



May 31st, 3:20 PM

## Digital Evidence Education in Schools of Law


Aaron Alva

*Center for Information Assurance and Cybersecurity, University of Washington, aalva@uw.edu*

Barbara Endicott-Popovsky

*Center for Information Assurance and Cybersecurity, University of Washington, endicott@uw.edu*

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

---

### Scholarly Commons Citation

Alva, Aaron and Endicott-Popovsky, Barbara, "Digital Evidence Education in Schools of Law" (2012).

*Annual ADFSL Conference on Digital Forensics, Security and Law. 3.*

<https://commons.erau.edu/adfsl/2012/thursday/3>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact [commons@erau.edu](mailto:commons@erau.edu).

**EMBRY-RIDDLE**  
Aeronautical University™  
SCHOLARLY COMMONS

(c)ADFSL



## DIGITAL EVIDENCE EDUCATION IN SCHOOLS OF LAW

**Aaron Alva**

**Barbara Endicott-Popovsky**

Center for Information Assurance and Cybersecurity

University of Washington

4311 11th Ave NE Suite 400 Box 354985

Seattle, Washington 98105

aalva@uw.edu, endicott@uw.edu

### ABSTRACT

An examination of *State of Connecticut v. Julie Amero* provides insight into how a general lack of understanding of digital evidence can cause an innocent defendant to be wrongfully convicted. By contrast, the 101-page opinion in *Lorraine v. Markel American Insurance Co.* provides legal precedence and a detailed consideration for the admission of digital evidence. An analysis of both cases leads the authors to recommend additions to Law School curricula designed to raise the awareness of the legal community to ensure such travesties of justice, as in the Amero case, don't occur in the future. Work underway at the University of Washington designed to address this deficiency is discussed.

**Keywords:** digital forensics, law education, ESI, admissibility, evidence

### 1. INTRODUCTION / BACKGROUND

There is an alarming gap in the legal and judicial community's understanding of digital evidence. This was brought home vividly after one of the authors received a call from an attorney acquaintance seeking advice on a case involving incriminating emails that were pending admission as evidence in a contentious divorce case. The accused wife was an injured Iraqi War veteran whose husband sought dissolution, as well as all of the couple's assets and full custody of their children, based on her alleged crimes of cyber stalking. As evidence, the husband's lawyer provided paper copies to the judge of incriminating emails that did indeed appear to emanate from the wife's account. Without legal challenge, the judge was inclined to admit it. Endicott-Popovsky recommended that the related digital email files be requested from the husband's lawyer, who agreed to forward them immediately. Three weeks later, the digital email files still were not forthcoming and the lawyer--and his client--dropped the allegations against the wife of violation of Washington State's strict cyber stalking statutes and withdrew the "evidence" from the judge's consideration. You can draw your own conclusion why this "evidence," initially so compelling according to the other side, was quietly withdrawn.

This entire episode gave pause. Had the wife's attorney not known of one Author's interest in digital forensics, he might not have called. Had the judge then admitted the evidence proposed by the husband's counsel, a serious miscarriage of justice almost surely would have ensued. The tragedy of a veteran of active duty service, and a woman at that, officially being labeled a cyberstalker, stripped of her parental rights and losing her assets (not to mention the effect that this would have on the children) was chilling to contemplate and reminiscent of the Julie Amero case which has become a legend among digital forensics experts and which will be discussed in more detail later. Examination of additional cases confirms this experience, resulting in our recommendation that education in a range of subjects related to digital evidence be added to law school curricula where, unfortunately, today it often is not.

Failing to provide lawyers and judges with sufficient education in digital evidence can result in serious miscarriages of justice and disruption of the legal system. The innocent will be wrongly convicted and incarcerated; those deserving of punishment will get away with crimes. Society as a whole would be

better served by increasing the legal and judiciary communities' understanding of digital evidence (Endicott-Popovsky and Horowitz 2012). This will require that schools of law engage in an effort to identify what needs to be taught.

## 2. STATE OF CONNECTICUT V. JULIE AMERO

*State of Connecticut v. Julie Amero* exposed how legal ignorance of digital evidence could have a profound impact on an individual's life. Defendant, Amero was convicted on four charges of Risk of Injury to a Child, which carried up to a 40-year sentence (Kantor 2007). Following four delays in sentencing, a new trial was granted when the conviction was overturned on appeal. After years of suffering under a cloud of suspicion, wanting to put the nightmare behind her, Amero pled guilty to disorderly conduct, her teaching license was revoked, and she paid a \$100 fine (Krebs 2008).

To summarize the facts of the case, Julie Amero was substitute-teaching a seventh grade classroom on October 19, 2004. After stepping out of the hallway for a moment, she found two students browsing a hairstyling site. Shortly afterwards, the computer browser began continuously opening pop-ups with pornographic content. She was explicitly told not to turn off the computer, and was unaware that the monitor could be shut off. Students were exposed to the pornography. The primary evidence admitted by the court was the forensic duplicate of the hard drive on the computer in question. While the forensic investigator did not use industry standards to duplicate the hard drive, the information was used in the investigation (Eckelberry et al. 2007). The evidence purported to show Internet history of pornographic links that indicated the user deliberately went to those sites (Amero Trial Testimony 2007).

Later *pro bono* forensics experts for the defendant showed that antivirus definitions were not updated regularly and at the time were at least three months out-of-date. Additionally, no antispyware or client firewall was installed and the school's content filter had expired (Eckelberry et al. 2007).

### 2.1 Evaluation of digital evidence by Judge and attorneys

During the trial, the judge refused to allow full testimony from the defense expert witness Herb Horner, noting that the information was not made available beforehand. That information was relevant to gaining a full understanding of the digital evidence crucial to the case. The decision not to admit it indicates a troubling lack of understanding of the nature of digital evidence. Horner's evidence should have been provided to the jury (Amero Trial Testimony 2007).

Maintaining a digital chain of evidence is essential for admissibility of any digital evidence. In *State v. Amero*, this is questionable based on the uncertainty of the forensic duplicate process (Eckelberry et al. 2007). Additionally, timestamp differences between the e-mail server (the time authority in the school system's network), and the computer in question, as a witness stated, "was ten or twelve minutes. I don't remember who was faster and who was slower" (Amero Trial Testimony 2007). Both of these discrepancies should put into question the authenticity of the digital evidence, although neither arose as a strong defense argument. This indicates that the attorneys did not have sufficient technical knowledge to evaluate the evidence.

Further, the judge did not find relevant the preparations taken by one expert witness to examine the hard drive forensically. This is necessary to provide foundation for admissibility and authenticity of digital evidence (Amero Trial Testimony 2007). The defense attorney did not question authenticity based on the time stamp differences between PC and server, nor did the defense make an argument regarding the process of the forensic investigation. Similarly, the prosecution did not have a proper understanding of how to show the digital evidence in ways consistent with the actual event, as seen by their display of full size pornographic pictures instead of thumbnails.

On the basis of the transcript of the case, the questions attorneys asked (or did not ask) of witnesses also indicated low computer literacy. While expert witnesses are important to the case, the technical knowledge of the attorneys (with the judge's permission) guided the questioning of the witnesses.

The prosecuting attorney, when questioning the defense expert witness, apparently did not understand the information being provided. A lack of understanding on the attorney's part resulted in a lack of precision in direct questioning that could have elicited more meaningful answers from the witness. The following dialogue between the prosecuting attorney (questioning) and the defense expert witness is an example:

Q So in order for it to show up on the temporary Internet files, that person would have to actively go to that site, correct? They were not redirected to that site, correct?

A Wrong.

Q Okay.

A You don't understand.

Q I hear you saying that. Give me more questions. (Amero Trial Testimony 2007)

One line of questioning by the defense regarded computer functions related to the Internet, adware, spyware, and viruses (Amero Trial Testimony 2007). Cross-examination containing phrases such as 'parasites' and other incompetent questioning further displayed a low level of computer literacy from attorneys on both sides. When the prosecutor displayed full-size pornographic pictures in the courtroom, the defense did not argue, as it should have, that the relative size of the pictures displayed for the jury was not consistent with the pop-up size thumbnails displayed in the classroom. The lack of a specific argument by the defense against using a full size display in the courtroom contributed to a false impression that prejudiced the jury (Willard 2007).

## **2.2 Expert witness testimony**

The following section will detail the expert witness testimony in the Julie Amero case.

### **2.2.1 Bob Hartz, IT Manager**

This case heard several expert witnesses, each of whom provided information that proved to be misleading. The jury heard testimony from Bob Hartz, IT Manager for the Norwich Public Schools first. Hartz's testimony provided information on server logs that provided a history of sites accessed from the computer in question. His testimony also provided a basic understanding of the computer environment at the School district, including notice that the timestamps between server/firewall logs and the computer were either 10-12 minutes ahead or behind. Additionally, he testified that the content filtering was not working, as it "had not been updated correctly" (Amero Trial Testimony 2007).

During Hartz's testimony, he was asked a series of questions regarding the possibility of certain events occurring, based on his 20-plus years of experience in the field. His answers provided misleading information. When asked if it were possible to be in an 'endless loop of pornography,' referring to the continual pornographic popups, Hartz stated, "I've never seen that, so I would have to say probably not" (Amero Trial Testimony 2007). Additionally, when asked whether spyware and adware generates pornography, Hartz replied, "I'm not aware they do" (Amero Trial Testimony 2007). Both of these replies were speculative and should have been challenged, along with his experience to respond competently to questions involving malicious activity on the Internet.

### **2.2.1 Detective Mark Lounsbury**

Detective Mark Lounsbury, the computer crimes officer for the Norwich Police Department, was the officer who personally copied and examined the hard drive. From testimony given by Lounsbury, it appears that he may have investigated the original hard drive rather than the copy he claimed to have made. Best practice is to preserve the original hard drive for evidentiary purposes, and to perform the investigation on the forensic duplicate (Noblett, Pollitt, et al. 2000). Any digital forensic expert should know that direct access to the hard drive, including opening files, will alter the files from the original state—which in turn alters the evidence.

Another revealing insight into the incompetence of Lounsbury's hard drive examination was revealed in his answer to the question, "Did you examine the hard drive for spyware, adware, viruses or parasites?" (Amero Trial Testimony 2007) He responded that he had not. Digital forensics best practices include examination for event correlation that searches for causes of activities in question (NIST 800-61 2008). It is safe to say that poor examination procedures, led to missed findings that were directly relevant to the case.

### 2.2.2 Herb Horner, defense expert witness

Herb Horner, a self-employed computer consultant, was called in by the defense as an expert witness. Horner obtained the hard drive copy from the police, and then created copies for his investigation. Horner's testimony was cut short by the judge's decision not to continue with information that was not provided beforehand to the prosecution. Horner later stated, "This was one of the most frustrating experiences of my career, knowing full well that the person is innocent and not being allowed to provide logical proof. If there is an appeal and the defense is allowed to show the entire results of the forensic examination in front of experienced computer people, including a computer literate judge and prosecutor, Julie Amero will walk out the court room as a free person." (Kantor 2007). The information that was to be presented by Horner was evidence of spyware on the computer, which was caused pornographic pop-ups (Amero Trial Testimony 2007). As Horner stated to the judge while the jury was dismissed, "there were things done before the 19th that led to this catastrophe, and this is a fact" (Amero Trial Testimony 2007). Despite this, evidence that spyware caused the pop-ups still was not allowed into the record.

## 2.3 Legal results

Legal precedence cited in *State v. Amero* was limited. There was one mention of *U.S. v. Frye* during an objection to the admissibility of expert testimony by Hartz on the basis that he did not lay proper foundation for his testimony (Amero Trial Testimony 2007). The prosecution argued that the Hartz's expertise was based on his described twenty years of experience, and the judge found this sufficient (Amero Trial Testimony 2007).

During the same exchange, the defense cited *State v. Porter* to argue that the reliability of scientific information was a major issue. In *State v. Porter*, the Connecticut Supreme Court adopted the Federal standard set by *U.S. v. Daubert*, however, questioning continued due to lack of clarity on what the defense was objecting to specifically (Amero Trial Testimony 2007).

The primary law cited in this case was risk of injury to a minor, Connecticut General Statute Section 53-21(a)(1), from which the charges stemmed. There were no laws or regulations cited relevant to digital evidence admissibility.

The defendant was found guilty on four counts of Risk of Injury to a Child, with the possibility of a 40-year prison sentence. After four delays in sentencing, the State Court of Appeals reversed the lower court decision and a motion for a new trial was accepted. She pled guilty to a misdemeanor to get the nightmare behind her. As part of the deal, she agreed to have her teaching license revoked. The emotional toll on her and her family was extreme, and the stress of trial resulted in many health problems. She has become a *cause celebre* for digital forensics experts ever since.

## 3. LORRIANE V. MARKEL AM. INS. CO.

There are a few examples where the justice system has properly handled the admission of digital evidence. We transition from an example of glaring misunderstandings and lack of knowledge of digital evidence (Amero case), to an analysis of a competent judicial opinion regarding digital evidence, the case of *Lorriane v. Markel American Insurance Company*. The opinion proceeding from the ruling made by Chief United States Magistrate Judge Paul W. Grimm has set major legal precedence (*Lorraine v. Markel Am.* 2007). The case arose from an insurance payment dispute. The actual facts of the case are not important; the opinion of Judge Grimm is. It provides a detailed

procedure for admitting digital evidence. The following section will summarize each step and requirement of the process.

### 3.1 Digital evidence admissibility process

The first criteria for gauging admissibility of digital evidence is based on Federal Rules of Evidence Rule 104. Judge Grimm explained that determining the authenticity of Electronically Stored Information (ESI) is a two-step process (*Lorraine v. Markel Am. 2007*). First,

“...before admitting evidence for consideration by the jury, the district court must determine whether its proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic” (*Lorraine v. Markel Am.* quoting *U.S. v. Branch*).

Secondly,

“...because authentication is essentially a question of conditional relevancy, the jury ultimately resolves whether evidence admitted for its consideration is that which the proponent claims” (*Lorraine v. Markel Am.* quoting *U.S. v. Branch*).

Relevance is the first requirement for admissibility of evidence (Fed. R. Evid. 401). Evidence is sufficient, in terms of relevance, if it has “...any tendency’ to prove or disprove a consequential fact in litigation” (*Lorraine v. Markel Am. 2007*). Of importance, if evidence is not relevant, it is never admissible according to Fed. R. Evid 402. In terms of the case at hand, Lorraine, the emails were determined to be relevant to the case (*Lorraine v. Markel Am. 2007*).

The next step in determining admissibility of ESI is its authenticity as guided by Federal Rules of Evidence 901 and 902. Judge Grimm submits that the authenticity of digital evidence is an important requirement, and that the degree of admissibility only need be sufficient in terms of showing the evidence is what it is purported to be (*Lorraine v. Markel Am. 2007*). Specifically, the non-exclusive examples provided by Rule 901(b) can be studied to know how to address authentication of ESI in Rule 901(a) (*Lorraine v. Markel Am. 2007*).

Federal Rules of Evidence 902 shows twelve non-exclusive methods that can be used for ‘self-authentication’ of digital evidence (*Lorraine v. Markel Am. 2007*):

- (1) Domestic Public Documents That Are Sealed and Signed.
- (2) Domestic Public Documents That Are Not Sealed but Are Signed and Certified.
- (3) Foreign Public Documents.
- (4) Certified Copies of Public Records.
- (5) Official Publications.
- (6) Newspapers and Periodicals
- (7) Trade Inscriptions and the Like.
- (8) Acknowledged Documents.
- (9) Commercial Paper and Related Documents.
- (10) Presumptions Under a Federal Statute.
- (11) Certified Domestic Records of a Regularly Conducted Activity.
- (12) Certified Foreign Records of a Regularly Conducted Activity.

These methods establish a practice of authentication that can be performed without the need for expert witness testimony, although the lack of such testimony does not exempt evidence of authentication from challenge (*Lorraine v. Markel Am. 2007*; Fed. R. Evid. 902).

Procedurally, evidence that is already deemed relevant and authentic must also withstand any argument of hearsay. Rule 801 governs hearsay, and states that electronic writings or other information generated entirely by a “computerized system or process” is not made by a person, and

therefore cannot be considered hearsay (*Lorraine v. Markel Am.*, 2007). There are exemptions to the hearsay rule within the Federal Rules of Evidence, which Judge Grimm linked to ESI in his opinion. These included Fed. R. Evid. 803(1-3, 6, 7, 17) (*Lorraine v. Markel Am.* 2007).

The Original Writing Rule is considered the next hurdle for electronic evidence admissibility, which is included in Federal Rules of Evidence 1001-1008. Rule 1002 ensures the ‘best evidence’ available and applies when a “writing, recording or photograph is being introduced to ‘prove the context of a writing, recording or paragraph’” (Fed. R. Evid. 1002). Rule 1003 states that duplicates of evidence can be admitted in place of originals unless the authenticity of the original is in question (*Lorraine v. Markel Am.* 2007). In determining whether secondary evidence can be included in place of an original, Rule 1004 provides guidance.

The summary of the guidelines from the Federal Rules of Evidence cited in the Lorraine opinion follows:

Table 1: Rules of Evidence Identified in *Lorraine v. Markel* as Guidance for Digital Evidence Admissibility

<i>Legal Guidance</i>	<i>Subject</i>
Federal Rules of Evidence 104(a)	Preliminary Questions; relationship between judge and jury
Federal Rules of Evidence 104(b)	
Federal Rules of Evidence 401	Relevance
Federal Rules of Evidence 402	
Federal Rules of Evidence 901	Authenticity; including examples of how to authenticate
Federal Rules of Evidence 902	Self-Authentication; including examples
Federal Rules of Evidence 801	Hearsay; including exceptions to the hearsay
Federal Rules of Evidence 803	
Federal Rules of Evidence 804	
Federal Rules of Evidence 807	
Federal Rules of Evidence 1001 through 1008	
Federal Rules of Evidence 403	Balance of Probative Value with Unfair Prejudice

(*Lorraine v. Markel Am.* 2007; LexisNexis 2007)

### 3.2 Applicability to State of Connecticut v. Julie Amero

The next section applies, retrospectively, digital forensic guidelines established in *Lorraine v. Markel* to *State of Connecticut v. Julie Amero* to determine whether this would have resulted in a different outcome. As a note, the trial portion of the *Amero* case preceded the *Lorraine v. Markel Am.* opinion by four months in 2007. While *Amero* could not have capitalized on the *Lorraine* opinion, an analysis helps identify knowledge the legal participants in *Amero* should have had to ensure the case was properly adjudicated.

## 4. ANALYSIS

### 4.1 Digital evidence admitted

The primary piece of digital evidence in the Amero case was the hard drive. The opinion of Judge Grimm includes methods describing how to handle the admissibility of this type of evidence (Section 4.5).

### 4.2 Evaluation of digital evidence by Judge and attorney

*State v. Amero* is an appalling example of the blindness of the legal system when computer literacy of the judge and lawyers is at the very low end of the spectrum. The proceedings of this case highlight the need for even the most basic understanding of how computers operate, including the threats to computer systems that can cause the pop-up symptoms argued by the defense. In *State v. Amero*, the lawyers did not question the authenticity of expert testimony describing the behaviors of viruses and spyware. Of more importance, the lawyers did not put forth a clear and full objection to the digital evidence presented. The *Lorraine v. Markel Am.* opinion specifically states that the burden of ensuring that digital evidence is what it purports to be depends largely on objections by opposing counsel. Thus, it is the responsibility of lawyers to be sufficiently knowledgeable to object competently to faulty evidence.

### 4.3 Expert and witness testimony

*Amero* provided an example of the affects expert testimony can have on a case. The numerous errors of so-called experts swayed the outcome of this case, and further exposed the lack of basic computer literacy among the professional legal participants. The opinion rendered in *Lorraine v. Markel Am.* references examples provided by Fed. R. Evid. 901 as methods to authenticate digital evidence, including the call for an expert witness. Laying proper foundation qualifying the expert witness, as well as directing a competent line of questioning, rely heavily on the computer literacy of the lawyers involved. Reliance on digital forensic “expert” witnesses was key to *State v. Amero*, although the line between testimony and speculation was crossed. An objection to speculation as to whether spyware could produce pop-up pornography would have been warranted, given that opposing counsel had some knowledge of computer threats.

### 4.4 Legal precedence

Legal precedence is scarce in the area of digital evidence, although it is building. Some cases establish sound precedence, as indicated in *Lorraine*. While *Daubert* and *Frye* have established general guidance for admission of scientific evidence, the science of digital forensics is new and evolving (*Daubert v. Merrell Dow* 1993; *Frye v. U.S.* 1923). The speed of technological change is at odds with the time it takes for legal precedence to accumulate. This impacts every court case involving a computer, and hardly any don’t—whether we’re talking civil cases, such as divorces, or criminal cases where digital evidence plays a significant role. The legal system lags in handling digital evidence adequately (Endicott, Chee, et. al. 2007). In *State v. Amero*, *Frye* and *Daubert* were cited in an objection by the defense, yet neither was applied appropriately. In order to build an adequate digital evidence curriculum for law schools, extensive review of relevant legal cases will be required. This is a matter for future research.

### 4.5 Laws and regulations identified

In *Amero*, first the court should have determined whether a satisfactory foundation had been laid before the jury viewed the evidence (*United States v. Branch* 1992; Fed. R. Evid. 104). Then relevance should have been considered (Fed. R. Evid. 401 and 402), then authenticity guided by Fed. R. Evid. 901 and 902. Application of the hearsay Rules (Fed. R. Evid. 801-807) and the Original Writing Rule (Fed. R. Evid. 1001-1008) would follow in order to fully ensure the evidence, and duplicates of the evidence, were what they purported to be (*Lorraine v. Markel* 2007).



#### 4.6 Legal Result

What is missing from most analyses of the *Amero* case is the larger picture of the emotional and health effects on the innocent. Julie Amero, who faced forty years in jail, went through tremendous emotional stress, and had a series of health issues arise including a tragic miscarriage (Cringly 2008). Her family relationships were also impacted. While the legal system eventually righted the wrong inflicted on Amero, the accumulated health and personal impacts cannot be undone. This will be repeated again and again until we have a more predictable legal system when it comes to the use of digital evidence. The contribution by Judge Paul W. Grimm's opinion in *Lorraine v. Markel Am.* provides the basis for guidance in this area. There are others emerging, but scant few.

#### 5. COMPUTER AND DIGITAL FORENSICS EDUCATION RECOMMENDATIONS

*State v. Amero* and *Lorraine v. Markel Am.* provide a basis for recommending digital evidence educational requirements in schools of law. The following recommendations will inform future curricula for the University of Washington's School of Law, and may be useful to others that wish to mitigate deficiencies in computer knowledge of lawyers and the judiciary. At a minimum, the curriculum must include:

- **Basic computer literacy.** This includes an understanding of computer vulnerabilities. A basic understanding that a compromised computer may show erratic actions not performed (or intended) by the user is important and would have prevented the Amero tragedy. This knowledge will enable lawyers to establish proper foundation and a proper line of questioning.
- **Understanding of the digital forensics process.** This includes basic knowledge of how easily digital evidence can be altered and what it means to have a proper chain of evidence, including storage and control. In addition, there should be sufficient knowledge of how evidence is collected on a computer hard drive (and on a network), how a hard drive is appropriately duplicated for forensic purposes, and then searched by forensic tools. This recommendation arises from the several glaring errors in the *Amero* case. It was never established that proper steps were taken to maintain a proper chain of evidence during forensic duplication and investigation (*State v. Amero* 2008). Additionally, the lack of a search for malware by police initially missed crucial evidence.
- **Knowledge of the Federal Rules of Evidence, and how they apply to electronic evidence.** The Federal Rules of Evidence are integral to understanding the process for admitting digital evidence. *Lorraine v. Markel Am. Insurance Co.* provides a framework for applying these rules to digital evidence. Fed. R. Evid. 901 and 902 specifically deal with authentication of digital evidence, including examples of how to do so. This is directly relevant to the *Amero* case; abiding by this framework would have provided a basis for questioning whether the digital chain of evidence was reliable, and not broken, during the investigatory process.
- **Survey of case law.** A thorough search for relevant cases and an extraction of precedence should be conducted before developing digital forensics curriculum. Knowledge of how to apply the Federal Rules of Evidence as well as *Daubert* and *Frye* in cases involving digital evidence will provide material for any classes developed (*Daubert v. Merrell Dow* 1993; *Frye v. U.S.* 1923). A thorough survey of other cases will provide and even more comprehensive understanding of the state of the practice regarding digital evidence. *Lorraine v. Markel Am.* emphasizes that the

burden of ensuring digital evidence admissibility rests largely on objections to such evidence by opposing counsel. The inability to competently challenge testimony of the State's 'expert' witness led to a travesty of justice in the Amero case.

## **6. CONCLUSIONS**

The above review provides insights into the legal and judicial communities' lack of sufficient knowledge of how to handle digital evidence appropriately and consistently. The authors believe this argues for additional curriculum in schools of law that educate law students in the challenges of digital evidence: digital evidence collection, chain of custody, the challenges of cybersecurity, basic computer literacy. The authors recommend that law schools consider adding courses in these subjects as they relate to digital evidence. A previously published digital forensics course conducted at the University of Washington for a combined audience of technical and law students, is an example of what can be accomplished with a collaboration between digital forensics/computer science and law faculty. Based on a successfully and competently prosecuted case of online digital theft and compromise, the course culminates in a moot court that requires law students to participate in the preparation and questioning of digital forensics experts (computer science students taking the same course) (Endicott-Popovsky, Frincke, et al. 2004). This is just the beginning of innovations that the authors recommend be incorporated into legal education and training.

## **7. FUTURE WORK**

Future work will involve researching existing case law in order to assist the University of Washington's School of Law, in partnership with the Information School, in revamping their curriculum to include interdisciplinary courses that will improve digital evidence literacy among law students. It is expected that a thorough analysis of cases where digital evidence has been inappropriately handled will further refine recommendations for curriculum content made above. Work on this project has begun, with preliminary findings discussed in this paper. Insights of a thorough examination of case law will be disseminated broadly to the digital forensics community.

## **AUTHOR BIOGRAPHIES**

Aaron Alva is a candidate of the Masters of Science in Information Management program and an upcoming candidate, Juris Doctorate at the University of Washington. He earned his Bachelor degree at the University of Central Florida studying political science with a minor in digital forensics (2011). His interests are in cybersecurity law and policy creation, particularly digital evidence admissibility in U.S. courts. He is a current recipient of the National Science Foundation Federal Cyber Service: Scholarship For Service.

Barbara Endicott-Popovsky, Ph.D., Director for the Center of Information Assurance and Cybersecurity at the University of Washington, holds a joint faculty appointment with the Information School and Masters in Strategic Planning for Critical Infrastructure, following a 20-year industry career marked by executive and consulting roles in IT and project management. Her research interests include forensic-ready networks and the science of digital forensics. She earned her Ph.D. in Computer Science/Computer Security from the University of Idaho (2007), and holds an MS in Information Systems Engineering from Seattle Pacific University (1987), an MBA from the University of Washington (1985).

## **REFERENCES**

Connecticut General Statute Section 53-21(a)(1)

Cringley, Robert (2008), 'The Julie Amero Case: A Dangerous Farce', [http://www.pcworld.com/businesscenter/article/154768/the\\_julie\\_amer0\\_case\\_a\\_dangerous\\_farce.html](http://www.pcworld.com/businesscenter/article/154768/the_julie_amer0_case_a_dangerous_farce.html), *PC World*, December 2, 2008.

Daubert v. Merrell Dow Pharmaceuticals, Inc., 113 S. Ct. 2786. (1993).

- Eckelberry, Alex; Glenn Dardick; Joel Folkerts; Alex Shipp; Eric Sites; Joe Stewart; Robin Stuart (2007), 'Technical review of the Trial Testimony State of Connecticut vs. Julie Amero', Technical Report, <http://www.sunbelt-software.com/ihs/alex/julieamerosummary.pdf>, March 21, 2007.
- Endicott-Popovsky, B. and Horowitz, D. (2012). Unintended consequences: Digital evidence in our legal system. *IEEE Security and Privacy*. (TBD) (Endicott-Popovsky and Horowitz, 2012)
- Endicott-Popovsky, B., Chee, B., & Frincke, D. A. (2007). "Calibration Testing Of Network Tap Devices", *IFIP International Conference on Digital Forensics*, 3–19.
- Endicott-Popovsky, B.E., Frincke, D., Popovsky, V.M. (2004), "Designing A Computer Forensics Course For an Information Assurance Track," Proceedings of CISSE 8th Annual Colloquium.
- Fed. R. Evid. 104, 401-402, 801-807, 901-902, 1001-1008
- Frye v. United States. 293 F. 1013 D.C. Cir. (1923).
- Kantor, Andrew (2007), 'Police, school get failing grade in sad case of Julie Amero', *USA Today* [http://www.usatoday.com/tech/columnist/andrewkantor/2007-02-22-julie-amero\\_x.htm](http://www.usatoday.com/tech/columnist/andrewkantor/2007-02-22-julie-amero_x.htm), February 25, 2007.
- Krebs, Brian (2008), 'Felony Spyware/Porn Charges Against Teacher Dropped', *Washington Post*, [http://voices.washingtonpost.com/securityfix/2008/11/ct\\_drops\\_felony\\_spywareporn\\_ch.html?nav=rss\\_blog](http://voices.washingtonpost.com/securityfix/2008/11/ct_drops_felony_spywareporn_ch.html?nav=rss_blog), November 24, 2008.
- LexisNexis (2007), 'Lorraine v. Markel: Electronic Evidence 101', [http://www.lexisnexis.com/applieddiscovery/LawLibrary/whitePapers/ADI\\_WP\\_LorraineVMarkel.pdf](http://www.lexisnexis.com/applieddiscovery/LawLibrary/whitePapers/ADI_WP_LorraineVMarkel.pdf) Accessed February 1, 2012.
- Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 D.Md (2007).
- NIST 800-61 Rev. 1 (2008), "Computer Security Incident Handling Guide", *National Institute of Standards and Technology*, <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>, March 2008.
- Noblett, M.G., Pollitt, M. M., & Presley, L. A. (2000). 'Recovering and Examining Computer Forensic Evidence' *Forensic Science Communications*, 2(4). <http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm>, October 2000.
- State of Connecticut v. Christian E. Porter, 241 Conn. 57, 698 A.2d 739, (1997).
- State of Connecticut v. Julie Amero Trial Testimony, (2007), Retrieved from <http://drumsnwhistles.com/pdf/amero-text.zip>, January 3-5, 2007.
- State of Connecticut v. Julie Amero, (2008).
- United States v. Branch, 970 F.2d 1368 4th Cir. (1992)
- Willard, Nancy (2007), 'The Julie Amero Tragedy', Center for Safe and Responsible Use of the Internet, <http://csriu.org/onlinedocs/AmeroTragedy.pdf>, February, 2007.