View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Embry-Riddle Aeronautical University

Security Studies & International Affairs - Daytona Beach

College of Arts & Sciences

2011

Judges' Awareness, Understanding, and Application of Digital Evidence

Gary C. Kessler
Norwich University, kessleg1@erau.edu

Follow this and additional works at: https://commons.erau.edu/db-security-studies

 Part of the Information Security Commons

Scholarly Commons Citation

Kessler, G. C. (2011). Judges' Awareness, Understanding, and Application of Digital Evidence. *Journal of Digital Forensics, Security and Law, 6*(1). Retrieved from https://commons.erau.edu/db-security-studies/25

This Article is brought to you for free and open access by the College of Arts & Sciences at Scholarly Commons. It has been accepted for inclusion in Security Studies & International Affairs - Daytona Beach by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

Judges' Awareness, Understanding, and Application of Digital Evidence

Gary C. Kessler
Gary Kessler Associates
Norwich University
Edith Cowan University
gck@garykessler.net

ABSTRACT

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 paper describes a recent study, using grounded theory methods, into judges' awareness, knowledge, and perceptions of digital evidence. This study is the first in the U.S. to examine 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 published digital forensics study, demonstrating the applicability of that methodology to this discipline. This paper describes the process of grounded theory, a high-level summary of results, and conclusions from the study.

Keywords: Digital evidence, judges, grounded theory

INTRODUCTION

In 2009 and 2010, the author surveyed and interviewed judges to learn about their knowledge and understanding of digital forensic evidence. This not only provided a greater understanding of how judges perceive digital evidence, but also led to a set of training and education recommendations based upon the interactions with the judges. This paper will describe the research project, its findings, and the recommendations.

The remainder of this paper is organized as follows. First, the problem description is provided. Second, the data gathering and analysis methodology, i.e., grounded theory, is briefly described. Next, the actual research method employed in this project is presented, followed by the project's findings and recommendations. The paper closes with some concluding remarks.

IDENTIFICATION OF THE PROBLEM

Forensics is the use of scientific or technical processes and procedures to address legal questions. Modern forensic science traces much of its roots to Emile

Locard's Principle (c. 1910), "Every contact leaves a trace." This concept is the basis of the forensic sciences; if one person hits another on the head with a tree branch, part of the victim's head is left on the branch and part of the branch is left on the victim's head. Comparing latent samples of blood, bullets, and deoxyribonucleic acid (DNA) found at a scene with known samples can identify or rule out suspects, while analysis of the state of a crime scene allows the forensic scientist to create a picture of the events that occurred related to the activity under investigation (Cohen, 2010; Jones, 2009; Kerr, 2009).

Digital forensics is similar -- yet different -- in several ways when compared to forensics based upon the physical sciences. First, the sources of information can come from devices physically found at a scene although other related information can come from devices in a telecommunication provider's network or from other end-user's device thousands of miles away from the search scene. Second, digital forensics is not necessarily a comparing science. Indeed, a digital forensic examiner is searching for latent digital information but uses that information to paint a picture of what has occurred rather than necessarily comparing it to other known samples (Casey, 2011; Cohen, 2010, Whitcomb, 2002).

Regardless of the differences, all of the forensic sciences follow the same basic process (Casey, 2011; Cohen, 2010):

1. *Identification:* Identify relevant, probative information that addresses issues related to the incident under investigation
2. *Preservation:* Protect and maintain the state of the information
3. *Acquisition and Collection:* Gather the relevant information and transport it to an examination facility without alteration
4. *Examination:* Search the collected information and extract data to assist in understanding the activities related to the incident under investigation
5. *Analysis:* Take all of the piece parts of the extracted data and re-create the events
6. *Reporting:* Document the findings, processes and procedures, methodologies, and conclusion related to the examination of the evidence

Digital Forensics

Unlike the forensic analyses that are based on the physical and life sciences (e.g., physics, chemistry, and biology), digital forensics has been largely driven by its practitioner community rather than by computer scientists. The practice of digital forensics within the law enforcement (LE) community dates back to at least the late-1980s. Even with the growth of electronic discovery (e-discovery) and the ever-growing number of civilians acting as digital forensic examiners, there is still a very parochial view of some within the LE community that computer forensics is a LE function.

As a case in point, the author attended a computer forensics curriculum development meeting sponsored by the National Institute of Standards and Technology (NIST) in 2005. A police officer at that meeting told the attendees that he believed that only sworn police officers should perform a computer forensics exam because only a sworn police officer knew how to conduct an investigation. The author has subsequently heard similar arguments in other venues around the world. Another one of the offered arguments is that civilians cannot handle dealing with images related to child sexual assault (child pornography), thus are unsuited for working as a computer forensics examiner in an LE environment. This particular discussion is beyond the scope of this paper, but speaks to the view of many within the digital forensics community.

As a discipline, digital forensics is young and still gaining acceptance by the larger forensic science community. The newness of the discipline is reflected, in part, by the lack of literature dedicated to computer forensics. The earliest journal devoted to this field was the *International Journal of Digital Evidence*, which started only in 2002 (and has not published an issue since 2007); today there are no more than a small handful of peer-reviewed journals specific to the discipline. Indeed, most of the journal articles have historically been written and reviewed by practitioners, with little (albeit growing) participation by the academic community. There have also been only a small number of published research studies related to computer forensics, and many papers based on anecdotes stand as the common wisdom in the discipline (Kessler, 2010).

In addition, digital forensics has only relatively recently been recognized as a forensic science by the academic and scientific communities. The earliest undergraduate degree programs in computer forensics did not appear in the U.S. until around 2003. Indeed, the discipline was only recognized as a forensic science by the American Academy of Forensic Sciences (AAFS) in 2008 and, even then, as Digital and Multimedia Sciences (AAFS, 2008).

Thus, there is a tiny body of literature about the *science* of digital forensics. Even though the Digital Forensics Research Workshop started in 2001, a true research agenda in digital forensics from the academic community did not start to appear until about 2008 (Beebe, 2009; Nance, Hay, & Bishop, 2009).

Most of the papers and by-products of research to date have been related to the technical aspects of computer forensics. And while there have been a few formal studies about practitioners, law enforcement officers, and prosecutors with respect to digital forensics, there have been none about judges (Losavio, Adams, & Rogers, 2006; Rogers, Scarborough, Frakes, & San Martin, 2007; Scarborough, Rogers, Frakes, & San Martin, 2009).

Judges and Digital Forensic Evidence

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 (Cohen, 2010; Jones, 2009; Kerr, 2009). For this reason, the author initiated a study focused on judges' awareness, knowledge, and perceptions of digital forensic evidence.

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, 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.

Searches conducted in 2008 and 2010 found that the literature is nearly silent on what judges know and how they perceive digital evidence because no publications have appeared focusing on judges in the U.S. and digital forensics (Losavio et al., 2006; Rogers et al., 2007; Scarborough et al., 2009). Several papers suggested that judges can be a difficult population from which to elicit information for several reasons (Mack & Anleu, 2008):

1. Their high social status, concerns about confidentiality, and professional aloofness
2. Reticence to participate in studies that might show areas in which they are intellectually weak
3. Lack of a priori relationship/trust with the researcher

The problem is somewhat exacerbated in the computer forensics space due to limited contact that many judges have with digital evidence in the first place (Rogers et al., 2007).

It is critical, however, that the knowledge, awareness, and perception of digital evidence by judges be understood because of the critical gatekeeper role that judges play. The *Daubert* (1993) and *Kumho Tire* (1999) decisions provide a standard by which scientific and technical evidence, respectively, should be reviewed by judges at the federal level (and about a third of the states). The four-pronged test to be applied to scientific and technical procedures asks:

1. Has the procedure been tested?
2. Has the procedure been described in a peer-reviewed publication?
3. Is there a known (or knowable) error rate?

4. Is the procedure generally accepted within the relevant scientific/technical community?

As it happens, police officers, lawyers, and prosecutors generally see more digital evidence than most judges because the majority of criminal and civil cases are resolved by plea agreements and settlements, respectively, rather than by going to trial. When digital evidence is challenged at trial, it is usually based on issues related to search, seizure, or relevance rather than on Daubert grounds so that judges have few technical decisions to make about digital evidence (i.e., judges deal primarily with questions of "was the seizure legal?" rather than "is the evidence authentic?") (Ball, 2008; Carlton, 2006; Casey, 2011; Rogers et al., 2007).

Judges need to make decisions about admissibility of an ever-increasing amount of digital evidence in terms of reliability, veracity, and accuracy. An understanding of judges' knowledge and awareness of digital evidence is important to both the integrity of the entire judicial process as well as to ensure that judges are appropriately prepared for this function.

OVERVIEW OF GROUNDED THEORY

Due to the lack of peer-reviewed publications related to judges and digital evidence, it was not possible to base a research study on a hypothesis derived from the literature. Instead, the author elected to use a qualitative research methodology called *grounded theory*. Grounded theory 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, Stevens, Troiano, & Schneider, 2002; Charmaz, 2006; Glaser & Strauss, 1967).

Grounded theory has been widely used in the social sciences since it was first described by Glaser and Strauss (1967). As practiced over the last 40 years, grounded theory studies provide an examination of individuals' response to various phenomena and provide a systematic, structured approach to qualitative research. Although initially designed for the social sciences, grounded theory has been applied for many years to studies related to information technologies (IT), ranging from software product development to the development of a business' IT strategy (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). In addition, grounded theory has already

been employed in one published study specifically focusing on digital forensics practitioners (Carlton, 2006, 2007).

Glaser and Strauss (1967) believed that people build structure through social processes; thus, even a technical topic such as the understanding digital forensic evidence would fall under their approach to research. Language is key to social interaction and responses emerge through action.

In a grounded theory-based research study, data gathering and data analysis occur simultaneously so that the researcher can identify trends. This iterative approach allows the researcher to categorize those trends, and more finely focus questions to further define and explore the trends. While several different approaches to grounded theory have been described over the years by a variety of researchers, all have the following elements in common (Brown et al., 2002; Charmaz, 2006; Leedy & Ormrod, 2010; Pogson et al., 2002; Schram, 2006):

- Data gathering and analysis occur in parallel, allowing themes to emerge
- Data gathering employs many types of instruments, such as surveys, interviews, and observation
- Analysis is performed by coding and categorizing responses
- An iterative approach to data gathering and analysis allows for the definition of the relationship between processes
- The results support the creation of a theoretical framework that defines the causes, actions, and effects of the processes

The phases of grounded theory research, as employed in this study, are (Charmaz, 2006; Leedy & Ormrod, 2010):

- *Data Collection:* Open-ended questions at first, more finely focused as themes emerge.
- *Note Taking:* Accurately reflect respondents' perspectives; note emerging themes and listen to participants. Although this phase is called note taking, it is best to gather transcripts of conversations or as much detail as possible rather than relying on simple notes.
- *Coding:* A multi-pass process to detect themes and compare respondents' statements, and to define categories and concepts. This is the phase of the study when the researcher is forming ideas and theories and must take great care to follow -- rather than lead -- the data.
- *Memoing:* Organize trends to define categories and relationships.

It is of critical importance to the integrity of the study that the researcher set aside his or her own prejudices and biases. Every person, of course, has his/her own cultural, temporal, and social context and perspectives; it is important to identify those up-front, acknowledge them, and then attempt to put them aside. 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).

RESEARCH METHODOLOGY

This section and the remainder of the paper summarize the study's methodology, findings, and recommendations (Kessler, 2010). The research study was performed in three phases (Figure 1):

- *Phase 1 Data Gathering:* Distribute initial survey to judges via national judicial organizations. This survey provided initial information about trends, attitudes, experiences, and base knowledge, and informed the researcher for the next phase of data gathering.
- *Phase 2 Data Gathering:* Individual face-to-face interviews with a group of judges in New England.
- *Output:* Based upon the data, propose a framework for judicial training and education related to digital forensic evidence.

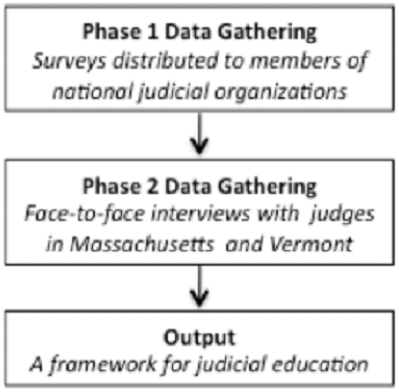

Figure 1. Phases of this research study.

It is important to note that, as a qualitative rather than quantitative study, statistical sampling is not a goal. It is sufficient that the researcher chooses survey and interview subjects that appear to be reasonably representative of the population being studied because this type of study is primary about generating

theory. Hypotheses based upon this new data can be studied in subsequent quantitative research (Charmaz, 2006; Leedy & Ormrod, 2010).

The author started discussions with several national organizations of judges in November 2008 for the purposes of gathering initial survey data. Contacts were made with individuals associated with the organizations' training function; in most cases, these individuals were judges. Although the organizations" leadership were generally supportive of the goals of the research, many concerns were expressed about the author actually obtaining data from their population. Concerns were raised that:

- The research was not sponsored by the organization itself
- The researcher might be biased and have an axe to grind
- The results might show the judges in a bad light

In the spring of 2009, the American Bar Association/Judicial Division (ABA/JD) gave the author permission to survey their membership. Initially, the author was invited to the annual meeting of the ABA/JD to be held that summer, with the goal of distributing the survey in person. The ABA/JD leadership also put a notice in their newsletter, along with a link to the author's Web site from where individuals could download the survey and mail it to the author (ABA, 2009). The National Judicial College (NJC) soon thereafter agreed to distribute a copy of the survey to their membership via e-mail.

The initial plan by the author was to conduct two or three rounds of written surveys, with each survey defining more finely focused questions than the last. To aid in the development of the surveys and to provide advice for the research, the author assembled an advisory board of 10 individuals, five of whom are long-time digital forensics practitioners and five of whom are attorneys with cybercrime and computer forensics expertise. Based upon the advice of the advisory board, the grounded theory literature, and the ABA/JD leadership, the survey was short, with a target time to complete of 20 minutes.

The initial research plan was to ask respondents to each survey whether they would participate in the next survey round, with a maximum of three rounds, so that the same set (or subset) of participants would be responding to increasingly focused survey questions. Given the likelihood of a decreased response with each survey round, the target was to obtain 50-100 responses to the initial survey.

PHASE 1 DATA GATHERING

The initial written survey was distributed in person at the ABA/JD Annual Meeting in July/August, 2009. The survey was then distributed on the ABA/JD via e-mail in August, 2009. Later that month, the NJC sent a link to the author's Survey Web site via their email list. The survey period extended until mid-

October, 2009.

The initial survey asked judges to comment on the following open-ended questions:

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, information and communication technologies (ICT), 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?

The first survey garnered 18 responses, which was disappointingly low, both to the author and the leadership of both the ABA/JD and NJC. Nevertheless, valuable information was elicited from these responses so that themes emerged, including observations that:

- Authentication of digital evidence is required as with other types of evidence, although that authentication requires different means than more traditional types of evidence
- Judges, particularly those that preside at trial, require additional expertise related to digital forensic evidence
- Judges, like most other people, learn about computer forensics, computers, the Internet, etc. based upon their own knowledge and use of technology, consistent with constructivist learning theories
- Judges do not get enough training about computers and digital forensics

The themes that emerged from the survey triangulated with the responses from Advisory Board. For that reason, the author felt confident that the results of the

written survey could be used to create questions for the next round of data gathering.

PHASE 2 DATA GATHERING

The initial surveys identified themes worth exploring but the number of responses to the survey was insufficient for additional rounds. The author then decided to change from written surveys to face-to-face interviews for the second phase of data gathering.

Because the initial survey did not elicit any responses from federal judges, the interviews also targeted state-level judges. The data-gathering plan was amended to interview judges in New England rather than attempt to distribute surveys to a national body of judges.

The author was introduced through intermediaries to four Vermont and three Massachusetts judges willing to participate in the research. As is typical throughout the country, both states have two levels of court, namely *trial* (aka district or superior courts) and *appellate* (aka appeals or supreme courts) (Figure 2).

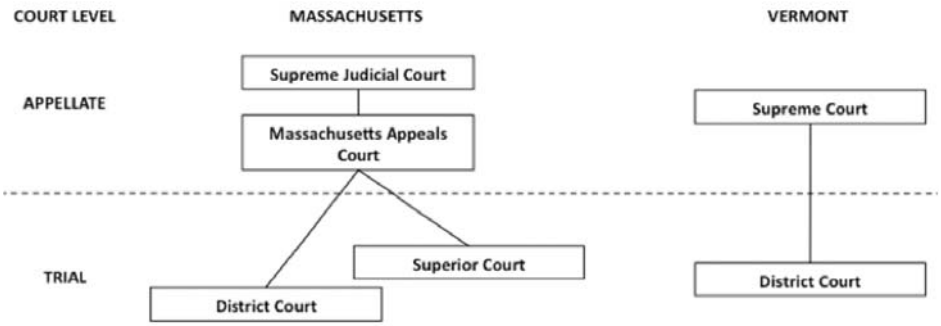

Figure 2. Criminal court levels in Massachusetts and Vermont.

The interviews with the judges took place in January and March, 2010. Interviews were taped and transcribed in order to minimize losing thoughts stated by the interviewees, losing the speaker's actual words, and introducing researcher bias when notes are taken. Because the set of questions were proscribed due to the Institutional Review Board (IRB) process -- which is at odds with the grounded theory method of allowing the conversation to go where the data leads -- interviewees were encouraged to tell stories in answer to the questions and elaborate as much as they wanted.

The interviewees were asked a number of questions, including:

1. What methods do 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? Do you feel that you have a good understanding, or could explain, the process by which e-mail moves across the Internet, in which Web pages are accessed via a browser, and the operation of the Internet?
2. Have you considered hiring, or have you actually hired, a digital forensics expert as a consultant to the court, independent of any experts hired by the parties to the trial case. What were the factors that prompted you to consider or hire such an expert?
3. How have you obtained the knowledge that you use to apply to the evaluation of digital forensics evidence, and how do you maintain currency with the technology and law? What kind of direct experiences and/or specialized education or training do you have related to computers, networks, technology, and digital forensic evidence?
4. What types of additional knowledge related to information technology and digital forensic evidence would help you on the bench?
5. Describe your own use of e-mail, the World Wide Web, and/or other Internet services (e.g., news services, chat rooms, instant messaging, e-mail, peer-to-peer services, social networks, online banking, online purchases).
6. Have your personal experiences with personal computer technology impacted your understanding of issues related to digital forensic evidence, and, if so, how?
7. What recommendations might you make to other judges to improve their own knowledge and awareness of digital forensic evidence?
8. What recommendations would you make for judicial education and training as it relates to digital forensic evidence?

The choice of interviewing three to four judges in two states is consistent with grounded theory's use of purposive sampling, meaning that subjects are selected that are, in the researcher's opinion, typical or otherwise of interest. Purposive sampling is not the same as statistically random sampling that might be used a typical quantitative study meant to describe a population (Charmaz, 2006; Leedy & Ormrod, 2010). In this case, the research was just trying to obtain data from which to draw some conclusions and provide a basis for future research.

Triangulation -- i.e., verifying the results using multiple sources -- is the method used in grounded theory to determine if the conclusions have any merit and provide that basis for future research. In this study, triangulation was accomplished by obtaining results via written surveys, interviews, and input from the advisory board to see where there were common suggestions of relationships.

Triangulation was the primary method of ensuring validity of the study's results.

Validity, in this context, refers to the ability of the researcher to state with some level of certainty that the study results accurately reflect the relationships being investigated. Internal validity refers to whether the results accurately represent the participants' viewpoints, which is accomplished by the use of multiple participants and multiple information gathering instruments. External validity refers to the generalizability of the results; the results found here may well be common only to Massachusetts and Vermont, or only to state-level judges. Construct validity addresses the correctness of the relationships (Charmaz, 2006; Leedy & Ormrod, 2010).

FINDINGS

The research 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.

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 computer users as a whole.

Judges generally recognize that 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.

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.

Judges noted that their role is to be moderators of a fair process, not advocates for one side or the other. Therefore, they observed, it is the role of attorneys, not judges, to mount challenges to 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 -- and the fact that judges cannot do their own independent research about matters before the bench. Some previous studies have suggested that attorneys do not believe that judges are as aware of digital evidence as attorneys

(Rogers et al., 2007; 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.

Indeed, digital evidence is likely to be admitted if the opposing 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 (Caloyannides, 2003; Van Buskirk & Liu, 2006).

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 technically 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. Interestingly, most 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.

The 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 in order to better understand the arguments presented by lawyers, testimony offered by technical witnesses, and basis of decisional law.

The findings were, in fact, much more detailed and nuanced than the scope of this paper allows. Interested readers are referred to the complete dissertation (Kessler, 2010).

RECOMMENDATIONS

One of the intended goals of the research was to propose a set of training topics that would address the gaps that judges identified in their knowledge of digital forensic evidence. Arthur C. Clarke is often quoted as observing that "[a]ny sufficiently advanced technology is indistinguishable from magic" (Moncur, 2007). In particular, use of ICT -- such as e-mail and Web browsing -- does not imply knowledge of the underlying technology. For that reason, one important

goal of any judicial education and training plan should be to remove the mystery about ICT.

It is also essential that such training be based upon principles of adult learning pedagogy, in particular (Phillips & Soltis, 2004):

- Active learning: Methods that allow the student to be actively engaged in the material to be learned by use of activities such as narration, project work, and hands-on activities.
- Problem-based, or project-based, learning: The use of real, relevant, and tangible problems rather than contrived assignments. Students will generally make real-world assumptions that come from their own environments in order to solve these problems, adding further relevance as they hone their problem-solving skills.
- Social constructivism: A learning theory that states that cognitive structures are the building blocks of learning and that learning is a social 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.

The focus of training to better prepare judges to better understand digital forensic evidence should focus on basic ICT and the computer forensics process. The intended bottom line is that judges better understand what digital forensic examiners can and cannot do, and about what digital forensics evidence can and cannot inform the Court. A suggested set of topics is provided below; while some of these topics might seem obvious to the digital forensics professional, these topics were derived from what the judges think they need to know:

1. *Basics of ICT:* Computers, hard drives, mobile devices, networks, the Internet, e-mail, the World Wide Web, social networks, other services and applications, voice/video over the Internet, 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; location of probative digital information in a residence or business; 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; mobile device forensics hardware and software; data carving;

metadata; 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, Zubulake guidelines, e-discovery software tools

CONCLUSION

The research study reported in this paper is the first published study in the U.S. to examine judges and digital forensics, thus opening up a new avenue of research. This is the second published digital forensics study that employs grounded theory, demonstrating the applicability of that research methodology to this discipline.

The proposed training and education plan is one that might better inform judges about the role of digital forensic evidence and examiners. It may also help in building trust by the community of judges in this discipline and its practitioners.

ACKNOWLEDGEMENTS

The author wishes to thank the leadership and members of the American Bar Association/Judicial Division and the National Judicial College for their participation in this study. The author is particularly indebted to the seven judges in Massachusetts and Vermont who willingly shared their time and expertise.

AUTHOR BIOGRAPHY

Gary C. Kessler is the president of Gary Kessler Associates, a training and consulting company specializing in computer and network security and digital forensics, and program director of the M.S. in Information Assurance program at Norwich University. He is also a member of the Vermont Internet Crimes Against Children (ICAC) Task Force and an adjunct associate professor at Edith Cowan University in Perth. Gary holds a Ph.D. in Computing Technology in Education, and is a Certified Computer Examiner (CCE) and Certified Information Systems Security Professional (CISSP).

REFERENCES

American Academy of Forensic Sciences (AAFS). (2008). *AAFS digital & multimedia sciences.* Retrieved June 13, 2011, from http://www.aafs.org/Digital-Multimedia-sciences

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

Ball, C. (2008). What judges should know about computer forensics. *National Workshop for District Judges II*. Retrieved June 13, 2011, from

http://www.craigball.com/ What_Judges_Computer_Forensics-200807.pdf

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.

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 June 13, 2011, 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. (2011). *Digital evidence and computer crime: Forensics science, computers and the Internet* (3rd ed.). Amsterdam, The Netherlands: Elsevier Academic Press.

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

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

Daubert v. Merrell Dow Pharmaceuticals, Inc. (92-102), 509 U.S. 579 (1993). Retrieved June 13, 2011, from http://www.law.cornell.edu/supct/html/92-102.ZO.html

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

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

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.

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 June 13, 2011, 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.

Kessler, G.C. (2010, September). *Judges' Awareness, Understanding, and Application of Digital Evidence*. Unpublished doctoral dissertation, Nova Southeastern University, Ft. Lauderdale, FL. Retrieved June 13, 2011, from http://www.garykessler.net/library /kessler_judges&de.pdf

Kumho Tire v. Carmichael (97-1709), 526 U.S. 137, 131 F.3d 1433 reversed (1999). Retrieved June 13, 2011, from http://supct.law.cornell.edu/supct/html/97-1709.ZS.html

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

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.

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

Moncur, M. (2010). *Quotation #776 from Michael Moncur's (cynical) quotations.* Retrieved June 13, 2011, from http://www.quotationspage.com/quote/776.html

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.

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*.

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.

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.

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

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

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