12-31-2006

Digital Forensics Curriculum Development: Identification of Knowledge Domains Learning Objectives and Core Concepts

Nicole Lang Beebe
The University of Texas at San Antonio

Jan Guynes
The University of Texas at San Antonio

Digital Forensics Curriculum Development: Identification of Knowledge Domains, Learning Objectives, and Core Concepts

Nicole Lang Beebe
The University of Texas at San Antonio
Nicole.beebe@utsa.edu

Jan Guynes Clark
The University of Texas at San Antonio
Jan.clark@utsa.edu

ABSTRACT

Digital forensics course offerings are being added to various curricula at colleges and universities world-wide at an amazing pace. This is due to significant student interest in the topic and job market demands for such skill sets. However, academia is struggling to establish a firm knowledge base and offer quality digital forensics education to its students. We contend that the identification and community acceptance of digital forensics knowledge domains, learning objectives, and core concepts is imperative to effectively and efficiently *educating* students in digital forensics. We argue that this goal has yet to be achieved. The purpose of this research and paper is to qualitatively test that presumption, and to methodologically identify and propose a set of digital forensics knowledge domains, supporting learning objectives, and necessary core concepts. Toward that end, we qualitatively analyzed digital forensics syllabi from 42 different colleges and universities and supplemented the analysis with our knowledge and experience. We conclude that our presumption is indeed correct, and thus propose a more structured approach toward digital forensics education and support it by presenting model course syllabi.

Keywords

Digital forensics, computer forensics, cyber forensics, curriculum, education, knowledge domain, taxonomy.

INTRODUCTION

Responding to computer and network security incidents often necessitates some form of digital investigation. The investigation may simply be a function of validating a suspicion, assessing the impact, and employing containment, eradication, and recovery strategies, or it may entail much more. The organization might decide to formally investigate—to preserve, collect, and analyze "evidence[1]" pertaining to a security incident to protect themselves (i.e. from liability or future incidents), or to support disciplinary and/or judicial action. This is the essence of digital forensics. Regardless of the motivation, an information security program that lacks an ability to conduct a digital investigation is incomplete. As more and more organizations are realizing this, the demand for information systems and information security personnel with education, training, and/or experience in digital forensics is increasing sharply.

The demand for individuals trained and/or educated in digital forensics is not limited to business. It is arguable that the need and the discipline itself started in law enforcement (Palmer, 2002). Unlike the traditional forensic science field, digital forensics emerged out of necessity, and its procedures, tools, and techniques were largely developed by law enforcement and those commercial entities serving law enforcement. The need is a function of the fact that computers are targeted for the information they contain; they are used to facilitate crime; and, the digital realm has become a new venue for committing crime. As computing becomes more and more ubiquitous, so does digital evidence. The natural by-product is a significant demand for more and more educated, trained, certified, and experienced digital forensic examiners/analysts. Today, computer crime investigators and digital forensic examiners and analysts exist at all levels of law enforcement (local, state, and federal), and formal computer forensics laboratories are becoming the norm.

Educational institutions traditionally respond to job market demands, and digital forensics is clearly demanded in both the private and pubic sectors. These institutions seek to develop students' intellectual skills, while teaching them core concepts

[1] The authors use the term "evidence" to apply to information of value derived from data, independent of whether the investigation is forensic or non-forensic in nature (the distinction being whether judicial actions are sought).

in relation to an academic field. Both pursuits are designed to "grow" better people, as well as prepare them for future employment. Traditional baccalaureate and graduate degree programs are not designed to "train" students for future jobs. Instead, they are designed to prepare students for the intellectual tasks associated with future jobs. But, intellectual growth related to job market forces is not the only driving factor; student interest plays a key role in course offerings as well. The "CSI effect" is a term coined to capture the recent increase in forensic science by non-scientists. The application of scientific knowledge to investigations is of great interest to people, including students (Willing, 2004). Students have found that digital forensics jobs range from $85,000-$120,000 per year, with management positions earning up to $160,000 (WorldWideLearn, 2005). Because of the "CSI effect" and job market demands, student interest in digital forensics college courses is strong and only increasing.

Because of student interest and commercial and governmental demand, new digital forensics course offerings are emerging in information systems, computer science, and criminal justice curricula at a phenomenal pace. While the exact number of college-level digital forensics courses is not known, the recent emergence of groups such as IFIP Working Group 11.9 on Digital Forensics and the Digital Forensics Working Group (DFWG) are evidence of the keen interest by academia in such curriculum development endeavors. Our experience suggests, however, that there is little consensus amongst academics regarding what should be taught and how it should be taught.

The purpose of this research was to review digital forensics course syllabi and *propose* a more structured approach toward digital forensics education. We relied upon these syllabi and prior experience to identify a parsimonious, yet ostensibly complete set of knowledge domains, learning objectives and core concepts for digital forensics courses. Model course outlines for these courses are also provided. It is our hope that the proposed ideas will facilitate discussion that will lead to a more methodologically rigorous means of identifying and validating knowledge domains, learning objectives and core concepts for collegiate digital forensics courses.

EDUCATION VERSUS TRAINING

Training refers to a narrowly focused program of instruction that leads to skill proficiency. It informs a student how to perform a given task, but not why. It provides technical, methodological, procedural, and factual knowledge. Conversely, education is more far-reaching. It is intellective by nature and encourages the student to think and problem-solve. The student learns to ponder and answer such questions as: Is there a better way to perform this task? Given several tasks, which one is most important? If the task cannot be performed in the standard way, can it be accomplished another way? If so, how? Is the standard way of performing the task the best way?

Digital forensics investigators (DFIs) need to understand more than simply how to perform a task, and it is the role of education to provide that foundational understanding. Such a foundation permits DFIs to effectively and efficiently respond to changing technology and problem sets. Simply put, tasks change. Digital forensic tasks in today's environment are very different from those only a few years ago. Hardware, software, and the potential perpetrator are all far more sophisticated. The DFI needs to be able to identify and define problems—to think "outside the box". Similar to other types of "knowledge work," investigators must react to an infinite combination of situations and scenarios. While similarities may exist, the variance is huge. Therefore, the DFI requires a thorough understanding of the basic fundamentals of digital forensics, as well as strong problem-solving skills.

DATA COLLECTION AND DISCUSSION

Sample

Through the IFIP WG 11.9 on Digital Forensics, the DFWG, extensive Internet-based searching, and academic listserves pertaining to information security, we identified 87 digital forensics courses currently incorporated into active curriculum. We subsequently obtained and qualitatively reviewed the course syllabi for 61 of those courses (we were unable to obtain syllabi for the remaining 26 courses). Receipt of the syllabi was facilitated by public posting on the Internet and email contact with instructors of record. Thirteen of the 61 syllabi were subsequently removed from the sample for a variety of reasons: (1) inadequate information available, (2) course content predominantly geared toward information and/or network security, with only a small focus on digital forensics, or (3) non-traditional course (e.g. internship). The remaining 48 qualitatively reviewed syllabi represented 42 colleges and universities located world-wide, although the majority were located in the U.S. (only syllabi written in English were sampled and reviewed). Twenty-five of the courses were offered at

the undergraduate level, sixteen were graduate courses, and nine were combined graduate-undergraduate courses[2]. The courses were offered in a variety of departments. We loosely categorized these departments, as shown in Table 1.

DEPARTMENT	FREQUENCY
Computer Science (and combined computer science depts.)	21
Computer Technology	4
Criminal Justice	5
Engineering	2
Information Security and/or Digital Forensics	4
Information Systems and Technology	9
Unknown	3
Total	**48**

Table 1. Department Distribution of Digital Forensics Course Offerings

Data Collection

Each syllabus was qualitatively reviewed and the following data was extracted:

- University
- Department
- Course number
- Course name
- Level (undergraduate, graduate, combined)
- Prerequisites
- Required reading
- Learning objectives
- Topics covered
- Laboratory credit (i.e. 3-credit course plus 1-credit laboratory session)
- Application of experiential learning methodology (hands-on labs assigned)
- Focus on media forensics, network forensics, both[3]

DATA ANALYSIS AND CURRICULUM DEVELOPMENT

Digital Forensics Knowledge Domains

Knowledge domains are a reasonably small, commonly accepted set of knowledge areas critical to a field of knowledge. It is toward the mastery of these knowledge domains that educators seek to educate students. It is our contention that the knowledge domains of digital forensics have yet to be identified, defined, and widely accepted. The resultant impact is an unacceptable level of variance in digital forensics education, which is neither helpful to students nor to their potential employers.

[2] Course level (graduate vs. undergraduate) was clear in some cases and assumed in others. Assumptions were based on standard course numbering conventions (e.g. 1-4xxx is undergraduate, whereas 5-6xxx is graduate).

[3] Media forensics is the study of analyzing digital *media* in order to confirm or refute allegations and/or obtain intelligence information. Network forensics is "the study of analyzing network activity in order to discover the source of security policy violations or information assurance breaches" (Mukkamala and Sung 2003: 1).

We qualitatively reviewed each syllabus for some semblance of commonly accepted digital forensics domains. Knowledge domains were not explicitly evident. However, we acknowledge that they are rarely articulated in individual course syllabi. As a result, we concentrated on identifying learning objectives and topics covered. From the syllabi, we identified two-hundred and twelve (212) learning objectives and six-hundred (600) topics. (Note: These are raw numbers and represent some repetition across learning objectives and topics.) The analysis confirmed the notion that the field of digital forensics is extremely broad in scope. Since the vast majority of colleges and universities only offer one digital forensics course, there is a huge variance in the knowledge imparted from one course to another.

In an effort to identify a proposed set of digital forensics knowledge domains, we qualitatively reduced the learning objectives to a set of 63 unique learning objectives. To do so, we relied largely on our digital forensics and academic experience to subjectively aggregate conceptually related learning objectives (i.e. "understand the 4th Amendment" and "be able to apply 18USC§2703(d)" can be aggregated to "be able to identify and apply computer crime related laws"). From that reduced set, we identified and proposed a set of ten digital forensics knowledge domains. The domains are as follows (presented alphabetically) and will be enumerated in greater detail in the next section.

1. Computer Science
2. Data Analysis
3. Digital Forensics Awareness
4. Documentation & Findings Communication
5. Evidence Preservation & Collection
6. Evidentiary Issues
7. Incident Response
8. Investigations
9. Law & Ethics
10. Preparation

Learning Objectives

Learning objectives represent desired student ability upon completion of the course. Table 2 shows how we mapped the learning objectives to their respective digital forensics knowledge domain.

Another important consideration in the curriculum development process is the determination of the desired level of mastery for each learning objective. Bloom's cognitive taxonomy (1956) is prevalently used in instructional design and education research to articulate the desired level of cognitive ability. Starting from the lowest to the highest level of cognition, the taxonomy is as follows (Srinivas, 2006).

1. Knowledge: ability to remember or recall previously learned material (i.e. facts)
2. Comprehension: ability to understand or explain the meaning of material and identify relationships
3. Application: ability to apply concepts and principles
4. Analysis: ability to analyze and break down a problem into subsets
5. Synthesis: ability to build up and compose to create a new whole
6. Evaluation: ability to appraise or judge the value of an idea or thought

Srinivas (2006) provides a list of verbs that reflect the various levels of cognitive ability reflected in Bloom's taxonomy. This list was cross-referenced against the verbs used in syllabi learning objectives to identify the desired level of cognitive ability associated with each learning objective. Where instructors omitted the use of verbs entirely, or where learning objective verbs were not on Srinivas's list, subjective judgment based on verb similarity, practical experience, and academic experience was utilized to identify the desired level of cognitive ability. Results of the analysis are shown in Table 2.

We acknowledge that there will likely be variability of opinion concerning the desired level of cognitive ability (AKA "mastery") for each learning objective. On the one hand, some degree of variability will be a function of the defined scope and intent of the program identified by each institution and their unique needs. On the other hand, the digital forensics education community should strive to achieve a reasonable level of consensus on this matter. If one considers more

Knowledge Domain	Learning Objective	Taxonomy Level
Computer Science	Password cracking	Application
	"Cause and effect" parameters of digital artifacts	Comprehension
	Data hiding mechanisms (data streams, steganography, watermarking, encryption, etc.)	Comprehension
	Disk geometry & addressing (cylinders, heads, sectors, clusters/allocation units, slack)	Comprehension
	File systems & concepts (partitions, boot records, file systems (FAT vs. NTFS vs. EXT3, etc.))	Comprehension
	Hashing - purpose, use in digital forensics, algorithms	Comprehension
	Intrusion detection & prevention methodologies (signature vs. anomaly, session termination,)	Comprehension
	Malicious code ("cause and effect")	Comprehension
	Operating systems (processes, RAM, swap/page files, Registry, libraries, I/O interfacing)	Comprehension
	Startup ("boot") and shutdown process	Comprehension
Conducting Investigations	Investigative techniques & procedures	Application
	How to create an investigation plan	Comprehension
	How to process a digital crime scene	Comprehension
	Investigative process (phases/steps and order of execution)	Comprehension
Data Analysis	Data examination/analysis - email	Application
	Data examination/analysis - file recovery by file type	Application
	Data examination/analysis - string search results analysis and data conversion/reconstruction	Application
	Data extraction - data location via string searching	Application
	Data extraction - email	Application
	Data extraction - file recovery by file type	Application
	Deleted file recovery	Application
	Digital forensic tools for data analysis - hardware	Application
	Digital forensic tools for data analysis - software	Application
	Evaluating metadata (e.g. file attributes or 'properties')	Application
	File/data comparison via hashing	Application
	How to "traceback" intrusions technically	Application
	Identifying and locating hidden data	Application
	Reconstruct and evaluate network traffic/sessions	Application
	Reconstruct events from audit logs	Application
	Recovering hidden data	Application
	User Internet history - event reconstruction	Application
	User Internet history - recovery	Application
	Factors that limit the conclusions that can be drawn from digital artifacts	Comprehension
	How to attribute digital artifacts to specific individuals	Comprehension

Table 2. Digital Forensics Learning Objectives Mapped to Knowledge Domains and Taxonomy **(cont. on next page)**

Domain	Learning Objective	Level
Digital Forensic Awareness	How to conduct cost-benefit analysis of potential investigation	Comprehension
	Audit logs -- types, location, information recorded, etc.	Knowledge
	Computer criminology (types of threats, sociology, psychology)	Knowledge
	Digital forensic lab accreditation standards and process	Knowledge
	Digital forensic tools and their capabilities	Knowledge
	Digital forensics and computer crime investigations as a profession	Knowledge
	Importance of digital forensic tool testing	Knowledge
	Need for digital forensics in various capacities (business, law enforcement, military, government)	Knowledge
	Role of technology in digital forensics	Knowledge
	Types of computer crimes	Knowledge
	Various types / sources of digital evidence (small/removable devices, hard drives, network storage)	Knowledge
Documentation & Findings Commun.	Investigative report writing	Application
	How to provide expert testimony	Comprehension
Evidence Preservation & Collection	Digital forensic tools for data collection - hardware	Application
	Digital forensic tools for data collection - software	Application
	Forensic imaging of static and volatile data/devices	Application
	Usefulness of various types of audit logs to various types of investigations	Comprehension
Evidentiary Issues	Determining evidentiary value of recovered data/information	Comprehension
	Evidence preservation - Need	Comprehension
	Evidence preservation - Process	Comprehension
	Rules of evidence for court admissibility	Knowledge
Incident Response	Incident response purpose and process (law enforcement and non-law enforcement capacity)	Comprehension
	How to validate, assess, contain, eradicate, and recover	Comprehension
Law & Ethics	Ethical implications of digital forensics	Comprehension
	How to "traceback" intrusions through the legal system	Comprehension
	Computer crime laws	Knowledge
	Laws governing investigative procedure (legal search & seizure, privacy protection, case law, etc.)	Knowledge
Preparation	How to create a useful incident response plan	Comprehension
	How to create useful incident response plans & policy	Comprehension
	How to prepare for conducting digital investigations and digital forensic investigations	Comprehension
	How to set up an investigative office and/or laboratory	Comprehension

Table 2. Digital Forensics Learning Objectives Mapped to Knowledge Domains and Taxonomy

established fields, such as mathematics or even computer science, one will find relative consensus regarding which topics should be taught to which level of cognitive understanding. The proposed categorization was derived from qualitative review of syllabi, and should thus emerge as a "good start." Further discourse and convergence within the community, however, is needed.

Core Concepts

It is critical that educators focus first and foremost on achieving student understanding and internalization of core concepts. Core concepts have many uses and can be extended to several areas of learning. They are frequently extended and applied in subsequent teaching modules and/or courses. To determine whether colleges and universities are currently and widely teaching digital forensics core concepts, we identified core concepts associated with the proposed knowledge domains (see Table 3; items presented alphabetically). This process was based primarily upon extensive training and practical experience in conducting digital forensic investigations, as well as several years of experience training digital forensic practitioners and educating college students in digital forensics. Such experience provides us the ability to suggest what foundational knowledge a learner must possess to achieve various learning objectives. The core concepts may be taught within the digital forensics curriculum (courses), or may be relegated to prerequisite coursework. It is interesting to note, however, that only ten of the 48 reviewed syllabi indicated prerequisite coursework. Those that did required courses pertaining to some portion of the following prerequisites: computers and telecommunication, operating systems, network, computer/network security, incident response and handling, and cryptography.

Access control	Elements of proof	Networking/telecommunication
Auditing (logging)	Ethical decision making	Partitioning
Bits & Bytes	Evidentiary integrity	Password cracking
Boot records	File signatures	Peer-to-Peer (P2P)
Client-server architecture	File system operation (multiple file systems, i.e. Windows, Linux, etc.)	Policy
Component (h/w, s/w) configuration	Hacking process	Privacy
Compression	Identification & authentication	Processes, threads, and resources
Computer & network protocols	Incident response	Programming
Cost-benefit analysis	Investigative process	RAID
Counting systems (i.e. binary, hexadecimal, decimal)	Judicial due process	Slack
Cryptography	Mathematical hash	Steganography
Disk geometry (cylinders, heads, sectors, tracks, clusters)	Memory (RAM, swap, allocation)	Technical writing
Electromagnetism	Metadata	Watermarking
	Networking devices	

Table 3. Proposed Set of Digital Forensics Core Concepts

We then compared this list of 40 core concepts to topics taught in each course, as identified in the syllabi. The qualitative review suggests that while the colleges and universities in our sample do seem to focus on education, as opposed to training, they do not adequately focus on teaching the digital forensics core concepts. Instead, they dedicate an inordinate amount of time to teaching non-core concepts. Current digital forensics course offerings at the vast majority of our sample schools appear more akin to special topics courses, focusing on making students aware of a smattering of digital forensics topics—

each of which vary from course to course and institution to institution. In summary, we are achieving breadth, but probably at the cost of depth of understanding of concepts critical to further education.

DISCUSSION

Implications for Digital Forensics Programs

The identification of ten large and conceptually varied knowledge domains, 63 learning objectives, and 40 core concepts accentuates the point that the field of digital forensics is large, and that educating students in it is not a trivial undertaking. We suggest that the model digital forensics curriculum program consist of a series of prerequisite courses, followed by a series of digital forensics courses. Experience suggests that while there is some overlap in learning objectives and core concepts with respect to teaching media and network forensics, there is enough separation that media and network forensics should be taught separately. We contend that the level of mastery/understanding for various learning objectives precludes universities from teaching both within the context of one course. The ideal scenario would be an introductory course aimed at teaching core concepts and learning objectives shared by both types of forensics, followed by an advanced course in media forensics and/or an advanced course in network forensics (and potentially additional advanced, more focused courses). Model course outlines are provided in Appendices A-C.

Contribution

To the best of our knowledge, this is the first concerted effort toward digital forensics curriculum development, with specific emphasis on identifying knowledge domains, learning objectives, desired mastery/understanding level, and core concepts. We argue that such a structure is critical to the success of academia's contribution to digital forensics. There has been a significant movement in recent years toward increasing scientific rigor within the digital forensics discipline—a mission for which academia has been invited and recruited (Palmer, 2001). The purpose of this research was to get that ball rolling.

Limitations and Future Research

There are several limitations with this research. Most prominently is the relatively informal nature of the qualitative review. While our experience in digital forensics was beneficial in the undertaking, it also serves as a potential source of bias. Another limitation is the wide variety in syllabi form and quality. Not all instructors choose to articulate the full range of topics covered and learning objectives sought on their syllabi. As a result, the data collection effort is arguably incomplete. Future research efforts should seek to validate these research findings via formal interviews with digital forensics instructors, instead of just relying on data collection from course syllabi. Future research should also seek to quantitatively validate the set of core concepts with both course instructor and potential employer populations. Questions asked should include whether or not the respondent views the concept as a core concept, its priority/importance, and the difficulty in teaching and/or understanding the core concept.

CONCLUSION

"True education involves drawing out the innate qualities of students, helping them to develop their own understanding, and nourishing their minds to achieve the greatest possible stature. It is a difficult goal to achieve, but one that is well worth our best efforts" (Moore, 1998 p. 135.). We heartily concur.

ACKNOWLEDGMENTS

The authors wish to thank those colleges and universities who promote knowledge sharing by posting their course information and materials on the Internet and/or who responded to our inquiries for information in support of this research. The authors also wish to thank Kennesaw State University for the knowledge imparted regarding curriculum development at the tenth Americas Conference on Information Systems (AMCIS) pre-conference workshop held in New York, New York in August, 2004.

REFERENCES

1. Bloom, B. S. (1956) Taxonomy of educational objectives, handbook: The cognitive domain, David McKay Co. Inc., New York.
2. Moore, J. W. (1998) Editorial: "education versus training", *Journal of Chemical Education*, 2, 75, 35.
3. Mukkamala, S. and Sung, A. H. (2003) Identifying significant features for network forensic analysis using artificial intelligent techniques, *International Journal of Digital Evidence*, 4, 1, 1-17.
4. Palmer, G. L. (2001) A road map for digital forensics research - report from the first digital forensics research workshop (dfrws) (technical report dtr-t001-01 final).

5. Palmer, G. L. (2002) Forensic analysis in the digital world, *International Journal of Digital Evidence*, 1, 1, 1-6.
6. Srinivas, H. (2006) Instructional design taxonomies, www.gdrc.org/info-design/instruct/blooms-taxonomy.html.
7. Willing, R. (2004) 'csi effect' has juries wanting more evidence, *USA TODAY*, August 5, 2004, http://www.usatoday.com/news/nation/2004-08-05-csi-effect_x.htm.
8. WorldWideLearn (2005) Guide to college majors in computer forensics, http://www.worldwidelearn.com/online-education-guide/technology/computer-forensics-major.htm.

APPENDIX A – MODEL COURSE OUTLINE FOR INTRODUCTORY DIGITAL FORENSICS COURSE

1) **Digital Forensic Awareness**
   a) **Need for digital forensics & types of computer crimes**
   b) **Computer criminology** (types of threats, sociology, psychology)
   c) **Various types and sources of digital evidence** (broad overview)
   d) **Role of technology in digital forensics**

2) **Preparation**
   a) **Policy** (core concept)
      i) Purpose, development, training, etc.
      ii) Types: acceptable use, information retention, incident response, investigation
   b) **Incident response capability development** (organizational, infrastructure, technical, personnel)
   c) **Digital forensics capability development** (organizational, infrastructure, technical, personnel)

3) **Law & Ethics**
   a) **Computer crime laws**
      i) Elements of proof*
   b) **Laws governing investigative procedure** (i.e. search & seizure law, privacy (core concept), case law, etc.)
   c) **Ethical considerations**
      i) Ethical decision-making*

4) **Conducting Investigations**
   a) **Investigative techniques & procedures**
      i) General – Investigative Process* (fact finding (WWWWWH), authority, etc.) & Due Process*
      ii) Network forensics – identifying rogue processes, binaries, files; network surveillance; log analysis; etc.
      iii) Media forensics – identifying, extracting, analyzing stored and/or deleted data
   b) **Investigative plan development**
   c) **Crime scene processing**
   d) **Investigation process** (i.e. preparation à incident response à data collection à data analysis… etc.)

5) **Evidentiary Issues**
   a) **Evidence preservation** (need, process, techniques for both static and dynamic data, evidentiary integrity*)
   b) **Rules of evidence**

6) **Evidence Preservation & Collection**
   a) **Preservation of evidence during incident response** (conceptual level only)
   b) **Forensic duplication processes and techniques** (conceptual level only)

7) **Computer Science**
   a) "Bits & bytes"*
   b) Electromagnetism*
   c) Counting systems*
   d) Disk geometry*
   e) Boot process and boot records*
   f) Partitioning
   g) File system operation*
   h) Slack*
   i) Memory* (RAM, swap, etc.)
   j) Metadata*
   k) RAID*
   l) File signatures*
   m) Mathematical hashes*
   n) Compression*
   o) Cryptography*
   p) Password cracking*
   q) Steganography*
   r) Watermarking*

8) **Documentation & Findings Communication**
   a) **Investigative & case documentation**
   b) **Technical writing* & investigative writing**
   c) **Expert testimony**

* Core Concept

Comments:

The "Incident Response" knowledge domain is not formally represented on the intro course outline because it is a very involved topic in network forensics and therefore addressed extensively there. While it exists conceptually in media forensics, it is less extensive and essentially covered under "Conducting Investigations," "Evidentiary Issues," and "Evidence Preservation & Collection.

The "Data Analysis" knowledge domain is deferred until the advanced courses in media and network forensics.

APPENDIX B – MODEL COURSE OUTLINE FOR ADVANCED DIGITAL FORENSICS COURSE FOCUSING ON MEDIA FORENSICS

1) **Digital Forensic Awareness**
   a) **Recap & review** of need for digital forensics and role of technology with focus on media forensics perspective
   b) **Various types and sources of digital evidence** (e.g. hard drives, PDAs, cell phones, removable media, etc.)
   c) **Digital forensics tools & capabilities** (e.g. forensic duplication h/w and s/w, media forensics tool suites, etc.)
   d) **Computer criminology** with emphasis on traditional criminals (i.e. "non-hackers")
2) **Preparation:** Recap & review only
3) **Law & Ethics:** Recap & review only
4) **Conducting Investigations:** Recap & review only
5) **Evidentiary Issues:** Recap & review only
6) **Evidence Preservation & Collection**
   a) **Preservation & collection of evidence from a variety of devices**
      i) Hard drives
      ii) Cell phones
      iii) PDAs
      iv) Removable devices (i.e. CDs, DVDs, "thumb drives," etc.)
      v) Memory
   b) **Forensic duplication process and techniques (hands-on)**
      i) Imaging
      ii) Wiping
      iii) Verification
      iv) Write-blocking
7) **Computer Science:** Recap & review only (no media forensics-specific CS concepts that are not taught in intro course)
8) **Data Analysis**
   a) File, folder, and partition recovery
   b) Analyzing metadata
   c) Identifying and locating hidden data
   d) String searching
   e) Finding files by file type
   f) Signature analysis
   g) Finding files via hashing
   h) Hash analysis
   i) Logical web history analysis
   j) Physical-level web data recovery
   k) Email investigations
   l) Email recovery
   m) "Cause & effect" parameters of digital forensics
   n) How to attribute digital artifacts to individuals
   o) Factors that limit the conclusions that can be drawn from digital artifacts
9) **Documentation & Findings Communication:** Recap & review with focus on media forensics perspective

* Core Concept

Comments:

The "Incident Response" knowledge domain is not formally represented on the intro course outline because it is a very involved topic in network forensics and therefore addressed extensively there. While it exists conceptually in media forensics, it is less extensive and essentially covered under "Conducting Investigations," "Evidentiary Issues," and "Evidence Preservation & Collection.

APPENDIX C – MODEL COURSE OUTLINE FOR ADVANCED DIGITAL FORENSICS COURSE FOCUSING ON NETWORK FORENSICS

1) **Digital Forensic Awareness**
   a) Recap & review with focus on network forensics perspective
   b) **Various types and sources of digital evidence** (e.g. IDS logs, firewall logs, victim system logs, etc.)
   c) **Digital forensics tools and their capabilities** (e.g. network-enabled/multiplatform investigation tools, network surveillance tools)
   d) **Computer criminology** with emphasis on hackers

2) **Preparation**
   a) Recap & review
   d) **Incident response capability development**
      i) Incident response team development
      ii) Computer and network base-lining
   b) **Digital forensics capability development**
      i) Incident response "toolkit" development

3) **Law & Ethics:** Recap & review only

4) **Conducting Investigations:** Recap & review only

5) **Evidentiary Issues**
   a) Recap & review
   b) Evidence preservation implications of incident response

6) **Incident Response*** ("triage")
   a) Suspicion validation
   b) Damage assessment
   c) Containment
   d) Eradication
   e) Recovery

7) **Evidence Preservation & Collection**
   a) **Preservation & collection of evidence**
      i) Processes
      ii) Memory
      iii) Logs
      iv) Binaries
   b) **Forensic duplication process and techniques (hands-on)**
      i) Imaging
      ii) Wiping
      iii) Verification
      iv) Write-blocking

8) **Computer Science**
   a) Hacking process
   b) Computer & network protocols
   c) Processes, threads, and resources
   d) Networking/telecommunication
   e) Networking devices
   f) Client-server architecture
   g) Peer-to-peer
   h) Access control
   i) Identification & authentication
   j) Auditing (logging)
   k) Intrusion detection & prevention
   l) Programming (minimal coverage will be possible, i.e. impacts of insecure programming techniques)

9) **Data Analysis**
   a) File, folder, and partition recovery
   b) Analyzing metadata
   c) Identifying and locating hidden data
   d) String searching
   e) Finding files by file type
   f) Signature analysis
   g) Finding files via hashing
   h) Hash analysis
   i) Intrusion "traceback"
   j) Log "reading" and event reconstruction
   k) Network transmission/session reconstruction
   l) "Cause & effect" parameters of digital forensics
   m) How to attribute digital artifacts to individuals
   n) Factors that limit the conclusions that can be drawn from digital artifacts

10) **Documentation & Findings Communication:** Recap & review with focus on network forensics perspective

* Core Concept