Global Information Assurance Certification Paper

Forensication Education: Towards a Digital Forensics Instructional Framework

GIAC (GCFE) Gold Certification

Author: J. Richard "Rick" Kiper, Ph.D., Richard.Kiper@leo.gov
Advisor: Christopher Walker, CISSP, GSEC, GCED, GWEB, GCWN, GCUX, CCISO
Accepted: January 30, 2017

Abstract

The field of digital forensics is a diverse and fast-paced branch of cyber investigations. Unfortunately, common efforts to train individuals in this area have been inconsistent and ineffective, as curriculum managers attempt to plug in off-the-shelf courses without an overall educational strategy. The aim of this study is to identify the most effective instructional design features for a future entry-level digital forensics course. To achieve this goal, an expert panel of digital forensics professionals was assembled to identify and prioritize the features, which included general learning outcomes, specific learning goals, instructional delivery formats, instructor characteristics, and assessment strategies. Data was collected from participants using validated group consensus methods such as Delphi and cumulative voting. The product of this effort was the Digital Forensics Framework for Instruction Design (DFFID), a comprehensive digital forensics instructional framework meant to guide the development of future digital forensics curricula.

1. Introduction

The definitions of digital forensics seem to be as varied as the number of forensic examiners in practice. Recognizing this fact, the National Institute of Standards and Technology (NIST) offered their own definition in *Guide to Integrating Forensic Techniques into Incident Response* (NIST, 2006):

> Digital forensics, also known as computer and network forensics, has many definitions. Generally, it is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data (p.15).

Similar to NIST, the National Initiative for Cybersecurity Careers and Studies (NICCS) provided a definition that focuses a bit more on the technical aspects of the job. According to NICCS (2016), the digital forensics professional "[c]ollects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations" (p.1).

However, other notable sources seem to give at least equal emphasis to what happens *after the forensic exam is completed:*

> "Digital forensics is the process of acquiring, analyzing, and presenting relevant and admissible digital data from different data states in a forensically sound manner suitable for litigation support" (Szabo, 2012).

With such a variety of opinions about the scope of digital forensics, it is not surprising that digital forensics instructors have failed to reach consensus on how to teach and assess mastery of its basic tenets. Some training programs provide hands-on learning experiences with a practical-based assessment, while others are mostly lecture-based, with assessments drawn from minutia buried in course textbooks. Some courses promote the presentation/admissibility aspect of digital forensics while others spend very little class time dedicated to legal considerations or reporting. There is simply no agreement regarding how to develop and implement the most important features of digital forensics instruction.

J. Richard "Rick" Kiper, Ph.D., Richard.Kiper@leo.gov

1.1. Purpose

The increasing number and variety of digital media communication and storage devices have wrought an explosion of digital evidence, much of which is not yet fully understood. Describing current challenges in the field of digital forensics, Lillis, Becker, O'Sullivan and Scanlon (2016) observed:

> It can be anticipated that the number of cases requiring digital forensic analysis will greatly increase in the future. It is also likely that each case will require the analysis of an increasing number of devices including computers, smartphones, tablets, cloud-based services, Internet of Things devices, wearables, etc. The variety of new digital evidence sources poses new and challenging problems for the digital investigator from an identification, acquisition, storage, and analysis perspective (p. 9).

Simply stated, the digital forensics community must be prepared to deal with enormous increases in the quantity and variety of digital evidence. More digital forensic examiners must be recruited, and they must be brought up to speed as efficiently as possible. A surge in digital forensics instruction is needed, and it must be as diverse and agile as the technologies and devices being examined.

The current study sought to contribute to the digital forensics domain by improving instructional strategies at the early levels of digital forensics education. This task involved the identification of such curricular features as which digital forensics skills need to be taught, which methods are most effective in teaching those skills, and how those skills should be assessed against defined standards. The goal of the study was to develop a framework for entry-level digital forensics instruction that draws from instructional design best practices as well as input from expert practitioners.

To attain this goal, the study was guided by the following research question:

What are the most important instructional design features of an entry-level digital forensics course?

This question served to focus the literature review and guide the development of methods used to create a digital forensics instructional framework. The following section summarizes the relevant literature in instructional systems design and reviews current attempts at defining digital forensics learning outcomes.

1.2. Background

The first step in developing any new curriculum is to adopt a method of instructional design, which "incorporates known and verified learning strategies into instructional experiences which make the acquisition of knowledge and skill more efficient, effective, and appealing" (Merrill, Drake, Lacy, & Pratt, 1996, p.2). The most common instructional design method is known as ADDIE, or Analysis, Design, Development, Implementation, and Evaluation (Branson, Rayner, Cox, Furman, King, & Hannum, 1975).

The ADDIE approach to instructional design is taught in nearly every instructor preparatory program, so its components are well known (Peterson, 2003). In the **Analysis** phase, the instructional designer identifies the overall knowledge gap and breaks down that learning need into discrete, observable tasks that are performed by a successful practitioner.

In the **Design** phase, the overall knowledge gap becomes the *instructional goal* for the course, while job tasks are transformed into *learning objectives*, which are specific descriptions of desired, observable behaviors that represent what the student should expect to gain from the course. The learning objectives then guide the creation of *instructional activities* (e.g., PowerPoint presentations, demonstrations, hands-on exercises, etc.) during the **Development** phase of ADDIE. The instructional content resulting from the first three phases of ADDIE is documented in a *lesson plan*.

The **Implementation** phase puts the lesson plan into practice, drawing upon the individual experiences and delivery skills of the instructor. This phase also includes scheduling, equipment, training venues, and other logistical concerns.

Finally, the effectiveness of both instructor and course content is assessed in the **Evaluation** phase of the design process. Kirkpatrick (1998) identified four levels of evaluation: learner reaction, mastery of the objectives, application to the job, and benefit to the organization. Most training programs exclusively focus on the first two levels, as they correspond to end-of-course surveys and student exams, respectively. As will be discussed in the Methods section, the current study examined Level Two (mastery of the objectives) evaluation features as they relate to digital forensics instruction.

Almost inseparable from the ADDIE model is a popular framework for defining learning objectives known as Bloom's Taxonomy (Bloom, 1956). This classification of learning objectives, which are defined in the Design phase, includes the cognitive categories of knowledge, comprehension, application, analysis, synthesis, and evaluation. Considering the diversity of these categories helps the instructional designer move beyond the more "rote" thinking of knowledge and comprehension type of learning activities (and corresponding test questions). Rather, the instructional designer should compose learning objectives that fit into a *variety* of these categories, which will help the student meet the overall educational goal of the course.

This powerful approach to creating learning objectives is extremely effective, but it is not complicated. Indeed, virtually any topic can spawn learning objectives in any category of Bloom. For example, a particular course might cover the topic of *IP Addresses*. Rather than simply listing the topic, an effective instructional designer will tell the students exactly what they are *expected to be able to do* by the end of the course or course segment, for instance:

- *Recognize* a legitimate IP address (**Knowledge**).
- *Describe* the purpose for an IP address (**Comprehension**).
- *Connect* to an IP address by the use of a browser (**Application**).
- *Determine* the class and type of a given IP address (**Analysis**).
- *Explain* the role of DHCP in Network Address Translation (**Synthesis**).
- *Assess* which IP subnets are appropriate for a given network (**Evaluation**).

Always led with a verb, these phrases are examples of specific, observable behaviors that may be taught in class and then assessed with a written test or practical exercise. Learning objectives provide not only a rich basis for structuring content but also a *mapping* of that content to assessment items, ensuring instructional validity. Bloom's Taxonomy facilitates the creation of a healthy mix of learning objectives that represent various levels of thinking.

Unfortunately, most digital forensics training programs have embraced neither ADDIE nor Bloom. As noted earlier, there is little consistency in how experts define the scope of the digital forensics domain. It follows, therefore, that the job tasks comprising

the digital forensic examiner profession are equally inconsistent and ill-defined among training organizations. Some examples are explored here.

NICCS (2016) publishes (and presumably maintains) an online "Cybersecurity Workforce Framework," which lists *Competencies, KSAs, Tasks,* and *Related Job Titles* for the Digital Forensics Specialty Area. However, what they call *competencies* is simply a list of sub-categories of digital forensics. The *KSAs* are introduced with the statement, "Experts in this Specialty Area have the following Knowledge, Skills, and Abilities:" followed by a list of "knowledge of…" and "skill in…" phrases that do not describe observable, testable behaviors. For example, "Knowledge of server and client operating systems" does not describe a discrete behavior to the level of detail required to create a learning activity or an assessment item.

The NICCS web page section labeled *Tasks* contains phrases that are closer to learning objectives. However, many of them are too narrow to have general applicability in digital forensics. For example, NICCS states that "Professionals involved in this Specialty Area…[a]ssist in the gathering and preservation of evidence used in the prosecution of computer crimes" (NICCS, 2016). It is unclear why NICCS would limit the purpose of gathering and preserving evidence to *computer* crimes (since nearly every category of crime has a digital nexus) or to *crimes* at all (since civil cases also use digital evidence).

The SANS Institute defines behavioral expectations somewhat better than NICCS. In the description for their course titled, *FOR408: Windows Forensic Analysis*, the course authors describe four general learning outcomes that begin with "Conduct in-depth forensic analysis…," "Identify artifact and evidence locations…," "Focus your capabilities on analysis…," and "Extract key answers and build an in-house forensic capability…" (SANS Institute, 2017). These phrases are broad descriptions of course *goals*, rather than learning objectives that can be used to build content or assessment items. While the practical exercises occasionally list a discrete behavior such as "Mount acquired disk images and evidence," the majority of the course description is simply a list of topics to be covered (SANS Institute, 2017).

The lack of specific learning objectives (or behavioral definitions) for each topic area in a SANS course presents a major challenge for creating corresponding

assessments, such as the GIAC certification exams. Without learning objectives, mapping specific test items (which measure discrete behaviors) to learning content is nearly impossible. And without consideration for Bloom's taxonomy, the cognitive levels of assessment items are haphazard at best. Students recognize this problem and it is a common critique of the GIAC exams, which seem to measure how well a student can look up a specific piece of knowledge in a book, rather than mastery of the content through any of the higher-order thinking categories of Bloom's taxonomy.

Facilitating a way to incorporate learning objectives –as well as the entire ADDIE methodology– into digital forensics instructional development is a primary aim of the current study. The following section describes the methods chosen to identify the most important instructional design features of an entry-level digital forensics course.

2. Method

When considering a digital forensics course as a focus for the current study, it was decided that an entry-level course would be most appropriate, since "[i]ntermediate and expert-level certifications presume that you have extensive job experience and a detailed grasp of the subject matter" (Cyber Degrees, 2016). A research-based methodology was used to develop a framework to guide the instructional design of such a course. This section describes the selection of participants, and the collection of data from those participants, in order to identify the important curricular features of an entry-level digital forensics course.

2.1. Selection of participants

To achieve consensus among a representative sample of stakeholders, it is not necessary to elicit input from a large number of people. In fact, groups of six to ten participants will often suffice to produce meaningful results, so long as the participants are knowledgeable in their fields (Landeta, Barrutia, & Lertxundi, 2011; Kiper, 2016).

For the current study, eight individuals were recruited for their expertise in digital forensics examinations and management of information security programs. These participants were experienced practitioners with advanced knowledge of the domain, and included three forensics professionals from separate cybersecurity companies, three

forensic examiners from two local law enforcement agencies, and two forensic examiners from a federal law enforcement agency. The mix of private and public sector professionals provided rich and diverse perspectives during the collection of data.

2.2. Data collection

To avoid the need to coordinate several in-person meetings, participant input was elicited and collected via e-mail communications. Collecting open-ended data via e-mail is becoming a common practice in qualitative research (Gay, Mills, & Airasian, 2009). Consistent with the Delphi technique (Landeta, et al., 2011), the participants anonymously submitted their input, which was aggregated and provided back to the group without attribution to individuals. The first phase of data collection involved a series of semi-structured questions to establish a foundation of instructional outcomes for the proposed digital forensics course. During the second phase, participants voted on the relative importance of those outcomes, as well as on other instructional design features derived from the ADDIE model.

2.2.1. Phase 1: Foundational responses

During the first phase of data collection, participants were contacted individually and asked to respond to a short list of open-ended questions:

1. How would you **define digital forensics** and in your opinion how is it different from "cyber investigations?"
2. What are the most **common types** of digital evidence your organization receives, and in what proportions?
3. What are the **toughest challenges** your organization faces with regards to digital evidence?
4. What **negative outcomes** has your organization experienced with regards to investigating cases with digital evidence?
5. When you think about ideal digital forensic training, how do you think of it being **organized or sequenced**? What are the large categories that should structure the training?

The participants responded individually as well as anonymously, and their answers were compiled and used to construct a portion of the second phase of data collection.

2.2.2. Phase 2: Delphi voting on features

In the e-mail sent to participants during this phase, they were asked to imagine they were designing an entry-level, 40-50 hour digital forensics course, one that will require some type of end-of-course assessment, such as a final exam, capstone exercise, or certification test. The student for this course could be:

- A computer science college student, who is considering information security as an academic track,
- An information technology specialist, who wants to have a greater organizational impact, or
- A tech-savvy law enforcement officer, who is self-taught but serves as the "go-to guy" for cyber evidence.

In other words, this course's student would already be familiar with basic computer concepts, such as computer hardware, operating systems, file systems, Internet applications, and so on.

During this phase of the study, the expert participants were asked to use a spreadsheet to assign relative importance to features of the hypothetical digital forensics course (see Attachment A). Using a cumulative voting technique (Berander & Svahnberg, 2009), participants were given 100 "tokens" with which to vote for features in each category. For example, in the first category (General Learning Outcomes), a participant may have felt that 30% of class time should be spent on theory and 70% on practical application of concepts. In that case, the participant would have entered a 30 in the yellow cell next to THEORETICAL and a 70 next to PRACTICAL (The totals for each category must add up to 100). In addition, participants were asked to add (optionally) a short justification for how they voted. For clarification purposes, an explanation for each feature was also provided for each feature in the spreadsheet.

As they entered their votes, participants were asked to keep in mind the type of students described previously. (They would likely change their scores for more advanced courses.) The very last section on the spreadsheet addressed artifact-related learning objective types. Unlike with previous sections, participants were asked to *rank* these types in order of what they thought to be the ascending level of critical thinking (i.e., the lowest level thinking receives a 1, the highest level receives a 5).

3. Results

The expert panel of participants responded to both phases of the data collection described in the previous section. To help define the general scope of the digital forensics course, participants responded to open-ended questions in the first phase. Those responses were compiled and then used to help define the instructional design features that were voted on during the second phase.

3.1. Phase 1: Foundational responses

Participants responded to the open-ended e-mail survey with rich descriptions drawn from years of experience in the digital forensics profession. This section contains representative excerpts of the responses to each of the questions.

1. How would you define digital forensics and in your opinion how is it different from "cyber investigations?"

In defining digital forensics, most of the experts listed many of the same technical components as was found in the descriptions mentioned earlier. For example: "…the science of recovering, processing, and analyzing digital information in relation to a security event, incident, and/or computer crime." Many experts described *cyber investigations* to be a more general or "holistic" concept, and some considered it a "superset of all the procedures, tools, & techniques… used to pursue an investigation which was focused on electronic technology." From this perspective, digital forensics would be a subset of cyber investigations.

2. What are the most common types of digital evidence your organization receives, and in what proportions?

The types of digital evidence varied significantly with each expert participant – perhaps owing to the diversity of their backgrounds and current jobs. Some mentioned specific device types, such as hard drives, loose media, and mobile devices. However, most of the participants reported that their intake consisted of *file types*, such as server logs, multimedia, and packet captures. Moreover, most of the experts could not provide an estimate of how much of each device or data type they examined. The lack of

attention to this type of information may be reflected in the low priority given to training students in *device types*, as described in the next section of this paper.

3. What are the toughest challenges your organization faces with regards to digital evidence?

The respondents were mixed in their opinions about whether the lack of trained forensic examiners was a problem in their organizations. Some complained of sharing their forensic examiners with other non-forensic IT entities, while others described challenges with dealing with outside organizations who participate in the investigations – primarily with regards to handling evidence.

4. What negative outcomes has your organization experienced with regards to investigating cases with digital evidence?

Most participants could not recall any specific negative outcomes related to digital forensics investigations in their organizations. Again, those who provided answers recalled problems with the handling of evidence and chain-of-custody, especially dealing with people outside of their organizations.

5. When you think about ideal digital forensic training, how do you think of it being organized or sequenced? What are the large categories that should structure the training?

The responses to this question were fairly robust, reflecting strong opinions about instructional content. The large categories identified by the group were transformed into the features listed under "Specific Learning Goals" in the spreadsheet in Attachment A. The participants' comments, clarifications and examples were also included in the *Feature Explanations* column. The spreadsheet was used to collect participant input regarding the relative importance of instructional features, which will be discussed in the next section.

3.2. Phase 2: Delphi voting on features

The unstructured participant responses from the first phase of data collection were used to inform the development of the survey/voting instrument in Phase 2. In the first five sections of the spreadsheet (see Appendix A), participants were asked to assign relative importance to the instructional features listed under each category. Explanations for each feature were adapted from the comments submitted during Phase 1.

Instructional features of the digital forensics curriculum were grouped into five categories: Learning Outcomes, Specific Learning Goals, Delivery Format, Instructor Characteristics, and Assessment. These categories roughly correspond to the ADDIE phases of Analysis, Design, Development, Implementation, and Evaluation. However, the use of educational jargon such as the ADDIE terms was intentionally reduced to avoid confusion for the participants. The results from voting in each category are summarized below in the following pages.

Learning Outcomes

As summarized in Table 1, the experts universally agreed that the majority of instructional time should be spent engaging the students in practical experiences related to digital forensics. Practical experiences include relevant case studies, instructor demonstrations, and hands-on exercises.

1. Learning Outcomes	Average (Mean) Score	Score Range
• THEORETICAL	36.25	30 - 40
• PRACTICAL	63.75	60 - 70

Table 1. Results of Voting on Learning Outcomes.

Specific Learning Goals

Average scores for identified learning goals ranged from 8.00 (Recall Digital Evidence TYPES) to 17.00 (Understand the basics of INVESTIGATION). In other words, the participants felt that a discussion of evidence types should receive a relatively low emphasis (8%) in the course – in fact, one participant commented that this area should be "mostly review" for the students in question. On the other hand, investigative processes received a higher percentage of the emphasis (17%), with a participant stating it was "[t]he basics, the fundamentals, the anchor of everything that comes after, so most time spent here." Other scores fell somewhere in the middle, indicating the experts thought the areas should be covered somewhat equally. The full results are summarized in Table 2.

2. Specific Learning Goals	Average (Mean) Score	Score Range
• Understand the basics of INVESTIGATION.	17.00	10 - 30

• Recall Digital Evidence TYPES.	8.00	5 -10
• Perform digital forensic PROCESSES.	13.25	10 - 20
• Follow appropriate EVIDENCE HANDLING procedures.	12.25	10 - 16
• Use Digital Forensic TOOLS.	15.50	10 - 20
• Locate and interpret specific digital ARTIFACTS.	12.75	10 - 16
• Discern USER ACTIVITIES from evidence.	11.25	10 - 15
• PRESENT and TESTIFY to evidence in a formal setting.	10.00	5 - 15

Table 2. Results of Voting on Specific Learning Goals.

Delivery Format

Surprisingly, the use of PowerPoint received the widest range of scores (see Table 3). While most experts downplayed the role PowerPoint should play in the delivery of digital forensics instruction, one expert's unusually high score of 40 brought the mean score up to a respectable 21.25. Unfortunately, that respondent did not offer a written justification for his/her voting. Regardless, demonstrations and hands-on exercises comprised the top two delivery formats (combined for 61.25), which is consistent with the results of learning outcomes voting for *practical* experiences (63.75).

3. Delivery Format	**Average (Mean) Score**	**Score Range**
• POWERPOINT or similar slide deck is used.	21.25	15 - 40
• HANDOUTS or textbooks are provided.	17.50	10 - 25
• Concepts are DEMONSTRATED.	27.50	20 - 30
• HANDS-ON EXERCISES are performed by students.	33.75	30 - 40

Table 3. Results of voting on Delivery Format.

Instructor Characteristics

As noted in Table 4, most of the experts indicated that the experience of the instructor was the most important characteristic (with a score of 35.25), while the ability to prepare students for an end-of-course assessment (such as a certification exam) was rated much lower (with a score of 12.00). The disparity may be due to the experts' stated admiration for credible teachers and their distaste for the practice of "teaching to the test." However, this latter attribute could also describe the instructor's desire *to emphasize the most important concepts,* which, if based on learning objectives, should be reflected appropriately in the assessment.

J. Richard "Rick" Kiper, Ph.D., Richard.Kiper@leo.gov

4. Instructor Characteristics	Average (Mean) Score	Score Range
• ENGAGING as a presenter.	19.75	15 - 26
• EXPERIENCED practitioner.	35.25	15 - 50
• Follows an organized STRUCTURE.	19.00	10 - 40
• Encourages DISCUSSION and student questions.	14.00	10 - 16
• PREPARES students for the end-of-course assessment.	12.00	7 - 20

Table 4. Results of voting on Instructor Characteristics.

Assessment

As summarized in Table 5, the experts' voting results revealed the most important features of an end-of-course *assessment* are that 1) it accurately represents the content, and 2) it does so in proportion to the learning objectives that drive the content. Although the score range was somewhat large, the participants did not seem as concerned about the clarity of assessment items.

5. Assessment	Average (Mean) Score	Score Range
• UNAMBIGUOUS.	15.50	5 - 25
• Measures what was ACTUALLY COVERED in the course.	30.00	25 - 40
• Tests learning objectives in PROPORTION to their emphasis in class.	30.25	25 - 40
• Covers IMPORTANT concepts rather than trivial knowledge/minutia.	24.25	15 - 30

Table 5. Results of voting on Assessment features.

Ranking Types of Learning Objectives

Finally, in the last section of the spreadsheet participants were asked to rank the learning objective types in the order of "thinking level." This exercise meant to determine if participants recognized *all knowledge is not equal,* and that some learning objectives require more sophisticated thinking. Their rankings are summarized in Table 6.

The participants were not briefed on Bloom's Taxonomy, nor did anyone mention Bloom in their feedback. Nevertheless, they all discerned lower-level learning objectives from those representing a higher level. For example, one expert noted the student must "be AWARE first," while giving a ranking of 1 to signify the lowest-level thinking. To justify a ranking of 5 for RELEVANCE, another expert stated, "Discerning the relevance for the case is the highest level thinking, because you need to know all parts of the case."

Ranking Types of Learning Objectives	Average (Mean) Score	Score Range
• ATTRIBUTES **(Components** and possible **variations** of the artifact).	2.25	1 - 4
• KNOWLEDGE **(Awareness** the artifact exists).	1.50	1 - 2
• RELEVANCE (**Significance** in the context of the specific investigation).	4.75	4 - 5
• ORIGIN/CAUSE (Emphasis on **why** the artifact exists).	3.75	3 - 5
• DISCOVERABILITY (How the artifact is **located/viewed** with tools).	2.75	1 - 4

Table 6. Results of ranking Types of Learning Objectives.

3.3. The framework

For the development of a digital forensics curriculum, the question is not *whether* to adopt the ADDIE methodology. The question is *how* to use the ADDIE model to identify and prioritize the most significant features of a digital forensics curriculum. The framework below is based on instructional design best practices as well as the collective feedback from the expert panel of digital forensics professionals who served as participants in the study. The working title for the framework is the Digital Forensics Framework for Instructional Design (DFFID), and it represents a first-of-its-kind guide for instructional designers of digital forensics curricula:

Digital Forensics Framework for Instructional Design (DFFID)	
Course Description: An entry-level, 40-50 hour digital forensics course, one that will require some type of end-of-course assessment, such as a final exam, capstone exercise, or certification test. **Student Description:** The audience for this course has prerequisite knowledge, skills, and motivations similar to: • A computer science student, who is considering information security as an academic track, • An information technology specialist, who wants to have a greater organizational impact, or • A tech-savvy law enforcement officer, who is self-taught but serves as the "go-to guy" for cyber evidence. In other words, a student in this course is already familiar with basic computer concepts, such as computer hardware, operating systems, file systems, Internet applications, and so on.	
CATEGORY	**RECOMMENDATIONS**
When thinking about overall **LEARNING OUTCOMES….**	• About **35%** of your instructional activities should deal with the **THEORY** behind the concepts. • About **65%** of your instructional activities should provide students with **PRACTICAL** experiences, such as case studies, instructor demonstrations, and hands-on exercises.
When defining the broad **GOALS** for the course…	• Do not spend a lot of class time reviewing **DEVICE TYPES** – students should already be familiar with them. • About **25%** of the course should address primary forensic **PROCESSES**, including the Collection, Evidence Handling, Preservation, Examination/Extraction, and Analysis of digital evidence.

J. Richard "Rick" Kiper, Ph.D., Richard.Kiper@leo.gov

	• About **40%** of the course should dive deeper on Examination and Analysis to cover the use of **TOOLS** to locate specific digital **ARTIFACTS** and discern **USER ACTIVITIES.** • About **15%** of your course should cover basic **INVESTIGATIVE** concepts, such as predications, drivers, and Civil versus Criminal proceedings. • Give your students an opportunity to make a formal **PRESENTATION** about the results of an exam.

When composing specific **LEARNING OBJECTIVES…**	• Create learning objectives that address **various levels of Bloom's Taxonomy*** or a similar taxonomy appropriate for *digital forensics*. For example, in teaching *digital artifacts,* learning objectives could address:
	  • KNOWLEDGE (**Awareness** the artifact exists).
	  • ATTRIBUTES (**Components** and possible **variations** of the artifact).
	  • ORIGIN/CAUSE (Emphasis on **why** the artifact exists).
	  • DISCOVERABILITY (How the artifact is **located/viewed** with tools).
	  • RELEVANCE (**Significance** in the context of the specific investigation).
	• Always start a learning objective with an **action verb**.

When selecting a **DELIVERY FORMAT…**	Use the **"Rule of Thirds":** • A third of your content delivery should be through the use of **POWERPOINT SLIDES** and **HANDOUTS**. • A third of your delivery should be spent on meaningful **DEMONSTRATIONS** of concepts. • A third of your delivery should involve **HANDS-ON EXERCISES** that teach learning objectives through application.
When recruiting **INSTRUCTORS** for the course…	Use the **"Rule of Thirds":** • A third of the instructor's value lies in his/her **EXPERIENCE** as a practitioner. • A third of the instructor's value lies in his/her ability to **ENGAGE** the audience and encourage **DISCUSSION**. • A third of the instructor's value lies in his/her ability to follow a lesson **STRUCTURE** to cover all learning objectives, thus preparing students for an end-of-course **ASSESSMENT**.
When developing an end-of-course **ASSESSMENT…**	• It is essential that an assessment accurately covers the **COURSE CONTENT**, and measures learning objectives in **PROPORTION** to their emphasis during course delivery. • Assessment items should test only the most **IMPORTANT** learning objectives, rather trivial knowledge or minutia. • Assessment items should be written in **UNAMBIGUOUS** language, making it clear to the examinee what is being measured. • The easiest way of ensuring instructional validity for assessments is to create a **MAPPING** of learning objectives to both course content and assessment items.

* The cognitive levels of Bloom's Taxonomy are Knowledge, Comprehension, Application, Analysis, Synthesis, and Evaluation. You can Google "Bloom's action verbs" for help writing learning objectives.

4. Conclusion

The goal of this research was to propose a framework by which digital forensics instruction may be developed for an entry-level course. Going beyond simple teaching

and testing of facts and details, this study sought to promote the substantive features of a course that gives the digital forensics student the greatest chance of success as an entry-level practitioner. This research contributes to the digital forensics body of knowledge by identifying the essential tasks of digital forensics and providing a guide for teaching those concepts to future practitioners. Several practical lessons may be drawn from the study, as well as ideas for future research.

4.1. Implications

All members of the expert team agreed that the majority of digital forensics instructional emphasis should be dedicated to the *practical* side of learning outcomes. According to the participants, approximately 65% of class time should be spent leading students to experience *the application of a concept,* either through a case study, an instructor demonstration, or a hands-on exercise. SANS Gold Paper author Jonathan Risto (2015) argued that regular, "cyber exercises" serve an important function by "providing a situation or scenario into which we place the participants to gain experiences and learnings that they can take back and apply" (p.3). As compared to platform instruction, however, practical exercises typically take longer for the instructor to cover the same amount of material. The idea of consuming more valuable class time is especially problematic in schedule-bound courses.

Therefore, to incorporate more practical applications the instructional designer is faced with several options:

- *Downsize* - Reduce the overall scope of the course to allow more time for practical exercises.
- *Replace* – Substitute PowerPoint slides with short, live demonstrations that cover the same learning objectives.
- *Redesign* – Rework and expand existing hands-on exercises to reinforce more learning objectives at a time.

Consistent with the desire for practical experience, the expert panel suggested as much as 25% of a digital forensics course should address primary forensic *processes*, including the Collection, Evidence Handling, Preservation, Examination/Extraction, and Analysis of digital evidence. To this end, instructors could add a *portfolio* component to both teaching and evaluation. With this method, students learn to conduct forensic exams by taking notes of procedures and documenting observations – culminating in a complete

report "package" that meets professional standards. A single digital forensics course may produce several such packages, and although the subject of the exams may represent fictitious data, the students can feel confident in presenting them as professional work product for career purposes.

The study participants felt the most important instructor attribute is that of *experience*. However, those who hire digital forensics instructors should also consider the ability to *engage* the audience, encourage *discussion*, and follow a *structure* (or lesson plan) to prepare students for an end-of-course *assessment*. Most of these characteristics are not readily apparent from reviewing a person's curriculum vitae, so it is important that training managers make efforts to observe the instructor in action.

Finally, the use of *learning objectives* is considered in the research literature to be the fundamental building block of instruction. They should be specific, observable descriptions of ideal student behavior that guide the creation of appropriate instructional content and delivery methods. The experts recognized learning objectives may be written at varying levels of thinking and recommended that about a third of the digital forensics instructional delivery be made via *PowerPoint* (lecture) and *handouts*, a third delivered with instructor *demonstrations*, and a third by way of *hands-on exercises*. Learning objectives also make possible the mapping of content to assessment items, ensuring that assessments accurately and proportionately measure the mastery of course content – the highest priority identified by the forensic experts.

4.2. Future work

Instructional designers in the digital forensics domain now have a research-based guide for developing an entry-level course. The next logical step is to define goals and learning objectives to meet the needs of a specific audience. Using the DFFID developed in this study, learning objectives may be defined – and then validated – by another group of experts. Alternatively, learning objectives may be composed with the help of a survey instrument (such as a SANS Survey) that targets a larger population of experts. Among the challenges of writing learning objectives for digital forensics instruction is how granular they must be to effectively describe a particular skill and to test for its mastery. For example, one must ask with regards to a given tool: "What is it about this tool that

students should remember?" (e.g., installation, configuration, target media/artifact, usage options, limitations, etc.).

Another recommendation would be to replicate the current study for intermediate to expert level courses. Sample research questions could include: How does the prerequisite knowledge of more advanced digital forensics students affect the approach to instructional design? Would there be a difference in the emphasis placed on any of the instructional design features? What is the earliest expertise level where a particular learning objective should be introduced into the digital forensics curriculum?

Finally, there is room for improvement of the spreadsheet of instructional design features – the instrument provided to the participants to collect their feedback. As one participant said of the *Perform digital forensics PROCESSES* goal, "Some of these other goals can be rolled up into this one." Feedback from other experts may help refine the feature definitions and thereby improve the accuracy of the DFFID framework. In turn, an improved framework will more effectively facilitate the development of quality digital forensics curricula.

And with the increasing demand for digital forensics training, instructional designers should welcome all the help they can get.

J. Richard "Rick" Kiper, Ph.D., Richard.Kiper@leo.gov

References

Berander, P. and Svahnberg, M. (2009). Evaluating two ways of calculating priorities in requirements hierarchies – An experiment on hierarchical cumulative voting. *The Journal of Systems and Software, 82,* 836-850.

Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (1956). Taxonomy of educational goals. *Handbook I: Cognitive Domain.* New York, NY: McKay.

Branson, R. K., Rayner, G. T., Cox, J. L., Furman, J. P., King, F. J., & Hannum, W. H. (1975). Interservice procedures for instructional systems development (4 volumes plus executive summary). Tallahassee, Florida: Florida State University. *Center for Educational Technology.(National Technical Information Service Nos. AD-A019 468 through AD-A019 490).*

Cyber Degrees (2016). A Guide to Cyber Security Certifications. Retrieved December 20, 2016 from Cyberdegrees.org: http://www.cyberdegrees.org/resources/certifications/

Gay, L.R., Mills, G.E., and Airasian, P. (2009). *Educational Research.* New Jersey: Pearson Education.

Jerian, M. (2014). The Complete Workflow of Forensic Image and Video Analysis. *Forensic Focus.* Posted July 28, 2014. Retrieved December 20, 2016 from Forensic Focus: https://articles.forensicfocus.com/2014/07/28/the-complete-workflow-of-forensic-image-and-video-analysis/.

Kiper, J. R. (2016, January). Needs to Know: Validating User Needs for a Proposed FBI Academy Knowledge Management System. In *2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 4334-4343)*. IEEE.

Kirkpatrick, D. L. (1998). *Evaluating Training Programs,* San Francisco: Berrett-Koehler Publishers.

Landeta, J., Barrutia, J., and Lertxundi, A. (2011). Hybrid Delphi: A methodology to facilitate contribution from experts in professional contexts. *Technological Forecasting & Social Change, 78,* 1629-1641.

J. Richard "Rick" Kiper, Ph.D., Richard.Kiper@leo.gov

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. *arXiv preprint arXiv:1604.03850*.

Merrill, M. D.; Drake, L.; Lacy, M. J.; Pratt, J. (1996). Reclaiming instructional design. *Educational Technology. 36* (5).

National Initiative for Cybersecurity Careers and Studies (2016). Cybersecurity Workforce Framework: Digital Forensics Retrieved December 16, 2016 from NICCS: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/digital-forensics.

National Institute of Standards and Technology (2006). Guide to Integrating Forensic Techniques into Incident Response. *Recommendations of the National Institute of Standards and Technology,* NIST Special Publication 800-86. Retrieved December 12, 2016 from National Institute of Standards and Technology: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.

Peterson, C. (2003). Bringing ADDIE to Life: Instructional Design at its Best. *Journal of Educational Multimedia and Hypermedia (2003) 12*(3), 227-241.

Risto, J. (2015). Exercise – not just for your body anymore: A comparative examination of the types of cyber exercises possible. Retrieved January 10, 2017 from SANS Reading Room: https://www.sans.org/reading-room/whitepapers/training/exercise-body-anymore-35782.

SANS Institute (2017). FOR408: Windows Forensic Analysis (a course description). Retrieved January 2, 2017 from the SANS Institute: https://www.sans.org/course/windows-forensic-analysis.

Szabo, Z. (2012). Digital Forensics is not just HOW but WHY. *Forensic Focus*. Retrieved December 16, 2016 from Forensic Focus: https://articles.forensicfocus.com/2012/07/03/digital-forensics-is-not-just-how-but-why/.

Appendix A
Delphi Voting Instrument

Relative Importance of Forensic Instruction Characteristics				
Features of Forensics Training	**Vote** (100 Tokens per Category)	**Justification (Optional)**	**Feature Explanation**	**Additional Comments**
1. Learning Outcomes				
• THEORETICAL			Time spent **explaining** a concept, including introduction, background, definitions, examples, and so on.	Please assign relative importance to these outcomes for an entry-level digital forensics course. As with each category, you have 100 "tokens" with which to vote.
• PRACTICAL			Time spent **experiencing** the application of a concept, either through a case study, an instructor demo, or a hands-on exercise.	
2. Specific Learning Goals				
• Understand the basics of INVESTIGATION.			e.g., Civil vs Criminal, objectives, drivers, predications, etc.	These goals address the basic **content** of the curriculum. What is the relative emphasis that should be applied to each goal?
• Recall Digital Evidence TYPES.			e.g., HDD, SSD, loose media, mobile devices, etc.	
• Perform digital forensic PROCESSES.			e.g., Legal authority, collection, preservation, examination, analysis, results, etc.	
• Follow appropriate EVIDENCE HANDLING procedures.			e.g., Rules of evidence, chain of custody, labeling, packaging, etc.	
• Use Digital Forensic TOOLS .			e.g., Software suites, write blocking equipment, imaging/downloading kits, etc.	
• Locate and interpret specific digital ARTIFACTS .			e.g., Those created by operating systems, file systems, application-specific, virtual device, etc.	
• Discern USER ACTIVITIES from evidence.			e.g., Storage, communication, modify, access, create, etc..	
• PRESENT and TESTIFY to evidence in a formal setting.			e.g., Courtroom testimony, executive briefing, etc.	
3. Delivery Format				
• POWERPOINT or similar slide deck is used.			For presentation purposes; Slides may also be reproduced in handouts.	Please vote on the relative importance of each of the format types, keeping in mind there will be an end-of-course assessment.
• HANDOUTS or textbooks are provided.			Handouts and textbooks typically contain more details regarding the testable content.	
• Concepts are DEMONSTRATED.			Live or in a recorded presentation.	
• HANDS-ON EXERCISES are performed by students.			e.g., In-class "labs", homework assignments, etc.	
4. Instructor characteristics				
• ENGAGING as a presenter.			This is the instructor's ability to hold the audience's attention.	How important is it that an instructor exhibit each of these traits? Please vote on their relative importance.
• EXPERIENCED practitioner.			The instructor has "been there and done that."	
• Follows an organized STRUCTURE.			The instructor follows a obvious plan, rather than spending time on unrelated topics.	
• Encourages DISCUSSION and student questions.			The ability to engage the students in meaningful dialogue.	
• PREPARES students for the end-of-course assessment.			Some students take the course in order to earn a certification or academic credit, making assessment prep more important.	
5. Assessment				
• UNAMBIGUOUS.			No tricky or badly worded questions.	An assessment may be **written** (as with a certification exam) or **practical** (as in a capstone exercise), or a combination of both. Please assign a relative importance to each aspect of an assessment.
• Measures what was ACTUALLY COVERED in the course.			Questions may be answered based solely on the course content.	
• Tests learning objectives in PROPORTION to their emphasis in class.			For example, a topic area that was emphasized in 20% of the class content should comprise about 20% of the assessment questions.	
• Covers IMPORTANT concepts rather than trivial knowledge/minutia.			Tests students on concepts that ultimately matter, rather than facts that can be looked up.	
Ranking Types of Learning Objectives - Rank in ascending level of critical thinking.				
• ATTRIBUTES **(Components** and possible **variations** of the artifact).			E.g., Student can interpret the timestamps of a .LNK file.	Using a score of **1** to **5**, please place these learning objective types in order of **ascending level of critical thinking.**
• KNOWLEDGE **(Awareness** the artifact exists).			E.g., Student can recognize a .LNK file.	
• RELEVANCE (**Significance** in the context of the specific investigation).			E.g., Student can describe how the .LNK file demonstrates specific user actions within a given time line.	
• ORIGIN/CAUSE (Emphasis on **why** the artifact exists).			E.g., Student can explain how the .LNK file was created.	
• DISCOVERABILITY (How the artifact is **located/viewed** with tools).			E.g., Student can use a tool to locate a .LNK file in a given data set.	

J. Richard "Rick" Kiper, Ph.D., Richard.Kiper@leo.gov