

THE JOURNAL OF
**DIGITAL FORENSICS,
SECURITY AND LAW**

**Journal of Digital Forensics,
Security and Law**

Volume 10 | Number 2


Article 3

2015

Rules of professional responsibility in digital forensics: A comparative analysis

Filipo Sharevski
Purdue University

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

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

Recommended Citation

Sharevski, Filipo (2015) "Rules of professional responsibility in digital forensics: A comparative analysis," *Journal of Digital Forensics, Security and Law*. Vol. 10 : No. 2 , Article 3.

DOI: <https://doi.org/10.15394/jdfsl.2015.1201>

Available at: <https://commons.erau.edu/jdfsl/vol10/iss2/3>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.



(c)ADFSL



RULES OF PROFESSIONAL RESPONSIBILITY IN DIGITAL FORENSICS – A COMPARATIVE ANALYSIS

Filipo Sharevski

Department of Computer and Information Technology

College of Technology

Purdue University

West Lafayette, IN, 47906

fsharevs@purdue.edu

ABSTRACT

The Committee on Identifying the Needs of Forensic Sciences Community (2009) accentuates the establishment of a uniform code of ethics emphasizing the importance of enforceability in strengthening the role that the forensic science plays within the criminal justice system. Equally pertinent to the domain of digital forensics, this imperative entails a research commitment in comparing and contrasting the respective codes of ethics to illustrate their *variety*, *specificity* and *enforceability* to inform the discussion on the associated regulative aspects. Accordingly, this paper reviews the professional regulation inaugurated in both the US and international digital forensics arena giving a detailed perspective on the consolidation of the practice.

Keywords: digital forensics code of ethics, digital forensics professional standards of conduct

1. INTRODUCTION

Understood as a “convention among professionals”, the coequal purpose in establishing a *code of ethics* is to protect forensic community members from certain pressures and consequences of the profession and serve as a collective recognition of their responsibilities, while providing rational sanctioning reference when the established professional norms are violated (Barnett, 2001; Bowen, 2009; Davis, 1991). Despite the necessity of a normative regulation, the operationalization of the proclaimed prescriptions remains an issue of concern since “most forensic disciplines still lack any consistent structure for the enforcement of ‘better practices,’ operating standards, and certification and accreditation programs

(Committee on Identifying the Needs of the Forensic Sciences Community, 2009, p. 214). In response to this challenge, the National Research Council (NRC) in its report on the status of forensics discipline recommends establishment of a national code of ethics for all forensic science disciplines and mechanisms of enforcement through a certification process.

While the full realization of this imperative is a subject of an extensive discussion among the forensics community, useful argumentation contributing to this engagement is a comparative revision of the current professional responsibility regulation present in different forensic societies. Being one of the youngest forensic sciences rapidly unfolding domain of application (Casey, 2011; International Standardization Organization, 2014b), digital forensics are particularly interesting for such

a research commitment. Recognizing the importance of the digital forensic ethics, Bassett, Bass, & Brien (2006) underline that “the computer forensics requires a well-balanced combination of technical skills, legal acumen, and ethical conduct,” knowing that forensic practice frequently entails facing ethical dilemmas. However, the lack of a unified governing body regulating the practice among the digital forensics societies (Casey, 2011) underlines the impression that the “widespread coverage, harmonization and enforceability” aspects of the digital forensics codes of ethics are still unaddressed (Harrington, 2011). Addressing exactly these issues of concern, the remainder of the paper provides a comparative assessment of the codes currently regulating the professional responsibility as established by the most prominent domestic and international digital forensics certification and training organizations. Following the contours outlining the course of the basic professional behavior given in the second part, the third section brings the analysis of the digital forensics codes of ethics by contrasting them against the prescriptive comprehensiveness, scientific method, examination and interpretation, adversary presentation, and general practice and profession (Melson, 2012). The enforceability is approached in the fourth section, discussing the incentives driving the operational regulation in the digital forensics arena. The paper concludes with a perspective on the regulative consolidation steaming out of the central analysis.

2. RELATED WORK

The ethical conceptualization being closest to the digital context of the forensics practice is comprehensively elaborated by both Barnett (2001) and Bowen (2009). Focusing on the necessity of the professional standards and protocols in the forensic sciences, Barnett

(2001) arguments their importance noting that they unequivocally define the relationship between the criminal justice system as a consumer and the practitioners as providers of forensic services in that the latter consider and employ the “entire gamut of scientific methods and tools that could resolve the issues relevant to the proceedings”, while the previous evaluate the process for yielding the forensic products and their admissibility according to defined rules of evidence, being respectively the *Daubert* and *Lorraine* models in the case of the digital forensics (Federal Judicial Center, 2011). As a stronghold for the forensic professionalism, Barnett (2001) further discusses the development process of codes of ethics, detailing several comprehensive primers (while noting the lack of nationally recognized and accepted one)—including the codes of ethics established by the American Academy of Forensic Sciences (2013), American Board of Criminalistics (2013) and the California Assotiation of Criminalists (2010) —and the complementary policies and procedures that deal with the issue of enforceability and sanctioning. Completing the elaboration, Barnett (2001) outlines the ethical requirements in terms of competence, thoroughness, relevance, reviewability and disclosure, while in the same time highlighting the threats of ethical conflicts raising related to the professional practice and technical competence. Extending the discussion further, Bowen (2009) thoroughly explicates the motivation and justification of an actual ethical misbehavior, providing case studies involving selective bias, dishonesty, conflicts of conscience and commitment, contingency, and favoritism. On this basis, Bowen (2009) sets the main accent on the structuring process for the forensics code of ethics—borrowing heavily from Barnett (2001)—and the ethical approach to forensic professionalism, providing, in addition with a research data on the ethical concerns,

examples of unethical behavior, and training in ethics.

Cognizant of the need for structuring a code of ethics specially tailored for the digital forensic professionals, Gay (2012) tries to extend both Barnett's (2001) and Bowen's (2009) conceptualizations by proposing a set of principles and precepts for the practitioners working in the private sector. However, Gay (2012) fails to provide a strong ethical reference generally applicable in the digital forensics realm, mainly because it misses to compare and extrapolate all the essential provisions from the currently valid regulative exemplars. By the same token, Harrington (2011) discusses the collaboration between the legal representatives and the digital forensic experts, focusing mainly on the ethical aspects. Analyzing the ethical rules that govern the digital forensic investigation, Harrington (2011) reviews several digital forensics codes of conduct, concluding that “although most digital forensics organizations do impose a code of ethics as a condition of membership, there is little known about frequency of enforcement, efficacy of enforcement, or ethics awareness among the membership” (p. 357). Beyond these efforts, no useful contributions towards the imperative of the particular research commitment exists. Given the dedication in contrasting digital forensics codes of ethics as to illustrate the “variety, specificity and enforceability” among them, the methodological approach can hardly borrow useful directions from these works. Therefore, the comparative assessment follows the scheme initially developed by Saks (1989) and extensively operationalized by Melson (2012) in reviewing the status of ethical regulation concerning the forensic practice. Reviewing and analyzing the “current status of ethics codes in professional organizations, both in US and international”, Melson (2012) illustrates “the variety, specificity and enforceability of these

codes” by cataloging the provisions in seven different categories: “(1) ethical considerations; (2) scientific method; (3) examination and conclusion; (4) adversary presentation; (5) general practice; (6) professional conduct; (7) additional provisions”. Towards the enforcement of the misconduct allegations, Melson (2012) analyzes the codes’ enforceability and the imposition of sanction, as a considerably important regulatory aspect of the forensic practice. An analogous illustration of the digital forensics codes of ethics is provided in Tables 2 = 8 (see Appendix).

3. COMPARATIVE ANALYSIS OF THE DIGITAL FORENSICS CODES OF ETHICS

The responsibility of the digital forensics professional regulation is left into the hands of various certification entities or professional digital forensic societies. Corroborating the initial premise outlined in the NRC report, Table 1 brings a representative sample of codes of ethics specially developed for the digital forensic science¹ together with the codes of ethics of the leading forensics organizations. The particular set includes the codes established by the AAFS, ABC and CAC as to enable logical coherence with Barnett's (2001) and Bowen's (2009) concepts, and in the same time to provide a reference in contrasting the codes purported to regulate the digital forensic

¹ (Consortium of Digital Forensic Specialists, 2013; Cybersecurity Institute, 2013; Digital Forensics Certification Board, 2008; EC-Council, 2013; High Technology Crime Investigation Association, 2013; International Association of Computer Investigation Specialists, 2013; SANS Institute, 2013; The American Society of Digital Forensics and eDiscovery, 2013; The International Society of Forensic Computer Examiners, 2013)

practice. This group includes US- (ASDFD, CDFC, CI, DFCB, ECC, SANS) and international-based (HTCIA, IACIS, ISFCE) digital forensics organizations, accenting the practice towards which the NRC recommendation is directed. Though somewhat subjective in the nature, the initial contrasting suggests disparate level of specificity, irrespectively to the domain of operation—while DFCB and ISFCE detail the ethical concepts to a greater level, the rest of societies devote moderate to brief attention. However, the comparison as of the number of precepts tells little about the contextual relevance of the codes, i.e., the commonality between them or the enforceability in action. Therefore, codes' precepts are further contrasted over the same dimensions used in Melson (2012) as to better illuminate the undertaken analytical effort.

3.1 A Comparison in Respect to Main Provisions

The catalogue of the codes subdivided by the *ethical considerations* and depicted in Table 2 indicates high similitude relative to the *professional diligence, competency, qualification, confidentiality, examination and analysis, and reporting* segments. This is intuitively rational, knowing that the digital forensic practice resembles with both the general praxis and the universal professional conduct. However, some of the codes remain silent respective to the *testimony* (CI, ECC, HTCIA, IACIS, SANS), *conflict of interest* (HTCIA, IACIS), *financial stakes* (DFCB, ECC, HTCIA, IACIS, SANS), *responsibility to client* (ASDFD, CDFS, HTCIA, IACIS) and *lawful compliance* (HTCIA, IACIS, SANS). Considered in conjunction with the similar comparison including the AAFS, ABC, and CAC code given in (Melson, 2012), the impression holds that the US-based societies are more explicit in distinguishing the “threats to the professional misconduct” (Barnett, 2001)

while remaining coherent with the *sine qua non* codes for the forensic practice (except for the ISFCE code, which potentially can serve as an additional reference of the professional regulation). Relating to the main imperative, Table 2 suggests that explicit precepts are additionally needed in detailing what the expert witness role entails, what constitutes conflict of interest and how should be resolved, the manner in which the reports need to be tailored as to establish legal compliance and the professional stakes in the relationship with the service consumers.

3.2 A Comparison in Respect to Scientific Method

Table 3 brings the comparison relative to the *scientific method* underpinning the digital forensics investigative process. The better relative explicitness mainly of the DFCB and CI codes against the international ones draws a justification in the precedent nature of the criminal justice system in the US, where the federal rules of evidence (Federal Judicial Center, 2011) tend to frequently cause dilemmas about the juristic conditioning of the forensic products due to incorrect interpretation precedent to different cases and under different circumstances (Ham & Davidoff, 2012). Notwithstanding this fact, the general impression is that the interpretation bias needs dedicated section as to explicate the threat and the consequences in diminishing both the evidentiary value and the credibility of the profession at all. Same conclusion holds for the investigative methodological path to which the forensic process standardization guidelines (International Standardization Organization, 2012, 2014b) might serve as a useful reference. A segment of immediate attention is the one concerning the proficiency maintenance among the professionals. Since the societies offer different certification and training courses in digital forensics, at least a

general frame on the professional training and education needs to detail the necessary knowledge units for each of the digital forensics subdomains in order to harmonize the content

covering various educational tracks. A good starting point on this topic can be found in (Bird & Cheah, 2014; Lang, Bashir, Campbell, & DeStefano, 2014).

Table 1

Explicitness of the codes of ethics relevant to the digital forensics practice

Organization	Number of provisions		
	1-10	11-20	21 or more
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 Specialists (CDFS)	✓		
Cybersecurity Institute (CI)		✓	
Digital Forensics Certification Board (DFCB)			✓
EC-Council (ECC)		✓	
High Technology Crime Investigation Association (HTCIA)	✓		
International Association of Computer Investigation Specialists (IACIS)	✓		
SANS Institute (SANS)	✓		
International Society of Forensic Computer Examiners (ISFCE)			✓

3.3 A Comparison in Respect to Examination and Conclusion

In regards to the *examination* and *conclusion* comparison given in Table 4, most of the domestic codes—in contrast to the international ones—only prescribe use of proven and accepted methods, without explicit notion on what is considered under “sufficient examination and interpretation” (Saks, 1989). A good alternative in striking balance between the codes’ flexibility and explicitness when it comes to examination and interpretation are the guidelines provided by the International Standardization Organization (2014a), complemented with the concept of “conclusions, qualifications and certainty conveyance” of the practical investigative

methodology using the *likelihood-ratio* or *certainty scale*, expressing the “degree of support for one of the alternative hypotheses relative to the interpretation of the evidentiary weight” (Association of Forensic Science Providers, 2009; Casey, 2011). The regulation might also extend towards expressing the investigative results, given the extensive set of potential outcomes and the threat of data alternation or elimination especially in environments with a high degree of volatility. Considering also the threat to the resultant interpretations imposed by the anti-forensics actions (Simmons, Jones, & Simmons, 2011), the regulative aspects might provide the contours of an investigative strategy that incorporates both the hypothesis-based approach (Carrier, 2006; Casey, 2011) and the

often necessary real-time digital forensics triage (Roussev, Quates, & Martell, 2013). By abstracting the characteristics of the investigative strategy, the deviations from the accepted norms identified with the interpretative bias, contingency and favoritism can be more easily recognized and eliminated.

3.4 A Comparison in Respect to Adversary Presentation

When it comes to adversary presentation, digital forensics codes of ethics prescribe only *actions for disclosing exculpatory findings when the prosecution is not going to make disclosure* and permit *giving opinions on matters not subjected to formal examination* (except CI's code, which explicitly prohibits *leaving false impressions in the minds of fact finders*), as depicted in Table 5. Compared to the respective regulation in the other forensic sciences (Melson, 2012), digital forensics organizations have not prescribed any similar actions in *conveying the findings in clear and understandable manner, implanting false impressions in assisting case contestants* and *giving more weight to the testimony than is due*. In improving the quality of the delivered products by mastering the compliance with the Dauber and Lorraine models (Federal Rules of Evidence, 2011), these segments certainly have the catalyzing effect on the maturation of the operative investigation process (Saleem, Popov, & Bagilli, 2014). Therefore, the regulative adaptation of postulates outlining the courtroom presentation of the investigative findings (Smith & Kenneally, 2008) is an utmost objective for the digital forensics societies, which in turn also contributes to the central imperative in that it reveals the specific arguments used in presenting and juristically communicating non-physical evidentiary data.

3.5 A Comparison in Respect to General Practice and Profession

The comparison focused on the general practice and profession provided in Tables 6 and 7, respectively, suggests that most of the digital forensics codes of ethics have disparate approaches towards the professional obedience and professional improvement. Except DFCB and CI, none of the others has addressed the *re-examination of the peer practitioners* and action for *taking undue credit*. Only CDFS code explicitly addresses the aspects of *professional misconduct reporting* and expelling of *members convicted of felonies* while none of the codes requires reporting of invalid and unreliable methods or any *discoveries* or *developments* from the society members. On the good side when it comes to the development of the profession, CDFS, CI, DFCB ECC and HTCIA clearly *encourage cooperation in improvement through research*. Whilst the research initiative certainly is a good attribute that shall be translated in the general forensics practice, the absence of prescripts regulating the professional misconduct can have negative effect not just on the credibility of the societies and their role within the criminal justice system, but moreover can hinder the very determination for discipline development. As to overcome this drawback and provide an enforceability reference, digital forensics communities have to first define which actions qualify as misconduct of the professionals investigating computer-related/cybercrimes—for which a useful reference can be found in the general forensics and information security arena (Barnett, 2001; Greenwald, Snow, Ford, & Thieme, 2008)—and then incorporate provisions that will protect themselves from both intentional and unintentional wrongdoing.

3.6 A Comparison in Respect to Additional Provisions

As in the other forensics branches (Melson, 2012), the field of digital forensics identifies the

practice with additional provisions in respect to the evidence integrity, confidentiality and lawful compliance, as depicted in Table 8. Being extremely fragile in its very nature (Saleem et al., 2014), digital evidence *integrity preservation* is expected to be leading postulate of the associated practice, though not all of the societies (i.e., ASDFD, CDFS and IACIS) explicitly require to guide the investigative operations in this manner. The same holds true for the *independence* and *impartibility* aspects of the professional conduct, where only DFCB, ECC and SANS have separate prescripts confronting the interpretation bias. Knowing that these attributes are presupposed to be maintained by every serious digital forensics professional, their central place within the code of ethics should indisputably be guaranteed. These aspects of the professional conduct—as incorporated also in the federal rules of evidence (Solomon & Hackett, 1996)—is what accents the credibility of the digital forensics societies within the criminal justice system (Smith & Kenneally, 2008), thus a further consolidation is needed in this context. In addition, Table 8 also suggests that only half of the US-based societies (ASDFD, CDFS, and CI) and none of the international ones require from their members not to impose *contingency fees* for their service, corroborating the same trend of non-uniformity depicted in Table 2 in the case of conflict of interest, lawful compliance, and responsibility to clients.

4. ENFORCEABILITY OF THE DIGITAL FORENSICS CODES OF ETHICS

Recalling the main purpose of the professional regulation, digital forensic societies are expected to have separate by-laws that regulate the actions taken upon professional

misconduct². However, the mere existence of an *enforceability* policy and processes—focused on the investigation of an alleged ethical code’s violations (Melson, 2012, p. 115)—does not imply that their execution, i.e. the actual *enforcement*, is a course of action rigidly followed by the forensics societies. While the purpose of the enforcement is mainly to “emphasize the importance of the ethical decision making in practice, promote the ends of justice and protect the reputation of the association” (Melson, 2012), the associated actions of collecting evidence supporting the misconduct, determining an actual violation of the code of ethics, hearing and imposing sanctions, and handling reinstatement procedures necessitates executional capacity that very few forensics organizations possess. The reason for missing an actual link between the enforceability and the enforcement within the forensics arena might be traced to two main factors. First, the overall process for instantiating and processing a case of professional misconduct (including the right to appeal for the accused parties) can be costly and overburdening process for most of the societies, given their limited financial and human resources. Second, even if such a proceeding is brought to a conclusion, the determination of the appropriate sanction is a difficult task, since the forensics organization needs to establish balance between the assuring of high standards for professional behavior and the ability to withstand the consequences of the imposed sanctions. Afraid of a negative impact in terms of financial loss, reputation damage or similar, many organizations are reluctant to expulse or decertify their members, go public with such matters, or take actions to reprove the violating member.

² An extensive elaboration on all the actions considered as forensics misconduct is given in (Goodstein, 2002).

Not surprisingly, most of the assessed digital forensic organizations here have not established strict by-laws as of the enforceability of their codes of ethics, despite that most have covered a substantive set of actions “qualifying as serious deviations from the accepted practice” (Goodstein, 2002). Except CDFS, SANS and ISFCE—which have made enforcement arrangements only respective to the *decertification* or *license revocation*—the represented digital forensics community is not strongly advocating a sanctioning course of action in “gatekeeping the rightful practice” (Goodstein, 2002; Melson, 2012). The abovementioned rationale indeed holds true in this case—due to their small size, limited recourses and not yet accumulated experience in recognizing the complexity of the professional misconduct and appropriate dealing with it, digital forensics societies are either not taking any actions at all or limit themselves only to revoking the license or certificate of the violating member. Building a full professional gatekeeping capacity follows a long process of maturation as evidenced with the actual cases of ethical misconduct litigations (Bowen, 2009; Melson, 2012), so it is likely to expect that the relatively young digital forensics community at this point counters the unethical behavior only by the persuasive nature of the regulating codes of ethics and peer practitioner pressure (as suggested in Table 7). However, the future actions in concordance with the other forensics communities as recommended by the Committee on Identifying the Needs of the Forensics Sciences Community (2009) should develop policies and procedures detailing the overall process of enforcement, as in the other forensic institutions, for example the AAFS, ABC, and CAC (Barnett, 2001; Bowen, 2009).

5. CONCLUSION

Aligning the perspective on the digital forensics professional conduct regulation with

the recommendation of the Committee on Identifying the Needs of the Forensics Sciences Community (2009), several observations deserve immediate attention. Regarding the main prescripts for professional behavior, the domestic digital forensic societies have to capitalize the experience of their peer organizations (Barnett, 2001) in detailing the conflict of interest together with the profile of digital forensics expert witness and its role within the criminal justice system, which in turn brings them the leading position in establishing the professional standards for the digital forensics practice on an international level. This is equally valid for the formal abstraction of the investigative methodology and the importance of the continuous proficiency improvement in eliminating the interpretation bias, producing highly admissible forensics products, and communicating them clearly in the courtroom. As of the general practice and profession, the forensics consolidation might in fact benefit from the digital forensics codes of ethics, given that the community itself is explicitly encouraging improvement of the practice through research cooperation. However, in a reverse direction, digital forensic societies need to fortify their position on the independence and impartiality, and the financial aspects in providing the professional service similarly as their peers.

The enforceability and actual enforcement of the instituted norms are tightly related to the varieties and specificities of the representative codes of digital forensics professional behavior. Although non-uniformly, digital forensics societies are aware of the importance of having policies and procedures for handling professional misconduct, which mainly impose sanctions such as license revocation or decertification. Still, digital forensics community is in the process of building enforcement capacity in fully

responding to the threat of professional deviations. Nonetheless, being this a long and resource consumptive engagement, digital forensics discipline has the benefit of the relative experience from the other forensic peers in extending and augmenting the professional regulation (Bowen, 2009; Melson, 2012). In sum, digital forensics maintains a relatively good position respective to the imperative for working under unified forensics code of ethics. Certainly, several segments can be subjected for further improvements, but the set of references and experiences from the other forensic sciences—as pointed through the forgoing sections—provide a good starting point in extending the research commitment in this direction.

REFERENCES

- American Academy of Forensic Sciences. (2013). *Code of Ethics and Conduct. AAFS Bylaws*. Retrieved from <http://www.aafs.org/aafs-bylaws#Art2>
- American Board of Criminalistics. (2013). *Rules of Professional Conduct. ABC Bylaws*.
- Association of Forensic Science Providers. (2009). Science and Justice Standards for the formulation of evaluative forensic science expert opinion. *Science & Justice*, 49(3), 161-164. doi:10.1016/j.scijus.2009.07.004
- Barnett, P. D. (2001). *Ethics in Forensic Science: Professional Standards for the Practice of Criminalistics*. Boca Raton, FL: CRC Press.
- Bassett, R., Bass, L., & Brien, P. O. (2006). Computer Forensics: An Essential Ingredient for Cyber Security. *Journal of Information Science and Technology*, 3(1), 22-32.
- Bird, R., & Cheah, M. (2014). The Development of Constructive Alignment in Activity Led Learning and Assessment of Digital Forensics. In *Proceedings of the Western Canadian Conference on Computing Education*, 1-6. New York: ACM Press.
- Bowen, R. (2009). *Ethics and the Practice of Forensic Science (International Forensic Science and Investigation)*. Boca Raton, FL: CRC Press.
- California Association of Criminalists. (2010). *Code of Ethics* (Vol. 1985). Retrieved from <http://www.cacnews.org/membership/handbook.shtml>
- Carrier, B. (2006). *A hypothesis-based approach to digital forensic investigations*. Purdue University. Retrieved from <http://search.proquest.com/docview/305266774?accountid=13360>. (305266774).
- Casey, E. (2011). *Digital Evidence and Computer Crime*, 3rd ed. Waltham, MA: Elsevier.
- Committee on Identifying the Needs of the Forensics Sciences Community. (2009). *Strengthening Forensic Science in the United States: A Path Forward*. Washington D.C. Retrieved from <https://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf>
- Consortium of Digital Forensic Specialists. (2013). *Code of Ethics*. Retrieved from http://www.cdfs.org/documents/CDFS_Code_of_Ethics_January_2013.pdf
- Cybersecurity Institute. (2013). *Code of Ethics and Conduct. Code of Ethics and Conduct*. Retrieved from <http://www.cybersecurityinstitute.biz/training/ethicsconduct.htm>
- Davis, M. (1991). Thinking Like an Engineer: The Place of a Code of Ethics in the Practice of a Profession. *Philosophy and Public Affairs*, 20(2), 150-167.
- Digital Forensics Certification Board. (2008). *Code of Ethics and Standards of Professional Conduct*. Retrieved from <http://www.dfcb.org/certification.html>
- EC-Council. (2013). *Code of Ethics. Code of Ethics*. Retrieved from <https://www.eccouncil.org/Support/code-of-ethics>
- Federal Judicial Center. (2011). *Reference Manual on Scientific Evidence*, 3rd ed. Washington D.C.

- Federal Rules of Evidence. (2011). Rule 402. General Admissability of Relevant Evidence. Retrieved from http://www.law.cornell.edu/rules/fire/rule_402
- Gay, J. R. (2012). *A Code of Conduct for Computer Forensic Investigator*. University of East London.
- Goodstein, B. D. (2002). Scientific Misconduct. *Academe*, 88(1), 28-31.
- Greenwald, S. J., Snow, B. D., Ford, R., & Thieme, R. (2008). Towards an Ethical Code for Information Security? In *Proceedings of the 2008 workshop on New security paradigm*, 75-87.
- Ham, J., & Davidoff, S. (2012). *Network Forensics: Tracing Hackers Thorough Cyberspace*. Upper Saddle River, New Jersey: Prentice Hall.
- Harrington, S. L. (2011). Collaborating with a Digital Forensics Expert: Ultimate Tag-Team or Disastrous duo? *William Mitchell Law Review*, 38(1), 353-396.
- High Technology Crime Investigation Association. (2013). *Code of Ethics. Code of Ethics and Bylaws*. Retrieved from <http://www.htcia.org/code-of-ethics-bylaws/>
- International Association of Computer Investigation Specialists. (2013). *Code of Conduct. IACIS membership*. Retrieved from <http://www.iacis.com/membership/overview>
- International Standardization Organization. (2012). ISO/IEC 27037:2012 guidelines for identification, collection, acquisition and preservation of digital evidence. Retrieved from <http://www.iso.org/>
- International Standardization Organization. (2014a). ISO/IEC 27042 -- Guidelines for the analysis and interpretation of digital evidence. Geneva, Switzerland. Retrieved from <http://www.iso.org/>
- International Standardization Organization. (2014b). ISO/IEC 27043 -- Incident investigation principles and processes. Geneva, Switzerland. Retrieved from <http://www.iso.org/>
- Lang, A., Bashir, M., Campbell, R., & DeStefano, L. (2014). Developing a new digital forensics curriculum. *Digital Investigation*, 11(1), S76-S84. doi:10.1016/j.diin.2014.05.008
- Melson, K. E. (2012). Codes of Ethics in Forensic Science Societies: The Organizational Parameters of Morality and Conduct. In J. C. Upshaw Downs (Ed.), *Ethics in Forensic Science*, 81-135. New York: Elsevier.
- Roussev, V., Quates, C., & Martell, R. (2013). Real-time digital forensics and triage. *Digital Investigation*, 10(2), 158-167. doi:10.1016/j.diin.2013.02.001
- Saks, J. (1989). Prevalence and Impact of Ethical Problems in Forensic Science. *Journal of Forensic Sciences*, 34(3), 772-793.
- Saleem, S., Popov, O., & Bagilli, I. (2014). Extended Abstract Digital Forensics Model with Preservation and Protection as Umbrella Principles. *Procedia Computer Science*, 35, 812-821. doi:10.1016/j.procs.2014.08.246
- SANS Institute. (2013). *Code of Ethics. Global Information Assurance Certification*. Retrieved from <http://computer-forensics.sans.org/certification/ethics>
- Simmons, C., Jones, D., & Simmons, L. (2011). A Framework and Demo for Preventing Anti-Computer Forensics. *Issues in Information Systems*, XII(1), 366-372.

- Smith, F. C., & Kenneally, E. E. (2008).
Electronic Evidence and Digital Forensics
Testimony in Court. In J. J. Barbara
(Ed.), *Handbook of Digital and Multimedia
Forensic Evidence*, 1st ed., 103-132.
Totowa, New Jersey: Humana Press Inc.
- Solomon, S. M., & Hackett, E. J. (1996).
Setting Boundaries between Science and
Law: Lessons from Daubert v. Merrell Dow
Pharmaceuticals, Inc. *Science, Technology
& Human Values*, 21(2), 131-156.
- The American Society of Digital Forensics and
eDiscovery. (2013). *Code of Ethics. Ethics
and Code of Conduct*. Retrieved from
<https://asdfed.com/domain3>
- The International Society of Forensic
Computer Examiners. (2013). *Code of
Ethics and Professional Responsibility.
Certified Computer Examiner -- High
Forensic Standards*. Retrieved from
<http://www.isfce.com/ethics2.htm>

APPENDIX

Table 2

Sub-categorization of the digital forensics codes of ethics in respect to the ethical considerations. Partially adapted from (Melson, 2012; Saks, 1989)

Ethical considerations	Digital Forensics Organization								
	ASDFD	CDFS	CI	DFCB	ECC	HTCIA	IACIS	SANS	ISFCE
Professional diligence	✓	✓	✓	✓		✓	✓	✓	✓
Competency	✓	✓	✓	✓	✓	✓	✓	✓	✓
Qualification	✓	✓	✓	✓	✓	✓		✓	✓
Examination and analysis	✓	✓	✓	✓	✓	✓	✓	✓	✓
Testimony	✓	✓		✓					✓
Conflict of interest	✓	✓	✓	✓	✓			✓	✓
Reporting	✓	✓	✓	✓		✓	✓		✓
Financial stakes	✓	✓	✓						
Responsibility to client			✓	✓	✓			✓	✓
Lawful compliance	✓	✓	✓	✓	✓				✓

Table 3

A comparison of the digital forensics codes of ethics provisions relating to the scientific method

Scientific method	Digital Forensics Organization								
	ASDFD	CDFS	CI	DFCB	ECC	HTCIA	IACIS	SANS	ISFCE
Should be unbiased, minimum anticipation of what results should be, maintain rigid impartiality	✓			✓			✓	✓	✓
Not bolster conclusions by using unwarranted and superfluous tests		✓	✓	✓			✓		✓
Not use “secret” methods or processes, not open to scrutiny			✓	✓					
Insist upon representative and reliable materials on which to perform examination			✓	✓			✓		✓
Not use unreliable, unproven, or discredited procedures			✓	✓	✓		✓		
Keep abreast of new developments	✓	✓	✓	✓		✓			
Keep skills sharp, participate in proficiency testing	✓	✓	✓	✓					

Table 4

A comparison of the digital forensics codes of ethics relating to the examination and conclusion

Examination and conclusion	Digital Forensics Organization								
	ASDFD	CDFS	CI	DFCB	ECC	HTCIA	IACIS	SANS	ISFCE
Should use proven and accepted methods		✓	✓	✓	✓		✓		
Should do sufficiently thorough examination			✓	✓			✓		✓
Should not knowingly distort tests or interpretations of them			✓	✓					
Should not go beyond own competence		✓	✓	✓		✓		✓	
Where results are capable of alternative interpretations, not select the one favoring the side by which he or she is employed	✓			✓			✓	✓	✓

Table 5

A comparison of the digital forensics codes of ethics relating to the adversary presentation

Adversary presentation	Digital Forensics Organization								
	ASDFD	CDFS	CI	DFCB	ECC	HTCIA	IACIS	SANS	ISFCE
Be available for pre-trial interviews with both prosecution and defense attorneys									
Disclose exculpatory findings to the court if it appears prosecution is not going to make disclosure	✓		✓	✓			✓		✓
Not give opinions on matters not subjected to formal examination	✓		✓	✓			✓		✓
Not leave false impressions in the minds of fact finders			✓						
Not testify in a way that wins it more weight than it is due									
Should see to it that the court understands the evidence as it is									
Not assist the contestants in a case in implanting false impressions									
Not confuse or conceal concepts from fact finders									

Table 6

A comparison of the digital forensics codes of ethics relating to the general practice

General practice	Digital Forensics Organization								
	ASDFD	CDFS	CI	DFCB	ECC	HTCIA	IACIS	SANS	SFCE
Should be willing to re-examine evidence submitted by another forensic scientist; however, should try to resolve discrepancy before case goes to trial;			✓	✓					
Members convicted of felonies or other crimes can be expelled		✓							

Table 7

A comparison of the digital forensics codes of ethics relating to the profession

Profession	Digital Forensics Organization								
	ASDFD	CDFS	CI	DFCB	ECC	HTCIA	IACIS	SANS	ISFCE
Should make new discoveries and developments widely known									
Should cooperate in improvement through research		✓		✓	✓	✓			
Direct attention to methods which appear invalid or unreliable									
Refrain from seeking personal publicity						✓			
Should not take undue credit			✓	✓					
Bring to the attention forensic scientist who has committed serious or frequent infractions		✓							

Table 8

A comparison of the digital forensics codes of ethics - additional provisions

Additional provisions	Digital Forensics Organization								
	ASDFD	CDFS	CI	DFCB	ECC	HTCIA	IACIS	SANS	ISFCE
Treat evidence with care to maintain integrity			✓	✓	✓	✓		✓	✓
Confidentiality	✓	✓	✓	✓	✓	✓		✓	✓
Maintain attitude of independence and impartiality to inspire confidence by public				✓	✓			✓	
Contingency fees	✓	✓	✓						

