2010

Judges' Awareness, Understanding, and Application of Digital Evidence

Gary Craig Kessler
Nova Southeastern University, kessleg1@erau.edu

Judges' Awareness, Understanding, and Application of Digital Evidence

by

Gary Craig Kessler

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Computing Technology in Education

Graduate School of Computer and Information Sciences
Nova Southeastern University

2010

We hereby certify that this dissertation, submitted by Gary C. Kessler, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

_____ _____

Marlyn Kemper Littman, Ph.D. Date
Chairperson of Dissertation Committee

_____ _____

Marcus Rogers, Ph.D. Date
Dissertation Committee Member

_____ _____

Ling Wang, Ph.D. Date
Dissertation Committee Member

Approved:

_____ _____

Leo Irakliotis, Ph.D. Date
Dean

Graduate School of Computer and Information Sciences
Nova Southeastern University

2010

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Judges' Awareness, Understanding, and Application of Digital Evidence

by
Gary C. Kessler

September 2010

As digital evidence grows in both volume and importance in criminal and civil courts, judges need to fairly and justly evaluate the merits of the offered evidence. To do so, judges need a general understanding of the underlying technologies and applications from which digital evidence is derived. Due to the relative newness of the computer forensics field, there have been few studies on the use of digital forensic evidence and none about judges' relationship with digital evidence.

This study addressed judges' awareness, knowledge, and perceptions of digital evidence, using grounded theory methods. The interaction of judges with digital evidence has a social aspect that makes a study of this relationship well suited to grounded theory. This study gathered data via a written survey distributed to judges in the American Bar Association and National Judicial College, followed by interviews with judges from Massachusetts and Vermont.

The results indicated that judges generally recognize the importance of evidence derived from digital sources, although they are not necessarily aware of all such sources. They believe that digital evidence needs to be authenticated just like any type of evidence and that it is the role of attorneys rather than of judges to mount challenges to that evidence, as appropriate. Judges are appropriately wary of digital evidence, recognizing how easy it is to alter or misinterpret such evidence. Less technically aware judges appear even more wary of digital evidence than their more knowledgeable peers.

Judges recognize that they need additional training in computer and Internet technology as the computer forensics process and digital evidence, citing a lack of availability of such training. This training would enable judges to better understand the arguments presented by lawyers, testimony offered by technical witnesses, and judicial opinions forming the basis of decisional law. A framework for such training is provided in this report.

This study is the first in the U.S. to analyze judges and digital forensics, thus opening up a new avenue of research. It is the second time that grounded theory has been employed in a digital forensics study, demonstrating the applicability of that methodology to this discipline.

Acknowledgements

Many people have helped me in significant ways to complete the research necessary for this study. I would like to start with five people who advocated on my behalf and made my data gathering possible: Judge Edward Cashman (ret.), Vermont District Court; Judge Herbert B. Dixon, Jr., Superior Court of Washington, D.C., Chair of the American Bar Association Judicial Division (ABA/JD) Court Technology Committee, and Technology Columnist for *The Judges' Journal*; William F. Dressel, President, National Judicial College (NJC); Christopher W. Kelly, Assistant Attorney General, Cybercrime Division, Commonwealth of Massachusetts; and Judge Barbara Lynn, President, ABA/JD. Without the encouragement and support of these individuals, this study would not have been completed.

I also, of course, thank the members of the ABA/JD and NJC who spoke with me and completed the research study survey. I owe a particular debt to the seven judges in Massachusetts and Vermont who took the time to allow me to interview them in person.

Ten of my professional colleagues (see Appendix A) agreed to act in an advisory capacity for this study. Their guidance in designing the surveys and validating results has been invaluable to the research study process and I thank them. I owe a particular debt to Bob Simpson, former Chittenden County (Vermont) State's Attorney, and Dr. Kieran Killeen, Assistant Professor of Education at the University of Vermont, both of whom gave me timely advice, information, and encouragement.

It was imperative to the integrity of this study that I receive survey results anonymously. I thank Julie Eldred and Melodie Woodward for ensuring that all personal identifying information was removed from surveys before I reviewed them.

My dissertation committee provided assistance throughout this process. I thank Dr. Marlyn Littman, my Dissertation Chair, for allowing me to do a research study that is a bit out-of-the-box. I also wish to thank my Dissertation Committee members, Dr. Marcus Rogers, for having been a mentor for many years, and Dr. Ling Wang, for guiding me through the Institutional Review Board process. I thank them all for their insightful comments on the project proposal and report.

My parents, Bernard and Mildred Kessler, and children, Joshua Kessler and Sarah Whitaker, have long inspired and encouraged me to do interesting things. Last, but not least, I thank my wife, Gayle Belin, for her love and encouragement throughout this process, and for being a patient editor. Final editing was done with the assistance of Dr. Sharon Bear, whose advice and suggestions are greatly appreciated.

This dissertation is dedicated to Mildred F. Kessler (1923-2010).

Table of Contents

Appendices

List of Tables

Table

List of Figures

Figure

Chapter 1

Introduction

This chapter presents an introduction to and an overview of the dissertation. The chapter begins with an overview of the literature on digital evidence and how this evidence can be introduced into court proceedings in the United States (U.S.). Then the factors affecting judges' understanding and application of digital evidence, the goals of the proposed research, and the additional concepts framing this study are presented. The chapter concludes with a summary.

An Introduction to Digital Evidence

Digital forensics combines computer science concepts, including computer architecture, operating systems, file systems, software engineering, and computer networking as well as legal procedures that describe criminal and civil litigation, cyberlaw, and rules of evidence (Kerr, 2009; Whitcomb, 2002). The digital forensics process encompasses identifying activity that requires investigating (including determining pertinent digital sources), collecting information, preserving the information from inadvertent changes, analyzing the information, and reporting the results of the examination (Casey, 2011; National Institute of Justice [NIJ], 2007; Palmer, 2002). Digital evidence (also called digital forensic evidence) is the product of the digital forensics process (Cohen, 2008, 2010).

Digital evidence comes from a variety of sources including computing devices (e.g., desktop and laptop computers, digital cameras, music players, personal digital assistants [PDAs], and cellular telephones); network servers (e.g., supporting applications such as Web sites, electronic mail [e-mail], and social networks); and network hardware (e.g., routers found in businesses, homes, and the backbone of the Internet) (Brown, 2010; Casey, 2011; NIJ, 2007). Information of evidentiary value may be found on digital media such as compact discs (CDs), digital versatile discs (DVDs), floppy disks, thumb drives, hard drives, and memory expansion cards found in digital cameras and mobile phones (Brown; Casey; NIJ).

To make informed and proper decisions about the acceptability of digital evidence sources and expert testimony, judges and other judicial panels must be knowledgeable in a variety of information and communication technology (ICT) areas (Casey, 2011; Frowen, 2009). All too often, however, this knowledge is based not on formal training and education but on personal experiences involving the use of computers and networks such as the Internet (Cohen, 2008, 2010; Losavio, Adams, & Rogers, 2006).

In any investigation for which the government seizes property for examination and analysis, the Fourth Amendment to the U.S. Constitution and similar language in every state's constitution require that a search warrant be issued; subsequent decisional law describe exceptions to the search warrant requirement (Kerr, 2009). This initial contact with digital evidence requires that judges have familiarity with the application of the Fourth Amendment and state constitution rules to digital devices (Kerr, 2010). In addition, judges must be able to balance the imperatives of a thorough examination with the needs of a speedy trial (Casey, Ferraro, & Nguyen, 2009).

Most people are not consciously aware of the impact that digital devices and the large volume of data stored in digital repositories have on everyday life (O'Harrow, 2006). As examples of this impact, consider automated operations and functions within computer-controlled buildings, utility company facilities, and telecommunication carrier networks; data gathered by security systems, closed-circuit television, surveillance cameras, and automobiles; and online activities such as e-mail, online payment systems, and social networks (O'Harrow). As a consequence of the increasing use of ICTs that, a few years ago, were used only by technologists and the increasing depiction of computer technology in the popular media, technology users have an overly simplistic or incorrect understanding of how these ICTs work (Del Bosque & Chapman, 2008). For this reason, it may be quite difficult for individuals to apply critical analysis to statements based on digital forensic evidence offered as fact in a courtroom (Dinat, 2004; Mason, 2008). Mason presented several examples of these complex situation, including:

- A judge is presented with network server logs showing a cyberintruder coming from a particular Internet Protocol (IP) address. Internet service provider (ISP) records show that the IP address in question was assigned to a computer system at a particular residence at the time of the incident. This information could be used to improperly identify an individual as a wrongdoer.
- A judge is presented with call history and service provider records showing that one mobile telephone was used to place a call to another mobile phone. The court and a jury might erroneously believe that this evidence conclusively proves that the owners of the two telephones actually had a conversation.

- Metadata in a Microsoft Word document include the name of the person who ostensibly registered the product. Unless that information is deliberately deleted or altered, the name will appear in every document generated by the Office application. A judge might erroneously conclude that the metadata in a given document conclusively proves that the named person is the actual author.
- The presence of a bona fide digital signature on an electronic document (e-document) might be accepted by a judge as proof that the signature's owner actually sent the document in question. If the digital signature program is compromised, the signing function can be manipulated. If this is not understood by the trier-of-fact, a forged document might inadvertently be accepted as legitimate.

Forensics refers to the application of scientific evidence in courts of law. Judges play a gatekeeper role in determining what scientific evidence is and is not admissible in their courtrooms (Cohen, 2008, 2010; Jones, 2009; Kerr, 2009). Rule 702 of the Federal Rules of Evidence (FRE) provides guidance to courts about qualifying expert testimony and places the particular burden of ensuring that scientific testimony is both relevant and reliable on judges (U.S. Courts, 2008c). The *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1993) decision describes a four-pronged test to determine whether science-derived evidence is admissible in U.S. Federal Court. The *Daubert* test applies to any scientific procedure used to prepare or uncover evidence and comprises the following four factors (*Daubert*, 1993):

- Testing: Can and has the scientific procedure been independently tested?

- Publication: Has the scientific procedure been published and subject to peer review?
- Error rate: Is there a known error rate, or potential to know the error rate, associated with the use of this scientific procedure?
- Acceptance: Is the scientific procedure generally accepted by the relevant scientific community?

Prior to *Daubert*, judges were guided by the *Frye v. United States* (1923) decision, which required that scientific evidence presented at a trial had to be derived from a method that was generally acceptable within the relevant scientific community but left it to the judges to make their own determination of general acceptance. The *Daubert* reliability test provides judges with an objective set of guidelines for accepting scientific evidence. The *Kumho Tire v. Carmichael* (1999) decision extends the *Daubert* guidelines to any form of technical evidence.

FRE Rule 702 provides guidelines for qualifying expert witnesses and minimizing adversarial bias in expert testimony (U.S. Courts, 2008c). As an aside, the Rule 702 requirement for reliability can actually work against the rule's design to balance the imperatives of maintaining an adversarial system and mitigating bias. In particular, Rule 702 can be used to prevent speculation by an expert that a judge might find useful because speculation cannot be shown to be reliable (Bernstein, 2008).

Although *Daubert*, *Kumho*, and Rule 702 apply specifically to courts at the federal level, similar guidelines are in use in over half of the states in the U.S., another third use the *Frye* standard, and the remaining states use some variant of these evidentiary rules (Kaufman, 2006). The Federal Rules of Civil Procedure add additional guidance in

delineating how digital evidence must be collected for use in civil litigation (U.S. Courts, 2008a; Zittrain, 2006).

The American Academy of Forensic Sciences (AAFS) identifies digital forensics as a forensic science (AAFS, 2008). Although the actual mechanics of digital forensics differ from the better-known physical and medical forensics, the processes of all forensic sciences are fundamentally the same: detection, preservation, collection, examination, analysis, and reporting (Casey, 2011; Palmer, 2002). Each phase in the process must be performed in such a manner so as to preserve the integrity of the evidence and assure its admissibility (Casey). Just as judges need to eliminate junk science from the courtroom, they also need to keep out poor-quality digital evidence (Cohen, 2008, 2010). Thus, the *Daubert* test and Rule 702, plus a plethora of additional laws, apply to digital evidence as well as other types of scientific evidence (Ieong, 2006; Meyers & Rogers, 2006; Noblett, Pollitt, & Presley, 2000; Rothstein, Hedges, & Wiggins, 2007).

Problem Statement and Goal

Problem Statement

The paucity of research related to judges and digital evidence does not provide a sufficient base from which to generate a hypothesis that could be tested in the present research (Beebe, 2009; Carlton, 2007; H. B. Dixon, Jr., personal communication, February 21, 2009; Rogers, Scarborough, Frakes, & San Martin, 2007; Scarborough, Rogers, Frakes, & San Martin, 2009). As a result, the researcher gathered basic data related to judges' knowledge about the digital evidence that they see in their courtrooms and use as the basis for decisions and opinions that are rendered from the bench. In

particular, the researcher gathered data about judges' awareness (i.e., do they know what exists?), understanding (i.e., do they have knowledge of the underlying ICTs?), and application (i.e., can they determine reliability, relevance, and veracity?) of digital evidence (Ball, 2008). Achieving this level of understanding can be accomplished only with specialized training and education (Ball, 2008; Galves, 2000). Such training must focus on what judges need to make them better able to apply legal standards to evidence (Carlton, 2007; NIJ, 2007; Rogers et al., 2007; Scarborough et al., 2009).

Goal

The goal of this study is to determine the factors influencing and informing judges as they evaluate digital evidence for admissibility at trial and interpret such evidence in their rulings. As such, this researcher sought to identify gaps between judges' understanding of ICTs underlying digital evidence and the perceived importance of such evidence in courts (Losavio, Adams, & Rogers, 2006; Rogers et al., 2007; Scarborough et al., 2009). Identifying such gaps provides a prioritized list of subject matter with which to design specialized judicial training and education programs (H. B. Dixon, Jr., personal communication, February 21, 2009; Rogers et al.; E. Zide, personal communication, November 12, 2008).

An additional goal is to provide a foundation and model for future research. According to the fundamentals of grounded theory, the themes that emerged from the answers to these questions and reported here will lead to subsequent analysis to build a framework with which to better understand the ways in which judges interact with digital evidence and to create a body of baseline data for future researchers (Charmaz, 2006; Dick, 2005; Pogson, Bott, Ramakrishnan & Levy, 2002; Robson, 2002; Schram, 2006).

Relevance and Significance of This Study

Judges decide what evidence will or will not be allowed in their courtrooms. As a consequence, in evaluating scientific and technical evidence, judges must make informed decisions about the admissibility of such evidence at trial (Wegman, 2005). In addition, judges must determine the acceptability of expert witnesses who might testify about scientific and technical issues (Ball, 2008). However, there is scant literature that describes how judges make these decisions (Carlton, 2006, 2007; Losavio, Adams, & Rogers, 2006; Rogers et al., 2007; Scarborough et al., 2009).

The vast majority of criminal charges result in a plea agreement and civil complaints in a settlement rather than a trial before a judge and jury; therefore, judges often have less direct experience with digital evidence than do attorneys representing plaintiffs, defendants, and the state (E. Cashman, personal communication, July 24, 2010; R. Simpson, personal communication, July 23, 2010). Since evidence from digital sources can be compelling, particularly when images are involved, cases with a substantial amount of digital evidence are even less likely to go to trial (Ball, 2008). Prosecutors and defense attorneys see significantly more digital evidence than do most trial judges and, as a result, have more familiarity with it (Casey, 2011; Carlton, 2006; Rogers et al., 2007).

In seminal papers, Marsico (2004) and Van Buskirk and Liu (2006) observed that, even when digital evidence and expert computer-related testimony are introduced, defense attorneys, particularly in criminal trials, rarely raise a challenge based upon *Daubert* grounds of reliability (i.e., authentic and dependable), accuracy (i.e., correct and

free from mistakes), and veracity (i.e., truthfulness). To date, no research has refuted these assertions or proven them otherwise.

This absence of challenges leaves judges with little opportunity to make decisions about the admissibility or authenticity of digital evidence (Marsico, 2004; Van Buskirk & Liu, 2006). Indeed, in some states, it is possible for a computer forensics report to be allowed into evidence even in the absence of a requirement that the report's author be available for cross-examination (Balko, 2009; *Melendez-Diaz v. Massachusetts*, 2009). As Neufeld (2005) stated, "If no one challenges the speculative science or scientist, there is nothing for a gatekeeper to tend to. Thus, the principal failing of *Daubert* is its misplaced reliance on a robust adversarial system to expose bad science" (p. S110).

Computers, e-mail, the Internet, mobile devices, and Web-based services are in widespread use throughout the world and are nearly ubiquitous in industrial nations (Crespo-Cuaresma, Foster, & Scharler, 2008). Losavio, Adams, and Rogers (2006) found that judges who are ICT aware tend to be more willing to accept digital evidence in their courts than are their peers who are less ICT. However, Losavio et al. did not explore whether judges had a sound understanding of the technology underlying the evidence or merely accepted the evidence due to their comfort with the technology.

Rogers et al. (2007) found that judges in larger courts and in jurisdictions with a higher population generally have greater familiarity with ICTs and, as a result, are more willing to admit digital evidence than are their counterparts with less familiarity with ICTs (Scarborough et al., 2009). Both Rogers et al. and Scarborough et al. suggested that judges in larger population centers were more familiar with the technology because they

have greater access to computers and to broadband network services, although their studies did not provide sufficient data to specifically support that conclusion.

Caloyannides (2003) and Van Buskirk and Liu (2006) have independently stated that most judges who accept digital evidence also tend to give that evidence a presumption of reliability that is possibly unwarranted. This high level of credibility attached to digital evidence may be due to the judges' lack of understanding of how the evidence is derived and, therefore, how the evidence might be altered, manipulated, or otherwise be open to misinterpretation (Caloyannides; Van Buskirk & Liu). Together, these studies suggest that the acceptance of digital evidence at trial is correlated to a judge's comfort with ICT and that judges who readily admit digital evidence generally accept that evidence as reliable.

Adding to how digital evidence factors in a trial is the role of juries. Shelton (2009) and Shelton, Kim, and Barak (2009) conducted empirical studies of jurors' expectations of seeing scientific and technical evidence in court. Their studies investigated the impact of what is known as the *Crime Scene Investigation (CSI) Effect* (i.e., asking whether judges and juries want to see more of the types of evidence that they see on popular television shows such as *CSI*, *Law & Order*, and *NCIS*). While the aforementioned researchers claimed that the television shows are not a major factor with today's juries, they observed that, due to the introduction of technology-derived evidence over the last two decades, juries increasingly expect to see technical evidence at trial and are often reluctant to convict a defendant without it (Shelton; Shelton, Kim, & Barak).

An understanding of judges' knowledge and awareness is important if they are to make decisions about the admissibility of digital evidence in terms of reliability, veracity,

and accuracy (H. B. Dixon, Jr., personal communication, February 21, 2009; E. Zide, personal communication, November 12, 2008). Indeed, statements about judges and digital evidence found in several peer-reviewed papers (e.g., Caloyannides, 2003; Marsico, 2004; Van Buskirk & Liu, 2006) and research studies (e.g., Losavio, Adams, & Rogers, 2006; Losavio, Wilson, & Elmaghraby, 2006; Rogers et al., 2007) are more than three years old because no subsequent publication has either refuted or substantiated those assertions; thus, these older papers remain the most current literature.

Although law enforcement officers, prosecutors, and defense attorneys may specialize in computer forensics and digital investigations, few, if any, judges do (H. B. Dixon, personal communication, November 16, 2008; N. L. Waters, personal communication, November 20, 2008). Thus, judges are not inherently more knowledgeable about matters related to science and technology than are other participants in the judicial system, and judges may need to educate themselves about those topics as warranted by the cases over which they preside (E. Cashman, personal communication, July 24, 2010; Losavio, Wilson, & Elmaghraby, 2006; R. Simpson, personal communication, July 23, 2010; Van Buskirk & Liu, 2006). The goal of the present study, then, was to determine an approach for enabling judges to achieve the appropriate level of technical knowledge necessary for accepting, understanding, and interpreting digital evidence, while remaining true to the *Daubert* and Rule 702 proscriptions of accuracy, veracity, and reliability (Ball, 2008).

According to Rogers et al. (2007), future research is needed in the area of judges and digital evidence "to implement broad initiatives that raise the level of expertise of state and local law enforcement agents (as well as attorneys and judges) to ensure that digital evidence is introduced routinely and successfully in legal proceedings" (p. 50). In this

investigation, the researcher studied judges' knowledge, understanding, and application of digital evidence, thereby responding to that need.

Barriers and Issues

A study of judges' perceptions about digital evidence has not been previously accomplished because the digital forensics research field has been, in large part, ill-defined. Specifically, the digital evidence domain still lacks a universally accepted definition, foundational research, and a substantial body of literature (R. B. Vaughn, personal communication, July 22, 2010). Further, recent efforts to define a research agenda for the digital forensics community involved an examination of technical issues such as network forensics, evidence modeling, and mobile devices rather than social aspects such as the understanding of digital evidence (Beebe, 2009; Nance, Hay, & Bishop, 2009).

Although computer forensics has been an area of active investigative practice by law enforcement (LE) for over 15 years, the use of digital evidence in court is still not widespread (Marsico, 2004; Rogers et al., 2007; Van Buskirk & Liu, 2006). As noted below, the reasons are varied and broad. Digital investigations are still not routinely taught in most police academies (Carlton, 2006; Rogers et al.); law schools and judicial colleges are just starting to emphasize digital evidence (Ball, 2008; Rogers et al.; Van Buskirk & Liu); the formal study of computer forensics, digital investigations, and cybercrime remains a relatively new academic discipline (Carlton); and the under-capacity of most LE agencies to examine all computers that could be seized results in an underuse of digital evidence (Rogers et al.).

As a consequence, a major barrier to this research was that similar studies have not been conducted with this target population. Establishing a credible research plan and building a trusting relationship with a group of judges to obtain candid insights about what they know, do not know, and believe that that they need to know about digital forensic evidence and computing technology was the largest hurdle in conducting this investigation (Ball, 2008; H. B. Dixon, Jr., personal communication, July 31, 2009; W. F. Dressel, personal communication, August 1, 2009; Mack & Anleu, 2008). Specifically, due to their high social status, concerns about confidentiality, professional aloofness, and reticence to participate in studies that might show areas in which they are intellectually weak, judges can be a difficult population from which to elicit information (H. B. Dixon, Jr., personal communication, February 21, 2009; Rogers et al., 2007; N. L. Waters, personal communication, December 10, 2008; E. Zide, personal communication, November 12, 2008). According to Mack and Anleu (2008), these same factors also directly influence the lack of research involving judges and their views of digital evidence.

Research Questions Investigated

The research questions for this investigation related to judges' attitudes about digital evidence. Specifically, research was performed in the areas of awareness, knowledge, and application of digital evidence. Any presuppositions about judges' attitudes held by the researcher were set aside; instead, the researcher conducted this study to gather baseline data about what those attitudes are.

For the investigation, the researcher utilized qualitative grounded theory methodology to gather data. The study examined several specific aspects of judges' attitudes about digital evidence, including those suggested from earlier studies by Losavio, Adams, and Rogers (2006), Rogers et al. (2007), and Scarborough et al. (2009). The questions below provided the guiding principles by which to design the data gathering instruments:

1. What issues do judges face when deciding on admissibility issues related to digital evidence?

2. To what standard of authentication do judges hold digital forensic evidence compared to traditional physical forensic evidence?

3. In what kind of cases are judges expecting digital evidence to be offered at trial and what kinds of digital evidence are they expecting in these cases?

4. What factors lead to effective presentation of digital evidence in hearings and trials?

5. What information do judges require in order to establish the reliability of testimony related to digital evidence?

6. How do judges rate their own familiarity with digital evidence, the digital forensics process, ICTs, and Internet applications; what factors affect their self-rating; and how do judges compare their own familiarity to that of their peers?

7. To what standard of competence do judges hold attorneys who are presenting digital evidence?

Assumptions, Limitations, and Delimitations

There were several assumptions, limitations, and delimitations associated with this investigation. Inasmuch as participation in the study was voluntary and limited to active trial judges, the researcher assumed that study participants had a genuine interest in the outcomes of the research, would provide candid responses, and had basic familiarity with the rules of evidence.

The researcher also assumed that the comfort level of participants was more important than obtaining data for the study. This assumption is a fundamental tenet of grounded theory (Charmaz, 2006).

Several factors were not under the researcher's control but may have affected the internal validity of the study. All participants were self-selected, and thus might not be truly representative of the total population of judges (Carlton, 2006; Terrell, 2006). Participants who completed the questionnaire were members of the American Bar Association Judicial Division (ABA/JD) and/or the National Judicial College (NJC), both national organizations of judges; as such, they might not be truly representative of the total population of judges in the U.S. (Carlton; Terrell). All participants were volunteers and could drop out at any time, potentially biasing the results (Carlton). Finally, at least some members of the judiciary expressed reluctance at having their opinions and views analyzed or felt, at least at the beginning of the study period, that interviews for this research were inappropriate (H. B. Dixon, personal communication, November 16, 2008; L. Suskin, personal communication, February 14, 2008). For this reason, a study involving judicial knowledge of a particular subject matter was not universally welcomed (Mack & Anleu, 2008).

The primary delimitation in this proposal concerned the target study population. The participants in the written survey (Phase 1) were judges at various levels of the judiciary from across the U.S., while interview subjects (Phase 2) were state trial and appellate court judges from Massachusetts and Vermont.

Definition of Terms

This section contains the legal, technical, and other conceptual terms used in this dissertation that are important to understanding the research.

Application of digital evidence. This refers to the ability to properly identify the role that digital evidence plays in the decision-making process related to admissibility and the legal process (Casey, 2011; Cohen, 2008, 2010).

Awareness of digital evidence. This refers to one's familiarity with the existence, various types, and sources of digital evidence (Casey, 2011; Cohen, 2008, 2010).

Best evidence. According to the best evidence rule, original documents and records must be submitted as evidence in court; thus, copies of documents are generally not accepted as evidence. If the original version of a document is unavailable due to no fault of the party offering the evidence, then the court can accept copies if those copies can be authenticated (U.S. Legal, 2010). This is often the case today because the majority of records, including credit card bills and bank statements, are produced and distributed in hard copy but stored electronically, and the paper copies are typically destroyed. When the original paper records are destroyed, the electronic record (e-record) is the best evidence, although the burden falls on the record holder to prove that the electronic copy (e-copy) matches the original (Kerr, 2009; Mason, 2008).

Computer forensics. This is used synonymously with the term *digital forensics* (Casey, 2011), which is defined below.

Constructivist theory. This is a branch of learning theory that is based on the belief that individuals learn new subject matter by applying new information to the body of knowledge which they already possess. New ideas and concepts are learned within the context of *a priori* knowledge and understanding (Phillips & Soltis, 2004).

Daubert reliability test. This refers to a four-pronged test guiding the acceptance of scientific and technical evidence in U.S. federal courts, which is employed by about half of the states. The four parts of the *Daubert* reliability test involve demonstrating (a) a repeatable procedure, (b) a known (or knowable) error rate of the procedure, (c) peer-reviewed publication of the procedure, and (d) peer acceptance of the scientific procedure used to present or uncover the evidence (Casey, 2011; *Daubert*, 1993; Kerr, 2009; *Kumho Tire*, 1999).

Digital evidence. Digital devices and network servers store and transport information in discrete values, as zeros and ones. This information is always stored electronically (Stallings, 2007). Digital evidence (also called *computer forensic evidence* or *digital forensic evidence*) refers to information offered at legal trials to aid in the legal decision-making process, which is derived from digital sources and the digital forensics process. Digital sources include contents of computing devices such as laptop and desktop computers, music players, cameras, PDAs, and mobile phones; logs from telecommunication network components such as routers and servers; and records from network service providers such as wireline and/or wireless telephone and data service providers and ISPs (Casey, 2002; Cohen, 2008, 2010). The term *digital evidence* is often

used synonymously with *electronic evidence* (*e-evidence*). Although the two terms are slightly different, the distinction, for purposes of this study, is irrelevant and neither term has any formal legal definition (Kerr, 2009; Mason, 2008).

Digital forensics. This refers to the forensic science related to the identification, preservation, acquisition, examination, analysis, and reporting of evidence from digital sources, and to the presentation of digital evidence in courts of law (AAFS, 2008; Casey, 2011; Cohen, 2008, 2010; Palmer, 2002).

Digital signature. This is a cryptography-based authentication scheme that acts in the digital world as the equivalent of a handwritten signature on a paper document. This method allows a person or organization to securely prove one's identity to another person or organization while communicating over an unsecure communications network such as the Internet (PGP Corporation, 2008).

Evidence. This refers to information that can be introduced at trial to help judges and juries make a decision in criminal and civil legal cases. The court has to balance the probative value of the evidence (i.e., whether the information has relevance to the case and can help prove or disprove a fact or question in dispute) against the potential prejudicial nature of the evidence (i.e., whether the information will unfairly influence the judge or jury) (Cohen, 2008, 2010; Kerr, 2009; U.S. Legal, 2010).

Fact-finder. At a trial, the fact-finder is the person or body responsible for listening to testimony and reviewing evidence to determine the facts of the case. In a jury trial, the jury is the fact-finder; in a bench trial, the judge is the fact-finder (U.S. Legal, 2010).

Forensics. This is the application of scientific or technical methods to the detection, examination, and presentation of evidence in civil and criminal legal proceedings (Saferstein, 2009).

Gatekeeper. Judges are considered gatekeepers. They determine what evidence is allowed in their courtroom following rules of evidence appropriate to their court; federal courts, for example, follow the FRE (U.S. Courts, 2008c), and local courts follow rules of evidence for their state or jurisdiction. Judges also are responsible for keeping inappropriate evidence, such as irrelevant, unreliable, and/or overly prejudicial evidence, out of the court (Jones, 2009; Kenneally, 2001b; Kerr, 2009).

Information and communication technologies (ICTs). This is an umbrella term referring to computer, telephone, and other communication device technologies; information stored on and transmitted between communication devices; and the networks that transport information (International Telecommunication Union, 2009).

Metadata. Sometimes described as *data about other data*, this term refers to descriptive information about computer files. Metadata might describe how, when, and by whom a particular file was received, created, accessed, and/or modified; how the file is formatted; and the type of content in the file (Brown, 2010; Casey, 2011). Some metadata, such as file dates and sizes, can easily be seen by the user of the computer, while other metadata is embedded in file locations requiring special software tools or user knowledge to be revealed. Metadata information is generally not reproduced in full form when a document is printed (Brown; Casey).

Rule 702. FRE Rule 702 guides judges as to the admissibility of expert testimony and specialized types of evidence including scientific and technical evidence (U.S. Courts, 2008c).

Trier of fact. In a court case, the trier of fact determines what the facts are and makes a decision based on those facts. A jury is the trier of fact in a jury trial, and a judge is the trier of fact in a bench trial. Trier of fact is also referred to as a *finder of fact* or *fact-finder* (Kenneally, 2001b; Kerr, 2009).

Understanding of digital evidence. This refers to the comprehension and ability to understand digital evidence, including knowledge of the underlying technologies from which the digital evidence was derived (Casey, 2011; Cohen, 2008, 2010).

Summary

Digital evidence has been offered in an increasing number of criminal and civil court cases over the last decade (Brown, 2010; Cohen, 2008, 2010; Kerr, 2010). Digital evidence must meet the standards of other scientific and technical evidence to be admissible in court (*Daubert*, 1993; *Kumho Tire*, 1999; U.S. Courts, 2008c). Judges and juries make decisions based upon their understanding of evidence that is presented at trial (Kerr, 2009). Familiarity with ICTs due to the everyday use of computers, the Internet, mobile phones, and other digital devices and network services might be interpreted by a fact-finder as understanding how evidence is derived from these digital sources (Losavio, Adams, & Rogers, 2006; Rogers et al., 2007; Scarborough et al., 2009). An understanding of how digital evidence is derived is a critical factor in weighing the

probative and prejudicial value of this evidence when introduced in court (Cohen, 2008, 2010; Frowen, 2009; Kerr, 2009).

Chapter 2

Review of the Literature

According to Saferstein (2009), forensics is the application of science to the detection, examination, and presentation of evidence in legal proceedings. Various disciplines of forensic science, such as toxicology, physics, and chemistry, provide a physical context by which to understand the evidence (Saferstein). Indeed, the evaluation of scientific evidence requires an understanding of the scientific method to apply the *Daubert* principles, although proper application of *Daubert* does not require one to be a scientist (Saferstein; N. L. Waters, personal communication, December 2, 2008). Digital evidence has a different context than do other forms of forensic evidence because it exists only in the form of zeros and ones, whereas other evidence has a physical manifestation (Kerr, 2005a, 2005b). This difference means that digital evidence is perceived and understood differently by judges and juries than is physical evidence and requires different treatment in terms of handling and explanation (Kerr; Saferstein).

This chapter presents a review of literature on key issues surrounding digital evidence, including its prevalence, characteristics, and reliability. Also included is the literature on grounded theory and its applicability to research related to technical topics such as digital forensics.

Literature Related to the Study of Digital Evidence

During the last three months of 2008, the researcher conducted a literature search related to judges' knowledge and understanding of digital forensic evidence and the extent to which judges understand the technologies underlying evidence derived from computers, the Internet, and other digital sources. The literature search utilized several computer science, criminal justice, and education databases, including the Association for Computing Machinery (ACM) Digital Library, EBSCOhost's Computers and Applied Sciences Complete, Education Resources Information Center (ERIC), Institute of Electrical and Electronics Engineers (IEEE) Computer Society Digital Library, National Criminal Justice Reference Service, and ProQuest's Criminal Justice Periodicals. These databases, as well as Google Scholar, were reviewed again during the first three months of 2010. The researcher found no articles about judges' knowledge and understanding of digital evidence.

The computer forensics literature base itself is still small, with no dedicated journals prior to 2002 (E. O. Casey, personal communication, July 23, 2010). The researcher has examined all issues to date of *Digital Investigations*, *International Journal of Digital Evidence*, *Journal of Digital Forensics, Security and Law*, and *Journal of Digital Forensic Practice* as well as all of the proceedings of the *Digital Forensics Research Workshops* and *International Federation of Information Processing (IFIP) Working Group 11.9 on Digital Forensics* meetings. None of these publications contains papers specifically about judges and their attitudes about digital evidence.

Google was also employed to search for information. While some blog postings were found, no substantive or peer-reviewed research studies were found related to this topic.

In this section, the literature on several aspects of digital evidence is provided as a foundation for examining how judges relate to and interact with this type of information.

Prevalence of Digital Evidence

Digital evidence plays an ever-increasing role in local, state, and federal courts in the U.S. (NIJ, 2007). Nevertheless, digital evidence is not universally used at the local and state level (Marsico, 2004; Rogers et al., 2007; Van Buskirk & Liu, 2006). In the U.S., computing devices such as laptop and desktop computers, mobile telephones, PDAs, and portable music players are nearly ubiquitous. Since the turn of the century, these devices have become increasingly the target, record keeper, and/or instrument of all types of illegal activities and, therefore, the source of a growing amount of evidence in criminal and civil court proceedings (Casey, 2011; Ieong, 2006; Volonino, 2003). The Federal Bureau of Investigation (FBI), for example, reports that nearly 80% of their cases involve some form of digital evidence, and the number is even higher for the U.S. Secret Service (Rogers et al., 2007). While the FBI, Secret Service, and other federal agencies respond to this growing need with well-trained and well-funded cybercrime units, the response at the local level is comparatively slight because most local law enforcement agencies in the U.S. have one (or no) investigator assigned to computer crimes (NIJ, 2007; Scarborough et al., 2009).

Managing the growing volume of digital evidence is even more daunting in civil litigation. With the pervasive use of e-mail in the corporate world, computer forensics has long been considered one of the most important processes in civil cases (Bensen, 2004). At least one-quarter of Fortune 10000 companies have had to turn over e-mail in response to a civil lawsuit or regulatory investigation (Manes, Downing, Watson, &

Thrutchley, 2007). Indeed, electronic discovery (e-discovery) is one of the fastest growing subdisciplines of computer forensics and is rapidly becoming the most costly part of civil litigation (Mack, 2008).

The growing popularity of mobile devices such as cell phones, PDAs, and digital cameras has made them so ubiquitous that such devices are found at nearly every arrest and crime scene. Increasingly, these devices contain information related to criminal activity (Losavio, Wilson, & Elmaghraby, 2006; Mislan, Casey, & Kessler, 2010). Digital devices are widely used by all segments of the population; are the source of a growing amount of evidence; and employ processing, storage, and communication technologies that are not fully understood by most users (Leroux, 2004; Losavio et al.; Van Buskirk & Liu, 2006).

Characteristics of Digital Evidence

According to constructivist learning theory in education, a person's learning, understanding, and perception of new ideas and concepts are generally integrated within the context of the things that he or she already knows and understands (Phillips & Soltis, 2004). Attempting to learn about the digital world based upon one's knowledge of the physical world, however, can lead to an imperfect understanding. Ravenscroft and McAlister (2006) noted that learning about cyberspace and the digital environment is best accomplished by starting afresh, without using physical world constructs.

As an example of some of the fundamental differences between the physical and digital worlds, consider one of the most basic work products, documents. Although the desktop metaphor has been used since the 1980s, when graphical user interfaces first became available, it is still common today to use the terminology of documents, the

desktop, and the office as the analog when describing files on computers (Agarawala & Balakrishnan, 2006). Yet, as Kenneally (2001a) demonstrated in a seminal paper, paper documents and digital documents differ in at least five key ways that affect how each might be used as evidence (Table 1).

Table 1. Characteristics of Paper-Based and Digital Documents

Characteristic	Paper-Based Documents	Digital Documents
Storage	Cumbersome	Volume not an issue
	Organized	Not well-organized
Backup	Backup is rare; stable	Backup is common; volatile
	Centralized	Distributed
Copying	Copies are same as original	Copies exist of all versions
	Deliberate	Inadvertent
	No metadata	Metadata present
Transmission	Traditional; perfect	Electronic; alterable
	One-to-one	Multicast
	Distribution limited	Distribution unlimited
Security	Defined perimeter	Global perimeter
	Lock-and-key	Encryption

Note. Modified from Kenneally (2001a); used with permission.

Table 1 shows some ways in which the storage of paper-based and digital documents differ. Every piece of paper occupies some amount of space so that the storage of a large quantity of documents requires a large amount of physical space. Computers store documents electronically, and an incredible volume of information can be stored in a very small area. Consider that 32 billion bytes (32 gigabytes) of storage, the equivalent of all of the books in most public libraries, can fit onto a single thumb drive at a cost of less than $100 (Anderson, 2008; Brown, 2010). Despite the volume, the filing cabinets in

which paper documents are stored are typically well organized and cataloged for retrieval purposes, and folders are labeled to identify their contents. In the digital environment, documents may not be as well organized, and a folder's name may have no necessary relationship to its contents; this seeming disorganization is offset by the fact that computers have powerful text string search capabilities, making retrieval of a document file relatively straightforward, regardless of its location. Individuals also sometimes purposely use file or folder names that have nothing to do with the actual content as a way of hindering a search, although this misdirection is less effective in the digital environment (Kenneally, 2001a; Rothstein et al., 2007; Volonino, 2003).

Backing up documents is the second differentiator between physical and digital documents. As suggested by Table 1, physical backup copies of physical documents are rarely maintained because paper documents do not change over time (as long as the environment is maintained and physical location protected), and the storage requirements of a large quantity of paper documents can be significant. It is quite common, in contrast, to find multiple backups of digital files due to the volatility of digital devices; failure of a single hard drive could cause the loss of hundreds of thousands of files. In addition, paper document storage is generally centralized at one or two locations, while digital backups may be stored in multiple locations (Anderson, 2008; Kenneally, 2001a; Rothstein et al., 2007; Volonino, 2003).

Copying documents is the third differentiator between physical and digital files, as shown in Table 1. Copies of physical documents are typically made purposely and are identical to the original. Copies of digital files may be made by an application, file system, and/or operating system so that there are many copies of many versions of a file,

many of which are unknown to the user. Additionally, a digital backup of physical paper is increasingly employed as companies attempt to reduce the volume of paper that is stored. This approach is causing a shift in the evidentiary value of records that are maintained electronically because when the original (paper) version is destroyed, the digital copy becomes the best evidence (Kerr, 2009; U.S. Courts, 2008c). In addition, digital files have metadata that describe a variety of characteristics about the file, whereas physical documents have no such metadata (Casey, 2011; Kenneally, 2001a; Rothstein et al., 2007; Volonino, 2003).

Document transmission presents another difference depicted in Table 1. In the physical world, documents are generally sent from one party to another, employing a copy of the original sent via postal service or courier. Barring some deliberate act by a third party, the document that the recipient receives is the same physical document that the sender sends, and because the sender seals a delivery package, the intermediary that transports the document does not maintain a copy of it (Anderson, 2008; Kenneally, 2001a). In the digital world, a single file can be sent to a nearly unlimited distribution list in a matter of seconds via e-mail, providing an opportunity for an unintended recipient to see a document, a network error to alter a message, or the message to be intercepted by a third party anywhere on the communication network. In addition, a single e-mail message may be transported by multiple network providers in multiple countries, each of which might maintain copies for some period of time on their servers (Anderson; Casey, 2011; Kenneally; Volonino, 2003).

Finally, Table 1 depicts differences in how security controls are applied to physical and digital documents. The security perimeter of physical files extends to the boundaries

of the building where the documents are stored. In the digital environment, physical devices on which files are stored are vulnerable to attacks that may come from an insider or anyone on the Internet. In addition, individuals can easily transmit even protected files via the Internet almost instantaneously (Anderson, 2008; Kenneally, 2001a; Volonino, 2003).

Another security difference is in how files are secured from unwanted readers. In the case of physical files, storage cabinets may be secured using a lock, and cabinets themselves may be stored in a vault. If the key is lost, other methods can be used to open the cabinet or vault to access the files. Digital files, in comparison, can be encrypted to protect them from a third party. In the case of a lost encryption key, these files may be beyond the reach of the rightful owner as well as the computer forensics examiner (Anderson, 2008; Casey, 2011, Kenneally, 2001a; Volonino, 2003).

Huang and Frince (2007) detailed other challenges that digital evidence provides as compared to traditional evidence. First, information on a computer may exist for a period of time, ranging from a fraction of a second to many years. Second, useful information on a computer might be found in an amount of data ranging from a single bit to a multi-gigabyte file. Third, all of the relevant information on a computer may be found in a single cluster on a hard drive or spread across many servers on the Internet.

Further, some types of data, such as audio recordings, may suffer from noise or distortion that makes completely reliable analysis impossible, causing a tension between good science and legal reasonable doubt (Maher, 2009; Tibbitts & Lu, 2009). Indeed, other types of evidence, such as photographic images, have historically had a high degree

of acceptability by judges and juries but can, today, be easily manipulated and altered (Farid, 2009).

There also may be legal hurdles associated with the acquisition and analysis of digital data; in particular, defining the scope of a search warrant, subpoena, or search incident to arrest may be difficult, given the interconnectivity of computing devices (Kerr, 2010). A final challenge is that correlating large datasets, demonstrating the nexus of the data to a crime, and assembling all of the information as cogent evidence can be difficult. Indeed, the management, processing, and analysis of digital evidence have been identified as important subject areas for future research (Beebe, 2009; Nance et al., 2009).

These differences in digital evidence and physical evidence have direct implications for the practice of digital forensics. Kerr (2005b), for example, has identified inconsistencies in Rule 41 of the Federal Rules of Criminal Procedure, which governs search warrants (U.S. Courts, 2008b). Rule 41 states that search warrants should be narrow in scope, clearly identify a specific time and place for the search, and specify the evidence that is being sought. These requirements are generally easy to meet when searching physical evidence.

The nature of digital evidence, however, usually requires that the entire store of digital data is seized at the search warrant location, while the actual search of the hard drives and other media to determine what information has probative value typically occurs at a specialized lab well after the warrant has been served (Kerr, 2005b, 2010). In addition, the search of digital evidence is often complicated by the large volume of digital evidence (due to growing disk drive capacity) that is seized (Kenneally & Brown, 2005).

Acceptance of Digital Evidence

While there is a general consensus that digital evidence is important and relevant in a large number of cases, its usefulness as courtroom evidence is still a matter of debate and, indeed, is often subject to an individual judge's own experiences, beliefs, and understanding (Insa, 2006; Kenneally, 2001b). Some judges, for example, place more trust in electronic evidence than in traditional evidence because of its perceived accuracy and objectivity. By contrast, other judges hold that digital evidence has limited value because of the difficulty in authenticating the original source of the information (Van Buskirk & Liu, 2006).

Another factor in a judge's acceptance of digital evidence is the mystique of computers and the Internet compared with the judge's own comfort level with ICTs (Losavio, Adams, & Rogers, 2006; Rogers et al., 2007). Judges may not possess sufficient knowledge of relevant digital technologies to always fairly and properly apply the *Daubert* reliability test to digital evidence or FRE Rule 702 to the qualifications of purported digital forensics experts (Insa, 2006; Van Buskirk & Liu, 2006). Generally, this resistance stems from the fact that at least some judges are opposed to using computers on a personal level (Galves, 2000).

This resistance may also be reinforced on an institutional level. The FRE, for example, gives a judge broad discretion in barring unfairly prejudicial evidence, and this latitude can affect how judges accept computer-based evidence or expert testimony given their own fear of, and unfamiliarity with, computers (Galves, 2000; Kerr, 2005a; U.S. Courts, 2008c). As a result, judges do not always make rulings that are consistent with the spirit of the laws related to digital evidence (Wegman, 2005).

Application of Digital Evidence

Judges sometimes render decisions that appear to be inconsistent with the spirit of relevant laws and/or based upon incorrect perceptions of ICT. These rulings hinge largely upon the judges' understanding of the evidence, technology, and/or expert witness testimony (Ball, 2008; Mason, 2008). The examples that follow are just a handful of cases that demonstrate some of the different and difficult issues with which judges need to wrestle when applying digital evidence at trial.

In the case of *New Jersey v. Reid* (2007), Reid was accused of using an anonymous e-mail account to break into the account of her work supervisor and alter customer information at her workplace. One of the key elements in this case was the method by which the police obtained incriminating evidence against her.

Police use subpoenas and search warrants to obtain information relevant to criminal investigations. Subpoenas are used to seize a company's business records, whereas search warrants are required to access more detailed information such as customer-owned files. In the case of an ISP, for example, a subpoena might be used to find the name of a person associated with a particular e-mail account, while a search warrant would be required to obtain the contents of e-mail or user files (Casey, 2011; Kerr, 2009).

Police investigating Reid served a subpoena on her ISP to obtain the information necessary to link her to the e-mail account. The trial judge observed that the use of an anonymous e-mail name was a clear indication that Reid did not want her identity known and was an obvious assertion of her expectation of privacy. The judge ruled that the police had, therefore, overstepped their bounds; they should have applied for a search warrant, which requires a higher level of proof and probable cause than that needed to

obtain a subpoena. As a result, the judge barred the evidence linking Reid to the anonymous e-mail account (*New Jersey*, 2007).

This case illustrates how the legal guidelines written for the real world of physical evidence and eyewitnesses might yield unexpected results when applied to digital evidence. For instance, one would not expect a judge to rule that a masked armed robber should be afforded additional constitutional protections because the use of a mask was an assertion of an expectation of privacy (Kerr, 2005a, 2009).

The second example is the case of *United States v. Councilman* (2004, 2005). Councilman worked at a company that dealt in rare books and provided e-mail accounts to several of its customers. Councilman directed the company's system administrator to configure the e-mail server so that it would intercept all incoming e-mail messages to their customers that came from the Amazon.com domain and make copies of them prior to the individuals' receiving the messages. Councilman was charged with conspiring to violate the Wiretap Act (1986), which specifically addresses the issue of monitoring real-time communication that is in transit. E-mail that is stored prior to being read is considered to be in transit, whereas e-mail that is stored after being read has a lower level of protection (Casey, 2011; Kerr, 2009).

There was no charge of a violation of the Stored Communications Act (1986), which protects e-mail that is stored prior to being read by the intended recipient. The judge in this case ruled that e-mail was protected by the Wiretap Act only while actually traversing the network and not when stored by computers during transit and delivery. In the original case, the government indicted Councilman for intercepting e-mails as a violation of the Wiretap Act. The district court disagreed and dismissed the indictment.

A divided panel of the 1st Circuit Court of Appeals affirmed the lower court's ruling (*U.S. v. Councilman*, 2004), but the full panel reversed the previous ruling (*U.S. v. Councilman*, 2005). The Councilman case is an example of the difficulties that judges have in understanding the subtleties of networking and e-mail as well as applying the applicable legislation (Kerr, 2009).

The third example is *American Express Travel Related Services v. Vinhnee* (2005). In this case, American Express (AMEX) sued Vinhnee for more than $21,000 in outstanding bills. At the original hearing, the bankruptcy court disallowed AMEX's use of e-records as their best evidence of the amount owned. This decision was based partially on FRE Rule 803(6), which defines a hearsay exception for records of regularly conducted activity (U.S. Courts, 2008c). According to this rule, business records can be introduced as evidence if it can be shown that the records were made at or near the time that the activity actually occurred; the records were created and maintained pursuant to regularly conducted business activity; and the source, method, or circumstances of preparation of the records can be shown to be trustworthy. Such records must be maintained by a records custodian and must be shown to be authentic and accurate (Mason, 2008). In Vinhnee, the records custodian testified that the AMEX records had met all of those tests. AMEX, however, offered into evidence duplicate copies of the records that had been reproduced from an electronic backup (*American Express*; Mason).

The court said that, because the records were stored electronically, additional information would be needed to prove authenticity and evidentiary value. At a later hearing, the court found that the records custodian was not qualified to answer even basic questions about the computer hardware, software, or database with which the e-copies

had been created and maintained. Even though the custodian testified that there was no way that the computer could change numbers on the electronically stored version of the customers' statements, the judge was not persuaded that there was sufficient proof that the e-copy matched the original billing statements, partially due to the custodian's lack of qualifications. Therefore, according to the judge, AMEX could not authenticate the billing record and was not allowed to enter those e-records as evidence. An appellate panel subsequently ruled that the judge did not abuse discretionary power in disallowing the evidence and affirmed the decision (*American Express*, 2005). In this case, the court followed the letter and spirit of the law, and AMEX failed in its responsibility to prove that e-copies were totally trustworthy (Mason, 2008).

The final example, *United States v. Boucher* (2007, 2009), deals with a legal issue that has been debated since encryption software became commercially available, namely, cryptographic keys and Fifth Amendment protections against self-incrimination (Clemens, 2004; Sergienko, 1996). Boucher was stopped at the U.S.-Canada border and admitted to having child pornography on a laptop computer in his car while being interviewed by Immigrations and Customs Enforcement (ICE) officials. He turned on the computer and the ICE officers saw incriminating images.

Boucher then invoked a sequence of keystrokes that locked his computer, which employed Pretty Good Privacy (PGP) whole disk encryption (PGP Corporation 2008). Computer forensics examiners were unable to crack the PGP passphrase after several months of effort, and prosecutors sought to compel Boucher to tell them the passphrase. Boucher refused and a hearing followed. Computer forensics examiners testified about the difficulty of cracking a PGP passphrase, telling the court that it could take decades to

break the passphrase by brute force (Casey & Stellatos, 2008). The judge ruled that Boucher could not be compelled to tell the passphrase to investigators as such an action would violate the suspect's protections against self-incrimination (*U.S. v. Boucher*, 2007).

Several legal questions were raised by this decision (McCullagh, 2007). Unlike most digital evidence cases, *U.S. v. Boucher* involved Fifth Amendment issues related to self-incrimination rather than Fourth Amendment search and seizure issues. The first question is whether all information provided verbally by a suspect can be considered testimonial. The second question is whether providing a password is, by itself, self-incriminating. Some legal experts observed, after the decision was rendered, that providing a password is similar to providing a key to a locked door in that the key itself is not incriminating even if the contents of the locked room are (McCullagh); this was, in fact, the reason that an appellate judge ordered a defendant to provide a password in a similar case in the United Kingdom (Kirk, 2008). Other experts observed that all verbal statements are testimony and any self-incriminating testimony is protected by the Fifth Amendment (McCullagh). If the passphrase had been written down on a piece of paper, compelling Boucher to provide it to law enforcement might not have been an issue, just as submitting physical evidence such as hair or fingerprints is not considered to be testimonial (McCullagh).

In 2009, another federal judge ordered Boucher to provide an unencrypted version of the hard drive contents to the authorities, a decision that did not directly address the question of whether saying a password is testimonial (McCullagh, 2009; *U.S. v. Boucher*,

2009). In the end, Boucher did provide the password as part of a later plea bargain (M. Touchette, personal communication, October 26, 2009).

Familiarity with Terminology

Appreciation of digital evidence requires an understanding of both the technology and the vernacular (Kerr, 2009). Consider the single most important step in computer forensics, that of making a forensically correct copy of the evidentiary medium (Brown, 2010). To ensure that the original evidence is not compromised in any way, a copy of the evidence medium is created, and the forensic examination and analysis are performed on the copy (Casey, 2011; Ieong, 2006).

The forensic copy of the evidence medium was historically called a mirror image (Gerber, 2001). This term is generally understood by a computer scientist or computer forensic examiner to mean an exact copy but can be misunderstood by lay audiences to mean a reverse copy because mirrors reflect an opposite image (Brown, 2010). The term mirror image was so confusing to courts that the process is now called a bit-for-bit forensic copy to avoid any such ambiguity (Casey, 2011).

To safeguard the integrity of the original data, the imaging process often copies the original evidence in fixed-sized blocks to the examination medium and each block is individually validated. The imaging process can be shown to produce a faithful replica of the original, but the copy may not necessarily look exactly the same as the original (Brown, 2010; Casey, 2011). Further, some imaging formats employ compression so that the examination copy is smaller than the original evidence (Common Digital Evidence Storage Format Working Group, 2006). Explaining that the forensically correct

examination copy is not a bit-for-bit identical copy of the original evidence can cause confusion for some audiences (Ieong, 2006; Kenneally & Brown, 2005).

According to Brown (2010), creating the forensic copy of the evidence medium is the only actual science that occurs in the computer forensics process. For imaging procedures to be accepted by the court as offering valid information of evidentiary value, these procedures must meet the *Daubert* reliability test (*Daubert*, 1993; Kerr, 2005a) and must be shown to be reproducible, so that two qualified, competent technicians using the same hardware and software are able to create identical forensic copies given the same original (Brown; Casey, 2011). This might not actually be the case, however. Suppose, for example, that the original evidence disk drive has a sector capable of being read just one more time. After the first technician makes an image of the evidence disk, that sector is no longer readable. When the second technician makes a forensic copy of the original, the second copy will not be identical to the first as a consequence of the bad sector, even though the same process was followed (Brown). Although the impact of this difference is minimal, only the most astute fact-finder will understand how to make a decision about the acceptability of this evidence (Oppliger & Rytz, 2003). Further, a procedure for precisely determining how different the two copies are and whether that difference actually affects the reliability of the evidence is not available (Kenneally & Brown, 2005; Lyle & Wozar, 2007; Roussev, 2009).

The disk imaging process is normally performed on a hard drive that has been removed from a computer system. In some circumstances, however, it is necessary to image a disk drive in a running computer such as when information is needed from an encrypted drive that may become unrecoverable if the system is shut down or from an

organization's server that can unduly disrupt a business if the system is shut down (Brown, 2010; Casey, 2011). Imaging a running computer system may cause some files associated with the imaging application to be written to the hard drive, thus altering the original evidence prior to the completion of the imaging process (Waits, Akinyele, Nolan, & Rogers, 2008). Imaging a live system also provides an opportunity to make a forensic copy of the system's random access memory (RAM). Since the imaging program has to be loaded into RAM to execute, some of the original contents of RAM are overwritten prior to the copy being made (Brown; van Baar, Alink, & van Ballegooij, 2008). In both of these instances, the court must be assured that whatever information is lost due to the live imaging process will not contain a sufficient amount of incriminating or exculpatory evidence to make a difference in reaching a just outcome of the case at hand (Kenneally & Brown, 2005).

Another emerging digital investigative procedure is network forensics, whereby data packets are read directly from the network itself using packet sniffing hardware or software. Typically, 100% of the packets will not be captured because the packet sniffing equipment may be unable to keep up with the volume of traffic on the network (Casey, 2011; Kessler & Fasulo, 2007). Offering an incomplete record of activity into evidence at trial must be accompanied with a clear, yet necessarily technical, explanation of the reasons why there is no bias to any missing data and, therefore, why such evidence should be admitted (Dinat, 2004; Kenneally, 2005).

While a lack of familiarity with digital technology and the resultant impact on court cases might suggest that new rules of evidence or specialist judges are necessary, the fact is that no such movement is currently underway within the judicial community (H. B.

Dixon, personal communication, August 1, 2009; Shaw, 2006; N. L. Waters, personal communication, November 20, 2008). This lack of technical understanding could possibly inhibit judges from critically evaluating the evidence presented to them as they perform their gatekeeper role and apply the *Daubert* test to presented evidence (Losavio, Adams, & Rogers, 2006; Losavio, Wilson, & Elmaghraby, 2006; Van Buskirk & Liu, 2006).

Reliability of Digital Evidence

The challenge of proving the accuracy and reliability of digital evidence is exacerbated by the fact that this type of evidence is sometimes neither. According to Van Buskirk and Liu (2006), a perception exists among many in the legal community that digital evidence, if accepted and admitted in court, is reliable and correct. However, the variability in forensics software, errors in the imaging process, and differences in examiners' knowledge affect the reliability, accuracy, and integrity of digital evidence (Casey, 2002; Cohen, 2008, 2010). In fact, Oppliger and Rytz (2003) and Van Buskirk and Liu make serious arguments that digital evidence is inherently unreliable largely because completeness cannot be verified and proven.

An example of the unreliability of digital evidence includes the timestamps commonly associated with files. Timestamps are metadata associated with a file and maintained by a digital device's operating system that indicates the date and time that the file was created, last accessed, and/or last modified (Casey, 2011). File timestamps can be important evidence because they allow the computer forensics examiner to build a timeline of activities. The order in which a set of events occurs can dramatically affect the interpretation of those events (Cohen, 2008, 2010). If the forensics software

inaccurately reports the timestamp information for any reason, the veracity of all of the information is suspect (Van Buskirk & Liu, 2006). In addition, not all programs update all instances of file timestamps in a consistent fashion, and even normal file system operations can provide seemingly contradictory timestamp information, such as when a file's reported last access time precedes the file's creation time (Brown, 2010; Casey, 2002, 2011).

As part of their gatekeeper role, judges must determine the reliability of reports and analysis gathered from forensics software (Jones, 2009; Kenneally, 2001b; Kerr, 2005a). While several well-known commercial and open source computer forensics software such as AccessData's Forensic Toolkit (FTK), Brian Carrier's Autopsy, Guidance Software's EnCase, and X-Ways Forensics are generally accepted by the courts, judges can rightfully question whether a given version of a particular application is as reliable, verifiable, error-free, and thorough as a previous version that has already been accepted by the court (Brown, 2010). Competent computer forensics laboratories will validate software as new versions are released, but the validation process is something that judges need to understand to properly apply the *Daubert* criteria to offered evidence (Brown; Kenneally; Van Buskirk & Liu, 2006).

An additional factor complicating the reliability of digital evidence is that of specific attacks on the computer forensics process and the forensics software. The Metasploit Anti-Forensic Investigation Arsenal (MAFIA), for example, is an open-source toolkit specifically designed to exploit known vulnerabilities and limitations in computer forensics software applications. The MAFIA toolkit includes applications that can change a file's timestamp metadata, hide information in the empty space in a data file,

and alter the metadata that identifies the format of the content in the file (Metasploit LLC, 2010). These tools work at a very low level and require a significant understanding of the underlying ICTs to appreciate their operation and the reasons why the digital evidence that was gathered might still yield plenty of information with evidentiary value (Harris, 2006; Newsham, Palmer, Stamos, & Burns, 2007).

Finally, not all data gathering is performed by trained investigators and computer forensics examiners. Numerous criminal investigations are initiated after a routine review at a private company reveals evidence of criminal wrongdoing that is then turned over to law enforcement (Casey, 2011). Meanwhile, the initial evidence gathering may be haphazard, and, therefore, it can be difficult to prove completeness and reliability of the data (Lathoud, 2004; Losavio, Adams, & Rogers, 2006).

Preliminary Studies of Digital Evidence

Given the importance of digital evidence in criminal and civil court cases in local, state, and federal jurisdictions, studies have started to emerge on the use and perception of such evidence by the various participants in the judicial system. In a small study in Kentucky, Losavio, Adams, and Rogers (2006) showed that most local judges did not see a lot of e-mail and Web site-related evidence offered in their courtrooms, and what little such evidence they did see was rarely challenged. Losavio et al. also found that the surveyed judges expected the amount of this kind of evidence to increase in the future. Finally, the judges also indicated that they received minimal training related to any type of digital evidence but would welcome more.

Rogers et al. (2007) performed a two-pronged study to determine how law enforcement officers (LEOs) around the U.S. view prosecutors' and judges' knowledge

of digital evidence and their respective willingness to prosecute cases that are largely dependent upon such evidence and admit that evidence into judicial proceedings. This investigation relied on respondents' answering questions using a Likert scale to evaluate their perception of the prosecutors and judges with whom they worked. Rogers et al. found that, in general, larger agencies serving urban populations appeared most comfortable with, knowledgeable about, and aggressive in the use of digital evidence. The study relied on the respondents' definition of "knowledge" and other terms of the survey rather than offering precise definitions. This same study also found that most of the LEOs surveyed reported a low rate of cases involving digital evidence. According to Rogers et al., this finding might be indicative of the LEOs' lack of awareness, knowledge, and/or training related to digital evidence in the first place.

In a similar investigation, Scarborough et al. (2009) surveyed state and local LEOs as well as district and county prosecutors to learn about their awareness and use of digital evidence. As in Rogers et al. (2007), respondents completed a Likert-scaled questionnaire to determine each group's perception of its own views as well as the views of the other group. They then used their own understanding of the terms of the survey (i.e., different respondents might use different criteria to rank knowledge at a particular level). Scarborough et al. found that, in contrast to prosecutors, LEOs considered digital evidence to be a routine part of their investigations. Further, each group rated only a small number of the individuals in the other group as very knowledgeable about digital evidence. Interestingly, prosecutors seemed more willing to pursue cases with digital evidence than did the LEOs. Both groups agreed that judges had less knowledge about

digital evidence than did LEOs and prosecutors, and that judges were hesitant about admitting digital evidence at trial.

A large study of digital forensic practitioners was performed by Carlton (2006, 2007). In this multi-phase study, Carlton worked with computer forensics examiners to identify and classify the critical tasks that comprise every examination of digital evidence. Carlton's participants were members of the High Technology Crime Investigation Association (HTCIA), an international organization that consists mostly of active or former members of the law enforcement digital forensics community. In the early phases of this study, Carlton identified individual tasks such as testing and validating forensics tools, properly inventorying and documenting evidence, and maintaining a proper chain of custody. In later phases, Carlton prioritized the tasks that were identified and compared the practitioners' rank ordering with that of two independent expert panels that assessed the tasks in terms of technical and legal necessity, respectively. Carlton also used grounded theory as the basis for foundational research related to digital forensics.

Literature Related to Grounded Theory

This section provides an introduction to grounded theory concepts. The literature presented describes the development of grounded theory since its inception in the mid-1960s for social science research and explains why grounded theory is applicable in scientific and technical fields such as digital forensics.

Overview of Grounded Theory

Grounded theory is a qualitative research methodology that employs an inductive process whereby data are gathered to develop a substantive theory. This is in contrast to

the deductive process whereby data are gathered to test a hypothesis (Charmaz, 2006; Dick, 2005; Pogson et al., 2002; Schram, 2006). Grounded theory is useful for early studies in a new discipline and enables an examination of how people respond to various phenomena (Charmaz). Grounded theory is well suited to examining the complex relationship between a person's actions (i.e., response to a situation) and his or her contextual understanding of the meaning (i.e., personal definition) of a situation (Brown, Stevens, Troiano, & Schneider, 2002; Glaser & Strauss, 1967).

A number of different approaches to grounded theory studies have been described in the literature (Brown et al., 2002; Charmaz, 2000, 2006; Dick, 2005; Elliott & Lazenbatt, 2005; Leedy & Ormrod, 2010; Pogson et al., 2002; Schram, 2006). Typically, these approaches employ similar fundamental strategies. Data gathering and analysis occur in parallel so that themes are allowed to emerge during the process of data collection. More specifically, data are gathered through a combination of interviews, surveys, observations, documents, and other relevant data sources and are analyzed by coding and categorizing the responses. These studies are primarily qualitative and focus on discovering the social, or interpersonal, processes found within the data. Further, an iterative approach to the study allows for the observation of processes and the construction of categories that define the relationship between those processes. Importantly, a theoretical framework that defines the causes, actions, and effects of the processes can be created.

The general approach of a grounded theory study is shown in Figure 1. Initial data gathering is open-ended. As trends appear from the data, additional questioning becomes increasingly focused and probing in an effort to seek explanations that lead to a better

understanding of the data. The key to grounded theory is to understand the responses or actions that occur due to the social interactions of people with each other or the surrounding events (Charmaz, 2000, 2006; Dick, 2005).

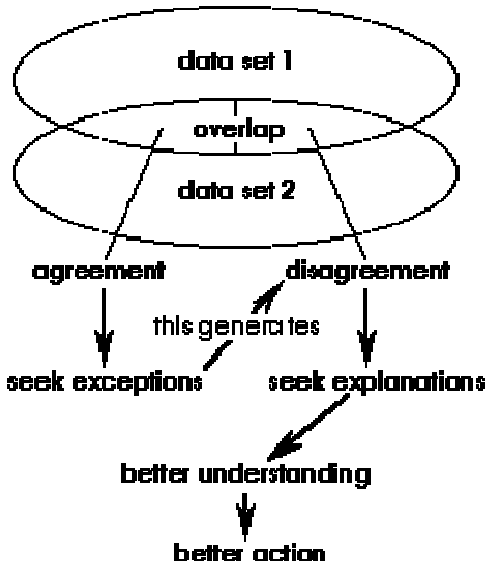

Figure 1. The grounded theory process (Dick, 2005; used with permission).

Evolution of Grounded Theory

The seminal work on grounded theory is a text by Glaser and Strauss (1967), *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Glaser and Strauss had been working on a study about dying in hospitals based on a new approach of developing theories based on the data from research, as opposed to deducing testable hypotheses from existing theories. With this methodology, Glaser and Strauss developed a framework for a researcher to describe his or her understanding about a research topic based upon observable trends from the raw data (Charmaz, 2006; Heath & Cowley, 2004).

Grounded theory offered a new approach to research when it was introduced in 1967. Research prior to this time was dominated by the classic scientific method of observing a phenomenon, conducting experiments, defining concepts, deducing hypotheses, and confirming theories with evidence. This approach, known as positivism, places the researcher as a neutral party separate from the subjects and data, and generally employs quantitative methods. Qualitative methods were not regularly employed as they were viewed to be unsystematic, unreliable, and biased when compared to the positivist approach (Charmaz, 2006; Glaser & Strauss, 1967).

Glaser and Strauss (1967) proposed an organized, systematic approach to qualitative research with its own logical constructs that could be used to generate new theory. Their methods involve the simultaneous activities of data gathering and analysis (Charmaz, 2006). This methodology allows the researcher to identify trends that emerge from the data, and the researcher can take an iterative approach to the categorization of those trends (Charmaz; Heath & Cowley, 2004). As an example, a researcher studying anxiety among individuals using self-contained underwater breathing apparatus (SCUBA) might start by asking divers open-ended questions about what causes them anxiety. As themes emerge from the answers, the researcher could start to ask more finely focused questions to better understand the root causes of divers' anxiety (Charmaz; Morgan, 1995).

Glaser and Strauss (1967) each brought a different perspective to the development of grounded theory. According to Charmaz (2006), a student of both Glaser and Strauss, Glaser is a positivist, employing quantitative methods and specific rules for codifying results as well as creating theories to describe specific social interactions. Strauss viewed people as active participants in their own lives, building structure through social

processes rather than the other way around. Indeed, the human ability to use language influences the personal and societal interpretation of social relationships. Together, Glaser and Strauss observed that responses emerge through action, and action is central to grounded theory research (Charmaz).

Scientific rigor is a key to grounded theory research, although these types of studies do not generally start with an exhaustive review of the literature. To minimize researchers' preconceptions about the subject under study, grounded theory depends upon literature only for providing a broad understanding of the topic area and to inform researchers about a wide range of possible responses (Fernández, 2004; Heath & Cowley, 2004). Charmaz (2006) stated that it is imperative that researchers recognize what they do not know. Reading the literature, then, is also an iterative process. Researchers should initially review relevant literature not to guide the study but also to inform the researcher and later use the literature to learn how the current study supports, refutes, modifies, or expands upon earlier research (Charmaz; Dick, 2005).

By the mid-1980s, Glaser and Strauss began taking divergent paths in their views and applications of grounded theory. Glaser remained most consistent with the pair's earlier work, maintaining the inductive process of grounded theory as a method of discovery whereby analysis of data yields patterns that result in generalized theories. Strauss moved toward a process that placed more initial emphasis on deduction and verification rather than on induction. According to Strauss, the role of induction is to elaborate on deductions rather than being a primary vehicle (Charmaz, 2006). Currently, there are several schools of thought about how to conduct grounded theory studies, although these

differences have a minimal impact on the methodology of this study (Charmaz, 2000, 2006; Dick, 2005; Heath & Cowley, 2004; Leedy & Ormrod, 2010).

In this study, the researcher followed the precepts of Charmaz (2006). Charmaz (2000) described Glaser and Strauss as objectivist grounded theorists, meaning that they assumed that different observers, given the same set of data, would describe a situation in the same way. Charmaz (2000) noted that strictly objective data analysis is not possible because the viewer (i.e., the researcher) unavoidably acquires, analyzes, and interprets data within his or her own cultural, temporal, and social context. The researcher, then, becomes part of the research. Charmaz (2006) employs what is called constructivist grounded theory. Constructivist grounded theory methods take into account that individuals learn new things based, in large part, upon who they are and what they already know (Mills, Bonner, & Francis, 2006; Phillips & Soltis, 2004). As a consequence, the hypotheses devised from a grounded theory study might be influenced by or dependent upon the prior knowledge of the researcher. The lack of objectivity does not, in and of itself, introduce unacceptable researcher bias any more than researcher bias necessarily affects a quantitative study in which the researcher selects the hypothesis (Charmaz, 2006; Mills et al., 2006).

Applicability of Grounded Theory to Digital Forensics Research

Grounded theory was developed primarily for social science research and is effectively employed to study social processes (Charmaz, 2006; Glaser & Strauss, 1967). A grounded theory study addresses the relationship between people and social phenomena such as serving jury duty, living with chronic illness, or interacting with ICT as well as expands understanding of that relationship by providing new perspectives

(Brown et al., 2002; Charmaz; Glaser & Strauss; Pogson et al., 2002; Schram, 2006). Qualitative research, which focuses on social interactions, is applicable to research related to information technology (IT) and other technical and scientific fields because people's interactions with information and information systems are largely social in nature (Fernández, 2004; Haig, 1995; Hunter, 1995).

Quantitative studies were developed for the natural world. One quality that distinguishes humans from everything else in nature is the use of language (Charmaz, 2006; Myers, 2010). Qualitative studies take advantage of the fact that participants can help the researcher understand the subtleties of a particular social or institutional context that is often lost when data are quantified (Charmaz). Grounded theory is well suited to IT research because these investigations generally involve the social interactions between people using IT or people's interactions with IT (Fernández, 2004; Myers). Grounded theory has been described in the IT research literature since the early 1990s and has been used to conduct, for example, research that focuses on improving software product development, developing an IT strategy for a large business, and using computer-aided software engineering (CASE) tools to effect organizational change (Baskerville & Pries-Heje, 1999; Mingers, 2001; Orlikowski, 1993). Moreover, an international conference on computer system sciences in 2009 included nine papers applying grounded theory to IT topics (Sprauge, 2009).

For this investigation, the researcher focused on the complex phenomenon of how judges understand, value, and apply (i.e., interact with) digital evidence. The body of literature specific to the digital forensics field is still small. A search of the literature reveals that much of the research on the technical aspects of computer forensics (e.g.,

analysis of RAM and examination of cellular telephone file systems) is based on computer science, whereas research on cyberlaw (e.g., exceptions to search warrant requirements and rules regarding e-discovery) is based upon a plethora of legal works (Carlton, 2006; R. B. Vaughn, personal communication, July 22, 2010). To date, studies about the understanding of digital evidence by law enforcement officers, prosecutors, and judges have been very limited (Carlton, 2006, 2007; Losavio, Adams, & Rogers, 2006; Rogers et al., 2007; Scarborough et al., 2009). Due to the small number of studies on this particular topic and because the subject matter involves interactions between people and technology, grounded theory provides a promising method for developing a framework upon which other investigators can build (Carlton, 2006; Myers, 2010).

Summary

Ball (2008), Brown (2010), Casey (2011), Kerr (2005a, 2005b), and Manes et al. (2007) have observed that digital evidence is growing in both volume and importance in criminal and civil litigation. Judges must decide what evidence will and will not be admitted in their courtroom, and they need to weigh the probative value against the prejudicial effect of any evidence that is offered (Cohen, 2008, 2010). These considerations apply to scientific and technical evidence as well as to other types of physical evidence such as crime scene photographs. To fairly and justly evaluate the merit of digital evidence, judges should have some understanding of the underlying ICTs and applications from which digital evidence is derived, such as computers, the Internet, and e-mail. The literature is nearly silent on what judges know and how they perceive

digital evidence (Losavio, Adams, & Rogers, 2006; Rogers et al., 2007; Scarborough et al., 2009).

The researcher employed grounded theory in this study. Although initially designed for the social sciences, grounded theory has been applied to information technologies (Charmaz, 2006; Sprauge, 2009). The interactions of judges with digital evidence have a social aspect that makes a study of this relationship well suited to grounded theory (Brown et al., 2002). Importantly, this investigation adds to the currently limited base of existing digital forensics research (Carlton, 2006; Rogers et al., 2007; Scarborough et al., 2009).

Chapter 3

Methodology

This chapter provides a description of the research methodology employed in this study. The chapter begins with a presentation of general grounded theory research methodology and then presents the specific procedures used in this study.

Research Design

Grounded theory consists of three basic elements: concepts, or the conceptualization of data rather than the data itself; categories, or the analysis of data that leads to developing theories; and propositions, or the relationships between a group of concepts and a category or between categories (Pandit, 1996). To tie these elements together, grounded theory studies involve a number of overlapping, iterative steps that move from gathering data to developing theory (Dick, 2005), as shown in Figure 2.

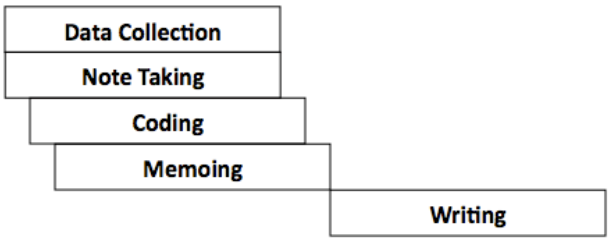

Figure 2. Phases of a generic grounded theory study (Dick, 2005; used with permission).

Data Collection

Grounded theory research starts with basic data collection, usually employing open-ended questions in the form of a questionnaire or interview. Data gathering and initial analysis occur concurrently, so the method of data collection must be flexible and might change during the course of the study (Charmaz, 2006). Consequently, almost all grounded theory research employs more than one round of questionnaires, interviews, or other data-gathering activities (Brown et al., 2002; Charmaz; Dick, 2005; Pogson et al., 2002).

Note Taking

As data are gathered, the researcher takes notes of emerging themes. It is important at this juncture that the researcher carefully listen to what the participants are saying rather than to make any attempt to fit the data to the researcher's expectations (Charmaz, 2006; Pogson et al., 2002). It is critical to the integrity of the study that the notes accurately reflect the participants' perspectives without an overlay of the researcher's interpretation (Charmaz; Dick, 2005; Leedy & Ormrod, 2010).

Coding

To compare the data supplied by the different study participants and to detect emerging trends, data are coded. Coding is a multi-pass process (Figure 3). The first step in coding is called initial (or open) coding, where the researcher reviews the interview or survey transcripts and notes and creates shorthand codes that reflect the statements of the participants (Charmaz, 2006; Robson, 2002). During this stage, the researcher also must remain totally open to whatever possibilities the data suggest and follow the data rather than try to lead (Elliott & Lazenbatt, 2005). The researcher can, at

this point, start to define simple categories and concepts for comparison and understanding (Charmaz; Robson).

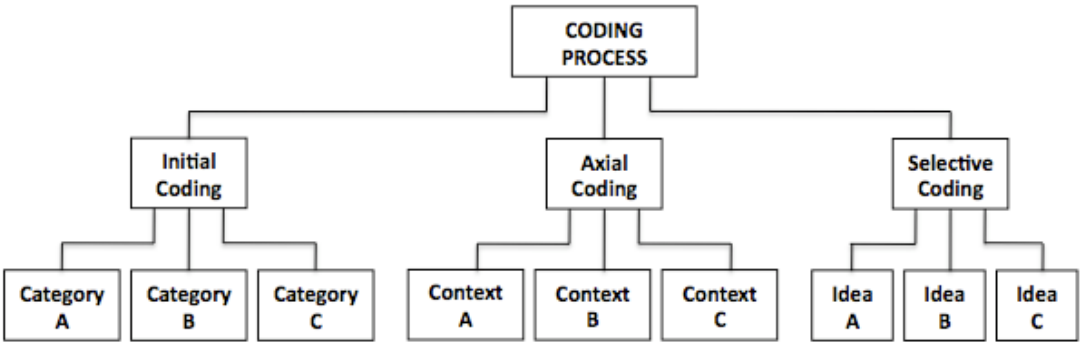

Figure 3. Summary of the coding process (Robson, 2002).

As concepts emerge, a second phase, called axial (or focused) coding (Charmaz, 2006; Robson, 2002), begins. Axial coding can be employed on the data to follow up on the analytic trends of interest. This is a way to narrow the focus of the research and to manage a large body of data (Brown et al., 2002). During this coding phase, the researcher examines the data to provide a contextual model of the interrelationships between conditions, actions, and consequences (Charmaz; Robson). The final stage is called selective coding and is the point in the coding process where central, unifying ideas emerge that explain the interactions that were observed (Charmaz; Robson).

Memoing

The next step in the process is to write memoranda (simply called “memos” in the vernacular of grounded theory), a critical intermediate phase between coding and publishing results (Charmaz, 2006). The memo-writing process entails organizing the trends to define categories and relationships. From here, the researcher can generate

theories that, in turn, are published to provide foundational literature (Charmaz; Dick, 2005).

Writing

The final step in the grounded theory process is to publish the results. A critical element in determining the value of any such publication, however, lies in the validity of the conclusions (Charmaz, 2006; Dick, 2005). Validity refers to the ability of the researcher to state with some level of certainty that the study results accurately reflect the relationships being investigated. Grounded theory studies are prone to the same types of errors as are any other qualitative study, so ensuring validity is important (Elliott & Lazenbatt, 2005; Leedy & Ormrod, 2010).

There are several types of validity pertinent to this method of research. Internal validity refers to credibility, addressing whether the results correctly represent the views of the study population. External validity refers to the generalization of the results, addressing whether the research can be applied to groups other than the study population (Miles & Huberman, 1994).

In the Assumptions, Limitations, and Delimitations section in the first chapter, the potential challenges to the internal validity of the study, including the self-selection of participants from professional organizations and the ability of study participants to drop out of the study at any time, were presented. According to Seale (as cited in Elliott & Lazenbatt, 2005), grounded theory studies do not need to rely on traditional methods of validating research results because a concurrent process of gathering and analyzing data is integral to this type of study. Instead, Seale observed that a critical element of grounded theory is that it is dependent upon the researchers' willingness to shape their

ideas to the emerging data rather than using data to confirm their *a priori* notions. According to Elliott and Lazenbatt, validity checking is typically an additional step in traditional research; in contrast, validity checking is inherent in the grounded theory process.

Construct validity is another form of research validity that applies to this investigation. Construct validity refers to the ability of the researcher to correctly identify the relationships, or constructs, that are actually being studied (Robson, 2002). By using triangulation, while involves multiple sources or perspectives, the researcher was able to determine a set of constructs that comprise the relationship between judges and digital evidence as a means to provide a framework for future research studies (Dick, 2005; Pogson et al., 2002).

All data gathered in this investigation represent the perspectives of the participants (Charmaz, 2006; Dick, 2005; Leedy & Ormrod, 2010). Pogson et al. (2002) identified two levels of interpretation of the themes that emerge from the data, namely first-order and second-order constructs. A first-order construct refers to the study participants' understanding of the phenomenon being investigated, while a second-order construct refers to how the researcher understands the phenomenon (Pogson et al.). First-order constructs, then, focus on what is happening from the perspective of the participants, while second-order constructs focus on the researcher's understanding of why something is happening. Since this study focuses on judges' attitudes and perceptions rather than the researcher's perspective, the conclusions address first-order constructs.

Research Methodology

As discussed by Brown et al. (2002), Charmaz (2006), and Pogson et al. (2002), the originally planned methodology evolved during the course of the study. The initial research plan called for the researcher to distribute multiple surveys to the participants. The initial survey was expected to bring up certain themes and information that would have been more fully explored in subsequent surveys (Brown et al.; Carlton, 2006; Charmaz; Pogson et al.). The number of respondents, generally, drops off with each new round of data gathering (Carlton; Charmaz). The design of the study had to balance following the grounded theory process through to its logical conclusion with not exhausting the pool of participants (Brown et al.; Pogson et al.). For these reasons, the researcher initially planned to narrow the focus of the study so that there would be only two or three rounds of surveys, as also suggested by Carlton.

The initial goal was to obtain between 50 and 100 completed surveys (Charmaz, 2006). This would have provided a sufficiently large pool with which to distribute one, or possibly two, follow-up surveys. The actual response rate to the initial survey was much lower than expected, however, as will be discussed in Chapter 4. While the initial survey results provided valuable information, the researcher determined that a second written survey instrument would not be the best way to elicit additional information. This change in strategy, consistent with grounded theory guidelines, involved utilizing face-to-face interviews with a small sample of judges for a second round of detailed data gathering (Charmaz; Leedy & Ormrod, 2010).

The evolutionary nature of grounded theory research makes it important to note and record the fact that initial research study design plans change during the course of the

data-gathering phase (Charmaz, 2006; Leedy & Ormrod, 2010). The remainder of this chapter concerns the study as it was actually carried out.

The framework for the study was based upon the work of Carlton (2006), who performed the largest study to date about how digital evidence is acquired and perceived by computer forensics examination practitioners. Carlton employed grounded theory largely due to the lack of literature in the field describing the interaction between practitioners with digital evidence. The three stages of this study involve two phases of data gathering and then the output (Figure 4), as described below.

Phase 1 Data Gathering: This stage of the study started with a written survey intended to gain an initial understanding of judges' attitudes about digital evidence. The survey was distributed to two national organizations of judges. The results were analyzed using the grounded theory methods described above (i.e., note taking, coding, and memoing) to detect common themes.

Phase 2 Data Gathering: A series of face-to-face interviews was held with judges in Massachusetts and Vermont. The interview questions were prepared as a result of the Phase 1 survey. The interview transcripts were analyzed using grounded theory methods to identify additional detailed themes.

Output: The output of the research is a series of findings about judges' knowledge, awareness, and attitudes about digital evidence as well as a proposed framework of judicial training and education about digital forensics.

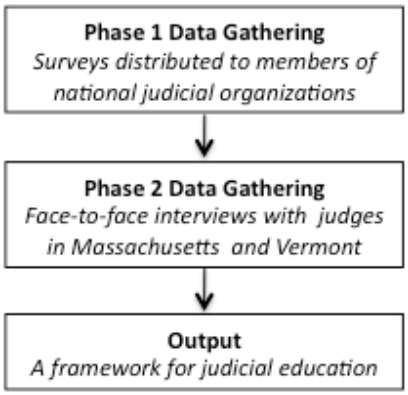

Figure 4. Stages of the study.

A major component of this research was to demonstrate the validity of the results (Elliott & Lazenbatt, 2005; Leedy & Ormrod, 2010). Triangulation is one method with which to test construct validity, the mechanism with which to ensure that a correct set of relationships between judges and digital evidence was identified. Construct validity is required to provide a framework for future research (Dick, 2005; Pogson et al., 2002). For the purpose of triangulation, the researcher assembled a panel of ten digital forensics professionals to assist and advise during various stages of this investigation, as described below. The advisory board comprises five attorneys and five practitioners, all of whom have computer forensics expertise and have volunteered to serve in this capacity (Appendix A).

Phase 1 Data Gathering

The study began with Phase 1 data gathering. During this phase, a survey instrument was prepared, Institutional Review Board (IRB) approval obtained, a target audience identified, initial data gathered, and results validated by the advisory board.

Initial Survey

The initial survey instrument (Appendix B) was designed to address the component issues of the research questions, as identified in the Research Questions to be Investigated section of this report. The questions in the survey were developed by the researcher to obtain a broad view of judges' knowledge of topics related to digital evidence. The questions were inspired primarily by the results of other studies (Losavio, Adams, & Rogers, 2006; Rogers et al., 2007; Scarborough et al., 2009). The questionnaire was then reviewed by the advisory board and representatives from two national organizations of judges from which the pool of respondents was obtained (Appendix C). These individuals advised that a survey for a population of judges needed to be short, advice that was also supported by the literature (Carlton, 2006; Mack & Anleu, 2008). One design goal of the questionnaire, then, was that the participants could complete it within 20 minutes.

The first question in the survey, which offered a definition of the term *digital forensic evidence*, was purposely leading. Although the remaining questions were open-ended, as a means to learn what judges know so that recurring themes could emerge from the data, advice from the advisory panel and professional organization contacts suggested that some judges taking the survey might have no idea how to define digital evidence. Those judges, therefore, were likely to stop participating either because they could not answer the first question or because they would not want to take the time to do research to answer the question (Charmaz, 2006). Alternatively, some judges might have a definition of digital evidence that was so off base as to render the answers to subsequent questions misleading (N. L. Waters, personal communication, December 10, 2008). The

common advice was to provide a definition for the survey participants that would provide a basis of understanding while still allowing participants to amend the definition if they chose to. The definition used in the survey comes from the Definition of Terms section in Chapter 1.

The survey form itself comprises three parts, namely an introduction and informed consent form for the survey (Part I), the survey questionnaire itself (Part II), and an informed consent form requesting contact information for participation in follow-up survey(s) that were part of the original plan (Part III) (Charmaz, 2006; Nova Southeastern University [NSU], 2009). Since this part of the survey posed minimal risks to participants and did not involve any protected populations, it was eligible for college/center level IRB review (NSU). IRB approval of the initial questionnaire was granted in April 2009.

Survey Distribution

To ensure a large potential pool of participants, the researcher contacted the American Bar Association Judicial Division, American Judges Association (AJA), National Center for State Courts (NCSC), and National Judicial College in November 2008 to request permission to distribute the survey to their members. All of the organizations were hesitant to participate at first, citing members' concerns that the researcher might have a preconceived negative attitude towards judges and/or that the results of the survey by an outsider would be used to show that judges were largely ignorant of matters related to digital evidence (H. B. Dixon, Jr., personal communication, November 16, 2008; W. F. Dressel, personal communication, November 17, 2008; N. L. Waters, personal communication, December 10, 2008; E. Zide, personal communication, November 12,

2008). Mack and Anleu (2008) suggested that such resistance might be offered, so this reluctance was expected.

The researcher received permission to attend the July 31 to August 1, 2009, annual meeting of the ABA/JD for the purpose of distributing the first survey questionnaire (ABA, 2009a). After the meeting, the ABA/JD sent an e-mail to their membership directing them to a Web site where members who had not attended the meeting could also access the survey. In August 2009, the NJC followed suit and sent information about the survey to their membership (NJC, 2009). The initial survey period lasted from July 31 to October 15, 2009.

Participants in the first survey were asked whether they would be willing to participate in one or two follow-up surveys; if they answered in the affirmative, they were asked to complete an informed consent form and provide contact information for subsequent surveys. All surveys contained two copies of the consent forms (Parts I and III), and respondents were instructed to keep one copy of each form for their records.

All survey packets submitted for the study were delivered in person to the researcher or sent by postal or e-mail. All packets were handled by a research assistant, who confirmed the presence of a signed informed consent form (Part I) and separated the consent forms (Part I), survey questionnaires (Part II), and follow-up contact forms (Part III) prior to delivery to the researcher. This process ensured anonymity and that the researcher had no way to associate participants' personal identifying information with any specific survey submission (Carlton, 2006; Charmaz, 2006).

Survey Review

The role of the initial survey was to provide preliminary data with which to inform and guide the researcher in the development of the more detailed interview protocol to follow. The researcher reviewed the survey results to find major points that would be of interest in an ongoing exploratory survey (Charmaz, 2006).

To provide external validation of the survey results, input was gathered from the researcher's advisory board. The advisory board provided an independent validation of the trends that the researcher identified from the survey data. The role of the board was not to provide a value judgment of the raw data obtained from the study subjects (in fact, the board had no access to any raw data) but rather to provide a review of the concepts, categories, and relationships identified by the researcher based upon their experience and expertise (Carlton, 2006). Obtaining input from multiple sources in this way is consistent with the concept of triangulation that is important to grounded theory. Multiple sources of independent measurements provide a means for data verification, greater confidence in the results, and a better opportunity to integrate more observations into a unifying explanation (Brown et al., 2002; Charmaz, 2006; Miles & Huberman, 1994; Pogson et al., 2002).

Phase 2 Data Gathering

The second stage was Phase 2 data gathering, which employed steps similar to those of Phase 1. Although the results of Phase 1 formed the basis for the Phase 2 information-gathering instrument, the entire grounded theory process was essentially repeated.

Interview Questionnaire

The original design for this study involved using a series of two, possibly three, written surveys. The low response rate and relatively short answers to the first survey suggested to the researcher that employing face-to-face interviews would be more productive for subsequent contact with this population. Among other things, interviews allow the respondents to provide more depth and thought into their answers as well as allow greater reflection and storytelling on the part of the respondents, key elements to the grounded theory process (Charmaz, 2006). Grounded theory interviews are specifically designed to draw out stories and free associations (Charmaz; Glaser & Strauss, 1967; Leedy & Ormrod, 2010; Robson, 2002).

Since the researcher sought to limit the time requirements of the study participants, the interview protocol was focused and comprised a small number of questions. The subject matter covered by the interview was inspired by the trends observed in the initial written survey, as validated by the advisory board. The interview instrument, with input from the advisory board, was honed down to nine primary questions, most with a few follow-up questions (Appendix D).

Interview and IRB Process

An additional advantage to the interview approach was that the researcher was able to see certain themes and issues emerge between the first and last interviews. Whereas the initial survey was written once and then distributed to potential participants, the researcher was able to detect emerging themes as each in-person interview transpired (Glaser & Strauss, 1967).

This is consistent with the grounded theory approach but posed a potential risk to the fundamental tenet of following, rather than leading, the data. Specifically, as data are gathered, the researcher takes notes of emerging themes. It is important during this process that the researcher carefully listen to what the participants are saying rather than make any attempt to fit the data to the researcher's expectations (Charmaz, 2006; Pogson et al., 2002). It is critical to the integrity of the study that the notes accurately reflect the participants' perspectives without an overlay of the researcher's interpretation or expectations (Charmaz; Dick, 2005; Leedy & Ormrod, 2010).

Note-taking during an interview, then, poses several threats to the integrity of the exploratory nature of grounded theory research. First, a note-taker can be distracting to the participants, causing them to shorten their answers or be less free-flowing in their ideas as they try to slow down to let the note-taker keep up with them. Second, note-taking can add to the discomfort of the interview participant, a situation that can be exacerbated if the note-taker is a third-person (Charmaz, 2006; Robson, 2002).

More importantly, however, taking notes means that not all of the ideas offered by the interview participant are written down. This can add bias in several ways. First, the actual words spoken by the interview participant are generally not written verbatim and in their entirety, meaning that the language of the speaker is lost data. Second, the notes that are taken are written in the words of the note-taker, losing the context in which they were spoken. Indeed, the ultimate bias is the fact that the note-taker, who generally is unable to record everything that the interview participant says, keeps track of only those things that he or she finds important. This latter situation means that important, yet subtle, information might be lost. The combination of missing the interview participant's

actual words, missing stated ideas, and inserting a subconscious bias by tracking those things that are important at the expense of the heretofore unimportant can be fatal to a grounded theory study (Charmaz, 2006; Dick, 2005; Robson, 2002).

The alternative to note-taking in this research study was to record and transcribe the interviews verbatim. Due to the additional intrusion and potential discomfort to the study participants, additional IRB approval at the institutional expedited review level was required (NSU, 2009). Since the recordings and transcripts memorialized the speaker in a way that note-taking would not, extraordinary steps were required in the creation of the informed consent form and stated methodologies with which to ensure and maintain the anonymity of the study participants and the confidentiality of their statements (Appendix E). IRB approval for the interviews was granted in December 2009.

There is a certain tension between the IRB's need to protect the safety and well-being of human study subjects and the exploratory nature of grounded theory studies. Indeed, the IRB required a detailed list of questions that would be asked of the interviewees. However, as Charmaz (2006) stated, "Such detail is inconsistent with the emergent nature of qualitative research in general and grounded theory methods in particular" (p. 30). This level of detail in the IRB application made it difficult to plan on asking follow-up questions of the participants if, and when, they broached new ground. Maintaining the dictates of the IRB process with the spirit of the grounded theory process was achieved by asking the interviewees—judges, who are largely used to a question-and-answer interview—to tell stories or anything else that they felt to be pertinent, without waiting for follow-up questions. The researcher did ask several clarifying questions during the interviews but did not deviate from the stated questions.

Interview Participants

The initial survey for Phase 1 data gathering was made available to the membership of the ABA/JD and NJC. The researcher approached these two organizations because they represent a large pool of trial judges from across the U.S.

When the decision was made to engage in face-to-face interviews, the researcher had to determine how to select the pool of judges for this activity. Selecting the number and source of participants for this study goes to the heart of the meaning of sampling within grounded theory. A grounded theory study employs purposive sampling, meaning that subjects are selected who are, in the researcher's opinion, typical or otherwise of interest (Robson, 2002). Sampling in grounded theory, called theoretical sampling, is very different from the traditional sampling often associated with other types of qualitative and quantitative studies (Charmaz, 2006). In particular, theoretical sampling is not intended to be representative of a given population, so there is no particular requirement for a level of randomness that might result in a grand, general theory (Charmaz; Robson). The initial theoretical sampling of grounded theory is where one starts to gather data with which to form theories rather than a way to gather data to prove or disprove a hypothesis (Charmaz; Robson). In short, theoretical sampling is not the same, nor intended to serve the same function, as sampling methods that are statistically representative of a given population, applicable to a given research question, searching for negative cases, or attempting to saturate the population until no new information can be found (Charmaz; Robson).

The Phase 2 data gathering was based on interviews with seven judges in Massachusetts and Vermont. This small number of participants was felt to be

manageable and adequate for an exploratory study of this nature (Charmaz, 2006; Leedy & Ormrod, 2010; Robson, 2002). Although not attempting to be representative of all judges in the U.S., the researcher did want the sample to have a distribution among judges with some differences in their court. The criteria for selection of the sample were (a) judges needed to be active trial or appellate judges; (b) judges would be at the local or state, rather than federal, level; (c) judges would be selected from two states; and (d) judges would be selected from at least two levels of court in each state.

For purposes of this phase of data gathering, experiential and demographic criteria such as the number of years on the bench, the amount of time served at this level of the court, experience prior to being a judge, gender, or age were not used to form the participant pool.

Massachusetts and Vermont were selected as the two states from which to draw the pool of judges for three reasons. First, the researcher lives in Vermont and is in easy driving distance of Massachusetts. The researcher believed that the interviews needed to be conducted face to face, rather than over the telephone, so the participant pool needed to be within geographic proximity.

Second, the researcher has contacts within the relevant judicial communities who agreed to help contact judges within the target pool and encourage their participation. This assistance was crucial to meeting judges who would agree to a taped interview with someone whom they did not know. Just as some within the leadership of the ABA/JD, NJC, and other national judicial organizations expressed initial hesitancy about the researcher's studying judges within their groups, individual judges would likely have the same concern if an unknown researcher approached them (Mack & Anleu, 2008). One

intermediary in Massachusetts and one in Vermont were able to both vouch for the researcher and to identify judges willing to speak about issues related to digital evidence.

Finally, although the court systems in Massachusetts and Vermont are different, they have several similarities in structure and in New England traditions. In general, states have two levels of court, namely, trial and appellate (Figure 5). Criminal and civil cases are heard at the trial level, while appeals of a verdict or decision from the trial court based upon state constitutional questions are heard in an appellate court (Kerr, 2009). This description is simplified, as it does not account for specialized courts such as Family Court, Juvenile Court, and Probate Court but does provide a sufficient definition for the purposes of this research study. The Massachusetts and Vermont court systems follow this structure and differ largely in scale due the difference in population. Massachusetts has 6.6 million people, and Vermont has 620,000 (U.S. Census Bureau, 2010).

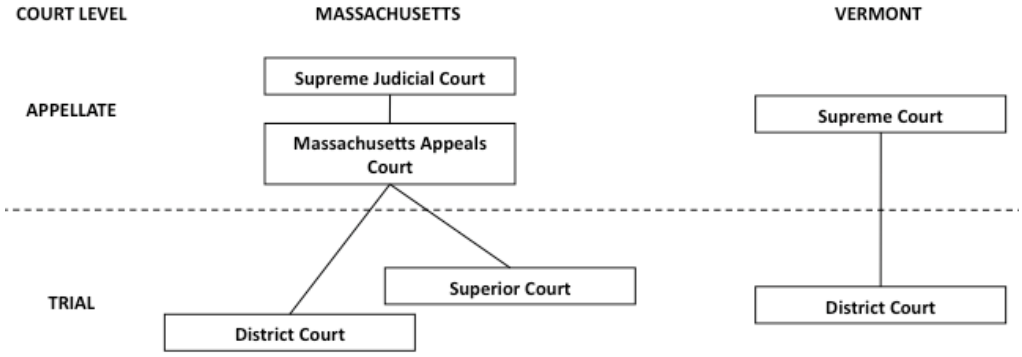

Figure 5. Criminal court levels in Massachusetts and Vermont.

Massachusetts has two trial court levels. District Courts, of which there are 62, hear minor criminal and civil cases. Superior Courts, one for each of the state's 14 counties, hear more serious criminal matters and large civil cases. Appeals from the trial courts

usually are heard in the Massachusetts Appeals Court, while some appellate cases go directly to the Supreme Judicial Court (Massachusetts Courts, 2010).

Vermont has the same basic model as do other states but has only two court levels. Most criminal and civil cases are tried in District Court; there is one court in each of Vermont's 14 counties. The only appellate court in Vermont is the Supreme Court (Vermont Judiciary, n.d.).

Seven judges agreed to be interviewed for this research study. All interviews were conducted between January 1 and March 31, 2010, and took place at a time and location chosen by the interview participant (in all but one case, their chambers). Each participant was provided with a list of the questions (Appendix D) at the beginning of the interview. The researcher followed the main questions in the order provided, asking the listed follow-up or other clarification questions as required. Each interview was taped and lasted between 30 and 50 minutes.

Output

The third, and final, stage of the research study is the Output, which, in this case, is a training and educational framework for judges related to digital evidence. The educational plan does not have a research methodology, per se, associated with it. Instead, it is derived from the findings discussed in Chapter 4 and the conclusions discussed in Chapter 5. The educational plan is described in the Recommendations section of Chapter 5.

Summary

This qualitative research study employed grounded theory to explore and gather initial data about judges' awareness, understanding, and perceptions of digital evidence (Charmaz, 2006; Leedy & Ormrod, 2010; Robson, 2002). The research was performed in a three-stage process: initial data gathering from judges across the U.S. via a written survey instrument, follow-up data gathering via face-to-face interviews with seven judges in Massachusetts and Vermont, and the development of the framework of an educational plan for judges in regard to digital evidence.

Chapter 4

Results

This chapter presents the major findings of the study. The study was conducted in two phases, an initial written survey followed by a series of face-to-face interviews. The chapter begins with the survey findings, including how the surveys influenced the design of the interview process, and the results of the interviews. Since grounded theory is derived from data and illustrated by examples, inferences from the data will be supported by quotes from participants (Carlton, 2006; Charmaz, 2006; Glaser & Strauss, 1967).

Survey Findings

As discussed in Chapter 3, a survey was distributed to the membership of the ABA/JD and NJC during the late summer and early fall of 2009. Notice of the surveys was sent to more than 10,000 members of the organizations' e-mail lists, but only 18 surveys were returned. Due to the low return rate, the researcher decided to employ face-to-face interviews for the next phase of data gathering rather than to employ a second survey as originally planned. Nevertheless, the surveys provided general findings with which to formulate questions for the follow-up interviews. This section presents the noteworthy findings.

In the sections below, references to specific survey questions will be in the form "(Q*n*)," where *n* is the question number. References to individual survey respondents will be in the form "(P*n*)," where *n* is the respondent identifier.

Survey Respondent Demographics

Although 18 surveys were returned, only 13 of them contained useful data, as five individuals returned essentially blank surveys. This was largely due to an error in the setup of the survey instrument.

The survey was first distributed in person at the annual meeting of the ABA/JD on July 31, 2009. The first question on the original version of the survey (Appendix B) was: "Has any party offered digital forensic evidence (or evidence from the computer forensics process) in any evidentiary motion or trial over which you have presided? (YES/NO)," followed by, "If your answer to question 0 is 'no,' please skip to question 11."

Five respondents answered "no" and left the remainder of the survey blank. When this design flaw was detected, the first two questions were reversed and respondents were no longer told to skip to the end. The updated version of the survey was subsequently sent to the ABA/JD and NJC e-mail lists. Table 2 presents demographic data for the 13 respondents.

Relevant correlations also were determined. For the 13 data points, $df = 11$, alpha = .05 (two-tailed), and the critical Pearson value = .553 (Terrell, 2006). The statistically significant correlations were as follows: between age and CF&E ($r = -.609$), between age and IT ($r = -.665$), and between YB and IT ($r = -.765$). These correlations indicate that younger individuals are more likely to be familiar with technology (Arning & Ziefle, 2007).

Table 2. Demographic Data for Survey Respondents

ID	CF&E	IT	Mean	YB	Age	Sex	Local	National	Population
P2	1.0	3.0	2.0	10	52	F	≥	<	100-500K
P3	2.0	2.0	2.0	20	55	F	=	<	100-500K
P4	2.0	2.5	2.25	10	53	F	=	=	No data
P6	2.5	2.5	2.5	7	51	F	>	<	< 50K
P7	3.0	3.0	3.0	10	56	F	>	>	1-5M
P9	1.0	1.0	1.0	15	64	M	<	<	50-100K
P10	2.5	2.5	2.5	20	58	M	=	=	< 50K
P11	3.0	4.5	3.75	6	53	M	>	≥	0.5-1M
P13	1.0	1.0	1.0	28	65	F	<	<	> 5M
P15	3.5	4.0	3.75	9	51	F	>	>	1-5M
P16	3.0	2.0	2.5	20	47	M	>	=	1-5M
P17	2.5	4.0	3.25	8	46	M	>	>	> 5M
P18	3.0	3.5	3.25	6	52	F	=	=	> 5M

Note. CF&E = Familiarity with computer forensics and digital evidence; IT = Familiarity with computers, the Internet, and IT; Mean = Mean of the CF&E and IT values; YB = Years on the bench; Local = Knowledge of computer forensics and technology relative to other local judges; National = Knowledge of computer forensics and technology relative to other national judges; Population = Population range of respondent's jurisdiction.

None of the survey respondents was an appellate judge. This was expected, given the experience of the researcher while attending the ABA/JD meeting for the purpose of distributing the original survey. At least half a dozen judges approached the researcher to say that they appreciated that the survey was being conducted but that they would not be participating because, as appellate judges, they did not see and make judgments about evidence, in general, particularly digital evidence. The lack of familiarity with digital evidence may be common among appellate judges, as all 18 survey respondents, including the five who submitted no usable data, were trial judges.

Definition of Digital Evidence

The definition of digital evidence provided in the survey (Q1 in the original version, Q0 in the revision) was intended to give all respondents the same baseline definition from which to work. The definition was taken from various sources in the literature and approved by the researcher's advisory board. All of the survey respondents, except one, agreed that it was a good starting point for discussion. In an attempt to provide a common starting point but not be overly leading, the researcher purposely used a definition that spoke broadly about sources of digital evidence (e.g., computers, networks) but did not provide examples of what actually comprised digital evidence (e.g., e-mail messages, cell phone call logs, registry contents, Web pages). The one editorial comment from a respondent, one who considers himself to be highly technically aware, only offered language suggesting the identification of additional sources, but not types, of digital evidence. Neither the respondent pool nor the advisory board suggested language clarifying what digital evidence might actually be.

The matter of defining digital evidence might, in and of itself, be confusing. While attending the ABA/JD meeting, several judges told the researcher that they would not participate in the survey because they had no experience with digital evidence or, at least, believed that to be the case. One stated, "I don't see any digital evidence in my court, well, except for e-mails." Other judges stated that their courts were too small to handle digital evidence but did not clarify or expand on those observations.

There also appeared to be some confusion about evidence that is obtained from digital devices owned by a suspect, victim, or witness, using a digital forensics process as opposed to evidence that is presented to the court in a digital fashion. As an example,

one of the survey questions asked about the type of cases in which a judge might be more likely to expect to see the introduction of digital evidence (Q4A). Three judges listed criminal cases, with two, who were among the higher self-rated respondents in terms of familiarity with the digital forensics process and technology (P7 and P15), specifically citing an expectation of seeing wiretap, audio, and video recordings, in addition to computer analysis. These recordings are certainly digital in nature because that is the way in which they are stored, but they are not forensic evidence extracted from a digital device.

Knowledge of the Computer Forensics Process and ICT

The survey respondents were asked to rate their knowledge of the computer forensics process, digital evidence, computer technology, and Internet applications. Respondents used a 5-level Likert scale, with 1 = low and 5 = high (Q7). As shown in Table 2, the mean score was 2.5, with familiarity of the computer forensics process and digital evidence averaging 2.3 and familiarity with ICT averaging 2.7.

Mack and Anleu (2008), the advisory board, and several leaders of national judicial organizations suggested that judges would be hesitant to acknowledge deficits in their own knowledge and, further, would not want a light shined on those areas where their knowledge might be construed as weak. These self-ratings, however, mostly in the 1 to 3 range (average to below average), suggest otherwise. Indeed, the (albeit few) judges who responded to the survey were quite open about the things that they did not know.

Related to this, the survey respondents tended to believe that judges nationally know at least as much about digital evidence and the computer forensics process as their local peers (Q9). Table 2 shows that all survey respondents except one (P11) rated their own

relative knowledge compared to local peers at the same or a lower level than their knowledge compared to their peers nationally. This implies that the respondents felt that there was a greater body of knowledge in this subject matter available nationally than there might be locally. Again, the answers spoke to the willingness of the respondents to acknowledge that others might know more about these topics than they.

All of the survey respondents except one (P16) rated their knowledge of ICT as greater than or equal to their knowledge of computer forensics. The level of technical training and experience varied widely among the survey participants; this would be expected in any population of individuals and more so, perhaps, in this group, given the range of self-reported scores by these respondents.

Most of the respondents (10 of 13) claimed that their own personal experience influenced their reported familiarity with ICT and computer forensics (Q8). While some judges cited the experience of having been a litigator prior to being a judge as influencing their score, several reported their own technical computer experience, such as one having a background as a software developer and another having used "computers . . . since the TRS-80, Osborne, and early PCs" (P17).

In general, the judges who scored higher in familiarity with ICT also cited formal education or training in information technology and/or use of computers as a hobby or personal interest. None cited judicial training or education. Indeed, the wide variance in background can be exemplified by the following two comments: "No professional training in the area & very limited use of computer technology with staff assistance" (P9, IT score = 1.0) and "Have worked with computers since mid 70s. I'm also gadget happy & love electronics" (P15, IT score = 4.0).

Role of Testimony

Four of the respondents reported that their courtroom experience and the testimony offered at trial informed their understanding of computer forensics and digital evidence. One respondent (P7), in particular, cited courtroom experience as the sole influence. Notably, all respondents who cited testimony at trial as an influencer rated themselves in the 2.0-3.0 range (with a mean of 2.5) for their CF&E scores. This information is suggestive of two questions. First, when a judge learns information at trial, how much is general and can be applied to later cases versus how much is case-specific and not generally applicable? Second, from whom is the judge primarily learning—attorneys or expert witnesses?

To the latter point, four of the respondents specifically cited the importance of the attorney's ability to understand and explain technical evidence in simple language to the judge's own learning (Q10). Seeing the attorney's role as one of educating the judges is consistent with the judge's role as an arbitrator or referee rather than as an advocate for one party or the other (Kerr, 2009). To that point, one respondent stated, "If the attorneys understand it, they can educate me. I can learn it" (P13).

The attorney's understanding of digital evidence and his or her subsequent presentation "affects [the judge's] ability to understand just what is being presented" (P10). This suggests a double-edged sword; if the attorneys at trial are educating a judge, the judge's learning can never be greater or more accurate than that of the attorneys. In this way, a technical misunderstanding by an attorney can become a misrepresentation of facts at trial, incorrect learning by the judge, and, ultimately, poor decisional law. Absent

a challenge by opposing counsel or external training/education, judges may know only what attorneys tell them. (This issue is addressed further in the sections below.)

Witnesses presenting technical evidence also play a role in educating judges. The majority of survey respondents said that the training and experience of a digital forensics examiner were sufficient credentials for acceptance of their testimony about digital evidence, and detailed knowledge of how particular tools work is not a necessary requirement (Q6). This speaks to the issue of whether a computer forensics examiner should be called as a technical witness (i.e., to explain the specific process in this case, what was done, and what was found) or as an expert witness (i.e., to explain the theory behind the process, describe the details about the architecture of the tools that are used, and offer opinions).

Most of the judges, and most of the researcher's advisory board, felt that testimony at a technical level is preferred and usually sufficient for trial. In most cases, the complexity of the evidence or process being presented is generally the key to the decision of putting a technical or expert witness on the stand. As one respondent observed, it "depends on whether that particular digital tool had already and consistently passed the *Frye* Test; if 'yes,' then I would require only that the examiner show sufficient training and experience [in how to use the tool]" (P10).

While having a computer forensics examiner testify as a technical witness is often a good trial strategy, there are times when an expert witness is required, such as when a *Frye* or *Daubert* challenge is mounted against the process, methodology, or interpretation of the evidence, or when the digital evidence is the linchpin in the case (Casey, 2011; Kenneally, 2001b). Some judges stated that they prefer expert testimony because it

removes some of the mystery about how any digital evidence was found and what it revealed, as exemplified by this statement:

> How it works. When testifying that these documents are what was found, can you tell me how the program looked. Similar to current non-digital technology. Telling me that you looked and there are no medical records for a particular person is not sufficient if you cannot describe that you know where the files are kept, that you are familiar with alphabetical or numerical system used in the file room, and that you looked in the correct places to be able to say there are none. The equivalent familiarity with the 'right' digital place will also be needed. (P17)

Witnesses may, in fact, be as important to judges' learning as are attorneys. When discussing the role of the standard of technical competence to which attorneys are held (Q10), one respondent noted that it is not the lawyers who need to be technically competent but rather the witnesses (P4). Indeed, one of the advisory board members stated that a "sub-par attorney can be saved by a knowledgeable, articulate, likeable expert."

The requirements of the *Frye* and *Daubert* standards also seemed to affect the judges' views, as several respondents cited that as a factor in some of their answers to the survey. Addressing this question on the role of the technical witness, one respondent wrote, "We are a *Frye* (not *Daubert*) state, so the factors generally would focus on trustworthiness & helpfulness to the fact-finder" (P16).

The respondents' statements on the survey suggest both that judges are looking to learn from the technical witnesses and that, in this case, documented experience and knowledge alone may not be sufficient to establish trust. Indeed, as several judges and

advisory board members noted, the believability of a witness is driven as much by personality as it is by professional credentials.

Several of the respondents did not choose an answer to the technical versus expert witness question, writing “both” (P2), “don’t know” (P9), or “depends on case” (P18). The general sentiment was summed up by an advisory board member who wrote that a witness should be evaluated the “same as any other examiner/tool used for any other scientific/technical matter that is latent in nature.”

Issues with Digital Evidence

Nearly all of the respondents stated that their issues or potential questions related to digital evidence (Q2) were essentially the same as with any other type of evidence, namely, is it relevant, is it authentic, and was it seized and searched in a manner consistent with the Constitution and Rules of Evidence? In the words of one of the respondents, the digital evidence has “many of the same issues as (physical) evidence with special focus on chain of custody” (P16). The advisory board echoed these sentiments, citing many of the same concerns, such as spoliation (destruction) of evidence, proper acquisition procedures, staying within the scope of a search warrant or other court order, and weighing the probative versus prejudicial value of the evidence.

All of the respondents mentioning relevancy of evidence as the major factor in acceptance have served on the bench between 6 and 10 years and had IT scores of 3.0 or greater. Those citing authenticity as the major factor in acceptance have served between 10 and 28 years, and had IT scores of 2.5 or below. This bifurcation, although not known to be statistically significant, suggests that the longer serving, less ICT-minded judges want to ensure authenticity of the evidence before admitting it, while less senior, more

ICT knowledgeable judges are primarily concerned with the relevance and the reason that the digital evidence is being introduced in the first place. One possible explanation for this is that the latter group feels more confident in the authenticity of the digital evidence being offered and is, therefore, looking beyond to the relevancy factor.

Caloyannides (2003) and Van Buskirk and Liu (2006) stated that less technologically aware judges are more likely to believe in the accuracy of computer-derived digital evidence. The survey results, albeit based upon a small number of respondents, suggest the opposite; the less ICT-knowledgeable respondents seemed the most wary about the authenticity of the offered digital evidence.

The question of authenticity was particularly interesting because the respondents who cited this as an issue wrote specifically about non-digital manifestations of digital evidence, such as playing cellular phone messages out loud in court directly from the phone, reading cellular telephone text messages aloud, or viewing printouts of Google maps or Web pages (P4). There were no comments about questioning the methodology or forensic correctness with which these items were originally found.

The results are also suggestive that the more ICT-aware judges ask more technical questions about offered evidence. Some of the questions about digital evidence related to the redacting of personal identifying information (P7), erasure of information (P11), and the cost and ease of producing information for discovery (P11). The less ICT-aware respondents indicated similar concerns about digital evidence as they would have for any other type of evidence, such as data tampering (P10), business records as an exception to the hearsay rule (P13), and chain of custody (P16).

Standard of Quality

Ten of the 13 respondents stated that they would not hold digital evidence to a higher standard of authenticity than they would for physical evidence (Q3). Instead, the prevailing attitude seemed to be that the authentication method might be different for digital evidence than for physical evidence, but the standard requiring authenticity is the same. The researcher's advisory board unanimously held the same view.

Although there was general agreement that authentication was the standard for admissibility, concerns were still expressed about how this standard was to be applied. At one end of the spectrum was the respondent who wrote that digital evidence should be held to the "same standard applied to a different setting" (P18). But even with that observation, a concern was expressed that digital evidence should be held to the "same standard—but often [that standard is] not satisfied" (P7). This last comment focused on the reliability and accuracy of the source (e.g., e-mail, Web pages) that would be required to authenticate digital evidence (P2 and P7).

At the other end of the spectrum was a respondent who agreed that digital evidence should be held to the same standard as digital evidence, yet wrote, "I am still struggling with the standard" (P13). This comment, in spirit, matched those of the respondents who wrote that digital evidence should be held to a higher standard than physical evidence (P2, P9, and P10). Among this group, plus one other respondent, was the concern that digital evidence could be altered by a third party (P2, P6, P9, and P10). This possibility also exists with physical evidence, of course, but two of these respondents specifically cited a concern that digital evidence might be remotely altered (P6 and P10), an astute observation given that mobile telephones, for example, can be wiped clean of evidence

by remote command while locked in an evidence room (Mislan et al., 2010). One judge wrote that he had "only hearsay that original source can be manipulated, changed or appear to originate from some source other than the true source" (P10). He also stated that his concerns would be alleviated if there were court rules that required specific steps to be taken to add to the certainty of the authentication of digital evidence.

Marsico (2004), Neufeld (2005), and Van Buskirk and Liu (2006) indicated that there are few challenges to digital evidence offered at trial. One respondent wrote about this very issue:

> Offering something printed off the web to prove the facts on the webpage is rarely enough. We all know web pages and web addresses can be faked, as evidenced by a recent news reports about fake emails from someone appearing to be the IRS. Thus I reject such things IF OBJECTED TO (which does not always occur—other side often does not object) absent someone with actual knowledge of the facts or a custodian of records to authenticate. (P4)

This respondent made it clear that she would accept evidence offered by one party if the other party did not object. As above, this speaks to the role of the judge as one who ensures a fair trial according to the rules of procedure rather than advocates for one side or the other (Kerr, 2009).

One respondent focused on issues related to e-discovery. While stating that he believed that digital evidence should be held to the same standard as physical evidence, he also observed that this standard might be more difficult to establish with e-records due to a lack of conceptual understanding of e-discovery by judges, lawyers, and others throughout the legal system. The first factor cited was the question of whether judges

have “comprehension of underlying terms and technology” (P17) with which to establish the competency of the records custodian. In particular:

> Common experience allows anyone to understand that papers are in a filing cabinet, that the custodian looked through the right drawer in the right cabinet and found these papers here today. Until there is a more universal understanding of digital records, fewer people understand that there is a peripheral(s), a server, auxiliary memory, and that data is saved here, archived there, and how your search program identified what is here as evidence today, and what makes you competent to say, and comfortable to say, that these documents today are the sum total of what there is that is responsive. (P17)

The second factor cited in establishing authenticity of e-records was a custodian who could competently and simply explain to a fact-finder that a search was thorough and complete as well as how it was accomplished.

Digital Evidence in Court

The survey respondents addressed the question related to the presentation of digital evidence in court (Q5) in two ways. Eight of the respondents, all with digital forensics and IT scores of 3.0 or less, focused on the actual courtroom presentation style. Comments from this group cited the need for the use of demonstrations, charts, printed documents, and/or simple PowerPoint presentations to effectively communicate information to the fact-finder.

The remaining respondents were generally more ICT knowledgeable, with scores of 2.5 or higher. The focus of their concerns was the quality of the explanation of the digital evidence being offered. Comments here included the points that effective presentations of digital evidence needed to include explanations of how digital systems work and why

digital evidence is reliable and that a clear foundation for the evidence should be established by an expert. Indeed, simple explanations about ICT that respect the listener are most effective, or, as one respondent wrote, "Competency without contempt for those who must understand technical processes" (P17).

The advisory board was also split when offering comments on this question. Approximately half mentioned issues related to the presentation style, while the remainder addressed the technical content of the evidence itself. While both are important, it appears that the less ICT-minded look to style while the more technical look at content.

Summary of Survey Findings

The sections above represent the themes that emerged from the data in terms of the interaction of judges with digital evidence. Many of these themes coincide with themes that have been suggested in the literature (although not formally studied) and/or substantiated by the researcher's advisory board, while some are suggestive of new information. In summary, the findings from the survey include:

- There is an inverse correlation between age and familiarity with digital forensics, age and familiarity with ICT, and years served on the bench and familiarity with ICT.
- There is some confusion about clearly defining what digital evidence is as opposed to describing where digital evidence might come from.
- Respondents generally rated their knowledge of digital evidence and the computer forensics process at a level less than they rated their knowledge of computer and Internet technology.

- Respondents generally felt that judges nationally knew as much or more about computer forensics as did judges in their local geographic area.
- Respondents generally appeared to feel free to discuss weaknesses in their knowledge, despite suggestions from the literature that they would be reluctant to do so.
- Respondents who rated their knowledge of ICT at a high level generally cited their own background and experience as the influencing factor; none cited judicial education as a factor.
- No respondent cited attending any judicial training related to digital technology or forensics.
- One of the important roles of attorneys and expert witnesses is to inform and educate judges about digital technology and forensics.
- Judges are arbiters of a fair process and not an advocate for one party or another; therefore, a judge will not make a decision about the admissibility of evidence unless one party objects to it.
- Most judges are satisfied with a technical witness who can demonstrate sufficient training and experience with digital forensics tools and processes rather than require the use of expert witnesses to offer opinions.
- The effectiveness of a technical witness is as much, or more, based on whether they come across as being believable and trustworthy than whether they are an actual expert.

- Judges have the same issues with digital evidence as they do with physical evidence, namely, Constitutional issues of seizure and search, Rules of Evidence, relevance, and authenticity.
- Longer serving, less ICT-minded judges focus more on the authenticity of digital evidence while newer, more ICT-aware judges are more concerned with the relevance of digital evidence.
- Most of the respondents believe that digital evidence is particularly prone to tampering and the introduction of bogus data and that some digital evidence is prone to remote access and alteration.
- Less ICT-aware judges are actually wary of digital evidence, despite suggestions from the literature that they would be more accepting of it.
- Many judges still see information offered in court from digital sources that are obtained in a non-forensic fashion (e.g., printouts of Web pages and e-mail messages).
- Judges who are more ICT-aware ask more technically involved questions when determining admissibility and authenticity of digital evidence than their less ICT-aware peers.
- Less ICT-aware judges tend to focus more on the style or form of testimony, while the more ICT-aware judges looked for technical content.
- Judges generally report that e-discovery processes are complex, expensive, and not well understood by most members of the legal system.
- Attorneys rarely raise a *Daubert* or *Frye* challenge to digital evidence.

- Effective presentation and testimony about digital evidence requires clear, simple, non-condescending testimony.

Interview Findings

The initial survey findings led the researcher to develop an interview questionnaire with which to further explore themes that emerged from the initial surveys. No decision was made to follow up one theme at the exclusion of another; instead, questions were formulated to solicit more information and insight into the subject matter. Upon review of the surveys, and in conjunction with the advisory board, the questions for face-to-face interviews were developed (Appendix D). The interview participants were asked to answer the questions in any way in which they felt most comfortable and not to hesitate to tell stories and/or go off on what they might perceive to be tangents.

Interview Participants

Seven judges were interviewed for this phase of the study. Due to the small population from which they were drawn, specific individual demographic information was not collected, as it would significantly compromise the anonymity of the respondents. Nevertheless, the breakdown of the judges' courts and states can be inferred from the quotes that appear later in this section and is provided here: (a) two participants (P1 and P2) were Supreme Court Justices from Vermont; (b) two (P3 and P4) were District Court judges from Vermont; (c) one (P5) was a District Court judge from Massachusetts; and (d) two (P6 and P7) were Superior Court judges from Massachusetts.

In addition, six of the judges were male and one female; gender did not seem to be a factor in any of the responses or observations. (To preserve anonymity, the male

personal pronoun is used to refer to the judges in the remainder of this section.) All of the judges had professional experience as litigators prior to serving in their current roles; two served as civil or criminal defense attorneys, and five were prosecutors before assuming the bench.

Authentication of Digital Evidence

As with the written survey respondents, authentication was identified by all of the interview subjects as the crucial criterion for admission of digital evidence into the record. Evidence, in general, comes before a judge in one of two ways, namely, by being offered at trial or as an attachment to a motion. In the former case, any debate about the evidence is verbal, while, in the latter case, debate is in the form of written motions. All of the judges stated that arguing the merits or weaknesses of the evidence is left to the attorneys and witnesses. In this context, the evidence needs to be shown to be real, correct, and what it purports to be. In that respect, traditional requirements for authentication of evidence apply equally to digital evidence.

All of the judges spoke about the importance of the authentication process but largely maintained that authentication of digital evidence is fundamentally the same as authentication of any other document, photograph, or similar evidence. As the survey respondents also suggested, the interviewees indicated that digital evidence would most likely be admitted absent a challenge from the other party. If a challenge is presented, an individual who has firsthand knowledge of the evidence might be asked to testify to its authenticity.

The judges also agreed that there is rarely a *Daubert* challenge to the authenticity of digital evidence. While challenges to the admission of digital evidence are relatively

common, such challenges are usually based upon procedure (e.g., the legality of the seizure or search of the evidence) and believability rather than on reliability and authenticity. As one judge stated, a lot of disputes over evidence, particularly in criminal cases, are around admissibility. At a suppression hearing, then, "the judge makes a decision not whether the evidence is correct or incorrect but whether it's admissible, meaning whether it could be construed as credible" (P4). The observation that there are rarely *Daubert*-based challenges appears to be consistent with the suggestions of others (Marsico, 2004; Neufeld, 2005; Van Buskirk & Liu, 2006), although there are more challenges to digital evidence than these other authors imply.

The digital evidence about which the judges spoke about in their interviews can be broadly categorized as communications (e.g., e-mail, text messages) and Web-based documents (e.g., Google maps, social network pages, general Web pages). None of the judges made any reference, outside of the context of e-discovery, to deleted files, browser cache and history files, calendar and address book files, documents, spreadsheets, temporary files, or any other of the myriad sources of information that would typically be found on a computer. It appears, then, that this kind of information is not what the judges typically see, and, although they might be able to identify these as sources of digital evidence, they are not the most obvious.

Authentication of E-mail

All of the trial judges spoke specifically about e-mail and text messages as the primary form of digital evidence that they see. Authentication of this type of evidence is generally based upon the sender and receiver agreeing that the offered message was the one that was sent and received.

In the case of a challenge, three of the five trial judges said that they would rely on an expert to testify as to whether the e-mail or text message did, in fact, come from the sender. Since e-mails are usually printed out when presented as evidence, one judge stated:

> I'm more skeptical about e-mail because, on a pure gut level, it looks to me like you could just type out a page and have it look exactly like an e-mail message so, you know, there's nothing that says where it came from or that it can't be duplicated or faked. But, I don't know, actually, unless I have some certificate from someone at [the ISP] saying, 'Yep, this is actually from Joe Smith's e-mail account because we see it here.' I'm not sure what else would convince me. (P3)

Third parties have a role in authenticating e-mail messages because e-mail servers and ISPs play a part in their transfer and, therefore, in testifying about their authenticity. In the words of another judge:

> I suppose that I would then require the party that's trying to get it in to present a person who can authenticate that this is something that was taken off of whatever archival or storage media they have, which would probably mean bringing in an IT person to swear under oath that he or she has certain responsibilities including . . . your basic record-keeper position. And that what this piece of paper reflects is digital information that is contained in the specified media and archives that they're responsible for maintaining, and this is how I got it out and this is what it is. And then I'd hear argument about whether that's sufficient or not, but that's probably what I would hear. (P7)

Another judge observed that the content and context of a message play a valuable role in aiding in authenticating messages that are in dispute, citing one of his cases when there was:

> sufficient identifying information in the text of the e-mail itself, various facts and things that were said to the recipient that could only come from the defendant, that I was satisfied that it was sufficiently identified. I allowed the evidence to come as the statement of the defendant. It was not seriously challenged after that. (P5)

Only two judges, both of the higher Massachusetts court, felt that they had an understanding of how e-mail moved across the Internet, although one said that he did not "know if it's a good understanding" (P6). The other five judges all reported that they did not feel that their technical understanding of e-mail was sufficient to determine authenticity, without the aid of an expert witness.

Authentication of Web Pages

Four of the trial judges spoke about the issue of the authenticity of Web pages, which are generally introduced as evidence in the form of printed pages. All indicated that they had a basic understanding that Web pages were containers of information that someone put on the Internet, that Web pages could link to other Web pages, and that the information contained in a Web page is not inherently reliable or correct. The level of understanding of the Web appears to be higher than that of e-mail as is the level of wariness in accepting a printed document as a real and true representation of a Web page.

The primary issue that judges face is the ease with which information can change on the Web or with which a printed document is altered. As one judge noted:

> I mean, what would I look at? If it's a Web page; when? At what point in time? How do we know that it is this Web page and not something doctored? It's the kind of thing that you'd ask for with any other piece of evidence that's subject to being faked. The fact it's technologically produced rather than by paper; the thinking process isn't any different. (P4)

As to the reliability of the information on a given Web page, another judge stated:

> I'm aware that Web pages, Web sites can be set up very easily by people who don't have to invest a whole lot of time or money to figure out how to do it. At least that's my impression. So I have a healthy skepticism that they're anything more than something somebody put up on the Internet. (P7)

In the same vein, one judge told of a product liability case over which he presided:

> The big question was whether or not a warranty or warning was communicated from one party to the next party. And one of the lawyers had a page off the Web site and said, 'See, on this page it says that you're supposed to [take a certain action]' and I didn't allow it in because there was nothing to tell me when that page was created, anything like that. (P6)

For this judge, authentication would have been substantiated if there had been a witness called who could testify about the page's contents on a certain date (either a record-keeper or a corporate spokesperson) rather than an offering of an uncorroborated piece of paper. He concluded by observing, "I think they could have done a better job with that" (P6).

Authentication and Impact of Social Networks

All of the judges spoke about Facebook and other social networks, specifically to state that they did not personally use them. In large part, the reasons cited were related to the potential appearance of a conflict of interest, problems that other judges have had (ABA, 2009b), and the recommendations of the ABA (2007).

In terms of evidentiary value, the judges all recognize that a Facebook page can be altered, either when printed out or online by a third party, which can affect the value of the evidence at trial. As one judge noted:

> I had a case that involved somebody's Facebook pages being submitted as evidence against them to show an inappropriate sexual relationship with a child. I don't really understand how Facebook works, I don't have a Facebook page . . . So, I certainly may have the thought, 'Well, gee, could someone else have put that on his Facebook page to plant it?' I don't know, I don't have any idea whether that's possible. I mean, I'm sure it is if someone's sophisticated enough. How easy is it for this young woman on the other side; is she sophisticated enough? . . . But those are questions that in that case came to mind but the other side didn't raise them so I didn't even go down that path. (P3)

Social networking is also having an impact on the very functioning of the court. Three of the trial judges stated that they had changed their jury instructions within the last few years to admonish jurors against use of services such as blogs, Web pages, Facebook, and Twitter to post messages about an ongoing trial, citing their fear of what one of them called a "Facebook mistrial" (P6). The concern is well founded, given the many cases for which the Internet has been cited as a factor in a mistrial (Schwartz, 2009).

Authentication of Google Maps

Three of the five trial judges specifically mentioned Internet-based maps as a source of evidence requiring authentication. Unlike other forms of digital evidence, a printed document generated from Google Earth, Google Maps, MapQuest, or another map service can be compared to something in the real world rather than a printed piece of paper that depicts the virtual existence of an e-mail, Web page, or Facebook page. As with other forms of digital evidence, a judge might be skeptical about the accuracy of an offered map but will probably admit it, absent an objection from the other party. The precision of a map can be important since it could affect the charges made against a suspect or the sentencing of a guilty party. As one judge explained:

> School zone cases are a classic example, where they used to pull a map off of Google to show that a certain drug transaction took place within 1,000 feet of a school, which is a separate offense since schools [are a drug-free zone]. I've seen objections on the use of the map; how do we know this map is to scale? The police officer or the map guy from the town comes in and says that this is the map that they used. 'Where'd you get the map?' 'Oh, I pulled it off the Internet.' 'Well, you didn't create the map yourself? You didn't take the photograph? Well, how do you know that this is to scale? Who knows what the distance is? You're going off a map. Well, who made the map? Why don't you bring that person in and tell us?' (P5)

Other judges throughout the country face this problem, as well. Dipalo (2010), for example, reported that a Pennsylvania judge accepted a map from Google Maps into evidence after prosecutors brought in a cartographer to verify the accuracy of the printed page.

Role of the Daubert Test

Both Massachusetts and Vermont follow the *Daubert* principles when evaluating scientific and technical evidence. Massachusetts follows a modification of the *Daubert* tests based on the case of *Commonwealth v. Lanigan* (1994), for which there is a heavier reliance on general acceptability of the scientific method than on proof of the method's reliability (Daley & Allen, 1999).

Several of the judges volunteered that the *Daubert* rules make the introduction of digital, as well as other scientific and technical, evidence easier rather than more difficult. One of the Vermont trial judges cited Vermont Supreme Court opinions that make it clear that the rule is intended to let evidence in rather than exclude it unless it is "clearly junk" (P3).

Two of the Massachusetts judges made similar observations. The *Daubert-Lanigan* tests focus on the reliability of the evidence guided by the judge's primary concern over general acceptance of the methodology by the relevant scientific community. While one judge commented that the decision "liberalizes the admission of a lot of evidence" (P5), the other noted that acceptance of evidence is "not simply purely quote hard science and hard technology" (P7).

Role of Attorneys

The consensus of the judges is that it is the role of attorneys to introduce evidence to the Court, to make arguments about why that evidence should (or should not) be admitted, and to speak to its accuracy and truthfulness. As with the survey respondents, all of the trial judges (and one of the appellate judges) were clear that it is the job of the

lawyers and their expert witnesses, if needed, and not the job of the judge, to argue the merits of evidence and/or raise challenges to it. As one of the judges explained:

> From a trial court perspective, in an adversary system that we have, I primarily rely upon the attorneys to see how successful the opposing attorney is in either attacking the foundation or the purported source of the evidence and from whence it derives, and see if the other side can either rehabilitate it, if necessary, or simply overcome the challenges by demonstrating, probably through expert testimony, depending upon the degree of attack, why it should be relied upon and be what it purports to be. (P1)

The judges were unanimous in their statements that it is the role of the lawyers to educate judges, as necessary, about evidence, including digital evidence. Indeed, while the judges feel comfortable with the rules of evidence and court procedures, attorneys need to educate the judges about specific evidence at a given trial. The technical nature of digital evidence has particular challenges when informing the Court. As one of the judges stated:

> I've seen people testify on computer forensics, it's extremely highly technical. I find that, in a lot of cases, that the jurors—much of it went over their heads even with an expert trying to explain it. I find that a lot of experts have a hard time bringing it down to a layperson's level. And I understood it the best I could but I would rely on the witness to relay that to the jury. (P5)

Several of the judges suggested that the technical nature of digital evidence and the difficulty of its being understood by laypeople might also extend to many lawyers themselves. One judge observed, "A lot of times attorneys don't themselves have the

knowledge or the awareness that they could be objecting to [digital evidence] on the grounds, 'How do we authenticate this?'" (P5).

Another judge noted that too many lawyers accept information from the Internet without question and rarely mount a challenge. Even then, most challenges are not on technical grounds. Said this judge:

> A lot of lawyers kind of treat the Internet as if it's all fine. You know, you print it from Google Maps and that's all I need, and surprisingly there's not an awful lot of objection to that sometimes. It's sort of becoming accepted that you can use documents from the Internet. (P3)

These results are consistent with the written surveys and the literature (Marsico, 2004; Neufeld, 2005; Van Buskirk & Liu, 2006). Some of the studies cited earlier suggest that many lawyers believe themselves to be more aware of, and knowledgeable about, digital evidence than are judges (Rogers et al., 2007; Scarborough et al., 2009). The interviews here suggest that judges may not believe that lawyers are sufficiently aware of issues related to digital evidence as might be required for competent representation.

Role of Judges

Judges play a gatekeeper role as it pertains to the admission of evidence. But the role of gatekeeper has several subtleties and complexities, as identified by the interview participants.

To a large extent, judges have constraints on their activities, and several factors guide their overall responsibilities. The roles of the trial judges and appellate judges are different, and the standards of review that guide appellate judges allow them less discretion than trial judges are allowed. As one appellate judge explained:

> An appellate court is not a court of original jurisdiction except in a few very limited circumstances. We don't try cases, we don't take evidence in our courtroom, witnesses do not appear before us to testify. What we do is pass judgment on legal issues that are raised by the parties that have come up during such proceedings, so that we do review rulings that are made by trial judges on evidence that is taken in the trial court, we pass judgment on those rulings under laws that are established by the legislature, under rules that we have established for proceedings that take place in court, and under precedent in case law where a similar or same question has been raised before. (P2)

When it comes to the question of evidence, appellate judges examine evidence only if an objection is raised and, even then, only to determine whether the evidence had been properly admitted or excluded according to rules of evidence. As the appellate judge further stated:

> An appellate court would look at an objection to the authentication of digital evidence for purposes of determining whether or not it meets the applicable evidentiary rules. So, in the first instance, it would depend upon whether an objection was made. If a party in the trial court offered a piece of evidence, let's say an e-mail message that was printed out and offered perhaps to impeach a witness, there could be an objection raised to that based on whether or not the document was properly authenticated. If no objection was raised, which sometimes could occur, we, of course, would not see it. (P2)

This statement is consistent with the views expressed by several appellate judges at the ABA/JD meeting who did not take the initial written survey. They all reported that

they had limited familiarity with digital evidence because they rarely took in any evidence at their level of court.

When asked to review a trial judge's decision about the admissibility of evidence, an appellate judge does not need to show agreement with the trial judge's decision, only that the trial judge had good cause to make the original decision in the first place. Thus, appellate judges do not make new rulings on the admissibility of evidence but only review whether the lower court made a proper decision. As the other appellate judge stated:

> Our job is just in seeing if the trial court's discretionary admission or exclusion of evidence was an abuse of discretion or not, and it gives the trial court very wide latitude. As long as you have a tenable reason for admitting it, or for that matter, excluding it, it will stand here, regardless of whether we would have done the same thing ourselves. So, reasonable judges might differ on the answer and as long as there's a rational basis for the answer given, that's good enough. Now, say, for example, we are to uphold a conclusion of law if it's supported by the findings and we will uphold the findings if supported by any evidence. So, if there's evidence suggesting A and there's also evidence suggesting Z, and the trial court picks A, as long as there's evidence to support A, we cannot say that it was an error even though we may have been more persuaded that it was Z. And these kinds of evidentiary rules are of the same sort; there are rules and the rules will set out certain little tests or formulas. As long as there's something to support each step of the formula, we will uphold the decision whether we agree with it theoretically or not. (P1)

For their part, all of the trial judges indicated that they are guided by rules of criminal or civil procedure and rules of evidence. Trial judges are also guided by precedents in case law as mentioned above, a concept known as *stare decisis* (U.S. Legal, 2010). Two of the trial judges added another factor that affects their thought process, namely, avoiding procedural errors that would provide grounds for an appeal. In the words of one judge:

> One of the things I worried about as a trial judge was about what the appeals court was going to say. I did not want to be reversed. I did not want a situation where people were going to try this case over again. (P4)

All of the judges also recognize that their own life experiences affect their thinking on the bench although they are bound by their code of conduct to be impartial and fair (ABA, 2009b). Yet, as one judge explained:

> It would be foolish to tell you that personal experience doesn't affect you. I mean, this is the question that they asked Sonia Sotomayor when she was being interviewed for the Supreme Court position last fall. You know, the idea that we live in bubbles and we don't have experience and we don't interact with human nature is absurd. And I don't think that people want judges that live in bubbles but I think they want judges who can be dispassionate, who will apply the law as it is and to the facts of the case. (P2)

Experience also applies to issues of technology, particularly as computer applications are now a part of everyday life rather than used by only a small segment of society. One judge noted:

> There's unique knowledge, or particular knowledge, and there's general knowledge. I generally know how to do word processing and generally know how documents are transmitted, although I don't know anything about documents in this particular case, so I don't have any particular knowledge. And while I say that we don't want to be driven by our experience, I think it's been settled that courts can't divorce ourselves from our common experience. (P1)

Several judges cited a concern about how much specific knowledge they can safely have without their own opinions overshadowing the arguments of the attorneys and witnesses at trial, thus interfering with the adversarial process by introducing bias. One judge observed:

> It's a mystery, which complicates the role of a judge—to get back to the ethical question. There are two messages they give us. One, we are required, in our position of judge, to be current with any number of things in the world besides the law; science certainly is one. And two, when we decide a case, we need to decide solely on the facts presented as if a blank slate. (P4)

In a related theme, another judge stated his perspective on staying current with technology by explaining:

> I don't claim to maintain currency with the technology in any way that is other than my own use of it. I've not studied it nor do I think I'm obligated to do that. I do think it's important for judges to have enough knowledge of the technology that they understand where the issues are when they arise in a given case. (P2).

Several judges noted that they would feel obligated to advise parties at trial if they believed that they had personal knowledge that would affect their decisions. This is

primarily motivated by a sense of fair play, so as to give the parties an opportunity to respond to the judge's particular knowledge rather than be blindsided by it. Said one judge:

> If we're going to make a decision that turns in part on some experience I have, I believe that it's incumbent upon the judge at either the trial level or the appellate level to say, you know, 'Based on X, I'm inclined to conclude a certain position' and, preferably, at least at the trial level or even at the appellate level, to give the advocates notice of that ahead of time so that they know what your leaning is or why you're thinking this way or not thinking this way so that they can have a chance to respond, refute, whatever your presumption is. So, a lot of this business turns on, did the parties get fair notice of what you were considering? And the ideal is that everybody's playing on the same playing field and they all have a chance to respond and no one has to get ambushed by some unknown fact that they're not familiar with. (P1)

A larger ethical issue comes in the form of independent research. All of the judges indicated that they cannot do an independent investigation of the facts related to a case but must rely only upon the evidence presented by the parties (ABA, 2007). One trial judge gave the following example of the problem:

> Judges have recently run into an ethical problem, which we never had before, which is that we have computers on the bench now. And we are able to access information about a particular topic very quickly. And sometimes that information may be at variance with what's being put into the record by the parties. You know, simple things like the location of a house on a street, where they'll testify that it's the fifth house down, and you pull up on MapQuest and it shows that it's the fourth house

down. Now, that may not seem like it's important but it could be, depending upon the circumstances. Then there's this other thing, where you're presented with conceptual information that's clearly at variance with the facts of the case. And so, judges are wrestling with that now, with concerns about whether you can [look for yourself]. (P4)

Similarly, another trial judge gave this example:

Another thing that comes up pretty frequently is that people submit certificates printed from the Secretary of State's office showing their corporation status and I kind of look at it and, you know, I've seen them online, and I know that's what they look like but how do I know if this one is valid or not? I mean, I presume that the lawyer is not giving me a falsely created document, but maybe their client gave it to them. How do I know? Are there ways that you can verify without going back on the computer and checking yourself, which we're not supposed to do because it's outside of the courtroom and it's not part of the record? (P3)

One solution, he went on to observe, is to refuse to admit evidence in the absence of such authentication but that just slows up a court system that is already mired.

These problems are not limited to the trial courts. One appellate judge noted:

So, if a case comes in that involves a subject matter that you don't know anything about, you've got to learn about it, you've got to read about it. And, they will have done that in the trial court before it gets here. So, what I would do is take the volumes of transcripts from that case, the depositions of the experts, of the forensics experts in that case, and study them and read them and understand. One of the reasons that I would limit myself to that is because under our rules, it really is not ethical to sit down at the computer and begin to compile a lot of evidence that has never been introduced

> in the trial court in the first instance. Now, that's not to say that we don't look at *Law Review* articles that are cited and maybe that are not cited by the parties in their briefs. And sometimes those articles will go quite far in describing a technological kind of question . . . But there has to be a limit to that and there's a difference, I would tell you, in judicial philosophy between judges in how far you go. (P2)

The judges clearly see the need to strike a balance between how much outside knowledge is reasonable and appropriate in terms of making them effective as jurists without crossing the line of adding potential prejudice in a given case. As one trial judge summed up:

> Your outside knowledge can be helpful to understanding what the lawyers are presenting to you and what the experts are presenting but as far as doing your own independent research into something that might come up in one of your cases, I would certainly tell any judge that you shouldn't, or even can't, do that. (P5)

The judges all agreed that digital evidence submitted by one party is likely to be admitted absent an objection by the other party. The philosophical role of the judges came to light when several observed that their personal knowledge might make them aware of a possible objection that an attorney fails to make. One trial judge stated:

> So you run into the conundrum which I've run into a number of times, where you know what the party's presenting is not only wrong but if they presented the correct information, it would benefit them. And what do you do? And, of course, that's very fact intensive how you respond to a set of circumstances. There's one theory that says that the fundamental fairness of the proceedings requires the judge to step in and make clear that there's a concern and gives the parties an opportunity to clear it up. And

there's another theory that says, no, your job is umpire; you're not supposed to be backstopping people, you're supposed to be calling balls and strikes. Which one's correct? Well, there's no bright line. (P4)

Another trial judge noted the same conundrum but observed that there may be a reason that an attorney does not make an objection. He noted:

Different judges have different theories on this. I'd say that the majority of judges will keep silent but there's a good minority who will step in. And I think that it is not my job to act as an advocate for either side. If it's something I know is objectionable and if the attorney's not going to object, I assume . . . he has a reason for it, either he's going to use this potentially inculpatory evidence to his advantage somehow, turn it around . . . so I'll leave it alone. I don't tend to step in unless it gets a little egregious and I find that the attorney is really falling down on the job. I do that to protect not only the defendant in a case like that—and it's not so much the prosecutor, I've never really seen the prosecutor need help prosecuting, so I don't get involved. But if the defense attorney's inept, and I think that the defendant's rights are seriously at issue, his right to counsel, then I'll step in. But it's rare. Because it always could be tactical, there could always be a strategic reason not to object to something which potentially could be objectionable. So I would tend, I'd say 90% of the time, to stay out and that 10% of the time is to, say, simply to save the defendant from either a wrongful conviction or a conviction based on evidence that would normally be inadmissible if he had an adequate lawyer. And to save the case from coming back on ineffective assistance of counsel grounds which I don't want to have to deal with after conviction. So, I try to step in if I think it's necessary. (P5)

Judges, of course, have an obligation to protect a greater good if there is concern about some aspect of the evidence that may not be specifically related to admissibility or the actual case. One judge offered the following:

> A very mundane example would be if someone offers a document that has somebody's Social Security number on it. Well, there's a privacy issue and I would say, if I noticed it, we need to redact that. That gets into issues that trials are public and documents are public records so, then, I have to make a finding that this Social Security Number, those are private, and, in fact, our Supreme Judicial Court just issued guidelines, an order on privacy and protecting litigants' and witnesses' privacy in court records. (P7)

The judges all acknowledged the complexity of digital evidence but observed that, fundamentally, it needs to be treated just like other forms of evidence. One trial judge summed it up as follows:

> When I looked at this issue and when I was trying to formulate my own recommendations to other judges, I told them to just basically approach it as you would any other evidentiary issue. It's not mysterious. And then it really has to do with personal knowledge or business knowledge or something to authenticate. And if you look at it that way, it either comes in or it doesn't come in. I think you just make it—maybe I'm oversimplifying it—it really comes down to basic evidence rules and I think it's completely transferrable to this medium. (P7)

There is a tension between the expectations of the level of judges' knowledge by lawyers and digital forensics investigators versus the judges' expectations themselves. Lawyers and investigators generally would like judges to have a deeper understanding of

the technical aspects and processes related to digital evidence so that they can better make decisions about that evidence (K. Muldoon, personal communication, May 6, 2010), whereas judges largely believe that it is up to the lawyers and witnesses to educate them, as noted in the sections above.

Finally, Caloyannides (2003) and Van Buskirk and Liu (2006) suggest that judges who accept digital evidence tend to grant it more credibility than it deserves. The comments by the judges in the interviews and in the written surveys suggest otherwise. The judges are appropriately wary of digital evidence and give it the amount of credibility that the lawyers and witnesses can show that it deserves.

Expert Witnesses

All of the judges spoke about the importance of witness testimony, particularly that of experts whose job it is to educate and inform the Court. The Vermont judges, however, all spoke to issues related to how they weigh the testimony of the experts. All carefully examine the credentials of experts offering testimony, although the weight that the testimony is given usually comes down to the credibility of the witness rather than the documented expertise of the witness. One judge explained his process of dealing with experts, which is wholly consistent with the *Daubert* test and the rules of procedure guiding the vetting of expert witnesses:

> I look at the credentials to begin with. I look at the experience factor the individual has in the field. I look at how acquainted the witness is to the particular item under consideration; is this something he tested himself or is he reviewing somebody else's report of somebody who testified? If there are generally accepted principles of the science in the field, is he following them? I also would try to test his logical

> processes; is he proceeding on sound premises to reach his conclusions? How much is conjecture? So there's a fact finding. Just because he's an expert doesn't mean he's any more credible than anybody else simply because he's an expert. Now, as a practical matter, he very well may be because of those other things that I talked about. (P4)

As this judge suggests, expertise does not automatically equate to credibility. The judges assert that they think that expert witnesses are, in general, truthful and certainly believe to what they are testifying. The issue for judges is whether they think that the testimony makes any sense and is logical. As another judge noted:

> Usually the weight, as opposed to the credibility, of what they have to say tends to stand up or fall of its own inherent logic and consistency, so that sometimes you'll have an expert well-credentialed and as sincere as can be, it's easiest for me just to say that I assume that you believe that what you're telling me is true. But sometimes the proposition just strikes me as so preposterous that it's not a matter of credibility but a matter of weight; I just don't accord it any weight. (P1)

The credibility factor is significant because, according to the judges interviewed, decisions are often based not upon technical knowledge but on awareness of people. This is particularly true when judges hear contradictory testimony from two witnesses. One judge shared:

> There's a lot that goes into my role here that isn't necessarily dependent on a real technical understanding. You know, if someone like you [the researcher] came in and gave me gobblygook about how you checked all of these Internet protocols and duh, duh, duh . . . and you said, 'It was [authentic],' I'd probably say, 'Okay, fine!" I

> don't know what you're talking about, but it sounds credible; you know what you're doing. I mean, it's like anything where you get into a very technical area and it turns out as a determination of, you know, is this expert credible? And if you're there and another computer expert is saying you're full of it, she's checked it, and, in fact, you're totally wrong, that comes down to who do I believe? And which one's story makes more sense? And does their logic follow through? And maybe that's the naiveté of feeling that I can sort out these two stories and figure out what the real answer is. (P3)

Another judge stated:

> We're very mundane, unlike what you see on *Law & Order*, it's a rather mundane world we're in. You know, 90% of the stuff we do is fact finding and of the fact finding, better than 50% is 'who do you believe?' And that's decided on criteria totally unrelated to the scientific method. (P4)

Indeed, credibility can develop over time as a witness testifies before a judge multiple times. This is an event that can commonly occur in a small venue, such as Vermont, or in a specialized field with few local experts. One judge told this story to make this point:

> You develop a rapport with experts, especially when they come in a lot. You know, [name deleted] for years was the breathalyzer expert—the machine I dealt with the most—and after a while, you clearly understood that this was an honest person and dedicated to his profession, and he was a true scientist, and he would not pull punches. He'd tell you the straight info and you could rely on it and often times the information was, 'I don't know,' which made you feel comfortable. (P4)

Third-Party Experts

Court rules allow judges to arrange for their own expert (known as a friend of the court), although they have to advise the parties to the trial that they are doing so (ABA, 2007). All of the judges spoke about this possibility, although none has ever sought use of such an expert related to digital evidence. Instead, they rely on what the two parties and their witnesses tell them, which sometimes becomes, in the words of one judge, a "battle of the experts" (P5).

Several of the judges went on to discuss the cost of hiring a third-party expert as a factor in their decision not to employ them. They all suggested that they might consider hiring their own expert if both parties agreed and paid the expert's fee. Experts might have their role in major cases, although that need has to be balanced against the cost burden on the parties. As one Vermont judge stated:

> You really need a very, very high-priced case to make it feel that that's not an undue burden to impose on people; you know, if we had a $20 million fight over something, maybe. But we don't have that many in Vermont that are huge cases like that. (P3)

Even so, two of the judges specifically called into question the value of such experts. In the words of one, "Why are three experts going to be any better than two? I mean, yes, they don't have an axe to grind because they're not hired by one side or the other, but that doesn't necessarily mean they're right, either" (P3). Another stated:

> If the parties agreed and paid for it, times being what they are, that would be essential. But, sure, I can imagine that both of the parties decide to agree on an independent expert and have that person be the court's expert. There's a whole debate about whether a court's expert is truly an independent expert. They all come with, it is

> argued, biases, prejudices, histories that tend to lead them into one camp or another, to the extent that there are camps. (P7)

The loss of credibility of an expert witness is, in fact, one of the reasons that might compel a judge to hire a third-party expert. If both experts lose their credibility in the eyes of the judge, he then has nowhere to turn. One judge described the situation in which:

> The credibility of the experts that the two parties bring in initially is somehow so damaged in the testimony that they give, in the judge's eyes, that the Court feels it's necessary to hire an independent [expert]. I can imagine that that would happen, particularly in the kind of case where you might find experts who are overstating their qualifications to a tremendous degree and whose testimony about that blows up in their face under cross examination, and now the judge can't trust what they're saying. Or there's some piece of evidence that's critical to what the expert is testifying about that is offered by the party [and] it's shown by the opposing party that the evidence itself has been fabricated. So now the credibility of the expert on whether he or she has accurately done their analysis is fundamentally flawed. (P2)

Knowledge Compared to Other Judges

Although none of the judges interviewed specifically spoke to the issue of his own knowledge of issues related to ICT and digital evidence compared to judges in other parts of the country, the general theme of the comments echoed those of the written survey respondents. In particular, many of the comments implied that the judges felt that their counterparts in larger population centers and/or serving on higher courts in the judicial

hierarchy either knew more about digital evidence or, at least, had more training and educational resources available.

The Vermont judges, for example, all stated that they had received no training nor attended any seminars in any aspect of computer forensics or digital evidence, partially due to the state's size, budget, and types of cases. As one Vermont trial judge observed:

> That's rural Vermont, with not a lot of money, not a lot of expertise. We're not all that sophisticated up here, at least in my experience. Now the feds may be different because they do have a higher tech courtroom, they've got more money. (P4)

One of his fellow judges similarly observed:

> I'm sure there are places like New York City where the general level of understanding is quite different from here because they probably do get these things much more. I mean, any time you have more money and bigger cases, there tends to be people who track down all of those little things more. (P3)

The dichotomy was also noted in the comments of the Massachusetts judges. The lower trial court judge believed that the higher trial court had more training opportunities than he had due to budgets and types of cases:

> I am not aware of any courses in my [less than five] years on the bench for judges on this issue. Now, you see it a lot more in Superior Court on the more serious felony cases. The thing is, in District Court, there's limited resources by the parties. They don't often go this far in these types of cases where they'll actually hire a forensics expert. It can be done. Budgets as they are right now in the state of Massachusetts means that most prosecutors won't hire a forensics expert in a District Court case. If it was a homicide in Superior Court, it would be a very different thing. (P5)

As if to reinforce the theme of an education and training disparity, both higher trial court Massachusetts judges cited the availability of training about digital forensics. One judge said that he has taken "a seminar concerning admissibility of digital evidence, authenticity of digital evidence, and the discovery of digital evidence in a criminal context using the various Federal statutes and, now, state statutes, as well" (P6). The other judge continued this thought by noting that the Superior Court "has an educational conference twice a year and we've [addressed digital evidence] within the last couple of years" (P7).

E-Discovery

All of the judges interviewed handle both criminal and civil cases, yet e-discovery was a major topic of discussion by only the two higher court Massachusetts judges. These judges provided insights about e-discovery, suggesting that this is a growing area in the law and one that judges, in general, need to learn more about. These themes are consistent with those of the written survey respondents.

Due to the relative newness of this area of the law, one judge suggested that this is a subject for which he might consider hiring a third-party expert as a friend of the court. He further said that this is already a topic of discussion within the ranks of judges:

> We've had a lot of discussions amongst judges about electronic discovery. A case in point. I work for the Acme Widget Co. I say I was discriminated against. My lawyer then says, 'Give me all the e-mails or texts regarding XYZ for the last seven years.' And then the Acme Widget Co. lawyer says, 'We'll do that, but it's going to cost us a bazillion dollars and take us seven years. We can't possibly do this; it's completely onerous.' As a judge, that's a difficult call to make and you really have to say to the

> parties, 'How much will it really cost?' I mean, you have to drill down and sometimes outside expertise might be valuable in that sense. (P6)

The primary issue of e-discovery is the quantity of information that might be available and the question of the potential financial burden in obtaining this information. These are issues that are not yet well understood by the judiciary. As one judge noted:

> I think the whole electronic-discovery boom is something that we judges [don't totally understand]. And the amount of information there to be discovered is almost infinite; it depends upon how much money the lawyers, the clients want to spend, how far back they want to go. So, we judges are making an analysis of what's there, trying to understand what's there, how much is there, what period does it cover, what subjects does it cover, what persons does it cover, how do you identify those portions on each score that might have relevant information to the case? The goal is to prevent discovery from becoming the tail that wags the dog and to control discovery, to identify up front, under principles known at proportionality—what makes sense in the context of this case, what's at stake, the amount of money, and so forth—for all aspects of discovery, including electronic discovery. So anything that gives me a better understanding of what electronic discovery is, what ESI—Electronically-Stored Information—is, and what metadata is and, to some degree, what that allows people who get it to figure out. But anything that would give me a better understanding of what I'm dealing with when I'm making decisions about what's in, what's not is helpful. (P7)

This same judge also said that the only judicial training he had received related to digital evidence was in the area of e-discovery.

Although only two of the judges addressed a large number of their comments to the subject of e-discovery, most of the judges made at least a passing reference to e-discovery in civil cases. None of the judges, however, made reference to any of the seminal rules of procedure, practical frameworks, or cases that provide the guidance for e-discovery in the courts. Nevertheless, all understood that there are many issues related to the cost of e-discovery and the possible financial burden that such discovery can create. One of the guiding cases is *Zubulake v. UBS Warburg* (2003, 2004), which provides for a multifactor test about the extent to which e-discovery should be pursued in cases, including the total cost of production, compared to the amount in controversy; the total cost of production, compared to the resources available to each party; the relative ability of each party to control costs and their incentive to do so; and the importance of the issues at stake in the litigation.

The judges in their statements implicitly or explicitly described all of the factors above about e-discovery. The rules themselves have elements of common sense to them, and it is this common sense that judges apply to evidence of all kinds, given their earlier statements.

In the absence of training in e-discovery, one of the judges offered the following advice about how judges can obtain needed information from attorneys, even at the risk of showing their lack of knowledge:

> Rely on the lawyers. These questions are going to come up before judges because one party wants something that the other party doesn't want to give, generally. If the information you're getting in the briefs on this motion isn't sufficient for your understanding, ask the attorneys; tell them what your questions are and ask them to

> submit further briefs that answer those questions. That's going to be a very direct way to pinpoint the things you don't understand. And, as a judge, I don't generally like to show my ignorance but I think that this is still a developing field so that it's okay to not know what metadata is, for example, or to be big enough to say, 'I know something about it but I don't know everything about it' . . . you know, that kind of thing, take advantage . . . the lawyers are trying to educate us. (P7)

It is telling that this judge openly states that requests for additional information might show a deficit in his knowledge. As the results of the written survey also showed, this statement directly suggests that at least some judges are willing to show some lack of knowledge, contradicting suggestions to the contrary in the literature (Mack & Anleu, 2008).

Judges' Use of Technology

All of the judges interviewed are active users of the Internet and ICT, and their usage parallels that of other similarly educated members of the public. As noted earlier, judges as a whole are not any more or less technologically astute than others in society. In the words of one judge, "I guess that there's a certain basic understanding that I have, a very basic understanding that I think the general public, at this point, has now that we're 15 or 20 years into the whole Internet explosion" (P5). Additionally, like the population as a whole, the amount and type of their usage varies. All of the judges cited use of computers and networks to access the Web to look at news, travel, entertainment, and other sites; perform legal research; use personal and professional e-mail; and employ their court system's intranet or other internal network.

Other activities were equally commonplace. Three of the interviewees stated that they used the Internet for online shopping, while two mentioned that they did not. Two noted that they did online banking, while three specifically stated that they did not. Five indicated that they accessed daily news online.

Each of the judges specifically volunteered that they did not personally engage in Facebook or other social networking sites, blogs, or Twitter. As one judge stated, their general use of the Internet is "very pedestrian" (P1).

The ages of the judges interviewed was purposely not collected for this phase of the study. Nevertheless, it is the impression of the researcher that, at least within this group, age is not a factor in the use of and comfort with the technology. Indeed, two of the younger judges indicated comfort with technology but limited time to use the Internet for personal use due to having young children, a growing family, and other demands on their time. Another said that he had his "brother set up wireless in my house because I'm far too intimidated to try to do that myself even though it wasn't really that hard. I have your average layperson's experience, really" (P3).

The two oldest judges represent the extremes of ICT awareness and use. One commented that older judges are, in fact, less aware of and interested in technology, stating:

> My experience with the cohort I worked with on the bench, which was a cohort that came on [in the 1980s], had little understanding of the computer world and less desire; still locked into books and paper and hard copy. So, there wasn't a respect for digital information. (P4)

Conversely, the other was one of the most ICT aware because he has been using computers for professional purposes since the 1970s, using early systems to scan decisions into searchable databases, and into the 1990s, with the development of judicial system intranets and the Internet. He viewed his own use as common, noting:

> I've used searchable legal databases for 25 years, 30 years, more. And then, not so much for professional purposes but for things you've become interested in, to find things on the Internet; music, restaurants, I mean whatever, just that sort of general thing. I've used that as most people do, for decades as well. (P7)

All of the judges cited use of the Internet for legal research and the trust that they placed in these systems. Most of the judges cited Westlaw® as their primary source of legal case citations, briefs, concordances, and other information. None of the judges, however, expressed any doubt as to the correctness of that information. This was in stark contrast to the judges' stated concerns about the veracity and integrity of other Web sites and digital evidence, in general, as mentioned in earlier sections.

Although there has been some suggestion in the literature that individuals with less technical knowledge are more impressed by the technology (Van Buskirk & Liu, 2006), the survey data appeared to call that supposition into question. Two of the interviewees indicated that a lack of technical sophistication actually adds doubt and suspicion in the minds of judges, as summed up by one who stated, "I'm quite primitive when it comes to these things. What I am, probably, on the other hand, because I'm primitive, I'm probably suspicious because it does seem to be so easily altered" (P1).

What Judges Want to Know

All of the judges who were interviewed acknowledged that training and education related to digital evidence is currently lacking and is a subject area for which they and their peers could benefit from more knowledge. The insights from the judges fell into three general subject areas that were split by the judges' current roles.

The two appellate judges spoke about the need to "elevate the consciousness of judges" (P2) with respect to issues surrounding digital evidence. Their primary concerns are related to the legal issues of admitting digital evidence into trial rather than to judging the reliability or veracity of the evidence. As one judge stated, questions about digital evidence "usually come up over warrant issues, probable cause, was there a sufficient basis to get in there; it doesn't have to do with the quality of the evidence itself" (P1).

Since these procedural questions are common to the ones brought before appellate judges, it is not surprising that this would be the focus of their comments. Their statements suggest that trial judges need to be better versed in the high-level concepts of digital evidence to better apply the existing laws and guidelines as well as to apply what other courts are doing. As the other appellate judge stated:

> We need judges who understand these concepts well and not just flying by the seat of their pants. These are complicated questions, and I think background information is probably extremely important with the more highly technical a subject is, the more important that background information is. We need judges who understand the language, aren't learning it as they go, come into court to sit on a case where these are tough issues that the parties are talking about, and they can intelligently apply the law to those facts. I think it's very important. (P2)

The two Vermont trial judges and the Massachusetts lower court judge made comments that were consistent with the appellate justices' comments but were more specific. This seems consistent with the trial judges' role in making the initial decisions of signing search warrants and other court orders related to digital evidence and ultimately deciding on the admissibility of that evidence at trial. All three of these judges stated or suggested three things. First, they believe that they have the same basic understanding of ICT as does the general layperson who uses these technologies. Second, they do not know what they do not know. Third, they expect to see a growth in the introduction of digital evidence in trials.

They also concluded, during the interviews, that the factors above give some urgency to additional training in this subject matter because they recognize that their knowledge is imperfect and has gaps. Their concerns were less focused on strict admissibility issues, per se, but more on the relevance, authenticity, and reliability of the evidence that is sought during an investigation or offered at trial.

One judge spoke of needing to know more about the capabilities of digital devices to make better decisions about granting court orders. He said, as an example:

> I did not know that you could determine from a cell phone where somebody was when they made a call, which clearly has application when you're talking about alibi defenses, when you're talking about people present in one spot or another. It never dawned on me that there's a GPS involved in those things. So, the capabilities of digital is a mystery. (P4)

The other judges cited similar questions related to e-mail messages, text messages, documents printed from the Internet, and other forms of digital evidence. All three

recognized that there is a limit to their understanding. To that end, all stated that they need a high-level knowledge of the process of computer forensics and the procedures by which digital evidence is acquired. Their comments suggested a need for understanding such basic issues as "How does a hard drive work? How do you get that stuff off? And how do you know what you're getting off is what it says it is?" (P4).

The judges' comments also showed that they are aware of the limits of what digital evidence can prove. One judge, for example, clearly stated the difference between showing what a device did as opposed to showing what a person did, when he stated, referring to a cell phone text message, "There's always issues of authentication. How do we know [who sent a text message]? It's not a voice on the phone, where you can identify someone's voice; how do you know this person sent it?" (P5).

These three judges were also clear that their peers, in general, want to know more and recognize the changing legal landscape as it relates to digital evidence. As one stated:

> We certainly have a desire . . .When you get into forensic issues, I think the situation is so fluid that we should be kept aware of developments with the understanding that there're going to be more developments and that things are not engraved in stone and probably never will be. (P4)

Finally, the two higher court judges in Massachusetts, the only ones who spoke at length about e-discovery, listed related topics such as electronically stored information (ESI) and metadata as the primary subject area in which judges need additional training and education. Both cited the growth in e-discovery issues at trial and how the sheer volume of information is affecting trial outcomes. As one of the judges observed:

> It seems to me that the ESI phenomenon is really pushing the limits of the old Rules for Civil Procedure, the way discovery rules work, and really presses hard on issues of relevance and relevance versus burden. I mean, the whole discovery [process] is too burdensome; it's too expensive. When it was paper documents, well that really ramps up with electronic discovery, which is so labor intensive. It takes experts to do it; you can't just send legions of people who can read into the warehouse, you need to have expertise. But by the same token, it's that much more accessible than a warehouse ever was but you've got to have the people who know how to do that, so I think that any program or education that helps judges recognize those issues and can come up with strategies for making the wise, the right, fair decision on the basis of real understanding to identify that which is worth pursuing and that which is not worth pursuing and identifying those factors that you take into account in deciding what's worth and what's not worth pursuing. That I think would be very helpful. (P7)

Their focus on an advanced topic suggests that they believe that they and their peers are already comfortable with the more basic issues brought up by the other judges.

All seven of the judges are aware that they need additional general ICT training. Part of that training can come from their own activities; the judges all commented that it is important that they use at least the basic ICTs, such as e-mail, the Web, and other Internet services. This is consistent with the judges' noting that they have similar knowledge as the lay user, but, in fact, mere usage of ICTs does not necessarily equate to understanding how those technologies work (Del Bosque & Chapman, 2008).

Summary of Interview Findings

The sections present the themes that emerged from the interviews with judges. These themes delved deeper into those introduced by the written surveys and added some insights to those suggested in the literature, the researcher's advisory board, and the surveys themselves. In summary, the findings from the interviews demonstrated that:

- Judges leave the arguments about the merits or weaknesses of digital evidence to attorneys and expert witnesses rather than relying upon their own knowledge; in fact, they are barred from relying solely on their own knowledge.
- Authentication of digital evidence is basically the same, albeit more complex, as authenticating other types of evidence; specifically, the evidence needs to be shown to be real, correct, and accurate. Thus, new rules are not needed for digital evidence, although the current rules do need to be modified to recognize the capabilities and limitations of digital evidence.
- Digital evidence is likely to be admitted if the other party raises no challenge to it. If the judge has personal knowledge that suggests that a challenge could be raised, he or she is unlikely, in most cases, to raise the issue unless the lapse is egregious.
- Challenges to digital evidence are more common than the literature suggests, although the challenges are usually based on the grounds of procedure or credibility. Consistent with the literature, challenges are rarely based on reliability or authenticity (i.e., *Daubert*) grounds.
- The digital evidence that most judges see is primarily related to communications, Web-based documents, or e-discovery. Forensic remnants such as deleted files,

Internet cache and history files, and system files do not appear to be commonly seen by judges or associated with digital evidence by judges.

- Judges are very aware that e-mails and Web pages can be altered. They are, in general, wary of technical evidence rather than overly impressed by it, contrary to suggestions in some of the literature.
- Judges, in general, do not have any more or less technical knowledge about the operation of e-mail, the Internet, and the Web than do other members of the Internet user population.
- The judges observed that attorneys freely accept information from the Internet and/or often do not know when they should object to digital evidence. Several surveys of lawyers cited earlier in this report show that lawyers, in general, believe the same about judges.
- Appellate judges review evidence only if there is a specific procedural or constitutional challenge to it. Even then, they make a judgment about the trial court's action based only upon whether the trial judge acted properly within the law rather than whether they agree with the trial judge's decision.
- Judges' *a priori* knowledge affects their decisions, but they are required, to the extent possible, to limit their decisions to the information provided by the attorneys and witnesses. They are barred from doing independent, case-specific research on their own.
- Expert testimony is usually weighed by judges based upon human elements (e.g., the credibility of the individual and believability of the testimony) rather than on

technical elements. The expertise of the witness does not automatically make him or her credible or his or her testimony believable.

- None of the judges has used a friend-of-the-Court or third-party expert; most cited the expense and questioned the value of such a witness in most cases.
- The judges appear to believe that their peers in larger and/or higher courts have more information, knowledge, and access to training opportunities related to digital evidence than they do.
- e-discovery is growing in importance, and most judges are not aware of the issues related to it.
- The judges demonstrated a willingness to show areas where they had limited knowledge, contrary to some reports in the literature.
- The judges all use computers, networks, and the Internet for both professional and personal purposes; the applications and services that they use personally are similar to those of other users. Age does not appear to be an issue affecting the use of ICTs.
- Judges do not, in general, want or feel that they need detailed knowledge about ICTs and computer forensics tools. They would like a basic understanding of these subjects to remove the mystery of the technology and the process.

Summary

The mission of this study was to help judges to better prepare to carry out the crucial gatekeeper role as digital evidence becomes more pervasive in criminal and civil court proceedings. The study also demonstrated that grounded theory methodology has an

application in digital forensics research, establishing a trust relationship with the judicial community and building a foundation for future research.

The study showed that judges need and want more information about digital evidence but that they also understand that the rudimentary rules of evidence apply equally to digital and non-digital forensic evidence. Contrary to some reports in the literature, judges who are less technologically aware are more wary, rather than less, about accepting and trusting digital evidence. Having the mystery about the technology removed and making judges aware of the capabilities of digital devices are key to assisting judges in their jobs and preparing them for the continued growth in the introduction of this type of evidence at trial.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

This chapter provides the conclusion to the dissertation and is organized in four parts. The chapter begins with the overall conclusions of the study, followed by the implications of this study for the field of digital forensics. The next section contains recommendations for future research in this area and for training judges in digital evidence. The chapter concludes with a summary of the research project.

Conclusions

Several objectives were laid out for this study. First, the researcher wanted to provide foundational data from which to determine the factors influencing and informing judges in regard to digital evidence. Second, the researcher wanted to identify gaps between judges' knowledge of digital evidence and their requirements in terms of additional knowledge as well as provide a framework for a training curriculum to bridge the gap between the two. Third, the researcher wished to build a trust relationship with judges in anticipation of future research.

Creation of Foundational Data

The face-to-face interviews and written surveys provided significant insight into the respondents' views about the factors that help judges form opinions about digital and other types of forensic evidence. Most notably, while some judges recognize the complexity of digital evidence, they believe that it must meet the same admissibility

requirements as other types of evidence introduced at trial, albeit meeting those requirements in a different way. Digital evidence must meet the same standards of authenticity and reliability as any other type of evidence, although these standards are met in different ways than they are for traditional physical evidence. Many judges believe, therefore, that they do not need specific expertise in all aspects of digital evidence, as it is the role of the contesting parties to introduce, challenge, and validate evidence offered to the court. The role of the attorneys and expert witnesses is to explain the evidence and educate the fact-finder(s); the judge needs to ensure fairness in the proceedings and balance the probative value against the prejudicial nature of any such evidence.

Judges do not need to become experts in computer forensics and ICTs but do need enough general knowledge so that they understand the subtleties and nuances when digital evidence is presented to them by lawyers and experts. Nevertheless, digital evidence is based upon science and engineering that has a fundamental difference from the other forensic sciences in that it is the only one for which the general population of judges and jurors are users of the science. Most people in the U.S. do not have daily exposure to chemistry, biology, physics, medicine, or the other sciences that underlie traditional forensics, but the vast majority of the population makes daily use of the Internet, computers, mobile telephones, e-mail, Google, and the other services that are the basis of digital evidence. That exposure forms the basis of a person's understanding, and that understanding, based on experience rather than education or research, is often incomplete or imperfect.

Judges, on the whole, recognize that they do need to understand the basic foundations and sources of digital evidence as well as the procedures and processes by which digital evidence is acquired, examined, and analyzed. Although the judges report that it is, indeed, not their job to be experts in information technology and the computer forensics process, they generally do want to know more so that they better understand what the attorneys and expert witnesses are telling them.

The data that came out of this study provide insights by which to better understand the type of training and education that judges could use related to ICTs and digital evidence. The research showed that judges need multiple levels in their knowledge base, which results in the tiered approach to training and education described later in this chapter. Judges, as a whole, tend to be logical thinkers and, therefore, need training that provides them with specific factual knowledge that they can then synthesize with their knowledge of the law and judicial process to make informed decisions.

The Role of Training

The discussion above has shown that judges do not evaluate evidence on their own but rely on the testimony of the lawyers and expert witnesses. Knowledge of the computer forensics process would aid judges in interpreting, understanding, and evaluating the arguments, as demonstrated by the following hypothetical example (although based on occurrences commonly observed in the researcher's practice of computer forensics).

Suppose a police officer has probable cause to believe that an individual has a warehouse containing stolen SCUBA equipment. Upon execution of a search warrant for the premises, computers and video cameras are among the items seized. The subsequent search warrant for the computer directs the computer forensics examiner to search for

images related to SCUBA equipment, such as masks, tanks, and wet suits. During the analysis, the examiner finds an image that appears to be of child sexual abuse. The examiner stops the analysis and advises the police officer of these new findings; the officer, in turn, obtains a new search warrant to include evidence related to the newly discovered crime. The examination and analysis continues, where it is discovered that the video equipment was used both to film the warehouse and to produce images and videos of child sexual exploitation.

At the later suppression hearing, the suspect's attorney petitions the Court to throw out the images of child sexual abuse because the examiner was originally directed to search only for images related to SCUBA equipment and nothing more. The discovery of images related to another crime, according to the defense, was found because the examiner was looking in places of the computer for which no search was authorized. The prosecutor's argument is that what the examiner saw was, from a legal perspective, in plain view and, therefore, admissible.

A judge who has seen how computer forensics tools work would have firsthand knowledge about whether the tools can or cannot limit the scope of what they display for the examiner. Knowing how the computer forensics tools and processes work is essential for the judge in making a determination about the merits of the arguments and appropriately applying the law.

Losavio, Adams, and Rogers (2006), Losavio, Wilson, and Elmaghraby (2006), Van Buskirk and Liu (2006), and others have suggested that courts should consider specialist judges to deal with digital evidence. Comments by the judges in this study would suggest that no such specialist judge is necessary. First, digital evidence is so widespread (and

inclusion at trial is expected to grow) that all judges need to have at least a basic understanding of it. Second, judges do not necessarily need to be experts in digital evidence to follow the arguments of the attorneys and expert witnesses, and it is on them that judges must rely when weighing evidence. Finally, while specialist judges are currently employed to handle certain types of cases (e.g., complex business litigation), it is less clear that specialist judges are needed to handle certain types of evidence.

Building the Trust Relationship

The final objective of this research study was to build a trust relationship with the judicial community, both in how the study would be conducted and in how the results would be interpreted and reported. As stated earlier in this report, the ABA/JD and NJC were initially hesitant to have a non-member of their organization conduct this research due to fears that the researcher might make the judges look ill-informed or show them in a bad light. Although the organizations eventually agreed to allow the researcher access to their membership, it is likely that these same concerns played at least a small part in the low participation rate in the written survey.

The researcher believes that this report is written in a manner consistent with a fair representation of what the respondents said and a non-pejorative report of the results. The researcher has attempted to portray the respondents honestly, as thoughtful, concerned professionals, and hopes that such treatment helps this and other researchers work with the judicial community for further explorations.

Implications

This study is the first in the U.S. to directly examine the attitude and knowledge of judges with respect to evidence derived from the computer forensics process. As such, it has significance for the field of digital forensics; it opens up a new avenue of research and adds to the dialogue between the community of judges and digital forensics practitioners. Indeed, similar studies have been performed on the attitude and knowledge of attorneys and digital evidence, and such studies added to the research base for that level of the judicial system. Bringing civil and criminal computer forensics practitioners, lawyers, and judges into a conversation using the same terms and concepts is expected to bring a higher degree of understanding all around and improve the practice of all of the parties.

This study is the second time that grounded theory has been employed in research in digital forensics. The first study (Carlton, 2006) focused on computer forensics examiners while this one focused on judges. Both studies generated new information for the computer forensics knowledge base as foundations for future research. In addition to generating new data, then, this study has again shown that grounded theory is relevant to this field of study.

Although the number of respondents to the survey and face-to-face interviews was small, their insights provided new information. Input from the survey respondents, interviewees, and advisory board members provided sufficient triangulation, or validation, of the findings to suggest that the themes indentified by the researcher provide a good starting point for the next round of research.

One significant insight gained by the researcher is that the role of judges must be well understood by researchers in this field. The researcher observed that many papers cited in this report seem to misunderstand the role of the judge, implying that judges make decisions about evidence in a vacuum, based upon their own knowledge and research. These same papers seem to downplay the boundaries and guidelines that judges must follow as well as the role that attorneys and expert witnesses play.

This study also shows the importance of working closely with judicial organizations at the state and national levels. Although initially reticent to allow the researcher access to their membership, both the ABA/JD and NJC were interested in the research topic and felt that the results of the study would be beneficial to both the field of computer forensics and their members. Indeed, the reticence was only about the potential feelings of the members regarding an individual conducting the research over which the organizations had no control; the leadership of the organizations expressed an interest from the very first discussions with the researcher about the subject and saw value in the outcome. (To offer one example, the researcher was invited to address the Vermont Judicial College about digital forensics topics in June 2010 as a direct result of the interviews with Vermont judges earlier in the year.)

The primary limitation of this study was balancing the conflicting goals of the IRB requirements and the grounded theory process (Charmaz, 2006). Grounded theory thrives when the researcher can adapt the interview process to tailor questions to individuals and to follow up answers with additional questions. The IRB process, however, requires that the interview questions be proscribed, thus limiting the discussion and ability to follow up on emerging themes, as demanded by grounded theory.

Employing grounded theory-style interviews can still be used to learn more about this topic, of course, but might well be more fruitful with fewer restrictions on the interview questions, thus allowing them to take their natural course. For that reason, while the researcher is confident in the validity of the themes described here, he also recognizes that the full power of grounded theory may not have been realized.

A second limitation of this study was time restrictions. The leadership of the ABA/JD and NJC, as well as the advisory board, advised the researcher to limit the amount of time that judges would have to spend on the written surveys. The original study design called for no more than three rounds of written contact with any participant (Carlton, 2006). The updated design followed up the surveys with face-to-face interviews, which themselves were limited to a single meeting of no more than an hour. Future studies might benefit from a series of interviews to better develop the themes that emerge from the data and to explore the subject more broadly.

A final limitation of this study was due to the relatively small number of survey respondents and interview subjects. The number of participants makes the reported themes appropriate for this early study but makes it impossible to make statistically valid generalizations about the population of judges.

Recommendations

Two types of recommendations are presented. The first type concerns questions for further research when addressing the audience of judges. The second type concerns judicial training and education related to digital forensics.

Research Recommendations

Grounded theory methodology continues to have a place in research related to judges and digital forensics, as there is still significant foundational data to be gathered. The experience of the researcher suggests that face-to-face interviews will be the most productive in terms of both gathering raw data and demonstrating the value of the research data to the participant pool. In the long term, given a track record of data that have value to the population of judges, written surveys might be used to gather more data from a larger number of respondents. In any case, it is important that the research have the support of a state, regional, or national judicial organization to continue to build the trust relationship between the judges and digital forensics research community.

The findings reported in the previous chapter suggest a large number of questions and follow-up themes to explore. There are a number of additional questions, however, that do not readily appear from those findings. Among these questions that might warrant future investigation are:

Why was the response rate to the written surveys so low? Several authors have suggested that judges would be a difficult population to survey; but, even so, the response to the written surveys was somewhat lower than expected by the researcher, the leadership of the ABA/JD and NJC, and the advisory board. Knowing why the rate was so low might itself provide valuable insight to future researchers. This is a particularly relevant question given the generosity of time that so many judges spent with the researcher in the design, preparation, and execution of this research. Indeed, future research may well garner a larger response rate if performed under the auspices of one (or several) of these judicial organizations rather than conducted by an outside researcher.

Is there a significant difference between the views of federal and state judges? By coincidence, all respondents to the initial written survey were municipal or state judges; no federal judges responded to the survey, although federal judges are members of both the ABA/JD and NJC. By design, all face-to-face interviews were with local or state judges, primarily to remain consistent with the written surveys. Federal judges, of course, are in a different system entirely, with their own training, education, laws, and procedures. One might suppose that a federal judge in California or Arizona might have similar responses to questions as would a federal judge in Massachusetts or Vermont, although conflicting decisions by judges in different federal appellate court circuits show that this is not the case at all. Focusing research on the federal level might produce a new set of results and offer insights about differences in rulings across the country.

Is there a significant difference between the views of elected and appointed judges? The legal background of elected and appointed judges can be very different in terms of training, education, experience, and background. Becoming a judge is a result of a political system, either by public election or by appointment, although the judicial branch is supposed to act independent of political and public pressure. It is unknown what, if any, differences exist among those who advance to the bench by these different pathways and how this affects decisions.

What is the impact of CSI Effect? Many professionals in the field, as well as the judges that were interviewed, allude to the CSI Effect. The common thinking suggests that television shows, both fictional and reality-based, and movies have made the secrets of crime scene analysis and examination, including computer and mobile phone forensics, so well known to the public that judges, lawyers, and juries have an

expectation of the types of evidence that they should see at trial. Indeed, having informed parties at trial is generally viewed as a good thing, but, given the way that television and movies portray the science, the expectations are often unreasonable in terms of the speed with which an examination can occur, the accuracy of the results, and the volume of probative information that will be found. In truth, though, the question still remains: If there is a real CSI Effect, what is its impact at trial?

The questions and recommendations above are only a start. The findings of this research are a first attempt to generate theory about this subject matter. Only further research can strengthen these ideas. As Glaser and Strauss (1967) stated, "Evidence and testing never destroy a theory (of any generality), they only modify it. A theory's only replacement is a better theory" (p. 28).

Educational Plan

The third phase of the study is to propose an outline for judicial education and training related to digital evidence. The ideas below are derived from the findings of the surveys and interviews reported above.

The overriding educational theme that came out of this research is to remove the mystery about digital evidence. As suggested earlier, a unique characteristic of evidence that derives from digital sources versus traditional physical evidence is that judges typically own digital devices (e.g., computers, mobile phones) and employ digital services (e.g., e-mail, the Web), whereas the majority of judges are not science hobbyists. The use of ICTs, however, does not necessarily yield detailed knowledge or expertise in those technologies.

In his book *Profiles of the Future*, Arthur C. Clarke stated, "Any sufficiently advanced technology is indistinguishable from magic" (as cited by Moncur, 2007, para. 1). This observation remains true a half-century later. While lawyers educate judges, it is the judges' knowledge that drives how they determine who is more credible and which arguments seem most logical and convincing. As it relates to digital evidence, how much information is necessary so that judges are appropriately informed but not biased?

Training and education in this subject matter should be based upon the foundations of adult learning that involve active, problem-based learning. To build the foundation of knowledge, the basic pedagogy should follow social constructivism. Piaget, who theorized that cognitive structures are the building blocks of learning, first advanced constructivism. Dewey and Vygotsky extended Piaget's theory by observing that learning is a social, rather than solitary, activity. Constructivism suggests that students create new knowledge based upon what they already know; students' mental organization skills need to be honed so that they learn new cognitive structures and how to build the linkages between them. Social constructivism suggests that this learning best happens in groups (Phillips & Soltis, 2004).

Problem-based learning further suggests that learning should be contextualized into problems and projects that are familiar to the student. Real, relevant, and tangible problems generally motivate learners more than do contrived, theoretical scenarios. Problem-based learning is well suited to constructivism because learners apply what they know to fully define the problem and find one of what may be many solutions to a stated problem (Duch, Groh, & Allen, 2001).

The primary focus of judicial education and training about digital forensic evidence should focus on ICTs and the computer forensics process. It is imperative in this context that judges understand the process by which computer forensics practitioners examine and analyze information from digital sources, in both the criminal and civil realm. In this way, they can get a better sense of how to weigh the evidence and testimony surrounding this type of evidence. It will also make judges better consumers of ICT products and services, as well as lead to better understanding and the ability to make more informed decisions about the credibility of witnesses, experts, and offered evidence.

Legal questions should be peripherally addressed but do not have to be the main focus of such technical education. While the technology and processes have some universal consistency, the applicable laws related to specific instances will vary by jurisdiction and may be better left to specialized training that addresses decisional law, emerging legal issues, and future trends.

A tiered approach to such training and education is also recommended. A tiered approach can implement constructivism by providing a structure by which judges can build the cognitive structures necessary to learn what they need to know about digital evidence. Problem-based learning can be implemented by employing sample case scenarios that introduce digital evidence in the same way in which it would be seen in real cases.

One possible tiered approach and sample topics are provided below as a basis from which to construct a training framework. This framework is meant to be a broad set of guidelines that can be modified for specific judicial communities, rather than a specific course syllabus, to familiarize judges with appropriate terms and concepts rather than to

bring them to a level of expertise. Indeed, the intention is that judges are sufficiently informed so that they better understand the arguments of the lawyers, testimony of expert witnesses, and emerging decisional law.

1. *Basics of ICT*

- Computers
- Hard drives
- Mobile devices
    - Information that can be found on mobile phones, music players, and others
    - The value of GPS information and call detail records
- Networks
    - Home networks versus business networks
    - The role of the router
    - Wireless networks
- The Internet
    - The structure of the Internet
    - Internet communication protocols: The Transmission Control Protocol/Internet Protocol (TCP/IP) Suite
    - ISPs
    - Obtaining information about Internet hosts and users
- E-mail
    - How e-mail travels through the Internet
    - The value of e-mail headers

- The World Wide Web
    - What is a Web page?
    - How browsers access Web pages
- Social networks
    - Facebook, MySpace, LinkedIn, and others
    - Privacy issues
- Other services and applications
    - Voice/video over the Internet (e.g., Skype)
    - Peer-to-peer networks
    - Instant messaging
    - Chat rooms

2. *The computer forensics process*

- The process of identification, preservation, acquisition, examination, analysis, and reporting of digital evidence
- Location of probative information on a computer
    - Internet history and cache
    - System files
    - Log files
    - Application files
    - Unallocated space and slack space
    - RAM and volatile data
- Location of probative digital information in a residence or business
    - Network router

    - Cable television box
    - Digital photocopier/scanner
    - Digital camera
    - Telephone (e.g., caller ID, answering machine)
    - CDs, DVDs
- Acquisition and analysis of a running system

3. *Digital forensics examination and analysis tools and methods*
    - Why computer forensics exams take so long
    - Distinguishing between television/movie and real-world capabilities
    - Imaging and the preservation of evidence
    - Different tools and what they show the examiner
        - E-mail
        - Internet history
        - Network information
        - Graphics
        - String searches
        - Registry
    - Mobile device forensics hardware and software
    - Data carving (recovering deleted files)
    - Metadata (system and application-specific data stored in a file)
        - Paper memos have only one copy but e-documents have multiple versions available
        - E-documents have metadata while paper memos do not

- Cryptography (secret writing) and the impact on digital forensics

4. *Decisional law related to sources of digital evidence*
    - Search-and-seizure laws and guidelines
    - Search incident to arrest
    - Searches of crime scenes
    - E-discovery
5. *E-discovery principles, concepts, and terms*
    - Volume of information
    - Cost of e-discovery
    - Sedona Principles
    - E-discovery software tools

The topics above should be accompanied by demonstrations and, where possible, hands-on activities and case studies related to real and hypothetical court cases. The list above is not meant to be a comprehensive set of topics but rather to sow the seeds of subjects that might be addressed and in an order that would allow judges to go from the basics to advanced topics, as appropriate.

Summary

Judges play a gatekeeper role in determining what evidence is allowed in their courtroom and which experts are allowed to testify. Due to the relative newness of the field of computer forensics, there have been few studies about the use of digital evidence in criminal and civil courts and no published studies about how judges perceive the

quality and usefulness of such evidence. Thus, this study focused on judges' awareness, knowledge, and perceptions of digital forensic evidence.

Judges are generally well versed in rules of evidence and procedure, all of which apply to digital evidence. Digital evidence, however, is different from more common forms of physical evidence in many ways, including its volatility, complexity, volume, and location. Although almost all judges in the U.S. use computers and the Internet, they are not, in general, any more knowledgeable about the underlying technologies of the hardware, software, and applications than is the population of users as a whole.

Ball (2008), Casey (2011), Kerr (2005a, 2005b), and others have observed that digital evidence is growing in both volume and importance in criminal and civil litigation. Judges must decide what evidence will be admitted in their courtroom and need to weigh the probative value against the prejudicial effect of any evidence that is offered (Cohen, 2008, 2010). These considerations apply to scientific and technical evidence as well as to other types of physical evidence such as crime scene photographs, shell casings, and blood splatter diagrams. To fairly and justly evaluate the merit of digital evidence, judges should have some understanding of the underlying technologies and applications from which digital evidence is derived, such as computers, the Internet, and e-mail. The literature is nearly silent on what judges know and how they perceive digital evidence because no studies focusing on judges have been conducted in the U.S. (Losavio, Adams, & Rogers, 2006; Rogers et al., 2007; Scarborough et al., 2009).

Due to a lack of data from which to form research questions, the author employed grounded theory for this study. Grounded theory is a qualitative research methodology that employs an inductive process whereby data are gathered to develop a substantive

theory, which stands in contrast to the deductive process whereby data are gathered to test a hypothesis (Charmaz, 2006; Dick, 2005; Pogson, Bott, Ramakrishnan, & Levy, 2002; Schram, 2006). Grounded theory is useful for early studies in a new discipline and enables an examination of how people respond to various phenomena. Grounded theory is well suited to examine the complex relationship between a person's actions (i.e., the response to a situation) and their contextual understanding of the meaning (i.e., the personal definition) of a situation (Brown et al., 2002; Glaser & Strauss, 1967).

Although initially designed for the social sciences, grounded theory has been applied for many years to studies related to information technologies (Charmaz, 2006; Sprauge, 2009). The interactions of judges with digital evidence have a social aspect, which makes a study of this relationship well suited to grounded theory (Brown et al., 2002).

Grounded theory research involves a number of steps leading from data collection to theory generation. Data collection is generally in the form of open-ended questions using questionnaires and/or face-to-face interviews. Analysis of the data, to detect emerging themes, may be done as data are collected. As themes emerge from the data, subsequent questionnaires and/or interviews are employed to cultivate additional information, better understand the detected themes, and validate earlier findings. It is essential to the grounded theory process that the researcher listens carefully to the study participants to follow where the data lead rather than attempt to use the data to support the researcher's own preconceptions (Charmaz, 2006; Glaser & Strauss, 1967).

This study gathered data from three primary sources. First, a questionnaire was distributed to the membership of the ABA/JD and NJC to gather initial data. Second, the results of the survey were validated in concert with input from an advisory board of

digital forensic practitioners and attorneys who work closely with digital evidence. Finally, more focused data were acquired using in-person interviews with a set of judges from Massachusetts and Vermont. The results included conclusions about judges' attitudes towards digital evidence and a proposed framework for education for judges in this subject matter.

The study found that, in general, judges recognize the importance of evidence that is derived from digital sources, although they are not necessarily aware of what all of those sources might be. Most of the evidence that is offered at trial, according to the judges, is e-mail, text messages, and Web pages, and these are generally offered in the form of a printed piece of paper.

Most judges expressed a need for additional training and education about digital evidence, citing a lack of availability of such training and often indicating a belief that judges at higher levels in the court hierarchy and/or in larger population centers have more access to training than they do. They believe that digital evidence, while different than other forms of evidence, needs to be authenticated, just like any type of evidence brought before the Court, and that it is the role of attorneys, not judges, to mount challenges to that evidence, as appropriate. Judges, in fact, rely on the attorneys and their expert witnesses to explain the nuances and meaning of digital evidence to the Court rather than relying on the inherent knowledge of the fact-finders. Some previous studies have suggested that attorneys do not believe that judges are as aware of digital evidence as attorneys are (Scarborough et al., 2009). The results of this study suggest that judges are concerned that lawyers do not always know enough about digital evidence to

effectively present it and/or properly challenge digital evidence offered by the opposing party.

Judges are, in general, appropriately wary of digital evidence, recognizing how potentially easy it is to manipulate or alter digital evidence. Some authors have suggested that non-technically aware judges are more likely to accept digital evidence than are their more technologically astute colleagues and are more likely to believe the implications of the digital evidence (Caloyannides, 2003; Van Buskirk & Liu, 2006). This study found the opposite, specifically that less technically aware judges were actually more wary of digital evidence than their more knowledgeable peers.

Judges at all levels of technical knowledge appear to recognize that they need additional training in computer and Internet technology as well as knowledge of the computer forensics process and digital evidence. The fundamental goal of such training is to remove the mystery surrounding digital forensic evidence so that judges can better understand the arguments presented by lawyers, testimony offered by technical witnesses, and basis of decisional law, thereby improving the entire judicial process.

Appendix A

Advisory Board Members

Abigail Abraham, J.D.

Ms. Abigail Abraham is a senior counsel for AOL Corp. She is a former Illinois State Police (ISP) trooper and started the ISP Computer Crime Unit. After graduation from law school, Ms. Abraham became a prosecutor for the Cook County State's Attorney's Office and then an Assistant Attorney General, responsible for prosecuting computer and high-technology crimes, and working on related legislation. Ms. Abraham wrote a chapter on evidentiary issues for *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes* (Marcella & Greenfield, 2002) and is a frequent speaker at industry conferences.

Christopher L. T. Brown

Mr. Christopher L. T. Brown is the Founder and Chief Technology Officer of Technology Pathways, a provider of security products and services. Mr. Brown is the chief architect of the ProDiscover family of computer security and forensics products. Mr. Brown teaches network security and computer forensics at the University of California at San Diego and has written numerous books on Windows, the Internet, and digital forensics, most recently *Computer Evidence: Collection and Preservation* (2010). Mr. Brown retired from a career with the U.S. Navy, where he managed a team of 80 technicians working in the area of Information Warfare and Network Operations.

Gregory Carlton, Ph.D.

Dr. Gregory Carlton is an Assistant Professor in the Computer Information Systems Department at California State Polytechnic University in Pomona, California. His dissertation was the first to use grounded theory in a study related to computer forensics. Dr. Carlton is active in the digital forensics industry as a teacher, author, and practitioner.

Eoghan Casey, M.S.

Mr. Eoghan Casey is the founding partner of cmdLabs. For over a decade, he has dedicated himself to advancing the practice of incident handling and digital forensics and has helped client organizations handle security breaches and analyze digital evidence in a wide range of investigations, including network intrusions with international scope. Mr. Casey has testified in civil and criminal cases, and has submitted expert reports and prepared trial exhibits for computer forensic and

cyber-crime cases. He has also performed thousands of forensic acquisitions and examinations, including e-mail and file servers, mobile devices, backup tapes, database systems, and network logs. In addition, he conducts research and teaches graduate students at Johns Hopkins University Information Security Institute, is Editor-in-Chief of Elsevier's *International Journal of Digital Investigation*, and has written several books, including *Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet* (2004).

Fred Cohen, Ph.D.

Dr. Fred Cohen is the Chief Executive Officer of Fred Cohen & Associates and President of the California Sciences Institute, site of the first Ph.D. in Computer Forensics. Dr. Cohen is well known for his seminal publications on computer viruses and defenses, critical infrastructure protection, and the use of deception and counter-deception in information assurance. Dr. Cohen has taught graduate courses in digital forensics since the late 1990s, is the author of *Challenges to Digital Forensic Evidence* (2008) and *Digital Forensic Evidence Examination*, 2nd ed. (2010), and has delivered lectures, courses, and expert testimony related to digital evidence for over a decade.

Christopher Kelly, J.D.

Mr. Christopher Kelly is the Managing Attorney for the Cybercrime Division of the Massachusetts Attorney General's Office (AGO). In addition to prosecuting and overseeing investigations of computer-related and cyber crimes, Mr. Kelly works with members of the Cybercrime Division to design and implement priority projects and training sessions as set forth in the Massachusetts Strategic Plan for Cyber Crime. Prior to joining the AGO, Mr. Kelly worked in the Suffolk County District Attorney's Office, where he created the Computer Crime Division and Computer Forensic Laboratory in 2004. During his tenure in Suffolk, Mr. Kelly prosecuted hi-tech, Internet, child exploitation, child sexual and physical abuse, and economic crime cases. Mr. Kelly is an EnCase Certified computer forensic examiner, International Association of Computer Investigative Specialist (IACIS) certified digital evidence collection specialist, and an adjunct professor of computer forensics at Bunker Hill Community College.

Erin Kenneally, M.F.S., J.D.

Ms. Erin Kenneally is Chief Executive Officer of Elchemy, Inc. and holds a Cyber Forensics Analyst position at the University of California, San Diego. She is a licensed attorney and forensic scientist, providing advice, performing research, and writing articles about prevailing and emerging issues at the crossroads of information technology and the law, including information forensics, privacy technology, and information risk. Ms. Kenneally consults with various private sector and government advisory committees and working groups,

and has served as Privacy Strategist for several federally funded integrated justice information programs.

Frederick Lane, J.D.

Mr. Frederick Lane is an author, attorney, lecturer, and expert witness who has appeared as a guest on *The Daily Show with Jon Stewart*, CNN, NBC, and other broadcast network news programs. Mr. Lane has written five books and many articles, and lectures frequently to college, university, and professional groups on the impact of emerging technologies on personal privacy. He provides expert witness testimony and consultation on computer forensic issues in civil and criminal litigation. Mr. Lane also offers a series of continuing legal education seminars to educate attorneys on emerging legal and technical trends in computer forensics.

Michael Schirling, M.Ed.

Mr. Michael Schirling is Chief of the Burlington Police Department and a co-founder of the Vermont Internet Crimes and Internet Crimes Against Children Task Forces. Specializing in high technology investigations, Chief Schirling has been conducting Internet investigations and computer forensics examinations for over 12 years. He trains and has lectured to audiences including police officers, investigators, and prosecutors regionally and nationally on topics that include cybercrime investigation, computer forensics, criminal law, interview and interrogation, and child exploitation. Chief Schirling also consults with a number of agencies and organizations such as the American Prosecutors Research Institute, National District Attorneys Association, and the U.S. State Department.

Robert Simpson, J.D.

Mr. Robert Simpson is a lawyer with over 30 years experience, nearly all of it litigating cases before juries, judges, and administrative boards. Mr. Simpson's criminal cases ranged from homicide and sex crimes to impaired operation of a motor vehicle and embezzlement. His administrative cases ranged from wildlife habitat preservation to hazardous waste cleanup. Mr. Simpson retired as Chittenden County (Vermont) State's Attorney in 2006 and currently directs the Criminal Justice program at Champlain College in Burlington, Vermont.

Appendix B

Initial Survey

DIGITAL FORENSIC EVIDENCE RESEARCH STUDY

Part I. Please separate and keep this page for your records.

Overview and Agreement to Participate in
Digital Forensic Evidence Research Study

Gary C. Kessler
Principal Investigator

You are being asked to participate in a study about trial judges in the U.S. and their attitudes related to digital forensic evidence. I am a Professor of Computer & Digital Forensics and Digital Investigation Management at Champlain College in Burlington, Vermont, and a member of the Vermont Internet Crimes Against Children (ICAC) Task Force. I am also a Ph.D. candidate in Computing Technology in Education (CTE) at Nova Southeastern University in Ft. Lauderdale, Florida, conducting this study as part of my dissertation research.

The purpose of this study is to identify issues related to trial judges' awareness, understanding, and application of digital forensic evidence. You are being asked to participate because you are a member of the American Bar Association Judicial Division.

I anticipate that completion of this survey will take no more than approximately 20 minutes. There will be one (possibly two) follow-up surveys in the next six months; the last part of the survey provides an informed consent form and contact information form which you can send me if you are willing to participate in the next round.

I believe that there is little or no risk to participating in this research project. In addition, no data is being requested or maintained that will link individuals to their responses. All data will be maintained in a private and confidential manner. All survey results will be reported only in the aggregate.

Participating in this research may be of no direct benefit to you, although it may make you more aware of your own attitudes about digital evidence. It is believed that the

results of this study will identify training and education that will benefit the larger community of trial judges.

You will receive no compensation for participating in this study. Participation in this research project is completely voluntary. You are free to withdraw from participation at any time during the duration of the questionnaire with no penalty or loss of benefit to which you would otherwise be entitled.

Research data will be confidential to the extent allowed by law. Agencies with research oversight, such as Nova Southeastern University's Institutional Review Board, have the authority to review research data. All research records will be stored in encrypted files on my computer and/or in a locked file in my office for the duration of the study. All other research records will be destroyed upon completion of the project.

Your participation is greatly appreciated, and I hope that it will benefit the practice of computer forensics and use of digital forensic evidence in court. If you have any questions or concerns regarding this research study, please contact me.

If you have any questions regarding your rights as a research participant, please contact the Nova Southeastern University Institutional Review Board at 866-499-0790 or irb@nova.edu.

Thank you very much.

I have read and understand the above information and agree to participate in this research project. Removing this page from the survey and returning the survey indicates my consent to participate in this phase of the study.

Gary C. Kessler
CTE Ph.D. Candidate
Principal Investigator, Digital Forensic Evidence Research Study
Nova Southeastern University
Ft. Lauderdale, FL 33314

2 Southwind Drive
Burlington, VT 05401
802-238-8913
gkessler@nova.edu

DIGITAL FORENSIC EVIDENCE RESEARCH STUDY

Part II. Please return this portion of the survey. Feel free to use additional pages, if necessary.

QUESTIONNAIRE A

Q0. Has any party offered digital forensic evidence (or evidence from the computer forensics process) in any evidentiary motion or trial over which you have presided? (Yes/No)

IF YOUR ANSWER TO QUESTION 0 IS "NO," PLEASE SKIP TO QUESTION 11.

Q1. Consider the following definition:

"*Digital forensic evidence* refers to information offered at legal proceedings to aid in the decision-making process that is derived from digital sources and the digital forensics process. Digital sources include computing devices (e.g., laptop and desktop computers, routers, music players, cameras, personal digital assistants, and cell phones) and telecommunication networks (e.g., wireline telephone and television services, wireless network providers, Internet service providers)."

Do you agree with this working definition? (Yes/No)

Q1A. If "no" to Q1, how would you modify the definition?

Q2. What issues, if any, have you faced in deciding on how to rule on challenges to the admissibility of digital forensic evidence?

Q3. Do you require lawyers to meet a higher standard than physical forensic evidence when they seek to authenticate and admit digital forensic evidence? For example, do you require a higher standard when they seek to authenticate and admit evidence retrieved from business records databases, e-mail, or Web sites?

Q3A. If "yes" to Q3, what are the concerns that prompt you to require this higher standard and/or what is the informational basis that catalyzed this higher standard?

Q3B. If "yes" to Q3, what specific facts and circumstances must the lawyer establish in order to satisfy your concerns?

Q4. Are there some types of cases where you are generally more (or less) likely to expect digital forensic evidence to be offered at trial than other cases?

Q4A. If “yes” to Q4, in what types of cases are you more likely to expect to see digital forensics evidence and what types of digital forensics evidence might you expect in those cases?

Q4B. If “yes” to Q4, in what types of cases are you less likely to expect to see digital forensics evidence?

Q5. Considering the presentation of digital evidence in hearings and trials in your courtroom, what factors lead to a more (or less) effective presentation of that evidence to a fact-finder?

Q6. Consider the testimony of a digital forensic examiner whose testimony is based, in significant part, on the use of forensic hardware or software tools. What would you require in order to establish the reliability of the forensic tools (e.g., would you require the examiner to have a detailed understanding of how/why the relevant software or hardware works, or would it be sufficient for the examiner to establish that he/she had significant training and experience in how to use the tools)?

Q7. On a scale of 1 to 5 (with 1 being the lowest and 5 being the highest), how would you rate your own familiarity with:

Q7A. Digital forensic evidence

Q7B. The computer forensics process

Q7C. Computer technologies

Q7D. Internet applications

Q8. What factors have influenced your ratings in Question 7 (e.g., education, personal experience, professional training)?

Q9. Do you believe that you have more, the same, or less understanding of digital forensic evidence than your peer judges:

Q9A. Locally?

Q9B. Nationally?

Q10. What is the standard of technical competence to which you hold attorneys who are handling cases involving digital forensic evidence? How does the technical understanding of the attorneys presenting digital evidence at hearings and at trial affect the effectiveness of that evidence to the fact-finder?

Q11. Demographic Information

Q11A. How long have you served on the bench?

Q11B. At what level of court do you currently preside?

Q11C. How many years have you been in your current position?

Q11D. What is your age?

Q11E. What is your gender?

Q11F. What is the approximate population of the jurisdiction in which you preside?

DIGITAL FORENSIC EVIDENCE RESEARCH STUDY

Part III. If you agree to participate in the survey follow-up, please return this page and one copy of the attached informed consent form.

SURVEY FOLLOW-UP REQUEST

The nature of this study is such that one, possibly two, follow-up surveys will be required in addition to this initial questionnaire. The follow-up survey(s) will be much like this one, with a series of short-answer questions and a target completion time of approximately 20 minutes.

If you would be willing to be contacted by e-mail or postal mail for a follow-up, please provide contact information below. All identifying information will be separated from any survey materials.

Because the information on this page is Personal Indentifying Information (PII), a signed informed consent form must be submitted prior to any subsequent contact. If you are interested in participating in the follow-up, please initial each page and sign one copy of the attached informed consent form, and retain one copy for your records.

Submitting these forms does not commit you for any further activity. Participation in this study is wholly voluntary, and participants may leave the study at any time.

Name: _____

Address: _____

_____

_____

E-mail: _____

Phone: _____

Please indicate preferred method to receive the follow-up survey:

E-mail Postal mail

Once again, you have my thanks.

Consent Form for Participation in the Digital Forensics Evidence Study

Funding Source: None

IRB approval # (Generated by IRB)

Principal investigator:
Gary C. Kessler, Ed.S.
2 Southwind Drive
Burlington, VT 05401
802-238-8913
gkessler@nova.edu

Co-investigator:
Marlyn Littman, Ph.D.
Nova Southeastern University
3301 College Avenue
DeSantis Building Room 4121
Ft. Lauderdale, FL 33314
954-262-2078
marlyn@nova.edu

Institutional Review Board (IRB)
Nova Southeastern University
Office of Grants and Contracts
(954) 262-5369/Toll Free: 866-499-0790
IRB@nsu.nova.edu

Description of the Study:

The nature of this study is such that one, possibly two, follow-up surveys will be required in addition to the initial anonymous questionnaire. The follow-up survey(s) will be much like the first one, with a series of short-answer questions and a target completion time of approximately 20 minutes.

The initial survey is being distributed and returned in person. Subsequent surveys can be distributed and returned by electronic mail or postal service. This approach requires the collection of personal identifying information (PII).

Because PII is being gathered, continued participation in this study requires a signed informed consent form. With this form, we are requesting your continued participation.

Risks/Benefits to the Participant:

There is a minimal risk of loss of confidentiality in submitting the survey by e-mail or postal mail. The process of immediately discarding the e-mail message or postal mail envelope when surveys are returned minimizes that risk. Survey results will not be saved in any way that will link back to an individual. Surveys and signed informed consent forms will be stored separately. Surveys will be stored on the researcher's computer in an encrypted form and/or in hard copy in a locked space in the researcher's office. All survey results will be reported only in the aggregate, and raw data will be destroyed at the first opportunity allowed by law.

There are no other anticipated or known risks associated with this study.

There are no direct benefits to the participant for taking part in this study.

If you have any concerns about the risks or benefits of participating in this study, you can contact Gary C. Kessler, Dr. Marlyn Littman, or the IRB office at the numbers indicated above.

Costs and Payments to the Participant:

There are no costs to you or payments made for participating in this study.

Confidentiality and Privacy:

Data will be stored in such a way as to protect the confidentiality and privacy of all participants while maintaining the integrity of the research process. No survey information will be stored in any way that will link back to an individual. Surveys and signed informed consent forms will be stored separately. Surveys will be stored on the researcher's computer in an encrypted form and/or in hard copy in a locked space in the researcher's office. All survey results will be reported only in the aggregate, and raw data will be destroyed at the first opportunity allowed by law.

All information obtained in this study is strictly confidential unless disclosure is required by law. The IRB and regulatory agencies may also review research records.

Use of Protected Health Information (PHI):

This study does not require the disclosure of any Protected Health Information.

Participant's Right to Withdraw from the Study:

You have the right to refuse to participate or to withdraw from this study at any time, without penalty. If you do refuse to participate or withdraw, it will not affect you in any way. If you choose to withdraw, any data that you have submitted will not be destroyed and will be kept for the length of this study; all raw data will be destroyed at the first opportunity allowed by law.

Other Considerations:

If significant new information relating to the study becomes available which may relate to your willingness to continue to participate, this information will be provided to you by the investigators.

Voluntary Consent by Participant:

I have read the preceding consent form, or it has been read to me, and I fully understand the contents of this document and voluntarily consent to participate in the research study "Digital Forensic Evidence Research Study." All of my questions concerning the research have been answered. I hereby agree to participate in this research study. If I have any questions in the future about this study they will be answered by Gary C. Kessler. A copy of this form has been given to me. This consent ends at the conclusion of this study.

Participant's Signature: _____ Date: _____

Witness's Signature: _____ Date: _____

Appendix C

Contacts at Judges' Associations

American Bar Association

Judge Herbert B. Dixon, Jr.
Chair, Court Technology Committee, Judicial Division
Former Chair, National Conference of State Trial Judges
Technology Columnist, *The Judges' Journal*

Judge Barbara Lynn
President, Judicial Division

American Judges Association

Judge Elliott Zide
Chair, Education Committee

National Center for State Courts

Nicole L. Waters, Ph.D.
Senior Court Research Associate
(Secretariat for the American Judges Association, the Conference of Chief Justices, and the National Association of Women Judges)

National Judicial College

William F. Dressel
President

Appendix D

Interview Questions

Gary Kessler
gkessler@nova.edu
802-238-8913

1. Tell me about the methods that you rely on in order to authenticate different types of digital evidence, such as, but not limited to, e-mail messages or a set of Web pages.

    a. Do you feel that you understand, or could explain, the process by which e-mail moves across the Internet? Do you feel that you understand how to apply applicable laws to e-mail in transit and in storage?
    b. Do you feel that you understand the way in which Web pages are accessed via a browser and information stored on a user's computer?
    c. Do you feel that you have a good general understanding of the operation of the Internet?

2. Tell me about any times that you have considered hiring, or have actually hired, a digital forensics expert as a consultant to the court, independent of any experts hired by the parties to the trial case.

    a. What were the factors that prompted you to consider or hire such an expert?
    b. In what ways, if any, did you find the court's expert helpful?
    c. How, if at all, do you think that the use of such an expert affected the outcome of the case?

3. Tell me about how you have obtained the knowledge that you use to apply to the evaluation of digital forensics evidence, and how you maintain currency with the technology and law.

    a. What kind of direct experiences do you have with computers, networks, technology, and digital forensic evidence?
    b. What kind of any specialized education or training do you have related to computers, networks, technology, and digital forensic evidence?
    c. How do you maintain currency in your knowledge of computers, networks, technology, and decisional law related to digital forensics evidence?

4. Tell me what types of additional knowledge related to information technology and digital forensic evidence would help you on the bench.

5. Describe for me your own use of e-mail, the World Wide Web, and/or other Internet services.

    a. For what purposes do you primarily use e-mail (e.g., personal communication, professional communication with colleagues, professional lists)?
    b. For what purposes do you primarily use the Web (e.g., general purposes, access to news, access to professional materials)?
    c. Do you use other Internet services (e.g., news services, chat rooms, instant messaging, e-mail, peer-to-peer services, social networks, online banking, online purchases) on a regular basis? If so, what kinds of services and for what purposes?
    d. Do you feel that your personal experiences with personal computer technology had impacted your understanding of issues related to digital forensic evidence? If so, how?

6. Tell me about recommendations that you might make to other judges to improve their own knowledge and awareness of digital forensic evidence.

7. Describe what recommendations you would make for judicial education and training as it relates to digital forensic evidence.

8. For purposes of judging the quality of scientific/technical evidence, does your state follow the Frye rules, Daubert rules, or a hybrid?

    a. If neither Frye nor Daubert, what are the rules that you follow?

9. Please share any other comments that would help me better understand judges and their knowledge, awareness, and application of digital forensics education.

Additional follow-up questions will depend upon the answers provided to the questions above and available time.

Appendix E

Interview Consent Form

Consent Form for Participation in the Research Study Entitled Judges' Awareness, Understanding, and Application of Digital Forensic Evidence

Funding Source: None

IRB approval #

Principal investigator:
Gary C. Kessler, Ed.S.
2 Southwind Dr.
Burlington, VT 05401
802-238-8913
gkessler@nova.edu

Co-investigator:
Marlyn Littman, Ph.D.
Nova Southeastern University
3301 College Avenue
DeSantis Building Room 4121
Ft. Lauderdale, FL 33314
954-262-2078
marlyn@nova.edu

Institutional Review Board (IRB)
Nova Southeastern University
Office of Grants and Contracts
(954) 262-5369/Toll Free: 866-499-0790
IRB@nsu.nova.edu

Site information:
Interviews related to this study will take place at locations selected by the study participants

Description of the Study:

This research study is investigating judges' awareness of digital evidence, their knowledge of the underlying technologies, and their application of digital evidence in court. The goals of this study are to increase the body of research literature in this area and to propose possible further directions for judicial training and education related to digital evidence.

The nature of this study requires interviews between the researcher and human subjects. In order to ensure accuracy in recording the contents of the interviews, to be able to focus on the actual words that are stated, and to minimize any bias or omissions that might occur due to simple note taking, the interviews will be recorded. Interviews are expected to last between 30 and 60 minutes.

Because audiotaping of the interviews will occur, study participants are required to sign an informed consent form. With this form, we are requesting your participation in the interview process.

Initials: _____ Date: _____

Audio Recording:

This research project will include the audio recording of an interview by the researcher with subjects of the study. This digital audio file will be available to be heard by the researcher, the university's human research oversight board (the Institutional Review Board or IRB), co-investigator/dissertation adviser Dr. Marlyn Littman, and no one else. The file will be transcribed by the researcher using headphones in a private office. The file will be stored as an encrypted file on storage media secured in the researcher's office. The recording will be kept for 36 months after the end of the study and destroyed after that time using a secure wiping process. Because your voice will be potentially identifiable by anyone who hears the recording, your confidentiality for things you say on the tape cannot be guaranteed, although the researcher will try to limit access to the recording as described above.

Risks/Benefits to the Participant:

There is a minimal risk of loss of confidentiality in submitting to the interview. The audio recording and any notes from the interview will remain on the researcher's person until secured in the researcher's office, as described above. Interview information will not be saved in any way that will link back to an individual, and audio files themselves will be encrypted upon storage in the researcher's office. Any notes about the interview will be stored in hard copy in a locked space in the researcher's office. All results will be reported only in the aggregate, and raw data will be destroyed 36 months after the end of the study.

There are no other anticipated or known risks associated with this study.

There are no direct benefits to the participant for taking part in this study.

If you have any concerns about the risks or benefits of participating in this study, you can contact Gary C. Kessler, Dr. Marlyn Littman, or the IRB office at the numbers indicated above.

Costs and Payments to the Participant:

There are no costs to you or payments made for participating in this study.

Confidentiality and Privacy:

Data will be stored in such a way as to protect the confidentiality and privacy of all participants while maintaining the integrity of the research process. No information will be stored in any way that will link back to an individual. Digital audio files of interviews will be stored in an encrypted form on external storage media and secured in the researcher's office. All resultant information will be reported only in the aggregate. Raw data will be retained for 36 months after the conclusion of the study (the minimum retention time allowed by the IRB); digital files will be destroyed at that time using a secure wiping process, and notes and other papers will be shredded.

All information obtained in this study is strictly confidential unless disclosure is required by law. The IRB and regulatory agencies may also review research records.

Use of Protected Health Information (PHI):

This study does not require the disclosure of any Protected Health Information.

Participant's Right to Withdraw from the Study:

You have the right to refuse to participate or to withdraw from this study at any time without penalty. If you do refuse to participate or withdraw, it will not affect you in any way. If you choose to withdraw, you may request that any of your data which has been collected be destroyed unless prohibited by state or federal law. Your data will be retained for 36 months from the end of the study.

Other Considerations:

If significant new information relating to the study becomes available that may relate to your willingness to continue to participate, this information will be provided to you by the investigators.

Voluntary Consent by Participant:

I have read the preceding consent form, or it has been read to me, and I fully understand the contents of this document and voluntarily consent to participate in the research study "Digital Forensic Evidence Research Study." All of my questions concerning the research have been answered. I hereby agree to participate in this research study. If I have any questions in the future about this study they will be answered by Gary C. Kessler. A copy of this form has been given to me. This consent ends at the conclusion of this study.

Participant's Signature: _____ Date: _____

Witness's Signature: _____ Date: _____

Appendix F

Other Individuals Providing Information

Several other individuals referenced in this paper provided information via personal communication that was of value to the author. Those individuals are:

- Judge Edward Cashman (ret.), Vermont District Court
- Kathleen Muldoon, Esq., Assistant State's Attorney, Cook County, Illinois
- Lee Suskin, Esq., Court Administrator, Vermont Supreme Court
- Michael Touchette, Vermont Department of Corrections
- Dr. Ray Vaughn, Department of Computer Science and Engineering, Mississippi State University

Appendix G

Acronyms and Abbreviations

ABA/JD	American Bar Association Judicial Division
AJA	American Judges Association
ESI	Electronically Stored Information
FRE	Federal Rules of Evidence
ICT	Information and communication technology
IP	Internet Protocol
ISP	Internet service provider
IT	Information technology
LE	Law enforcement
LEO	Law enforcement officer
NCSC	National Center for State Courts
NJC	National Judicial College
NSU	Nova Southeastern University
PDA	Personal digital assistant
RAM	Random access memory

Reference List

Agarawala, A., & Balakrishnan, R. (2006). Keepin' it real: Pushing the desktop metaphor with physics, piles and the pen. In *ACM Conference on Human Factors in Computing Systems (SIGCHI)* (pp. 1283-1292). New York, NY: Association for Computing Machinery.

American Academy of Forensic Sciences (AAFS). (2008). *AAFS digital & multimedia sciences.* Retrieved April 6, 2010, from https://www.aafs.org/content/aafs/sections/digital_multimedia.asp

American Bar Association (ABA). (2007, February). *ABA model code for judicial conduct*. Retrieved April 23, 2010, from http://www.abanet.org/judicialethics/ABA_MCJC_approved.pdf

American Bar Association (ABA). (2009a). A study about judges' perceptions of digital forensic evidence. *Judicial Division Record, 12*(4), 3.

American Bar Association (ABA). (2009b, June 1). Judge reprimanded for friending lawyer and Googling litigant. *ABAJOURNAL Law News Now*. Retrieved April 28, 2010, from http://www.abajournal.com/news/article/judge_reprimanded_for_friending_lawyer_and_googling_litigant/

American Express Travel Related Services v. Vinhnee, 336 B.R. 437 (U.S. Bankruptcy Appellate Panel, 9th Cir. 2005).

Anderson, R. (2008). *Security engineering* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Arning, K., & Ziefle, M. (2007). Understanding age differences in PDA acceptance and performance. *Computers in Human Behavior, 23*(6), 2904-2927.

Balko, R. (2009). *Cross-examining forensics.* Retrieved April 4, 2010, from http://reason.com/news/printer/135325.html

Ball, C. (2008). What judges should know about computer forensics. *National Workshop for District Judges II*. Retrieved April 6, 2010, from http://www.craigball.com/What_Judges_Computer_Forensics-200807.pdf

Baskerville, R., & Pries-Heje, J. (1999). Grounded action research: A method for understanding IT in practice. *Accounting, Management and Information Technology, 9*(1), 1-23.

Beebe, N. L. (2009). Digital forensic research: The good, the bad, and the unaddressed. In G. Peterson & S. Shenoi (Eds.), *Advances in Digital Forensics V*, IFIP AICT 306 (pp. 17-36). Berlin, Germany: International Federation of Information Processing.

Bensen, R. J. (2004). The increasing significance of computer forensics in litigation. *Intellectual Property & Technology Law Journal*, *16*(11), 1-4.

Bernstein, D. E. (2008). Expert witnesses, adversarial bias, and the (partial) failure of the Daubert revolution. *George Mason University Law and Economics Research Paper No. 07-11*. Retrieved May 5, 2010, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=963461

Brown, C. L. T. (2010). *Computer evidence: Collection and preservation* (2nd ed.). Boston, MA: Course Technology.

Brown, S. C., Stevens, Jr., R. A., Troiano, P. F., & Schneider, M. K. (2002, March/April). Exploring complex phenomena: Grounded theory in student affairs research. *Journal of College Student Development*, *43*(2), 1-11. Retrieved May 5, 2010, from http://www.colgate.edu/portaldata/imagegallerywww/4119/ImageGallery/Grounded_Theory.pdf

Caloyannides, M. A. (2003). Digital "evidence" and reasonable doubt. *IEEE Security & Privacy*, *1*(6), 89-91.

Carlton, G. H. (2006). *A protocol for the forensic data acquisition of personal computer workstations*. Unpublished doctoral dissertation, University of Hawaii, Honolulu.

Carlton, G. H. (2007). A grounded theory approach to identifying and measuring forensic data acquisition tasks. *Journal of Digital Forensics, Security and Law*, *2*(1), 35-55.

Casey, E. (2002). Error, uncertainty, and loss in digital evidence. *International Journal of Digital Evidence*, *1*(2). Retrieved May 5, 2010, from http://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf

Casey, E. (2011). *Digital evidence and computer crime: Forensics science, computers and the Internet* (3rd ed.). Amsterdam, The Netherlands: Elsevier Academic Press.

Casey, E., Ferraro, M., & Nguyen, L. (2009). Investigation delayed is justice denied: Proposals for expediting forensic examinations of digital evidence. *Journal of Forensic Sciences*, *54*(6), 1353-1364.

Casey, E., & Stellatos, G. J. (2008). The impact of full disk encryption on digital forensics. *Operating Systems Review*, *42*(3), 93-98.

Charmaz, K. (2000). Grounded theory: Objectivist and constructivist methods. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (2nd ed., pp. 509-535). Thousand Oaks, CA: Sage.

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Thousand Oaks, CA: Sage.

Clemens, A. M. (2004). No computer exception to the Constitution: The Fifth Amendment protects against compelled production of an encrypted document or private key. *UCLA Journal of Law and Technology, 2*. Retrieved May 5, 2010, from http://www.lawtechjournal.com/articles/2004/02_040413_clemens.php

Cohen, F. (2008). *Challenges to digital forensics evidence*. Livermore, CA: ASP Press.

Cohen, F. (2010). *Digital forensic evidence examination* (2nd ed.). Livermore, CA: ASP Press.

Common Digital Evidence Storage Format Working Group (CDESF). (2006). *Survey of disk image formats (Version 1.0)*. Retrieved May 5, 2010, from http://www.dfrws.org/CDESF/survey-dfrws-cdesf-diskimg-01.pdf

Commonwealth v. *Lanigan*, 419 Mass. 15, 641 N.E.2d 1342 (1994).

Crespo-Cuaresma, J., Foster, N., & Scharler, J. (2008). Barriers to technology adoption, international R and D spillovers and growth. *Economics Bulletin, 15*(3), 1-7. Retrieved May 5, 2010, from http://www.accessecon.com/pubs/EB/2008 /Volume15/EB-08O30001A.pdf

Daley, J. D., & Allen, Jr., T. F. (1999). Judicial gatekeeping in Massachusetts. *The Judicial Gatekeeping Project, Berkman Center for Internet and Society and Harvard Law School*. Retrieved May 3, 2010, from http://cyber.law.harvard.edu/daubert/ma.htm

Daubert v. Merrell Dow Pharmaceuticals, Inc. (92-102), 509 U.S. 579 (1993). Retrieved May 5, 2010, from http://www.law.cornell.edu/supct/html/92-102.ZO.html

Del Bosque, D., & Chapman, K. (2008). Users 2.0: Technology at your service. In R. Tennant (Ed.), *Technology in libraries: Essays in honor of Anne Grodzins Lipow* (pp. 49-55). Retrieved May 5, 2010, from http://techinlibraries.com/delbosque.pdf

Dick, B. (2005). *Grounded theory: A thumbnail sketch.* Retrieved May 5, 2010, from http://www.scu.edu.au/schools/gcm/ar/arp/grounded.html

Dinat, J.-M. (2004). The long way from electronic traces to electronic evidence. *International Review of Law, Computers and Technology*, *18*(2), 173-183.

Dipalo, M. (2010, April 26). *Google earth.* Posting on High Technology Crime Consortium e-mail list.

Duch, B. J., Groh, S. E., & Allen, D. E. (Eds.). (2001). *The power of problem-based learning*. Sterling, VA: Stylus.

Elliott, N., & Lazenbatt, A. (2005). How to recognise a “quality” grounded theory research study. *Australian Journal of Advanced Nursing*, *22*(3), 48-52.

Farid, H. (2009). Image forgery detection. *IEEE Signal Processing Magazine*, *26*(2), 16-25.

Fernández, W. D. (2004). The grounded theory method and case study data in IS research: Issues and design. In D. Hart & S. Gregor (Eds.), *Proceedings of the Information Systems Foundations: Constructing and Criticising Workshop,* Australian National University, July 16-17. Retrieved May 5, 2010, from http://epress.anu.edu.au/info_systems/mobile_devices/ch05.html

Frowen, A. (2009). *Computer forensics in the courtroom: Is an IT literate judge and jury necessary for a fair trial?* Retrieved April 20, 2010, from http://www.articlesnatch.com/Article/Computer-Forensics-In-The-Courtroom--Is-An-It-Literate-Judge-And-Jury-Necessary-For-A-Fair-Trial-/568057

Frye v. United States, 54 App. D.C. 46, 293 F.1013 (1923).

Galves, F. (2000). Where the not-so-wild-things are: Computers in the courtroom, the Federal Rules of Evidence, and the need for institutional reform and more judicial acceptance. *Harvard Journal of Law & Technology*, *13*(2), 161-301.

Gerber, L. (2001). Computer forensics: High-tech law enforcement. *IEEE Computer Magazine*, *34*(1), 22-27.

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. New Brunswick, NJ: Aldine Transaction.

Haig, B. D. (1995). Grounded theory as scientific method. *Philosophy of Education Yearbook 1995*. Retrieved May 5, 2010, from http://www.ed.uiuc.edu/EPS /PES-yearbook/95_docs/haig.html

Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation, Special Issue: The Proceedings of the Digital Forensics Research Workshop 2006*, *3S*, S44-S49. Retrieved May 5, 2010, from http://www.dfrws.org/2006/proceedings/6-Harris.pdf

Heath, H., & Cowley, S. (2004). Developing a grounded theory approach: A comparison of Glaser and Strauss. *International Journal of Nursing Studies*, *41*(2), 141-150.

Huang, M.-Y., & Frince, D. A. (2007). Editorial: Systematic approaches to digital forensic engineering: Moving from art to disciplines. In *Proceedings of SADFE 2007: Second International Workshop on Systematic Approaches to Digital Forensic Engineering, 2007* (pp. viii-xii). Retrieved May 5, 2010, from http://csdl.computer.org/comp/proceedings/sadfe/2007/2808/00/2808viii.pdf

Hunter, M. G. (2005). Editorial preface: In support of qualitative information systems research. *Journal of Global Information Management*, *13*(4), i-iv.

Ieong, R. S. C. (2006). FORZA: Digital forensics investigation framework that incorporates legal issues. *Digital Investigation, Special Issue: The Proceedings of the Digital Forensics Research Workshop 2006* (pp. S29-S36). Retrieved May 5, 2010, from http://dfrws.org/2006/proceedings/4-Ieong.pdf

Insa, F. (2006). The admissibility of electronic evidence in court (A.E.E.C.): Fighting against high-tech crime: Results of a European study. *Journal of Digital Forensic Practice, 1*(4), 285-289.

International Telecommunication Union (ITU). (2009). *Measuring the information society: The ICT development index 2009.* Geneva, Switzerland: ITU. Retrieved July 26, 2010, from http://www.itu.int/ITU-D/ict/publications/idi/2009/material/IDI2009_w5.pdf

Jones, A. (2009). Computer science and the Reference Manual for Scientific Evidence: Defining the judge's role as a firewall. *Intellectual Property Law Bulletin, 14*(1), 23-40.

Kaufman, M. S. (2006). *The status of Daubert in state courts.* Retrieved July 19, 2010, from http://www.atlanticlegal.org /daubertreport.pdf

Kenneally, E. E. (2001a). *Computer forensics.* Retrieved May 5, 2010, from http://www.cs.ucsd.edu/classes/sp02/cse190_A/computerforensics.ppt

Kenneally, E. E. (2001b). Gatekeeping out of the box: Open source software as a mechanism to assess reliability for digital evidence. *Virginia Journal of Law and Technology, 6*(3). Retrieved May 5, 2010, from http://www.vjolt.net/vol6/issue3/v6i3-a13-Kenneally.html

Kenneally, E. E. (2005). Confluence of digital evidence and the law: On the forensic soundness of live-remote digital evidence collection. *UCLA Journal of Law and Technology, 9*(2). Retrieved May 5, 2010, from http://www.lawtechjournal.com/articles/2005/05_051201_Kenneally.php

Kenneally, E .E., & Brown, C. L. T. (2005). Risk sensitive digital evidence collection. *Digital Investigation, 2*(2), 101-119.

Kerr, O. S. (2005a). Digital evidence and the new criminal procedure. *Columbia Law Review, 105*(1), 279-318.

Kerr, O. S. (2005b). *Search warrants in an era of digital evidence* (The George Washington University Law School Public Law and Legal Theory Working Paper No. 128). Retrieved May 5, 2010, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=665662

Kerr, O. S. (2009). *Computer crime law* (2nd ed.). St. Paul. MN: Thomson/West.

Kerr, O. S. (2010). Fourth Amendment seizures of computer data. *The Yale Law Journal, 119*(4), 700-724. Retrieved May 5, 2010, from http://www.yalelawjournal.org/images/pdfs/853.pdf

Kessler, G. C., & Fasulo, M. (2007). The case for teaching network protocols to computer forensics examiners. In G. Dardick (Ed.), *Proceedings of the Conference on Digital Forensics, Security and Law* (pp. 115-137). Farmville, VA: Longwood University.

Kirk, J. (2008, October 14). UK appeals court rejects encryption key disclosure defense. *IDG News Service*. Retrieved May 5, 2010, from http://pcworld.about.com/od/businesscenter/UK-Appeals-Court-Rejects-Encry.htm

Kumho Tire v. Carmichael (97-1709), 526 U.S. 137, 131 F.3d 1433 reversed (1999). Retrieved May 5, 2010, from http://supct.law.cornell.edu/supct/html/97-1709.ZS.html

Lathoud, B. (2004). Formalization of the processing of electronic traces. *International Review of Law, Computers and Technology, 18*(2), 185-192.

Leedy, P. D., & Ormrod, J. E. (2010). *Practical research: Planning and design* (9th ed.). Upper Saddle River, NJ: Pearson Education.

Leroux, O. (2004). Legal admissibility of electronic evidence. *International Review of Law, Computers and Technology, 18*(2), 193-220.

Losavio, M., Adams, J., & Rogers, M. (2006). Gap analysis: Judicial experience and perception of electronic evidence. *Journal of Digital Forensic Practice, 1*(1), 13-17.

Losavio, M., Wilson, D., & Elmaghraby, A. (2006). Prevalence, use, and evidentiary issues of digital evidence of cellular telephone consumer and small-scale digital devices. *Journal of Digital Forensic Practice, 1*(4), 291-296.

Lyle, J. R., & Wozar, M. (2007). Issues with imaging drives containing faulty sectors. *Digital Investigation, Special Issue: The Proceedings of the Digital Forensics Research Workshop 2007* (pp. S13-S15). Retrieved May 5, 2010, from http://www.dfrws.org/2007/proceedings/p13-lyle.pdf

Mack, K., & Anleu, S. R. (2008). The national survey of Australian judges: An overview of findings. *Journal of Judicial Administration, 18*(5), 5-21.

Mack, M. (2008). *A process of illumination: The practical guide to electronic discovery*. Portland, OR: Fios. Retrieved April 4, 2010, from http://www.fiosinc.com/e-discovery-knowledge-center/electronic-discovery-book.aspx?id=586

Maher, R. C. (2009). Audio forensic examination. *IEEE Signal Processing Magazine, 26*(2), 84-94.

Manes, G. W., Downing, E., Watson, L., & Thrutchley, C. (2007). New federal rules and digital evidence. In G. Dardick (Ed.), *Proceedings of the Conference on Digital Forensics, Security and Law* (pp. 31-40). Farmville, VA: Longwood University.

Marcella, Jr., A. J., & Greenfield, R. S. (2002). *Cyber forensics: A field manual for collecting, examining, and preserving evidence of computer crimes.* Boca Raton, FL: Auerbach.

Marsico, C. V. (2004). *Computer evidence v. Daubert: The coming conflict* (CERIAS Tech Report 2005-17). Retrieved May 5, 2010, from https://www.cerias.purdue.edu/ bookshelf/archive/2005-17.pdf

Mason, S. (2008). Judges and technical evidence. Keynote address at *CFET 2008: The 2nd International Conference on Cyberforensics Education and Training,* Canterbury Christ Church University, Canterbury, UK, September.

Massachusetts Courts. (2010). *Massachusetts Court System* Web site. Retrieved April 15, 2010, from http://www.mass.gov/courts/courtsandjudges /courts/index.html

McCullagh, D. (2007, December 14). Judge: Man can't be forced to divulge encryption passphrase. *CNET News*. Retrieved May 6, 2010, from http://news.cnet.com /8301-13578_3-9834495-38.html

McCullagh, D. (2009, February 26). Judge orders defendant to decrypt PGP-protected laptop. *CNET News*. Retrieved May 6, 2010, from http://news.cnet.com /8301-13578_3-10172866-38.html

Melendez-Diaz v. Massachusetts, 69 Mass. App. 1114, 870 N. E. 2d 676, reversed and remanded. (2009). Retrieved August 9, 2010, from http://www.law.cornell.edu/supct/html/07-591.ZS.html

Metasploit LLC. (2010). *Metasploit Anti-forensics*. Retrieved May 5, 2010, from http://www.metasploit.com/research/projects/antiforensics/

Meyers, M., & Rogers, M. (2006). Digital forensics: Meeting the challenges of scientific evidence. In M. Pollitt & S. Shenoi (Eds.), *International Federation for Information Processing (IFIP): Vol. 194. Advances in Digital Forensics* (pp. 43-50). Boston, MA: Springer.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). Thousand Oaks, CA: Sage.

Mills, J., Bonner, A., & Francis, K. (2006). The development of constructivist grounded theory. *International Journal of Qualitative Methods, 5*(1), Article 3. Retrieved May 5, 2010, from http://www.ualberta.ca/~iiqm/backissues/5_1/pdf/mills.pdf

Mingers, J. (2001). Combining IS research methods: Towards a pluralist research methodology. *Information Systems Research, 12*(3), 240-259.

Mislan, R. P., Casey, E., & Kessler, G. C. (2010). The growing need for on-scene triage of mobile devices. *Digital Investigation, 6*(3-4), 112-124.

Moncur, M. (2007). *Quotation #776 from Michael Moncur's (cynical) quotations.* Retrieved June 26, 2010, from http://www.quotationspage.com/quote/776.html

Morgan, W. P. (1995). Anxiety and panic in recreational scuba divers. *Sports Medicine, 20*(6), 398-421.

Myers, M. D. (2010). Qualitative research in information systems. *MIS Quarterly, 21*(2), 241-242. Retrieved May 3, 2010, from http://www.qual.auckland.ac.nz

Nance, K., Hay., B., & Bishop, M. (2009). Digital forensics: Defining a research agenda. In R. Sprauge (Ed.), *Proceedings of the Forty-Second Annual Hawai'i International Conference on System Sciences.* Los Alamitos, CA: IEEE Press.

National Institute of Justice (NIJ). (2007, January). *Digital evidence in the courtroom: A guide for law enforcement and prosecutors* (NIJ Special Report NCJ 211314). Washington, DC: U.S. Department of Justice, Office of Justice Programs. Retrieved May 5, 2010, from http://www.ncjrs.gov/pdffiles1/nij/211314.pdf

National Judicial College (NJC). (2009, September 9). What do you know about digital forensics evidence—and why? *NJC News*. Retrieved April 4, 2010, from http://www.judges.org/news/news090909.html

Neufeld, P. J. (2005). The (near) irrelevance of Daubert to criminal justice and some suggestions for reform. *American Journal of Public Health, 95*(S1), S107-S113. Retrieved May 5, 2010, from http://ajph.aphapublications.org/cgi/reprint/95/S1 /S107.pdf

New Jersey v. Reid, 389 N.J. Super. 563, 914 A.2d 310 (NJ Super. Ct. Appellate Div. 2007).

Newsham, T., Palmer, C., Stamos, A., & Burns, J. (2007). *Breaking forensics software: Weaknesses in critical evidence collection* (iSEC Partners White Paper, Version 1.1). Retrieved April 4, 2010, from https://www.isecpartners.com/files/iSEC- Breaking_ Forensics_Software-Paper.v1_1.BH2007.pdf

Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and examining computer forensics evidence. *Forensic Science Communication, 2*(4). Retrieved May 5, 2010, from http://www.fbi.gov/hq/lab/fsc/backissu/oct2000 /computer.htm

Nova Southeastern University (NSU). (2009, December). *Manual for research with human subjects*. NSU Institutional Review Board. Retrieved April 15, 2010, from http://www.nova.edu/irb/manual/forms/irb_manual.pdf

O'Harrow, Jr., R. (2006). *No place to hide*. New York, NY: Free Press.

Oppliger, R., & Rytz, R. (2003). Digital evidence: Dream and reality. *IEEE Security & Privacy, 1*(5), 44-48.

Orlikowski, W. J. (1993). CASE tools as organizational change: Investigating incremental and radical changes in systems development. *Management Information Systems Quarterly, 17*(3). Retrieved May 5, 2010, from http://misq.org/archivist/bestpaper/misq93.html

Palmer, G. L. (2002). Forensics analysis in the digital world. *International Journal of Digital Evidence, 1*(1). Retrieved May 5, 2010, from http://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E938F-E3BE-8D16-45D0BAD68CDBE77.doc

Pandit, N. R. (1996). The creation of theory: A recent application of the grounded theory method. *The Qualitative Report, 2*(4). Retrieved May 5, 2010, from http://www.nova.edu/ssss/QR/QR2-4/pandit.html

PGP Corporation. (2008). *PGP whole disk encryption.* Retrieved May 5, 2010, from http://www.pgp.com/products/wholediskencryption/index.html

Phillips, D. C., & Soltis, J. F. (2004). *Perspectives on learning* (4th ed.). New York, NY: Teachers College Press.

Pogson, C. E., Bott, J. P., Ramakrishnan, M., & Levy, P. E. (2002). A grounded theory approach to construct validity: Investigating first-order constructs in organizational justice to triangulate with current empirical research. *Research Methods Forum, 7*.

Ravenscroft, A., & McAlister, S. (2006). Digital games and learning in cyberspace: A dialogical approach. *E-Learning, 3*(1), 37-50.

Robson, C. (2002). *Real world research* (2nd ed.). Malden, MA: Blackwell.

Rogers, M., Scarborough, K., Frakes, K., & San Martin, C. (2007). Survey of law enforcement perceptions regarding digital evidence. In P. Craiger & S. Shenoi (Eds.), *International Federation for Information Processing (IFIP): Vol. 242, Advances in Digital Forensics III* (pp. 41-52). Boston, MA: Springer.

Rothstein, B. J., Hedges, R. J., & Wiggins, E. C. (2007). *Managing discovery of electronic information: A pocket guide for judges*. Washington, DC: Federal Judicial Center.

Roussev, V. (2009). Hashing and data fingerprinting in digital forensics. *IEEE Security & Privacy, 7*(2), 49-55.

Saferstein, R. (2009). *Forensics science: From the crime scene to the crime lab*. Upper Saddle River, NJ: Pearson Education.

Scarborough, K. E., Rogers, M., Frakes, K., & San Martin, C. (2009). Digital evidence. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 477-488). Upper Saddle River, NJ: Pearson Prentice Hall.

Schram, T. H. (2006). *Conceptualizing and proposing qualitative research* (2nd ed.). Upper Saddle River, NJ: Pearson Education.

Schwartz, J. (2009, March 17). As jurors turn to Web, mistrials are popping up. *The New York Times Online*. Retrieved May 3, 2010, from http://www.nytimes.com/2009/03/18/us/18juries.html

Sergienko, G. S. (1996, February 13). Self incrimination and cryptographic keys. *The Richmond Journal of Law and Technology, 2*(1). Retrieved May 5, 2010, from http://jolt.richmond.edu/v2i1/sergienko.html

Shaw, B. Z. (2006). Judging juries: Evaluating renewed proposals for specialized juries from a public choice perspective. *UCLA Journal of Law and Technology*, *10*(2). Retrieved May 5, 2010, from http://www.lawtechjournal.com/articles/2006/03_061117_shaw.pdf

Shelton, D. E. (2009). Twenty-first century forensic science challenges for trial judges in criminal cases: Where the "polybutadiene" meets the "bitumen." *Widener Law Journal, 18*(2), 309-396. Retrieved April 4, 2010, from http://works.bepress.com/donald_shelton/12

Shelton, D. E., Kim, Y. S., & Barak, G. (2009). An indirect-effects model of mediated adjudication: The CSI myth, the tech effect, and metropolitan jurors' expectations for scientific evidence. *Vanderbilt Journal of Entertainment and Technology Law*, *12*(1), 1-43. Retrieved April 4, 2010, from http://works.bepress.com/donald_shelton/15

Sprauge, R. (Ed.). (2009). *Proceedings of the Forty-Second Annual Hawai'i International Conference on System Sciences*. Los Alamitos, CA: IEEE Press.

Stallings, W. (2007). *Data and computer communications* (8th ed.). Upper Saddle River, NJ: Prentice Hall.

Stored Communications Act, 18 U.S.C. §§ 2701-2712 (1986). Retrieved May 5, 2010, from http://www.usdoj.gov/criminal/cybercrime/ECPA2701_2712.htm

Terrell, S. R. (2006). *Five steps to statistics: A consumer's guide to inferential decision making*. Unpublished manuscript, Nova Southeastern University, Ft. Lauderdale, FL.

Tibbitts, J., & Lu, Y. B. (2009). Forensic applications of signal processing. *IEEE Signal Processing Magazine, 26*(2), 104-111.

U.S. Census Bureau. (2010). *State & county quickfacts.* Retrieved July 27, 2010, from http://quickfacts.census.gov/qfd/index.html

U.S. Courts. (2008a). *Federal rules of civil procedure*. Administrative Office of the U.S. Courts. Washington, DC: U.S. Government Printing Office. Retrieved May 5, 2010, from http://www.uscourts.gov/rules/CV2008.pdf

U.S. Courts. (2008b). *Federal rules of criminal procedure*. Administrative Office of the U.S. Courts. Washington, DC: U.S. Government Printing Office. Retrieved May 5, 2010, from http://www.uscourts.gov/rules/CR2008.pdf

U.S. Courts. (2008c). *Federal rules of evidence*. Administrative Office of the U.S. Courts. Washington, DC: U.S. Government Printing Office. Retrieved May 5, 2010, from http://www.uscourts.gov/rules/EV2008.pdf

U.S. Legal. (2010). *Legal definitions & legal terms defined*. Retrieved May 5, 2010, from http://definitions.uslegal.com/

United States v. Boucher, WL 4246473 (2007).

United States v. Boucher, WL 424718 (D. Vt.) (2009).

United States v. Councilman, 373 F.3d 197 (1st Cir. 2004).

United States v. Councilman, 418 F.3d 67 (1st Cir. 2005).

van Baar, R. B., Alink, W., & van Ballegooij, A. R. (2008). Forensics memory analysis: Files mapped in memory. *Digital Investigation, Special Issue: The Proceedings of the Digital Forensics Research Workshop 2008* (pp. S52-S57). Retrieved May 5, 2010, from http://www.dfrws.org/2008/proceedings/p52-vanBaar.pdf

Van Buskirk, E., & Liu, V. T. (2006). Digital evidence: Challenging the presumption of reliability. *Journal of Digital Forensic Practice*, *1*(1), 19-26.

Vermont Judiciary. (n.d.). Court information. *Vermont Judiciary.org*. Retrieved April 15, 2010, from http://www.vermontjudiciary.org/GTC/default.aspx

Volonino, L. (2003). Electronic evidence and computer forensics. *Communications of the Association for Information Systems*, *12*, 457-468.

Waits, C., Akinyele, J. A., Nolan, R., & Rogers, L. (2008). *Computer forensics: Results of live response vs. memory image analysis*. Carnegie Mellon Software Engineering Institute, Technical Note CMU/SEI-2008-TN-017. Retrieved May 5, 2010, from http://www.cert.org/archive/pdf/08tn017.pdf

Wegman, J. (2005). Computer forensics: Admissibility of evidence in criminal cases. *Journal of Legal, Ethical and Regulatory Issues*, *8*(1). Retrieved May 5, 2010, from http://findarticles.com/p/articles /mi_m1TOS/is_1-2_8/ai_n25121965/? tag=content;col1

Whitcomb, C. M. (2002). An historical perspective of digital evidence: A forensics scientist's view. *International Journal of Digital Evidence*, *1*(1). Retrieved May 5, 2010, from http://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf

Wiretap Act, 18 U.S.C. §§ 2510-2522 (1986). Retrieved May 5, 2010, from http://www.usdoj.gov/criminal/cybercrime/wiretap2510_2522.htm

Zittrain, J. (2006). A history of online gatekeeping. *Harvard Journal of Law & Technology*, *19*(2), 253-298. Retrieved May 5, 2010, from http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf

Zubulake v. UBS Warburg, 217 F.R.D. 309, 2003 U.S. Dist. LEXIS 7939, 55 Fed. R. Serv. 3d (Callaghan) 622, 91 Fair Empl. Prac. Cas. (BNA) 1574 (S.D.N.Y. 2003).

Zubulake v. UBS Warburg, 2004 WL 1620866 (S.D.N.Y. July 20, 2004).