THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 7 | Number 3 Article 2

2012

On the Development of a Digital Forensics Curriculum

Manghui Tu
Purdue University, Calumet

Dianxiang Xu
Dakota State University

Samsuddin Wira

Cristian Balan
Champlain College

Kyle Cronin
Dakota State University

Recommended Citation

Tu, Manghui; Xu, Dianxiang; Wira, Samsuddin; Balan, Cristian; and Cronin, Kyle (2012) "On the Development of a Digital Forensics Curriculum," *Journal of Digital Forensics, Security and Law*: Vol. 7 : No. 3 , Article 2.
DOI: https://doi.org/10.15394/jdfsl.2012.1126
Available at: https://commons.erau.edu/jdfsl/vol7/iss3/2

On the Development of a Digital Forensics Curriculum

Manghui Tu[1]
Department of Computer Information Technology and Graphics
Purdue University Calumet

Dianxiang Xu
College of Business and Information Systems
Dakota State University, USA

Samsuddin Wira
Department of Public Service
Malaysia

Cristian Balan
Computer and Digital Forensic Program
Champlain College

Kyle Cronin
College of Business and Information Systems
Dakota State University, USA

Abstract

Computer Crime and computer related incidents continue their prevalence and frequency, resulting in losses approaching billions of dollars. To fight against these crimes and frauds, it is urgent to develop digital forensics education programs to train a suitable workforce that can effectively investigate computer crimes and incidents. There is presently no standard to guide the design of digital forensics curriculum for an academic program. In this research, previous work on digital forensics curriculum design and existing education programs are thoroughly investigated. Both digital forensics educators and practitioners were surveyed and results were analyzed to determine the industry and law enforcement need for skills and knowledge for their digital forensic examiners. Based on the survey results and the topics that make up certificate programs in digital forensics, topics that are desired in digital forensics courses are identified. Finally, based on the research findings, six digital forensics courses and required

[1] Corresponding author. Tel: +1 219 989 3253,
Email: manghui.tu@purduecal.edu

topics are proposed to be offered in both undergraduate and graduate digital forensics programs.

Keywords: Digital Forensics, curriculum, survey, undergraduate program, graduate program

1. INTRODUCTION

With continuing advances of computer and Internet technology, the use of digital devices has become embedded in our business and personal lives (Rogers, 2003; Rogers & Seigfried, 2004). For example, communication using email and online chat has become ubiquitous. Businesses and organizations use computer systems and the Internet for e-commerce, business communication, and internal management. Society is very dependent on computers and Internet technologies such that the Internet infrastructure has become the foundation of communications, banking, healthcare, transportation, warfare, etc. (Berghel, 2003; Huebner, Ben, & Ruan, 2008; NIPC, 2003). With the high impact on our society, the computing infrastructure has become the target of criminals, fraudsters, and terrorisms (Berghel, 2003; Huebner et al., 2008; NIPC, 2003; Wolf, 2009). In recent years, many criminals employ computers and computer programs to commit sophisticated financial frauds (Singleton, Singleton, Bologna, & Lindquist, 2006), and more and more hackers attack the computing infrastructure for various reasons (CERT, 2003, 2006; Huebner et al., 2008; Kessler & Haggerty, 2008; Kessler & Schirling, 2006; Rogers, 2004; Wolf, 2009).

Computer crime and computer related incidents continue their prevalence and frequency (CERT, 2003, 2006) and result in billions of dollars in losses (Singleton et al., 2006), which introduces the urgency to build a suitable workforce to contain, prevent and prosecute these crimes, frauds, and attacks by effectively conducting digital investigations (Yasinsac, Erbacher, Marks, Pollitt, & Sommer, 2003). However, computer and Internet technologies are very complex and dynamic, which require digital forensic practitioners to have appropriate knowledge and a wide set of skills (Carlton, 2007; Yasinsac et al., 2003). The U.S. Government Accountability Office (GAO) reported that there are many challenges in fighting against computer crimes and attacks. Some examples include the lack of mechanisms to detect and report cyber-crimes, the lack of education or training standards to ensure adequate analytical and technical capabilities for law enforcement and the lack of guidelines to implement information security practices and raise awareness (Carlton, 2007; Wolf, 2009). Key to addressing such challenges is a comprehensive forensics education, development of better forensic techniques for forensics practitioners and improvement of forensics and security awareness for user.

The computer forensics community is very concerned with the lack of education and training standards for its industry (Huebner et al., 2008; Kessler & Schirling, 2006; Rogers, 2004; Yasinsac et al., 2003). Until now, only a few efforts have been devoted to the development of digital forensics program guidelines (FEPAC,

2008; Huebner et al., 2008; NIST, 2007; Rogers, 2004; Yasinsac et al., 2003). The American Academy of Forensics Science (AAFS) has provided guidelines for forensic science education and training that was developed by the Forensic Science Education Programs Accreditation Commission in 2008 (FEPAC). These works only give general guideline on digital forensic education and training, such as the number of credits needed, the core forensics topics that should be taught, etc. The National Institute of Standards and Technology (NIST) also published guidelines for forensic science education and training that was developed by West Virginia University Forensics Science Initiative (NIST, 2007; West Virginia, 2007). NIST gave general guidelines for program development as well as detailed topics for digital forensics curriculum design. One such example is the student learning in 24 proposed courses amounting to 57 credit hours that includes sample topics (West Virginia, 2007).This work can be an excellent guide for educational program development. However, it would be too expensive for education and training institutes to design an educational program strictly following these recommendations; 24 courses is a substantial amount in an academic program. Actually, none of the existing educational and training programs have implemented such large number of courses in digital forensics. A recently revised program at Champlain College is comprised of 11 digital forensics courses, which is one of the more in-depth curriculums in an undergraduate program. There are some other guidelines for computer related program development. The IEEE and ACM communities provide great recommendations for computer related program design and curriculum development, but very little on addressing the computer forensics program and its curriculum (Liu, 2006). In the past few years, many more universities and colleges started offering courses and even developing programs in computer forensics (Gottschalk, Liu, Dathan, Fitzgerald, & Stein, 2005; Huebner et al., 2008; Kessler & Haggerty, 2008; Kessler & Schirling, 2006; Lang, 1999; Liu, 2006; Troell, Pan, & Stackpole, 2003). Unfortunately, due to the lack of standards, the quality of some these academic courses are suspect (Rogers, 2004).

There are a few research works addressing the computer forensics curriculum design (Berghel, 2003; Gottschalk et al., 2005; Kessler & Schirling, 2006; Liu, 2006; Rogers, 2004; Yasinsac, 2002; Yasinsac et al., 2003). Most of these programs in higher education contain general and survey courses on digital forensics topics (Gottschalk et al., 2005; Kessler & Schirling, 2006), others have modules or topics in computer courses (Yasinsac et al., 2003) and few have a full, in-depth digital forensics curriculum to support an expanded program (Kessler & Schirling, 2006; Peterson, Raines & Baldwin, 2007). Some of the research works recommend courses that should be offered in digital forensic education or training programs (Kessler & Schirling, 2006; Liu, 2006). These research works describe the design of digital forensics courses but do not clearly outline specific learning modules that should be embedded in digital forensics curriculum. Hence, we feel it is necessary to conduct a survey of the digital forensics education programs in

the U.S. in order to develop a more detailed curriculum for digital forensics. The work in West Virginia (2007) provides detailed topics for digital forensics curriculum design; however, the large number of courses in digital forensics makes it difficult to implement in a college program. Therefore, there is an urgent need to identify what digital forensics topics are most needed, and then attempt to create guidelines with a highly compact digital forensics curriculum.

Due to its multidisciplinary nature, digital forensics deals with the arrests, investigations, seizures, preservation, and storage of physical digital devices and objects. As such, digital forensics education is composed of large set of topics (Berghel, 2003; Yasinsac et al., 2003). The objective in this research is to identify the most important topics that should be part of digital forensics courses as viewed by both practitioners and academics. For example, some programs focus on free and open source tools (FOSS), while forensics practitioners in public sectors prefer commercial software tools that have been accepted in the industry (Sam Houston State University, 2009). This point introduces the questions on what tools should be used in the academic classroom, and what skill levels should the students have with these tools. The average cyber-crime perpetrator tends to lack technical skills beyond that of a typical end user, however, hackers may commit a crime using sophisticated computer and Internet techniques (Berghel, 2003; Sam Houston State University, 2009; Yasinsac, 2002; Yasinsac et al., 2003). This leads to questions about the additional topics that should be covered beyond the general forensics skills. Do future digital forensics practitioners need to know the hacking methodologies and approaches? Should an ethical hacking course be part of a digital forensic program? These and other topics should be carefully discussed and examined to ensure that future graduates of digital forensic programs and training are adequately prepared for this constantly changing professional field.

In this research, some of the existing works on digital forensics curriculum design will be first discussed. Then, a survey is presented on courses offered by the existing digital forensic programs, as evident from an analysis of course catalogs and syllabuses. After that, we present the results of a survey of digital forensics educators and practitioners and the analysis of the different sets of questions and responses that were collected. The results of this survey were analyzed to support the proposed course modules. The main contribution of the research is to provide a list of modules for digital forensics courses and to identify digital forensics analysis tools and software to be used in the laboratory environment in preparation for professional work in the field.

2. RELATED WORK

Yasinsac et al. (2003) proposed a model for digital forensics education and training. Their model illustrated digital forensics training based on the role of digital forensics practitioner. Their model divides digital forensics practitioners into four roles, namely, Computer Network Forensics Technician, Computer

Network Forensics Policy Maker, Computer Network Forensics Professional, and Computer Network Forensics Researcher. The topics that are part of the education program are fundamentally different than a training program. An education program focuses on theory and knowledge, while a training program focuses more on practical skills and application. The authors of the model argue that an undergraduate program can ideally integrate topics that are found in both education and training programs. (Troell et al., 2003) describes the development of an undergraduate and graduate course in computer forensics. The undergraduate course introduces the student to the basic tools and procedures of the field. The graduate course has the above undergraduate course as a prerequisite and discusses advanced issues related to analysis and presentation of evidence, as well as the customization and integration of available tools into standard operating procedures. It does not give a detailed guide on the specific topics, especially the practical use of tools, and skills that would fit into the forensics education programs. The High Tech Crime Consortium (HTCC) proposed an online certification program, which demonstrates the perspectives or competencies required of a graduate of a computer forensics program (Lang, 1999). Two programming courses, security concepts, system administration, web publishing, and two courses in computer forensics were recommended. Its main focus was on topics of network and security, and students are not expected to learn practical skills and tools. Erbacher and Swart (2007) pointed out the need to integrate training and education topics in computer forensics education programs, but its main focus is on the managerial or administrative aspect of digital forensics.

Other research works focus on the implementation of the computer forensics curriculum (Huebner et al., 2008; Kessler & Haggerty, 2008; Kessler & Schirling, 2006; Liu, 2006; Wassenaar, Woo, & Wu, 2009). Liu (2006) describes the design of the computer forensics undergraduate program at Metropolitan State University. Their curriculum is made up of forensics laws and criminal justice topics and has a solid foundation in computer technologies. Huebner et al. (2008) summarize the computer forensic courses developed in Australia, however, a detailed computer forensics curriculum and the topics covered in these programs were not given. Kessler & Haggerty (2008) focus on the online delivery of a computer forensics program in forensics management, while Kessler & Schirling (2006) give a very detailed description of the computer forensics curriculum, which focuses largely on the legal procedures. Wassenaar et al. (2009) gives an overview of a computer forensics certificate program and listed a series of courses included in the program, but failed to provide details on computer forensics topics and module in these courses.

3. EXISTING AND PROPOSED DIGITAL FORENSICS COURSES

Champlain College was one of the first colleges to provide a comprehensive computer forensics program (Kessler & Schirling, 2006). The Champlain program offers a broad range of courses related to computer forensics, such as criminal justice, basic computer science courses, and some core computer forensics courses. The two computer forensic courses (Computer Forensics I and II) focus on the investigation of digital data following legal rules of evidence and forensics investigation procedures. Advanced topics such as anti-forensics and networks forensics are introduced in the anti-forensics course along with network security topics that are introduced in the network security course. Due to the success of Champlain College undergraduate program, they moved one step ahead by offering a Master's degree program (Kessler & Haggerty, 2008; Kessler & Schirling, 2006). This program concentrates on digital forensics investigation management and has a limited number of courses that include practical or hands-on training on computer technology. Prominent digital forensics education programs have been developed at other universities such as Metropolitan State University (Liu, 2006), Sam Houston State University (2009), Bloomsburg University of Pennsylvania, University of Central Florida (Craiger, Ponte, Whitcomb, Pollitt, & Eaglin, 2007; UCF, 2010), and University of Rhode Island (URI, 2012). These programs offer courses covering basic digital forensics investigation topics. Some of these programs offer some unique courses. Sam Houston State University (2009) offers an excellent course on hardware forensics and file system forensics that cover different types of digital media, such as cell phones, and uses basic digital forensics tools such as hex editor. Bloomsburg University of Pennsylvania offers courses focusing on topics of various file systems and searching for evidence in windows environment, as well as a course focusing on forensics analysis of small digital media, such as cell phone, PDAs, etc. At Bloomsburg, the primary tool for forensics analysis is Encase. The University of Rhode Island probably offers the most comprehensive courses in digital forensics. They focus on forensics tools practices, network forensics, enterprise computer server forensics, and research topics in digital forensics. The University of Central Florida offers a unique course on forensics practice which focuses on legal procedures of data acquisition, and a special track that gives the student courtroom experience. There are numerous educational digital forensics programs developed throughout the United States that offer many courses covering various topics, but each with a different focus.

Many state laws in the United States require computer forensic expert witnesses and private investigators to have a professional certification or a private investigator's license (Barbara, 2009). A group of professionals from academia met with the aim to change the state requirements by providing guidance for higher learning institutions to develop a neutral digital forensics program that does not rely on any vendor's products. As a result, a model for digital forensics programs at four different levels (i.e., associate degree, baccalaureate degree,

graduate degree, and academic certificate) was developed (West Virginia, 2007). This group proposed that a baccalaureate program should consist of general education, computing and information science core, forensics science core, other additional required courses, digital forensics laboratory and additional upper division digital forensics courses, These upper division courses consist of advanced digital forensics, technical electives, and university level electives open to all students (West Virginia, 2007). They suggested that each of the technical subjects must be accompanied by one-hour labs to practice the procedures and skill they learned from class lectures. The purpose of this lab is to provide students with hands-on experience in digital forensics (West Virginia, 2007).

4. SURVEY RESULTS

In order to determine the technical skills computer forensics practitioners should possess and the tools that should be taught in digital forensics courses, digital forensics practitioners in both public and private sectors were surveyed, each group with a different set of questions.

Digital forensics educators were asked what analysis tools they used in their digital forensics program and were questioned on their willingness to collaborate with digital forensics practitioners for education purposes. Additionally, they were surveyed on their reasons for not collaborating with digital forensics practitioners for education purposes. The survey also asked their opinion in improving digital forensics education. These survey questions were sent out to universities/colleges with computer forensic programs.

Digital forensics practitioners were queried on the involvement of their organization in digital forensics, the type of organization that they are representing, the type of digital forensics investigations they conduct in house, most frequent operating systems found in their investigation, digital forensics analysis tools used, and the willingness to collaborate with a college or university for education purposes. Similarly, the survey also asked digital forensics practitioners' opinion in improving digital forensics education. The survey was conducted among the participants of 2008 Digital Forensics Research Workshop, being that they were experienced researchers and practitioners in the computer forensics field.

In this section, we will discuss the findings of the survey that has been conducted among both digital forensics practitioners and colleges or universities that offer a digital forensics program. Seventeen volunteers from a variety of colleges and universities along with nine volunteers from the digital forensics practitioner group within the United States participated in this survey. Among them, 67% of digital forensics practitioner respondents have less than 10 years of experience with digital forensics. The highest number of respondents was from the digital forensics practitioners group, of which 44.4% was from corporation or private companies. The next largest group of respondents was from law enforcement agencies and non-government organizations at 22.2%. Meanwhile, 11.1% of

digital forensics practitioners were from government agencies and there were no respondents from private investigation.

Digital Forensic Tools	Response from Universities or Colleges (percent)	Response from Digital forensic practitioners (percent)
EnCase	94.1%	66.7%
Access Data Forensic Tool Kit (FTK)	70.6%	55.6%
X-Ways	35.3%	33.3%
iLook	0.0%	33.3%
SMART	0.0%	33.3%
WinHex	64.7%	55.6%
DriveSpy	5.9%	11.1%
FTK Imager	70.6%	66.7%
BlackBag	11.8%	22.2%
MacQuisition Boot Disk	5.9%	33.3%
BlackBag Macintosh Forensic Suite	11.8%	22.2%
MacQuisition	5.9%	22.2%
Autopsy Forensic Browser (TSK)	23.5%	11.1%
HELIX	64.7%	55.6%
Knoppix Live CD	35.3%	22.2%
Knoppix STD	5.9%	11.1%
Foremost	17.6%	0.0%
pyFLAG	5.9%	0.0%
LiveView	29.4%	22.2%
John the Ripper Ethereal	23.5%	33.3%
dcfl-dd	29.4%	33.3%
dd	58.8%	44.4%
memdump	17.6%	22.2%
md5sum	29.4%	55.6%
PTK	0.0%	11.1%
ProDiscover	23.5%	22.2%
DFT	0.0%	0.0%
Device Seizure (Paraben)	23.5%	33.3%
MOBILedit! Forensic	11.8%	55.6%
Wolf iPhone Forensic Software	0.0%	33.3%
XRY	0.0%	22.2%
Athena and Aceso	0.0%	0.0%
FINALMobile Forensics	5.9%	22.2%
Oxygen Forensic Suite 2	5.9%	33.3%
CellDEK®	0.0%	11.1%
STEGALYZERAS (COMMERCIAL)	23.5%	11.1%
STEGALYZERSS (COMMERCIAL)	23.5%	11.1%
STEGDETECT	23.5%	22.2%
STEGHIDE	11.8%	11.1%
OUTGUESS	11.8%	0.0%
Stego Suite (Commercial)	11.8%	11.1%
VideoFOCUS	0.0%	0.0%
dTective	0.0%	11.1%
ClearID DAC QuickEnhance®/AS	0.0%	11.1%
dVeloper	0.0%	11.1%
MagnifiSpotlight	0.0%	11.1%
Other (please specify)	11.1%	11.1%

Figure 1 – Digital forensics analysis tools usage

Figure 1 shows the usage of popular digital forensics tools by both digital forensics practitioners and digital forensics educators. In this figure, both 94.1% of digital forensics educator and 66.7% of digital forensics practitioners use EnCase as their main digital forensics acquisition and analysis tool and they seem to be the most widely used tool for both educators and practitioners. The second-most widely used tool is FTK, as 70.6% of digital forensics educators use it and 56.6% of digital forensics practitioners use it. Some other tools, such as WinHex, HELIX, md5sum and MOBILedit! Forensic are also widely used by digital forensics practitioners, but they seem to be rarely used by educators. Other tools that are not used by digital forensics educators but are used by some digital forensics practitioners are iLook and SMART, PTK, CellDEK, VideoFOCUS, dTective, ClearID, dVelepor and Magnifi. Meanwhile, the tools that are not used by digital forensics practitioners, but used by digital forensics educators, are Foremost, pyFLAG, and OUTGUESS.

Also, in this survey, digital forensics practitioners were asked to describe the type of cases that are involved in their investigations. The result is shown in Figure 2. The most common digital forensic investigation cases, 77.8% of overall cases, are those that deal with single personal computer (PCs). Surprisingly, the second-most common digital forensic investigation cases, 55.6% of overall cases, involve mobile media. The third-most common digital forensic investigation cases, 44.4% of overall cases, involve networks, hacking, and multimedia. Only a small number of cases, i.e., 11.1% of overall cases, are concerned with stenography and other sophisticated computer techniques. Note that the total percentage is over 100% due to the fact that some cases may involve multiple devices. For example, a cell phone, PDA, as well as desktop PCs, laptops, etc may be part of the same case.

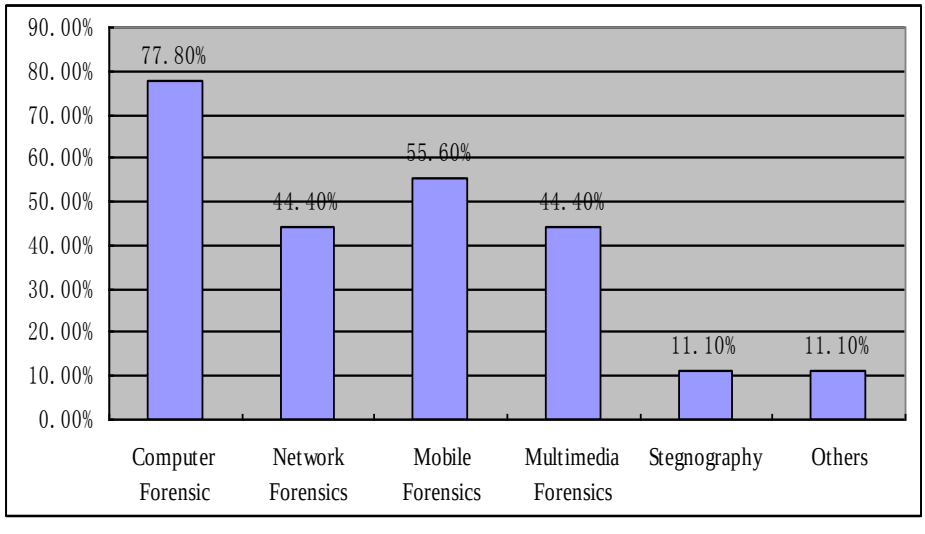

Figure 2 –The percentages of different digital forensics investigation cases

Furthermore, digital forensics practitioners were also asked to indicate what types of operating systems were encountered in their recent investigations and the results are shown in Figure 3. It is not surprising that 100% of digital forensics practitioners responded that the Windows operating environment was part of their investigations. It is followed by Mac OS and Sun Solaris with 55.56%, Linux and FreeBSD with 44.44%, and UNIX and other operating systems with 22.22%. We did not expect Sun Solaris to command such a high percentage as it is not prominently taught in education and training programs. This might be an indication of an important oversight by both education and training programs.

OS involved	Rank
Windows (All type of Windows)	1 (100%)
Linux	3 (44.44%)
FreeBSD	6 (44.44%)
Mac OS	2 (55.56%)
Sun Solaris	5 (55.56%)
Unix	4 (22.22%)
Others	7 (22.22%)

Figure 3 Operating System involved in investigations

To find how close the industry and related organizations can work together with academia for digital forensics education, the willingness to conduct collaborative work for the two entities (e.g., digital forensics educators and practitioners) were surveyed. The survey results are shown in Figure 4.

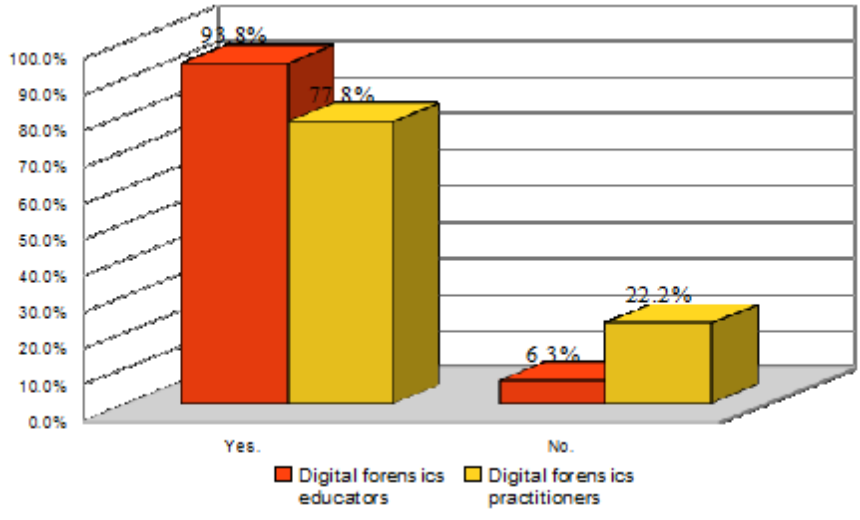

Figure 4 – The willingness of digital forensics educators and digital forensics practitioners to work together in the development of digital forensics education

Answer Options	Response Percent
Budget	100.0%
Security	0.0%
No networking (contacts)	0.0%
Lack of experience lecturers	0.0%

Answer Options	Response Percent
Budget	0.0%
Security issues	50.0%
No networking (contacts)	0.0%
No time to participate	50.0%

Figure 5. Digital forensics educators' (a) practitioners' (b) reasons for not collaborating with each other

It is not surprising that 93.8% of digital forensics educators and 77.8% of digital forensics practitioners are willing to cooperate in the development of digital forensics education programs. The most predominant reason or concern why digital forensic educators (6.3% of digital forensics educators) would not (or cannot) work with digital forensics practitioners in the near future is related to the budget (Figure 5a).

Meanwhile, the reasons that 22.2% of digital forensics practitioners are not willing to collaborate with educators revolve around security issues and time to devote to the collaboration. In certain cases collaboration with educators is simply irrelevant to their scope of work (Figure 5b). It has been discussed in the digital forensics community that a close collaboration between industry, government agencies, and educational institutes would be beneficial to every party. Within such collaborative infrastructure, faculty members and researchers will collaboratively have a better knowledge of what is needed for the forensic community. Students will have a stronger learning motivation associated with the application of what they have learned to real world scenarios. The industry and government agencies will have a better channel to recruit forensics examiners to staff their laboratories and incidents response teams.

5. PROPOSED DIGITAL FORENSICS MODULES

As indicated by Figure 1, it is not difficult to notice that most of the digital forensic practitioners either use Encase or FTK as digital forensics examination tool in their investigations, and this is easily explained by the large market share that these two commercial products command.. Aside from these two tools, WinHex, HELIX, md5sum and MOBILedit! were selected as frequently used digital forensics analysis. To examine cell phones, MOBILedit! is one of the most frequently used tools for analysis. In addition, HELIX is becoming popular among digital forensics practitioners and digital forensics educators. One of the reasons for its popularity is the fact that HELIX is a complete digital forensics analysis tool that has a large set of programs and plug-ins that are required for digital investigation. Based on the survey results, there is an indication that a digital forensic practitioner should be proficient in using most popular tools, such as FTK and Encase. Thus, it is beneficial to have students graduating from

forensic programs to have ample training on these tools. Moreover, a heavy module on forensic tools, which focuses on FTK and Encase, and covers Helix, WinHex, and other open source tools, should be built into forensic courses. The Technical Working Group for Education and Training in Digital Forensics recommends that a designated computer forensics lab should be designed to provide equipment and software to train student on the practical skills (West Virginia, 2007), especially using the popular digital forensic tools presented in our results.

Digital forensics requires an investigator to have ample knowledge on a variety of operating systems. As shown in Figure 3, almost all operating systems were part of investigations carried on by digital forensics practitioners, such as Windows, which was the most common, followed by Unix/Linux and Mac OS. Based on practitioners' experience, Windows machines are the most common in the investigative caseload, while Unix/Linux comprises about 20% of the overall systems (Pogue, 2008). This indicates that a variety of operating systems should be addressed in digital forensics curriculum, but the focus should be primarily on Windows, with a secondary focus on Unix/Linux and Macintosh. Even though theoretically, it is desirable to teach as many operating systems as possible, unfortunately, there are limited resources available in educational programs, including time, equipment, and faculty resource. Due to the rapid development of learning tools available, student or digital forensics practitioners would be able to learn from external sources, such as the Internet, conferences and vendor specific training. While not part of the survey, it is our opinion that the use of virtual machines has minimized the need for multiple hardware platforms and has made access to multiple Operating Systems in the classroom more affordable.

Most white-collar crimes in the public sector deal with single machines. The counter-investigative skills involved are not beyond typical end users (Berghel, 2003). However, there are substantially increasing numbers of cases dealing with networks, protocols/devices, and Internet applications as observed from the survey results shown in Figure 2. Furthermore, there are many incidents in the private sector that go unreported due to various reasons (Berghel, 2003; Rogers, 2004). Many of these incidents deal with adversaries that have a set of skills that are well beyond that of normal end users. These skills deal with a variety of protocols/software to include end user applications, operating systems, networks, and Internet. To effectively and efficiently investigate these criminal cases and their perpetrators, to find relevant evidence, digital forensic practitioners need to have a more elaborate set of knowledge and skills, which introduce the discipline of network/internet forensics. Until now, there are very few education programs that offer such training, and no consensus exists as to the tools and topics that should be covered in education courses to address network/internet forensics. To successfully investigate Internet crimes, students need to understand the fundamental mechanisms, methodologies, and approaches employed by these sophisticated criminals while committing such crimes, as well as possible

countermeasures organizations and companies can use to defend themselves. Based on the above observations, network forensics related courses need to cover a large amount of topics, such as operating systems, network and internet protocols, malwares, devices, applications, network hacking methodology and techniques as well as countermeasures and security mechanisms.

With the advances in computer and Internet technology, mobile computing has become more and more popular. A large number of mobile devices are available and have been used to play music and store photos, contacts, and files or even play movies (Kiley, Shinbara, & Rogers, 2007). Tools such as XRY, Cellebrite, and Oxygen can be used for logical extraction from mobile devices, while the tools such as XACT and Cellebrite PA can be used for physical extraction of data from mobile devices. Some of the tools, such as Paraben Device Seizure, can be used for both physical and logical extraction from mobile devices, but each has its limitations as each mobile vendor uses their own operating system. The popularity and ubiquity of mobile devices continue to grow in every corner of our personal and business lives, and also in modern cybercrimes (Kiley et al., 2007). The survey indicates that more than half of the cases included mobile devices. Additionally, due to vast difference in configurations and settings among mobile devices, digital forensics practitioners need to have ample exposure to mobile devices. It is important to include a module in computer forensics curriculum that addresses mobile forensics topics, such as wireless Local Area Network (WLAN), Personal Digital Assistant (PDA), iPod, iPhone, Blackberry, etc.

There seems to be a great deal of concern on how to train students to meet both the industry and law enforcement needs (Liu, 2006). There are multiple approaches to address this issue; the proposed approach is to collaborate with digital forensics practitioners from both industry and law enforcement community. Based on the survey results, more than 75% of digital forensics educators and digital forensics investigators agreed to cooperate in the development of a digital forensics program at universities or colleges. The reasons why forensics practitioners and educators resist collaboration include budget, security reasons, time, and lack of applicability to their scope of work. It is unrealistic to have digital forensic practitioners devote a large block of time to the development of educational programs and these road blocks include budgetary and scheduling constraints. It is imperative that coursework in digital forensics should incorporate the experience and ideas from the industry and law enforcement. Appropriate courses that can be fit into this category are professional project, internships and/ or courtroom experience. Further research should explore the relationship between students completing professional projects and internships and the students competiveness in the job market once they graduate. Anecdotal data indicates that students completing internships in the field obtain relevant employment within six months of graduation, more so than students that did not undergo an internship.

The Professional Project course should be a research project which requires the application of the knowledge, techniques, methodology, and skills learned from other digital forensics courses. Topics could be either from academia or from industry. The survey result indicates that multimedia forensic analysis has been conducted by digital forensics practitioners, which requires the use of a suite of tools including VideoFOCUS, dTective, ClearID DAC, dVeleloper and Magnifi Spotlight. Several research issues on multimedia forensics exists which need to be undertaken to improve the efficiency and accuracy of the results. Another important topic is the deployment of a honeypot which has been recently used for cyber security protection and network forensic investigation (Spitzner, 2003), due to its cost effectiveness and usefulness for security and forensic education and research. Other important topics include malware forensics analysis, social computing forensics (for example, forensics investigation on Facebook, MySpace, Twitter, Blogosphere, etc.), accounting and financial fraud detection and investigation. Furthermore, evidence should be presented in a in a clear, concise, professional way so that audiences in a courtroom, such as a jury, judge, and attorneys, can easily understand it. The Courtroom Experience course is an application of the knowledge, skills, and methodology learned from all the courses in the education program, including forensic law, criminal justice, communication, digital forensics investigation, and other computer courses. In a mock courtroom, judges and attorneys from industry and law enforcement can participate, and the cases may be a simulation of real world scenarios. In a mock trial course, the students can apply what they have learned and gain real world experiences.

Another approach to collaborate with industry and law enforcement is to incorporate topics emphasized in certification programs into the curriculum design of educational programs. There are many certification programs available, including EC Council's CHFI (Compute Hacking and Forensic Investigator Certification), AccessData's ACE (AccessData Computer Examiner), Guidance Software's EnCE (Encase Certified Examiner), CCE (Certified Computer Examiner) administrated by the International Society of Forensic Computer Examiners, CIFI (Certified Information Forensic Investigator) offered by International Information Systems Forensic Association, CFCE (Certified Forensic Computer Examiner) managed by the International Association of Computer Investigative Specialists, DFCP and DFCA Certifications managed by DFCB (Digital Forensic Certificate Board), and GCFA (GIAC Certified Forensics Analysts) managed by SANS. Some common topics were identified from these certification programs that would be appropriate for an education program. Modules from CHFI, CCE, ACE, and EnCE could be included in both graduate and undergraduate curriculum. As a matter of fact, AccessData offers its training material to colleges that sign up for their educational bundle and have two faculty members that are ACE certified.

Courses and topics	
Digital Forensics Fundamentals	Digital forensic investigation procedures, private regulations and public law issues, Windows FAT and NTFS, *nix and Mac File Systems, open and commercial forensic tools (Encase, FTK), evidence acquisition, preserving, analysis, report, and presentation.
Advanced Computer Forensics	Advanced features of forensics tools (search, KFF Management, encryption and decryption, data carving), windows registry, memory analysis, advanced file system analysis (deleted and hidden data, metadata, temporary file, unknown\executable file analysis), applied decryption
Network/ Internet Forensics	Internet and Network security, ethical hacking, network traffic analysis, log analysis, web attack and DOS investigation, Email forensics, internet application forensics, social computing forensics (social networks/Web2.0), malware analysis
Mobile Digital Forensics	Wireless security and attacks, wireless track and investigation, cell phone, IPhone, IPod, PDA, Blackberry, etc.
Professional Project on Digital Forensics	Integrate existing knowledge and skills in digital forensics and conduct research to understand advanced cyber-crime methodologies and techniques and research on advanced digital forensics investigation and analysis techniques (honeynet, etc)
Courtroom Experience	Work with digital forensic practitioners from public/ private sectors on a mock case, integrating knowledge and skills from forensics law, criminal justice, forensic psychology, and digital forensics fields, and present in a mock courtroom

Figure 6 –Proposed Digital Forensics courses.

Based on the survey results, the following six courses are proposed as the core digital forensics topics for digital forensics education programs: 1) Digital Forensics Fundamentals, 2) Advanced Computer Forensics, 3) Network/Internet Forensics, 4) Mobile Digital Forensics, 5) Digital Forensics Professional Project and Courtroom Experience. These courses could be designed to fit both undergraduate and graduate programs with minor adjustments. For example, the professional project could be optional for undergraduate studies but it could be required by graduate programs. Another example would be mobile forensics being required by undergraduate programs but it could be optional for graduate studies. The detailed topics for each course are shown in Figure 6. Note that in this paper, only those courses related to computer technology are discussed. The coursework in criminal justice and forensic law are not discussed here as they have been discussed in many other publications (Gottschalk et al., 2005; Huebner et al., 2008; Kessler & Schirling, 2006; Liu, 2006; Rogers, 2004).

The above courses and modules have been recently implemented at Champlain

College in the Computer and Digital Forensics Program Curriculum in 2011 (Champlain College, 2011). For example, the topics defined in Digital Forensics Fundamentals are implemented in FOR 320 (*File System Forensics*) and FOR 340 (*Operating System Forensics*), the topics defined in Advanced Computer Forensics are implemented in FOR 430 (*Advanced Practice in Digital Investigations*), the topics defined in Mobile Digital Forensics are implemented in FOR 310 (Mobile Device Forensics), the topics defined in Professional Project on Digital Forensics are implemented in FOR 490 (*Computer Forensics Internship*), the topics defined in Network and Internet Forensics is implemented in FOR 270 (*Anti-Forensics & Network Forensics*) and FOR 420 (*E-Discovery and Data Analytics*), and the topics defined in Courtroom Experience are implemented in CRJ 480 (*Crime Scene Investigation*) and CCC 410 (*Capstone*).

6. CONCLUSION

This research investigated digital forensics curriculum design and existing education programs, which provides a list of computer forensics courses in general, but without much indication on what topics should be included and what tools should be taught. To determine the set of knowledge, methodology and skills that the industry and law enforcement require, both digital forensics educators and practitioners were surveyed and the results were analyzed. The most prevalent tools in use are commercial tools, such as Encase and FTK, and most cases deal with Windows operating systems, followed by Unix/Linux and Macintosh. Also, most digital forensics educators and practitioners are willing to collaborate to develop digital forensics educational programs, but most organizations are limited by budget and time availability. Based on the identified digital forensics topics, courses that support the industry and law enforcement needs are recommended. Specifically, courses that simulate real world digital forensics investigation are designed to enhance the collaboration with digital forensics practitioners from industry and law enforcement sectors.

Based on our findings, some future research directions are recommended. First, to provide flexibility and cost-effectiveness, as well as improve enrollment, we would like to investigate the issues and approaches to design online security and forensic courses. The online courses should have access to all the commercial and open source tools similar to on-campus learning environment, and the solution should be well scaled and flexible to adapt to the rapid changing computer and forensics technologies. Second, the design of both undergraduate and graduate digital forensics programs should be explored on how to incorporate with those existing computer and network security programs. Clear delineation between information security and digital forensics, especially when discussing network forensics, does not appear to exist. There is evidence to suggest that students can benefit professionally from information assurance skills and knowledge when undertaking network forensics incidents. Third, it is recommended to integrate a large portion of the business management and business information systems

component into the digital forensics program design, since fraud and other white-collar crimes are significant threats to businesses. Such interdisciplinary curriculum design and education fit the mission of many business programs and can be incorporated in criminal justice, information systems, and computer science programs at other colleges and universities.

7. REFERENCES

Barbara, J.J. (2009). The Case Against PI Licensing for Digital Forensic Examiners. *Forensics Magazine*, *6*(2), 23-29.

Berghel, H. (2003). The discipline of Internet forensics. *Communications of the ACM*, *46*(8), 15-20.

Brueckner, S., Guaspari, D., Adelstein, F., & Weeks, J. (2008) Automated computer forensics training in a virtualized environment. *Journal of Digital Investigation*, *5*(2008), S105-S111.

Carlton, G.H. (2007). A grounded theory approach to identifying and measuring forensic data acquisition tasks. *Journal of Digital Forensics, Security and Law, 2*(1), 35-56.

CERT. (2003). CERT statistics. Retrieved from http://www.cert.org/stats/

CERT. (2006). CERT statistics. Retrieved from http://www.cert.org/stats/

Champlain College. (2011). Computer & Digital Forensics Major. Retrieved from http://www.champlain.edu/Undergraduate-Studies/Majors-and-Programs/Computer-and-Digital-Forensics.html.

Craiger, P., Ponte, L., Whitcomb, C., Pollitt, M., & Eaglin, R. (2007). Master's Degree in Digital Forensics. In *Proceedings of the 40th Hawaii International Conference on System Sciences*.

Erbacher, R.F., & Swart, R. (2007) Computer Forensics: Education and Training. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.97.6123&rep=rep1&type=pdf

FEPAC. (2008). America Academy of Forensics Science. Forensics science education programs accreditation commission, accreditation standards. Retrieved from http://aafs.org/sites/default/files/pdf/FEPACStandards072410DRAFT.pdf

Gottschalk, L., Liu, J., Dathan, B., Fitzgerald S., & Stein, M. (2005). Computer

Forensics Programs in Higher Education: A Preliminary Study. *Metropolitan State University*. In *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education*.

Huebner, E., Ben, D., & Ruan, C. (2008). Computer Forensics Tertiary Education in Australia. *2008 IEEE International conference on computer Science and Software Engineering.* Dec 12-14, 2008.

Kessler, G.C. (2007). Online Education in Computer and Digital Forensics: A Case Study. In *Proceedings of the 40th Hawaii International Conference on Systems Sciences (HICSS 40)*, Jan 3-6, 2007, Hawaii, USA.

Kessler, G.C. & Haggerty, D. (2008). Pedagogy and Overview of a Graduate Program in Digital Investigation Management. In *Proceedings of the 41st Hawaii International Conference on System Sciences*.

Kessler, G.C. & Schirling, M.E. (2006) The Design of Undergraduate Degree Program in Computer & Digital Forensics. *Journal of Digital Forensics*, Security *& Law*, *1*(3), 37-50.

Kiley, M., Shinbara, T., & Rogers, M. K. (2007). IPod Forensics Update. *International Journal of Digital Evidence*, *6*(1), 1-9.

Lang, D. (1999). Design and Development of a Distance Education Paradigm for Training Computer Forensics Examiners: A Limited Review of Literature. Retrieved from http://www.computerteacher.org/CFLR.htm

Liu, J. (2006). Developing an innovative baccalaureate program in computer forensics. In *Proceedings of the 36th ASEE/IEEE Frontiers in Education Conference*. October 28–31, 2006, San Diego, CA.

NIPC. (2003). National Infrastructure Protection Center white paper -- Risk Management: An Essential Guide to Protecting Critical Assets. Retrieved from http://www.nipc.gov/publications/ nipcpub/newnipcpub.htm

NIST. (2007). National Institute of Standards and Technology (NIST). Education and Training in Digital Evidence: A Guide for Law Enforcement, Educational Institutions, and Students. Gaithersburg, MD: NIST, Technical Working Group for Education -- Digital Evidence.

Peterson, G.L., Raines, R.A., & Baldwin, R.O. (2007). Graduate Digital Forensics Education at the Air Force Institute of Technology. In Proceedings of the 40th

Annual Hawaii International Conference on System Sciences (HICSS'07).1530-1605/07. Jan 3-6, 2007, Hawaii, USA

Pogue, C., Altheide, C., & Haverkos, T. (2008). Unix and Linux Forensics Analysis DVD Toolkit. Syngress.

Rogers, M.K. (2003). The role of criminal profiling in computer forensic investigations. *Journal of Computer Security*, *22*(4), 292-298.

Rogers, M.K. & Seigfried, K. (2004). The future of computer forensics: A needs analysis survey. *Journal of Computer and Security*, *23*, 12-16.

Sam Houston State University. (2009). The Digital Forensics undergraduate program. Department of Computer Science. Retrieved from http://www.shsu.edu/catalog/df.html#df390

Singleton, T.W., Singleton, A.J., Bologna, G.J., & Lindquist, R.J. (2006). *Fraud Auditing and Forensics Accounting*, 3rd ed. John Wiley & Sons, Inc.

Spitzner, L. (2003). The Honeynet Project: Trapping the hackers. *IEEE Security and Privacy*, *1*(2), 15-23.

SWGIT. (2004). Scientific Working Groups on Digital Evidence and Imaging Technology. SWGDE/SWGIT Guidelines & Recommendation for Training in Digital Multimedia Evidence. Version 1.

Taylor, C., Endicott-Popovsky, B., & Philips, A. (2007, April). Forensic Education: Assessment and Measures of Excellence. IEEE ADFE. 155-165.

Troell, L., Pan, Y., & Stackpole, B. (2003). Forensic Course Development. In *Proceedings of the Conference on Information Technology Curriculum 4 (CITC4 '03)* (Lafayette, IN, October 16-18, 2003). 265-269.

UCF. (2010). Master of Science in Forensic Program. University of Central Florida. Retrieved from http://msdf.ucf.edu/curriculum.html

URI. (2012). Digital Forensics Programs. The University of Rhode Island. Retrieved from http://forensics.cs.uri.edu/courses.php

Wassenaar, D., Woo, D., & Wu. P. (2009). A Certificate Program in Computer Forensics. *Journal of Computing Science in College*, *24*(1), 158-167.

West Virginia University. (2007). West Virginia University Forensic Science Initiative. Technical Working Group for Education and Training in Digital Forensics.

Wolf, U. (2009). Cyber-Crime: Law Enforcement Must Keep Pace With Tech-Savvy Criminals. Retrieved from http://www.govtech.com/dc/articles/575223

Yasinsac, A. (2002). Information Security Curricula in Computer Science Departments: Theory and Practice. *The George Washington University Journal of Information Security*, *1*(2) 1-9.

Yasinsac, A., Erbacher, R.F., Marks, D.G., Pollitt, M.M., & Sommer, P.M. (2003). Computer Forensics Education. *IEEE Security & Privacy*, *1*(4), 15-23.