Legal Aspects of Digital Forensics: A Research Agenda

Kara Nance
Department of Computer Science
University of Alaska Fairbanks
klnance@alaska.edu

Daniel J. Ryan
Information Operations & Information Assurance Dept.,
iCollege of the National Defense University
ryand@ndu.edu

Abstract

The evolution of the Information Age has necessitated and facilitated the relatively new field of digital forensics. As a largely practitioner-driven field, there is no clearly defined research agenda to promote top-down research in related areas so that the evolution can be more solidly based on research findings. This paper builds on previously published topical research agendas for digital forensics and introduces a preliminary research hierarchy for legal issues associated with digital forensics. Topics discussed include constitutional law, property law, contract law, tort law, cybercrime, criminal procedure, evidence law, and cyber war. In addition some special associated problems and overarching areas are identified for consideration and for future research.

1. Introduction

The field of digital forensics presents many challenges, including the development of associated research agendas. "Digital evidence has undergone a rapid maturation process. This discipline did not start in forensic laboratories. Instead, computers taken as evidence were studied by police officers and detectives who had some interest or expertise in computers." [1] Thus, historically, the field has been practitioner-driven with contributions being made by creative professionals in the field out of necessity rather than by following a carefully orchestrated and thorough research and development plan. The evolution of digital forensics has been further complicated by the rapid evolution and widespread application of a wide-range of information technologies that have played an increasing role in associated legal cases. While traditional computers and floppy disks may previously have provided the digital evidence, today digital and multimedia evidence can be found in a wide range of devices that can help recreate an event, including laptops, netbooks, cell phones, facsimile machines, printers, thumb drives, iPods, and a continually expanding plethora of other devices. Sewing machines incorporate computers to enable fancy stitching [2], refrigerators have computers to facilitate shopping [3], supervisory control and data acquisition systems manage industrial processes [4], automobiles use computers to provide sophisticated engine controls to meet emissions and fuel-economy standards [5], and the list grows daily.

The issues associated in keeping up with the rapid technological advances have presented significant challenges in legal and regulatory areas. In order to begin to meet these challenges, research into the coupling between digital forensics and the effects of rapid information technology evolution on the legal field is important. This symbiotic relationship presents an opportunity for proactive investigation and development of a solid research foundation, which can then be applied to ensure that the concepts are well understood and that there is body of knowledge that facilitates the further evolution of appropriate laws and policy.

2. Background

Previous works have identified research agendas for virtualization in digital forensics [6], education in digital forensics [7], and general digital forensics. [8] For each of the previous topics, a top-down approach was used to develop a hierarchy of research topics that could be used to help identify research needs in this challenging area. The legal arena is more complex than many of the other areas that are tightly coupled with digital forensics, due to the strict admissibility requirements for scientific and technical evidence. To be admissible, digital evidence must, of course, be relevant, material and competent. The application of Federal Rule of Evidence 702 through such cases as *Daubert v. Merrell-Dow Pharmaceuticals*, [9] *General Electric Co. v. Joiner,* [10] and *Kumho Tire Co. v. Carmichael*, [11] together with analogous developments in State courts, adds a layer of complexity to any digital and multimedia research agenda.

Similar to the previously defined research agendas, the goals of this research effort are to 1) help researchers identify the significant challenges associated with the legal aspects of digital forensics and 2) further develop communities of researchers that can work together to contribute to the legal body of knowledge associated with digital forensics.

1530-1605/11 $26.00 © 2011 IEEE

3. Research areas

The prototype research hierarchy for legal aspects of digital forensics is the result of a several open workshop sessions at security conferences and workshops from 2007 through 2010, in addition to consultation with working professionals in the technology and legal communities. This uses the approach of and extends the methodology used to formalize associated research agendas in Virtualization in Digital Forensics, Digital Forensics Research, and Education in Digital Forensics. [6, 7, 8] The preliminary result of applying the methodology to this domain was the identification and enumeration of nine distinct research categories, with several preliminary sub-areas for categories identified as shown in Figure 1. Each category and the associated research areas are briefly described in the following sections. In addition, some special research problems and overarching themes were identified and are discussed further in section 4.

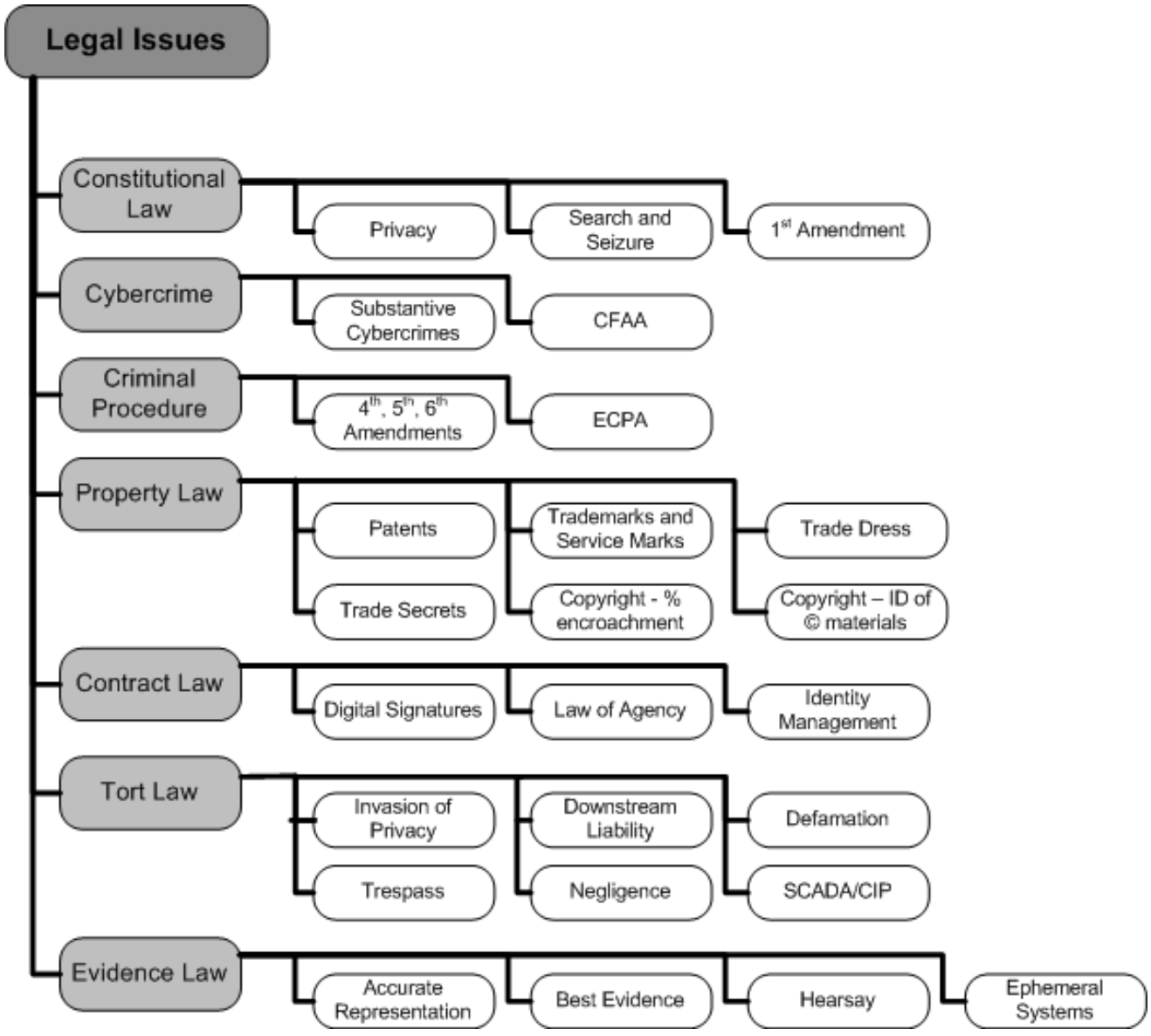

Figure 1: Legal Issues Research Areas

3.1 Constitutional law

While the U.S. Constitution provides the *foundation* for our legal system, the evolution of the Information Age has presented new challenges for interpretation of the constitution. Guarantees of free speech and free press apply in cyberspace as well as in traditional domains, but how they apply is often fact- and context-based. Justice Breyer, in *Denver Area Educational Telecommunications Consortium v. FCC*, says, "[N]o definitive choice among competing analogies (broadcast, common carrier, bookstore) allows us to declare a rigid single standard, good for now and for all future media and purposes. ... [A]ware as we are of the changes taking place in the law, the technology, and the industrial structure related to telecommunications, ...we believe it unwise and unnecessary definitively to pick one analogy or one specific set of words now." [12] Research associated with digital and multimedia forensics regarding the first amendment as applied to cyberspace has, to date, focused primarily on content-neutral and content-specific regulations, cyberstalking, cyberbullying, and countering hate speech [13]. Highly-charged issues such as pornography and child pornography, spam, and government censorship have provided the courts with a steady stream of cases involving digital and multimedia evidence, and are likely to continue to do so.

Privacy, as it applies to digital and multimedia forensics, has also provided a rich field for research. Unlike other countries, (such as Germany where informational self-determination is better defined), privacy law in the U.S. is more ambiguous. Contradictory imperatives, such as a perceived right to privacy versus the need for information about criminal conspiracies and activities, state-sponsored and industrial espionage, and terrorist plans and attacks, clash with each other amid individual and cultural assumptions that aren't necessarily congruent with either statutory or case law. Nissinbaum observes that "privacy has been the rallying cry against…computer-based, digital electronic technologies that have hugely magnified the power of human beings over information." [14]

Constitutional privacy provisions are supplemented and complemented by statutory guarantees of privacy. The Electronic Communications Privacy Act [15], the Stored Communications Privacy Act, [16] and the pen register Act [17], are statutory protections for privacy. The first two bring into sharp focus how law and technology can diverge, as seen in the digital wiretap cases. [18] Statutes passed with traditional circuit-switched networks in mind ran into trouble when different standards needed to be applied to the packet-switched networks that comprise the Internet. Packet switches store the packets for a short period while their routing protocols decide where to send the packets next, so a communication in progress may be accessed while in storage in the switch, or while in motion traversing cables or fiber-optic links. But the rules for collecting electronic evidence are different for data in motion and data at rest, so there are two dramatically different rules depending on how where the communication is collected. In one case, the U. S. District Court judge said, ""Storage" means storage, in whatever form and for however long." [19] A divided panel of the U. S. Court of Appeals for the First Circuit affirmed, [20] but an *en banc* rehearing by the full court found that the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process for such communications.

Tort law also has a role in privacy in the United States. Four "invasion of privacy" tort causes of action exist: appropriation of a person's name, likeness or identity for commercial purposes without consent; [21] a physical, electronic or mechanical intrusion upon seclusion; [22] publication of non-newsworthy, private facts about an individual that would be highly offensive to a reasonable person whose privacy was so violated; [23] and placing a person publically in a false and degrading light. [24]

Litigation involving digital and multimedia forensics may arise based on Constitutional, statutory or tort causes of action. Consequently, significant research into the issues of constitutional law in association with digital and multimedia forensics is essential as our information technologies continue to evolve.

3.2 Cybercrime

While cybercrimes extend into many areas of the hierarchy and extend beyond and between traditional jurisdictional boundaries, it is important that there be a significant focus on cybercrime in the digital forensics hierarchy since it is a motivating factor for much of the field of digital forensics. It is particularly challenging as, in the virtual world, the crime scene may not be well defined and may not be easy to delineate. When a crime scene is not clearly defined, the relevant jurisdiction is not easy to identify.

Further complicating this research area is the role that context plays, especially when these activities are compared with the special research areas discussed in section 4. Where is the line between hacking and penetration testing? How can we create legislation that restricts and allows us to investigate and prosecute illegal penetration activities while protecting the valuable ability of ethical hackers to conduct formal penetration testing?

Especially significant in the cybercrime area are hacking, viruses, digital espionage, and cyber terrorism. The coupling between digital forensics and substantive cybercrimes, as well as the issues that become apparent as cybercrimes cross fluidly across and through state, federal

and international jurisdictions, is important, and one that receives a lot of media attention. The Consumer Fraud and Abuse Act (CFAA) is a criminal statute that addresses cybercrime issues. [25] (The USA PATRIOT Act modified provisions of the CFAA with regard to the context of evidence law, criminal procedure, or Constitutional Law for digital forensics.) Research into these areas is important, and a perspective that includes all three of the tightly coupled fields (digital forensics, procedural law, and cybercrime) is essential to move forward in this area.

3.3 Criminal procedure

Criminal Procedure encompasses the legal process for determining if someone has violated criminal law. Over half (twelve) of the twenty-three rights included in the first eight Amendments affect criminal procedure. With respect to digital forensics, criminal procedure is especially concerned with the 4th, 5th, and 6th amendments, as well as statutory provisions such as ECPA. Concerns associated with the 4th amendment focus primarily on search for and seizures of digital evidence. The impact of the USA PATRIOT ACT is of particular research interest to the digital forensics community as terrorists' use of digital media for communications, planning, fundraising and recruiting is becoming increasingly common. [26]

While there are many 5th amendment legal issues associated with digital forensics, among the most interesting are self-incrimination issues concerning compelled disclosure of encryption keys. [27] 6th amendment issues with respect to digital forensics concern reports without confrontation, a right delineated in the 6th amendment. [28]

Two current trends are likely to make digital forensics and criminal procedure increasingly complex. First, the role of digital forensics in criminal procedure is likely to become increasingly challenging as we migrate infrastructure and services to a cloud computing environment. The ephemeral nature of the cloud will make personal and corporate boundaries much less well-defined, further complicating the evolution of this research area. Second, the rapid evolution of the technologies that comprise the digital footprint that we leave as we interact with and use technologies is making associated criminal procedure increasingly complex.

3.4 Property law

Property Law is concerned with real and personal property. Applications of digital forensics are more likely to fall under personal property law than real property law. Research topics in this area include patents, trademarks and service marks, trade dress, trade secrets, and issues associated with copyright (e.g., % encroachment) and identification of digital materials.

Many of issues of digital forensics and property law stem from the ease at which property can be acquired, used and replicated and the challenges associated with attribution of those actions. Trade secrets are particularly challenging in cyberspace as the definition and protection of a security perimeter has become increasingly complicated. Prior to the migration of trade secrets to digital formats, a clear perimeter around a physical secret could be identified and protected. For example, the *plans* could be locked in a safe, thus requiring only physical security to guarantee that one of the main attributes, *secrecy*, was maintained. [29] While still vulnerable to other threats associated with physical security, such as that of a malicious insider, the protection of the secret was simplified.

As the information age evolved, the primary storage media for many trade secrets shifted to digital media and the security perimeter became less well defined. Requirements for protection of the secret now extend far beyond physical security. From a digital forensics perspective, traces of a secret can be left behind on every digital media through which all or part of the secret passes. A controversial act, passed in 1998 addressing copyright in the digital age is the Digital Millennium Copyright Act (DMCA). This act was passed to fulfill US commitments under WIPO treaties and basically extended copyright to address new issues associated with Internet transmissions and other associated issues. This act has significant impact on digital forensics from a legal perspective and this is further extended by so-called super-DMCA statutes at the State level.

The application of digital forensics as applied to evolution of property law is an extremely important and rapidly evolving research area as related to the legal realm. This area is largely motivated by the migration of data to digital media, which significantly impacts the acquisition, use, and replication of many assets that are protected through property law.

3.5 Contract law

Cyberspace presents some unique challenges with respect to consumer protection. The fluidity of e-commerce and multi-jurisdictional characteristics of businesses in cyberspace make it difficult to protect consumers from unscrupulous vendors. Businesses can quickly spin up, take money, not fulfill contracts, and effectively *disappear* from the virtual world. Particular demographic groups are frequently targeted for exploitation, and research into the legal issues associated with the digital forensics process is essential in order to find way to help mitigate this ongoing threat.

In addition, consumers face challenges associated with adhesion contracts and confusion between licensing versus sales. Other issues that are included in this area are digital signatures and the law of agency. Research into digital signatures as well as processes to facilitate creation and authentication of the same are important and significantly impact contract law. Tightly coupled with this area is the evolving research into identity management and identity attributes and the role these advances play in the protection of consumers.

3.6 Tort law

Tort law is intended to provide a means for private dispute resolution. Digital forensics has an increasing role in both cybertort litigation as well as a growing and evolving role in traditional tort law. Cybertorts, which are "civil actions to recover chiefly economic, reputational, or privacy-based damages arising from Internet communications such as email, blogs, or other Internet communications" [30] are an important research area for digital forensics. Digital forensics has an additional ancillary role as digital assets are increasingly being used in general tort law cases. Issues associated with tort law that may involve digital forensics include invasion of privacy, downstream liability, defamation, negligence, and trespass. In addition, there are important tort law issues associated with control systems and critical infrastructure protection.

While there are many challenges associated with this area, a major contributor driving the need for research in this area is the ubiquity of digital media and the lack of definition and elasticity of the associated perimeters. The rapid evolution of digital communication, including email, social media sites and blogs and their associated acceptance and usage in mainstream society further necessitate research into the role of digital forensics in tort law. Early evolution of laws associated with digital forensics are likely to be seen in the tort realm as the flexible nature of tort law is well suited to address the unpredictable Internet-related forms of injury that are still evolving. [30]. As the United States has tended to have a stronger tort regime than countries that favor top-down regulation, it is even more important that researchers focus on the tight coupling between the evolution of digital forensics and how associated issues can be applied to tort law in the United States.

3.7 Rules of evidence

Evidence law is challenging to isolate as a research discipline separate from the others in the hierarchy as evidence is so frequently a part of another silo in the hierarchy. But it is perhaps the place in which most of the current research associated with digital forensics is evolving. Sommers notes that "[digital] evidence is not intrinsically different from other types of evidence; rather the problems are raised from the fragility and the transcience of many forms of computer evidence."[30] Research areas within evidence law that should be investigated include accurate representation, best evidence, and digital forensic tools. Charles Adams has begun foundational work legal issues pertaining to the development of digital forensics tools [31] and identifies some specific subcategories for further research.

Research into digital evidence is likely to become increasingly challenging as infrastructure as a service (IaaS) and software as a service (SaaS) through the cloud become increasingly common. The ephemeral characteristics of cloud computing, where infrastructure and services can be created and utilized on demand, with the same resources then repurposed for potentially unrelated clients, is a particularly challenging research area for legal aspects of digital forensics. Another area ripe for legal research, which becomes increasingly important in virtualized environments such as the cloud, is the area of live analysis which presents some unique digital forensics challenges as discussed in [32].

4. Special research problems

There are ancillary special research problems that do not fit well within a single category in the preliminary hierarchy presented here. These issues bear mention as they provide a rich collection of associated research problems that will affect other items in the research hierarchy. The areas include penetration testing, intrusion detection, incident response, and cyberwar.

Penetration testing (ethical hacking) is an important part of a defense-in-depth strategy, but under current state and federal law is close to the line defining criminal behavior and can be illegal in some contexts. It is important that research be undertaken into legal means for sanctioned penetration testing, while prohibiting destructive or unsanctioned penetration testing so that we can use this methodology to protect our networks, systems and data.

Intrusion detection is a second special situation that could present legal challenges in some contexts. [33] Methods to enable intrusion detection systems (IDS) to be used, developed, tested, and integrated into system security strategies are paramount to increasing real and perceived levels of security.

A third special consideration is associated with incident response. As the continually expanding family of devices that house digital media becomes increasingly wide and fluid, the method in which first responders handle incidents must evolve. An example of a current area in which there is great concern is the requirement in some States that limits the collection and analysis of

digital evidence to licensed private investigators and the associated fallout that has occurred, as discussed in [34].

Cyberwar is a frightening concept. Assembling an armed force used to require significant time, money, and effort, today the barrier to entry into the playing fields of war has become lower and lower as enabling information technologies continue to evolve. This area is tightly coupled with digital forensics and the evolution of the legal system concerning armed conflict and represents a category of specialized research problems that need to be addressed.

In addition to the preliminary hierarchy and special research problems, experts participating in the workshops and discussions identified some overarching extensions that could be coupled with investigation of any single item or group of items in the research hierarchy. These include applicable international law and issues associated with multijurisdictional legal situations.

5. Conclusions

The categories presented in this preliminary hierarchy and discussed in this paper demonstrate the areas in which additional research in legal issues associated digital forensics is needed. The rapid advancement of technologies, the increased globalization of the virtual environments, and the reactive nature of the U.S. regulatory process further complicate research into these important areas. The research areas outlined in this paper are identified as starting points and will continue to evolve as the field continues to mature. The authors suggest that this work could serve as the foundation for a more comprehensive research framework that also considers the special problems and overarching extension in our attempt to secure and protect our digital assets.

6. References

[1] National Research Council (2009) *Strengthening Forensic Science in the United States: A Path Forward.* Washington, DC: National Academies Press, p. 181.

[2] Bernina Computerized Sewing Machine Review. Retrieved, August 20 2010 from http://products.howstuffworks.com/bernina-activa-220-computerized-sewing-machine-review.htm;

[3] Computer/keyboard built into refrigerator door. Retrieved, August 20 2010 from www.patentstorm.us/ patents/6483695/description.html.

[4] Kilpatrick, T., J. Gonzalez, R. Chandia, M. Papa, S. Shenoi (2008) *Forensic analysis of SCADA systems and networks*. International Journal of Security and Networks, Volume 3, Number 2. Inderscience Publishers.

[5] How Car Computers Work. Retrieved, August 20 2010 from http://auto.howstuffworks.com/under-the-hood/ trends- innovations/car-computer.htm

[6] Pollitt, M., K. Nance, B. Hay, et al (2008) *Virtualization and Digital Forensics: A Research and Education Agenda.* Journal of Digital Forensic Practice, 2 (2), 62-73.

[7] Nance, K., H. Armstrong, and C. Armstrong. (2010) *Developing a Research Agenda to Improve Digital Forensics Education*. Digital Forensics Minitrack of 43rd Hawaii International Conference on Systems Sciences.

[8] Nance, K., B. Hay, M. Bishop. (2009) *Digital Forensics: Defining a Research Agenda.* 42nd Hawaii International Conference on System Sciences. Digital Forensics Research Track.

[9] 509 U.S. 579 (1993).

[10] 522 U.S. 136 (1997).

[11] 526 U.S. 137 (1999).

[12] 518 U.S. 727, 742 (1996).

[13] Rustad, M.L., (2009) Internet Law: in a nut shell. Thomas Rueters. St. Paul, MN.

[14] Nissinbaum, H. (2010) Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford law Books. Stanford University Press. Stanford, CA.

[15] 18 USC §2510 et seq.

[16] 18 USC §2701 et seq.

[17] 18 USC §3121 et seq.

[18] *United States v. Councilman*, 245 F. Supp. 2d 319 (D. Mass. 2003).

[19] 373 F.3d 197 (1st Cir. 2004).

[20] 2005 U.S. App. LEXIS 16803 (US Ct. App. 1st Cir. 2005).

[21] Restatement of the Law, Second, Torts, §652C.

[22] Restatement of the Law, Second, Torts, §652B.

[23] State Law: Publications of Private Facts. Retrieved, August 20 2010 from http://www.citmedialaw.org/legal-guide/state-law-publication-private-facts.

[24] Restatement of the Law, Second, Torts, §652E.

[25] See 18 USC §1030, for example.

[26] Eban Kaplan (2009) Terrorists and the Internet. Retrieved August 20, 2010 from http://www.cfr.org/publication/ 10005/terrorists_and_the_internet.html.

[27] *In Re Boucher*, United States District Court for the District of Vermont, 2007 WL 4246473 (Nov. 29, 2009).

[28] *Melendez-Diaz v. Massachusetts*, 129 S.Ct. 2527 (2009).

[29] Uniform Trade Secrets Act. Retrieved, August 20, 2010 from http://euro.ecom.cmu.edu/program/law/08-732/Trade Secrets/utsa.pdf.

[30] Sommer, P., (2008) "Digital Footprints: Assessing Computer Evidence", Criminal Law Review - Special Edition 1998, pp. 61-78.

[31] Adams, C. (2008) Legal Issues Pertaining to the Development of Digital Forensic Tools. Proceedings of the IEEE Third International Workshop on Systematic Approaches to Digital Forensic Engineering. May, 2008 IEEE DOI 10.1109/SADFE.2008.17

[32] Hay, B., M. Bishop, and K. Nance. (2009) *Live Analysis: Progress and Challenges*. IEEE Security & Privacy. Volume 7, Issue 2. March-April 2009. pp. 30-37.

[33] Shvern v. Desrosiers, No. 99-2159 (U. S. Ct. App. 4th Cir., 2000) Retrieved, August 20 2010 from http://pacer.ca4.uscourts.gov/opinion.pdf/992159.U.pdf.

[34] Phillips, A. and K. Nance. (2010) *Computer Forensics Investigators or Private Investigators: Who Is Investigating the Drive?* Proceedings of the IEEE Fifth International Conference on Systematic Approaches to Digital Forensic Engineering. Oakland, CA, May, 2010.