




May 1st, 8:30 AM

## Developing a Baccalaureate Digital Forensics Major

John H. Riley

*Dept. of Mathematics, Computer Science and Statistics, Bloomsburg University, jriley@bloomsburg.edu*

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

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

---

### Scholarly Commons Citation

Riley, John H., "Developing a Baccalaureate Digital Forensics Major" (2010). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 7.

<https://commons.erau.edu/adfsl/2010/friday/7>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact [commons@erau.edu](mailto:commons@erau.edu).

**EMBRY-RIDDLE**  
Aeronautical University™  
SCHOLARLY COMMONS

(c)ADFSL



## **Developing a Baccalaureate Digital Forensics Major**

**John H. Riley, Jr.**

Dept. of Mathematics, Computer Science and Statistics  
Bloomsburg University  
400 East Second Street  
Bloomsburg, PA 17815  
570-398-4627  
jriley@bloomsburg.edu

### **ABSTRACT**

As colleges and universities consider instituting a bachelor's degree in digital forensics or computer forensics, there are numerous questions to be addressed. While some of these normally occur in the development of any new major, there are aspects of digital forensics which do not often (if ever) occur in other majors. We discuss the issues that should be resolved in the development of a baccalaureate degree program in digital forensics.

**Keywords:** Digital forensics major. Computer forensics major.

### **1. INTRODUCTION**

For a number of reasons, a college or university may consider offering a baccalaureate degree program in digital forensics. We do not examine these reasons, but caution both institutions and individuals to check that a digital forensics major fits the institution. Mission statements and strategic plans must be consulted to determine this fit. The questions and alternatives we describe in this paper not only help the development of a digital forensics major, but also give those considering such a major a sense of what it entails. At the very least, this should help institutions and individuals to be realistic about what a digital forensics major will require.

There are always questions to be answered when new programs are being discussed and developed. Since this happens regularly in higher education, institutions have procedures that direct faculty and administrators through curriculum development and ensure questions common to all new programs are addressed. These institutional procedures are valuable and should be the starting point for anyone who is thinking about starting a digital forensics major.

Some of the areas we discuss may be covered in a general way in an institution's curriculum development process. In these cases, the specific alternatives mentioned will be useful in meeting institutional requirements. However digital forensics, as an academic major, has aspects that are not included as part of an institution's normal curriculum development process. How much of what follows normally is considered in a particular institution's process will vary. The parts that don't should not be ignored.

There are very few baccalaureate degree programs in digital or computer forensics. Utilizing the sites (Christine 2009 and Morris 2010), it appears that there are fewer than ten such programs in the United States. Furthermore, some of these are combined majors (e.g. Computer Investigations and Criminal Justice at St. Ambrose University, Davenport, Iowa) or concentrations within majors (e.g. Information Technology with a concentration in Computer Forensics, online at American Intercontinental University). Examining the curricula of these programs reveals that decision makers have faced many of the questions that we discuss.

While we have grouped the questions in six general areas, the questions and their answers are not independent. Proposers will need to address questions from all areas in conjunction with one another.

## 2. PROGRAM EMPHASIS OR EMPHASES

Just as a career in digital forensics can follow many different paths, majors in digital forensics can have different emphases. In this section we describe some of the underlying emphases of digital forensics to be considered in building a digital forensics major. While these emphases are not disjoint, which are in the minds of the designers and implementers will influence the major, particularly as a program begins.

While law enforcement (LE) is often is the first area of digital forensics that comes to mind, there is a need for digital forensics in corporate information technology (IT). While LE and IT digital forensics overlap, a conscious or unconscious slant toward one or the other will influence choices. A curriculum with an LE slant would probably have more emphasis on legal issues (e.g. the need for search warrants and chain of custody issues) than one with IT in mind. An IT emphasis would necessitate more education about networks. An LE based curriculum would also need to acquaint students with the hierarchical (quasi-military) organization of LE. With IT in mind, courses in business should be considered. Finally, an institution's culture may be more accepting of LE or IT and proposers should know their audience when using references to either LE or IT.

Similarly, designers of a major in digital forensics will need to decide how much emphasis to put on the technical and legal facets of the discipline. While neither can be omitted, students in a program which is more technically oriented may find employment in IT outside of digital forensics. In contrast, students graduating with a good background in legal matters may work in ediscovery.

Higher education curricula also can be designed to emphasize theory over practice or vice-versa. While a digital forensics major is inherently practically oriented, some theory must be present and decisions about how much must be made. For example, while binary and hexadecimal numbers are a *sine qua non* it may not be essential to cover two's complement arithmetic. An operating systems course which focuses on the design principles or criteria of an operating system is not inappropriate but is not the same as giving students the ability to use Linux. Again, an institution's culture should be considered in this discussion.

These emphases may not be explicitly mentioned or considered in the development of a program. They may arise as consequences of other decisions. However, realizing that they exist can eliminate difficulties. Using an operating system course taught by a traditional computer scientist may be acceptable if the digital forensics program is theoretically oriented but not if the program needs practical skills (e.g. familiarity with a command line environment). Discussing where incidence response (more of an IT emphasis) fits in the program with high level administrators who are expecting an LE orientation might be difficult. Establishing some understandings or being explicit about a program's emphasis or emphases will make the program development process much easier by providing a framework for decisions.

## 3. PROGRAM CONTENT

As soon as one begins to consider what might be good to put in any curriculum, one discovers there is always too much. The main challenge is to decide what not to include. In this section, we discuss many of the areas that might be included in a digital forensics major. These must be approached in the framework outlined above.

Traditionally, colleges and universities have thought of a major as being defined by the courses in the major. Towards the end of the twentieth century, a shift toward defining curricula, including majors, by the desired outcomes for students occurred. Consequently, designers of a digital forensics curriculum should not start by thinking about the courses needed for their major, but about what students should know or be able to do when they finish a course or complete the major. Proposers should become familiar with their institution's outcomes assessment procedures and requirements. Ultimately the outcomes of the digital forensics major will need to be assessed.

Two aspects of hardware are essential to a digital forensics major. First, the need to preserve evidence means students must have some sense of the ability of media to lose or retain data. Second, since storage and other digital devices must be connected to examination machines, experience doing this is necessary. The wide variety of digital devices (consider cell phones) means that even the coverage of even these basic topics will have some omissions. Additional topics from computer and network architecture certainly can be considered for inclusion.

Since operating systems and file systems determine what evidence may or may not be present on a storage medium, forensics examiners need a grounding in these areas. File systems are particularly problematic for curriculum designers. Understanding them at some level is needed, but it is impossible to include everything about a modern file system in a curriculum.

Operating systems and applications produce and leave many artifacts. Students must have some experience finding and recovering artifacts but decisions about how many and which ones must be made. For example, the registry in a Windows system has thousands of entries. Some can be crucial in an investigation. Curriculum designers must determine what will be included in their major.

Almost all of the programs in existence include some coverage of the preceding topics.

We have intentionally used the descriptor digital forensics instead of computer forensics. A forensics curriculum which only covered computers (in the strictest sense) is feasible. However, the proliferation of digital devices (cell phones, GPSs, PDAs, ...) and the data they contain makes the inclusion of digital devices in a forensics major desirable. The wide variety of devices and the lack of standards (particularly among cell phones) makes complete coverage of this domain impossible. To a certain extent, the coverage will be determined by logistic constraints, e.g. which types of cell phones are available for study.

The incorporation of forensics tools such as EnCase® or FTK® must be done carefully in an undergraduate curriculum. A college or university should not be training students in how to use a specific tool or tools. Rather the use of a tool should occur in the context of some other end such as case work or the recovery of artifacts. Consequently, one question to answer is how will a curriculum use a forensics tool to meet other objectives. It is also important to consider when in the major (first semester, second semester, ...) students will be introduced to these tools. Because they are so powerful, if the tools are introduced too early, students may not be motivated to understand some important concepts. For example, if a tool recovers deleted files, students may not appreciate what file deletion entails. Worse yet, when the tool fails in some task, they may not have any sense of what to do next. On the other hand, slogging through manual tasks unnecessarily will discourage some students. Deciding the place of forensics tools in the curriculum is very important.

While a network in the most literal sense only transfers data, the impact of networks on computers and the data they contain means some aspects of networks should be considered for inclusion in a digital forensics major. Designers of a digital forensics major may want to discuss the use of networks in forensics work, e.g. to transfer data from a target machine to an examination machine. Network forensics and incident response are viable topics for the major. All existing programs include an introduction to networks course. One program (at Rochester Institute of Technology) includes four (quarter) courses in networking with an advanced track that centered on networking.

An introduction to programming should help digital forensics students have some sense of the algorithmic nature of programs and give them some background in data structures. Both of these are useful in understanding the functioning of digital devices. Most collegiate level programming courses meet these ends. Beyond or instead of general purpose programming, programming in a digital forensics major may be specialized for two other purposes. First, being able to write scripts (e.g. in Perl) to automate some tasks is useful. Second, C or assembly language programming can be used to delve deeply in computer workings and is useful in malware investigations. Despite the centrality of programming to computing, most forensics degrees do not include a programming course.

There are several areas of computer science which may be incorporated in a digital forensics curriculum. Data bases, data mining, computer and network security are possibilities. Information systems topics, such as systems administration, can be useful. One way of handling this, particularly when courses already exist, is to allow students to choose from a list of courses. Most programs do this, but there is wide variation among the actual computer science and information systems courses that may be used in the digital forensics major.

Topics from criminal justice and legal areas may be included in a digital forensics major. Evidentiary issues are pertinent for both LE and IT. When law enforcement is being considered, search and seizure are important. White collar crime is another area which is useful for all students. Only two programs (both at very technically oriented institutions) do not include courses in this area.

Business topics can be useful for students majoring in digital forensics. As accounting discrepancies are often important, an introduction to accounting and fraud accounting fit well into a digital forensics major. At least three programs include an accounting course. A basic of understanding of organizations can be obtained from the area of management and a management course is required by one program.

Most undergraduate degree programs have a general education component. There are areas in general education which can be specified for a digital forensics major. A vital area is communication, both written and verbal. Technically oriented students are often weak in communication skills, so a digital forensics major must provide students the means of improving their communication skills. Since most undergraduate general education programs require communications courses, these are present in most programs. It's reasonable to expect that many digital forensics graduates will work with sensitive issues, so practical ethics may be part of the major. Mathematics topics such as probability, statistics and cryptography should be reviewed to see if they support the major. Most programs have an explicit mathematics requirement. Typically the requirement is discrete or finite mathematics and introductory statistics.

The preceding outlines the main considerations for the areas for inclusion in a digital forensics major. Within the areas chosen, many more decisions about material will need to be made.

Furthermore, while the designers of a digital forensics major at an institution may desire a particular set of topics for the major, some decisions and options will be dictated by local resources. Utilizing existing courses, when appropriate, is generally helpful.

#### **4. STUDENTS**

One reason an institution may consider starting a digital forensics major is to enroll or retain more students. The major should be realistically designed for the students of the institution. Students in a digital forensics major will most likely be similar to students already at an institution.

Faculty in science, engineering or technical areas may not be aware of the range of abilities of students at their institutions. Since digital forensics is a new field, students may enter the major unaware of its demands. Administrators may also be unrealistic and expect that a digital forensics major will not have the attrition rates of other STEM (science, technology, engineering and mathematics) fields. Resolving questions about expectations of the major in terms of enrollment and retention will help to minimize problems when the major is in place.

Depending on the institution, students may enter the major as new freshmen, transfer students from other two and four year institutions or as internal transfers from other majors at the institution. Transfer students (both internal and external) often believe they should be able to finish the major fairly quickly, say in four semesters (two years). If an institution has significant numbers of transfer students (especially external transfers) proposers should determine how the program will accommodate transfer students. A digital forensic major, like other STEM majors, will have some sequential structure. Minimizing course dependencies will help transfer students complete the major

in a timely manner.

Digital forensics graduates will have knowledge and abilities that can be applied malevolently. It is tempting to consider background checks for students entering digital forensics. There are many difficulties with background checks. It is much better to be clear about professional and individual responsibilities and duties in the curriculum. At the same time, some employers do require background checks and students should be aware of this.

Students and their families will often inquire about employment and internships in digital forensics. The institution's program development process will probably require the proposers to address employment prospects. These answers are useful, but cannot be considered definitive. Like any new program, hard data about digital forensics graduates' employment and internships will not be available for years. It's also wise to keep in mind that economic conditions years in the future are always uncertain and will influence employment opportunities. The U.S. Department of Labor's Occupational Outlook Handbook (U.S. Dept. of Labor, 2010) is a useful source of data in this regard.

Finally, the number of students expected in the major should be stated, almost certainly as part of the program development process. Enrollment in entry level courses will include nonmajors, particularly if a digital forensics minor is established. Anticipating these demands is important for planning.

## **5. FACULTY**

The implementation of a digital forensics major depends essentially on the faculty involved. The digital forensics faculty can (and should) be valuable, contributing members of the institution. However, the expectations of these faculty may need to be different from other faculty.

An institution's usual program development process will determine such matters as number of faculty, use of adjuncts, course load, advisement load and so on. To a certain extent these numbers will be driven by the number of students in the major.

Recruiting (either internally or externally) the faculty for the digital forensics major can pose problems. What level of credentials (masters, doctorate) will fit the institution? If the institution desires doctorate level faculty (particularly for permanent appointments) it needs to determine which fields (e.g. computer science, criminal justice) are acceptable. If the institution accepts other credentials (e.g. work experience in digital forensics) for digital forensics faculty, those faculty may be at a disadvantage in obtaining tenure or advancing in rank.

Faculty involved in a digital forensics program will most likely be changing or adapting from their original areas of expertise. Training will normally not be in an academic venue, particularly if the program has a practical emphasis. The faculty must be comfortable being with nonacademics and recognize that they may be receiving instruction from individuals who do not have academic credentials. Administrators must recognize the value of training offered by commercial entities. Similar comments apply to conferences that digital forensics faculty will attend.

Teaching digital forensics courses imposes burdens on faculty that are atypical. For example, text books are almost nonexistent. As a consequence, faculty must develop exercises and assignments on their own from scratch. Laboratory assignments can be very time consuming to develop, if only for the sheer volume of data that is needed. The institution should determine how much help to give digital forensics faculty. An extremely valuable, but costly way, of helping faculty is to reduce their teaching load. Agreements about teaching loads need to be in place as a program begins and develops.

Institutions frequently expect faculty to do research or produce scholarly results. Other activities may be more relevant for digital forensics faculty, particularly as they develop curricula for students. For example, working with local police or a district attorney's office will help a faculty member understand the needs of law enforcement and provide the police or district attorney with technical advice they might not have otherwise. Obtaining a forensics certification is also a worthwhile endeavor for faculty as it provides insight to the practice of digital forensics. Digital forensics faculty

need to know beforehand how such activities will be viewed by academic administrators and other faculty at the institution to enable digital forensics faculty to obtain tenure and advance in rank.

These issues are less thorny if existing faculty, particularly tenured associate and full professors, are associated with the program. Such faculty will not be concerned about meeting tenure and promotion criteria. In addition, having well regarded faculty working in the digital forensics program will legitimize it within the academy. However, even these faculty will feel the pressures outlined above. They will also be responsible for recruiting and then mentoring new digital forensics faculty. As new faculty may have a background not in digital forensics, mentoring them may include educating them in digital forensics, which is usually not part of mentoring.

Institutions and individuals developing a digital forensics major should understand that faculty work in this field will be quite demanding in ways that probably not have been experienced in other disciplines. Recognizing and accommodating these different facets of faculty work is important. Furthermore, they may not be covered in an institution's program development process. Developers of a digital forensics major should be conscious of the distinct role of faculty in the program.

## **6. LABORATORIES AND RESOURCES**

A digital forensics major should have a substantial laboratory or hands-on component. All campus laboratories involve space, cost and maintenance so discussions about digital forensics laboratories will occur naturally. However, there are special considerations for digital forensics laboratories that need to be addressed.

Computer forensics software often needs access privileges more like an administrator than a user. Understandably, campus technology departments are uncomfortable with this. One solution to this is to isolate the computer forensics laboratory from the rest of the campus. There are many advantages to doing this, but it does make administering the laboratory more difficult. Another solution is to use virtual machines.

Commercial computer forensics software can be very expensive. Decisions about what software to use in a program will need to be made. Since licenses can be restrictive, a program must ensure it can provide access for the number of students it enrolls. If students are to do work beyond the scheduled laboratory hours, they will need access to the laboratories when they are not in use.

Free computer forensics software exists and can be utilized. Beyond its lack of cost, freeware has the advantage that it can be used by students on their own machines outside of the laboratories. Since freeware is not advertised, it takes special effort by faculty to find it and evaluate it before utilizing it. Support (e.g. updates and documentation) for freeware is often minimal which also limits its utility. Finally, a good deal of free computer software is single purpose (e.g. an MD5 hash utility) so assembling all the tools needed for a computer forensics laboratory from freeware can be problematic.

The amount of data that must be handled by practicing digital forensics examiners can be large (terabytes). A computer forensics laboratory should be equipped to handle large amounts of data. In particular, it must be able to store and serve disk images. While there are ways of storing a disk image in pieces, storage requirements will be extensive and must be anticipated.

Computer forensics examiners encounter a range of devices and software. The laboratories for the digital forensics major should not be completely monolithic. This means decisions about, for instance, which operating systems (or versions of operating systems) exist in a laboratory must be made.

Forensics laboratories may include actual work with hardware, e.g., extracting a hard disk from a computer. If a campus has a replacement cycle for its computers, computers that have been taken out of use can be put in a laboratory for students to work on. Of course, the data on the hard disk must be wiped to meet privacy concerns.

The preceding addresses the laboratories for computer forensics. If networks or digital devices are

part of the curriculum, they should exist in laboratory environments. A laboratory network which already exists for a computer science program may be used for the digital forensics program. Computer science and digital forensics faculty should cooperate (and learn from one another) in this endeavor. A laboratory for digital devices may be harder to establish.

Cell phones illustrate most of the problems that occur with digital devices in a laboratory setting. First, a cell phone doesn't sound like a piece of laboratory equipment. Without some actual use (air time) there will be no data on a cell phone, so a cell phone plan may be needed. Finally, experience with different cell phones is useful. A funding request for twenty different cell phones along with a cell phone plan for them will raise many questions. Donated cell phones are of limited utility. If there's data on them, it needs to be securely erased to eliminate privacy liabilities. They then need use (as before). In addition, the rapid evolution of cell phones means donated cell phones may not be realistic examples. A plan for maintaining the physical security of the laboratory's cell phones must also be established. Finally, the specialized equipment and software needed for cell phone forensics must be in the laboratory.

It is possible to have combined classrooms/laboratories or separate classrooms and laboratories. An advantage of the first is that instruction can mix class lectures and discussions with hands-on experience fluidly. The disadvantages of the combined classroom/laboratory are students will be distracted by the laboratory equipment (computers) and when it is being used as a classroom, it is not available as a laboratory.

Laboratories need support. This support can be provided by the faculty, the institution's IT staff or a lab technician. If the faculty do this, this must be compensated by a reduction in their other responsibilities. Institutional IT staff or lab technicians will need guidance and assistance from the forensics faculty about the particular, and perhaps peculiar, needs of digital forensics laboratories.

As the laboratory component of a digital forensics major is very important, developers should have an initial laboratory plan in place when the major begins. As the major progresses and digital forensics changes, laboratories will need to evolve.

## **7. ADMINISTRATION**

A digital forensics major must be administered in a way that is suitable for its institution. Usually this means that it is administered by a department. It is unlikely that a new department will be created for the major.

If the digital forensics major is proposed by faculty in an existing department, that department will almost certainly be the host department for the major. If it is proposed by faculty from several departments, one of those departments may be chosen as the administrative unit for the department. This situation will require coordination among the departments and a dean's assistance may be required. A clear understanding of faculty members' commitment to the digital forensics major (particularly in terms of course assignments) must be in place. If new faculty are being hired for the digital forensics program, there may be several possible departments for the major. Before agreeing to host the digital forensics major and its faculty, a department should review the concerns that have been outlined in the preceding sections. If a department cannot satisfactorily address these concerns, particularly those about faculty, it should not host the digital forensics major.

In addition, any new major is an opportunity for publicity. Typically this involves the faculty in the new major. Faculty in the host department who are not involved with the digital forensics major should be comfortable with the attention the new program will attract.

More generally, while the institution as a whole must accept and value the different kind of work the digital forensics faculty do, the host department has a special obligation to understand and support digital forensics. There is an enormous amount of work involved in developing and maintaining a digital forensics program. Doing this with indifferent or hostile colleagues is an almost impossible



burden. For all of these reasons, a good host department for the digital forensics major must be found.

While the digital forensics major does not necessitate the creation of a new department, the program should have one faculty member coordinating it. Titling a person as Assistant Chair for Digital Forensics or Digital Forensics Program Coordinator may be helpful. Compensation, especially in the form of a reduced teaching load, should be considered. Ideally, this person knows the field of digital forensics, has good organizational skills and is able to work with colleagues, administrators and external stakeholders.

Determining the host department for the digital forensics major may occur naturally as the major is developed. If it does not, a host department should be chosen carefully. Currently, digital forensics majors are hosted in a variety of departments, divisions, or schools: Computer Information Science; Information Technologies, Networking, Security and Systems Administration; Business and Justice Studies; Information Technology & Sciences; Behavioral and Applied Social Sciences; Mathematics, Computer Science and Statistics.

## **8. CONCLUSIONS**

Any new major poses opportunities and challenges for an institution and the individuals involved. The first question that should be addressed when a new major is being considered is how well it will fit the institution. If a major in digital forensics major seems desirable for an institution, the institution should recognize that digital forensics poses some characteristics which are not typical for a baccalaureate major. The areas discussed in this paper outlines the questions that arise from these characteristics. An institution should address these questions as it develops its digital forensics major.

## **ACKNOWLEDGEMENTS**

The author is grateful for the opportunity to have worked with Scott Inch in the digital forensics curriculum at Bloomsburg University. Discussions with Dr. Inch have been very valuable in developing this paper.

## **BIOGRAPHY**

John Riley teaches computer forensics at Bloomsburg University. He has worked on curriculum and accreditation at both the department and university level.

## **REFERENCES**

- Christine (2009), 'e-evidence: The Electronic Evidence Information Center', <http://e-evidence.info/education.html> , accessed April 8, 2010.
- Morris, Jamie (2010), 'Forensic Focus', <http://www.forensicfocus.com/computer-forensics-education-north-america>, accessed April 8, 2010.
- U.S. Dept. of Labor (2010), 'Occupational Outlook Handbook, 2010-11 Edition', <http://www.bls.gov/oco/>, accessed April 15, 2010