hold true for all investigations. It can be concluded that each of these techniques is only applicable to a small niche of forensic scenarios.

The increasing rate of software development places a burden on forensic examiners to keep up with the latest software packages, both commercial and free. Each of the models discussed in this paper lacks a comprehensive database of information to conduct analysis with the highest accuracy. We highlight the need for a community-driven, updated catalogue of file hashes, machine states, and probability metrics for use in forensic analysis. The changing nature of technology and software necessitates that researchers and law enforcement collaborate to ensure the digital forensic process is as reliable as possible.

CHAPTER 5: DIGITAL FORENSIC EDUCATION INITIATIVE

The Information Trust Institute (ITI) at the University of Illinois at Urbana-Champaign is developing an entirely new multidisiplinary undergraduate curriculum focused on digital forensics. A preliminary plan for the introductory course was presented to a workshop of digital forensic experts in May 2013 and received strong approval [34].

To help address the need for qualified digital forensics professionals, we developed an adoptable curriculum. With the goal is to distribute it as a self-contained curriculum package. This includes an instructor handbook, a lab instructor handbook, lecture slides, and question sets. This will be a significant contribution to the digital forensics education community [26]. When complete, the program will consist of an introductory, and advanced course in digital forensics with accompanying hands-on laboratory sessions, and a special topics course. The introductory course is accessible to a wide range of students from many disciplines and valuable as a stand-alone offering. The second course is more technically intensive, but it is intended to be accessible and valuable to students from non-technical disciplines [104].

This DF program is not necessarily a job-track training program intended to prepare students to directly enter the job market as digital forensic examiners and analysts. Instead, it provides a broadly applicable education in the field of digital forensics that will be valuable for students going into many disciplines related to digital forensics, such as law, in addition to forensic analysts. It is expected that these students will receive additional education training specific to their career paths and some on-the-job training specific to their eventual professional roles. At the time of writing, this project developed curriculum for the introductory and advanced course. The pilot courses of both were taught and in the process of curriculum revision for distribution to other institutions [26]. The content includes modules developed collaboratively by faculty experts in multiple fields of computer science, law, psychology, social sciences, and accountancy. The content of this program is modeled on the NSA/DHS CAE Digital FOrensic Working Group proposal for a standardized DF curriculum [105]. The core curriculum development team includes Illinois faculty members Masooda Bashir (an expert on the psychology of cyber-crime); Roy H. Campbell (a computer security expert); Syed Faisal Hasan (a networking expert); Jay P. Kesan (a las professor with expertise in technology law); Anna-Maria Marshall (an expert on the civil and criminal justice systems, from the Department of Sociology); Frank Nekrasz (an expert on fraud invesitgation from the Department of Accountancy in the College of Business); David M. Nicole and William H. Sanders (experts on secure and trustworthy computing

and networking from the Department of Electricial and Computer Engineering); and Jana Sebestik (a K-12 outreach expert from the College of Education).

5.1 METHODOLOGY

The vision and strategy for this standardized Digital Forensics education curriculum proposes that digital forensics would be best suited as a specialization within a technical domain. The curriculum design envisioned a three-course sequence. The hallmarks of the program include a multidisciplinary approach to digital forensics education. Also, domain experts from multiple fields related to digital forensics develop and teach the curriculum. The course work is modular and portable. Also, live evaluation feedback of the curriculum and teaching was part of the entire design for this project from the beginning. The modules are combined to form a coherent narrative and introduce students to the complex and multiple dynamics of digital forensics. The laboratory assignments from the project 's introductory course solely use open source content. Further, the modular course content is designed with the intention of being easily adaptable and integrated at various educational institutions.

Digital Forensics is essentially multidisciplinary encompassing evidence collection, evidence preservation, evidence presentation, forensic preparation [26] the research team for this project is also multidisciplinary and includes computer science, electrical and computer engineering, criminal justice, law, psychology, and educational assessment experts. The proposed curriculum introduces students to various application areas of digital forensics, including topics such as fraud investigation and digital archives, with the aim of demonstrating the breadth of application for diverse knowledge in the field. The sections below will detail the specifics for Digital Forensics 1, and Digital Forensics 2.

To satisfy the multidisciplinary aims of this two-course curriculum sequence, professors and experts in digital forensics and related fields deliver subject-specific course material during lectures. The fields of study mentioned above, including technical and non-technical topics, were carefully chosen as the result of an extensive review of literature that outlined relevant intersecting topics in the expansive field of digital forensics. Experts, who attended the Digital Forensics Research Workshop (DFRWS 2011 2013), confirmed the accuracy of structuring the course to include these specific fields.

5.2 DIGITAL FORENSICS 1

Digital Forensics 1 is an introductory course designed to offer an initial overview of the field to students from a broad range of disciplines. Designing a digital forensics curriculum that is appropriate for a large target audience creates particular problems and challenges. It is difficult for a single class to offer a comprehensive introduction to a field as complex as digital forensics; however, the pilot course covered the major forensics related fields computer, network, and mobile device precisely because its pedagogical strategy focuses on education rather than training.

The introductory course was taught in 2013 and 2014. The classes consisted of two 75-minute lecture sessions and an hour-long laboratory session each week for a 16-week term. To create a multidisciplinary and modular-based curriculum to correspond with the multidisciplinary nature of the field, the project assembled a development team to include domain experts in computer security, computer networks, law, civil and criminal justice, fraud investigation, and psychology. This approach allows the content developers to receive feedback from student interactions and more efficiently revise their materials. Various modules were combined to form a coherent narrative and introduce students to various perspectives of the field.

The learning objectives that guided the curriculum development were that students should understand:

- Common terminology, techniques, and investigative procedures of digital forensics, including the related disciplines of computer forensics, network forensics, and mobile device forensics
- Applications of the scientific method to digital forensics investigation and its importance
- Various types of digital forensics evidence acquired and the limitations of current techniques
- Basic operations of the U.S. justice system and court proceedings
- Areas related to digital forensics, such as data recovery, psychology, cybercrime, and fraud examination

5.3 DIGITAL FORENSICS 2

Digital Forensics 2 (DF2) is an advanced lecture and lab course designed to offer students an in-depth look at particular multidisciplinary topics related to digital forensics. The class consists of two 50-minute lecture sessions and two hour-long laboratory sessions each week

for a 16-week term. The learning objectives that guided the curriculum development were that students:

- Should be familiar with the known barriers and challenges in digital forensics research
- Should be able to use their investigative skills in real world scenarios
- Should be able to contribute research to the digital forensics community

DF2 includes greater focus on technical topics and more rigorous laboratory assignments than the introductory course. It also requires students to complete a research project. Notably, despite recent consumer trends, research continues to neglect the forensics of non-Windows operating systems, file systems, and user applications. The course aims to encourage students to research Linux, Mac, and iOS operating systems as they become increasingly prominent in our daily lives. Students understanding of multiple operating systems contributes to their ability to adapt the digital forensics investigative process for use in different systems.

Another design decision that is important to the curriculum and this advanced course is the inclusion and option for students to learn in a virtual laboratory environment. The program established a virtualized laboratory called ISLET. ISLET allows professors to demonstrate various digital forensics tools and students to complete their laboratory exercises remotely. ISLET is a container-based virtualization system for teaching Linux-based software with minimal participation and configuration effort. The participation barrier is set very low, and students need only a Secure Shell (SSH) client in order to participate [106].

Inspired by the extensive range of open research questions in the field of digital forensics, this curriculum requires students to contribute to solutions rather than only learn about the issues. To achieve this end students chose a topic for a semester-long research project. Students were guided to design manageable and relevant research topics and were provided with a list of research project ideas. Students formed groups and submitted a project proposal. Each proposal was scrutinized to establish feasibility and likelihood of contributing to digital forensics research and/or education community. The midterm progress report indicates whether students are on-track for the semester. Significantly, the report reveals any particular challenges experienced by the students at that point in the semester. This offers an opportunity for instructors to help students develop strategies for addressing challenges as they continue working on their projects. Near the end of the semester, students present their research projects in the form of oral presentations to their peers and instructors. Ultimately, they submit final project reports.

5.4 EVALUATION METHODOLOGIES

The construction, modifications, and updates to the curriculum are based on workshops, surveys, student evaluations and performance. The construction of the initial curriculum vision is based on summaries of a series of workshops (the proceedings are now in press) that included experts in the field of digital forensics. Findings and guidance gathered from these workshops significantly added to the curriculum development process. An external evaluation team was hired to conduct a formal evaluation of the initiative by providing:

1. Ongoing feedback to inform the implementation and delivery of the curriculum
2. Comprehensive assessment of program effectiveness and outcome attainment

Being responsive to the multiple groups of individuals involved with the initiative helps to legitimize a diversity of perspectives and experiences and contribute to a comprehensive understanding of the curriculum being developed. To that end, the evaluation design includes both quantitative and qualitative methods developed in collaboration with the initiatives leadership team.

Three student surveys were developed, which were distributed throughout the academic semester. The initial paper-based survey is administered to registered students during the first week of the course. Its purpose is to gather initial information about enrolled students, including major, technical background, ethnicity, and gender. The second survey is administered mid-course and online after the midterm exam. This survey records how students are experiencing the course. The third survey is an end course survey administered online during the last week of class. Its aim is to gather information about students perspectives, experiences, and suggestions. All surveys include multiple-choice questions whereby students indicate their level of agreement with a statement on a scale from 1 to 5. Surveys also included open-ended items, inviting students to include additional comments about specific aspects of the course.

The evaluation team observed most of the lecture and lab sessions. The purpose of these observations was to assess the delivery of the curriculum content, and students engagement and experience with the course. Information related to the following categories was noted during the observations:

1. Social or interpersonal setting: how groups and individuals were situated
2. Activities: a systematic description of activities and timeframes
3. Content: a description of resources and materials used and discussed
4. Interactions: a description of student-professor verbal and nonverbal interactions

Group or individual interviews were conducted in the middle and at the end of the course to explore students experiences, reactions to, and opinions on the course in detail. Each group or individual interview involved a dialogue between students and one of the evaluators, who prompted conversations about course-related topics. In an effort to maintain student confidentiality and privacy, there were no members of the courses staff or instructors present during the interviews.

5.5 RESULTS, OPPORTUNITIES, CHALLENGES

This project found Digital Forensics to be a complex curriculum to teach in a higher education institution. This curriculum model and course outlines contribute to a stronger basis for a standardized curriculum. The results are based on teaching the first course twice and the second course once and the results are supplemented with evaluations, surveys and exam results. Below is a summary of the projects findings so far, commenting on opportunities to improve the curriculum, and outlining some challenges that remain.

5.5.1 Findings About Students

The program attracted students from various majors, including law, psychology, math, computer engineering, and computer science. Perhaps unsurprisingly, a major problem with designing a curriculum for multiple majors is that there was a wide difference in students expectations. Students with a technical background desired to learn more about technical topics, and typically they failed to understand the importance of non-technical topics. Students with a non-technical background and interest tended to appreciate the course overall; however, they struggled with the technical concepts and assignments of the course. The large number of possible careers includes digital forensics analyst, examiner, practitioner, security specialist, expert witness, security researcher, digital archivist, and fraud investigator added to student expectations. We further display the findings of the students in Figures 5.1, 5.2.

5.5.2 Team Development of a Course

Lacking any individual with the full range of Digital Forensics expertise, the course sequence is team-taught. The project struggled to present a cohesive course and maintain course integrity related to the differing approaches of the team. Multiple professors did achieve the aim to provide students with a broader understanding of the topics presented. However, many students failed to grasp all of the connections. The intention for the final

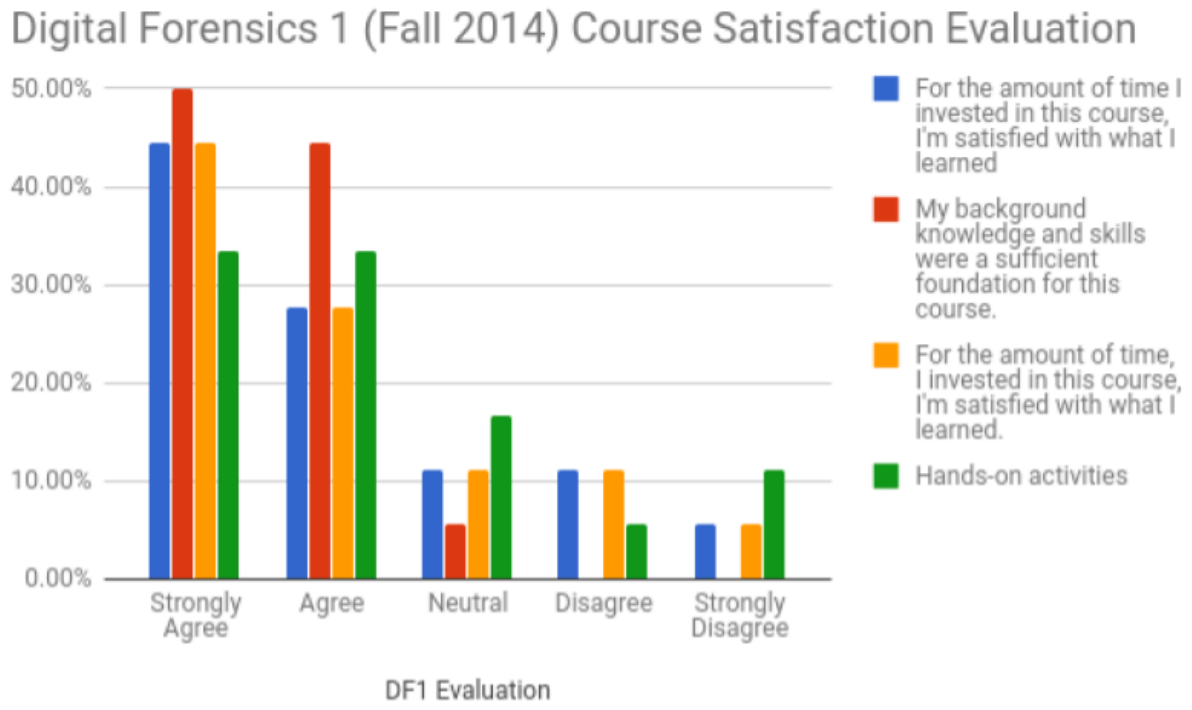

Figure 5.1: Results from the End of the Year Survey for Digital Forensics 1 in Fall 2014

product is that one instructor will be able to teach all the materials. Part of this project involves providing background material as a teaching aid.

5.5.3 Digital Forensics Theory and Practice

Approaching Digital Forensics education using a scientific approach requires evaluation of methods and experimental results. However, scientifically evaluating Digital Forensics methods and reasoning about that evidence using logic is immature in theory and in practice. The project introduced a module in Digital Forensics 2 on *Reasoning about Evidence* with the intention of promoting a more scientific approach to digital forensics research than was offered in the introductory course. The following challenges resulted from this approach. First, the time limitations of a 16-week course limited covering several topics in depth. Second, digital forensics practitioners, educators, and researchers identified that a robust scientific basis for the evaluative methods involved with digital forensics investigations was ongoing research. The Scientific Working Group on Digital Evidence (SWGDE) [48], for instance, have released several documents since 1999 concerning digital forensics standards, best practices, testing, and validation processes, and these were considered in the development of our curriculum.

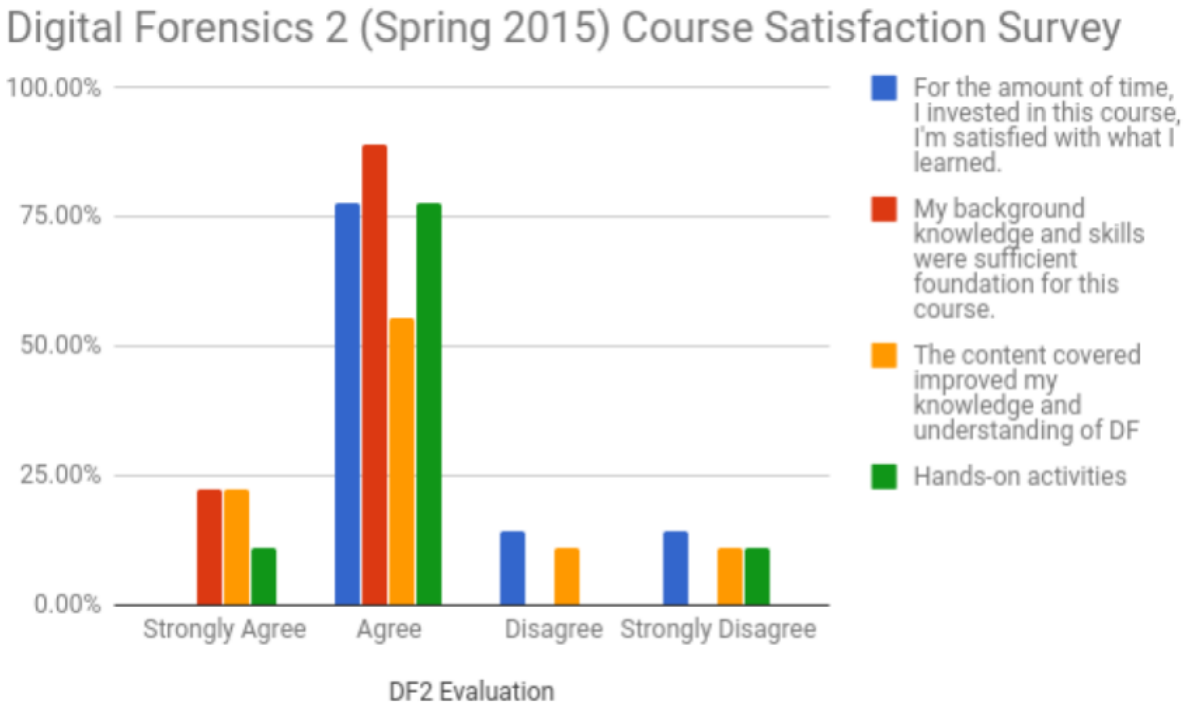

Figure 5.2: Results from the End of the Year Survey for Digital Forensics 2 in Spring 2015

Additionally, in 2001, the U.S. National Institute of Standards and Technology (NIST) [107] began the Computer Forensic Tool Testing (CFTT) Project. It subsequently established and implemented validation test protocols for several digital forensics tools. Moreover, DF2 includes a module entitled tool validation but remains challenging because tool evaluation technologies are unavailable.

The first Digital Forensics Research Workshop (DFRWS 2011) initiated a gathering of over 50 researchers, investigators, and analysts. It aimed to establish a research community that would apply the scientific method in finding focused near-term solutions that were based on practitioner requirements. The community addressed future aims for developing the field of digital forensics. The related curriculum emphasizes the need to bring rigorous scientific methodological approaches to evidence evaluation. One example is *fuzzy logic*, a particular form of reasoning about digital evidence. Fuzzy logic allows elements to be identified as true or false to some degree. A *fuzzy engine* provides a solution to human errors (such as word misspellings) that might skew the results of analysis by selecting an acceptable degree of *fuzziness*. A fuzzy expert system regards a misspelled or mistaken word as input and then finds relationships for it with other similar words.

5.5.4 Project Opportunities

The Digital Forensics 2 advanced course implements a semester-long research project. This provided the students with opportunities to explore different concerns of Digital Forensics. For example, several students decided to develop a case study as their research project that will be available to other institutions to be used in future work and may also be incorporated into the next iteration of the introductory course, Digital Forensics 1. A group interested in social media investigated the amount of shared information by considering application programming interfaces that could potentially be used to extract data about individuals. The project involves the creation of a correlation engine that would be able to demonstrate a connection between application programming interfaces and the ability to extract information about an individual from an online environment. Another group of students introduced digital forensics to high school students. Modeled on their own abbreviated curriculum they also created challenge exercises for the high school students. The goal of the students is to produce outcomes of their project that will contribute to outreach programs that engage students of all ages in digital forensics education. Yet another research group designed a lab for students to examine Mac operating system malware and relevant legal aspects of an investigation.

5.5.5 The Laboratory Environment: Results and Challenges

ISLET is an orchestration tool for education and training built around Docker. It provides custom interactive command-line environments quickly to a user via a shell. It solves a number of the problems associated with virtual machine and shared Unix system training, including the deployment and distribution of large virtual machine files, scalability, mutability of training materials, and account management. Its components include a user interface, an account manager, a container maintenace process, and a deployment configuration. It reduces the administrative burden of creating and distributing training images to a simple process that involves creation of a Docker image and an ISLET configuration file.

Limitations of ISLET include the fact that is it bound to a system supporting Docker, currently a 64-bit GNU/Linux machine, which means that software for other operating systems is not supported. However, it is anticipated that future work will enable support for FreeBSD using ZFS and jails, and other GNU/Linux-based userland container runtimes, to avoid solely relying on Docker. Also, ISLET excels at training in which users are given an interactive command-line shell or interface from which they can gain practical experience with software. However, although it can support X11 applications and provider user-facing

services such as web server training from containers, support is limited, and at this time these features are experimental.

The collaborative virtual lab environment also led to some challenges. It requires students to be knowledgeable about the Linux command-line, which is a challenge for many non-technical students. This will hopefully be overcome in the future by designing a laboratory assignment based on an introduction to the Linux command-line.

5.5.6 Evaluation Methodology Challenges

The evaluation progressed with some challenges. As the aim of the evaluation is to provide ongoing feedback to the initiatives leadership team, a mid-course survey is administered to students during each course. Much of the feedback provided by students is related to the structural organization of the course, which is not feasible to change in the middle of the semester. Another challenge is the variability in student participation. Encouraging students to participate in surveys and interviews was difficult as students participation declines closer to the end of the semester. Different strategies are being explored to maintain and encourage student participation. Another challenge is that the data gathered are representative of the perspectives and experiences of students enrolled at a particular university. As an alpha version of the curriculum is in the process of being distributed, the goal is to also gather data from institutions adopting the curriculum. Gathering a broad range of data will potentially provide support for the initiatives goal of the curriculums acceptance as a national standard.

The course enrolls students from various majors, including law, psychology, math, computer engineering, and computer science. Conducting course and lab session observations yielded a significant amount of insight about the curriculum being implemented. First, these observations offered an immediate impression of how the courses are progressing, which informs and further enlightens data gathered from surveys and interviews. For instance, during the evaluation of the introductory course in the fall of 2014, it was observed that students struggled with answering and finishing lab assignments. Students were asked in an open-ended question format about the pace and structure of the lab, especially if they were dissatisfied with the lab section. Second, conducting observations allowed for the evaluation team to further understand the curriculum because it was situated within a classroom environment. Observing the curriculums implementation and development progress revealed how it was being structured, delivered and received by students. Third, classroom presence, for the purposes of observation, helped to build rapport between the evaluation team and enrolled students. Conducting observations is time consuming, but it is an important method as it helps to situate the program overall.

This proposed project offers a standardized multidisciplinary curriculum model for digital forensics education. It is being made available to institutions for adoption. This project transformed the multidisciplinary undergraduate education at a Midwest university in the United States by institutionalizing this program and the collaborations upon which it is built. In accordance with the multidisciplinary nature of the field of digital forensics, the curriculum development team included domain experts in computer security, computer networks, law, civil and criminal justice, fraud investigation, and psychology. The modular approach to curriculum development is organized by a three-course digital forensics education sequence, and the modules are combined to form a coherent narrative, thus exposing students to multiple perspectives on digital forensics. The curriculum package provides a strong theoretical foundation for the techniques learned by the students as well as an array of studies in fields related to digital forensics. Hopefully this paper will initiate a conversation with the international community, note that standards need to continue to be developed for digital forensics curriculum, and recognize the multidisciplinary need for this field of study. This project, curriculum, and course outline are available on the website `http://publish.illinois.edu/digital-forensics/` and a content package containing all of these materials have been to the schools listed in Table 5.1.

Wilmington University	Bellevue University
Mount Hood Community College	Air Force Institute of Technology
Excelsing College	San Bernardino Valley College
University of South Alabama	University of Houston at Clear Lake
National Security Agency (NSA)	Jackson State Community College
Liberty University	Radford University
Saint Martin's University	Fairleigh Dickinson University
University of Maryland University College	Eastern Washington University
Ivy Tech Community College	Mery College
Tulse Technology Center	Fordham University
California University of Pennsylvania	Iowa State University
Washington University in St. Louis	Daytona State University
Rochester Institute of Technology	Purdue University
Moraine Valley Commmunity College	University of Central Florida
Champlain Community College	University of Central Oklahoma
Oregon State University	University of Nebraska at Omaha
Florida Institute of Technology	Ivy Tech Community College of Indiana
University of Kansas	University of Texas at San Antonio
Marshall University	Roane State Community College
Delta College	

Table 5.1: The different community colleges, colleges & universities in use of the digital forensics curriculum.

CHAPTER 6: THE SCIENTIFIC METHOD AND THE DIGITAL FORENSIC PROCESS

There is great difficulty in analyzing digital evidence, this is only further complicated by failures in the investigative mindset. Failures in the criminal investigative process can lead to unsolved crimes, unsuccessful prosecutions, unpunished offenders, and wrongful convictions[108]. There are common failures that lead to errors in the reasoning process. We will identify key areas of potential error in the digital forensic process.

6.1 THE FORENSIC PROCESS MODEL

Computer forensic methodologies consist of these main components, also known as the three As [109].

- Acquisition: The evidence while ensuring that the integrity is preserved
- Authentication: The validity of the extracted data, which involves making sure that it is as valid as the original
- Analysis: The data while keeping its integrity

There are many process models that combine the three As [110] including the Forensics Process Model [2], the Abstract Digital Forensics Model [111] and the Integrated Digital Investigation Model [112].

6.2 INVESTIGATIVE FAILURES

Individuals view the world differently and these differences a creates mindsets. These mindsets are quick to form and hard to change. These mindsets are dangerous in the generating of a hypothesis. A hypothesis is generated based on mindset and not entirely on the evidence. This bias can lead to serious investigative failures. Tunnel vision develops from a narrow focus. Tunnel vision results in the elimination of hypothesis without thorough vetting. Tunnel version can allow to go down a mistaken course. People estimate the likelihood of an event by recalling a comparable incident and assuming the likelihood of the two are similar. This heuristic is partly prompted by the urge to categorize everything. The similarity in one aspect, however, does not imply similarity in others [108].

Perceptions of cause and effect are susceptible to several mental biases. Crime linkage could be undermined if an investigator fails to differentiate internal (psychological) from external (situation) causes of behavior when examining offender modus operandi. The identity

fallacy holds that big events must have big causes. Illusory correlations can prove misleading on several levels. Events may appear correlated when, in fact, they are not. And, even, if they are connected, correlation does not always equal causation. The relationship may be spurious or caused by an intervening event. The relationship may be spurious or caused by an intervening event. Confirmation bias constitutes a type of selective thinking whereby individuals notice or search for evidence that confirms their theory while ignoring or refusing to look for contradicting information. Efforts to only verify and not falsify a hypothesis often fail. After all, a single item of refuting data (e.g., DNA exclusion) can outweigh a mass of evidence against a suspect. The components of confirmation bias include failure to seek evidence (e.g., a suspect's alibi) that would disprove the theory, failure to use such information if found, failure to consider alternative hypotheses, and failure to evaluate evidence diagnostically. Investigators often fail to account for the absence of evidence, something that can prove quite important under certain circumstances [108].

We hope to limit digital forensic investigative failures through the quantification of the reasoning process. Reasoning begins with a hypothesis whose validity needs to be established. The task then is to quantify the uncertainty in the hypothesis ascribed to corroborate and collaborate multiple events that are relevant to the investigation. Give a list of hypotheses sorted by confidence and annotated by digital evidential support for each hypothesis, it would be very easy for a human analyst to decide which hypotheses deserve further investigation. The key question then is how to calculate a hypothesis' likelihood of being true based on both the reasoning structure from which it is derived and the evidence that supports it. There have been few attempts to achieve this goal specifically.

There exist fundamental flaws that currently hinder the development and establishment of evidence analysis models. These flaws must be identified and understood to avoid the possibility of injudicious assumptions resulting from the forensic process [17].

In graph theory, the degree of a vertex in a graph is the number of connections it has to other vertices. The degree distribution is the probability distribution of the known degrees over the entire graph. Centrality is an indicator of the most important vertices within a graph. The concept of centrality aims to quantify the influence of a vertex in a graph. We also rely on link analysis to aid in the examination process. Link analysis is a data analysis technique used to evaluate relationships between vertices. Relationships may be identified among various types of vertices, including organizations, people, and transaction. Link analysis has been used for investigation of criminal activity, computer security analysis, search engine optimization, market research, medical research, and art.

Previous digital forensic methods fail to find information that is anomalous or even slightly altered [4]. Graph theory is able to determine possible correlations among the evidence. This

is achieved through analysis of the graphs. As we analyze the graph, we are able to interpret more from the evidence.

6.3 SCIENTIFIC METHOD

The scientific method is used as a process to formulate and test hypotheses. The general process has four phases.

- Observation: information and resources relevant to the investigation are collected and observed.
- Hypothesis formulation: based on the observations, hypotheses are formulated about the system. Different levels of hypotheses will be formulated over the course of the investigation.
- Evaluate Hypotheses: To support or refute a hypothesis, predictions about what evidence will exist are made.
- Report Results: Based on the evidence predictions, tests and searches are conducted.

These phases can be see in Figure 6.1.

6.3.1 Observe Evidence

In the observation phase, an investigator, or program, makes observations about states and events for the purpose of formulating a hypothesis. Sources of observations include data defined in the inferred history and output from analysis tool. Some examples are given here: The list of running processes is observed using the ps tool The list of files in a directory is observed using a specialized investigation tool The contents of an e-mail are observed in an e-mail client This phase is equivalent to an investigator looking at a physical crime scene. In a digital crime scene, the investigator must rely on hardware and software to observe data [10].

In both the physical and digital world, there are different types of observations. A direct observation occurs when a component is aware of something based on its sense (i.e. it is the observer). An indirect observation occurs when a component is aware of something based on the observations of other components. A component can be software, hardware, or a person and sense for hardware or software include any form of data input [10].

For example, an investigator can directly observe the state of a monitor because he can see it, but he cannot directly observe the digital state of a hard disk sector. When a

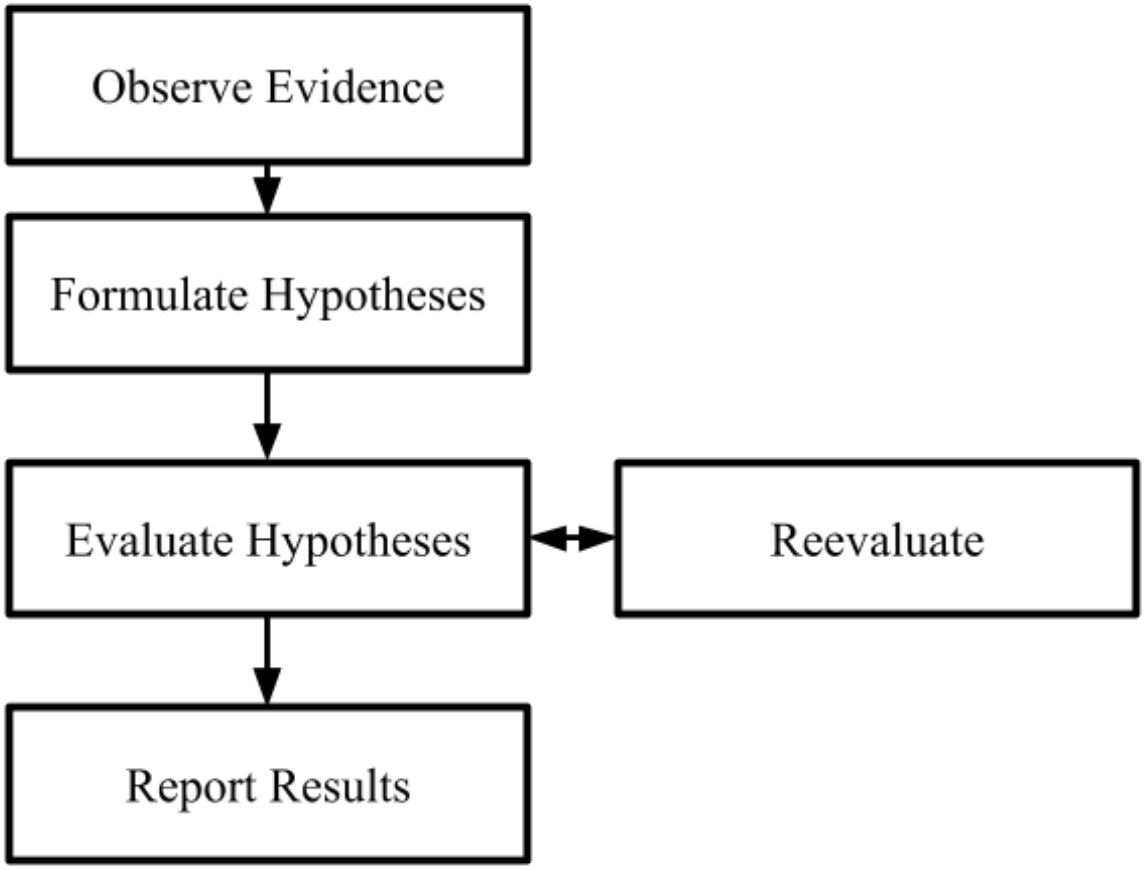

Figure 6.1: The Scientific Method

program displays the contents of a hard disk to the screen, the investigator is making a direct observation of the monitor and an indirect observation of the hard disk sector. An indirect observation would also occur if someone told the investigator about the contents of the sector [10].

In general, the investigator trusts direct observations over indirect observations because he trusts his sense more than other components or people. Trust is a belief in the accuracy and reliability of a component. Because indirectly observed data are not fact, the accuracy of the observed data should be tested when the data are used to formulate hypotheses. The amount of testing will depend on how much trust has been placed in each component. If the software and hardware being used to indirectly observe the state of a hard disk sector have reliably produced accurate data in the past then the investigator may not test each observation. If the software is new and has not been reliably used or if it is from an untrusted system then the investigator will be more likely to test the observation.

In current systems, all important observations that an investigator makes of digital states are indirect because the state of output controllers are not frequently of direct relevance to him. This means that he must evaluate the accuracy of nearly every observation. Consider if he used an automated analysis that formulates and test hypotheses about various states and events. The program stores the data that have been defined in the inferred history and displays the results [10].

A body of evidence can be graphically represented using a graph $G = (V, E)$ where V is a set of vertices E is a set of directed edges. Each component is a vertex and an edge exists from vertex a to vertex b if information flows from a to b. Component b can directly observe component a if a line exists from a to b. Component b can directly observe component a if a line exists from a to b. Component c can indirectly observe component a if a path exists from a to c and c cannot directly observe a [10].

Graph theory is the study of graphs. Graphs are a mathematical representation of a network used to model pairwise relations between objects. A graph G consists of a set of nodes V that are representative of objects, with certain pairs of these nodes connected by edges E. The edges determine the relationship between the nodes. A graph may be either directed or undirected. An undirected graph means there is no distinction between two nodes associated with each edge. A directed graph means that its edges may be directed from one node to another, this relationship is better defined and can represent many ideas such as node A happened before node B, node A is parent of node B and etc. An example of a directed graph is shown in Figure 6.2.

We rely on Hyperlink-Induced Topic Search (HITS) in order to determine which vertices are important to other vertices. We believe that in determining these vertices will allow inferring the high-level actions taken by the user [113].

HITS was originally designed as a method of filtering results from web page search engines in order to identify results most relevant to a user query. The output of this algorithm is two scores for each vertex. The authority value, which estimates the value of the vertex, and its hub value, which estimates the value by the links to other vertices. We focus on the hub value in order to understand the high-level actions occurring in the system. A high-level action is an activity that either the system or user can partake. This includes the opening of a web browser, a system update or using a specific application. These high-level actions typically lead to other more specific actions such as sending an email, creating a file or removing unnecessary memory [113].

PageRank is a link analysis algorithm that computes the ranking of the vertices in the graph based on the structure of the incoming edges. PageRank was first developed as a method for computing a ranking for every web page based on the graph of the web. The

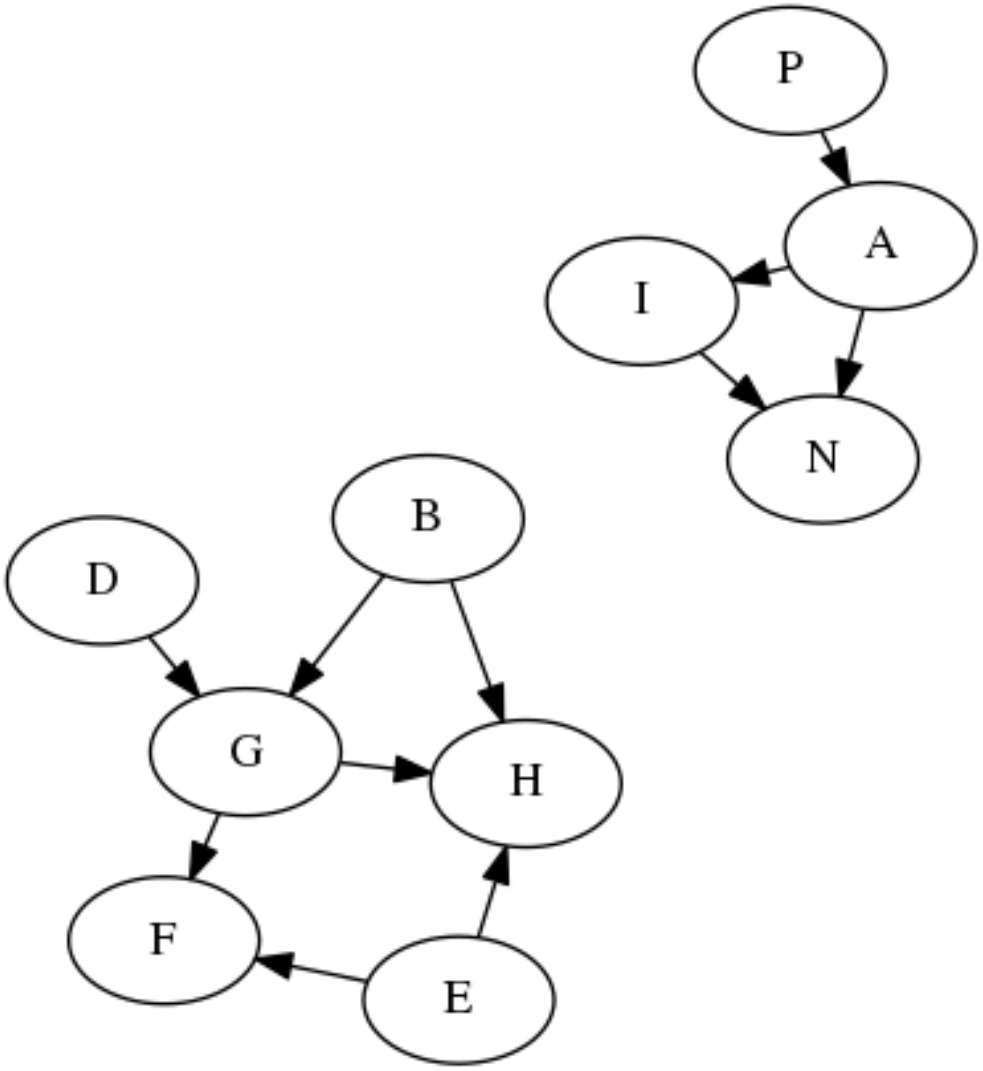

Figure 6.2: A Directed Graph

rank value indicates the importance of a particular page. We employ this concept to our case study. We believe this ranking will identify key pieces of evidence from our memory image that we should further examine [113].

6.4 FORMULATE HYPOTHESES

This phase is where the investigator or program interprets the data observed in the previous phase and formulates hypotheses. In the formal approach, the hypotheses are about the variables in the inferred history, occurrence of events in the system [10].

Hypotheses that define variables in the model must be formulated in a specific order. For

example, before hypotheses are made about the contents of a file, hypotheses about the existence of the file must be formulated and tested [10].

In practice, hypotheses are not always about specific events and specific times. For example, based on the observation of a file and the programs that are installed on the system, a possible hypothesis is that either program X or Y was used to download the file from the Internet. The investigator formulated this hypothesis based on knowledge that both programs are capable of downloading files from the Internet, but he has not enumerated all possible events for each program. Another general hypothesis is that the system is behaving strangely because it was compromised. The tests for this hypothesis will require additional hypotheses about specific types of attack events [10].

To be a scientific process, the hypotheses must be capable of being refuted. If a hypothesis is supported and not refuted, then the relevant data are added to the inferred history. If a hypothesis is neither supported or refuted, than an assumption can be made that it is true, but the investigator must be capable of justifying the assumption [10].

If a hypothesis is refuted based on data in the inferred history, then it does not mean that events and states in the hypothesis did not occur. It means only that they did not occur in that inferred history, but that inferred history may not be correct.

In theory, hypotheses could be formulated and tested for the occurrence of every known event at each time and every program on the system could be analyzed to determine which complex events could occur. In practice, that would be impossible and instead hypotheses and predictions are frequently made based on a combination of system and incident characteristics [10].

Complex arguments ought to be separated in small ones. The synthesis is the composition of the partial solutions of the decomposed problem. In the context of forensic investigations solving a problem should be interpreted as *collecting information to prove or disprove the occurrence of an event in the real world*. In other words, in order to be able to draw conclusive assessment about a case, detectives need to find significant tests to evaluate the simplest hypotheses. They have to analyze the scene of the crime in order to find elements that may enable them to estimate their rational belief in hypotheses. In other words, detectives perform tests aimed at collecting data that are relevant (i.e., provide information about discrimination between a hypothesis and its negation) in the assessment of a given hypotheses. We denote mapping between evidence set E_i and hypothesis H as $H \rightarrow E_1, E_2, E_3, ..., E_n$ [113].

Graph traversal is the process of visiting each vertex in a graph. There are multiple algorithms to aid in graph traversal the shortest path problem. The shortest path problem deals with the problem of finding a path between two nodes in a graph such that the sum

of the weights of its constituent edges is minimized [113].

The problem of finding the shortest path between two intersections on a road map (the graph's nodes correspond to intersections and the edges correspond to road segments, each weighted by the length of its road segments). The shortest problem can be defined for graphs whether undirected or directed. We will now evaluate how each of these elements of graph theory can contribute to a digital forensic investigation [113].

System characteristics are properties of hardware and software that make some states events more common for some systems than others. These characteristics allow us to formulate hypotheses based on only the type of software and hardware being investigated. Frequently, these hypotheses are based on the assumption that the hardware and software have not been modified to make them operate differently from similar hardware and software. For example, based on the type of OS, hypotheses about the file system types can be formulated [10].

Incident characteristics are the general properties of a crime or incident and are system independent. These characteristics may allow the investigator to conduct searches for specific types of evidence using only knowledge about the type of incident. Consider an investigation where a computer is suspected of being used to formulated that a web browser was used to download the files. Next, the system characteristics for the web browsers that are installed are used to predict where evidence may exist. Other examples of incident characteristics are keywords and hash databases. The one-way hash of files that are associated with a type of incident can be calculated, saved, and searched for subsequent investigations [10].

6.5 EVALUATE & REEVALUATE HYPOTHESES

Each hypothesis must be tested and that if it identifies evidence that, if it exists, would support or refute a hypothesis [10].

Based on the test results, new predictions may be made and hypotheses may be revised [10].

If the test supports the hypothesis then the investigator, or automated analysis program, can choose to define the relevant functions and sets in the inferred history. He may also choose to conduct more tests and obtain more support before defining the sets and functions [10].

If the test refutes a hypothesis then the data used in the test will dictate what actions the investigator can perform next. If the test relied on data from the inferred history, then the refuted hypothesis cannot be used to define sets and functions in that inferred history. If the data used to refute the hypothesis was defined based on a direct observation, such as

the state of the video card, then the hypothesis that was tested must be revised or no longer considered because it conflicts with a direct observation, which the investigator will likely have a high amount of trust in. If the data used to refute the hypothesis was defined based on another hypothesis, then the investigator can choose to define a new inferred history [10].

If a hypothesis is refuted based on data that is not in the inferred history, then the reliability and accuracy of the test data should also be considered before refuting the hypothesis. For example, if a tool is executed on the system could have a rootkit or other malicious software that will produce incorrect data. The tool may also be faulty and produce incorrect data. The tool may also be faulty and produce inaccurate data [10].

6.6 REPORT RESULTS

In order to complete the scientific method, an investigator must communicate the results. The resulting confidence score from our evaluation will provide as a baseline to present results. The likelihood ratio formulate represents an economic and intuitive way the hypotheses about the probabilistic relations existing among the variables of interest [114].

CHAPTER 7: DISCUSSION

This chapter focuses on applying my model to a hypothetical court case. This hypothetical court case is based on *State of Connecticut v. Julie Amero*. *State of Connecticut v. Julie Amero* exposes the potential impact of digital forensics on an individual's life. Julie Amero was a substitute teacher in a seventh grade classroom on October 19th, 2004. She returned from the hallway when she found two students browsing a hair styling website [18]. Afterwards, the computer browser began continuously opening pop-ups with pornographic content. She was told not to turn off the computer, and was unaware she could have turned off the computer monitor. The students were exposed to the pornography [115]. Amero was convicted on four charges of Risk of Injury to a Child, which carried up to a 40-year sentence [116]. The primary evidence admitted by the court was the forensic duplicate of the hard drive on the computer in question. While the forensic investigator did not use industry standards to duplicate the hard drive, the information was used in the investigation [115]. The evidence showed Internet history of pornographic links that indicated the user deliberately went to those sites [117]. The defense evidence showed that anti-virus definitions were not updated regularly and at the time were at least three months out-of-date. No antispwayre or client firewall was installed and the school's content filter expired [115].

The examination of *State of Connecticut v. Julie Amero* provides insight into how a general lack of understanding of digital evidence can cause an Innocent defendant to be wrongfully convicted. Amero was convicted on four charges of Risk of Injury to a Child. Following delays in sentencing, a new trial was granted when the conviction was overturned on appeal. Years later, Amero plead guilty to disorderly conduct, her teaching license was revoked, and she paid a $100 fine [118].

There is a gap in the legal community's understanding o digital evidence. The failure of providing sufficient education in digital evidence results in serious miscarriages of Justice and disruption of the legal system. The innocent wrongly convicted and incarcerated; those deserving of punishment get away with crimes. Society as whole is better served by increasing the understanding of digital evidence.

This section will serve as a platform for discussion on the usage of the technique in a criminal court system. Where the prosecution and defense will both have an opportunity to use my technique to present to the jury a story of the digital evidence. This section will shine a light on he current problems of the digital forensic process, how the problems affect the legal system, and the potential of the technique to resolve these problems.

7.1 THE CASE STUDY

A substitute teacher returned from the hallway when she found two students browsing the internet. When the teacher began to restart the lesson the computer screen she was projecting to the students began to continuously opening pop-ups with pornographic content. The substitute teacher was arrested on charges of Risk of Injury to a Child. The police called in a digital forensic examiner. The digital forensic examiner is able to obtain a memory image from the computer. The substitute teacher hires his own lawyer and digital forensic expert.

In the initial investigation the police will obtain the school's computer and deliver to their corresponding digital forensic examiner. The digital forensic examiner will obtain a memory image from the school's computer. The digital forensic examiner will apply Sherlock to obtain a conclusion from this evidence.

In the observation of evidence the digital forensic examiner obtains an image shown in Figure 7.1. This figure is overwhelmed with noise. They would find it difficult to further understand what is occurring in this graph. In order to reduce this noise we rely on a method of differential forensic analysis known as node edge coupling. Differential forensic analysis compares any pair of digital artifacts and reports the differences between them. Focusing on the changes allows the examiner to reduce the amount of information that needs to be examined, while simultaneously focusing on the changes that are thought to be the result of a subject's activities. Differential analysis is widely practiced today [87]. The result of the differential analysis is shown in Figure 7.2.

Node ID	**Hub Value**
firefox.exe	0.8090
paint.exe	0.1909
explorer.exe	0.7.1993e-09
23.209.190.81	0.0
202.209.188.81	0.0
202.209.133.81	0.0
103.41.299.18	0.0
192.168.1.255	0.0
54.201.188.11	0.0

Table 7.1: The hub values of figure 7.2.

For further observation, we rely on our two link analysis algorithms. The HITs to determine pieces of evidence that provides us with overall knowledge of what has occurred in the system. Table 7.1 shows the results from the HITs algorithm. We are shown a number of processes that have an integral part to the events in the system. There are three nodes

with hub values paint.exe, firefox.exe and explorer.exe. The paint.exe process provides access to the paint the application. The firefox.exe process represents the Mozilla Firefox web browser and the explorer.exe process provides a graphical user interface used to interact with the windows operating system. The next step is to look at the results from the PageRank algorithm to determine if there are other pieces of evidence to investigate.

The PageRank algorithm leads us to nodes that are an important part of our evidence graph. Showing us key pieces of evidence to investigate for this case. The results are shown in Table 7.2.

Node ID	**PageRank Value**
firefox.exe	0.1725
192.168.1.255	0.1076
103.41.299.18	0.1076
202.209.133.81	0.1076
paint.exe	0.1067
202.209.188.81	0.1067
23.209.190.81	0.1067
54.201.188.11	0.1067
explorer.exe	0.0774

Table 7.2: The page rank values of figure 7.2.

As shown in Table 7.2, firefox.exe is an important node. This makes sense from the evidence provided by the examiner is able to show that a user used Mozilla Firefox to surf the web. The next node 202.209.133.81 is a network connection made by paint.exe. This is interesting as the case report does not report on the usage of the paint application. It is also interesting to note that paint was making multiple network connections. This is abnormal behavior for this application. Next, the examiner begins to formulate possible hypotheses.

The initial hypothesis is if the computer displayed any pornographic pop ups. This hypothesis is also backed up by a set of evidence E.

Hypothesis H_1: Computer displayed pornographic pop ups

Evidence 1 E_1: explorer.exe
Evidence 2 E_2: firefox.exe
Evidence 3 E_3: 23.209.190.81

To note that the DNS resolution for the IP address 23.209.190.81 resolves to a pornographic

webpage. Next in order to evaluate this hypothesis a Bayesian network. The result of the evaluation is

Yes	No	Maybe
0.59	0.05	0.17

Table 7.3: The results of evaluation.

The examiner is presented with a high probability of 59% of the display of popups. This evidence is presented to the defense and another forensic examiner. That is able to examine the evidence for themselves. The defense's digital forensic examiner examines the evidence for himself and is able to see why the initial examiner concluded H_1 from the evidence $E = E_1, E_2, E_3$. However, he observes that the paint application was also making connections to malicious popups. This is abnormal behavior for this application. This examiner determines a different hypothesis from the evidence graph.

Hypothesis H_2: Malware displayed pornographic pop ups

Sub hypothesis H_2^1: User went to a malicious web page
Evidence 1 E_1: explorer.exe
Evidence 2 E_2: firefox.exe
Evidence 3 E_3: 23.209.190.81

Sub hypothesis H_2^2: Drive-by-Download of fake paint application
Evidence 2 E_1: firefox.exe
Evidence 4 E_4: paint.exe
Evidence 5 E_5: 21.524.301.97
Evidence 6 E_6: 103.41.299.18
Evidence 7 E_7: 202.209.18.81

The defense's examiner further corroborates the witness statement of students web surfing. This allows the examiner to add the fact that a user was surfing the web. The defense examiner also decides to look for corroboration that the paint.exe is create by malware. He is able to find and dissect the malware to determine that it creates a paint.exe process to access the malicious sites shown to the children and add this as a fact in the evaluation. The results of the defense's evaluation is shown in Table 7.4.

Yes	No	Maybe
0.77	0.0	0.0

Table 7.4: The results of the evaluation.

The results from the separate evaluations are able to be detailed in front of the jury. The graphical visualizations allow the evidence to exist in a narrative sequence to allow for storytelling to affect comprehension of the evidence [119]. The jury is able to rely on the confidence scores help them make assessments about the data. Previously the statistical reasoning surrounding the evaluations of digital evidence is casual and intuitive, rather than explicit and rigorous. This methods allows for the continual refinement and reexamination of hypotheses. Bayes' Theorem provides a means of updating prior probability estimates in light of new information. Prior probabilities are contained in the prior odds ratio, while the diagnostic or probative value of the new information is capture in the likelihood ratio. The Bayesian approach not only can clarify one's thinking about evidence. From the usage of Bayes' Theorem we can see what information about the evidence is needed, where the absence of data is replaced by assumptions of witnesses or fact finders, and ultimately, what impact the evidence should have on the established preexisting beliefs. The decision-maker has helpful guide posts for updating beliefs, and avoids falling victim to many biases [120]. Without the usage of Bayesian analysis, the digital forensic examiner would be able to testify about why their hypothesis is true and debate with the defense in front of the court. However, it would be duty of jury to determine the validity of the facts, and the validity of the testimony.

Bayes' theorem approach identifies the accuracy of the tests in practice, combining the inherent properties of the test with the imperfections of the humans and the tools performing the tests. That, rather than the theoretical best performance, is what a fact finder needs to know. The results in terms of the likelihood ratio associated with any particular test or series of tests makes it difficult to confidently identify the likelihood of an error. The testimony some analysts give is replete with invisible assumptions and guesswork. These assumptions and guesses must be returned to the law's control. If hard data does not exists, then the expert may not be in a better position to guess than anyone else [120].

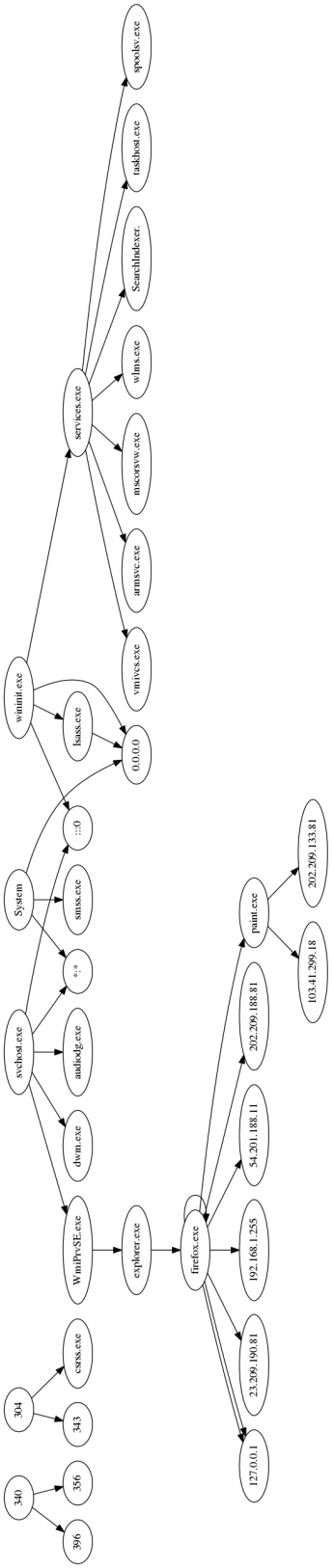

Figure 7.1: The initial graph obtain from the evidence.

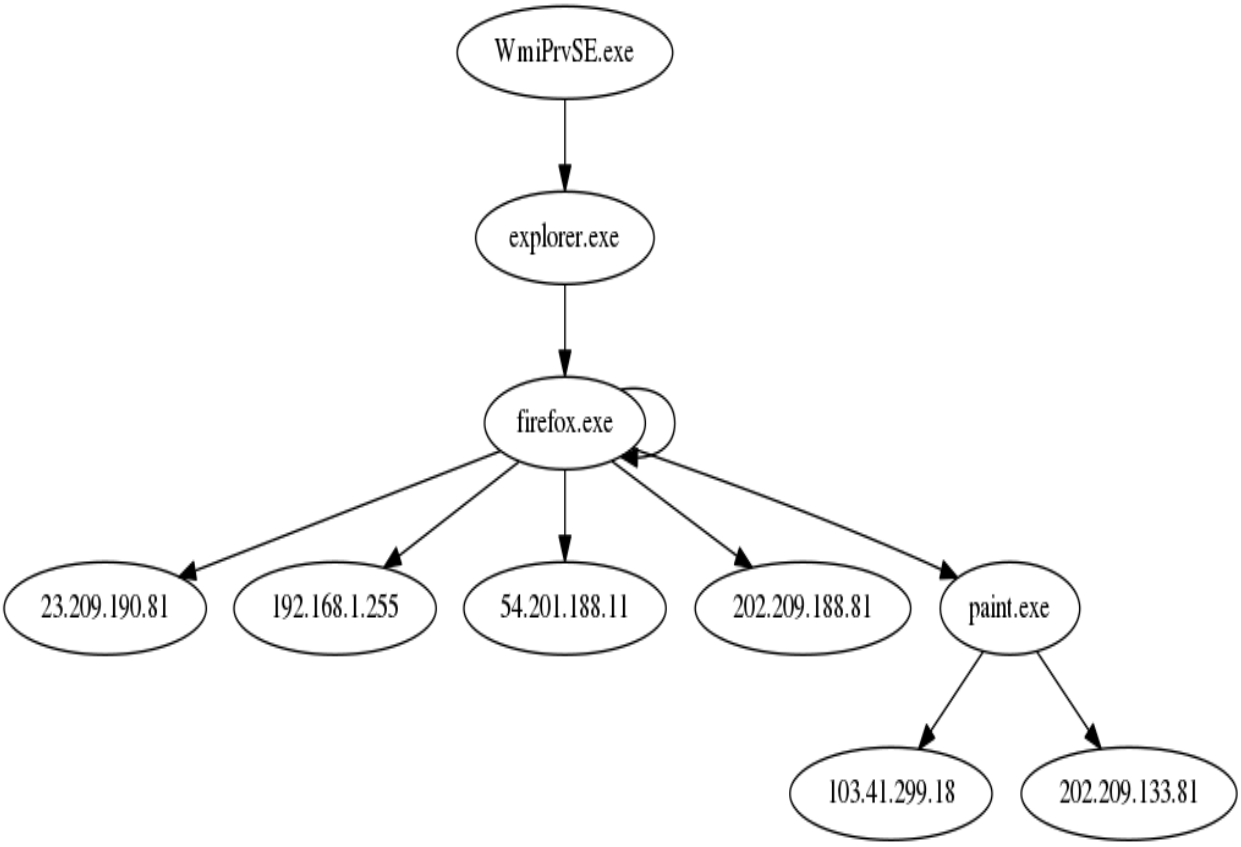

Figure 7.2: The resulting evidence graph after differential analysis.

CHAPTER 8: CASE STUDY EVALUATIONS

We investigate several cases in order to explore the ability of this techniques to facilitate digital forensic investigations. Each of these case studies vary in difficulty in terms of the ability of investigation in order to show both the advantages and disadvantages of this technique. We focus on a specific type of forensic analysis. Memory forensics is the forensic analysis of a computer's memory dump (RAM).

Memory forensics is the branch of digital forensics exploring the contents of a machines volatile memory (typically DRAM and SRAM). There is a wealth of information in volatile memory, ranging from modifications to kernel data structures, to network sockets, to encryption keys which could unlock otherwise useless disks. The analysis of a dump of physical memory can be a daunting process [121]. Comprehensive and unique information about a system's state can be extracted from an image of its main memory. In addition to the current state, it is possible to derive alot of information about a system's past from the memory dump. Among other things there is time stamped information about processes, threads and network activity [122].

In order to analyze the contents of memory, first and foremost, one needs a source of memory dumps. Obviously, we had quite a number of options available to use to capture memory. To test and run our techniques, we created a variety of use case scenarios created by myself as well as digital forensic challenges created by the digital forensics communities. We chose the software VirtualBox [123] to virtualize our system and collect memory dumps. Like most virtualization setups ti allows for a variety of useful functionalities, including snapshots, memory y capture and more. VirtualBox was selected over a handful of other virtualization options due to it compatibility, ease of memory capture and ease of use.

Volatility is an advanced memory forensic framework which analyzes RAM dumps from 32- and 64-bit windows, linux, mac and android systems. Volatility's modular design design allows it to easily support new operating systems and architectures. The extraction techniques are performed completely independent of the system being investigated but offers visibility into the runtime state of the system [67]. This technique focuses on exploring the relationships of the data structures shown in memory.

8.1 CASE STUDY: DROPBOX PROBLEMS

We demonstrate the potential of this analysis with a case study. In our case study, a company has requested forensic analysis on an employees computer. One of its employees

found a PDF file on the company shared Dropbox account. Upon opening the file the employee did not seem to notice anything, however, the IT department has verified that the employee's credentials have been stolen.

We first define the nodes and links of our graph. We are given a memory image from the employees Windows 7 virtual machine. Memory images contain a great deal of volatile evidence. We determine our nodes to be both processes and network connections. The links are exemplified by processes that fork other processes or make network connections. This forms a directed graph as a parent process initializes a child process or network connections.

The first step involved in the scientific method is the observation of the evidence. The analyst must observe the evidence. In order to observe our evidence, in this case, we build our graph. The graph-based representation of our evidence is shown in Figure A.1.

We are inundated with evidence, however, not all of the evidence is important to our case. We rely on differential analysis to remove the noise from Figure A.1. We are able to accomplish this by create a graph based on a clean Window 7 machine. Then, we perform node-edge coupling in order to remove the nodes and edges from the graph that are routine functions in Windows 7 machines, which leaves the user related activities that are important to the case. We are presented with a new evidence graph shown in Figure A.2.

Next, we rely on our two previous link analysis algorithms to make more observations. We use HITs to determine pieces of evidence that provide us with overall knowledge of what has occurred in the system. Table A.1 shows our results from the HITS algorithm. We are shown a number of processes that have integral parts of the routine operating of a Windows 7 operating system. The services.exe correlates to the Services Control Manager, which is responsible for running, ending, and interacting with the system services. The svchost.exe is a system process that hosts multiple Windows services and is essential in the implementation of shared service processes. The wininit.exe is the Windows Initialize is a core system process that aids in the startup of the operating system. The System is a system process that is responsible for the system memory and compressed memory. The lsass.exe generates a users access token, which is used to launch the initial shell. The VboxService.exe is required for the guest services of VirtualBox to work properly. The WmiPrvSE.exe is a component that provides management information and control in an enterprise environment. These processes are established hub operating within the system, they all are important in starting up other processes and connections. We are also able to identify three other hubs firefox.exe, explorer.exe, and AcroRd32.exe. The explorer.exe process provides a graphical interface you use to interact with most of Windows. From here we infer that the user relied on the graphical user interface in order to interact with the computer. The firefox.exe process represents that the Mozilla Firefox web browser available for surfing the web. We are able

to infer that there was an activity involving web surfing activity. Lastly, the AcroRd32.exe process that runs the Adobe Reader, typically to use to view PDF files. We infer that the user opens a PDF file. This is in line with information we received about the case. The next step is we rely on the PageRank algorithm to determine if there are other pieces of evidence we should investigate. TableA.2 shows our results from the PageRank algorithm.

As shown in Table A.2, we receive a ranking of pieces of evidence. Some pieces were all also identified as a hub, explorer.exe, and firefox.exe. We then are shown another address 192.168.1.115. This address is unknown to us and warrants further investigation. When we look at the graph and see that the AcroRd32.exe makes the connection to the unknown address. This is interesting as this is not within the norm for the AcroRd32.exe process. Now that we have made some observation about the evidence. Next, we begin to formulate possible hypotheses.

In order to formulate valid hypotheses, we rely on graph traversal. Graph traversal is the process of visiting each vertex in a graph. In order for a hypothesis to be valid, we rely on a mapping between a set of evidence E, and hypothesis H as $H \rightarrow E_1, E_2, E_3, ..., E_n$. From our case study, we identified an unknown address. This makes us suspicious that the user had a malicious PDF file that made a network connection to another machine. The goal would be then to find a path from explorer.exe to 192.168.1.115. The corresponding path is explorer.exe - AcroRd32.exe - 192.168.1.115. From our prior knowledge of the case, we know that the employee found the PDF on a company shared Dropbox folder. We can see that the employee accesses firefox.exe and we can assume downloaded the PDF. After opening the file with Adobe Reader, we determine a malicious course of action through the direct access to a network connection by Adobe Reader. We have successfully used elements of graph theory to provide a logical view of events from the evidence as well as determine a valid hypothesis. The next step is to evaluate our hypothesis.

Stemming from our case study hypothesis H is the root node of the Bayesian network. The root node does not have a parent node, its prior probabilities are unconditional. To begin with, the probabilities of H are evenly distributed among its three states, i.e., $P(H)$ (0.333, 0.333, 0.333).

Hypothesis H: Employee downloaded a PDF from Dropbox, the PDF made an unwarranted network connection and ran a keylogger.

Evidence 1 E_1: explorer.exe
Evidence 2 E_2: firefox.exe

Evidence 3 E_3: Dropbox
Evidence 4 E_4: AcroRd32.exe
Evidence 5 E_5: 192.168.1.115
Evidence 6 E_6: notepad.exe

H_1: Downloaded PDF from Dropbox: $E_1 \rightarrow E_2 \rightarrow E_3$
H_2: PDF made unwarranted network connection: $E_1 \rightarrow E_4 \rightarrow E_5$
H_3: PDF ran keylogger: $E_1 \rightarrow E_4 \rightarrow E_6$

Items of digital evidence correspond to past digital events (or posterior evidence) that can be used to support or refute the hypothesis H. One of the main challenges in applying a Bayesian network to evaluate evidence is assigning probability values of posterior evidence. This is because the assignments are usually based on subjective personal beliefs. Although the personal beliefs of a digital forensic analyst are assumed to arise from professional knowledge and experience, there are no means to determine whether they truly represent the accepted views of the digital forensic discipline, let alone whether the probability values assigned to posterior evidence are, in fact accurate.

To enhance the reliability and accuracy of the probability assignments for posterior evidence, we attempted to use objective probability assignments obtained through the probability mass function. The probability mass function is a function that gives the probability of a discrete random variable is exactly equal to some value. In the evidentiary context, a higher probability is assigned to pieces of evidence which is better supported by other pieces of evidence. We are able to determine the probability mass function with the degree distribution of our evidence graph in Figure A.2. Table A.3 and Table A.4 shown both the degree distribution and the results of the probabilistic mass function from the evidence chain of our hypothesis.

In forensic cases, it is necessary to account for 0 or 1 facts of the case. This happens when an entire file is found or the investigating the effects of malware on the system. This, as shown above, leads to changes in our results of yes and no and only slightly affects the maybe depending on the importance of the evidence. Now, that we have results, the next to report them. In this case, we can apply 1 to the fact of the keylogger as after further evaluation of the evidence the malware for the keylogger was found. The results of the evaluation are shown in Table A.5.

8.2 CASE STUDY: BANKING TROUBLES

In this case study, from Honeynet Project: Banking Troubles [124]. A company X has contacted an digital examiner to perform forensics work on a recent incident that occurred. One of their employees had received an email from a fellow co-worker that pointed to a PDF file. Upon opening, the employee did not seem to notice anything, however, recently they have had unusual activity in their bank account. Company X was able to obtain a memory image of the employee's virtual machine upon suspected infection. Company X wishes you to analyze the virtual memory and report on any suspected activities found.

The EPROCESS structure is the kernel's representation of a process object. This contains information about both the parent process of each process object. The relationship between a parent process and child process, is that the parent process forks a newly created process known as the child process. The operating system kernel identifies each process by its process identifier. We first define the vertices and edges of our graph. We are given a memory image from a Windows XP SP2 x86 as our sole source of evidence. Memory images contain a great deal of volatile evidence. We determine our vertices to be both processes and network connections. The edges are exemplified by processes that fork other processes or make network connections. This forms a directed graph as a parent process initializes a child process or network connection. We begin by building the a graph focused on the relationships between the parent process and child process. The pictorial representation of the process structure in this memory image provides us with information shown in Figure B.1. We are presented with two subgraphs. Our initial subgraph appears to show routine computer activity as shown in Figure B.3. In Figure B.2 we see a variety of nodes that pertain to our case. To further observe the evidence we rely on HITs in order to determine which vertices are important to other nodes. The results of running this link analysis algorithm will allow inferring the actions taken.

Because we decided that one subgraph was of the most importance to us based on the nodes in that graph we run HITs on that subgraph. explorer.exe has the highest hub values. explorer.exe is the user shell, which is represented as the the Windows taskbar, desktop, and other user interface features. This indicates that a user of this system relied on the graphical user interface. firefox.exe has the second highest hub value. This indicates that the user opened the web browser known as Mozilla Firefox indicating the user intended to access the internet. This information aligns with the case study. As the employee stated they received an email, we can see they relied on web browser to access their email this is shown in Table B.1.

Next, we look at the results of PageRank. The highest ranking value shown in Table B.2

is AcroRd32.exe. AcroRd32.exe is the executable file that runs the Adobe Reader, a tool to view, print and share files in portable document format (PDF). This also aligns with the information given about the case as the co-worked downloaded a PDF.

Now, that we have observed the evidence, I begin to formulate a hypothesis about what has occurred. It appears that the employee downloaded a PDF base.

Hypothesis H: X accessed firefox.exe and downloaded a PDF which made a connection to 212.150.164.20

E_1: explorer
E_2: firefox.exe
E_3: AcroRd32.exe
E_4: 212.150.164.20

H_1: X access Firefox: $E_1 \rightarrow E_2$ H_2: PDF is downloaded: $E_2 \rightarrow E_3$ H_3: PDF connects to 212.150.164.20: $E_3 \rightarrow E_4$

We determine the prior probability for each piece of evidence based on the results of the probability mass function with results shown in Table B.3 and Table B.4. The results of the evaluation is shown in Table B.5.

In order to highlight the potential of this method, we should the reevaluation of the evidence after new evidence obtained. As shown in Figure B.4. Evidence was found that connected the ip address to the user's bank server. This update extends to changes in the prior probability of each piece of evidence shown in Table B.6 and Table B.7. The updated results are shown in Table B.8.

8.3 CASE STUDY: W32.CRIDEX

W32.Cridex is a worm, a type of malware that replicates and circulates without human intervention. W32.Cridex can replicate and spread not only inside of your computer, but also to other computers connected to your network. The W32.Cridex is extremely dangerous because of its ability to spread quickly [125].

W32.Cridex infects your computer, it tries to create a copy of itself as a Windows executable file. After infecting your computer, W32.Cridex will attempt to use your network to connect with its source computer. The primary goal is to update itself and download other malware programs and files [125].

W.32 Cridex also attempts to infect the Windows Registry of your computer. The purpose is to remain undetectable, protect other malicious programs its downloads, start up when the computer boots, and ultimately take full control over your computer [125].

We review the implementation of this method on W32.Cridex. The analyst must observe the evidence. The graph-based representation of our evidence is shown in Figure C.1. We are presented with two graphs show in Figure C.2 and Figure C.3. We focus on Figure C.2.

Next, we rely on our two previous link analysis algorithms to make more observations. We use HITs to determine pieces of evidence that provide us with overall knowledge of what has occurred in the system. Table C.1 shows our results from the HITS algorithm. Table C.2 shows the results from the PageRank algorithm.

We see that reader_sl is a child process of explorer.exe. The parent process of explorer.exe is 1463. reader_sl.exe is process associated with Adobe Speed Launcher however, the launch chain is interesting. We also see that explorer.exe is a parent node for an active connection to a remote IP address 41.165.5.140. This IP address is traced back to a corporation Neotel Operations in Johannesburg, South Africa. It is interesting to note that 1484 made a connection to the IP address 125.19.103.198. This IP address is traced back to Bharti Tele-Ventures Limited in New Delhi, India.

We implement my methodology in order to obtain a better understanding of this malware.

Hypothesis H: Malware makes unwarranted network connections.

Evidence 1 E_1: 1464
Evidence 2 E_2: explorer.exe
Evidence 3 E_3: 125.19.103.198
Evidence 4 E_4: 41.168.5.140

H_1: $E_1 \rightarrow E_3$
H_2: $E_1 \rightarrow E_2 \rightarrow E_3$

The we shown the evaluation results in Table C.3, Table C.4 and Table C.5. In this case, the result is not truly satisfying to us as we have a very high statistical likelihood for either of our categories. This is due to the lack of evidence provided in the graph. With limited supporting evidence for the root hypothesis, weakens the results of the evaluation. This problem can be solved by looking at evidence from varied mediums. At the moment we only look at memory, however, there is more information to be found in network traffic, files,

documents, and the file system.

8.4 CASE STUDY: WEBSITE PROBLEMS

A company's web server has been breached through their website. A team arrived just in time to take a forensic image of the running system and its memory for further analysis [126].

In this case, we find that the cmdscan plugin searches the memory of csrss.exe on XP/Vista and conhost.exe on Windows 7 for commands that attacker entered through a console (cmd.exe). This is one of the most powerful commands you can use to gain visibility into an attackers actions on a victim system, whether they opened cmd.exe through an RDP session or proxied input/output to a command shell from a networked backdoor [67].

This plugin finds structures known as COMMAND_HISTORY by looking for a known constant value (MaxHistory) and applying sanity checks. The structures used by this plugin are not public, thus they're not available in WinDBG or any other forensic framework. They were reverse engineered by Michael Ligh from the conhost.exe and winsrv.dll binaries [67].

In addition to the commands entered into a shell, this plugin shows:

- The name of the console host process (csrss.exe or conhost.exe)
- The name of the application using the console (whatever process is using cmd.exe)
- The location of the command history buffers, including current buffer count, last added command, and displayed command
- The application process handle

Due to the scanning technique this plugin uses, it has the capability to find commands from both active and closed consoles. Current memory forensics tools concentrate mainly on system-related information like processes and sockets. The command history operating system a prime source of evidence in many intrusions and other computer crimes, revealing important details about an offender's activities on the subject system [127].

The Microsoft Windows command prompt (cmd.exe) is often used by perpetrators of computer crime, and being able to reconstruct what instructions were executed on the command line can be important in a digital investigation. Computer intruders go so far as to place their own copy of the command prompt executable on a compromised system to facilitate their unauthorized activities. The command history maintained by the Windows command prompt can contain valuable information such as what programs were executed with associated arguments, files and folders that were accessed, and unique information such as IP addresses, domain names and network shares [128].

The first step involved in the scientific method is the observation of the evidence. The analyst must observe the evidence. In order to observe our evidence, in this case, we build our graph. The graph-based representation of our evidence is shown in Figure D.1. A table to reference the commands found is shown in Table D.1.

We use HITs to determine pieces of evidence that provide us with overall knowledge of what has occurred in the system. Table D.2 shows the results from the HITS algorithm. There are a notable pieces of evidence from these results. We see that explorer.exe is a hub, as well as services.exe, 192.168.56.1, mysqld.exe, and xampp-control.e. This information lets us know that there is a web site hosted on this machine. services.exe is associated with Services Control Manager which is responsible for running, ending, and interacting with system services. mysqld.exe is associated with MySQL Server. xampp-control.e is associated with XAMPP an open source web server.

The results of the PageRank algorithm is found Table D.3. From these results we see other important pieces of evidence. httpd.exe is associated with Apache HTTP Server and cmd.exe is associated with the Windows N/T command line interpreter. We take a further look at the command performed using cmd.exe in Table D.1. ipconfig displays all current TCP/IP network configuration values. net user /add adds a user to certain group and it appears to add a user to the remote desktop users group.

Stemming from our case study hypothesis H is the root node of the Bayesian network.

Hypothesis H: Company's website was hacked and gained access to the company's machine.

Evidence 1 E_1: explorer.exe
Evidence 2 E_2: xampp-control.e
Evidence 3 E_3: mysqld.exe
Evidence 4 E_4: httpd.exe
Evidence 5 E_5: FileZillaServer
Evidence 6 E_7: 472
Evidence 7 E_8: csrss.exe
Evidence 8 E_9: cmd#

H_1: Company is up Website: $E_1 \rightarrow E_5$
H_2: Hacker tries to gain access: $E_6 \rightarrow E_8$

The evaluation and results are shown in Table D.4, Table D.5, and Table D.6. In forensic

cases, it is necessary to account for 0 or 1 facts of the case. This happens when an entire file is found or the investigating the effects of malware on the system. This, as shown above, leads to changes in our results of yes and no and only slightly affects the maybe depending on the importance of the evidence. Now, that we have results, the next to report them.

We rely on the implementation of a likelihood ratio in order to estimate the credibility of the analysis performed by the examiner and the strength of the evidence. The likelihood ratio is a way of comparing probabilities conditioned a hypothesis. While the possibility of using likelihood ratios are still being weighed in the legal system we believe it is a great tool to contribute the scientific method during a digital forensic investigation. It would bring a careful and balanced approach to expert evidence.

We rely on the implementation of a likelihood ratio in order to estimate the credibility of the analysis performed by the examiner and the strength of the evidence. The likelihood ratio is a way of comparing probabilities conditioned a hypothesis. While the possibility of using likelihood ratios are still being weighed in the legal system we believe it is a great tool to contribute the scientific method during a digital forensic investigation. It would bring a careful and balanced approach to expert evidence.

CHAPTER 9: CONCLUSION & FUTURE WORK

This dissertation explores the need to improve the field of the digital forensics and proposes that the computer science and digital forensics community begin to work in tandem to reach this goal. I presented multiple methods in order to accomplish this goal.

The Digital Forensic Education Initiative offers a standardized a multidisciplinary curriculum model for digital forensics education. This project transformed the multidisciplinary undergraduate education at the University of Illinois at Urbana-Champaign by institutionalizing this program and the collaboration upon which it is built. In accordance with the multidisciplinary nature of the field of digital forensics, the curriculum development team included domain experts in computer security, computer networks, law, civil and criminal justice, fraud investigation, and psychology. The modular approach to curriculum development is organized by a three-course digital forensics education sequence and the modules are combined to form a coherent narrative, thus exposing students to multiple perspectives on digital forensics. The curriculum package provides a strong theoretical foundation for the techniques learned by the students as well as an array of studies in fields related to digital forensics. Hopefully this paper will initiate a conversation with the international community, note that standards need to continue to be developed for digital forensics curriculum, and recognize the multidisciplinary need for this field of study. This project, curriculum, and course outline are available on the website `http://publish.illinois.edu/digital-forensics/` and a content package containing all of these materials will be posted there in the near future.

I examined the methods used during the analysis phase of the digital forensic process. Evidence reasoning models are an important part of the forensic process. Unlike traditional forensic sciences, digital forensics deals almost exclusively with objects of non-deterministic nature; there is great difficulty in analyzing and scrutinizing digital evidence. Fundamental flaws hinder current evidence analysis models in their ability to assess accurately the likelihood of crime occurrence. Furthermore, conclusions based on probabilities complicate explanations in the courtroom. These flaws must be identified and understood to avoid the possibility of injudicious assumptions resulting from the forensic process.

Differential analysis of digital evidence becomes difficult when the scope of the investigation is widened; unintentional noise in the form of benign modifications may lead to dubious conclusions about system integrity. Furthermore, recent obfuscation techniques have successfully averted detection by traditional methods. Event reconstruction models are limited in their ability to provide investigators with clear attack scenarios, because they rely on the

exhaustive identification of possible machine states; there is yet to be a resource providing such information. Probabilistic reasoning models rely on prior probabilities known to the investigator, which have so far mainly been determined from surveying others in the field. Besides the obvious expenditure of time and effort in conducting such surveys, it is reckless to underestimate the potential for entropy and reason that small samples of observed probabilities hold true for all investigations. It can be concluded that each of these techniques is only applicable to a small niche of forensic scenarios.

The increasing rate of software development places a burden on forensic examiners to keep up with the latest software packages, both commercial and free. Each of the models discussed in this paper lacks a comprehensive database of information to conduct analysis with the highest accuracy. We highlight the need for a community-driven, updated catalog of file hashes, machine states, and probability metrics for use in forensic analysis. The changing nature of technology and software necessitates that researchers and law enforcement collaborate to ensure the digital forensic process is as reliable as possible.

I realized the potential of integrating computer science research in the field of digital forensics. I rely on graph theory to serve as the basis for further analysis of data generated from digital forensics tools. In particular, the graphical representation of evidence allows an investigator to not only visualize but perform data analysis on evidence. This analysis enables forensic investigators to locate information of interest efficiently.

Initial work with graph theory has identified several areas for future research. The first area is an exploration of relationships among the evidence. This research has begun in previous works however, it still needs to be continued alongside the exploration of time-dependent graphs. Digital evidence has multiple relationships that are both dependent on time and not. Exploring this area can lead to further insight and greater knowledge. The second area of exploration is the potential to develop algorithms based on graph theory. In digital forensics, outlier detection is not enough to detect everyday user actions. However, through the exploration of link analysis, this might be possible to determine potentially unique events. This area of exploration will require a lot of well-documented datasets open to the public. The third area of exploration is the automation of this tool. The automation of determining relationships among artifacts as well as the interpretation of them. This work is also already in progress by many previous works.

I explored the potential benefits of using graph representation in digital forensics. It is possible to get a high-level view of the system without requiring extensive knowledge of the operating system and its applications. In this paper, we successfully showed the potential of using graph representation in the analysis. We show this by exploring a case studies.In the future, we believe that this work can be greatly improved by exploring more relationships.

We plan to further these efforts by building a prototype and implementing more forms of analysis.

I presented a structured method for implementing and maintaining the scientific method, as well as, determining a likelihood of a hypothesis. The assignment of likelihoods provides us with great a benefit. We can quantify the likelihood of a hypothesis in relation to digital evidence, limiting examiner bias as well as being better able to test everything hypothesis. However, we are still hindered by the common digital forensic practice problems, such as the amount of data, varying data types and how the legal system view these computational techniques. Yet, this method is necessary to begin a formalization.

Future work involves researching existing case law in order to assist in revamping curriculum to improve digital evidence literacy among law students. It is excepted that a thorough analysis of cases where digital evidence has been inappropriately handled will further refine recommendations for curriculum content made above. Also, insights of thorough examination of case law will be disseminated broadly to the digital forensics community.

I also plan to research of evidence-based on techniques. In the case study scenarios, we define evidence as memory artifacts and we limit our memory artifacts to a small set. This worked for our case, however, may not work in all scenarios. Second, the development of a Bayesian network for each hypothesis would be time-consuming to perform manually the development of an automated system would ease this process greatly. Lastly, the ability to identify all the possible hypotheses is crucial, however, they may not be evident. The development of methods to examine evidence and identify key areas of interest will aid examiners in the investigative process.

Overall this work shows the connection between computer science and digital forensics. It is of uptmost importance to begin to further research in the field of digital forensics with the support of the computer science community. Digital forensics is in need of objective methodologies to obtain conclusions from evidence. We presented a method to regulate the analysis process. We believe that after an implementation of this method we can use various computational techniques and apply them to digital forensic analysis in order to determine standards for current cases. We also plan to analyze already other potential analysis models in order to compare their advantages and disadvantages.

CHAPTER 10: REFERENCES

[1] H. Edwards, C. Gatsonis, M. Berger, J. Cecil, M. Bonner-Denton, E. Fierro et al., "Strengthening forensic science in the united states: A path forward," *ISBN-13*, pp. 978–0 309 131 353, 2009.

[2] T. W. G. on Crime Scene Investigation, *Electronic Crime Scene Investigation: a Guide for First Responders*. US Department of Justice, Office of Justice Programs, National Instit. of Justice, 2001.

[3] S. Ballou, *Electronic crime scene investigation: A guide for first responders*. Diane Publishing, 2010.

[4] S. L. Garfinkel, "Digital forensics research: The next 10 years," *digital investigation*, vol. 7, pp. S64–S73, 2010.

[5] N. Beebe, "Digital forensic research: The good, the bad and the unaddressed," *Advances in digital forensics V*, pp. 17–36, 2009.

[6] D. B. Parker, *Crime by computer*. Charles Scribner's Sons, 1976.

[7] S. Y. Willassen and S. Mjolsnes, "Digital forensic research," *Telektronikk*, vol. 101, no. 1, p. 92, 2005.

[8] C. Stoll, *The cuckoo's egg: tracking a spy through the maze of computer espionage*. Simon and Schuster, 2005.

[9] P. A. Collier and B. J. Spaul, "A forensic methodology for countering computer crime," *Artificial intelligence review*, vol. 6, no. 2, pp. 203–215, 1992.

[10] B. D. Carrier, "A hypothesis-based approach to digital forensic investigations," 2006.

[11] S. Peisert, M. Bishop, and K. Marzullo, "Computer forensics in forensis," in *Systematic Approaches to Digital Forensic Engineering, 2008. SADFE'08. Third International Workshop on*. IEEE, 2008, pp. 102–122.

[12] P. Sommer, "Intrusion detection systems as evidence," *Computer Networks*, vol. 31, no. 23, pp. 2477–2487, 1999.

[13] R. Moore, *Cybercrime: Investigating high-technology computer crime*. Routledge, 2010.

[14] F. P. Buchholz and C. Falk, "Design and implementation of zeitline: a forensic timeline editor." in *DFRWS*, 2005.

[15] M. M. Pollitt, "An ad hoc review of digital forensic models," in *Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007. Second International Workshop on*. IEEE, 2007, pp. 43–54.

[16] G. C. Kessler, *Judges' awareness, understanding, and application of digital evidence*. Nova Southeastern University, 2010.

[17] S. Nagy, I. Palmer, S. C. Sundaramurthy, X. Ou, and R. Campbell, "An empirical study on current models for reasoning about digital evidence."

[18] A. Alva and B. Endicott-Popovsky, "Digital evidence education in schools of law," *The Journal of Digital Forensics, Security and Law: JDFSL*, vol. 7, no. 2, p. 75, 2012.

[19] M. Rigby, "Child porn investigations may snare the innocent," 2010.

[20] T. C. United States Court of Appels, "United states of america v. donald r. miller jr., appellant," 2008.

[21] L. Marziale III, "Advanced techniques for improving the efficacy of digital forensics investigations," Ph.D. dissertation, University of New Orleans, 2009.

[22] K. Martire, R. Kemp, M. Sayle, and B. Newell, "On the interpretation of likelihood ratios in forensic science evidence: Presentation formats and the weak evidence effect," *Forensic science international*, vol. 240, pp. 61–68, 2014.

[23] W. C. Thompson, J. Vuille, A. Biedermann, and F. Taroni, "The role of prior probability in forensic assessments," *Frontiers in genetics*, vol. 4, 2013.

[24] J. Keppens, "On modelling non-probabilistic uncertainty in the likelihood ratio approach to evidential reasoning," *Artificial intelligence and law*, vol. 22, no. 3, pp. 239–290, 2014.

[25] J.-J. C. Meyer and W. Van Der Hoek, *Epistemic logic for AI and computer science*. Cambridge University Press, 2004, vol. 41.

[26] A. Yasinsac, R. F. Erbacher, D. G. Marks, M. M. Pollitt, and P. M. Sommer, "Computer forensics education," *IEEE Security & Privacy*, vol. 99, no. 4, pp. 15–23, 2003.

[27] D. Bem and E. Huebner, "Computer forensics workshop for undergraduate students," in *Proceedings of the tenth conference on Australasian computing education-Volume 78*. Australian Computer Society, Inc., 2008, pp. 29–33.

[28] G. C. Kessler and M. E. Schirling, "The design of an undergraduate degree program in computer & digital forensics," *Journal of Digital Forensics, Security and Law*, vol. 1, no. 3, pp. 37–50, 2006.

[29] C. A. Lee, A. Russel, K. Kearton, D. Dittrich, K. Woods, and S. Garfinkel, "Creating realistic corpora for forensic and security education," 2011.

[30] E. S. Ismand and J. A. Hamilton Jr, "A digital forensics program to retrain americas veterans," in *5th Annual Symposium on Information Assurance (ASIA10)*, 2010, pp. 62–66.

[31] S. Al Amro, F. Chiclana, and D. A. Elizondo, "Application of fuzzy logic in computer security and forensics." 2012.

[32] H. Chi, F. Dix-Richardson, and D. Evans, "Designing a computer forensics concentration for cross-disciplinary undergraduate students," in *2010 Information Security Curriculum Development Conference*. ACM, 2010, pp. 52–57.

[33] S. Srinivasan, "Computer forensics curriculum in security education," in *2009 Information Security Curriculum Development Conference*. ACM, 2009, pp. 32–36.

[34] M. Bashir, J. A. Applequist, R. H. Campbell, L. DeStefano, G. L. Garcia, and A. Lang, "Development and dissemination of a new multidisciplinary undergraduate curriculum in digital forensics," in *Proceedings of the Conference on Digital Forensics, Security and Law*. Association of Digital Forensics, Security and Law, 2014, p. 161.

[35] J. Liu, "Implementing a baccalaureate program in computer forensics," *Journal of Computing Sciences in Colleges*, vol. 25, no. 3, pp. 101–109, 2010.

[36] D. Wassenaar, D. Woo, and P. Wu, "A certificate program in computer forensics," *Journal of Computing Sciences in Colleges*, vol. 24, no. 4, pp. 158–167, 2009.

[37] A. Lang, M. Bashir, R. Campbell, and L. DeStefano, "Developing a new digital forensics curriculum," *Digital Investigation*, vol. 11, pp. S76–S84, 2014.

[38] R. J. Walls, B. N. Levine, M. Liberatore, and C. Shields, "Effective digital forensics research is investigator-centric." in *HotSec*, 2011.

[39] M. Kwan, K.-P. Chow, F. Law, and P. Lai, "Reasoning about evidence using bayesian networks," *Advances in Digital Forensics IV*, pp. 275–289, 2008.

[40] M. Bishop, "Academia and education in information security: Four years later," in *Proceedings of the Fourth National Colloquium on Information System Security Education*, 2000.

[41] P. Craiger, L. Ponte, C. Whitcomb, M. Pollitt, and R. Eaglin, "Master's degree in digital forensics," in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on.* IEEE, 2007, pp. 264b–264b.

[42] K. Nance, H. Armstrong, and C. Armstrong, "Digital forensics: Defining an education agenda," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on.* IEEE, 2010, pp. 1–10.

[43] S. Cooper, C. Nickell, L. C. Pérez, B. Oldfield, J. Brynielsson, A. G. Gökce, E. K. Hawthorne, K. J. Klee, A. Lawrence, and S. Wetzel, "Towards information assurance (ia) curricular guidelines," in *Proceedings of the 2010 ITiCSE working group reports.* ACM, 2010, pp. 49–64.

[44] L. Gottschalk, J. Liu, B. Dathan, S. Fitzgerald, and M. Stein, "Computer forensics programs in higher education: a preliminary study," in *ACM SIGCSE Bulletin*, vol. 37, no. 1. ACM, 2005, pp. 147–151.

[45] F. A. Standards, American Academy of Forensic Sciences, 2012.

[46] C. Curricula, "Report of the acm/ieee-cs joint curriculum task force," *Association for Computing Machinery*, 1991.

[47] W. V. U. F. S. Initiative et al., "Technical working group for education and training in digital forensics," *Retrieved October*, vol. 7, p. 2009, 2007.

[48] R. Policy, "Swgde/swgit guidelines & recommendations for training in digital & multimedia evidence."

[49] B. Carrier, "Defining digital forensic examination and analysis tools using abstraction layers," *International Journal of digital evidence*, vol. 1, no. 4, pp. 1–12, 2003.

[50] "Encase forensic software," Guidance Software.

[51] B. Carrier, "The sleuth kit and autopsy: forensics tools for linux and other unixes, 2005," *URL http://www. sleuthkit. org*, 2009.

[52] N. Bassetti, "Caine: Computer aided investigative environment."

[53] G. G. Richard III and V. Roussev, "Scalpel: A frugal, high performance file carver." in *DFRWS*, 2005.

[54] A. Data, "Forensic toolkit," *Disponível online www. accessdata. com/media/en_US/print/papers/FTK2. 0_cutsheet_Core _Print. pdf*, 2005.

[55] "Registry recon." [Online]. Available: http://arsenalrecon.com/apps/recon/

[56] "Libforensics." [Online]. Available: http://code.google.com/p/libforensics/

[57] "Cellebrite ufed." [Online]. Available: https://www.cellebrite.com/en/home/

[58] "Xry logical." [Online]. Available: https://msab.com

[59] "Plainsight." [Online]. Available: www.plainsight.info

[60] "P2 explorer." [Online]. Available: https://p2-explorer.soft112.com

[61] "Mandiant redline." [Online]. Available: https://www.fireeye.com/services/freeware/redline.html

[62] "Xplico - open source network forensic analysis tool (nfat)." [Online]. Available: https://www.xplico.org/

[63] "Bulk extractor." [Online]. Available: https://github.com/simsong/bulk_extractor

[64] "Oxygen forenisc suite." [Online]. Available: https://www.oxygen-forensic.com/

[65] "The coroner's toolkit." [Online]. Available: www.porcupine.org/forensics/tct.html

[66] "Windows scope." [Online]. Available: www.windowsscope.com

[67] "The volatility framework," The Volatility Foundation.

[68] C. Hargreaves and J. Patterson, "An automated timeline reconstruction approach for digital forensic investigations," *Digital Investigation*, vol. 9, pp. S69–S79, 2012.

[69] A. Case, A. Cristina, L. Marziale, G. G. Richard, and V. Roussev, "Face: Automated digital evidence discovery and correlation," *digital investigation*, vol. 5, pp. S65–S75, 2008.

[70] S. Jeyaraman and M. J. Atallah, "An empirical study of automatic event reconstruction systems," *digital investigation*, vol. 3, pp. 108–115, 2006.

[71] V. Roussev and G. G. Richard III, "Breaking the performance wall: The case for distributed digital forensics," in *Proceedings of the 2004 digital forensics research workshop*, vol. 94, 2004.

[72] N. Beebe and J. Clark, "Dealing with terabyte data sets in digital investigations," in *Advances in Digital Forensics: IFIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, February 13-16, 2005*, vol. 194. Springer, 2005, p. 1.

[73] P. Sanderson, "Mass image classification," *digital investigation*, vol. 3, no. 4, pp. 190–195, 2006.

[74] P. Craiger, P. Burke, C. Marberry, and M. Pollitt, "A virtual digital forensics laboratory," *Advances in digital forensics IV*, pp. 357–365, 2008.

[75] L. Marziale, G. G. Richard, and V. Roussev, "Massive threading: Using gpus to increase the performance of digital forensics tools," *digital investigation*, vol. 4, pp. 73–81, 2007.

[76] B. Fei, J. Eloff, H. Venter, and M. Olivier, "Exploring forensic data with self-organizing maps," *Advances in digital forensics*, pp. 113–123, 2005.

[77] N. Murilo and K. Steding-Jessen, "Chkrootkit v. 0.43," 2007.

[78] M. Tyson, P. Berry, N. Williams, D. Moran, and D. Blei, "Derbi: Diagnosis, explanation and recovery from computer break-ins," Technical Report DARPA Project F30602-96-C-0295 Final Report, SRI International, Artificial Intelligence Center, Tech. Rep., 2001.

[79] R. Leigland and A. W. Krings, "A formalization of digital forensics," *International Journal of Digital Evidence*, vol. 3, no. 2, pp. 1–32, 2004.

[80] C. Elsaesser and M. C. Tanner, "Automated diagnosis for computer forensics," *The Mitre Corporation*, pp. 1–16, 2001.

[81] T. Stallard and K. Levitt, "Automated analysis for digital forensic science: Semantic integrity checking," in *Computer Security Applications Conference, 2003. Proceedings. 19th Annual.* IEEE, 2003, pp. 160–167.

[82] 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, pp. 1–11, 2004.

[83] B. D. Carrier, E. H. Spafford et al., "Automated digital evidence target definition using outlier analysis and existing evidence." in *DFRWS*, 2005.

[84] A. L. Vickers, "Daubert, critique and interpretation: What empirical studies tell us about the application of daubert," *USFL Rev.*, vol. 40, p. 109, 2005.

[85] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," *NIST Special Publication*, vol. 10, pp. 800–86, 2006.

[86] R. S. Ieong, "Forza–digital forensics investigation framework that incorporate legal issues," *digital investigation*, vol. 3, pp. 29–36, 2006.

[87] S. Garfinkel, A. J. Nelson, and J. Young, "A general strategy for differential forensic analysis," *Digital Investigation*, vol. 9, pp. S50–S59, 2012.

[88] M. Gielen, "Prioritizing computer forensics using triage techniques," 2014.

[89] Microsoft, "Microsoft windows," 2015.

[90] S. Bunting and W. Wei, *EnCase Computer Forensics: The Official EnCE: EnCase? Certified Examiner Study Guide.* John Wiley & Sons, 2006.

[91] B. Carrier, "The sleuth kit," *TSK). http://www. sleuthkit. org/sleuthkit/.[Online*, 2011.

[92] U. Fiore, "Selective redundancy removal: A framework for data hiding," *Future Internet*, vol. 2, no. 1, pp. 30–40, 2010.

[93] S. Mead, "Unique file identification in the national software reference library," *Digital Investigation*, vol. 3, no. 3, pp. 138–150, 2006.

[94] R. E. Overill and J. A. Silomon, "Digital meta-forensics: Quantifying the investigation," in *Proc. 4th International Conference on Cybercrime Forensics Education & Training (CFET 2010), Canterbury, UK (September 2010)*, 2010.

[95] P. Huygen, "Use of bayesian belief networks in legal reasoning," in *17th BILETA Annual Conference*, 2002.

[96] R. E. Overill, J. A. Silomon, K.-P. Chow, and H. Tse, "Quantification of digital forensic hypotheses using probability theory," in *Systematic Approaches to Digital Forensic Engineering (SADFE), 2013 Eighth International Workshop on.* IEEE, 2013, pp. 1–5.

[97] K. Stoffel, P. Cotofrei, and D. Han, "Fuzzy methods for forensic data analysis," in *Soft Computing and Pattern Recognition (SoCPaR), 2010 International Conference of.* IEEE, 2010, pp. 23–28.

[98] G. Shafer, "Probability judgment in artificial intelligence and expert systems," *Statistical science*, pp. 3–16, 1987.

[99] S. Al-Kuwari and S. D. Wolthusen, "Fuzzy trace validation: Toward an offline forensic tracking framework," in *Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on.* IEEE, 2011, pp. 1–4.

[100] P. Gladyshev and A. Patel, "Finite state machine approach to digital event reconstruction," *Digital Investigation*, vol. 1, no. 2, pp. 130–149, 2004.

[101] C. Liu, A. Singhal, and D. Wijesekera, "Using attack graphs in forensic examinations," in *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on.* IEEE, 2012, pp. 596–603.

[102] P. Xie, J. H. Li, X. Ou, P. Liu, and R. Levy, "Using bayesian networks for cyber security analysis," in *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on.* IEEE, 2010, pp. 211–220.

[103] A. J. Izenman, "Introduction to two views on the shonubi case," *Statistical Science in the Courtroom*, pp. 393–403, 2000.

[104] I. Palmer, E. Wood, S. Nagy, G. Garcia, M. Bashir, and R. Campbell, "Digital forensics education: a multidisciplinary curriculum model," in *International Conference on Digital Forensics and Cyber Crime.* Springer, 2015, pp. 3–15.

[105] "Digital forensics working group," 2010. [Online]. Available: http://digitalforensicswg.wikispaces.com/

[106] J. Schipp, J. Dopheide, and A. Slagell, "Islet: an isolated, scalable, & lightweight environment for training," in *Proceedings of the 2015 XSEDE Conference: Scientific Advancements Enabled by Enhanced Cyberinfrastructure.* ACM, 2015, p. 17.

[107] P. Linstrom and W. Mallard, "National institute of standards and technology: Gaithersburg," *MD, March*, vol. 20899, 2003.

[108] D. K. Rossmo, *Criminal investigative failures.* CRC press, 2008.

[109] V. Baryamureeba and F. Tushabe, "The enhanced digital investigation process model," in *Proceedings of the Fourth Digital Forensic Research Workshop*, 2004, pp. 1–9.

[110] I. Kruse, "Warren and jay, g. heiser (2002) computer forensics: Incident response essentials."

[111] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *International Journal of Digital Evidence*, vol. 1, no. 3, pp. 1–12, 2002.

[112] B. Carrier and E. H. Spafford, "Getting physical with the investigative process international journal of digital evidence. fall 2003," 2003.

[113] I. Palmer, B. Gelfand, and R. Campbell, "Exploring digital evidence with graph theory," 2017.

[114] F. TARONI and P. GARBOLINO, "Bayesian networks and the evaluation of scientific evidence: A theoretical approach."

[115] A. Eckelberry, G. Dardick, J. Folkerts, A. Shipp, E. Sites, J. Stewart, and R. Stuart, "Technical review of the trial testimony state of connecticut vs. julie amero." [Online]. Available: http://dfir.com.br/wp-content/uploads/2014/02/julieamerosummary.pdf

[116] A. Kantor, "Police school get failing grade in sad case of julie amero," 2007. [Online]. Available: http://wwww.usatoday.com/tech/columnist/andrewkantor/2007-02-22-julie-amaro_x.htm

[117] "State of connecticute v. julie amero trial testimony," 2007. [Online]. Available: http://drumwhistles.com/pdf/amero-test.zip

[118] B. Krebs, "Felony spyware/porn charges against teacher dropped," 2008. [Online]. Available: http://voices.washingtonpost.com/securityfix/2008/11/ct_drops_felony_spywareporn_ch.html?nav=rss_blog

[119] J. Hullman, S. Drucker, N. H. Riche, B. Lee, D. Fisher, and E. Adar, "A deeper understanding of sequence in narrative visualization," *IEEE Transactions on Visualziation and Computer Graphics*, vol. 19, no. 12, pp. 2406–2415, 2013.

[120] M. J. Saks and J. Koehler, "What dna fingerprinting can teach the law about the rest of forensic science," *Cardozo L. Rev.*, vol. 13, p. 361, 1991.

[121] B. Dolan-Gavitt, "The vad tree: A process-eye view of physical memory," *digital investigation*, vol. 4, pp. 62–64, 2007.

[122] A. Schuster, "The impact of microsoft windows pool allocation strategies on memory forensics," *Digital Investigation*, vol. 5, pp. S58–S64, 2008.

[123] V. Oracle, "Virtualbox," 2015.

[124] L. Spitzner et al., "The honeynet project," 2004.

[125] "W.32 cridex." [Online]. Available: https://www.symantec.com/security_response/writeup.jsp?docid=2012-012103-0840-99

[126] "Digital forensic challenge." [Online]. Available: https://www.binary-zone.com/2015/09/16/digital-forensic-challenge-4/

[127] R. M. Stevens and E. Casey, "Extracting windows command line details from physical memory," *digital investigation*, vol. 7, pp. S57–S63, 2010.

[128] C. H. Malin, E. Casey, and J. M. Aquilina, *Malware Forensics: Investigating and Analyzing Malicious Code*. Syngress, 2008.

APPENDIX A: CASE STUDY: DROPBOX PROBLEMS

Node ID	Hub Value
firefox.exe	0.9999
AcroRd32.exe	7.9396e-09
explorer.exe	7.9396e-09
WmiPrvSE.exe	1.1282e-22
notepad.exe	0.0
54.201.155.11	0.0
192.168.1.115	0.0
23.209.190.51	0.0
Dropbox	0.0

Table A.1: The hub value results from the hyperlinked-induced topic search from Figure A.2

Node ID	PageRank Value
firefox.exe	0.1235
AcroRd32.exe	0.1235
notepad.exe	0.1216
192.168.1.115	0.1216
Dropbox	0.1041
23.209.190.51	0.1014
54.201.155.11	0.1014
WmiPrvSE.exe	0.0691

Table A.2: The PageRank value results from Figure A.2

Degree	Degree Probability
1	0.6666
3	0.2222
4	0.1111

Table A.3: The results of the probability mass function for Figure A.2.

Node	Prior Probability Value
explorer.exe	0.2222
firefox.exe	0.1111
Dropbox	0.6666
AcroRd32.exe	0.2222
notepad.exe	0.6666
192.168.1.115	0.6666

Table A.4: The prior probability for each piece of evidence.

Yes	No	Uncertain
0.7722	0.33	0.5578

Table A.5: The results from the evaluation.

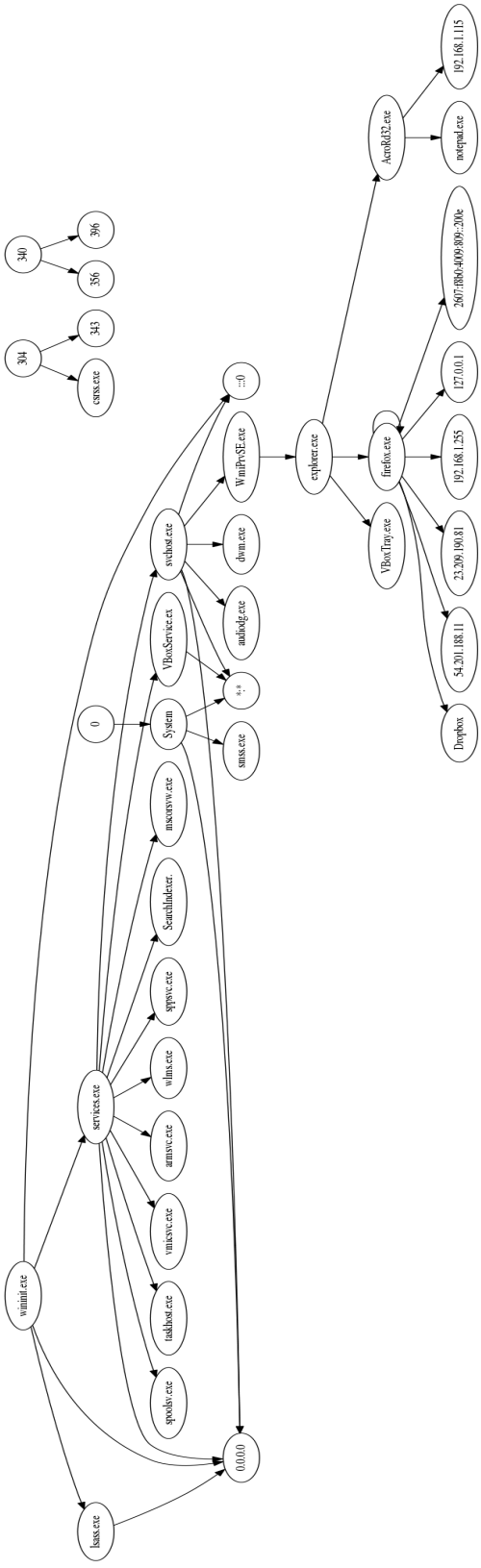

Figure A.1: A graph-based representation of the evidence.

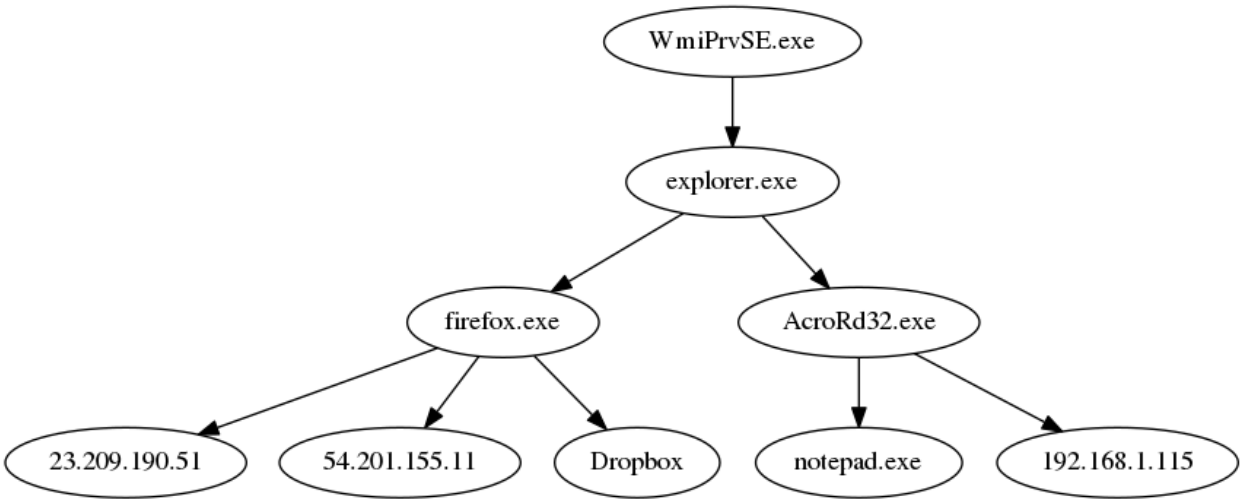

Figure A.2: A graph-based representation of the evidence after differential analysis.

APPENDIX B: CASE STUDY: BANKING TROUBLES

Node ID	Hub Value
firefox.exe	0.9999
explorer.exe	1.0314e-08
AcrodRd32.exe	6.8715-e26
1660	6.8715e-26
VMwareUser.exe	0.0
VMwareTray.exe	0.0
212.159.164.203	0.0
127.0.0.1	0.0
66.249.91.103	0.0
212.150.164.203	0.0
66.249.90.104	0.0

Table B.1: The hub value results from the hyperlinked-induced topic search from Figure B.2.

Node ID	PageRank
212.159.164.203	0.1311
explorer.exe	0.1171
firefox.exe	0.0965
VMwareUser.exe	0.0965
VMwareTray.exe	0.0965
AcroRd32.exe	0.0797
66.249.91.103	0.0797
127.0.0.1	0.0797
212.150.164.203	0.0797
1660	0.0633

Table B.2: The PageRank values for Figure B.2.

Degree	Degree Probability
1	0.7272
2	0.0909
4	0.0909
6	0.0909

Table B.3: The results of the probability mass function for Figure B.2.

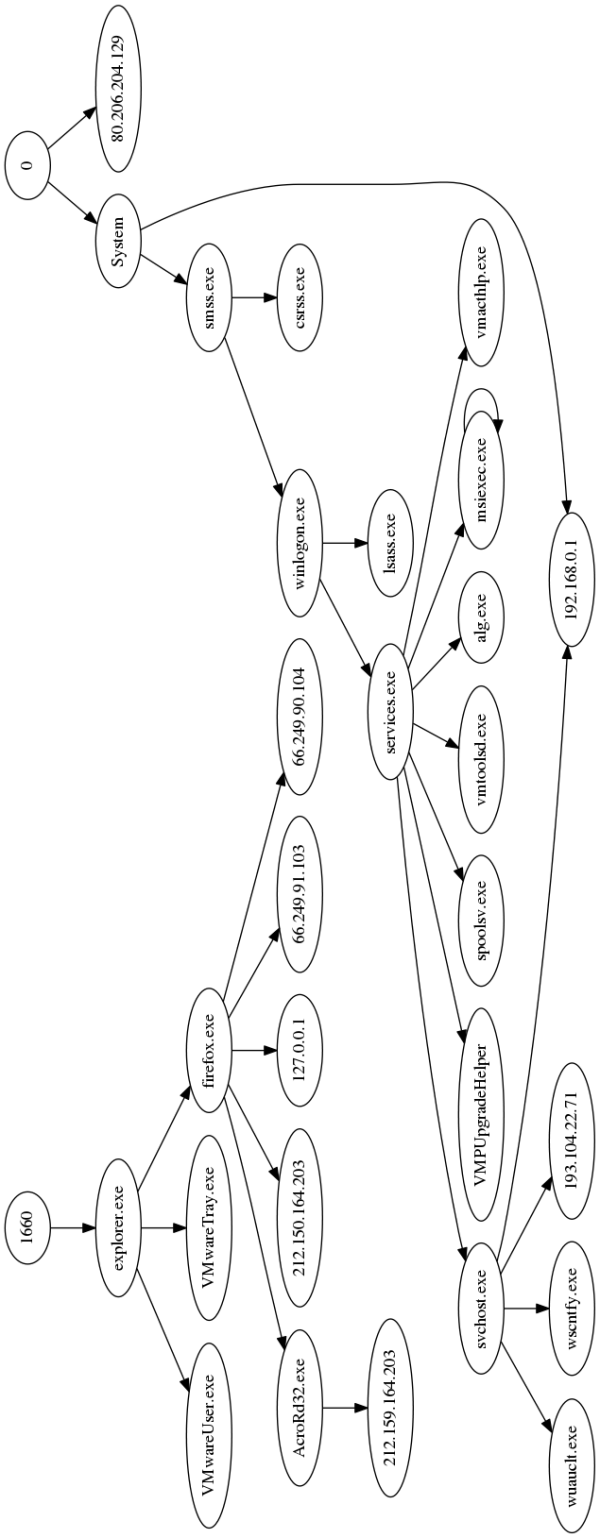

Figure B.1: A graph-based representation of the evidence.

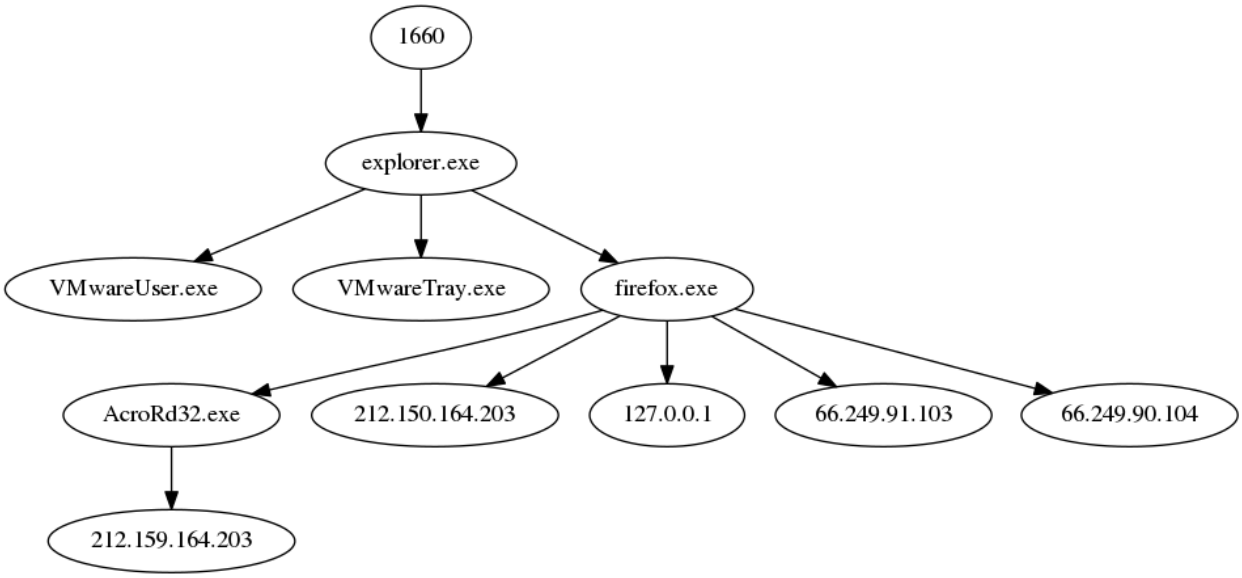

Figure B.2: A subgraph of Figure B.1.

Node	Prior Probability Value
explorer.exe	0.0909
firefox.exe	0.0909
AcroRd32.exe	0.0909
212.150.164.203	0.7272

Table B.4: The prior probability for each piece of evidence.

Yes	No	Uncertain
0.3305	0.4890	0.8404

Table B.5: The results from the evaluation.

Degree	Degree Probability
1	0.7692
2	0.0769
3	0.0769
4	0.0769
6	0.0769

Table B.6: The updated results of the probability mass function.

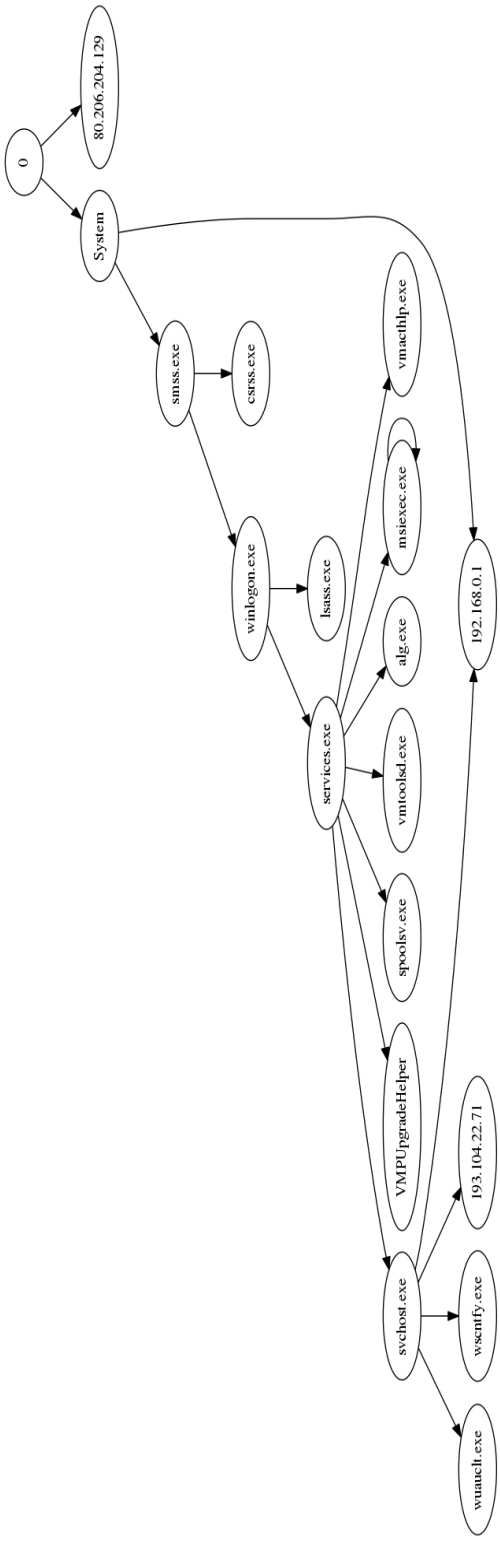

Figure B.3: A subgraph of Figure B.1.

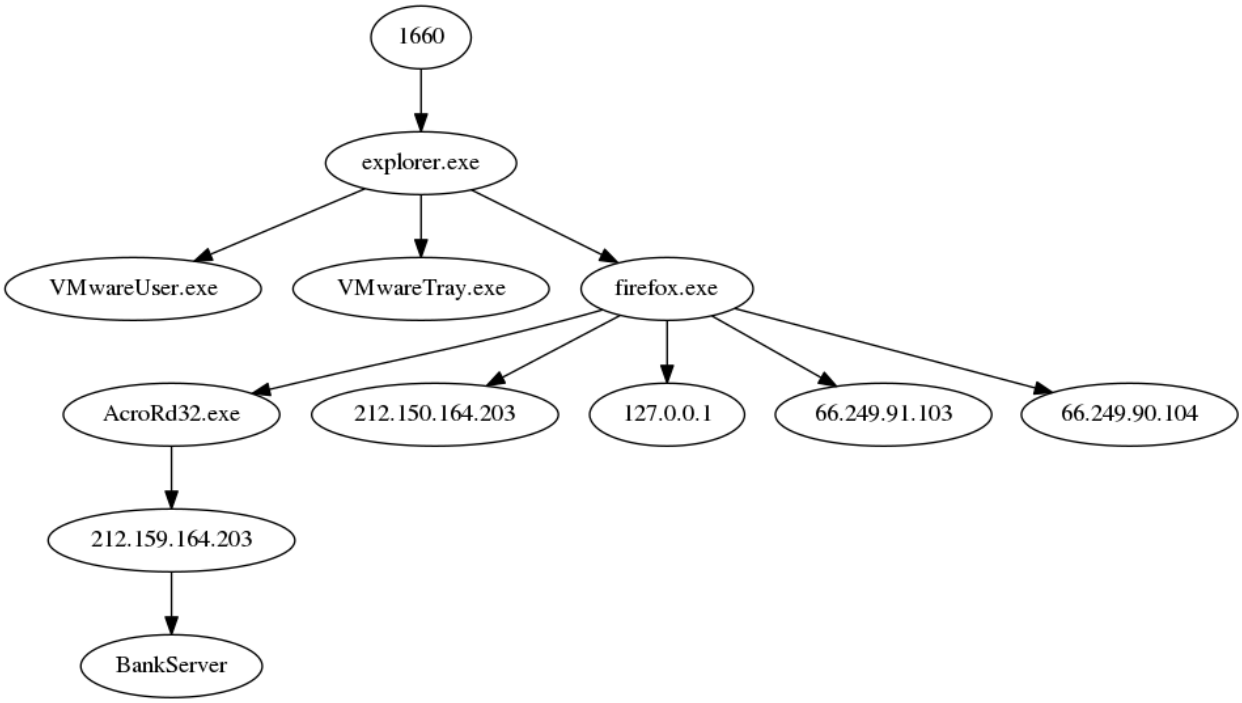

Figure B.4: An updated subgraph of Figure B.2.

Node ID	**Prior Probability Value**
explorer.exe	0.0769
firefox.exe	0.0769
AcrodRd32.exe	0.0769
212.150.164.203	0.7692
Bank Server	0.7692

Table B.7: The prior probability of each piece of evidence.

Yes	**No**	**Uncertain**
0.6366	0.4662	0.5571

Table B.8: The updated results from the evaluation.

APPENDIX C: CASE STUDY: W32.CRIDEX

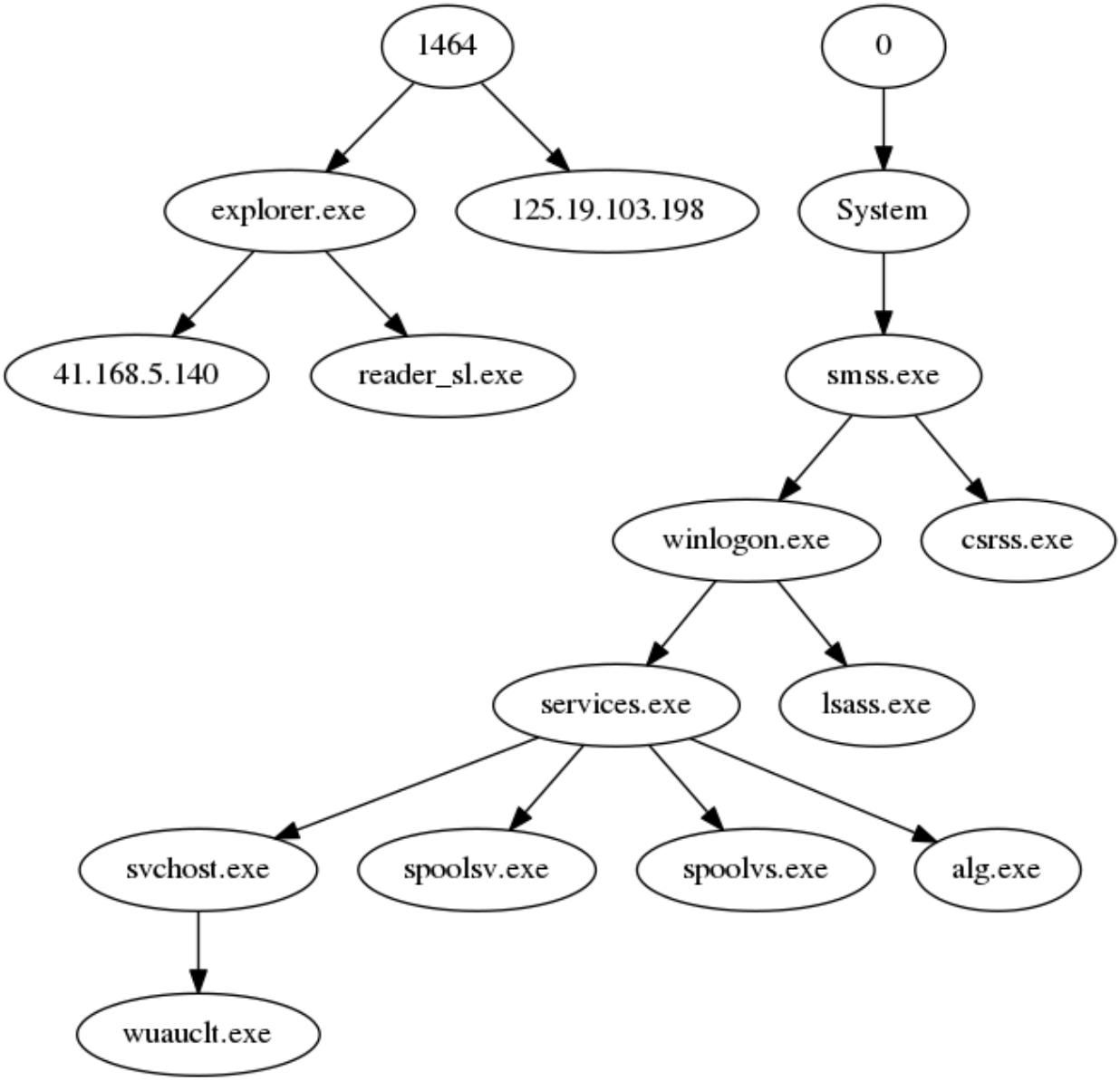

Figure C.1: A graph-based representation of the evidence.

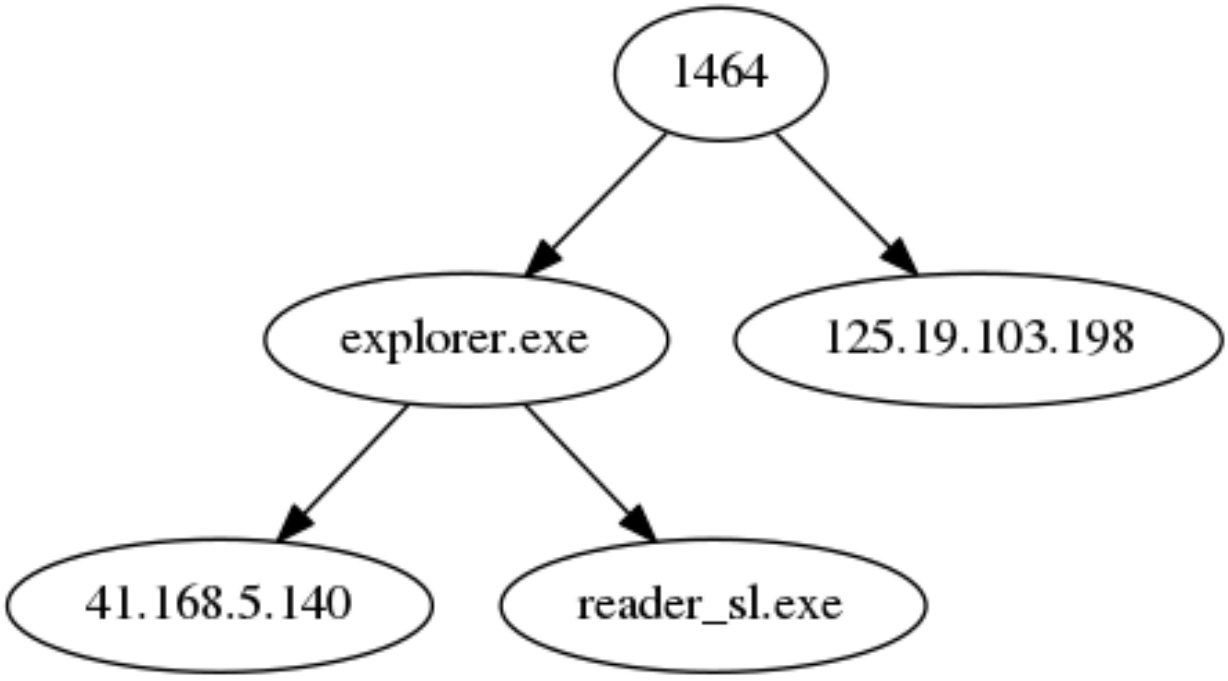

Figure C.2: A subgraph of Figure C.1.

Node ID	Hub Value
explorer.exe	0.9999
1464	2.5811e-09
41.168.5.140	0.0
reader_sl.exe	0.0
125.19.103.198	0.0

Table C.1: The hub value results from the hyperlinked-induced topic search from Figure C.2.

Node ID	PageRank Value
explorer.exe	0.2492
125.19.103.198	0.2053
41.168.5.140	0.2053
reader_sl.exe	0.2053
1464	0.1347

Table C.2: The results from the pagerank algorithm from Figure C.2.

Degree	Degree Probability
1	0.8
4	0.2

Table C.3: The results of the probability mass function for Figure C.2.

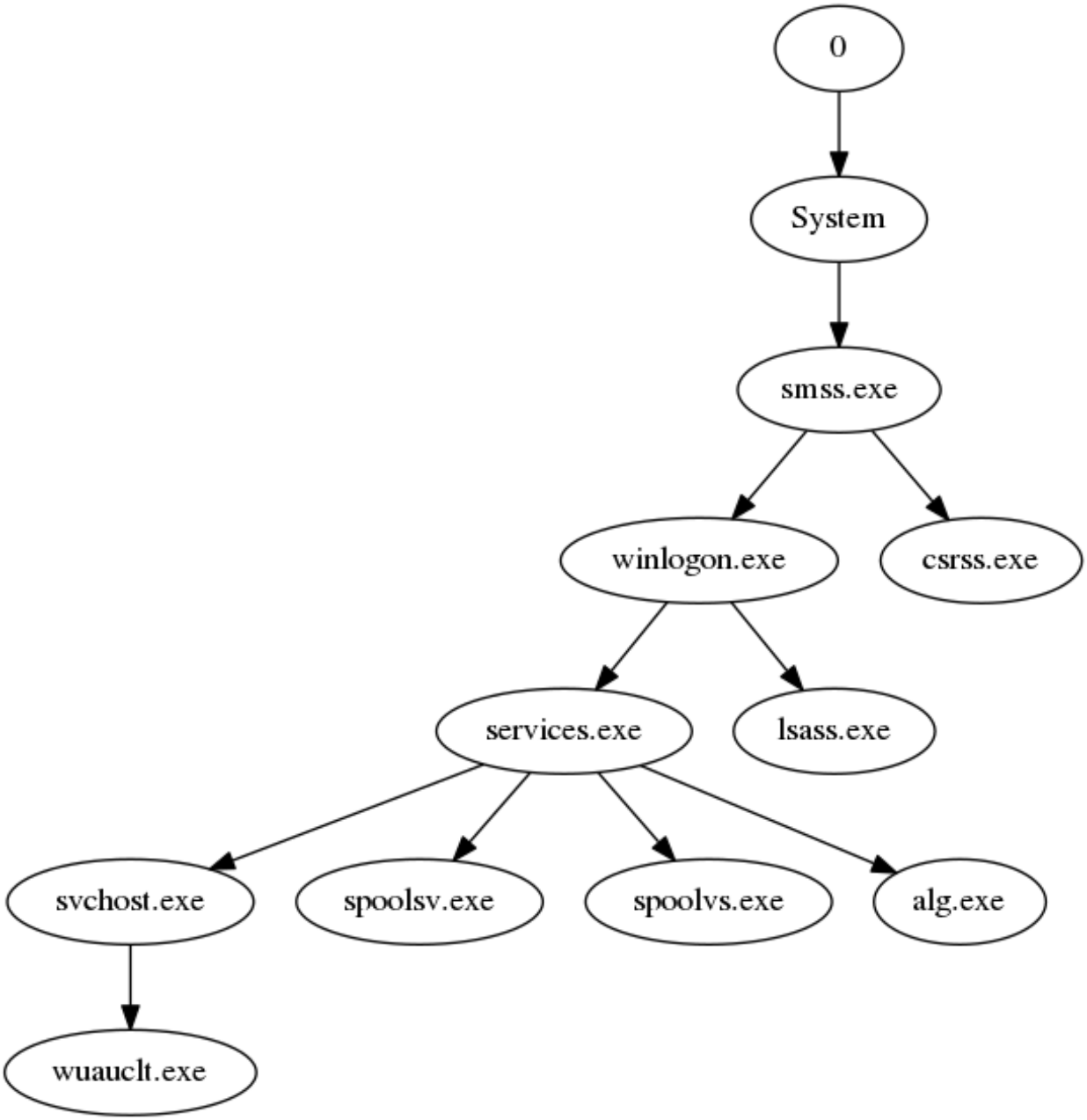

Figure C.3: A subgraph of Figure C.1.

Node	**Prior Probability Value**
explorer.exe	0.2
reader_sl.exe	0.8
41.168.5.140	0.8
125.19.103.198	0.8
1464	0.8

Table C.4: The prior probability for each piece of evidence.

Yes	**No**	**Uncertain**
0.027	0.0004	0.0004

Table C.5: The results from the evaluation.

APPENDIX D: CASE STUDY: WEBSITE PROBLEMS

CMD ID	Command
cmd1	ipconfig
cmd2	cls
cmd3	net user user1 user1 /add
cmd4	net user user1 user1 root@psut /add
cmd5	net user user1 Root@psut /add
cmd6	net /?
cmd7	net localgroup /?
cmd8	net localgroup “Remote Desktop Users” user1 /add
cmd9	netsh /?
cmd10	netsh firewall /?
cmd11	netsh firewall set service type = remotedesktop /?
cmd12	netsh firewall set service = remotedesktop enable
cmd13	netsh firewall set service type=remotedesktop mode=enable
cmd14	netsh firewall set service type=remotedesktop mode=enable scope=subnet
cmd15	netsh fireall set service type=remotedesktop mode=enable scope=subnet
cmd16	et.exe

Table D.1: The list of commands with their node identification labels shown in the Figures D.1.

Node ID	Hub Value	Node ID	Hub Value
explorer.exe	0.9999	services.exe	4.3789e-09
192.168.56.1	1.0253e-09	myslqd.exe	9.8977e-10
xampp-control.e	2.2989e-10	msdtc.exe	2.6843e-20
wininit.exe	2.6843e-20	472	2.6843e-20
516	2.6843e-20	svchost.exe	3.1498e-25
System	3.1498e-25	FTKImager.exe	3.1498e-25
676	3.1498e-25	0	0.0
taskeng.exe	0.0	lsm.exe	0.0
lsass.exe	0.0	SLsvc.exe	0.0
cmd.exe	0.0	httpd.exe	0.0
smsss.exe	0.0	csrss.exe	0.0
winlogon.exe	0.0	VBoxService.exe	0.0
spoolsv.exe	0.0	TrustedInstalle	0.0
FileZillaServer	0.0	cmd1	0.0
cmd2	0.0	cmd3	0.0
cmd4	0.0	cmd5	0.0
cmd6	0.0	cmd7	0.0
cmd8	0.0	cmd9	0.0
cmd10	0.0	cmd11	0.0
cmd12	0.0	cmd13	0.0
cmd14	0.0	cmd15	0.0
cmd16	0.0	0.0.0.0:0	0.0
:::0	0.0	*:*	0.0

Table D.2: The hub value results from the hyperlinked-induced topic search from Figure D.1.

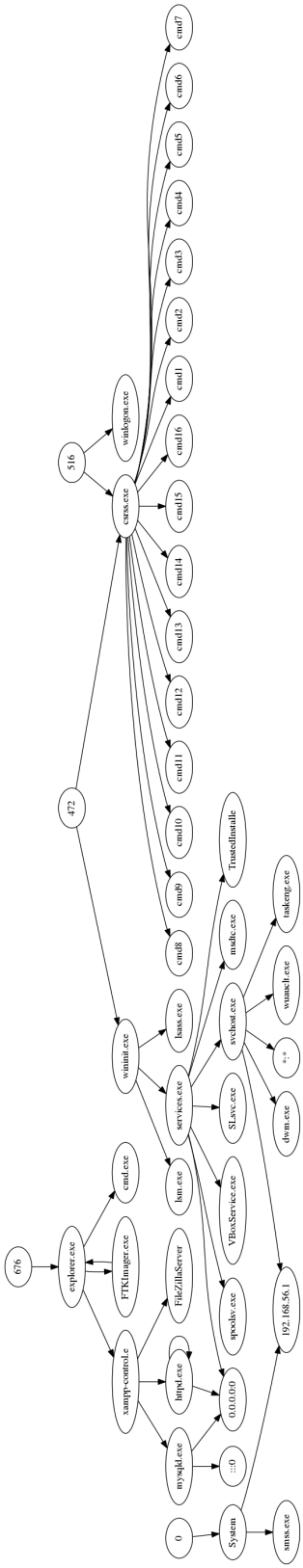

Figure D.1: A graph-based representation of the evidence.

Node ID	PageRank Value	Node ID	PageRank Value
explorer.exe	0.05468	0.0.0.0:0	0.0460
httpd.exe	0.0419	winlogon.exe	0.0378
xampp-control.e	0.0308	cmd.exe	0.0308
FTKImager.exe	0.307	csrss.exe	0.0284
System	0.0284	192.168.56.1	0.0274
smss.exe	0.0274	:::0	0.02653
mysqld.exe	0.0241	FileZillaServer	0.0241
:	0.0230	taskeng.exe	0.0230
wininit.exe	0.0219	lsass.exe	0.0215
services.exe	0.0215	lsm.exe	0.0215
spoolsv.exe	0.0179	msdtc.exe	0.0179
svchost.exe	0.0179	TrustedInstalle	0.0179
SLsvc.exe	0.0179	VBoxService.exe	0.0219
cmd1	0.0169	cmd2	0.0169
cmd3	0.0169	cmd4	0.0169
cmd5	0.0169	cmd6	0.0169
cmd7	0.0169	cmd8	0.0169
cmd9	0.0169	cmd10	0.0169
cmd11	0.0169	cmd12	0.0169
cmd13	0.0169	cmd14	0.0169
cmd15	0.0169	cmd16	0.0169
472	0.0153	516	0.0153
0	0.0153	676	0.0153

Table D.3: The results from the pagerank algorithm from Figure D.1.

Degree	Degree Probability
1	0.7111
2	0.0666
3	0.0888
4	0.0666
5	0.0222
8	0.0222
17	0.0222

Table D.4: The results of the probability mass function for Figure D.1.

Node	Prior Probability Value
explorer.exe	0.0666
xampp-control.e	0.0666
mysqld.exe	0.0666
httpd.exe	0.0888
FileZillaServer	0.7111
472	0.0666
csrss.exe	0.0222
cmd#	0.7111

Table D.5: The prior probability for each piece of evidence.

Yes	No	Uncertain
7.5844e-10	0.0	0.3296

Table D.6: The results from the evaluation.