



Annual ADFSL Conference on Digital Forensics, Security and Law

2006
Proceedings


Paper Session IV: Toward Understanding Digital Forensics as a Profession: Defining Curricular Needs (**Research in Process **)

Michelle Wolf
Central Connecticut State University

Alan Shafer
Central Connecticut State University

Michael Gendron
Central Connecticut State University

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

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

Scholarly Commons Citation

Wolf, Michelle; Shafer, Alan; and Gendron, Michael, "Paper Session IV: Toward Understanding Digital Forensics as a Profession: Defining Curricular Needs (**Research in Process **)" (2006). *Annual ADFSL Conference on Digital Forensics, Security and Law. 2.*
<https://commons.erau.edu/adfsl/2006/session-iv/2>

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.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



***** Research in Process *****

Toward Understanding Digital Forensics as a Profession: Defining Curricular Needs

Michelle Wolf

Central Connecticut State University

Alan Shafer

Central Connecticut State University

Michael Gendron

Central Connecticut State University

ABSTRACT

This research paper presents research in process which attempts to define the common body of knowledge (CBK) of digital forensics. Digital forensics is not well defined nor does it have a generally accepted CBK. The first three phases of completed research, in a four-phase research process are discussed. The early results have created a preliminary CBK, and final validation is underway.

1. INTRODUCTION

The FBI estimates that cyber-crime in the United States costs more than \$10 billion per year, with up to 80% of the losses unreported, in part because law enforcement agencies cannot respond effectively to these kinds of incidents (Holsapple 2004). A key challenge of investigating computer crime is that the computer is both a principal instrument of the criminal activity and a key source of evidence about that activity. Digital evidence (i.e., a file on a disk drive), because it is less tangible than physical evidence (i.e., a print-out of the file), presents special challenges to the criminal investigator. Finding, authenticating, and preserving digital evidence, and documenting the chain of custody in a way that is legally admissible in a court of law, are all activities that the field of digital forensics encompasses. However, that field needs better definition.

The digital forensic(s) (DF) analyst is trained to copy and examine digital data in ways that leave the original data intact. They are trained to maximize the amount of information they can recover during an investigation, not only by searching files left in place by suspects, but also by checking for residual traces of files that were erased by the users, maximizing the amount of relevant information retrieved during the investigation (Feldman et al. 1998). However, the training received by these analysts is not well defined. This paper explores the concepts that underpin DF and reports on research that creates a conceptual framework for professional training in this field. It reports on research in process that can be used to give definition to this emerging topic as well as to create appropriate curriculum.

Our approach to determining a conceptual framework for DF parallels the work that created a framework for data quality (Wang et al. 1996). Our research uses a similar methodology for explicating the professional knowledge which defines DF by:

- Identifying DF attributes via an intensive review of digital forensics related programs and courses offered in the United States at technical schools, colleges, and universities;
- Reducing the attributes to a smaller number of DF dimensions;
- Categorizing the dimensions into a conceptual framework for digital forensics.

2. IS DIGITAL FORENSICS A PROFESSION?

A profession has four defining hallmarks:

- a durable domain of human concern;

- a codified body of conceptual knowledge;
- a codified body of practices – embodied knowledge including competence;
- standards for competence, ethics and practice. (Denning 2001)

In today's technology-driven world, DF is clearly a ***durable domain of human concern***. In fact, the use of computers in criminal activity is a growing concern; digital evidence is less tangible than physical evidence and presents special challenges to criminal investigators. DF involves finding, authenticating, and preserving digital evidence, and documenting the chain of custody in a way that is legally admissible in court. The socio-legal and technical nature of DF support the necessity of a creating a framework for the DF profession (Feldman et al. 1998). However, since DF is not well defined, the questions of whether it is a profession is fuzzy, at best – there appears to be no universally accepted ***codified body of conceptual knowledge, codified body of practices, or standards for competence, ethics, and practice***. This research attempts to create a ***codified body of conceptual knowledge*** that can get us another step closer to recognition of DF as a profession.

3. DIGITAL FORENSICS EDUCATIONAL OFFERINGS

DF, as a recognizable skill set has emerged fairly recently, thus the common body of knowledge is not well established. DF education is offered at many levels, from tool-specific technical courses to graduate degrees. It is interdisciplinary - that is, the education is a combination of several fields such as criminal justice, law, network security, etc. Whether DF is a profession or discipline in the academic sense is open to question. A common conceptual approach is needed for DF to be recognized as a profession and accepted in the courts (Rogers et al. 2004). We believe that DF is a profession that is in need of an accepted ***common body of conceptual knowledge***. The study reported in this paper is being undertaken to uncover that knowledge and to create a categorical conceptual framework that gives substance to it

4. METHODS

This research consists of four phases. To date, phases one through three are completed. The phases are:

- **Phase 1** - Review of existing courses and content, creating DF attributes
- **Phase 2** - Collapse the DF attributes in dimensions and prepare statements for VCS
- **Phase 3** – Create a preliminary conceptual framework
- **Phase 4** – Validate the preliminary conceptual framework (in process)

In order to simplify discussion of the methodology for this study, the following terms are used:

- **Attribute** - concepts uncovered during the review of courses and content
- **Dimensions** - attributes that have be grouped together since they are intuitively similar
- **Statements** – dimensions that seem to be in similar *a priori* knowledge domains

5. PHASE 1 - REVIEW OF EXISTING COURSES AND CONTENT

As a first step in constructing a preliminary conceptual framework for digital forensics, 89 attributes were uncovered from college catalogs and college/technical course descriptions. Organizations were selected in two ways:

- Academic institution were identified through an online search service, ***College Source Online*** (www.collegesource.org). They bill themselves as “the worldwide leader in college information resources.”

- Additional on-line searches for technical and non-academic training programs were conducted using Google

The only keyword used for the searches was computer forensics. This was done because, after initial preliminary searching, computer forensics seemed to best capture the type of results that the researchers were attempting to retrieve and using just one keyword simplified the searches.

Phase 1 resulted in 89 attributes (Table 1 – Digital Forensics Attributes), yielded from 19 different academic and non-academic organizations. The dimensions were gleaned from the organizations online course and program catalogues. Our review included:

- 1 organization that did only tool-based training;
- 5 organizations that offered professional certifications;
- 3 associate degree granting schools;
- 2 Bachelors granting schools; and
- 8 schools offering graduate degree programs.

6. PHASE 2 - COLLAPSE THE ATTRIBUTES IN DIMENSIONS AND PREPARE STATEMENTS FOR VCS

The 89 attributes that were uncovered in Phase 1 were somewhat vague and overlapping. There were intuitively apparent relationships between the attributes that led the researchers to collapse them. A three-step method was employed to create the statements:

- attributes were collapsed because they were so similar as to apparently belong to the same *a priori* knowledge domain
- attributes were eliminate if they were extremely vague and a more representative attribute already existed (in all cases more representative ones were on the list);
- attributes which were grossly overlapping were collapsed were grouped together.

The result was a set 19 statements and associated dimensions that appropriately represent the intent of the 89 attributes. Some dimensions were added to the statements to maintain integrity and to be true to the original content. Each statement consists of a statement label created by the researchers to succinctly describe the content of the statement, followed by a list of dimensions which describe the statement. During statement creation, no more than 4 attributes/dimensions could be assigned to any one statement.

7. PHASE 3 – CREATE A PRELIMINARY CONCEPTUAL FRAMEWORK

During Phase 3, a preliminary conceptual framework was created. This framework was created by grouping statements together into like categories using visual card sorting (VCS). The goal of VCS is to discover latent structure in an unsorted listed of statements or ideas (Bevan 2006). VCS is appropriate to show how individuals categorize concepts within particular knowledge domains. Using VCS generate similarity matrices by having the subject identify salient categories and identifying the pattern of statement assignment to them (Budwar 2000). The researchers did multiple VCS passes in order to create the preliminary conceptual framework – the preliminary framework was not considered finalized until all researchers agreed to its structure and content. Once all the dimensions were properly placed, the categories were named and the preliminary conceptual framework was complete (Figure 1 - Digital Forensics Preliminary Conceptual Framework).

Table 1 - Digital Forensics Attributes

Access Control Systems and Methodology	Introduction to Computer Forensics and the Law
Access Controls	Introduction to Digital Forensics (4th Amendment search and seizure, media imaging, hard drive/storage device investigation, network attacks, investigating Windows and Unix systems, security through forensics)
Administration	Introduction to Forensic Technology
Advanced Computer Forensics (UNIX, TCP/IP, firewalls, network scanning and tools, etc.)	Intrusion Detection (includes lab with Smartwatch or other industry software)
Analysis of Digital Media	Intrusion Detection Forensic Analysis
Application Development and Security; Operations Security	Intrusion detection systems
Applied Cryptography; Security Risk Management	Investigating High Technology Crime (privacy, copyright laws, how to conduct a forensic examination, etc.)
Assessment; Information Systems Forensics	Investigation of pc workstations, servers; and PDAs; media analysis
Audit and Monitoring	Investigative Interviewing
Business Continuity Planning	Law, Investigations and Ethics
Collection and analysis of digital evidence	Malicious Code/Malware
Computer Forensic Technology	Methods used to hide or disguise digital information
Computer Forensics	Network Security
Computer Forensics (includes lab with Expert Witness or other industry software)	Network, & Internet Security
Computer Forensics (operating systems, file systems, disk cloning, forensic tools, etc.)	Physical Security
Computer Forensics I	Principles of information security
Computer Forensics II	Procedures for the admissibility of evidence
Computer Systems and Networks	Profiling
Criminal Activities & Investigative Procedures	Response and Recovery
Criminal Investigation	Risk
Criminal Law I	Search and Seizure
Criminal Law II	Security Architecture and Models
Cryptography	Security Management Practices
Cyber crime	Security System Design and Analysis
Data Communications	Seizure and Examination of Computer Systems; Computer Forensics II
Economic Crime Investigation	Stenography
Ethics, Privacy & Digital Rights	Techniques of intrusion detection
Forensic Accounting	Technology Issues in Computer Forensics Investigation (wireless and mobile communications, security aspects of software engineering, database management, etc.)
Forensic Collection and Examination of Digital Evidence	Telecommunications
Forensic Internship	The criminology of cyber-crime
Forensic Technology	Topics in Forensic Science
Foundations of Information Assurance	White Collar Crime
Gathering and preserving evidence in ways that ensure its admission in courts	
Hidden or deleted files	
Illegal software	
Information extraction from digital devices	
Intelligence Analysis	
Internet Vulnerabilities	

Table 2 - Digital Forensics Statements

Statements	Number of Dimensions
Statement Label: dimension 1, dimension 2, etc.	
Accounting: General Accounting; Forensic Accounting	2
Computer Forensics Theory: Disk Cloning; File Systems; Forensic Tools, Etc.; Technology Issues In Computer Forensics Investigation	4
Criminal Law: Computer Forensics Law; Cyber Crime; Ethics, Privacy And Digital Rights	3
Criminology: Criminology Of Cyber Crime; Economic Crime Investigation; Profiling	3
Cyber-Criminal Procedures: Computer Systems Seizure And Examination; Evidence Admissibility Procedures; Evidence Gathering and Preservation	3
Digital Media Analysis: Digital Device Information Extraction; Digital Evidence Collection And Analysis; Hidden Or Deleted Files	3
General Business: Business Continuity Planning; Human Resource; Introduction To Business	3
Illegal Software Activity: Malicious Code/Malware; Stegnography	2
Infrastructure Security: Access Control Systems; Internet Security; Physical Security	3
Intelligence Analysis: Analysis Of Massive Volumes; Multilingual And Multimedia Data	2
Internship/Practicum: Assessment; Forensic Internship; Information Systems Forensics	3
Introduction To Networking: Computer Systems And Networks; Telecommunications	2
Intrusion And Vulnerabilities: Internet Vulnerabilities; Intrusion Detection Methods And Techniques; Intrusion Detection Systems; Risk	4
Investigative Procedures: Conducting A Forensic Examination; Criminal Activities; Investigation Of Desktop Devices, Servers, And PDA's	3
Legal Topics: 4th Amendment; Investigations And Ethics; Law (privacy, copyright)	3
Operational Security: Operations Security; Response And Recovery; Security Risk Management	3
Security Practices: Audit And Monitoring; Security Management Practices	2
Security Theory: Information Assurance Foundations; Information Security Principles; Security System Analysis And Design	3
Software Security: Application Development Security; Applied Cryptography; Operating Systems	3
TOTAL DIMENSIONS	54

8. PHASE 4 – VALIDATE THE PRELIMINARY CONCEPTUAL FRAMEWORK (IN PROCESS)

The final conceptual framework will be created using a closed VCS to validate the preliminary framework created in Ohase-4. A convenience sample from both the ISWORLD and JDFSL ListServe will be selected for this purpose. Each ListServe will be sent a request for subject participation. The request will contain URL. By visiting the URL, subjects will receive instruction (Figure 2 - Instruction Screen), a small amount of demographic information will be collected (Figure 3 - Demographics Screen), and then subjects will be asked to complete the closed VCS exercise (**Figure 4 - VCS Screen**). The VCS is considered “closed” because the categories are pre-labeled in accordance with the preliminary conceptual framework. Subjects will be given the 19 statements and will be asked to sort the dimensions into the pre-named categories, as was done in the creation of the data quality framework (Wang et al. 1996). This will validate the researchers’ preliminary framework. Some dimensions/statements may be moved based on the results of the VCS. Results of the visual card sort exercise will be analyzed using the Chi Squared technique to compare the expected results that were determined in the Preliminary Conceptual Framework to the actual results that were received from each user.

9. DISCUSSION

Ways of comparison – Like Wang and Strong the researchers used both an intuitive and the empirical approach to create the preliminary conceptual framework. The collection of the attributes, and the proposed validation of the preliminary conceptual framework use an empirical approach, while the collapsing of attributes into dimensions and statements use an intuitive one. These approaches seem well suited to the tasks to be performed. These approaches were further buttressed by using Denning’s paradigm as a way to define a profession.

The descriptive survey of digital forensics education programs conducted by the researchers during the summer of 2004 disclosed a relatively wide variety of digital forensics instruction. Some of the potential reasons for this are:

- DFs relative infancy as a field of study;
- the interdisciplinary nature of the educational offerings for DF;
- the fact DF education is offered at many different levels including tool-based courses, professional certificates, undergraduate degrees, and graduate degrees.

This review uncovered differences, which leave the expertise of DF analysts open to question; it is at least unpredictable, and at best variable. Certificate programs are often vendor-specific, and academic programs vary in their depth, rigor, and approach to the subject. The degree of disparity in the approach to and subject matter of digital forensics education raises the question- is digital forensics a discipline/profession in an academic sense and if so, how should it be defined? This study sets out to do start that definitional work.

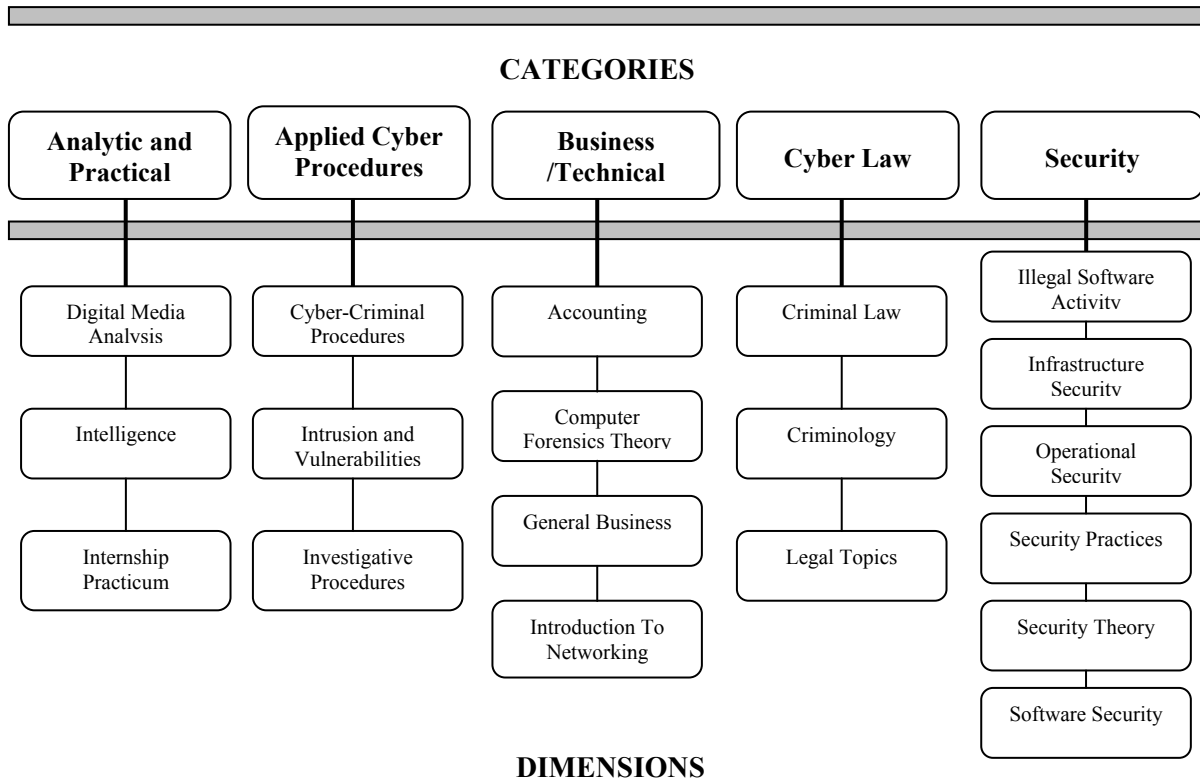


Figure 1 - Digital Forensics Preliminary Conceptual Framework



Figure 2 - Instruction Screen

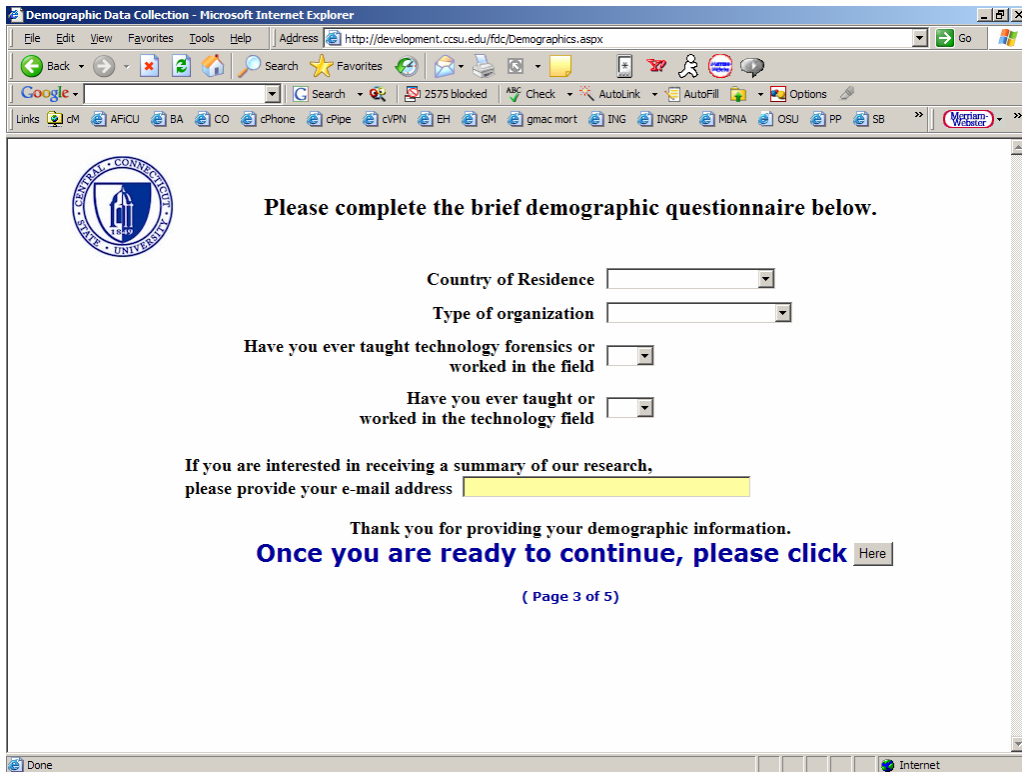


Figure 3 - Demographics Screen

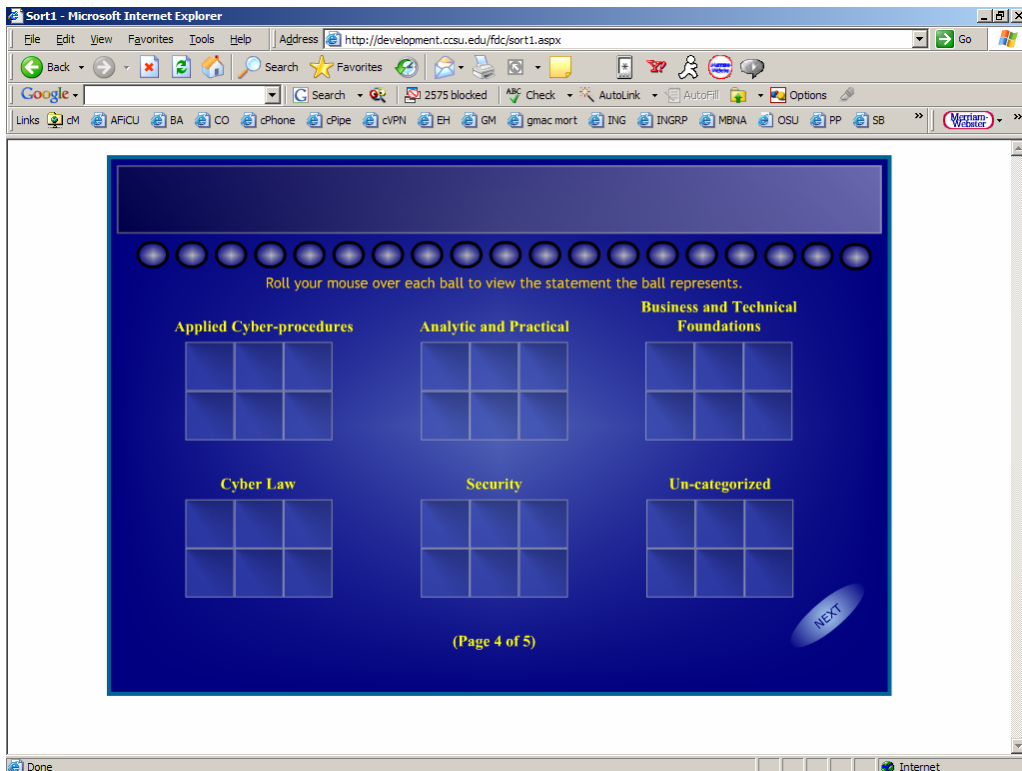


Figure 4 - VCS Screen

10. REFERENCES

- Bevan, N. "Card sorting," Usability.Net, 2006.
- Budwar, P. "The Use of Visual Card Sorting Techniques to Study Managers' Belief Structure," *Journal of Managerial Psychology* (15:5) 2000, pp 440-459.
- Denning, P.J. "Who Are We?," *Communicaitons of the ACM* (44:2), February 2001, pp 12-19.
- Feldman, J., and Kohn, R. "Collecting Computer-Based Evidence," in: *New York Law Journal*, 1998.
- Holsapple, M. "Purdue University, Law Enforcement Probe Digital World of Computer Forensics. ," in: *Ascribe Law News Service*, Ascribe Law News Service, 2004.
- Rogers, M., and Seigfried, K. "The Future Of Computer Forensics: A Needs Analysis Survey," *Computers & Security* (23:1), February 2004.
- Wang, R.Y., and Strong, D.M. "What Data Quality Means To Data Consumers," *Journal of Management Information Systems* (12), Spring 1996.

