



---

Annual ADFSL Conference on Digital Forensics, Security and Law

2017  
Proceedings

---

May 16th, 9:15 AM


## Development of A Professional Code of Ethics in Digital Forensics

Kathryn C. Seigfried-Spellar  
*Purdue University*, [kspellar@purdue.edu](mailto:kspellar@purdue.edu)

Marcus Rogers  
*Computer Information & Technology, Purdue University*, [rogersmk@purdue.edu](mailto:rogersmk@purdue.edu)

Danielle M. Crimmins 2184089  
*Purdue University*, [dcrimmin@purdue.edu](mailto:dcrimmin@purdue.edu)

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

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

---

### Scholarly Commons Citation

Seigfried-Spellar, Kathryn C.; Rogers, Marcus; and Crimmins, Danielle M. 2184089, "Development of A Professional Code of Ethics in Digital Forensics" (2017). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 12.

<https://commons.erau.edu/adfsl/2017/papers/12>

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



# DEVELOPMENT OF A PROFESSIONAL CODE OF ETHICS IN DIGITAL FORENSICS

Dr. Kathryn C. Seigfried-Spellar  
Purdue University  
Computer and Information Technology  
West Lafayette, IN 47907  
kspellar@purdue.edu

Dr. Marcus K. Rogers  
Purdue University  
Computer and Information Technology  
West Lafayette, IN 47907  
rogersmk@purdue.edu

Danielle M. Crimmins, M.S.  
Purdue University  
Computer and Information Technology  
West Lafayette, IN 47907  
dcrimmin@purdue.edu

## ABSTRACT

Academics, government officials, and practitioners suggest the field of digital forensics is in need of a professional code of ethics. In response to this need, the authors developed and proposed a professional code of ethics in digital forensics. The current paper will discuss the process of developing the professional code of ethics, which included four sets of revisions based on feedback and suggestions provided by members of the digital forensic community. The final version of the Professional Code of Ethics in Digital Forensics includes eight statements, and we hope this is a step toward unifying the field of digital forensics as a profession.

**Keywords:** digital forensics, computer forensics, code of ethics, professional ethics

## 1. INTRODUCTION

Digital forensics is defined as "the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence divided from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations"

(Palmer, 2001, p 16). In short, digital forensics is the identification, recovery, analysis, and presentation of digital evidence in the court (Losavio, Seigfried-Spellar, & Sloan, 2016). Almost all criminal and civil investigations include some form of digital evidence (Clifford, 2006), and in many cases, these investigations include more than one form of digital device (e.g., mobile phone, computer, global positioning system). Law enforcement is experiencing an exponential increase in digital evidence, yet digital forensics is the newest

branch of forensic science, and in many ways, is still in its infancy (Holt, Bossler, & Seigfried-Spellar, 2015; Losavio et al., 2016). We expect there to be a continued increase in the variety and quantity of digital forensic evidence in the courtroom, and investigators will be called upon to testify on the digital forensic process and findings. However, not all who testify in court have the appropriate accreditations and training in digital forensics.

For instance, in September of 2016, Chester Kwitowski was arrested for falsifying his credentials as an expert witness in computer forensics; he testified as an expert witness in five jury trials involving sexual battery of a minor and/or possession of child pornography (Sullivan & Marrero, 2016). Kwitowski lied on his resume with regards to his educational background, professional certifications, military services, and government clearances (Sullivan & Marrero, 2016). Similarly, in 2014, Judith Gosselin was found guilty for misrepresenting her computer forensic certifications (Timmins, 2014). She claimed to be a certified computer examiner, and subsequently was hired as a private investigator, who worked for the state and federal public defender's office, as well as civil and criminal defense attorneys (Timmins, 2014).

These are just two examples of individuals falsifying their credentials as experts in computer forensics. This problem is exacerbated by the fact that there is no professional code of ethics in digital forensics. Unlike Medicine and Law, which have a professional code of ethics that is enforced and backed by state and federal law, digital forensics is currently lacking an overarching professional code of ethics (Losavio et al., 2016; Seigfried-Spellar & Gilliland, 2016; Sloan & Seigfried-Spellar, 2015). Instead, there is a "hodgepodge" of digital forensic organizations that provide training and certifications, and

they each have their own code of ethics (Sloan, 2015). Roux and Falgoust (2012) argue, although these individual codes of ethics exist, there is still a lack of research which justifies such codes. With no unifying professional code of ethics, it would be possible for an individual to violate the code of ethics for one certifying body, and instead of being banned from the digital forensics community, the individual could be certified under a different organization.

Thus, members of the digital forensic community have expressed the importance and need for a unifying professional code of ethics in digital forensics (Gay, 2012; Greenwald, Snow, Ford, & Thieme, 2009; Harrington, 2014; Losavio et al., 2016; Payne & Landry, 2005; Roux & Falgoust, 2012; Seigfried-Spellar & Gilliland, 2016; Sharevksi, 2015; Sloan & Seigfried-Spellar, 2015; Sloan, 2015). Over two decades ago, Pollitt (1995) suggested the lack of standards would "complicate and slow the acceptance of computer evidence" (p. 6), and a set of standards would be necessary to continue to utilize computer evidence in the criminal justice system. Additionally, Meyers and Rogers (2004) warned that the lack of standardization and certification surrounding digital forensics could ultimately lead to digital forensic being classified as a "junk science." Similarly, Sloan (2015) referred to the current state of digital forensic as the "wild west, because there is no code of ethics which governs digital forensics examiners behaviors" (p. 3). Further, Harrington (2014) argued digital forensic examiners are inevitably going to face ethical dilemmas in the course of an investigation and need a code of ethics to seek guidance in these situations (e.g., conflicts of interest, forensic confirmation bias). Harrington (2014) also stated a code of ethics served an important role in an organization, by providing "prestige and credibility for the organization, the elimination of unfair

competition, and fosters cooperation among professionals" (p. 3).

Jamal and Bowie (1995) conclude the most common way to deal with ethical dilemmas in business and professions is by creating a code of ethics. A code of ethics is an attribute of many professions, such as Medicine, Law, Professional Engineers, Psychology, and Nursing, just to name a few. Losavio et al. (2016) examined the difference between occupations and professions in order to determine if the field of digital forensics could be considered a profession in its current state. Based on the sociological definition of occupations and professions, Losavio et al. (2016) discussed how professions and occupations are separated by a specific set of traits that guide professional behavior, as cited by Volti (2011). According to Volti (2011), "a guidance of professional behavior" refers to a code of ethics, which must include the following: (1) definition of the key values of the profession and provides general guidance for its practitioners, (2) provide a process for investigating alleged unprofessional behavior, and (3) provide sanctions for violating the code.

Losavio et al. (2016) concluded that without an overarching code of ethics for digital forensics, digital forensics could not be considered a profession in its current state. Further, Sloan (2015) draws attention to the fact that unlike the code of ethics for medicine and law, which are backed by the state and enforced by both civil and criminal law, there is currently no equivalence for digital forensics. In addition, Sloan, Seigfried-Spellar, and Rogers (2015) compared the general requirements in education, certification, training, and skills for the practice of medicine, law, and digital forensics in the United States (see Table 1). In a similar fashion, Greenwald et al. (2009) conducted a workshop on the *possible* need for a code of ethics in information

security. Overall, many individuals expressed a need for a code of ethics while some believed the "discipline did not have the maturity" to formulate a code of ethics (Greenwald et al., 2009, p. 86). Although in its infancy, Sloan et al. (2015) and Losavio et al. (2016) concluded that it was time for the field of digital forensics to develop a unifying professional code of ethics.

Table 1.  
*General Requirements for the Practice of Medicine, Law, and Digital Forensics in the U.S (Sloan, Seigfried-Spellar, & Rogers, 2015).*

	Medicine <sup>a</sup>	Law <sup>b</sup>	Digital Forensics <sup>c</sup>
<b>Education</b>	Doctorate (MD)	Juris Doctorate (JD)	Variable <sup>d</sup>
<b>Degree Field</b>	Medicine	Law	Computer science; information systems; information technology; criminal justice; forensic science; digital forensics; computer forensics; cybersecurity
<b>Licensure/ Certification</b>	M.D.s must pass all three parts of the U.S. Medical Licensing Examination and D.O.s must pass the Comprehensive Osteopathic Medical Licensing Examination-USA; board certification by the ABMS is optional	J.D.s wishing to practice law must pass state bar examination (which includes multi-state bar exam) and pay licensing fees that vary by state	No licensure requirements <sup>e</sup> ; Certification requirements vary based on certifying body, may have to pay membership fee to voluntary association issuing certification
<b>Experience</b>	Most doctors complete a residency (three – eight years)	Most lawyers will have either (1) worked for a firm during the summer between their 1 <sup>st</sup> and 2 <sup>nd</sup> year and 2 <sup>nd</sup> and 3 <sup>rd</sup> year or (2) completed a clerkship with a local, state, or federal judge, or both	Varies and may not be required; Completed a college internship with LE agency or within industry; Self-taught (interest-driven or agency had a "need" to fill)
<b>Key Skills</b>	Problem solving, leadership, empathy, and communication	Problem solving; interpersonal relations; written communication	Puzzle solving (fact-finding, investigation) Written and verbal (testifying) communication
<b>Computer Skills</b>	Medical software; Microsoft Excel; Accounting software	Legal software; Microsoft Word, Excel, Outlook	Specialized digital forensics software; Microsoft Office (Word, PowerPoint), Networking, programming, database, and wireless telecomm.
<b>Technical Skills</b>	Use of medical and diagnostic equipment (surgical clamps, ophthalmoscopes)	Issue spotting; knowledge of federal and local rules of evidence and procedure; technical writing (e.g., briefs, memoranda of law)	Knowledge of digital forensics investigative procedures and laws; Identifying, analyzing, interpreting and/or organizing digital data; report writing, Network and Systems Administration.
<b>Additional Requirements</b>	Must continue education to maintain licensure or certification; requirements vary by state	Must continue education to maintain licensure by earning a specific number of continuing legal education credits (CLEs) annually with specific number of credits required varying by state	Some certification bodies require re-certification (e.g., ISFCE, IACIS) after a stated number of years; Some states require independent examiners obtain private investigator certification

<sup>a</sup> Source: [http://study.com/steps\\_to\\_become\\_a\\_doctor.html](http://study.com/steps_to_become_a_doctor.html). Retrieved August 13, 2015.  
<sup>b</sup> Source: <http://hirealawyer.findlaw.com/choosing-the-right-lawyer/what-are-the-professional-requirements-for-becoming-a-lawyer.html>. Retrieved August 15, 2015.  
<sup>c</sup> [http://study.com/articles/How\\_to\\_Become\\_a\\_Computer\\_Forensic\\_Examiner.html](http://study.com/articles/How_to_Become_a_Computer_Forensic_Examiner.html). Retrieved August 17, 2015.  
<sup>d</sup> Ranges from a high school diploma to a bachelor's degree, depending on agency and job-related activities.  
<sup>e</sup> Some states (e.g., Alabama, Indiana) require digital forensics practitioners to be licensed as private investigators (PIs).

In 2015, Sharevski's compared the codes of ethics for 12 organizations in digital forensics. Both national and international digital forensic organizations were included in the comparison: American Academy of Forensic Science (AAFS), American Board of Criminalistics (ABC), American Society of Digital Forensics and e-discovery (ASDFD), California Association of Criminalists (CAC), Consortium of Digital Forensic Specialist (CDFFS) , Cyber Security Institute (CI), Digital Forensics Certification Board (DFCB), EC-Council (ECC), High Technology Crime Investigation Association (HTCIA), International Association of Computer Investigations Specialists (IACIS), SANS Institute (SANS), and the International Society of Forensic Computer Examiners (ISFCE). Sharevski (2015) detailed the sub-

categorization of digital forensic codes with regards to ethical consideration (see Table 2). Sharevski (2015) found similarity with regards to the ethical considerations dealing with professional, diligence, competency, qualification, confidentiality, examination and analysis, and reporting. However, there were differences with respect to testimony, conflict, financial stakes, responsibility to client, and lawful compliance.

Table 2

*Sub-categorization of the Digital Forensic Codes of Ethics in Respect to Ethical Consideration (Sharevski, 2015)*

Ethical Consideration	<i>Digital Forensic Organization</i>								
	ASDFD	CDFS	CI	DFCB	ECC	HTCIA	IACIS	SANS	ISFCE
Professional Diligence	X	X	X	X		X	X	X	X
Competency	X	X	X	X	X	X	X	X	X
Qualification	X	X	X	X	X	X		X	X
Examination and analysis	X	X	X	X	X	X	X	X	X
Testimony	X	X		X					X
Conflict of Interest	X	X	X	X	X			X	X
Reporting	X	X	X	X		X	X		X
Financial Stakes	X	X	X						
Responsibility to client			X	X	X			X	X
Lawful compliance	X	X	X	X	X				X

*Note.* From Sharveski (2015, p. 51)

## 2. DEVELOPING A CODE OF ETHICS

After momentum from a National Science Foundation (NSF) funded workshop (Sloan & Seigfried-Spellar, 2015), Seigfried-Spellar and Gilliland hosted a workshop at the American Academy of Forensic Sciences (AAFS) annual conference in 2016. The workshop brought together academics, practitioners, and vendors from the digital forensics field and aimed at discussing the need and development of a professional code of ethics in digital forensics. As a result of the workshop, members of the digital forensics community agreed there was a need for a singular, unified professional code of ethics in digital forensic. This led to the development of the current professional code of ethics in digital forensics.

As shown in Table 3, the development process began at the AAFS conference meeting in February 2016. For the first draft, we identified comparable codes of ethics from a variety of professions, including the National Society of Professional Engineers, American Nurses Association, and the American Bar Association. We also reviewed the comparison conducted by Sharevski (2015) to identify

overarching themes in the code of ethics from different digital forensic organizations and certifying bodies. Finally, we consulted the seven core values provided by Payne and Landry (2005) which are meant to help achieve a "comprehensive, clear, positive in nature, and enforceable" code of ethics (p. 84). These seven values include: consistency, respect of individuals, autonomy, integrity, justice, utility, and competence. Based on the overarching themes between the different organizations, coupled with the outline provided by Payne and Landry (2005), the first draft code of ethics in digital forensics was created.

Table 3

*Timeline of the Development Process for the Professional Code of Ethics*

Month	Action
February	AAFS workshop
May	1st draft created
July - August	E-mail was sent to members of the digital forensics community for comments and suggestions
August	Revisions to first draft
September	2nd draft was posted on blog for comments and suggestions
October	2nd round of revisions based on blog & e-mail feedback
November	3rd draft was posted for 15 days
December	3rd round of revisions based on blog & e-mail feedback
February (2017)	Ad Hoc group meeting for comments and feedback
March (2017)	Final round of revisions based on ad hoc group feedback
<i>Note.</i> Development took place in 2016, unless stated otherwise	

### 2.1 Draft #1

Between July-August 2016, the first draft of the Professional Code of Ethics in Digital Forensics was sent out to members of the digital forensic community, including academics, practitioners, government employees, and vendors. Specifically, the link to the blog was shared for each round of feedback with the American Academy of Forensic Science (AAFS) Digital and Multimedia Sciences' listserv as well as the Organization of Scientific Area Committee's (OSAC) Digital Evidence subcommittee listserv. In addition, the link was shared with members from the National Institute of Standards and Technology (NIST), as well as on LinkedIn, and with the individuals who attended the various workshops discussing the need for a professional code of ethics (see Seigfried-Spellar & Gilliland, 2016; Sloan & Seigfried-Spellar, 2015; Sloan, Seigfried-Spellar, Rogers, 2015).

This first round of feedback resulted in three comments. These comments included support for the draft and basic grammatical errors/suggestions which were addressed and corrected. After receiving minimal feedback on the first draft, the authors decided to post the

second draft on a free, open-source website, Word Press. This website would also allow us to track the number of visitors, views, and comments.

### 2.2 Draft #2

On September 7, 2016, the 2nd draft of the Professional Code of Ethics in Digital Forensics was posted online. Just as before, the link to the blog was shared with the American Academy of Forensic Science (AAFS) Digital and Multimedia Sciences' listserv, the Organization of Scientific Area Committee's (OSAC) Digital Evidence subcommittee listserv, members of the National Institute of Standards and Technology (NIST), with the individuals who attended the previously mentioned workshops, and on LinkedIn. The blog was available for viewing and comments for 30 days. During this time, the website received 321 visitors and was viewed 500 times. After 30 days, the blog was removed; in total, the second draft received 11 comments on the blog post and one comment via e-mail.

For example, a number of comments were directed at the original clauses IV(a) and V. The original IV(a) clause stated: *In cases where conclusions warrant multiple*

*interpretations, a member should not favor the side which he or she is employed, nor should a member conceal information from fact finders / courts, which if omitted, would cause a distortion of facts.* This clause received multiple concerns, such as:

- "lawyers have a duty to represents clients' interests, and if you are selected and retained as their testifying expert witness, this is nothing wrong with explanation that aligns with your attorney's case"
- "examiners often do not have enough time to examine every piece of data and it maybe be possible an examiner misses a piece of data which could convict or exonerate someone"

Based on the second round of feedback, the authors decided the main components were covered in additional clauses, so the suggestions made were valid. Therefore, clause VI, subsection a, was removed.

With regards to clause V, one commenter suggested adding "scientifically invalid or otherwise discredited methods" instead of "proven and accepted methods." Clause V was changed accordingly. Additionally, the authors added clause III as a subset of II based on feedback from the community. Finally, one reviewer suggested making clause I as an opening statement for the professional code of ethics: "A member shall, at all times, demonstrate a commitment to professionalism, integrity, and competency in all of their duties so as to enhance the honor, reputation, and usefulness of the profession."

### 2.3 Draft #3

After round two of feedback, the 3<sup>rd</sup> draft Professional Code of Ethics in Digital Forensics was posted online for comments and suggestions on November 2, 2016 for an additional 15 days via the previously discussed

avenues for distribution. In total, the 3<sup>rd</sup> draft received 83 visitors, 141 views and 2 comments (1 blog comment; 1 email comment). With regards to clause VII, *A member shall not reveal any confidential information obtained during an examination without proper authorization and shall preserve the integrity of evidence*, one reviewer pointed out that the "and shall preserve..." seemed unnecessary. Upon review of this clause and the entire code, the authors agreed with the suggestion and removed this part of the clause, as this was already articulated in a previous clause. The second comment was a personal email supporting the authors' third draft of the professional code of ethics.

### 2.4 Draft #4

In February 2017, an ad hoc group was given the fourth draft and asked to provide suggestions and feedback. This group presented a unique comment which was not addressed in previous rounds of revisions. The ad hoc group pointed out the current code of ethics lacked a clause pertaining to serving the public interest, specifically putting the public's interest before an individual's personal gain. This type of clause is present in a variety of professional codes of ethics, including accounting, law, medicine, and the National Society for Professional Engineers. Therefore, in March 2017, the authors added an additional clause pertaining to the public interest; specifically, "individuals should hold paramount the welfare of the public, and a member shall put individuals over personal gain, while prioritizing the pursuit of truth."

### 2.5 Final Version

After four rounds of revisions, utilizing feedback and suggestions from members of the digital forensics community, the end result was the following Professional Code of Ethics in Digital Forensics:



A member shall, at all times, demonstrate a commitment to professionalism, integrity, and competency in all of their duties so as to enhance the honor, reputation, and usefulness of the profession.

1. A member shall hold paramount the welfare of the public.
  - A member shall put welfare of individuals over personal gain, while prioritizing the pursuit of truth
2. A member shall not engage in any illegal, or unethical conduct, or any activity which would constitute a conflict of interest.
3. A member shall never knowingly misrepresent their education, training, experience or areas of expertise.
  - a. A member shall, at all times, exhibit the highest level of honesty in their examination and only provide services in areas of their competence.
  - b. A member shall comply with the orders of the courts and only testify to matters truthfully.
4. A member, when conducting examinations, shall not use scientifically invalid or otherwise discredited methods.
5. A member shall not give opinions / testimony on matters not subject to formal examinations unless requested to do so by the courts.
6. A member shall not misrepresent data or scientific principles upon which their conclusions or professional opinions are based.
7. A member shall keep abreast of new developments, strive to increase one's competence, and advance education and research within the field.

8. A member shall not reveal any confidential information obtained during an examination without proper authorization.

### 3. CONCLUSION

While the authors have presented an initial attempt at the construction of a "universal" code of ethics for the field of digital forensics, it is understood that this is the beginning of a long journey. The code of ethics presented serves as a stake in the sand (so to speak), in order to begin the long overdue exercise of formalizing the field into a profession. We anticipate and encourage there to be numerous debates regarding the proposed code, as these are needed to mature our field.

However, medicine and law both have a professional code of ethics which is enforced and backed by state and federal law, as well as a universal governing association (e.g., bar association for law). Currently, digital forensics is lacking an overarching governing body to enforce a professional code of ethics. Moving forward, the authors suggest that in order for the field of digital forensics to continue to mature, a "universal" governing body must also be established.

The field of digital forensics can no longer default back to the arguments that we are too diverse to have a common, even high-level professional code of conduct; or, while we claim to be a profession within the forensic sciences, we are different from the other forensic sciences therefore we do not need to be structured like them. We need to remember that it is possible for a code of conduct to be forced upon the field of digital forensics from an outside government body; therefore, these hollow claims are, at best, excuses not to tackle a difficult, but not intractable, problem.

## REFERENCES

- Clifford, R.D. (Ed.). (2006). *Cybercrime: The investigation, prosecution, and defense of a computer-related crime* (2<sup>nd</sup> ed.). Durham, NC: Carolina Academic Press.
- Gay, J. R. (2012). *A Code of Conduct for Computer Forensic Investigators*. Unpublished Doctoral Dissertation, University of East London, London, UK.
- Greenwald, S. J., Snow, B. D., Ford, R., & Thieme, R. (2009, August). Towards an ethical code for information security?. In *Proceedings of the 2008 workshop on New security paradigms* (pp. 75-87). ACM.
- Harrington, S. (2014, March 4). *Professional Ethics in the Digital Forensic Discipline: Part 1*. *Forensic Magazine*. Retrieved from [www.forensicmag.com](http://www.forensicmag.com).
- Holt, T., Bossler, A., & Seigfried-Spellar, K. (2015). *Cybercrime and digital forensics: An introduction*. Abingdon, UK: Routledge.
- Jamal, K., & Bowie, N. E. (1995). Theoretical considerations for a meaningful code of professional ethics. *Journal of Business Ethics*, 14(9), 703-714.
- Losavio, M., Seigfried-Spellar, K. C., & Sloan III, J. J. (2016). Why digital forensics is not a profession and how it can become one. *Criminal Justice Studies*, 29(2), 143-162.
- Meyers, M. & Rogers, M. (2004). Computer forensics: The need for standardization and certification. *International Journal of Digital Evidence*, 3(2), 1-11.
- National Research Council (2009). *Strengthening Forensic Science in the United States: A Path Forward*. Washington, DC: US Department of Justice.
- Palmer, G. (2001, November 6). *A Road Map for Digital Forensic Research*, DFRWS 16. Retrieved from <http://www.dfrws.org/>
- Payne, D., & Landry, B. J. (2005). Similarities in business and IT professional ethics: The need for and development of a comprehensive code of ethics. *Journal of Business Ethics*, 62(1), 73-85.
- Pollitt, M. M. (1995, April). Principles, practices, and procedures: An approach to standards in computer forensics. Paper presented at the Second International Conference on Computer Evidence, Baltimore, MI.
- Roux, B. & Falgoust, M. (2012). Ethical issues raised by data acquisition methods in digital forensics research. *Journal of Information Ethics*, 21(1), 40.
- Seigfried-Spellar, K.C. & Gilliland, R.G. (2016, February). Developing a professional code of ethics in digital forensics. Chair, Workshop at the American Academy of Forensic Sciences 68<sup>th</sup> Annual Scientific Meeting, Las Vegas, NV.
- Sharevski, F. (2015). Rules of professional responsibility in digital forensics: A comparative analysis. *Journal of Digital Forensics, Security and Law*, 10(2), 39-54.
- Sloan, J. (2015, August 10). There's no code of ethics to govern digital forensics – And we need one. *The Conversation*. Retrieved September 5, 2015, from <https://theconversation.com>
- Sloan, J. & Seigfried-Spellar, K. (2015, May 13-14). *Professional Ethics in Digital Forensics Workshop*. Co-Chair, 2-day workshop conducted at NSF Headquarters, Washington, D.C.
- Sloan, J., Seigfried-Spellar, K., & Rogers, M. (2015, September 9). *A Code of*

Professional Ethics for Digital Forensics: Need, Challenges, and Next Steps. Roundtable session at the Southern Criminal Justice Association, Charleston, SC.

Sullivan, D. & Marrero, T. (2016, September 22). Tampa man charged with faking credentials, testifying for the accused in child sex cases. Tampa Bay Times. Retrieved from [www.tampabay.com](http://www.tampabay.com)

Timmins, A. (2014, February 3). Computer investigator pleads guilty to misrepresenting credentials. Concord Monitor. Retrieved from [www.concordmonitor.com](http://www.concordmonitor.com)

Volti, R. (2011). An introduction to the sociology of work and occupations. Thousand Oaks, CA: Sage