

4-27-2010

The Development of a Standard Digital Forensics Master's Curriculum

Kathleen Strzempka

Kathleen A. Strzempka, kstrzemp@purdue.edu

Follow this and additional works at: <http://docs.lib.purdue.edu/techmasters>

Strzempka, Kathleen, "The Development of a Standard Digital Forensics Master's Curriculum" (2010). *College of Technology Masters Theses*. Paper 8.

<http://docs.lib.purdue.edu/techmasters/8>

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries. Please contact epubs@purdue.edu for additional information.

THE DEVELOPMENT OF A STANDARD DIGITAL
FORENSICS MASTER'S CURRICULUM

A Thesis

Submitted to the Faculty

of

Purdue University

by

Kathleen Strzempka

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

May 2010

Purdue University

West Lafayette, Indiana

TABLE OF CONTENTS

Table	Page
LIST OF TABLES	iv
ABSTRACT	v
CHAPTER 1: INTRODUCTION	1
1.1 Statement of Problem	2
1.2 Significance of the Problem	2
1.3 Purpose of the Study	4
1.4 Definitions	4
1.5 Assumptions	5
1.6 Delimitations	5
1.7 Limitations	6
CHAPTER 2: REVIEW OF THE LITERATURE	7
2.1 The Need for a Standard Curriculum	7
2.2 Curriculum Development	8
CHAPTER 3: METHODOLOGY	12
3.1 Identification of Master's Programs	12
3.2 Categorization of Courses	14
3.3 Statistical Analysis	16
3.4 Standard Curriculum Development	16
CHAPTER 4: DATA ANALYSIS AND FINDINGS	18
4.1 Current State Analysis by University	18
4.2 Frequency Analysis	31
4.3 Suggested Model Curriculum	32
4.3.1 Scope	33
4.3.2. Courses and Descriptions	34
CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS	38

LIST OF REFERENCES.....	40
APPENDIX.....	43

LIST OF TABLES

Table	Page
Table 3.1 List of Identified Master's Programs	13
Table 3.2 DFCB KSA Domain Descriptions	14
Table 3.3 Beebe and Clark's Knowledge Domain Descriptions.....	15
Table 4.1 Frequency Analysis of DFCB KSA Domains	31
Table 4.2 Frequency Analysis of Beebe and Clark's Knowledge Domains.....	32
Table 4.3 List of Required Courses and Electives	34
Appendix Tables	
Table A.1 Carnegie Mellon University	43
Table A.2 George Washington University.....	44
Table A.3 John Jay College	45
Table A.4 Purdue University	46
Table A.5 Sam Houston State University	47
Table A.6 Stevenson University.....	48
Table A.7 Texas State University.....	49
Table A.8 University of Central Florida.....	50
Table A.9 University of New Haven.....	51
Table A.10 University of Rhode Island.....	52
Table A.11 University of Eastern Michigan.....	53
Table A.12 Model Curriculum.....	54

ABSTRACT

Strzempka, Katie. MS, Purdue University, May, 2010. The Development of a Standard Digital Forensics Master's Curriculum. Major Professor: Dr. Marcus Rogers.

This research focuses on the development of a standard digital forensics master's curriculum. A current state analysis has been done of various master's programs across the United States. Each of the courses were analyzed and compared against digital forensic domains from previous studies, including the Digital Forensic Certification Board's (2009) KSA domains and Beebe and Clark's (2006) knowledge domains. The courses were charted under their appropriate categories in an effort to identify the topics covered within each curriculum. Both a qualitative and frequency analysis were then completed to review the domains covered within each program. The results showed a wide variety of topics from school to school. Eight of the twelve master's programs were more generalized and touched briefly on a majority of the domains, while the remaining programs emphasized more specific areas such as computer science, law, and criminal justice. Using the data gathered from the analyses in combination with the KSA and knowledge domains, a standard digital forensics curriculum has been identified as a starting point for future research. This model curriculum includes required courses, potential electives, and descriptions of each. Future research should further test whether this standard curriculum is generalizable to all programs within this field.

CHAPTER 1: INTRODUCTION

Many academic disciplines that have been around for decades have already developed required certifications or training courses that are needed for an individual to work in that field. For example, a lawyer must pass the bar examination in order to practice law, just as an individual must pass a medical licensing exam to become a doctor. What happens when a discipline is so new that standards haven't even been developed? This is one of the obstacles that digital forensics is currently facing. While there are academic programs being offered in this area, there is not a standard curriculum to base this education on. This lack of standards can lead to several issues.

A lack of a standard curriculum with required course topics could result in little consistency across the university programs being offered. A master's degree in digital forensics at one school could vary drastically with that of another school. This is a problem because graduates of these programs are joining the workforce without anything or anyone validating their knowledge and skill sets. On top of that, an individual who has taken a course in digital forensics may claim to be an expert in this area. While there are certainly educated cyber forensic professionals out there, it is difficult to determine those that are deserving of this title without an agreed upon set of standards. Another issue involves the quality of the available courses, content, and faculty of these programs (Beebe & Clark, 2006). In developing a digital forensics curriculum, there may be difficulty determining which courses should be required because of the multi-disciplinary nature of the field. One school may determine that the majority of the courses should focus on criminal justice, whereas another may conclude that the concentration should be on computer security (Gottschalk, Liu, Dathan, Fitzgerald, & Stein, 2005). Furthermore, how can it be shown that the faculty and course content are up to par if there is no set of expectations, guidelines, or standards?

Various studies have identified education as an area requiring much improvement. Surveys have been done involving law enforcement officers, researchers, and practitioners in both private and public sectors. The participants in these studies have reported "Education, training and certification" as one of the major issues (Rogers & Seigfried, 2004). Many of the studies that have been done to identify challenges in this

area have combined education and training into one general category. For the purposes of this research, issues related to both of these areas were discussed; however, the focus of this study will be on the educational side.

The subsequent portions of this thesis will further prove this need for standards and suggest a starting point by developing a standard digital forensics master's curriculum.

1.1 Statement of Problem

The use of digital devices in everyday life is increasing exponentially, but the lack of knowledge in those examining these devices is causing a backlog of unresolved cases (Bhaskar, 2006). Many law enforcement officers do not have the qualifications to extract electronic evidence off of computer systems, laptops, cell phones, GPS devices, etc. Organizations do not have the expertise for electronic discovery in the event of an incident, leading them to ignore problems with disgruntled employees or improper use of company resources. One of the main reasons why these individuals are not qualified is because there is a lack of proper education within the field. More specifically, there needs to be a standard digital forensics curriculum created as a basis for future academic programs. In this thesis, the curricula of various schools have been analyzed and a standard curriculum developed.

1.2 Significance of the Problem

The field of digital forensics is a relatively new area whose popularity has grown with the proliferation of electronic devices around the world (Etter, 2001). Challenges come along with any new area of study, and digital forensics is no exception. Various studies have been done to determine the main challenges in the cyber forensics arena. Both Stambaugh et al., (2001) and Rogers and Seigfried (2003) determined Education, Certification, and Training to be the primary issue, as reported by law enforcement agencies, researchers, students, academics, and private/public sector practitioners within the field. Additionally, Dartmouth College performed a National Needs Assessment. A large majority of the law enforcement survey participants (90%) indicated an urgent need

for additional training (Technical Analysis Group, 2002). The combination of these studies and the information contained in this section demonstrates the significance of educational standards for all sectors of cyber forensics.

To date there is not a specific certification or requirement to be a digital forensic examiner. This means that there are potentially untrained practitioners collecting digital evidence, analyzing the data, and when applicable, presenting it in a court of law as an expert witness. On the law enforcement side, something as simple as pressing the power button at the wrong time can destroy an investigation. Improper handling of digital evidence could result in dismissed cases, innocent people being found guilty, and guilty suspects going free. Within industry, issues with employees are being excused despite their illegal or unethical use of company computers and/or resources (Craiger, Ponte, Whitcomb, Pollitt, & Eaglin, 2007). One explanation for this is because companies are not willing to report these individuals and risk their reputation with the public. For this reason, interest in gathering digital evidence, or electronic discovery, has been expanding to sectors other than law enforcement (Yasinsac, Erbacher, Marks, Pollitt, & Sommer, 2003).

Several academic programs have been developed throughout the world, despite the fact that curriculum development standards do not exist. While the existence of such educational programs is important, without a standard curriculum the quality of the courses, content, and faculty is something to be considered (Rogers & Seigfried, 2003).

The development of a standard curriculum will improve the content and quality of the current programs, inspire the creation of additional programs throughout various universities, and increase the amount of educated practitioners. Qualified individuals can then accurately and efficiently analyze digital devices, resulting in the potential reduction of backlogged cases. On the legal side, this development will complete a small part of the puzzle in identifying who is truly an expert in the field. In the past, courts have accepted individuals to testify as an expert witness based on previous work experience (Meyers & Rogers, 2004). This will allow them to have some criteria to determine whether an individual should or should not be accepted.

1.3 Purpose of the Study

The goal of this thesis is to critically analyze current programs that have a digital forensics concentration, and by comparing the content of these programs, suggest a standard curriculum for this area. In other words, the study has identified where the field currently is in terms of master's curricula. Though undergraduate and graduate programs were both researched, the focus was on the analysis and development of a master's curriculum, as they are more flexible and therefore a good starting point (McGuire & Murff, 2006). A master's degree is typically limited to two years and has a specific focus, whereas undergraduate degrees are more complex. Once a master's curriculum is created, it can be further developed into an undergraduate or doctorate degree.

1.4 Definitions

Cyber forensics ontology – A proposed model, consisting of a 5-layer hierarchical structure, to be used for specialization, certification, and education within the cyber forensics domain (Brinson, Robinson, & Rogers, 2006).

Digital evidence – Information of probative value that is stored or transmitted in a binary form (Scientific Working Group on Digital Evidence [SWGDE], 2000).

Digital forensics – The use of an expert to preserve, analyze, and produce data from volatile and non-volatile media storage. This is used to encompass computer and related media that may be used in conjunction with a computer (Meyers & Rogers, 2004).

Digital Forensics Certification Board (DFCB) – Developed with the National Institute of Justice (NIJ) funding in an effort to create a professional digital forensics certification.

DFCB domains – An outline of topics which must be mastered in order to achieve the Digital Forensics Certified Practitioners (DFCP) or Digital Forensics Certified Associate (DFCA) certifications (Digital Forensic Certification Board [DFCB], 2009).

Electronic discovery (e-discovery) – Refers to the discovery of all electronically stored information (ESI) such as e-mail messages, instant messages, voice mails, cell phone and pager text messages, websites, call logs, word processing documents, databases, digital photos, spreadsheets and accounting software, specialized engineering software, as well as backup and archived copies of that same information (Institute for the Advancement of the American Legal System [IAALS], 2007).

Forensic Science Education Programs Accreditation Commission (FEPAC) – “The mission is to maintain and to enhance the quality of forensic science education through a formal evaluation and recognition of college-level academic programs. The primary function of the Commission is to develop and to maintain standards and to administer an accreditation program that recognizes and distinguishes high quality undergraduate and graduate forensic science programs” (American Academy of Forensic Sciences [AAFS], 2009).

Knowledge Domains – “A reasonably small, commonly accepted set of knowledge areas critical to a field of knowledge” (Beebe & Clark, 2006). In this thesis, knowledge domains will refer to the ten digital forensic categories identified by Beebe and Clark.

1.5 Assumptions

During the analysis portion of this thesis, digital forensics master’s programs were identified and the courses analyzed. It is assumed that the curricula listed on each of the university websites were accurate and current.

1.6 Delimitations

In an effort to limit the scope, it was the intent of this study to review all master’s programs within the United States which had a curriculum available online. This type of graduate program is an ideal starting point since they are limited to the discipline in question and are typically practical versus theoretical. Once a standard master’s curriculum is developed, it can then be expanded into a 4-year degree, doctoral degree, or

other type of curriculum. The reason for including only programs within the United States is because educational and curriculum issues vary from country to country, as do laws and admissibility requirements. Taking these delimitations into account, 12 master's programs were identified and critically analyzed.

1.7 Limitations

One limitation of this study is that the only master's programs that were researched are those that have a curriculum or list of courses available online. As a result, a full description of each course wasn't always included, preventing that particular course from being categorized at a more specific level. In this circumstance, an instructor or other individual was contacted for more details. On top of this, some of the programs focus strictly on digital forensics, whereas others focused on a more general area and only specialized in forensics. This factor was the cause of some of the inconsistent results from school to school. Another limitation is that this study is not representative of all digital forensics master's programs; only a sample of the programs were used in this analysis. Finally, though the development of the standard curriculum was loosely based on a current state analysis, some subjective decision making was required as part of the qualitative analysis, which could serve as potential researcher bias.

CHAPTER 2: REVIEW OF THE LITERATURE

This section discusses literature related to the need for and development of a standard curriculum.

2.1 The Need for a Standard Curriculum

The overall consensus of many of the references is that cyber forensics education is a critical issue and requires improvement. Yasinac, Erbacher, Marks, Pollitt, and Sommer (2003) discussed the importance of computer forensics and the need for appropriate training and education for all individuals involved, including technicians, policy makers, professionals and researchers. Craiger, Ponte, Whitcomb, Pollitt, and Eaglin (2007) agreed that this lack of training is a major contribution to the backlog of cases discussed earlier.

Though few studies have been done which actually identify challenges within the field of digital forensics, those that were implemented were all in agreement on this need for education and training standardization. Stambaugh et al., (2000) conducted a one-year study in which law enforcement officers identified what was needed to allow them to successfully combat electronic crime. “Uniform training and certification courses” was among the top ten priority needs identified. A similar study initiated by the Institute for Security Technology Studies at Dartmouth College resulted in 90% of law enforcement participants reporting that the need for additional training was urgent. This particular assessment went on to suggest the development of a baseline curriculum in future research (Technical Analysis Group, 2002). From these two studies, the significance of a standard curriculum was apparent from a law enforcement perspective, but what about the other sectors involved in digital forensic examinations?

In 2003, a needs analysis survey was implemented which asked participants to identify the top five issues within the area. This time the participants included computer forensics researchers, students, academics, and private/public sector practitioners. The most frequently reported issue was “Education, training and certification” (Rogers & Seigfried, 2004).

Finally, Beebe and Clark (2006) were seemingly the first to complete an extensive study in the area of digital forensics curriculum development. This research consisted of a qualitative analysis resulting in the identification of digital forensic knowledge domains, learning objectives, and core concepts. The idea behind this study was that the development and acceptance of these within the community would further enhance digital forensics education, increasing the number of qualified practitioners. While the authors acknowledge that this effort was a “good start,” further validation from the digital forensic community was suggested (Beebe & Clark, 2006).

2.2 Curriculum Development

Many factors must be considered in the development of a standard curriculum. How general or specific should the topics be? Should the curriculum be geared towards a certain job function? Within what school or department should the program be housed? These and many other questions must be reflected on in order to create a curriculum that is truly a standard and can be applied to all areas of digital forensics, including academia, industry, and law enforcement.

Yasinac et al., (2003) recognized that computer forensics education consisted of multiple skill levels. Within law enforcement, officers need to be trained as well as judges, prosecutors, and defense attorneys involved in a case. Industry requires its forensic examiners to be trained in the event of an incident, and academia focuses on education and training for students, faculty, and researchers (Yasinac et. al, 2003). A standard academic curriculum should be general enough to cover all aspects of the field, but not too specific in any direction. Students can learn general concepts, theories, and practical application, but it is not realistic to expect them to be fully trained for a job after completing the program (Beebe & Clark, 2006).

Another issue to reflect on is where to place a digital forensics curriculum within a university setting. A computer forensics education can include courses in law, criminal justice, computer science, psychology, etc. A study done by Gottschalk, Liu, Dathan, Fitzgerald, and Stein (2005) surveyed various computer forensic programs in North America and found programs to be located in departments such as computing, an

economic crime institute, a division of account and computer systems, and a criminal justice program. With this in mind, which department is best suited to house a program in this area? The master's programs of McGuire and Murff (2006) and Craiger et al., (2007) are within the universities' Computer Science program, whereas Troell, Pan, and Stackpole (2003) suggest their graduate course be located in the computer security department.

A frequency analysis was conducted on 48 digital forensic courses, representing 42 universities worldwide. Though the majority of the courses were located in the school's department of Computer Science, the departments varied across different colleges and universities (Beebe & Clark, 2006). Determining the best possible location for a Digital Forensics master's program is going to vary from school to school, and be dependent on the main focus of that particular school's master's program.

One of the most critical decisions to be made in the creation of a standard curriculum is the actual topics to be covered. The idea of hands-on knowledge and practical approach was a significant topic in the development of this curriculum. McGuire and Murff (2006) suggest that a working relationship with agencies outside the academic realm will enhance the curriculum by allowing such practical experience. The master's program discussed by Craiger et al., (2007) includes a capstone course, which brings together all the methods, theories, and concepts covered throughout the program and allows the students to apply the acquired knowledge (Craiger et. al, 2007).

The Technical Working Group for Education and Training in Digital Forensics report was created in 2007. This report contains information on education and careers in Digital Forensics. The chapter on Graduate Degree Programs in Digital Forensics contains a section on *Curriculum Considerations*. These are a list of general topics to potentially be included in a graduate digital forensics curriculum, though not specific enough to be a baseline for a standard curriculum. A few examples of the general topics to be included are Criminal and Civil Legal Issues, Complex Data Analysis, and Data communications and Network Systems. While there are several topics listed, the authors point out that a curriculum could be based on one or more of the available topics, but not necessarily include them all (West Virginia University Forensic Science Initiative, 2007).

To assist in the process of deciding which topics should be included, Brinson, Robinson, and Rogers' (2006) cyber forensics ontology, the DFCB (2009) KSA domains, Beebe and Clark's (2006) knowledge domains, and the FEPAC Self-Study Report (2009) will be utilized. These references originated from various areas of education and training. The KSA domains were developed by the Digital Forensic Certification board, while the cyber forensics ontology and knowledge domains were created by research done within academia. Using these references to develop a standard curriculum will help align these various areas of education and training and ensure consistency between some of the certifications and curricula being developed. The following is a breakdown of each of these resources.

The ontological model divides the field of Cyber Forensics into five levels of categories with the goal of these categories being used as potential courses within a curriculum or training program (Brinson, Robinson, & Rogers, 2006). The first level of subtopics includes *Technology* and *Profession*. The technology side would apply more towards training and certification. The profession side contains the four main sectors of cyber forensics: Law, Academia, Military, and Private Sector. This model was used as a reference in the development of a standard curriculum.

The DFCB came up with seven Knowledge, Skills, and Abilities (KSA) topics which a candidate must have a general knowledge of in order to receive one of the available certifications. These KSA domains are *Legal, Ethics, Storage Media, Mobile and Embedded Devices, Network Forensics, Program and Software Forensics, and Quality Assurance Control and Management*. Each domain is also broken down into smaller, more specific sub-parts (DFCB, 2009). The master's curricula in this current study were compared against these DFCB domains to see which area they fall under, similar to the approach taken by Shanklin (2009). Her gap analysis mapped existing educational programs, both graduate and undergraduate, to the KSA domains. In Shanklin's (2009) analysis, it was only mentioned whether or not the program covered each domain. The current study has taken this idea one step further and mapped each of the courses to its appropriate domain. This was done for each of the master's programs and will be explained further in the Methodology section.

The Digital Forensics Curriculum Development study done by Beebe and Clark (2006) included the analysis of 48 course syllabi across 42 distinct universities. These courses were offered at an undergraduate level, graduate level, and a combination of both. The authors first did a frequency analysis to determine department distribution of the courses. The most predominant department in which the courses were contained was Computer Science. After reviewing each syllabus, the researchers went on to identify ten digital forensics knowledge domains, which the curricula were also mapped to in this thesis. Learning objectives were then created for each of the domains, followed by the level of mastery expected of the students for each objective (Beebe & Clark, 2006).

The FEPAC Self-Study Report (2009) for Digital Forensic Science is a compilation of standards and program requirements at both an undergraduate and graduate level. While it contains some general admission and curriculum standards, including the *Curriculum Considerations* mentioned above, the graduate section does not include course requirements (FEPAC, 2009). Nevertheless, once this standard curriculum was developed, it was compared against this self-study report to ensure it followed the general curricular requirements, objectives, and considerations. In the future, the newly developed standard curriculum could potentially be included as a section in this self-study.

CHAPTER 3: METHODOLOGY

The methodology section discusses the master's programs that were used in this research and how they were identified, the categorization of the courses within each program, the statistical analysis of the data, and finally the development of a standard curriculum.

3.1 Identification of Master's Programs

A current state analysis was done of 12 digital forensics master's programs to identify the similarities and differences of the various curricula. These programs were chosen based on the delimitations of this study and are representative of the population. Many searches were done and resources used in an attempt to identify all digital forensics master's programs within the United States in which the curriculum was available online. The majority of these schools were retrieved from the Digital Forensics Association website (College Education in Digital Forensics). In addition, Gottschalk et al., (2005) looked at four master's programs whose universities were already included in this list. The programs used in Shanklin's (2009) gap analysis were also reviewed, though the only school it contained that wasn't already listed was Carnegie Mellon University. It is recognized that some programs may have been missed. The information in Table 3.1 includes a final list of the universities and programs that were looked at in this study:

Table 3.1 List of Identified Master's Programs

School	Program	Location
Carnegie Mellon University	Master of Science in Information Networking with a concentration in Computer Forensics and Incident Response	Pittsburgh, PA
Champlain College	Master of Science in Digital Investigation Management	Burlington, VT
George Washington University	Master of Forensic Sciences with a concentration in high technology crime investigation	Washington, DC
John Jay College of Criminal Justice	Master of Science in Forensic Computing	New York, NY
Purdue University	Master of Science in Cyber Forensics	West Lafayette, IN
Sam Houston State University	Master of Science in Digital Forensics	Huntsville, TX
Stevenson University	Master of Science in Forensic Studies with an Information Technology track	Stevenson, MD
Texas State University	Master of Science with a Minor in Forensic Systems	San Marcos, TX
University of Central Florida	Master of Science in Digital Forensics	Orlando, FL
University of New Haven	Master's in Criminal Justice with a concentration in Forensic Computer Investigation	West Haven, CT
University of Rhode Island	Master's Degree in Computer Science with a Digital Forensics track	Kingston, RI
University of Eastern Michigan	Master of Science in Technology Studies with a concentration in Digital Investigations	Ypsilanti, MI

3.2 Categorization of Courses

The first step in analyzing the programs listed above involved the DFCB domains (DFCB, 2009). The courses within each program were compared against the domains using the charts shown in the Appendix. For example, every course contained in the John Jay curriculum was analyzed and listed under its appropriate domain. Continuing with this same example, the “Criminal Justice 710” course was listed under the *Legal* domain, whereas the “Small Scale Digital Device Forensics” course at Purdue University fell under the *Mobile & Embedded Devices* domain. This process was done with all courses in all universities identified in the previous section. Table 3.2 includes a breakdown of the DFCB domains and includes a few examples of each of the subparts to give the reader a better understanding of the categories.

Table 3.2 DFCB KSA Domain Descriptions

Domain	Description
Legal	This domain covers privacy issues involved in investigations, knowledge of the Fourth Amendment, chain of custody, electronic evidence laws, and relevant case laws.
Ethics	This domain covers Professional Ethics in relation to the field and roles and duties of expert witnesses.
Storage Media	This domain covers various file formats, acquisition and examination of digital evidence, documentation of evidence collection, and imaging hardware, software and process.
Mobile & Embedded Devices	This domain covers knowledge and examination of mobile devices and SIM cards.
Network Forensics	This domain covers identification and acquisition of digital evidence on a network and knowledge of network topologies and protocols.
Program and Software Forensics	This domain covers programming languages, malicious code, and malware.
Quality Assurance, Control, and Management	This domain covers standards and controls, certification, and quality in relation to the field of digital forensics.

Another current state analysis involved mapping the courses to Beebe and Clark's knowledge domains (Beebe & Clark, 2006) using a similar process. These domains can also be viewed within the charts in the Appendix. As an example, the "Incident Response Technologies" course offered by the University of Central Florida fell under the *Incident Response* knowledge domain. Table 3.3 is a breakdown of the knowledge domains and includes a few examples of each of the subparts to give the reader a better understanding of the categories.

Table 3.3 Beebe and Clark's Knowledge Domain Descriptions

Domain	Description
Computer Science	This domain covers password cracking, data hiding, hashing, malicious code, and operating systems.
Conducting Investigations	This domain covers investigative techniques and procedures, how to process a digital crime scene, and the investigative process.
Data Analysis	This domain covers the examination of digital evidence, deleted file recovery, data analysis hardware and software tools, and locating hidden data.
Digital Forensic Awareness	This domain covers computer criminology, importance of tool testing, the need for digital forensics, types of computer crimes, and various sources of digital evidence.
Documentation & Findings Communication	This domain covers investigative report writing and how to provide expert testimony.
Evidentiary Issues	This domain covers evidence preservation and rules of evidence for court admissibility.
Incident Response	This domain covers the purpose and process of incident response and how to validate, assess, contain, eradicate and recover.
Law & Ethics	This domain covers ethical implications of digital forensics, how to "traceback" intrusions, computer crime laws, and laws governing investigative procedure.
Preparation	This domain covers the creation of incident response plans and how to prepare for digital forensic investigations and laboratories.

Both the DFCB domains (2009) and Beebe and Clark's (2006) knowledge domains were used in an effort to allow these resources to run in parallel with the newly

developed curriculum. Aligning these different areas of education simplifies the goal of creating an overall standard. Prior to the analysis, it was understood that there might be a circumstance where a course would fall under multiple areas. This proved to be true. For example, in some cases there was a general digital forensics course that covered multiple domains and/or categories. In this circumstance, the course was listed under each topic that it covered. It was also recognized prior to the study that it might not be appropriate to list a course under any of the available categories or domains. This assumption also became realistic after completing the analysis. In this event, the course was removed if it was not specifically related to digital forensics. If it was related to digital forensics but still did not cover any domains, that was discussed in the qualitative analysis.

3.3 Statistical Analysis

Once all the courses were plotted, a current state qualitative analysis was done to determine which topics are covered most often across the various universities and which are not covered enough. A frequency analysis was also done to determine how many programs covered each of the domains. Popular domains and categories were identified as well as those that require more representation. The results of this analysis are expanded upon in Chapter 4.

3.4 Standard Curriculum Development

Creating a suggested standard curriculum was a complex process. Several factors were considered including general topics to include and mandatory versus optional courses. These, among other items, were determined by analyzing the data gathered in the previous stages of this process.

Required courses, possible electives, and course descriptions were identified and created based on the current state analyses, frequency analysis, and other information gathered throughout the study. Guidelines from literature were also utilized to assist in this process, including the FEPAC Self-Study, the Technical Working Group for Education and Training in Digital Forensics, and suggestions mentioned throughout other related references. Finally, the FEPAC Self-Study report was reviewed to ensure the

curriculum complied with the general standards (FEPAC, 2009). Details on the resulting standard curriculum can be found in Chapter 4.

CHAPTER 4: DATA ANALYSIS AND FINDINGS

The results of the current state analysis are broken down in this section by university. Within each school, all courses that have been compared against the various domains are listed, followed by a qualitative analysis of the results. Specific data for each school can be found in the charts within the Appendix.

The diversity of each of these programs is significant to mention. While some of the programs offer a master's degree in Digital or Computer Forensics, others may have an alternative primary focus. For example, some schools offer a master's degree in Information Technology, Forensic Science, or Criminal Justice, with a focus on Digital Forensics. For this reason, some of the programs may only fall under a few domains in this study. This analysis is in no way a review of the quality of these programs, but instead is purely identifying the topics covered in each of the digital forensics courses of each program to gain a better understanding of the curricula being offered.

The following sub-sections include the results of the current state analysis, frequency analysis, and suggested model curriculum.

4.1 Current State Analysis by University

Carnegie Mellon University – Master of Science in Information Networking with a concentration in Computer Forensics and Incident Response

The following is a list of digital forensics courses within the program:

- 14-761: Advanced Information Assurance
- 14-822: Host-Based Forensics
- 14-823: Network Forensics
- 14-824: Advanced Host-Based Forensic Analysis
- 14-825: Advanced Network Analysis
- 14-826: Event Reconstruction and Correlation

As displayed by the title of this program, the majority of the curriculum is composed of Information Security and Networking courses. The concentration in

Computer Forensics and Incident Response includes those courses listed above. Information on these courses was retrieved from the curriculum available on the program's website (Carnegie Mellon) as well as a contact within the program. The Advanced Host-Based Forensic Analysis course is a more difficult, in depth version of the Host-Based Forensics course. Both cover domains relating to conducting investigations, examining data, and dealing with digital evidence. Host-Based Forensics also would appear to fall under Digital Forensic Awareness and Documentation and Findings Communication, as it is more of an introductory course than the advanced version. Network Forensics and Advanced Network Forensics are very similar courses, except they deal with digital evidence off of the network as opposed to stationary media. Finally, Advanced Information Assurance provides hands-on experience in both an information assurance exercise and an incident response exercise. It covers a wide range of topics such as network traffic management, intrusion detection, encryption, cyber law, and persistent data. Within this course, all domains are covered with the exception of Mobile & Embedded Devices and Computer Science.

Champlain College – Master of Science in Digital Investigation Management

The following is a list of digital forensics courses within the program:

- MBA 500: Integrated and Reflective Practice
- DIM 500: The Practice of Digital Investigations
- MBA 525: Process Improvement and Operations
- MIT 505: Project Management
- MIT 525: Financial Decision Making for Management
- MIT 530: IT Security and Strategy
- MIT 550: Reflective Leadership and Planned Change
- DIM 530: Legal Aspects of Digital Investigations
- DIM 540: Current Topics in Digital Investigation Techniques
- DIM 550: Laboratory Operation and Accreditation
- DIM 560: Digital Investigation for Civil Litigation
- DIM 570: Research Methodology

After further review, this particular program was not analyzed because its courses were management focused and did not apply to any of the domains. Information on the courses was retrieved from the curriculum available on the school's website (Champlain College, 2009). Champlain does offer an undergraduate degree in Computer and Digital Forensics, but as it is not a master's program, was outside the scope of this study.

George Washington University – Master of Forensics Sciences with a concentration in high technology crime investigation

The following is a list of digital forensics courses within the program:

- FORS 259: Computer-Related Law
- FORS 265: Ethics and Leadership
- FORS 277: Computer Forensic I - Investigation and Evidence Gathering
- FORS 279: Intrusion I - Understanding and Identifying Network-Based Attacks
- FORS 285: High Technology Crime Investigation Capstone Course
- FORS 274: Video Forensic Analysis
- FORS 278: Computer Forensics II - Evidence and Analysis
- FORS 280: Intrusion II - Investigating Network-based Attacks
- FORS 283: Steganography and Electronic Watermarking
- FORS 290: Selected Topics
- FORS 295: Research
- FORS 298: Forensic Sciences Practicum

As there was no available contact to speak with, the program brochure (George Washington University) was utilized to conduct this analysis. This document contains information about the program including the curriculum, course descriptions, and admissions information. Many of the digital forensic courses shown above appeared to cover the Storage Media and data Analysis domains. As a pair, Computer Forensics I and Computer Forensics II touch on several of the knowledge domains, from Conducting Investigations through Evidentiary issues. There is also a capstone course offered in the students' final semester, which, as described in the brochure, allows the students to go

through a simulated computer forensic investigation from start to finish.

The domains that did not appear to be mentioned include Mobile & Embedded Devices, Program & Software Forensics, Quality Assurance, Control, & Management, and Incident Response. Given that information, there are also several opportunities for these topics to potentially be covered in the Research courses in which each individual student focuses on their specific interests.

John Jay College of Criminal Justice – Master of Science in Forensics Computing

The following is a list of digital forensics courses within the program:

- Forensic Computing/Criminal Justice 752: The Law and High Technology Crime
- Criminal Justice 710: Issues in Criminal Justice I
- Criminal Justice/Forensic Computing 727: Cybercriminology
- Forensic Computing 753: Digital Forensics Applications
- Forensic Computing 700: Theoretical Foundations of Computing
- Forensic Computing 710: Architecture of Secure Operating Systems
- Forensic Computing 742: Network Security
- Forensic Computing 740: Data Communications and Forensics Security
- Forensic Computing 745: Network Forensics
- Forensic Computing 760: Forensic Management of Digital Evidence
- Criminal Justice 708: Law, Evidence and Ethics
- CRJ 733: Constitutional Law
- CRJ 750/PAD 750: Security of Information and Technology
- Forensic Computing 780: Capstone Seminar and Fieldwork
- Forensic Computing 791: Forensic Computing Prospectus Seminar

The Forensics Computing master's program at John Jay College offers both general and specialized courses on topics within the digital forensics realm. The available courses touch on all of the DFCB (2009) domains and Beebe and Clark's (2006) knowledge domains with the exception of Preparation. The course entitled Forensic Management of Digital Evidence provides an overview of digital forensics and discusses

theory on how to perform digital investigations, whereas the Digital Forensics Applications course takes the theory learned and applies it to mock investigations. This applications course allows students to understand the collection and preservation of evidence, examine mobile devices, write investigative reports, and provide expert testimony.

There are also several courses offered which cover the legal domains, including The Law and High Technology Crime, Issues in Criminal Justice I, Constitutional Law, and Law, Evidence and Ethics. A Capstone Seminar and Fieldwork course is offered in the final semester, allowing the students to apply what they've learned by completing 200 hours of fieldwork.

Looking at the course descriptions available online (John Jay College of Criminal Justice), the program did not appear to cover the Preparation domain, which was confirmed by a contact within the program. Most of the remaining courses did not specifically fall under any of the domains because the course topics were very specialized or offered the students an Independent Study option.

Purdue University – Master of Science in Cyber Forensics

The following is a list of digital forensics courses within the program:

- CIT 556: Basic Cyber Forensics
- CIT 557: Advanced Research Topics in Cyber Forensics
- CIT 5XX (499d): Small Scale Digital Device Forensics
- CIT 581V: Current Topics
- CIT 5XX (499c): File System Forensics
- CIT 5XX: Expert Witness Testimony
- CIT 5XX (499e): Hardware Essentials
- CIT 590: Digital Forensics Internship
- Electives

Overall, the offered courses within Purdue University's Cyber Forensics program (Purdue University) covered a large majority of the domains they were compared against.

The Basic Cyber Forensics course alone touched on many of the categories at a high level. The specialized courses, such as Small Scale Digital Device Forensics, File System Forensics, and Hardware Essentials only fell under one category; whereas Advanced Research Topics and Expert Witness Testimony covered multiple. Expert Witness Testimony allows the students to complete the digital investigation process from start to finish. A case is assigned at the start of the semester, worked on by each student individually, and their findings are written into a final report and defended as an expert witness.

This program also offers the students a unique opportunity to complete an internship with the local police department for course credit. During this internship, the students work closely with the detective on digital forensic investigations, allowing them to apply the knowledge learned in prior courses.

Within Purdue's Cyber Forensics curriculum, there were no courses identified which touched on the following areas: Network Forensics, Program & Software Forensics, and Incident Response. Having said that, the program offers six credit hours of electives, allowing the students to choose related courses based on their interests. So while the master's program does not specifically require courses in these domains listed above, a student may choose one of these areas to study as an elective or independent study.

Sam Houston State University – Master of Science in Digital Forensics

The following is a list of digital forensics courses within the program:

- DF 534: Digital Security
- DF 583: Digital Forensics Investigation
- DF 584: Software Forensics Evidence Management
- DF 630: Cyber Law
- DF 531: Principle and Policy in Information Assurance
- DF 535: Malware
- DF 560: Special Topics
- DF 587: File Systems Forensics

- DF 589: Disaster Recovery
- DF 670: Internship

A majority of the domains are covered within the Sam Houston Digital Forensics curriculum. Information was gathered via the Sam Houston State University Graduate Catalog (Sam Houston State University, 2009). Further details on the curriculum were obtained by speaking with one of the instructors within the program.

In Digital Forensics Investigation, Special Topics, and File systems Forensics, the students receive the opportunity to get hands-on experience in digital investigations. In addition, an Internship opportunity is available, allowing further practical knowledge. These four courses cover all of the domains related to conducting investigations, including the analysis of mobile and embedded devices.

To address the other domains, Cyber Law is included in this curriculum, which discusses laws specific to digital investigations. Malware and Software Forensics Evidence Management fall under the Program & Software Forensics domain as well as Computer Science. These two courses are targeted at the collection and tracing of malware. Finally, a Disaster Recovery course is offered which covers Incident Response and Preparation.

Based upon the discussion and review of the course descriptions, the following domains do not appear to be covered: Network Forensics and Quality Assurance, Control & Management.

Stevenson University – Master of Science in Forensic Studies with an Information Technology track

The following is a list of digital forensics courses within the program:

- FSCOR 601: Criminal Justice
- FSCOR 604: Evidence
- FSCOR 606: Internet Research
- FSCOR 607: Forensics Review Journal
- FSCOR 664: Litigation Practice and Procedure

- FSCOR 702: Mock Trial Capstone
- FSIS 600: Computer and Network Essentials for Forensic Investigators
- FSIS 640: Technology Law and Enforcement Activities
- FSIS 642: File Systems Forensic Analysis
- FSIS 643: Incident Response and Evidence Collection
- FSIS 644: Windows Forensic Examinations
- FSIS 646: Windows Intrusion Forensic Investigations
- FSIS 648: Disaster Recovery
- FSIS 650: Hacking Exploits and Intrusion Detection

This particular program differs from some of the others in this study in that its primary focus is on forensic science, with an optional Information Technology track. Because of this, many of the required courses didn't necessarily pertain to digital forensics. The results of this particular analysis were based on the School of Graduate and Professional Studies Catalog (2009) that was provided by a contact at Stevenson University as well as discussions with one of the instructors within the program.

As mentioned, several of the required courses were not specifically related to digital forensics. Those that remained, however, covered many of the domains listed in both charts. The domains related to law were well represented in this program with at least three courses allowing students to understand the legal requirements for digital forensic evidence collection, handling, and preservation. Though the Criminal Justice, Evidence, and Litigation Practice and Procedure courses do not specifically cover any of the digital forensic domains, students have some flexibility in their written assignments to incorporate material from digital investigations. Several of the courses provide the students with hands-on exercises and cover the analysis of digital evidence, which can be seen in the related table within the Appendices. The Mock Trial Capstone course was of most significance, as it touched on a large majority of Beebe and Clark's (2006) knowledge domains. The main focus of this class centered on presenting the evidence in a court of law, including opening and closing statements and cross-examinations. In preparation for the mock trial, students in the IT track were to examine a hard drive,

locate and analyze relevant digital evidence, and construct the investigative theory which would then be presented in court.

Based on the course descriptions offered in the catalog, the following domains were not covered: Program & Software Forensics, Quality Assurance, Control & Management, and Digital Forensic Awareness. There is, however, a Forensic Journal Review elective in which the student may research a topic of interest and perhaps delve deeper into one or more of these domains.

Texas State University – Master of Science with a Minor in Forensic Systems

The following is a list of digital forensics courses within the program:

- CS 5369F: Digital Forensics
- CS 5369R: Digital Forensics Research

At Texas State University, the master's program is heavily focused on Computer Science, with a minor in Forensic Systems. Only the digital forensics courses are listed, however the curriculum also includes advanced courses on computer security, network and communications, algorithm design, and more.

The Digital Forensics course was of most significance to this study. Within this course, which is run as a seminar, various digital forensics research areas are discussed as well as network and system security. The students are then able to apply this knowledge by analyzing hard drives, imaging, conducting live response and reverse engineering malware. Also included is a final project chosen by each student. Many of the domains are touched on with the exception of Legal, Ethics, Mobile & Embedded Devices, Quality Assurance, Control & Management, Incident Response, Law & Ethics, and Preparation.

The other related course is Digital Forensics Research. The intentions are to go beyond the Digital Forensics course and have the students conduct original research papers with the goal of receiving a publication. Specific domains could not be identified for this course as the topics vary depending on the research interests of each student.

University of Central Florida – Master of Science in Digital Forensics

The following is a list of digital forensics courses within the program:

- CGS 5131: Computer Forensics I
- CGS 5132: Computer Forensics II
- CHS 5503: Topics in Forensic Science
- CET 6887: The Practice of Digital Forensics
- CAP 6133: Advanced Topics in Computer Security and Computer Forensics
- CNT 6519: Wireless Security and Forensics
- CAP 6135: Malware and Software Vulnerability Analysis
- COP 6525: Distributed Processing of Digital Evidence
- CIS 6395: Incident Response Technologies
- CIS 6386: OS & File System Forensics
- CCJ 6074: Investigative and Intelligence Analysis, Theory and Methods
- CCJ 6706: Quantitative Methods and Computer Utilization in Criminal Justice or
ESI 5219: Engineering Statistics
- PLA 5587: Current Issues in Cyberlaw
- CHS 5596: Forensic Expert in the Courtroom
- CHS 5518: Forensic Examination of Digital Evidence or CJE 5688: Cyber Crime
and Criminal Justice

The digital forensic courses offered within the University of Central Florida's master's program contain both general courses that cover many domains as well as specialized courses that focus on just a few. The information for a majority of the courses was gathered by speaking with a contact within the program, whereas data on the remaining courses was collected via course syllabi provided by the instructors as well as the curriculum provided online (University of Central Florida).

Some of the general courses include The Practice of Digital Forensics, Computer Forensics I, and Computer Forensics II. The combination of these courses covered all domains with the exception of Mobile & Embedded Devices, Computer Science, and Incident Response. To fill in the gaps, there were several courses focusing on more

specific topics. According to the syllabi, Malware and Software Vulnerability Analysis and Advanced Topics in Computer Security and Computer Forensics both deal with malicious code, software testing, and log analysis. They fell under the Program & Software Forensics and Computer Science domains.

The Practice of Digital Forensics is one of the more significant courses within this program as it not only covers a large majority of the domains, but it also provides the students with the opportunity to conduct four examinations throughout the semester. It is considered to be a capstone course, covering the entire investigation process from start to finish.

With the Incident Response Technologies course falling under the Incident Response category, the only remaining domain that did not appear to be covered based on the information gathered was Mobile & Embedded Devices. Further details on Wireless Security and Forensics and Distributed Processing of Digital Evidence was unavailable.

University of New Haven – Master’s in Criminal Justice with a concentration in Forensic Computer Investigation

The following is a list of digital forensics courses within the program:

- CJ 600: Computer Crime: Legal Issues and Investigative Procedures
- CJ 603: Internet Vulnerabilities and Criminal Activity
- CJ 604: Network Security, Data Protection, and Telecommunication

New Haven’s master’s program is in Criminal Justice with an emphasis on digital investigations. For this reason, the Legal and Law & Ethics domains are covered in depth in a few of the courses. Information on these courses was gathered from the course descriptions provided on the department website (University of New Haven) as well as feedback from a contact within the department.

Also included in this program are courses on how to proceed with an investigation, however it was confirmed that these classes focus strictly on traditional forensics. Therefore, these courses were not looked at in this study. With the information available, it appears that the following domains are not covered: Ethics, Storage Media, Mobile & Embedded Devices, Network Forensics, Program & Software Forensics,

Quality Assurance, Control, & Management, Computer Science, Data Analysis, Evidence Preservation & Collection, and Evidentiary Issues.

University of Rhode Island – Master’s Degree in Computer Science with a Digital Forensics track

The following is a list of digital forensics courses within the program:

- CSC414: Computer System Fundamentals
- CSC485: Computer Forensics
- CSC486: Network Forensics
- CSC590: Digital Forensics Research/Practicum

Data on the offered courses was gathered from the course descriptions and introductory lectures provided on the department website (University of Rhode Island, 2008). The degree’s main focus is on computer science, however there are a few digital forensic courses offered which cover several of the domains. From the descriptions provided, it appears that both Computer Forensics and Network Forensics allow the students to conduct digital investigations. Computer Forensics covers legal issues, tools and procedures, and data acquisition. In Network Forensics, the students acquire data on servers and perform a real-time analysis of a live system in order to determine who is accessing the system.

The domains that do not appear to be covered are Mobile & Embedded Devices, Program & Software Forensics, Quality Assurance, Control & Management, Evidentiary Issues, Incident Response, and Preparation. However, a contact for this program was unavailable, so it is possible that some of these domains are covered in the current courses. Questions that would have been asked include the following:

- Is the entire investigative process covered from start to finish?
- Do the students learn about imaging and write blockers, documenting and report writing, and the need for evidence preservation?
- Is Incident Response discussed in any of the courses (i.e. how to validate, contain, eradicate and recover)?

- There appears to be a separate class on Forensic Toolkit (FTK), but do the students still analyze images using FTK in CSC 485 and/or CSC 486?
- For CSC 590, it is understood that images are analyzed using FTK, but are any other phases of the investigative process covered, such as evidence collection and preservation, imaging, or report writing?

Eastern Michigan University – Master’s of Science in Technology Studies with a concentration in Digital Investigations

The following is a list of digital forensics courses within the program:

- IA 533: Cyber Crime Investigation I
- IA 557: Cyber Crime Investigation II
- IA 558: Computer Forensics I
- IA 559: Computer Forensics II
- SSC 529: Foreign and Domestic Terrorism
- IA 691: Enterprise Incident Response

The concentration in Digital Investigations at Eastern Michigan University offers ample opportunity for the students to get hands-on experience. With this degree, the students also have the opportunity to graduate from the program with a forensic examiner certification. In order to complete this analysis, curriculum and course information was gathered from the program’s website (Eastern Michigan University) as well as one of the instructors within the program.

Cyber Crime Investigation I and II are both applied courses, which provide the opportunity for students to identify and evaluate cyber crime investigations. These courses fall under domains such as Computer Science and Program & Software Forensics, with topics within including fraud investigations, malicious logic, encryption, intrusion detection, hacking and cracking, and Internet child pornography. Computer Forensics I and II are where the majority of the domains are covered. In both courses, the students go through the entire digital forensic investigation process ranging from electronic evidence collection to analysis and report writing. Standard computer forensic

investigations are practiced in addition to data acquisition off mobile devices. Though the courses are similar in format, Computer Forensics II covers more advanced investigations including network forensics and data hiding. As for the Legal and Ethics domains, students have the option to take courses outside of those specified in the master's curriculum such as Computer Ethics and Cyber Law and Compliance. Finally, the Incident Response domain is discussed in both the Foreign and Domestic Terrorism and Enterprise Incident Response courses, which focus on incident and investigation preparation. The Quality Assurance, Control & Management, domain did not appear to be covered based on the information gathered.

4.2 Frequency Analysis

A frequency analysis was done on each set of domains to identify how often each of the domains was covered within the current state analysis. There were 11 master's programs involved in the analyses. Tables 4.1 and 4.2 display the results of the frequency analyses done on the two sets of domains. The "Frequency" column includes the total number of schools that offered a course covering that particular domain. The "Percentage" column includes the percentage of schools covering that domain.

Table 4.1 Frequency Analysis of DFCB KSA Domains

	Frequency	Percentage
Legal	10	91%
Ethics	8	73%
Storage Media	10	91%
Mobile & Embedded Devices	6	55%
Network Forensics	8	73%
Program & Software Forensics	6	55%
Quality Assurance, Control, & Management	5	45%

Table 4.2 Frequency Analysis of Beebe and Clark’s Knowledge Domains

	Frequency	Percentage
Computer Science	10	91%
Conducting Investigations	11	100%
Data Analysis	10	91%
Digital Forensic Awareness	10	91%
Documentation & Findings Communication	11	100%
Evidence Preservation & Collection	10	91%
Evidentiary Issues	9	82%
Incident Response	7	64%
Law & Ethics	10	91%
Preparation	8	73%

The frequency analysis accomplished two things. First, it validated the two sets of domains that were already in existence. Each of the DFCB (2009) domains was covered by at least half of the programs analyzed, with the exception of “Quality Assurance, Control, & Management” (which was covered by 45% of the schools). All of Beebe and Clark’s (2006) knowledge domains were covered by 60% or more of the schools. Second, the results of the frequency analyses were used to help decide which domains should be included in the suggested model curriculum.

4.3 Suggested Model Curriculum

The following standard curriculum has been developed with the intention of being used as a model in the creation of a digital forensics master’s program. The model curriculum was created by taking into account the DFCB (2009) KSA domains, Beebe and Clark’s (2006) knowledge domains, and the data gathered from this current study. Both required courses and potential electives are suggested. Course descriptions for both were written by reviewing some of the topics covered in similar courses within the programs in this study.

This curriculum is being suggested as a standard because it takes the ideas from current master’s programs and incorporates them into one general model. In addition, this curriculum has not only been created with the use of the domains in this study, but also

applied to them just as the other curricula were in Chapter 4. Table A.12 shows that all of the domains are covered by at least one of the courses in the model curriculum.

The following section includes the scope of the curriculum as well as a breakdown of the courses and their descriptions.

4.3.1 Scope

The suggested curriculum includes a list of required courses, possible electives, and descriptions of each. The required courses are those in which all digital forensics master's programs should have, regardless of the emphasis of that particular program. The electives will be available so each school can then use only the courses that support the focus of their program.

The descriptions are a general overview of what is to be covered in each of the courses. They are not extremely specific as this is meant to be a model and applicable to all schools offering a master's program in digital forensics.

In addition, while the idea of suggesting pre-requisites for each course was considered, it was decided that they would not be included in this model curriculum for two reasons. First, as mentioned earlier, there are a variety of digital forensics programs which all have their own emphasis, whether it be criminal justice, computer science, or law. Also, it would be impossible to provide course pre-requisites as each school has very different undergraduate courses. Therefore, it should be the decision of each school to determine whether they will require the students to have certain skills or have taken certain courses prior to participating in these master's courses.

Finally, the model curriculum only includes courses related to digital forensics. Each school has its own graduate program course requirements, such as statistics or research. While a course on statistics would be beneficial, and probably should be required in a Master of Science program, it was not included in this model as it did not fall under any of the domains. For this reason, non-digital forensic courses were not included as a required course or elective in this standard curriculum.

4.3.2. Courses and Descriptions

The following outlines a suggested standard digital forensics master's curriculum. Table 4.1 provides a list of the required courses and electives, which is followed by the course descriptions. The required courses are listed in the order that they should be taken. The electives can be taken at any time following the Introduction to Digital Forensics, as they have a specialized focus and only require basic prior knowledge in the area of digital forensics. Each curriculum should include all of the required courses and at least three of the electives, resulting in approximately 24 credit hours. The remaining credits can be chosen based on the school requirements and student interests.

Table 4.3 List of Required Courses and Electives

Required Courses	Electives (Specialized Courses)
Introduction to Digital Forensics	Network Forensics
Advanced Digital Forensics	Mobile Device Forensics
Research in Digital Forensics	File System Forensics
Digital Forensics Capstone Course	Anti-Forensics
Thesis or Directed Project	Incident Response
	Digital Law
	Malware Forensics

The required courses were chosen based on both the current state analyses of the programs and the frequency analyses of the domains. It was decided that the domains that were covered by 90% or more of the programs would be required in the model curriculum. Therefore, the following domains are included in one or more of the required courses as depicted in the course descriptions: Legal, Storage Media, Computer Science, Conducting Investigations, Data Analysis, Digital Forensic Awareness, Documentation & Findings Communication, Evidence Preservation & Collection, and Law & Ethics.

The remaining domains were incorporated into the curriculum as either specialized electives or as a topic to be covered in one of the courses. For example, specific electives were created based on the following domains: Network Forensics, Mobile & Embedded Devices (Mobile Device Forensics), Program & Software Forensics

(Malware Forensics), and Incident Response. Also, because the Legal and Law & Ethics domains were so popular, being covered by all but one of the programs, a specialized course on Digital Law was also listed.

Quality Assurance, Control & Management, Ethics, Evidentiary Issues, and Preparation were also covered in many of the programs, and were therefore listed as suggested topics to be covered in one or more of the courses in the model curriculum. As many of the courses within the current programs covered multiple domains, it was not appropriate to simply suggest a course called “Preparation” or “Storage Media”. On top of that, the intent of this study was to develop a standard curriculum based not only on the already existing domains, but also on what is currently being offered in other master’s programs.

The following section provides a description of each of the courses listed in the suggested model curriculum.

Required Course Descriptions:

Introduction to Digital Forensics: This introductory course should be taken in the students’ first semester and include both a lecture and hands-on section. The lecture portion should act as an overview for Digital Forensics and briefly introduce a wide range of topics including ethics, law, and digital forensic awareness. Both the lecture and lab section should prepare the students on how to conduct a digital forensic investigation at a high level, including the creation of investigation procedures, collecting and preserving evidence, imaging a hard drive or other media, examining digital evidence, and investigative report writing.

Advanced Digital Forensics: This advanced course should be thought of as “Part II” of the Introduction to Digital Forensics. The lecture portion should cover similar topics as the previous course, but in greater detail. It should also cover discussion topics such as incident response and how to prepare for a digital investigation. The lab section should allow the students to conduct multiple digital forensic investigations and include more advanced topics such as network forensics, mobile device forensics, and/or program and

software forensics. By the end of this course, the students should feel comfortable conducting various types of digital forensic investigations.

Research in Digital Forensics: This course will be a research-based seminar with optional class meetings, and will allow for flexibility within each school. It should be taken after the completion of the Introduction to Digital Forensics. Common digital forensics topics should be discussed or researched such as how to overcome challenges in digital forensics, the development of standards and certifications, case law relating to the field, and how statistics and data analysis relates to research. The resulting deliverable should contribute to the digital forensics community in some way, such as in the form of a published research paper.

Digital Forensics Capstone Course: This course should be taken in the students' final semester and encompass many of the topics learned in prior coursework. The student should complete an investigation from start to finish, including the development of an investigative plan, collection and analysis of digital evidence, writing an investigative report, and presenting their findings as an expert witness.

Thesis: Thesis credit hours should be required during the final semester(s) in which the student is working on their master's thesis. A topic should be selected based on the individual's specific research interests pertaining to the field of digital forensics.

Elective Course Descriptions:

Network Forensics: This course should be cover the identification of digital evidence on a network, capturing that data, and analyzing the digital evidence. Students should gain an understanding of packet inspection and how to view network activity to determine common versus uncommon behavior.

Mobile Device Forensics: This course should cover the preservation, collection and analysis of digital evidence on a variety of mobile devices. The specific devices used will be dependent on the availability for each school, but at a minimum should include cellular phones, SIM cards, thumb drives, and media cards. Students should gain an

understanding of various wireless preservation techniques and forensics software, including how the software works.

File System Forensics: This course should cover the identification and analysis of file systems. Students should gain an understanding of some of the common file system types (i.e, NTFS, FAT, HFS) and be able to analyze digital evidence within them.

Anti-Forensics: This course should cover topics such as data obfuscation, malicious code, and various types of data hiding including cryptography, steganography, and encryption. Students should gain an understanding of how to identify various types of data hiding and read malicious code.

Incident Response: This course should cover how to create an incident response plan as well as intrusion detection and prevention methodologies. Students should understand how to validate, assess, contain, eradicate and recover in the event of an incident.

Digital Law: At a minimum, this course should cover the following topics: privacy issues in investigations, chain of custody, Internet laws and statutes, expert witness testimony, and relevant case laws. The students should also gain an understanding of professional ethics.

Malware Forensics: This course should provide an introduction to various types of malicious code, software testing, reviewing source code, and vulnerability prevention techniques.

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

It is evident from the data gathered in this study that digital forensics topics vary from school to school. While there appear to be a few common threads across the board, the bottom line is that each program is unique in its own way. Some schools focus on the development of forensic tools, whereas others have an emphasis on law and how it relates to digital investigations. However, these differences are not such a bad thing. The field of digital forensics encompasses so many different academic areas, including science, law, criminal justice, and information technology. It is impossible for one master's program to cover all aspects of the field in the amount of detail that they need to be covered. This is one of the reasons why each program has a certain area of emphasis in which they can delve deeper. It is also why the suggested model curriculum only requires certain courses, while others remain optional. It is important that academic programs in this field offer a range of options; otherwise, the forensic examiners coming out of these programs and entering the workforce will all have the same skills and knowledge, rather than complementing one another with various specialized skill sets.

While offering a variety of topics is encouraged, some general curriculum standards are also required. The model curriculum suggested in this study was an attempt to produce the standards that are needed in this field, yet allow flexibility within each school. The required courses address the need for all master's programs in this area to cover the basic digital forensic essentials. Acquiring knowledge in digital forensic awareness, cyber law, and conducting digital investigations is a fundamental part of any program. To accomplish this, an introductory course was suggested followed by courses on advanced digital investigations, research topics, and a capstone course. To wrap up the requirements, a thesis option was suggested. The goal of including a master's thesis in a curriculum is to compel the students to choose a topic of interest and contribute new knowledge to the discipline. This standard curriculum also includes optional electives, allowing the schools to be flexible and distinct based on their emphasis. The electives were intentionally vague, allowing each program to enhance the course based on its skills and expertise.

The development of a standard curriculum is essential to the success of digital investigations. Once a standard is agreed upon within the scientific community, it will confirm the validity and quality of the programs in which many digital forensic examiners are receiving their education and knowledge. If inaccurate instructions are being provided in any given program, that misinformation could be carried on through future digital examinations, potentially ruining the integrity of the evidence and investigation. This would reflect poorly on the school as well as the discipline as a whole.

A standard curriculum could also benefit the scientific domain. The Daubert standard states that an expert witness must be "...qualified as an expert by knowledge, skill, experience, training, or education" (Cornell University Law School, 1998). The development of educational standards, including a standard curriculum, could help define what an expert in the field of digital forensics consists of.

The limitations of this particular study included only master's programs in the United States. Those interested in future research on this topic could expand this study and involve programs with both undergraduate and graduate degrees, as well as international programs. Also, only courses specific to digital forensics were involved in this study. If this research was continued, supplemental courses may want to be taken into consideration. For example, courses offered in computer security, psychology, or statistics may want to be looked at in terms of how they might complement a degree in digital forensics. Other resources could also be considered in addition to the two sets of domains used in this study. Future researchers could potentially bring in resources from public and private sector or law enforcement, rather than just academia.

This model curriculum is just a stepping-stone towards the development of a standard digital forensics master's curriculum. Its intent is to encourage discussions on the topic and perhaps be modified or enhanced in future studies. Hopefully, this model will be a key contribution in the creation of academic curriculum standards.

LIST OF REFERENCES

LIST OF REFERENCES

- American Academy of Forensic Sciences. (2009). *Forensic science education programs accreditation commission (FEPAC)*. Retrieved November 1, 2009, from: http://www.aafs.org/default.asp?section_id=aafs&page_id=committees&subpage_id=fepac
- Beebe, N.L. & Clark, J.G. (2006). Digital forensics curriculum development: Identification of knowledge domains learning objectives and core concepts. *Proceedings of the Twelfth Americas Conference on Information Systems*, Acapulco, Mexico.
- Bhaskar, R. (2006). State and local law enforcement is not ready for a cyber Katrina. *Association for Computing Machinery. Communications of the ACM*, 49(2), 81.
- Brinson, A., Robinson, A., & Rogers, M. (2006). A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Digital Investigation*, 3, 37-43.
- Carnegie Mellon. *Courses Under the Computer Forensics and Incident Response Track*. Retrieved March 22, 2010 from The Information Networking Institute: http://www.ini.cmu.edu/degrees/pgh_msistm/courses.html
- Champlain College (2009). *MS in Digital Investigation Management: Curriculum*. Retrieved February 9, 2010 from <http://extra.champlain.edu/master/msdim/curriculum.php#dim540>
- Cornell University Law School (1998). *Supreme Court of the United States: Kumho Tire Co. v. Carmichael Syllabus*. Retrieved April 11, 2010 from <http://www.law.cornell.edu/supct/pdf/97-1709P.ZS>
- Digital Forensics Association. *College Education in Digital Forensics*. Retrieved October 22, 2009 from <http://www.digitalforensicsassociation.org/masters-level/>
- Craiger, P., Ponte, L., Whitcomb, C., Pollitt, M., & Eaglin, R. (2007). Master's degree in digital forensics. *Proceedings of the 40th Hawaii International Conference on Systems Sciences (HICSS 40)*, January 2007.
- Digital Forensic Certification Board. (2009). *DFCB KSA Domains*. Retrieved November 2, 2009, from Digital Forensic Certification Board: http://www.ncfs.org/dfcb/DFCB_Final_KSAs-submitted-3-15-2009.pdf
- Eastern Michigan University. *Information Assurance – Graduate Program*. Retrieved March 20, 2010 from <http://www.emich.edu/ia/graduate.html>

- Etter, B. (2001). The forensic challenges of e-crime. *7th Indo-Pacific Congress on Legal Medicine and Forensic Sciences*, Melbourne, Australia.
- Forensic Science Education Programs Accreditation Commission. (2009). *Digital forensic science self-study report*. Unpublished manuscript, American Academy of Forensic Sciences, Colorado Springs, CO.
- George Washington University (2010). *Master of Forensic Sciences in High Technology Crime Investigation*. Retrieved March 25, 2010, from George Washington University: http://nearyou.gwu.edu/htc/htc_brochure.pdf
- Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., & Stein, M. (2005). Computer forensics programs in higher education: A preliminary study. *SIGCSE Bull.* 37, 1 (Feb. 2005), 147-151.
- Institute for the Advancement of the American Legal System. (2007). *Navigating the hazards of e-Discovery: A manual for judges in state courts across the nation*. Retrieved November 1, 2009, from University of Denver: <http://www.du.edu/legalinstitute/publications2007.html>
- John Jay College of Criminal Justice. *Master of Science in Forensic Computing*. Retrieved January 21, 2010 from <http://www.jjay.cuny.edu/academics/690.php#Courses>
- McGuire, T. J., & Murff, K. N. (2006). Issues in the development of a digital forensics curriculum. *Journal of Computing in Small Colleges.* 22, 2 (Dec. 2006), 274-280.
- Meyers, M., & Rogers, M. (2004). Computer forensics: The need for standardization and certification. *International Journal of Digital Evidence*, 3(2).
- Purdue University. *Cyber Forensics Master's Area of Specizlization*. Retrieved April 2, 2010 from <http://cyberforensics.purdue.edu/masters.aspx>
- Rogers, M., & Seigfried, K. (2003). The future of computer forensics: A needs analysis survey. *Computers & Security*, 23, 12-16.
- Sam Houston State University (2009). *Digital Forensics Course Descriptions*. Retrieved February 23, 2010, from Sam Houston State University Graduate Catalog: <http://www.shsu.edu/gradcat/df.html>
- Scientific Working Group on Digital Evidence. (1999). Digital evidence: Standards and principles. *Forensic Science Communications*, April 2000, 2 (2).
- Shanklin, T. (2009). *Digital forensics as a scientific discipline: Gap analysis in forensics education*. Unpublished manuscript, Purdue University, West Lafayette, IN.

- Stambaugh, H., Beaupre, D., Icove, D. J., Baker, R., Cassaday, W., & Williams, W. P. (2000). State and local law enforcement needs to combat electronic crime. *National Institute of Justice Research in Brief*.
- Stevenson University (2009). *School of Graduate and Professional Studies Catalog*. Retrieved March 12, 2010 from <http://catalog.stevenson.edu/pdf/graduate09.pdf>
- Technical Analysis Group. (2002). *Law enforcement tools and technologies for investigating cyber attacks: A national needs assessment*. Retrieved October 23, 2009, from Institute for Security Technology Studies: <http://www.ists.dartmouth.edu/projects/archives/lana.html>
- Texas State University. *Master of Science, Minor in Forensic Systems: Course Requirements*. Retrieved March 2, 2010 from http://www.cs.txstate.edu/grad_program/msfs.php#introduction
- Troell, L., Pan, Y., & Stackpole, B. (2003). Forensic course development. Proceedings of the 4th conference on information technology curriculum on Information technology education. *ACM Press NY*, 265-269.
- University of Central Florida. *Master of Science in Digital Forensics: Curriculum*. Retrieved March 17, 2010 from <http://msdf.ucf.edu/curriculum.html>
- University of New Haven. *Criminal Justice: Concentration in Forensic Computer Investigation*. Retrieved February 17, 2010 from <http://www.newhaven.edu/5927/#FCI>
- University of Rhode Island (2008). *Computer Science Course Descriptions*. Retrieved February 17, 2010 from <http://www.cs.uri.edu/academics/course-descriptions/cs-course-descriptions/>
- West Virginia University Forensic Science Initiative. (2007). *Technical working group for education and training in digital forensics*. Retrieved October 7, 2009, from National Criminal Justice Reference Service: <http://www.ncjrs.gov/pdffiles1/nij/grants/219380.pdf>
- Yasinac, A., Erbacher, R., Marks, D., Pollitt, M., and Sommer, P. (2003). Computer forensics education. *IEEE Security & Privacy*, July/August 2003, 15-23.

APPENDIX

APPENDIX

Table A.1 Carnegie Mellon University

DFCB KSA Domains	Legal	Ethics	Storage Media	Mobile & Embedded Devices	Network Forensics	Program & Software Forensics	Quality Assurance, Control, & Management
14-761: Advanced Information Assurance	X	X	X		X	X	X
14-822: Host-Based Forensics			X	X			X
14-823: Network Forensics			X		X		
14-824: Advanced Host-Based Forensic Analysis			X	X			
14-825: Advanced Network Analysis			X		X		
14-826 Event Reconstruction and Correlation			X				

Beebe and Clark's Knowledge Domains	Computer Science	Conducting Investigations	Data Analysis	Digital Forensic Awareness	Documentation and Findings Communication	Evidence Preservation & Collection	Evidentiary Issues	Incident Response	Law & Ethics	Preparation
14-761: Advanced Information Assurance		X	X	X	X	X	X	X	X	X
14-822: Host-Based Forensics	X	X	X	X	X	X				X
14-823: Network Forensics	X	X	X		X	X		X		X
14-824: Advanced Host-Based Forensic Analysis	X	X	X		X	X				X
14-825: Advanced Network Analysis	X	X	X		X	X				X
14-826 Event Reconstruction and Correlation		X	X		X					X

Table A.2 George Washington University

DFCB KSA Domains	Legal	Ethics	Storage Media	Mobile & Embedded Devices	Network Forensics	Program & Software Forensics	Quality
							Assurance, Control, & Management
FORS 259: Computer-Related Law	X						
FORS 265: Ethics and Leadership		X					
FORS 277: Computer Forensic I - Investigation and Evidence Gathering			X		X		
FORS 279: Intrusion I - Understanding and Identifying Network-Based Attacks					X		
FORS 285: High Technology Crime Investigation Capstone Course			X				
FORS 274: Video Forensic Analysis			X				
FORS 278: Computer Forensics II - Evidence and Analysis			X				
FORS 280: Intrusion II - Investigating Network-based Attacks					X		
FORS 283: Steganography and Electronic Watermarking			X				
FORS 290: Selected Topics							
FORS 295: Research							
FORS 298: Forensic Sciences Practicum	X		X				

Beebe and Clark's Knowledge Domains	Computer Science	Conducting Investigations	Data Analysis	Digital Forensic Awareness	Documentation and Findings Communication	Evidence Preservation & Collection	Evidentiary Issues	Incident Response	Law &	Preparation
									Ethics	
FORS 259: Computer-Related Law							X		X	
FORS 265: Ethics and Leadership									X	
FORS 277: Computer Forensic I - Investigation and Evidence Gathering		X	X	X						
FORS 279: Intrusion I - Understanding and Identifying Network-Based Attacks										
FORS 285: High Technology Crime Investigation Capstone Course		X	X		X	X				X
FORS 274: Video Forensic Analysis			X							
FORS 278: Computer Forensics II - Evidence and Analysis			X			X	X			
FORS 280: Intrusion II - Investigating Network-based Attacks		X	X							
FORS 283: Steganography and Electronic Watermarking	X	X	X							
FORS 290: Selected Topics										
FORS 295: Research										
FORS 298: Forensic Sciences Practicum		X	X		X	X				

Table A.3 John Jay College

DFCB KSA Domains	Legal	Ethics	Storage Media	Mobile & Embedded Devices	Network Forensics	Program & Software Forensics	Quality Assurance, Control, & Management
Forensic Computing/Criminal Justice 752: The Law and High Technology Crime	X						
Criminal Justice 710: Issues in Criminal Justice I	X						
Criminal Justice/Forensic Computing 727: Cybercriminology							
Forensic Computing 753: Digital Forensics Applications			X	X			
Forensic Computing 700: Theoretical Foundations of Computing							
Forensic Computing 710: Architecture of Secure Operating Systems							
Forensic Computing 742: Network Security							
Forensic Computing 740: Data Communications and Forensics Security							
Forensic Computing 745: Network Forensics					X	X	
Forensic Computing 760: Forensic Management of Digital Evidence		X					X
Criminal Justice 708: Law, Evidence and Ethics	X	X					
CRJ 733: Constitutional Law	X						
CRJ 750/PAD 750: Security of Information and Technology							
Forensic Computing 780: Capstone Seminar and Fieldwork	X	X	X				
Forensic Computing 791: Forensic Computing Prospectus Seminar							

Beebe and Clark's Knowledge Domains	Computer Science	Conducting Investigations	Data Analysis	Digital Forensic Awareness	Documentation and Findings Communication	Evidence Preservation & Collection	Evidentiary Issues	Incident Response	Law & Ethics	Preparation
Forensic Computing/Criminal Justice 752: The Law and High Technology Crime									X	
Criminal Justice 710: Issues in Criminal Justice I									X	
Criminal Justice/Forensic Computing 727: Cybercriminology										
Forensic Computing 753: Digital Forensics Applications		X	X		X	X	X			
Forensic Computing 700: Theoretical Foundations of Computing										
Forensic Computing 710: Architecture of Secure Operating Systems										
Forensic Computing 742: Network Security	X									
Forensic Computing 740: Data Communications and Forensics Security										
Forensic Computing 745: Network Forensics										
Forensic Computing 760: Forensic Management of Digital Evidence				X			X			
Criminal Justice 708: Law, Evidence and Ethics									X	
CRJ 733: Constitutional Law									X	
CRJ 750/PAD 750: Security of Information and Technology								X		
Forensic Computing 780: Capstone Seminar and Fieldwork		X	X		X	X	X			
Forensic Computing 791: Forensic Computing Prospectus Seminar										

Table A.4 Purdue University

DFCB KSA Domains	Legal	Ethics	Storage Media	Mobile & Embedded Devices	Network Forensics	Program & Software Forensics	Quality Assurance, Control, & Management
CIT 556 - Basic Computer Forensics	X		X				X
CIT 557 - Advanced Research Topics in Cyber Forensics	X	X					X
CIT 499d - Small Scale Digital Device Forensics				X			
CITxxx - Expert Witness Testimony	X	X					X
CIT 581v - Current Topics							
CIT 499e - Hardware Essentials			X				
CIT 499c - File System Forensics			X				
Internship	X	X	X	X			X
Elective							

Beebe and Clark's Knowledge Domains	Computer Science	Conducting Investigations	Data Analysis	Digital Forensic Awareness	Documentation and Findings Communication	Evidence Preservation & Collection	Evidentiary Issues	Incident Response	Law & Ethics	Preparation
CIT 556 - Basic Computer Forensics	X	X	X	X	X	X	X		X	X
CIT 557 - Advanced Research Topics in Cyber Forensics				X					X	
CIT 499d - Small Scale Digital Device Forensics			X			X				
CITxxx - Expert Witness Testimony		X	X		X	X	X		X	
CIT 581v - Current Topics										
CIT 499e - Hardware Essentials										
CIT 499c - File System Forensics	X									
Internship		X	X		X	X	X			
Elective										

Table A.5 Sam Houston State University

DFCB KSA Domains	Legal	Ethics	Storage Media	Mobile & Embedded Devices	Network Forensics	Program & Software Forensics	Quality Assurance, Control, & Management
DF 534: Digital Security			X				
DF 583: Digital Forensics Investigation		X	X				
DF 584: Software Forensics Evidence Management						X	
DF 630: Cyber Law	X	X					
DF 531: Principle and Policy in Information Assurance							X
DF 535: Malware						X	
DF 560: Special Topics			X	X			
DF 587: File Systems Forensics			X				
DF 589: Disaster Recovery							
DF 670: Internship			X				

Beebe and Clark's Knowledge Domain	Computer Science	Conducting Investigations	Data Analysis	Digital Forensic Awareness	Documentation and Findings Communication	Evidence Preservation & Collection	Evidentiary Issues	Incident Response	Law & Ethics	Preparation
DF 534: Digital Security						X				
DF 583: Digital Forensics Investigation		X	X	X	X	X	X		X	
DF 584: Software Forensics Evidence Management	X									
DF 630: Cyber Law									X	
DF 531: Principle and Policy in Information Assurance										
DF 535: Malware	X									
DF 560: Special Topics		X	X		X	X	X			
DF 587: File Systems Forensics		X	X		X	X	X			
DF 589: Disaster Recovery								X		X
DF 670: Internship		X	X		X	X	X			

Table A.6 Stevenson University

DFCB KSA Domains	Legal	Ethics	Storage Media	Mobile & Embedded Devices	Network Forensics	Program & Software Forensics	Quality Assurance, Control, & Management
FSCOR 601: Criminal Justice							
FSCOR 604: Evidence							
FSCOR 606: Internet Research							
FSCOR 607: Forensics Review Journal							
FSCOR 664: Litigation Practice and Procedure							
FSCOR 702: Mock Trial Capstone	X	X	X	X			
FSIS 600: Computer and Network Essentials for Forensic Investigators							
FSIS 640: Technology Law and Enforcement Activities	X						
FSIS 642: File Systems Forensic Analysis			X				
FSIS 643: Incident Response and Evidence Collection	X	X					
FSIS 644: Windows Forensic Examinations			X				
FSIS 646: Windows Intrusion Forensic Investigations					X		
FSIS 648: Disaster Recovery							
FSIS 650: Hacking Exploits and Intrusion Detection					X		

Beebe and Clark's Knowledge Domains	Computer Science	Conducting Investigations	Data Analysis	Digital Forensic Awareness	Documentation and Findings Communication	Evidence Preservation & Collection	Evidentiary Issues	Incident Response	Law & Ethics	Preparation
FSCOR 601: Criminal Justice										
FSCOR 604: Evidence										
FSCOR 606: Internet Research										
FSCOR 607: Forensics Review Journal										
FSCOR 664: Litigation Practice and Procedure										
FSCOR 702: Mock Trial Capstone		X	X		X	X	X		X	
FSIS 600: Computer and Network Essentials for Forensic Investigators	X									
FSIS 640: Technology Law and Enforcement Activities									X	
FSIS 642: File Systems Forensic Analysis	X		X							
FSIS 643: Incident Response and Evidence Collection					X	X	X	X		
FSIS 644: Windows Forensic Examinations		X	X							
FSIS 646: Windows Intrusion Forensic Investigations		X	X					X		
FSIS 648: Disaster Recovery								X		X
FSIS 650: Hacking Exploits and Intrusion Detection			X							

Table A.7 Texas State University

DFCB KSA Domains	Legal	Ethics	Storage Media	Mobile & Embedded Devices	Network Forensics	Program & Software Forensics	Quality Assurance, Control, & Management
CS 5369F: Digital Forensics			X		X	X	
CS 5369R: Digital Forensics Research							

Beebe and Clark's Knowledge Domains	Computer Science	Conducting Investigations	Data Analysis	Digital Forensic Awareness	Documentation and Findings Communication	Evidence Preservation & Collection	Evidentiary Issues	Incident Response	Law & Ethics	Preparation
CS 5369F: Digital Forensics	X	X	X	X	X	X	X			
CS 5369R: Digital Forensics Research										

Table A.8 University of Central Florida

DFCB KSA Domains	Legal	Ethics	Storage Media	Mobile & Embedded Devices	Network Forensics	Program & Software Forensics	Quality Assurance: Control: & Management
CGS 5131: Computer Forensics I	X		X				
CGS 5132: Computer Forensics II	X				X	X	
CHS 5503: Topics in Forensic Science							X
CET 6887: The Practice of Digital Forensics	X	X	X		X	X	X
CAP 6133: Advanced Topics in Computer Security and Computer Forensics					X	X	
CNT 6519: Wireless Security and Forensics							
CAP 6135: Malware and Software Vulnerability Analysis						X	
COP 6525: Distributed Processing of Digital Evidence							
CIS 6395 Incident Response Technologies					X	X	
CIS 6386 OS & File System Forensics			X				
CCJ 6074: Investigative and Intelligence Analysis, Theory and Methods							
CCJ 6706: Quantitative Methods and Computer Utilization in Criminal Justice or ESI 5219 Engineering Statistics							
PLA 5587: Current Issues in Cyberlaw	X						
CHS 5596: Forensic Expert in the Courtroom	X	X					
CHS 5518: Forensic Examination of Digital Evidence or CJE 5688: Cybercrime and Criminal Justice	X						

Beebe and Clark's Knowledge Domains	Computer Science	Conducting Investigations	Data Analysis	Digital Forensic Awareness	Documentation and Findings Communication	Evidence Preservation & Collection	Evidentiary Issues	Incident Response	Law & Ethics	Preparation
CGS 5131: Computer Forensics I									X	
CGS 5132: Computer Forensics II						X	X		X	
CHS 5503: Topics in Forensic Science				X					X	
CET 6887: The Practice of Digital Forensics		X	X		X	X	X			
CAP 6133: Advanced Topics in Computer Security and Computer Forensics	X									
CNT 6519: Wireless Security and Forensics										
CAP 6135: Malware and Software Vulnerability Analysis	X									
COP 6525: Distributed Processing of Digital Evidence										
CIS 6395: Incident Response Technologies								X		
CIS 6386: OS & File System Forensics		X	X							
CCJ 6074: Investigative and Intelligence Analysis, Theory and Methods										
CCJ 6706: Quantitative Methods and Computer Utilization in Criminal Justice or ESI 5219 Engineering Statistics										
PLA 5587: Current Issues in Cyberlaw									X	
CHS 5596: Forensic Expert in the Courtroom									X	
CHS 5518: Forensic Examination of Digital Evidence or CJE 5688: Cybercrime and Criminal Justice				X					X	X

Table A.9 University of New Haven

DFCB KSA Domains	Legal	Ethics	Storage Media	Mobile & Embedded Devices	Network Forensics	Program & Software Forensics	Quality Assurance, Control, & Management
CJ 600: Computer Crime: Legal Issues and Investigative Procedures	X						
CJ 603: Internet Vulnerabilities and Criminal Activity	X						
CJ 604: Network Security, Data Protection, and Telecommunication							

Beebe and Clark's Knowledge Domains	Computer Science	Conducting Investigations	Data Analysis	Digital Forensic Awareness	Documentation and Evidence Findings Communication	Preservation & Evidence Collection	Evidentiary Issues	Incident Response
CJ 600: Computer Crime: Legal Issues and Investigative Procedures		X		X				
CJ 603: Internet Vulnerabilities and Criminal Activity					X			
CJ 604: Network Security, Data Protection, and Telecommunication								X

Table A.10 University of Rhode Island

DFCB KSA Domains	Legal	Ethics	Storage Media	Mobile & Embedded Devices	Network Forensics	Program & Software Forensics	Quality Assurance, Control, & Management
CSC414: Computer System Fundamentals			X				
CSC485: Computer Forensics	X	X	X				
CSC486: Network Forensics	X				X		
CSC590: Digital Forensics Research/Practicum			X				
Research/Thesis							

Beebe and Clark's Knowledge Domains	Computer Science	Conducting Investigations	Data Analysis	Digital Forensic Awareness	Documentation and Evidence Findings Communication	Preservation & Collection	Evidentiary Issues	Incident Response	Law & Ethics	Preparation
CSC414: Computer System Fundamentals	X									
CSC485: Computer Forensics		X	X	X	X	X			X	
CSC486: Network Forensics		X	X			X			X	
CSC590: Digital Forensics Research/Practicum			X							
Research/Thesis										

Table A.11 University of Eastern Michigan

DFCB KSA Domains	Legal	Ethics	Storage Media	Mobile & Embedded Devices	Network Forensics	Program & Software Forensics	Quality Assurance, Control, & Management
IA 533 Cyber Crime Investigation I			X				
IA 557 Cyber Crime Investigation II						X	
IA 558 Computer Forensics I	X		X	X			
IA 559 Computer Forensics II			X	X	X		
SSC 529 Foreign and Domestic Terrorism							
IA 691 Enterprise Incident Response							

Beebe and Clark's Knowledge Domains	Computer Science	Conducting Investigations	Data Analysis	Digital Forensic Awareness	Documentation and Evidence Findings Communication	Preservation & Collection	Evidentiary Issues	Incident Response	Law & Ethics	Preparation
IA 533 Cyber Crime Investigation I		X								
IA 557 Cyber Crime Investigation II	X	X								
IA 558 Computer Forensics I		X	X	X	X	X	X		X	
IA 559 Computer Forensics II		X	X		X	X	X			
SSC 529 Foreign and Domestic Terrorism								X		X
IA 691 Enterprise Incident Response								X		X

Table A.12 Model Curriculum

DFCB KSA Domains	Legal	Ethics	Storage Media	Mobile & Embedded Devices	Network Forensics	Program & Software Forensics	Quality Assurance, Control, & Management
Introduction to Digital Forensics	X	X	X				
Advanced Digital Forensics			X	X	X	X	
Research in Digital Forensics	X						X
Digital Forensics Capstone Course			X				
Network Forensics			X		X		
Mobile device Forensics			X	X			
File System Forensics			X				
Anti-Forensics						X	
Incident Response					X		
Digital Law	X	X					
Malware Forensics						X	

Beebe and Clark's Knowledge Domains	Computer Science	Conducting Investigations	Data Analysis	Digital Forensic Awareness	Documentation and Findings Communication	Evidence Preservation & Collection	Evidentiary Issues	Incident Response	Law & Ethics	Preparation
Introduction to Digital Forensics		X	X	X	X	X	X		X	
Advanced Digital Forensics	X	X	X		X	X		X		X
Research in Digital Forensics									X	
Digital Forensics Capstone Course		X	X		X	X	X			X
Network Forensics		X	X		X	X				
Mobile device Forensics		X	X		X	X				
File System Forensics	X									
Anti-Forensics	X									
Incident Response								X		
Digital Law									X	
Malware Forensics	X	X	X		X	X				