Digital Forensics: Defining an Education Agenda

Kara Nance
Department of Computer Science
University of Alaska Fairbanks
klnance@alaska.edu

Helen Armstrong
School of Information Systems
Curtin University of Technology
h.armstrong@curtin.edu.au

Colin Armstrong
School of Information Systems
Curtin University of Technology
colin.armstrong@curtin.edu.au

Abstract

While many fields have well-defined education agendas, this is not the case for digital forensics. A unique characteristic of the evolution of digital forensics is that it has been largely driven by practitioners in the field. As a result, the majority of the educational experiences have been developed in response to identified weaknesses in the system or to train individuals on the use of a specific tool or technique, rather than as a result of educational needs assessments based on an accepted common body of knowledge. In June, 2008 a group of digital forensics researchers, educators and practitioners met as a working group at the Colloquium for Information Systems Security Education (CISSE 2008) to brainstorm ideas for the development of a research, education, and outreach agenda for Digital Forensics. This paper presents the research in education needs that the group identified associated with the development of a digital forensics education agenda.

1. Introduction

As a result of the increase in digital crime and the need to incorporate digital evidence into investigations of traditional crimes, skills and knowledge in the digital forensics domain are in demand. Unlike many other professional fields, there is no globally accepted digital forensics oversight organization or accrediting body to ensure consistency across educational agendas. Nor has a concise needs assessment been conducted that identifies the current challenges associated with meeting the needs of the diverse associated population base. Further, there is no research agenda that identifies the advances that are needed in educational methodologies, materials and environments to educate the digital forensics community.

Representatives from the 2008 CISSE Working Group on Digital Forensics presented their preliminary digital forensics research agenda at the Digital Forensics Minitrack of the Hawaii International Conference for Systems Science in January 2009. In addition to the presentation of the Digital Forensics Research agenda, a discussion of the digital forensics *research in education* agenda was presented including the identification of issues relating to education that caused the working group to separate education and educational research issues from the general research issues (see Figure 1). The motivation for this was that the identified educational issues tended to be overarching themes that were related to every identified research issue. The motivational summary that initiated the working group on Digital Forensics Education Research states that:

> The education research agenda was difficult to approach as it is challenging to separate the *research in education* needs, where we are conducting research to help identify better ways to educate our constituencies with respect to digital forensics, from education and training needs. Research in education for digital forensics will help us to identify the educational methodologies, materials, and environments that will assist educators in meeting the educational and training needs of their diverse constituencies.[1]

The resulting goals of the Digital Forensics Research in Education Working Group include the following:

1. To provide academic researchers, with challenging and interesting problems related to digital forensics education.
2. To develop communities of researchers that can work together to advance the state-of-the-art in digital forensics education
3. To develop an education agenda to meet the needs of the diverse constituencies who need digital forensics education and training.

978-0-7695-3869-3/10 $26.00 © 2010 IEEE

While the long-term objective of formalizing the digital forensics education agenda is still under development, the progress made at the initial working group meetings marks a substantial contribution towards the development of an education agenda for digital forensics.

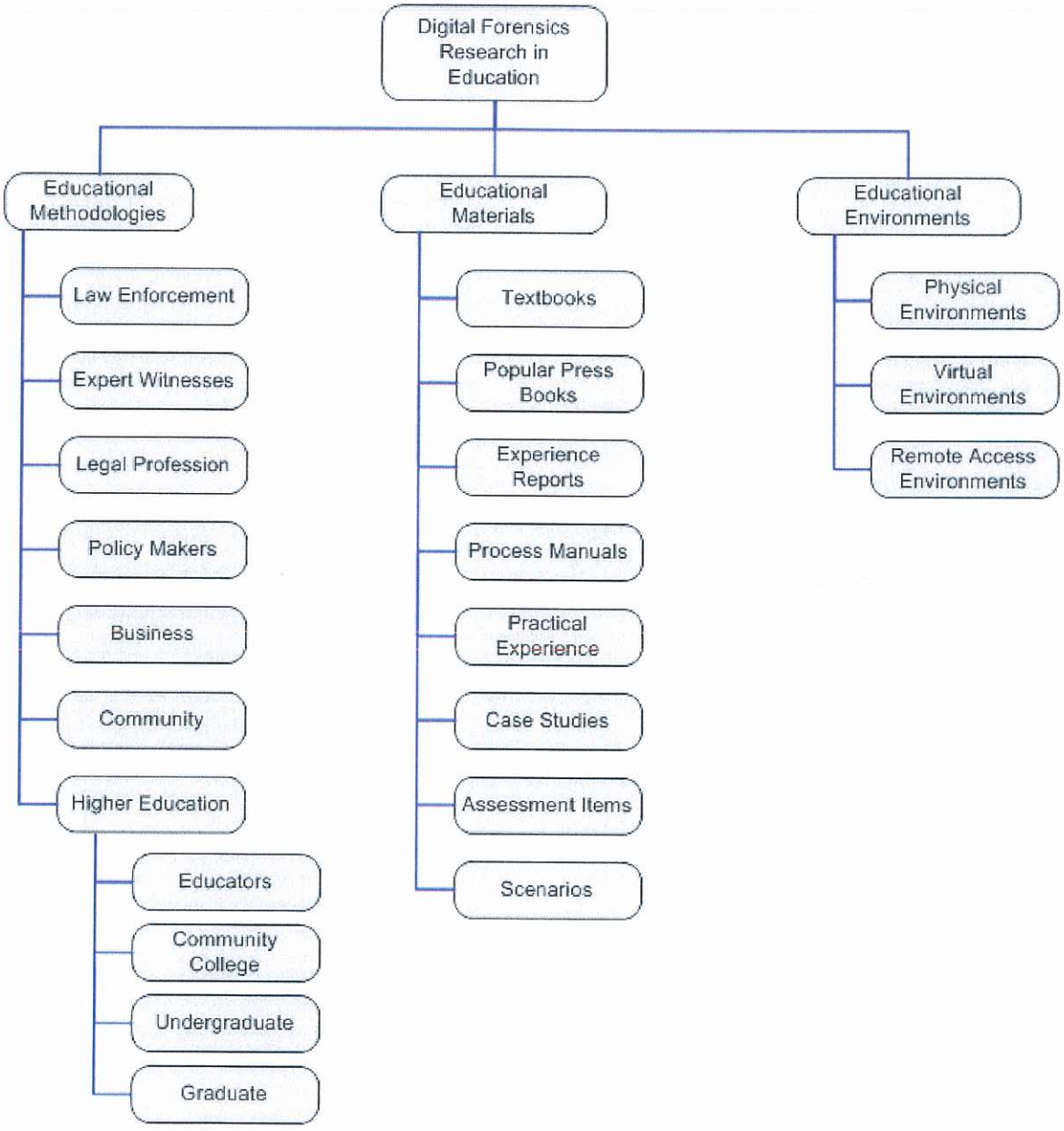

Figure 1: Preliminary Digital Forensics Research in Education Agenda

2. Background

The increase in computer-related crime and the use of digital evidence for traditional crimes has raised the profile of digital forensics research and education. Far from focussing entirely on technical digital forensic aspects, the field encompasses law enforcement, expert witnesses, the legal profession, forensic practitioners as well as a host of other stakeholders in government, business and the community. Concerns with the disjointed and piecemeal approach evident thus far in the field have been voiced. Carrier and Spafford [1] observe the dominance of vendors and applied technologies rather than establishing a sound theoretical foundation for the field and the scientific validity of current methodologies and procedures questioned by judiciary across the globe [2]. Unfortunately Rogers and Siegfried [3] observe that there is little evidence of any unified strategy being developed in the field to address these problems.

Research in the recent past highlights the need for frameworks that incorporate a more expansive view of the field. Ieong [4] states that digital forensics is a group of investigation tasks and processes, and specialists in the field (including information technologists, legal practitioners and investigators) require technical-independent frameworks in order to remove the technical barriers of current approaches. This supports Losavio and Adams [5] view that there exists a gap between the digital forensics technical process and the judicial process with legal practitioners finding the technical aspects too difficult to grasp.

Broucek and Turner [6] observe that coherent frameworks for understanding and responding to digital forensics issues, their impacts and interrelationships are still a long way off. They propose an additional methodological step for the development of a framework to map a merging of the differing sets of responses within a dynamically evolving forensic computing landscape.

With the emphasis on law enforcement in current applications of science to computer-related crime in education the need for a more expansive mindset for pedagogical programs is apparent. Yasinsac and colleagues emphasize that a convergence of theory and practice to produce a usable pedagogical model is seriously needed. [7]

In order to address these needs, the original brainstorming session of the Digital Forensics Working Group identified specific areas in which significant research was needed. They included the following:

- Digital Forensics Training for Law Enforcement
- Accreditation Criteria for Digital Forensics Programs
- Case Study/Demo Sharing Between Institutions
- Digital Forensics Training for the Legal Profession
- Tools
- Certifications
- Digital Forensic Training for Professionals
- Digital Forensics Training for Professors
- Digital Forensics Training for Students

In addition, the following areas were listed as issues for the working group to consider as they were developing the research in education agenda, but are not part of the research in education agenda, but rather ancillary issues and that should be investigated while conducting research to help meet the goals of the agenda:

- Bootcamps
- Summer Camps
- Evidence Generation
- Scenario Generation
- Accreditation of Forensics Programs
- Expert Witness Preparation
- Current Level of Use
- Steganography

The previous lists were generated during a facilitated brainstorming session on day 1 of the meeting. This is the list that the Digital Forensics Research in Education Working Group has spent the past year discussing and evolving into a hierarchical preliminary research agenda to improve digital forensics education. Once the education categories and issues listed above had been isolated from the other research categories, the resulting content areas were more amenable to a hierarchical organization. The preliminary lists were assimilated into three major categories as shown in figure 1. The remainder of this paper briefly discusses each of the hierarchical items in the diagram with an intent of introducing the associated research in education concept.

3. Educational Methodologies

The Educational Methodologies category includes research that needs to be conducted in order to effectively educate the many diverse populations that use, apply and evaluate digital forensics. The initial populations identified in figure 1 include Law Enforcement, the Legal Profession, Policy-makers, Corporations, Community, and Higher Education.

3.1 Law Enforcement

One might consider the structure of law enforcement digital evidence practitioners as consisting of three levels; police first responders, digital forensic analysts, and federal agency officers. Digital evidence considered in its broadest sense includes individual mobile communication devices, home and small business computing, and corporate networked computer systems.

Police first responders operating at the village and town levels of U.S. communities often have little appreciation of the significant role digital forensic work can play in resolving criminal investigation challenges. Those officers that are aware of the digital forensic role commonly appear to possess unrealistic expectations as to how digital evidence can and should be managed, or how a qualified practitioner functions within the investigation process.

At this lower level of law enforcement first responders the needs are very basic. The basic requirement for this group is to provide sufficient training and education so that they are can recognize potential digital evidence, are not a danger to the digital evidence and that they do no harm to the investigation process.

The second level of responder tends to be a law enforcement officer facing a different set of challenges. As a digital evidence analyst there are expectations from others related to the investigation process. There is frequently a heavy workload placed on digital evidence analysts in law enforcement operating with limited resources. This creates a conflict between management seeking improved returns on investments and investigators requesting more effort be expended to resolve cases. This leaves practitioners with little opportunity to maintain required levels of knowledge and skills to deal with the rapidly changing technologies that they are examining.

At higher levels of the practitioner's hierarchical structure there is more support and resources available to practitioners. At the federal level practitioners are able to work in teams with better resourced laboratories.

The problem is exacerbated by the lack of integration between the three levels and in many cases a lack of understanding of other associated roles. As the three digital evidence roles; data collectors, data processors, and information conveyers; apply across the three levels discussed above it is important from an educational perspective to separate teaching materials in this manner. The practitioner's proficiency in each of these three basic tasks determines how their digital forensic capacity will be measured.

The techniques employed in collecting data as digital evidence varies according to the roles of the law enforcement officer, as well as related jurisdictional issues. Village level police may be required to do little more than to secure data on digital devices. If this is not done appropriately from the very beginning, data critical to an investigation may become worthless.

The second level responder requires additional knowledge, skills, tools and techniques which may be limited to meet the expected workload of that laboratory. As the type and seriousness of investigation cases escalate, the final level of better resourced practitioners undertake the three digital evidence tasks.

Integrating educational approaches to accommodate the roles and tasks of law enforcers at these different levels will resolve current confusion and provide a sound foundation for effective data collection, processing and conveying of digital forensic evidence.

3.2 Expert Witnesses

Expert witnesses are predominantly digital forensics practitioners and law enforcement, involved in the tasks of data conveyance. Their main role is to take collected digital evidence that has been analyzed and processed and form expert opinions about the results obtained. The expert witness uses specialized software as a tool to make judgments regarding the evidence content and it is important that their opinion be bent neither toward the prosecution nor the defense, but an unbiased statement of fact. The judiciary relies upon the expert witness to provide an opinion of the evidence based upon their analysis and experience in the profession.

Research is needed into the requirements for the education and certification of the expert witness to ensure the scope and depth of the education given is appropriate for their role as a friend of the court

3.3 Legal Profession

Educating the legal fraternity is a priority due to long-held views within the profession. Members of the legal profession have adopted different attitudes to digital forensic evidence in accord with their particular judicial perspective. There are three distinct perspectives that may be adopted by legal professionals; prosecution argues for the accused's guilt, defense argues their innocence, and the finder of fact being either the judge or the jury is expected to be neutral until persuaded by legal argument. Prosecution lawyers tend to become involved in legal issues early in the investigation case and develop legal argument to support prosecution as cases progress. Defense lawyers tend to become involved with cases only after prosecution lawyers determine that a prosecution is likely to be successful. As such defense lawyers do not necessarily have the depth of case data exposure that is available to their fellow counsel. This brings about the situation where legal counsel may be widely at variance with each other as to what the digital forensic evidence may be interpreted as meaning in a legal framework.

There is also a tendency for defense lawyers to have gained their early legal experience working with prosecutors. Legal representations from both perspectives tend to rely on legal precedent and legal interpretations to support legal argument rather than becoming learned in every scientific disciple they are likely to become engaged with in court. Specialized publications to meet this legal need include "Expert Evidence" [2].

The third perspective, the finder of fact, is that of the judge or jury. It is at this point in the justice system that possessing expert levels of knowledge and skill in digital forensic might be considered a burden or even a hazard. Finders of fact are expected to determine case outcomes based solely on the evidence presented to the court. To do otherwise might be seen as reaching a conclusion of a person's guilt or otherwise based on preconceived ideas and not solely on presented evidence as the current system demands.

Education courses at tertiary level equipping the legal profession with the skills and knowledge required are increasingly including digital forensics as part of the curriculum. Research is needed in order to identify areas of digital forensics required in each of the legal roles, together with appropriate and effective means of communicating the theory and practice required by each. An understanding of the bigger picture as well as depth in the legal aspects of digital forensics is required by the legal profession. Better education by all parties will help make the justice system work.

3.4 Policy-makers and Legislators

This group includes legislators (e.g., Senators and Congressmen at various levels of government in the United States), their staff members, and staff members in a wide variety of agencies that have some level of responsibility for an area of government (e.g., the U.S. Federal Communications Commission). This group is responsible for producing the legal and regulatory framework in which a given society operates. Members of this group are often drawn from the legal and business communities. However, the legal sense in which this group views the world is significantly different from that faced by their colleagues practicing in the legal profession. In the legal profession the need for digital forensics education is typically at the level of "what does this evidence mean for this specific case" and the role of the participants is clear with respect to their goals (e.g., defend a client in a criminal case). From a policy and legislation perspective, digital forensics must be viewed in light of "what is good for society", and the role of the participants is much close to that of a judge or jury in the legal profession that to the attorneys (i.e., they listen to arguments from groups on many sides of an issue, and ultimately need to decide what most effective meets the needs and goals of society), although the structure of this process is often much less formal than the trial process. As such the need in this domain is at a far higher level of abstraction aimed at ensuring that legislators and policy makers can make decisions from an informed perspective.

3.5 Corporations

Populations included here are corporate security officers, ethical hackers, system analysts, etc. with a focus on education rather than training. There can be some considerable time between the occurrence of an incident and the recognition that an incident has occurred. It is during the period of time between the recognition of an incident and when it has been determined that law enforcement must become involved that the corporate warrior can define the success of an investigation. Without properly understanding the requirements of digital evidence practitioners the corporate security officer is likely to contribute to the problem rather than the solution. The maintenance of corporate computing system's data and log files in a manner conducive to digital

evidence practices can assist practitioners and lead to successful prosecutions.

This requires a proactive approach to information security better enabling digital forensic practitioners to do their work successfully. Often the corporate security officer is technically if not forensically competent and possesses a capacity to ensure data is maintained in a forensically sound manner as a matter of course rather than something undertaken only when a problem occurs. By ensuring that working professionals understand the needs of law enforcement practitioners the prosecution of corporate digital crime are more likely to be successful.

The focus in the corporate world may also be significantly different from that in the legal world, based on the differing goals and rights. For example, a corporate security officer may be far more interested in quickly determining the cause and extent of an incident and then remediating the problem than in ultimately pursuing some legal action. In addition there is likely to be far more latitude in terms of access to and the configuration of corporate IT assets in pursuit of the investigation that would be available to an investigator from a law enforcement agency (although the ability to access devices outside the direct corporate environment is likely to be much less without the involvement of a law enforcement agency). As a result the focus of digital forensics education in the corporate world may be substantially different from that provided to legal investigators, based on the potential difference in the goals of these two groups.

3.6 Community

While research into community education, including K-12 populations may not appear to play a critical role in the evolution of digital forensics, community awareness can, in fact, have a significant impact on the digital forensics process. Educated community members are more likely to be aware of threats and vulnerabilities and can take actions to minimize the potential for and effects of digital crime.

Research needs to be conducted into the best methods to reach the general public and to ensure that they are prepared to protect their digital assets to the best of their abilities. While research into methodologies for educating the diverse constituencies on both sides of the digital divide is important, equally important is the development of support materials to facilitate the educational experience.

3.7 Higher Education

There are many levels of higher education that need to be considered in order to identify appropriate content and educational methods for digital forensics topics that work well for the various higher education markets including community colleges, undergraduate programs, graduate programs, and educators.

As discussed earlier, law enforcement requirements are different to those of working professionals. Different they are, but educators need to understand the requirements and learning outcomes for the array of learners in the digital forensics field. This will require an understanding of the entire field as well as solid knowledge of theories and practice in digital forensics for the array of learning audiences.

Students at the various levels including community college, undergraduate, and graduate programs will have different outcomes and skillsets based on the specialization and academic programs in which they are enrolled. While difference across institutions is expected, there are underlying foundational aspects of the educational process which research in education can drastically improve. At university levels we see digital forensic classes distributed across many disciplines including computer science, electrical engineering, justice, law, and business schools. These diverse academic homes in which digital forensics courses originate provide a rich research-in-education environment that will allow us to evolve multi-disciplinary educational resources and programs.

As educators it is important to understand the needs of each level of student and offer learning knowledge and experiences that are appropriate to that level. At university levels we may still find students wishing to engage in digital forensic studies that are not in possession of requisite background skillsets. To address this issue, we need to develop remediation programs that rapidly assist student in gaining the prerequisite foundational knowledge. Also important are bridging programs that facilitate transitions between the various levels of higher education, including the potentially challenging transition to educator.

Although digital forensic practitioners can provide a wealth of information in skills transfer they may not be able to provide an academically sound educational experience to all levels of the disparate digital forensics audience. In addition, researchers involved in narrowly scoped projects within the discipline lack the breadth of understanding that comes with a holistic educational approach in the

discipline. Practitioners and researchers may not have the depth of understanding of the entire domain nor the theoretical foundations to teach all types of learners in the digital forensics field. As research expertise and practical experience do not necessarily map to good educators, it is important that *educate-the-educator* programs and materials are available to ensure to meet the overall educational need of their target audiences.

Regardless of the comfort level that an educator has with the technical course content, the educational process is not complete without supporting materials to assist the educator is the presentation of the material to the target audience. Whether instructors develop their own support materials, or adopt those created by others, it is important that the appropriate educational material be available to provide an enriched educational experience that ensure that the learners meet the identified outcomes objectives and can demonstrate mastery of the course content.

4. Educational Materials

The education materials utilized must contribute to the stated learning objectives for the level of digital forensics learner, and research into effective and appropriate education materials is key to the success of the endeavor. As the scope of the audience spans all stakeholders in the digital forensics field, there is a need to determine the types of materials most effective for the education of each stakeholder group. Included in such considerations should also be effective approaches to educating the educators in the differing learning environments previously identified.

People learn in different ways – some learn by reading and theory, some by doing, some by explanation, and some by seeing. Kolb [3] categorized these into the following learning styles:

- assimilators, who prefer being presented with sound logical theories to consider
- convergers, who prefer practical applications of concepts and theories
- accommodators, who prefer hands-on experiences
- divergers, who prefer to observe and collect a wide range of information

In the experience of the authors very few can gain concrete learning without practical experience, thus supporting Kolb's four-step experiential learning approach of Do, Observe, Think and Plan [3].

In order to meet the needs of the four types of learners the following types of materials need to be investigated:

- Textbooks and books for further reading
- Lecture notes and working guides providing further explanation of lecture content
- Supporting written materials including glossaries, procedure manuals, statutory and regulatory body publications and the like
- Reports of experience published in a variety of sources including conference proceedings, professional magazines, journals and white papers, illustrating how success has been achieved in real situations
- Practical laboratory exercises for reinforcement of skills and knowledge
- Moot courts where learners can experience the machination of the court room in an isolated and safe learning environment
- Case studies for the practical application of knowledge and skills
- Practice examination questions and answers
- A bank of assessment items to ensure learning objectives are reached at all levels.
- Scenarios that can potentially be part of a library for educators

Effective learning will require a broad-based approach where skills and knowledge are mapped to Bloom's cognitive domain levels for different groups of learners, ranging through Knowledge, Comprehension, Application, Analysis, Synthesis and Evaluation [4]. The learning objectives will dictate the level of mastery required. For example, a network administrator whose role is to collect digital forensic data would require action-based learning at the lower levels of Bloom's taxonomy, possibly up to application of theory at level 3, whereas the forensic practitioner required to appear as an expert witness in court would operate across all six levels.

The divergence of education and training requirements across the digital forensic domain necessitates a more structured and educationally sound approach where the needs of data collectors, data processors and information conveyers are fully addressed. In the current piecemeal situation gaps are clearly evident and a more holistic educational model is needed.

Achievement of the above is challenging without a clearly defined body of knowledge. Much of the current education in digital forensics tends to be training on specific items which quickly become outdated rather than providing students with

capabilities to achieve higher levels of Bloom's taxonomy of educational objectives. Further research is needed to map this body of knowledge to the level of skill and knowledge required of each group of learner.

In addition to educational methodologies and educational materials, there remains the complex problem of providing environments that enrich the educational experience. Due to the complex nature of digital forensics, current computer labs cannot always be repurposed to fulfill this important role. Therefore research to determine the best approaches to developing educational environments is necessary.

5. Educational Environments

There is great benefit in providing students with the opportunity to put their newfound knowledge into practice, whether the student is a novice in the Digital Forensics arena or a seasoned professional. As such, providing appropriate educational environments for practical act ivies is a vital component of this effort.

5.1 Physical Environments

It is easy to envision a physical DF lab environment for which consists of DF hardware and software, but while such a lab has its place it is really only a starting point in the attempt to ensure that educational environments are provided in a manner that is specific to the target audience. For example, it is possible to build physical environments for the following populations:

1) First Responders: Those who initial respond to an incident (e.g., a crime scene, or a computer intrusion) are unlikely to be digital forensics experts, but they are likely to be pivotal in the identification and preservation of digital evidence. For this group a physical lab environment may consist of a simulated crime scene (e.g., a staged room) in which the first responder is charged with identifying and properly securing potential sources of digital evidence, which may include computers, cell phones, PDAs, digital video recording devices, game consoles, and printers. Another lab environment may target system administrators, who may be the first person to investigate some unusual activity in their network, and may then have to determine which devices contain potentially relevant evidence, and how such evidence should be managed in the short term.

2) DF Analysts: Lab environments for this group are likely to focus much more on the analysis effort from the point at which they typically become involved in a case (after the efforts of the first responder). Requirements for this group are likely to include access to DF hardware (e.g., write blocking devices) and software, and scenarios (which may consist of some set of digital media containing evidence, in addition to a backstory that provides some context for the investigation).

3) Legal Community: In many cases the evidence discovered by a DF analyst is used in a legal proceeding, and it is important that the participants, including expert witnesses (who may also be the DF analysts), attorneys, and judges, in such a proceeding understand how to present and challenge digital evidence. An example of an educational environment in this case is a moot court in which students (training as DF analysts) are given the opportunity to present evidence in front of real attorneys and a judge.

5.2 Virtualized Environments

While physical lab environments can certainly model real world situations very well, there are some associated drawbacks. First, and perhaps most obviously, they require physical space and as such don't scale particularly well. The staged crime scene, for example, works quite well in a spare dorm room or office on campus, and the moot court may be able to be held in a real courtroom on weekend once per semester, but it is unlikely that these approaches could be scaled to meet the demands of large numbers of students, or for more frequent use.

Another problem with physical labs is the difficulty in resetting the environment to the initial state for the next student, or group of students, which is again a challenge as the use of the lab scales. Finally, physical labs generally require physical proximity on the part of the students, and while this may be reasonable in some cases (e.g., a training session held in a large metropolitan area) it is less appropriate in others (e.g., providing training resources for police officers in small rural communities). While some physical lab environments can be portable, this is not always the case.

The use of virtualized labs may allow some of these obstacles to be overcome, particularly with respect to the ability to scale the environment to manage larger numbers of students or increased

frequency. Virtualization in this domain can take several forms, including:

1) System virtualization: Computers and networks can be virtualized using many techniques today, with the result that a single physical computer (even a laptop) can concurrent emulate or simulate multiple computing and networking devices. From the perspective of labs aimed at the system administrator first responder for example, this could result in a lab environment which included several hardware and software systems, all of which could be distributed on a DVD or run on each workstation in a computing lab. The DF analyst could also be targeted with this approach by providing virtual machines preconfigured with analysis software and acquired media images. While some of the physical interaction is lost when using such virtual devices, the user interaction with the device is generally identical. Modern virtualization solutions typically offer some form of quick reset functionality (sometimes referred to as a snapshot) which allows the scenario to be immediately reset to one of any number of predefined configurations, thus addressing the difficulty with which physical labs can be reset.
2) Virtual Reality (VR): This generally involves an immersive 3D environment with which the user can interacts, and while such environments have been expensive in the past the availability of high performance commodity hardware now places this in a much more financially attainable range. VR could, for example, be particularly effective as a training tool for first responders by allowing them to interact with crime scenes seeded with potential digital evidence sources, for example.
3) Virtual Worlds: While VR environments typically have some physical component in which the user operates (e.g., a room quipped with projectors, cameras, and sensors), Virtual Worlds (such as Second Life) are entirely contained with the computer systems in which they are executing. The same "world" can be accessed by many users concurrently, and as such it addresses the scalability issue seen in the physical labs. This type of environment seems to be particularly useful in addressing the needs of first responders and the legal community (e.g., moot courts in a virtual world).

5.3 Remotely Accessible Environments

While having all participants physically located in one place may be the easiest option from a lab design point of view, this may not be possible or desirable for the participants due to budgetary and travel limitations. In addition, the rise in the use of distance education in both synchronous and asynchronous modes has provided students with increased flexibility in their education, and as such we should consider how educational lab environments can support these distance learners. System virtualization can support this delivery mode by allowing students to connect via the Internet to a central system on which their virtual machine are executed, or alternatively by the distribution of virtual machines to end users through the distribution of DVDs. Many of the needs of the DF analysts and some of the first responders could be targeted in this manner. Virtual Worlds are similarly flexible, allowing users from all over the world to interact with the same virtual world across the Internet, and this approach would be particularly relevant to first responders and the legal community. Finally, other forms of remote communication tools, such as video conferencing, could be used to provide access for remote users to environments such as a physical moot court.

6. Future Work

The research in education working group has made significant progress towards defining a research in education agenda, but much work remains to be done. The initial hierarchical organization shown in Figure 1 is a starting point, but is by no means complete, nor does it represent the single optimal organization of the categories presented. The Working Group has also investigated a hierarchy with educational populations at the highest level and then investigating the methodologies, materials, and environments that would work best for each. This hierarchical organization and the one shown in figure 1 share the same elements, but this presentation may provide a format that makes research in education for specific groups, such as a community college, more easy to identify and to begin augmenting the research in education agenda as they will have an inherent expertise and experiential background in their particular branch of the hierarchy. The hierarchy presented in figure 1, on the other hand, facilitates research into materials and environments that can meet the needs of more than one of the educational methodology targets, and thus capitalizes on the

potential for reuse and concurrent resource development. There are likely other presentations that could be investigated including dividing the first level of the hierarchy into the part of the digital forensics process that the constituencies are involved in including evidence collection, evidence interpretation, and result conveyance.

7. Conclusions

While much work remains to be done to enumerate the many research in education items that are needed to advance the state-of-the-art in digital forensics education, this foundational work is an important first step in meeting the educational needs of the divers constituencies that are part of the digital forensics process.

8. References

[1] Carrier, B, Spafford, E, Getting physical with the digital forensics investigation, International Journal of Digital Evidence, 2003, Vol. 2, No. 2, Fall, pp 1-20

[2] Smith, F. and Bace, R, A guide to forensic testimony: the art and practice of presenting testimony s an expert technical witness, Boston, MA, Addison-Wesley, 2003

[3] Rogers, Marcus, Seigfried, Kate, The future of computer forensics: a needs analysis survey, Computers & Security, 2004, Vol. 23, pp 12-16

[4] Ieong, Ricci, FORZA- Digital forensics investigation framework that incorporate legal issues, Journal of Digital Investigation, 2006, Vol 3, pp29-36

[5] Losavio, M., Adams, J. Gap analysis: judicial experience and perception of electronic evidence, Journal of Digital Forensic Practice, 2006, Vol 1, pp 13-17

[6] Broucek, Vlasti, Turner, Paul, Winning the battles, losing the war? Rethinking methodology for forensic computing research, Journal in Computer Virology, 2006, Vol , No. 1, August, pp 3-12

[7] Yasinsac, A, Erbacher, R, Marks, D, Pollitt, M, Sommer, P, Computer Forensics Education, IEEE Security & Privacy, July/August, 2003, pp 15-23

[8] Nance, K., B. Hay, M. Bishop. Digital Forensics: Defining a Research Agenda. 42nd Hawaii International Conference on System Sciences. Digital Forensics Research Track. January, 2009.

[9] Freckelton, Ian R. & Selby, Hugh, 2005 Expert evidence : law, practice, procedure and advocacy / by Ian Freckelton and Hugh Selby Lawbook Co.

[10] D.A. Kolb, "Experiential Learning: experience as the source of learning and development," New Jersey, Prentice-Hall

[11] B.S. Bloom (ed.), "Taxonomy of Educational Objectives, the classification of educational goals – Handbook I: Cognitive Domain," New York, McKay (1956)