A Ph.D. Curriculum for Digital Forensics

Dr. Frederick B. Cohen, Ph.D.
(dr.cohen at mac.com)
and Dr. Thomas A. Johnson, Ph.D.
(tomjohnson at attglobal.net)
California Sciences Institute
572 Leona Drive
Livermore, CA 94550

Abstract:

This paper presents a curriculum for a doctorate in digital forensics and discusses the implementation of that curriculum in a graduate program. It includes overviews of all of the classes and in-depth coverage of specific areas that go beyond the Masters level. It also discusses how that program is being implemented at the California Sciences Institute, a Non-profit California Public Interest Educational Institution oriented toward graduate education in the areas of Advanced Investigation and National Security

Keywords digital forensics, curriculum

Background:

This paper is about a curriculum for a doctorate level degree in digital forensics, and it is based on the curriculum currently being implemented at California Sciences Institute.

The state of the population of digital forensics experts

In examining the state of the art in the field of digital forensics, we considered the fundamental baseline to be the knowledge, skill, training, education, and experience identified in the Daubert decision [1] as the requirement for producing expertise relevant to the field, and the extent to which current witnesses qualified as experts in the digital forensics field compare to experts in other scientific fields.

Witnesses admitted as experts to testify in almost every field of scientific study today hold doctorate degrees in a specific field of expertise associated with their testimony. It is very likely that few if any courts would accept medical testimony in a legal matter unless it came from someone holding a medical doctorate. The testimony of a nurse, for example, would certainly be discounted if it related to the things that only an expert can testify about, and even an MD in a different specialty would likely be disallowed unless they could show specific knowledge in the key subfields of import to the matter at hand. The same is true in statistics or other mathematical fields, in biology, in chemistry, in psychology, and in fact, in almost any scientific field, this is also true. However; in the field of digital systems, digital forensic evidence is almost never presented in court or legally opined upon by someone holding a Ph.D. in a relevant field. And, because of the relative youth of the field and lack of academic attention to it until now, in most cases where a Ph.D. is involved, they have relatively little knowledge, skill, training, education, or experience in the field of digital forensics. Typically, they are experts in some other field relevant to the matter at hand, such as computer science or electrical engineering. While we are not aware of any formal studies in this area, even in Federal criminal cases, almost every expert we have identified presenting opinions related digital forensic evidence is less educated than experts in other fields. Typically, they have B.S. degrees with training certificates from commercial companies.

To get a sense of how dire the situation is, select reviews of documents presented to judges for searches showed that many of these documents contain stock language that is not, strictly speaking, factually accurate. Review of expert reports commonly shows errors in the analysis such as incorrect interpretation of Internet RFCs. And many expert witnesses treat RFCs and similar documents as if they were definitive statements about the manner in which networks actually operate and in some cases, as if they defined a legal mandate for behavior in the Internet.

There seems to be little interest or attention paid to experimental technique, and as a result, many statements made in legal matters are not consistent with empirical data. Most of the expert reports fail to indicate any calibration or validation of the tools in use, information on the reliability of these tools is largely lacking, and there is rarely any depiction of the accuracy of numerical results, descriptions of sources of error, and indication of how errors are resolved and results validated. It seems that most of this gets past the legal system because nobody involved in the matter knows enough, bothers, or is adequately resourced to challenge the evidence and testimony.

If this continues to be the case, it is highly likely that the legal system will start to build substantial precedents that are based on expertise that is inadequate to the need, and that these precedents will be used for many years to come, producing outcomes and process that is not in the interest of justice. Furthermore, unless and until Universities start to create doctorate level programs and expertise in this area, the “seed corn” will not exist to generate the large number of individuals with expertise to educate others, do research to advance the field, and work on and testify in legal matters.

Masters degree programs

Many Masters programs in digital forensics exist today, and their coverage is reasonably well known.[3] Typically, they involve classes in evidence identification, imaging and other collection, transportation, storage, and analysis, and presentation; and they commonly involve laboratory experiments or other practical experience in doing standard disk images, Internet searches, basis investigations, computer-related crime, and some coverage of legal issues. Many MS degrees involving digital forensics are concentrations within MS programs in computer science or criminal justice departments. For example, in one program in the context of a computer science department, [2] the curriculum includes:

- Forensic Digital Imaging
- Introduction to Cybercrime
- Advanced Digital Evidence Detection and Recovery
- Digital Evidence Search and Seizure

In our own program, which emerged from the program at the University of New Haven, the Masters degree is in the context of either a national security or advanced investigation program, and includes:

- Computer crime and legal and investigative issues
- Digital Forensics 1
- Digital Forensics 2
- Challenges to digital forensic evidence

The program also has mandatory courses in white collar crime, deception, counter-deception, and critical thinking, law and evidence, a survey of forensic science, and a research project or internship. But even this is not the full set of issues that must be addressed in order to truly understand the issues in the field.

Simply put, there just isn't enough time in a Masters program to teach more than the basics of evidence identification and collection, limited analysis, limited presentation, limited legal coverage, and very limited experience.

The doctorate program

In order to address what we believe to be the need for more in-depth knowledge, better education, and more experience and skill, we identified the key items that we believe to be missing in the present digital forensics programs at the MS level and created a program based on other doctorate level programs in similar fields.

The objective of the additional curricula

What we believed to be missing from current programs, including our own, was a clarity and completeness of coverage. This goes from understanding how digital systems work from the physics through the user interfaces to understanding the legal issues from the basics of the laws through presentation and challenges in court. Of course there are limits to what can be done in a few years of full time study in a graduate program, but the education and knowledge we provide should be focussed on what the student will need to know as well as what they will need to be able to understand throughout the remainder of their career and life, based on what we can teach them.

While we would very much like every digital forensics expert to understand everything from device physics to electromagnetic of communicants systems, to theory of computation, to operating system design, to ergonomics, and everything about the legal system associated with a lawyer; in practice, we simply cannot go that far. But we can take them from the lowest levels of physics to realistic legal settings stopping every step along the way for enough understanding to seed their knowledge and interests, and enough information so that when they give depositions, write reports, advise others, and testify, the things that they write and say are strictly accurate in every way from a scientific standpoint, and reasonably well presented and relevant from a legal standpoint. At least that is our goal.

Additional courses

At the doctorate level, we augment the M.S. level expertise, which must be achieved in order to gain standing as a Ph.D. student, with the following advanced courses:

- The physics and mechanisms of digital systems
- Information physics: Time, Space, and Computation
- Operating systems, networks, and applications
- Programming digital forensic analysis
- Digital crime scene reconstruction
- Challenges to digital forensic evidence (at the doctorate level)
- Research methods
- Probability and statistics
- Research with guidance

The outline of this curriculum projected into a quarter system is provided in Figure 1. The required courses must be taken in sequence in order to get the full effect of the mock trial, which occurs as part of the final quarter and is integrated into the Challenges to Digital Forensic Evidence II courses.

During the first 30 credit hours (red), students must have completed all 600 level courses or have accepted equivalent transfer courses and credits. All students must participate in at least 2 internships during their first 30 credit hours and must maintain a suitable average and not be on probation at the end of the first 30 credit hours of courses. Students wishing to terminate the program at this point, may opt to receive an M.S. degree in digital forensics by taking an additional 6 credits.

During the last quarter of the second 30 credit hours (yellow), students normally study and sit for their qualifying exams. Upon advancement to candidacy, the student will seek a dissertation topic, begin work on their dissertation proposal, and select a dissertation committee. Before starting their dissertation (green), the student must form a dissertation committee, propose a thesis topic, and gain approval for that topic by their dissertation committee.

Fall	***Winter***	***Spring***	***Summer***
Law and Evidence	Digital Forensics 1	Digital Forensics 2	Challenges to digital forensic evidence
Internet and criminal activities	Deception, counter-deception, & critical thinking	White collar crime	600-level research
Internship	Internship	Internship	Internship
Probability and Statistics	Research Methods	Operating Systems, Networks, and Applications	Programming Digital Forensic Analysis
The Physics and Mechanisms of Digital Systems	Information Physics: Time, Space, and Computation	Digital Crime Scene Reconstruction	Challenges to digital forensic evidence 2
Research	Research	Research	Qualifying exams
Ph.D. Seminar	Ph.D. Seminar	Ph.D. Seminar	Ph.D. Seminar
Dissertation	Dissertation	Dissertation	Dissertation

Figure 1 – The overview of the curriculum

The physics and mechanisms of digital systems

This course focuses on the details of digital systems and how they operate at the physical, electronics, optical, and other low-levels. This course is designed to provide knowledge of the underlying technical basis for how digital systems work so that the digital forensics expert can gain clarity around the underlying mechanisms involved in digital systems and understand, explain, and testify about these mechanisms as well as evaluate the use of these mechanisms when applied to legal matters.

Information physics: Time, Space, and Computation

This course focuses on the underlying mathematics of computation and communication, covering the basics of information theory, issues of time, space, complexity, and computability, number theory, their general applications, and their use in analysis of digital forensic evidence, questioned digital documents, and related matters.

Operating systems, networks, and applications

This course reviews principles and specifics of operating systems and applications ranging from cell phones to large-scale distributed computing networks. It covers system bootstrap, execution, shutdown, file systems, network interfaces, protocols, system calls, execution control, sharing, locking mechanisms, and a range of other related topics.

Programming digital forensic analysis

This course focuses on writing special purpose programs to do analysis of digital evidence. It includes laboratory exercises ranging from the creation of simple shell and perl scripts to the customization of special purpose programs for use in forensic analysis. It brings in open source software tools and customizes them, works through issues in the use of commercial tools, and works on the development of test tools to test other forensics software for properties, validation, and calibration.

Digital crime scene reconstruction

This course focuses on the use of technology to make high quality reconstructions of digital crime scenes and the limitations of those reconstructions in a legal setting. It goes from simple testing of basic claims and theories to partial and nearly complete reconstructions of complex digital crime scenes involving multiple systems and networks.

Challenges to digital forensic evidence (at the doctorate level)

This course focusses on how digital forensic evidence is challenged in a legal setting. At the MS level, this course uses the characteristics and features described in Masters level courses, but at the doctoral level, students with the advanced courses from the rest of the Ph.D.

curriculum challenge the challenges of the MS students and challenge the evidence by taking advantage of the additional knowledge gained through deeper understanding of the physics of the digital and informational mechanisms, probability and statistics and research methods, advanced knowledge of operating systems, networks, and applications, programmed analytical techniques, and digital crime scene reconstruction techniques. This course uses real evidence from real cases and includes realistic creation of reports, taking of depositions, challenges to other students' and witness testimony, and concludes in a mock trial.

Probability and Statistics

This course covers basic issues in probability and statistics from the perspective of challenging claims about these results. It addresses underlying notions of causality, the use of statistical methods to refute the null hypothesis, and the limits of those methods for proving causality. It also looks at the issues of correlation and the implications of these methods as they apply to digital evidence.

Research methods

This course focuses on qualitative and quantitative research methods. It is a course that helps the student gain clarity around the issues of research, including understanding the limitations of research and science, the reliability of different scientific claims, scientific validation processes, and how to evaluate and present limitations of scientific analysis. This is critical to being able to properly present and evaluate digital forensic techniques and define error rates and reliability necessary for presentation in legal settings.

Research requirement

All students must complete at least two quarters of research before taking their qualifying exams. This research is under the guidance of a professor in the program and is typically in some area of digital forensics. In these courses, the students are expected to become familiar with research as it is done by the faculty and to apply the things they are learning in their courses to that research. In most cases, during the course of this research, students will co-author one or more publication quality articles and gain experience in the whole process of research and research publication.

Admissions and qualifications

To be admitted to the program, students must possess a B.S. degree in a related field from an accredited university, submit examples of previous writings or publications that demonstrate their ability to do research, submit scores from the GRE, and submit transcripts from their previous university courses and degrees.

Students holding M.S. degrees in a relevant field from an accredited university may seek to have select courses from their previous programs counted as equivalent courses to those within this program to reduce the course requirements prior to entering into the doctorate level courses. These will be evaluated on a case by case basis or, for schools with pre-existing agreements, accepted based on performance in the previous institution in authorized M.S.-level transfer courses. However; in no case shall the 30 resident credit requirement for admission to candidacy be waived or reduced. All courses from the first 30 credit hours must be satisfactorily completed before entering the second 30 hours, however; select courses from the 2nd 30 hours may be entered upon instructor approval. Specifically, the probability and statistics, research methods, and operating systems, networks, and applications courses. The remaining courses must be taken in sequence for full effect.

Dissertation and research requirements

As in most doctoral programs, students must do meaningful research that advances the state of the art, and write up their results along with the necessary background, in a dissertation that is comparable in quality to what would be found in a refereed journal associated with a professional society. Each student must complete and publish an original empirical or theoretical research dissertation. Prior to starting the actual dissertation, students must first submit a prospectus for their dissertation that includes a detailed background of the specific area of research, and they typically include this, in large part, in the body of the dissertation as background to their specific work.

Ph.D. seminar, internships, and related work

In addition, the program requires that students take part in a seminar series in which experts from various disciplines related to digital forensics present up-to-date information on the field. This is likely to involve presentations of issues in legal cases, talks from local, state, and federal law enforcement, results of investigations, talks by visiting faculty members from other universities, and so forth. Internships are typically required, however; for students who are currently employed in the field, internships may be waived if their regular work meets the same requirements.

Other challenges

There are four major challenges that we face in trying to build this emerging program.

Obtaining faculty

At this point in time, there are very few individuals with Ph.D.s in related fields and who have research and practical experience in the field of digital forensics. Most of them are very occupied. As a result, there is a substantial challenge in finding faculty to support a program such as this, and in creating a program that will produce Ph.D.s in this field. As in any emerging discipline, this challenge is met by using a mix of experts from other fields and creating a faculty that fuses their expertise to build the new discipline. As the discipline emerges, some of the doctorate level graduates then help to populate other universities, which produce more resources that then allow the universities that seeded these programs to reseed themselves.

The approach we have taken is to build faculty from the practical community that exists. CSI is starting to operate in the Bay Area near San Francisco, and as a location where much of the software and hardware of the information age was developed, this area is particularly rich in expertise and experienced in dealing with computer-related crime. While we draw faculty in specialized areas from all over the country, we don't have the resources or demand required to hire the full time faculty necessary to completely cover all of the expertise involved in our curriculum. As a result, we use active and recently retired professionals from the various communities involved, engage the local community leaders in relevant fields, and spend time and effort getting involved with groups like the local Electronic Crimes Task Force, local law enforcement agencies and their forensic laboratories, high technology businesses, and engage those who have worked in the national security arena. Each of these communities have both substantial expertise and substantial need for additional expertise, and by acting as a conduit for the exchange of knowledge and formalization of that knowledge, we can help them while engaging those who have the proper background, experience, knowledge, and desire to become members of the faculty.

At the same time, teaching Ph.D. students requires that all or most of the faculty have a Ph.D. in a relevant area. We are very fortunate to have formed relationships with professors from around the country who have expertise and experience in this field, and our faculty also helps to engage with those other universities to collaborate in helping them to provide expertise for their programs. For the next 5-10 years, a combination of Ph.D.s from other fields and professors from other universities, industry, and government, will be used to build this program and, hopefully, other universities will engage in this process as well, to provide us with the seed corn that we need to sustain our program over time and build the next generation of our faculty.

Up-to-date materials and cases

A major impediment to success in such programs that has been reported to us by others, and that we have experienced as well, is the difficulty in getting up-to-date materials for many of these courses. For example, in seeking challenges to digital forensic evidence, the use of current cases is potentially problematic because we may find challenges that destroy existing cases. While this is potentially an substantial benefit for the overall system of justice, the system of justice as it exists today is oppositional by nature. The strategy and tactics of cases limits the willingness of many attorneys to provide information on active cases, and many cases are under seal, or otherwise problematic in terms of getting access to evidence.

While the ideal drama may come from a current multiple homicide case in which one of the accused claims innocence and is proven so by a challenge to digital forensic evidence, the reality is that most cases are civil litigations that are settled with all evidence and other materials destroyed or returned without public disclosure. In many senses, the openness of the university is exactly the opposite of the closed and confidential nature of the relationship between a client and their attorney.

We have been very fortunate in that out relationships with local law enforcement, those in the legal community, and those in the business community, have allowed us to have a unique perspective on and access to information and situations that allows us to get involved with public information relating to a few cases per year. For those without such relationships, a bit more effort can bring similar results from the public records or from information published by individuals in specific cases. For example, in one case we are using in classes, we were pointed to a public release of formerly sealed court papers including an indictment and the supporting information from a search warrant. This provides the sort of material that makes for a realistic homework assignment for some classes.

Another approach we have taken is to create our own cases. Of course this is problematic in many ways, because in order to get a real case with real evidence you have to commit a real crime. The quality of your simulation drives the realism of the digital forensic evidence, the investigation process, and the results produced. Another problem in this space is that real cases may take years to evolve, while in graduate classes, we have to get something completed within a semester, or in our case, a quarter. While patience is a virtue, our students need a high volume of experience in a short period of time. So unlike real matters where you might drill down for weeks or longer on a specific matter, our students often take small fragments of large complex cases and drill down into them, and then move on to the next matter. This is a reasonably good simulation of what law enforcement does because of the high volume of cases they process per unit time.

Arranging practical internships

Practical internships are one of the keys to success in a program such as the one we are forming and the program that it emerged from at the University of New Haven. While many internship programs end up placing students in work environments related to their fields, many such students end up not doing work similar to what they expect from their field of interest. In digital forensics an intern without a clearance cannot work on national security-related forensics, and unless they sign non-disclosure agreements and are adequately trusted by the hiring party, they cannot reasonably work on almost any case that can be identified. As a student, they cannot get involved in the aspects of cases requiring testimony because, among other things, they are expecting to graduate and move on, legal matters often have delays of months or years, and things change on a moment's notice as a case is closed or settled.

A best-case scenario for many programs is for a student to get an internship in a local crime laboratory working on digital forensic evidence related to cases, but on fairly standard cases where one after another piece of evidence is treated in a uniform manner. While this is excellent training for a student expecting to get a Masters degree and start to work after graduation in a crime lab, and helps to build up relationship for both the university and its students, there are only so many crime lab jobs near any given location, and this sort of internship at the doctorate level is not as useful and does not use the full set of skills that would be desired for dealing with legal matters, won't likely produce opportunities to review live legal cases, and provides only limited insight.

One of the approaches we have been trying to get to work better is in the development of long-term relationships with local attorneys, prosecutors offices, and national security facilities that deal with the more complex issues in cases, and for whom limited reviews can be helpful. As an example, the language used in many legal processes ends up being copied from previous cases by individuals who either don't know enough about the details of digital systems to do it themselves or don't have the time to do a custom document for each case. If a police officer needs a search warrant to get evidence from computers, they cannot really be expected to have a doctorate in digital forensic evidence, and the prosecutor's office may have similar limitations. Projects that serve the community as a whole may be effective here. For example, taking the sorts of paragraphs in use today, you might create an internship program in which the students develop standard paragraphs for describing standard situations from a legal perspective with regard to digital forensic evidence. These can then be fused into libraries that make the processes more accurate and more efficient for the legal community as a whole. The university benefits from the good relationship, the students benefit from the experience, the faculty gets engaged in verifying the results of the effort, and the legal and law enforcement community benefits from having a more sound basis for legal process and better precedents over time.

We were very fortunate in building these sorts of relationships at the University of New Haven because of the efforts of many of our faculty and the support of our administration of this effort, and this has translated well into the new programs we are now creating.

Mock trials and similar legal processes

Mock trials and other similar legal process simulations are important and very useful to integrating the knowledge acquired within the program into practical use. Of course for students who have never seen a courtroom or had any experience on a witness stand or in a legal proceeding, almost any simulation, even with a faculty member acting as judge, might seem like a novel experience. Many of our students are mid-career professionals who have had some of this experience already. For them, the learning comes from seeing how different approaches are challenged and succeed or fail, and take things to a deeper level, particularly for new situations that are emerging.

Substantially meaningful mock trials take considerable time and effort to coordinate and execute. In order for this to be effective, students and faculty must be working on the cases for months in advance. This starts with introducing the cases to the students; making the evidence available for review; having students do the analysis and write expert reports; taking depositions from the students based on those reports; having students review other student depositions and reports and prepare counter-reports and counter-arguments; preparation of exhibits for presentation at trial, and setting the order of presentation for the date of trial. This is done as part of the course work in the quarter in which the mock trials are to be held, and these trials acts as the capstone experience for the year of study. For this reason, it is our goal to have one week of trials per year, in which judges and lawyers are brought in to try the cases, all of the pending cases are presented to juries, and decisions are rendered. The court reporters' transcripts are then used to review the trial efforts with the students and become part of the permanent record for use in future studies and mock trials.

By combining mock trials between the students in the Masters program and the Ph.D. program, redundant effort can be saved, and Ph.D. students can take the stand after Masters students to demonstrate how taking the science to the next level can help to make or break a case. If each of 25 students is to gain experience in testifying, it will take several days to get through a normal trial process. Jury are empaneled from the student body and the faculty.

It is advantageous if there are several relatively small and simple cases rather than one large case, because this reduces complexity and allows those who are on one side or another in one case to be jurors in another case.

These trials are designed to have only expert witnesses, no jury selection process (usually volunteers from the audience), and lawyers with limited roles and almost no preparation time. Juries don't get to deliberate for long, but they do get to vote on the outcomes with majority rule instead of total agreement. Specific issues are brought up across the period of the trials, like commonly used trick questions and questioning techniques. There are improper questions with objections, surprise pieces of evidence for the witnesses, and other similar things to keep the trial lively, but these are also designed to have educational value. For example, if a student makes a mistake at trial, it may be identified for discussion after the trial when the transcripts are reviewed.

We envision participation by local judges and prosecutors and we hope that they can also gain experience with specific types of evidence they are likely to see in legal cases through these mock trials. This prepares all of us to better understand the issues at trial, to better understand the challenges and testimony, and it helps build relationships. This also helps to open opportunities for students and faculty and has the potential to engage local law schools in joint collaborative efforts.

Summary and conclusions

The Ph.D. program and curriculum is designed to move from the level of knowledge typically available in legal matters today, to a level comparable to what is expected in other scientific fields. It does this by extending both toward the underlying physics and details of how digital systems operate and toward more in-depth examination of and experience with legal processes. It is intended to provide the “seed corn” required to meet future needs in both education and at trial, and is highly cooperative with the local legal and investigative communities while still meeting the academic standards common to doctorate programs in other fields.

This program is still under development and the authors welcome feedback, collaboration, and participation from and with the community. For those wishing to find out more, please contact the authors at California Sciences Institute.

References

[1] Daubert v. Merrell Dow Pharmaceuticals, Inc. 509 US 579, 125 L. Ed. 2d 469, 113 S. Ct. 2786 (1993).

[2] Marshall University's digital forensics specialization (http://forensics.marshall.edu/MSDegree/MSDegree-Computer.html)

[3] Taylor, Endicott-Popovsky, Phillips, "Forensics Education: Assessment and Measures of Excellence", Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07) 0-7695-2808-2/07 $20.00 © 2007, IEEE