Ten-Year Synthesis Review: A Baccalaureate Program in Computer Forensics

Jigang Liu

Department of Information and Computer Sciences

Metropolitan State University

700 East Seventh Street

St. Paul, MN 55106 USA

Jigang.liu@metrostate.edu

Abstract

This study is a ten-year synthesis review on running a baccalaureate program in computer forensics at a public university in the states. As an emerging field in technology as well as in law and legal systems, computer forensics has established its own position in the modern society. Although there are many similarities to introducing a new product or starting up a new company, having a new four-year program in a cutting edge field out of ground and running presents different hurdles and unique challenges. Based on the analysis and assessment on how a baccalaureate program in computer forensics has been implemented at a public university for last ten years, lessons learned and recommendations made in the paper are helpful to those who are currently running or about to begin offering or thinking to propose a similar program in an emerging technology field. While the technology never stops advancing, the higher education should continue updating its curricula to prepare its students in adapting to and thriving in this ever changing world.

1. INTRODUCTION

After the “ILOVEYOU” computer virus struck the world with about 10% computers on the internet affected in early May, 2000, the concept of computer security was realized and accepted by the public [2] [23]. While prosecuting the criminals who wrote and spread the virus, the field of computer forensics was emerged to the public although the digital evidence had been already collected and analyzed in the law enforcement community as early as 1980s [29].

“Forensic” is defined as “relating to or dealing with the application of scientific knowledge to legal problems” by Merriam-Webster. As a multi-disciplinary professional organization that provides leadership to advance science and its application to the legal system, the American Academy of Forensic Sciences (AAFS) further states that “any science used for the purposes of the law is a forensic science” [1]. Due to the fact of digital evidence found in computers as well as in other digital devices, the field of computer forensics is classified as “Digital and Multimedia Forensic Sciences” by AAFS along with other ten forensic science disciplines. In this study, we use the definition of computer forensics given by the US-CERT as follow, computer forensics is “the discipline that combines elements

of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law [27].”

In addition to AAFS, another professional group, Scientific Working Group on Digital Evidence, SWG-DE, was heavily involved in the early development of the field [24]. Established in 1998 by the Federal Crime Laboratory Directors group, SWG-DE brought together organizations actively engaged in the field of digital and multimedia evidence. In addition to coordinating the creation of the standards and principles among the crime labs around country from various legal and government sectors, the group contributed the early training materials and developed some baseline definitions in the field [21] [24].

The recently published three investigations in [8] have illustrated how critical the digital evidence to the criminal justice community. In finding the killer of Christian Aguilar, a freshman at University of Florida in 2012, digital evidence recovered from Pedro Bravo’s cell phone played a pivotal role in Bravo’s conviction of first-degree murder. The study also shows how inconsistent or tampered digital evidence collected and presented by inexperienced digital investigators has eventually provided reasonable doubt to jurors in the murder trial of Casey Anthony in 2011. The critical mistakes made in court were the number of browser searches on a chemical word “chloroform,” once instead of 84 times, and the browser Anthony used, Mozilla’s Firefox instead of Microsoft’s Internet Explorer. The last case presented in this study highlights the challenges for modern investigation when digital evidence is limited or does not even exist.

In next section, the development of computer forensics education and evolvement of the curricular is discussed. The current status of the program developed at Metropolitan State University, Minneapolis/St. Paul, Minnesota, is presented in section 3, followed by the retrospective analysis and synthetic review of the program for the past ten years in section 4. The accreditation consideration and autonomy concerns are discussed in section 5. Finally, in section 6, the conclusion and future plan are provided.

2. Evolvement of Computer Forensics Education

Led by the National Institute of Justice (NIJ), the research, development, and evaluation arm of the DOJ, the early computer forensic community had made the education in computer forensics (uniform training and certification courses) as one of the ten critical needs for supporting electronic crime needs assessment for state and local law enforcement in March 2001 [29] along with other nine needs in public awareness, data and reporting, on-site management assistance, updated laws, cooperation with the high-tech industry, special research and publications, management awareness and

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

SIGITE'16, September 28–October 1, 2016, Boston, MA, USA.

© 2016 ACM. ISBN 978-1-4503-4452-4/16/09...\$15.00

DOI: <http://dx.doi.org/10.1145/2978192.2978226>

support, investigative and forensic tools, and structuring a computer crime unit.

While some training courses created by the professional organizations, the early effort in developing courses in computer forensics in the academic area were emerged, such as the courses introduced in [25] and [26], and minor programs in computer forensics in [3] and [5]. Some early studies in computer forensic education could also be found in [7] and [30].

For a four-year institution, in addition to a four-year program, computer forensics can also be introduced by creating a track, a concentration, or a minor to some existing four-year programs, such as Information Technology and Criminal Justice programs. Since different ways of the implementation have different strengths and limitations, how to run a computer forensics program will largely depend on the availability of the resources, namely potential faculty expertise, student demography, community support, and available funding, etc., an institution can offer. The early studies on the issues in [7], [10] and [11] demonstrated how the different programs were created and evolved with their institutions. The challenges in selecting textbooks for this emerging field and how to work with the students with limited technical background were well discussed in [14] and [16]. An early comparative study on the education between forensic science and the computer forensics can be found in [10].

Based on the official publications, the very first baccalaureate program in computer forensics was fully introduced in 2004 [11] followed by several early programs introduced in 2005 [13], 2009 [9], and 2010 [22], respectively. A recent study in [17] has shown that there are 13 baccalaureate programs in computer forensics currently running in the states (online programs are not included). Out of those 13 programs, 8 programs are implemented at private institutions while 5 are offered by public colleges/universities. From the administration point of view, the programs are mainly managed by an integrated center at a private institution while the programs are often administrated by an academic department at a public university. In terms of the nature of the centers or departments, the majority of them are either business administration or computer technology with two programs managed by criminal justice related centers or departments. Since Computer Forensics is a multidisciplinary program, it is expected that the program would be managed by different departments from different colleges. For the five public institutions, 3 out of 5 programs are operated by a department related to computer technology while one with either business administration or criminal justice related department. Geographical wise, Pennsylvania hosts 3 programs, Michigan and Ohio have 2 each, and a single program is offered in Iowa, Minnesota, New York, Oklahoma, Vermont, and D.C. [17].

Although private institutions have taken the lead in offering a four-year program in computer/digital forensics as the study shows [17], it is anticipated that the impact on promoting a four-year program in computer/digital forensics program from public institutions will be increased significantly in the near future as University of Albany and University of Michigan Dearborn have joined the group recently.

While the evolution of this emerging field continues, computer forensics has been recognized by the National Science Foundation as one of the STEM (Science, Technology, Engineering, and Mathematics) disciplines since 2012 [19]. Supported by the NSF grant, the most recent effort in developing a self-contained curriculum package in introducing this emerging field as a track or minor for an existing baccalaureate program has been on the way at University of Illinois at Urbana Champaign since fall 2012 [12].

Due to the fact that more electronic evidences are found in digital devices as well as the nature of the multidisciplinary, the name of the field has been evolved from Computer Forensics to Digital

Forensics. Although digital forensics does sound closer to the reality, a valid assessment can also be made as data mining, artificial intelligence, cloud computing, and database management have been well developed the curriculum of computer science. As illustrated in Table 2.1 (the google searches made on July 29, 2016 for the phrases “Computer Forensics” and “Digital Forensics” over the interested domains from a Safari 9.0.2. browser, respectively) below, the terms of Computer Forensics and Digital Forensics have been almost equally used over the internet.

Table 2.1 Google Search Hits: Computer Forensics vs. Digital Forensics

	.edu	.com	.gov	.org
Computer Forensics	56,300	905,000	10,900	145,000
Digital Forensics	41,700	842,000	5,480	91,500

In addition to the consideration discussed above, the title of “Computer Forensics” helps our students easily locate the department that offers the program. In this paper, we use “Computer Forensics” and “Digital Forensics” exchangeably.

3. Current Status of the Computer Forensics Program

Metropolitan State University is a comprehensive public urban university serves more than 11,500 students throughout the metropolitan area of Minneapolis/St. Paul, Minnesota. As a non-traditional university with its students at an average age of 32 and nine out of 10 are working adults, the university builds on its strengths as an innovative, comprehensive university that meets the higher education needs in the region. The department of Information and Computer Sciences has nine full time and more than 20 part-time faculty members, and offers four undergraduate and two graduate programs. Among the four undergraduate programs, Computer Science program was established in 1998 and has become the largest program in terms of the number of the students enrolled in the program. Computer Information Technology program is a revision and replacement of our oldest program in Computer Information Systems, which occurred in 2012. Since Computer Application Development is the newest program (established in fall 2014), the statistics discussed in this section will not include this program.

After two years’ effort in having the program proposal approved by each of the required academic units as well as the university system of the state, we began to offer the Computer Forensics program in fall 2005. Since we were unable to hire a computer forensics faculty until fall 2007, running the program in the first two years was very challenging as well as exciting. Although we were fortunate to have a few computer forensics experts from local industry and the state’s agencies to help us to cover the new courses on the subject, the pressure and demand on finding a right instructor for a new course for a particular schedule as well as developing the new courses, seeking funding, and recruiting and advising students was overwhelming. There were many reasons for how those initial obstacles were overcome. The consistent support from within the department as well as other departments, especially from the department of Criminal Justice, was tremendous. The understanding and encouragement from the administration, especially from the dean of the college, was critical. Moreover, our adult and risk-taking students responded to the new program very well, which was an anticipated indicator for the potential success.

Our very first student graduated from the program in spring 2007 and the program has been growing and operated steadily for the past 10 academic years as the numbers of the graduates shown in Figure 3.1. along with the numbers of the graduates from other two programs in Computer Science and Computer Information Technology. Each academic year shown in the figure represents the

previous year’s summer and fall semesters and the current year’s spring. For instance, the academic year 2007 includes summer 2006, fall 2006, and spring 2007.

Figure 3.1 The numbers of the graduates for CFS, CIT, and CS from 2007 to 2016

As the numbers shown in Figure 3.1, computer forensics program reached its graduation peak in 2012 with 38 graduates comparing 27 in computer science and 23 in computer information technology.

To see the balance among the three programs, Figure 3.2 presents the percentage of the yearly graduates of each majors to the total number of the graduates from the department. This figure proves that computer forensics program has established its position as one of the solid programs in the department.

Figure 3.2 Graduation percentage among the three majors

Overall, 177 students have graduated from the computer forensics since the establishment of the program in fall 2005, which composes 22% all the graduates from the department as shown in Figure 3.3 below.

Figure 3.3 total graduates in CFS, CIT, and CS from 2007 to 2016 (N=820)

Since most of our students are transferring students with an average of 70 earned college credits when they join the program, to know what they have been studied will certainly help us in knowing what they have learned and what they need to learn. In addition, to know their academic background will also help us to identify the students who are more interested in our program. Following the study, we did four years ago, on the academic background of our students in [15], we update the study with the new data we have collected since then and present it in Figure 3.4, the applicant counts

in each of the categories, and Figure 3.5, the percentage of the applicants in each of the categories below.

Figure 3.4 Background of the applicants to CFS program

Background	Percentage (N=495)
IT	27
Criminal Justice	20
Liberal Arts	20
CS	9
Others	8
Natural Sciences	8
Business	7
MIS	1

Figure 3.5 Proportions of the applicants to the CFS program

The data presented in Figure 3.4 is based on an incomplete collection prior to 2011 and a complete collection afterwards. the category IT, Information Technology, includes the studies in network, databased, and system administration, and any other IT areas which are not based on programming skills. Category CS, Computer Science, is specially interesting to us because we would like to validate that computer forensics program is not competing with our computer science program or computer information technology program with the respect of students, which was the bottom line our Dean asked us to follow when he approved the program proposal. The Dean’s point was if a newly proposed program would compete with an existing program for students, the new program would not help the department and then the university to grow with regard to serving more students. The data shown in Figure 3.5 has proven we have met the Dean’s request with only 9% of the applicants were with a background in Computer Science or a program that concentrates in programming. The brightest point shown in the figures is our program has attracted 278 applicants who have no background in STEM, which is 56% of all recorded applicants.

4. Retrospective Analysis and Synthetic Review

Designing and implementing a new academic program is similar to running a startup company where there are not any existing procedures to follow or proven approaches to apply. The six guidelines in designing and implementing a new baccalaureate program in digital forensics program introduced in [22] are well summarized what we have encountered and fully reflected through our implementation experience.

4.1 The emphases of the program

Since computer forensics is a multidisciplinary field, the program actually could be constructed with different emphases, such as criminal justice, law enforcement, paralegal, computer science, information technology, or management information systems. As discussed in [13], our program was motivated in having a four-year

program that is not emphasized on programming so that it could be well matched with the need of the students who have earned a two-year degree in network administration, system administration, database administration, and information technology. In other words, our primary goal was to have a four-year program created to complement with our existing programs in computer science and computer information technology that are heavily relied on programming skills. Based on this consideration, our computer forensics program is more emphasizing on the knowledge in system, networking, law, legal issues, civil litigation, and criminal investigation.

As a Bachelor of Applied Science degree, our program primarily serves to the students who have earned a two-year degree. If the scope of the program is very narrow, it is difficult to cover various backgrounds the students have. On the other hand, if the program includes too many subjects, it is unlikely for students to obtain some critical knowledge in depth. Since the goal of the program is to fill the gap between criminal justice and information technology, we have been trying to recognize our students' previous course work as long as it contributes any component of this multidisciplinary field.

4.2 Content of the program

Generally speaking, a new program provides new knowledge so it definitely needs new courses. However, computer forensics is a multidisciplinary field, which means the new subjects are formed largely by overlapping the existing fields. In other words, many new concepts and knowledge can be introduced by updating the existing courses rather than proposing new courses. The burden in introducing many new courses at the initial stage of a new program could not be underestimated. A good balance between existing courses, updated courses, and new courses is critical to a smooth start of a new program. New courses not only create pressure in getting the course proposals written and approved by various committees but also raise the challenge in finding the faculty to teach them. The approach we took was to use as many existing courses as possible and make the number of the new courses at the minimum initially. In addition to emphasizing the knowledge on the foundation, principles, and common legal procedures, we are focusing on constructing the knowledge between criminal justice, law, and information technology. Specifically, our approach was to select 2 to 3 courses as the prerequisites of a new course so that the number of the new courses could be considerably reduced. This not only helped us in minimizing the effort in recruiting new faculty members to teach the new courses, but also reduced the time pressure in proposing new courses. As it is stated in [4] that "start small and incremental progress are the key to success for an innovation."

4.3 Recruitment and retention

Although the quality of a baccalaureate program is commonly echoed by its outstanding curriculum, the success of a program is practically assessed by the number of the students graduated from the program. Moreover, without enough students enrolled in the courses designed for the new program, those courses must be cancelled due to the economical reasons by the universities. In other words, unless a new program could attract enough students to take the courses designed for it, one cannot even think about the number of the students who could eventually graduate from the program. All preparations in the curriculum design and faculty training should focus on the students who are interested enough in taking all needed courses of the new program.

With the dean's guidance as "the new program should not compete the student with our existing programs in Computer Science and Computer Information Technology," we paid our attention mainly on the students who have strong interest in systems,

networking, database administration, criminal justice, and legal technology. In other words, instead of building our computer forensics program on the top of our Computer Science or Computer Information Technology program, we emphasized our new program on the combined knowledge between legal issues and information technology. Since our strategy is fully based on the unique characteristics of the university, it has been proven working very well in attracting a different array of students as shown in previous section in Figure 3.5., as well as complementing the department in graduating more students as indicated in the previous section in Figure 3.3. Our experience taught us that you might not be able to get the students you want but you need to try to keep the students who come to you as many as possible. Therefore, how to keep the students who come to you is relatively more practical than how to attract the students you would like to have. The bottom line is that unless you could keep the students who come to you, the new program could not survive.

4.4 Faculty preparation and evaluation

Since computer forensics has been just developed into a technical field as well as its multidisciplinary nature, it is very challenging for many institutions to recruit faculty members at the PhD level for a baccalaureate program in computer forensics. Although it is possible to train existing faculty members to teach computer forensics courses, it is equally challenging to motivate them to switch from their current interests to the field of computer forensics due to many reasons. Since the theory and practice of the computer forensics is not covered by any traditional computer science or computer engineering sub-fields, the faculty members need to learn the subject from top to bottom all by themselves. This learning process is not only time consuming but also practical difficult due to the lack of the preparation in laws, legal procedures, and investigation technologies. Limited funding and lack of publication opportunity are also the concerns. To cope with those consideration, we have provided those faculty members with the proper arrangement on their teaching loads and favorable consideration on their corresponding research and professional development.

4.5 Laboratories and other resources

Due to the sensitivity of the computer forensic data and the destructive tendency of the digital investigation, a dedicated digital environment is critical to a successful computer forensics program. A Java IDE might be enough for a computer science major to build their applications, a computer forensics major requires a set of tools and a dedicated digital environment before they can conduct the primary tasks in collecting, preserving, analyzing, and presenting digital evidence. Discussed in [6], a 30TB digital evidence corpus has been well studied in evaluating the diversity of digital data, the capacity of the digital data, and the mismatch of the skills in handling the digital data. To setup a dedicated lab requires at least funding and space while obtaining a sufficient lab space is commonly more challenging for many institutions, including us.

4.6 Administration

To run a new program, one has to consider the management part in addition to the consideration in the curriculum design, faculty preparation, student recruitment and advising, and lab equipment and space. The administration responsibility includes the authority of allocation of funding, personnel, and space. Therefore, the author in [22] suggests that the person who administrates a new program should be the chair of the department or at least an associate chair of the department or an independent director. Our experience has well mirrored the suggestion as it was managed by the chair of the department for the first three years of the implementation and proven that the suggestion was practical and critical.

When we looked back the years we had run our program, one of the biggest challenges we have been facing is the uncertainty. There were many times we had no clue how to solve the problems and felt helpless and would like to drop the ball. We managed to pass them by finding a workable solution or the problems were simply dismissed as the time passed. We have been very grateful for our students, faculty, administration, and the university's community for their consistent support and trust.

5. Accreditation Consideration and Autonomy Concern

Instead of education for the enrichment of the life, more academic programs are asked to focus on learning outcome assessment and the job placement potentials. Computer forensics program is no exception.

As the accreditation body of the forensic science, Forensic Science Education Programs Accreditation Commission (<http://fepac-edu.org/>) has classified digital forensics as “Digital and Multimedia Sciences” as its one of eleven sub-disciplines. Out of all 34 accredited programs (updated by March 4, 2016), only the Master of Forensic Science Degree program offered at Marshall University in West Virginia is emphasizing in digital evidence.

While there is no sub-discipline in computer science for computer forensics, a government effort has been made in defining the common knowledge and skills in Digital Forensics with respect of the practitioners, which is Center for Digital Forensics and Academic Excellence (CDDFAE, <http://www.dc3.mil/cddfae>), a national program in promoting digital forensics education.

Figure 5.1 The steps of the application for CDDFAE (by courtesy of DC3)

Established in 2012, the CDDFAE is an NSA certified center program and operated by Defense Cyber Crime Center (DC3) at the Air Force Office of Special Investigations. As stated at its website, the goal of the program is to “develop a partnership between academia and the government to establish standards and best practices for digital forensics practitioners, educators, and researchers to advance the discipline of digital forensics and increase the number of qualified professionals in the law enforcement, counterintelligence, national defense, and legal communities.” Indicated in Figure 5.1, any two or four-year institutions are qualified to apply for the CDDFAE designation. The application starts with mapping the course objectives to the learning outcomes/objectives of eight knowledge domains defined by the CDDFAE. Those eight knowledge domains are 1) Legal and Ethics; 2) Investigative Processes; 3) Storage Media; 4) Mobile and Embedded Devices; 5) Network Forensics; 6) Program and Software Forensics; 7) Quality Assurance, Control and Management; 8) Lab and Forensic Operation, and their learning outcomes/objectives are categorized into four different levels, where Level 100 and 200 target the CDDFAE’s Cyber Incident Responder (CIR) Certification and level 300 and 400 aim to the CDDFAE’s Digital Forensic Examiner (DFE) Certification. Supported by the DCITA, Defense Cyber Investigation Training

Academy, the CDDFAE’s CIR is recognized as the DCITA’s Digital Media Collector (DMC) certification and the CDDFAE’s DFE is accepted as the DCITA’s Digital Forensic Examiner Certification. Institutions do not require having an existing or a potential program in computer/digital forensics before applying the designation and will be designated as long as the curriculum matches the CDDFAE guidelines. Currently two out of eight the CDDFAE currently designated 4-year institutions are offering a four-year program in computer/digital forensics (last checked on July 31, 2016 at www.dc3.mil) and both are private colleges.

Led by the National Institute of Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE at <http://csrc.nist.gov/nice/>) has drafted the cybersecurity workforce framework based on a comprehensive and taxonomic analysis of cybersecurity jobs. There are 8 categories and 34 specialty areas are classified by NICE, where “Digital Forensics” is listed as one of the two specialty areas under the category of “Investigate” along with “Cyber Investigation” as another specialty area. As shown in Table 5.1, there are two work roles within “Digital Forensics” and each is further defined with the critical tasks specified and the desirable KSAs (Knowledge, Skills, and Abilities) required for performing the work roles.

Table 5.1 Work Roles for Specialty Area of “Digital Forensics” (NICE)

Work Role	# of Tasks	# of KSAs
Forensics Analyst	33	61
Cyber Defense Forensics Analyst	39	69

Although Digital Forensics is not classified as an individual category in NICE’s framework, the details of the tasks and KSAs associated with Digital Forensics summarized by NICE provide us a tremendous resource in understanding the field from an employer’s point of view and will have a significant impact in improving Digital Forensics education as well as the accreditation.

It has been a common effort in pursuing an accreditation for a newly established program. However, computer forensics is an emerging multidisciplinary field with various changing factors so that we must consider the balance in maintaining flexibility and pursuing standardization. As the new technology and cyber environment advances with the big data and internet of things [20] joining the stage, more significant changes and updates are expected in the field. While the five aspects of “creative destruction” introduced in [18] as 1) new technology; 2) new product; 3) new materials; 4) new market; and 5) new organization, we can find something accordingly in education as 1) new online resources; 2) new programs; 3) new characteristics of next generation of students; 4) new job markets; and 5) the new forms of higher education. We might not be able to see the changes now but changes are expected and coming. A flexible position in running a program in an emerging field will be more applicable for us to adapt the new changes.

6. Conclusion and Future Plan

The technology has kept advancing since the turn of the century, the field of computer forensics has been changed dramatically. As the focuses of the primary investigations are shifted from desktop stations to mobile devices, local networks to remote clouds, and digital forensics to electronic discovery [28], computer forensics curriculum should be updated accordingly and timely. According to the study in [17], the IT related courses takes about 56% in our program comparing 70% from programs offered by other four public institutions. Along with two new courses in eDiscovery included in our program, we are planning to have two more new courses in “Mobile Forensics and Security” and “Privacy Protection and Technology” added to the program in the near future so that the

percentage of IT related courses in our program could catch up with the other programs in the country.

There is an old Chinese idiom that says “it takes a decade to forge a sword,” which might not be the reality but the commitment and persistence implied by it is vital for any innovation at any time. For instance, it took ten years for Robert Metcalfe to transfer the Ethernet from an innovative idea in 1973 to an international standard, IEEE 802.3, in 1983 [4]. Although running an innovative program in computer forensics is not as big as a world-shaker and does not require the work of geniuses, its impact on those 177 graduated students with their careers, families and community cannot be underestimated. Our ten-year experience in running an innovative baccalaureate program in computer forensics has helped us to realize that we have been on the right direction in helping our students as well as the university in meeting the needs of the society. After the implementation of the program for ten years, we believe our program has matured and will grow to serve more students in the next ten years. We also hope that our experience and lessons presented here could be beneficial to those who are currently running, developing, or planning to propose a similar or different innovative program for their students. As stated by Professor Peter Denning, a well-known computer science educator and researcher, “innovation is no ugly weed. Like a big garden of small flowers, innovation is beautiful [4].” Computer Forensics is not going to be a primary degree program like Computer Science or Computer Information Technology, but it is an innovative program that has diversified the IT field and made its unique contribution to our modern society.

ACKNOWLEDGMENT

The author gratefully acknowledges partial supports of this research by both National Science Foundation grant DGE-1500055 and Metropolitan State University faculty research grant for summer 2015.

REFERENCES

- [1] AAFS, “What is Forensic Science,” last accessed on March 20, 2016, at <http://www.aafs.org/students/choosing-a-career/what-is-forensic-science/>
- [2] Cisco Systems, “Economic Impact of Network Security Threats,” white paper, last accessed on April 26, 2016, at http://graziadiovoice.pepperdine.edu/wp-content/uploads/2010/10/roi1_wp.pdf
- [3] Dardick, G. S. and Lau, L. K., “Interdisciplinary Minor in Digital Forensics, Security and Law,” SIGITE’05, Newark, New Jersey, USA, October 20–22, 2005
- [4] Denning, P. J., “How to Produce Innovations,” Communications of the ACM, Vol. 59, No. 8, June, 2016, pp28 - 30
- [5] Figg, W. and Zhou, Z., “A Computer Forensics Minor Curriculum Proposal,” Journal of Computing Sciences in Colleges, Volume 22 Issue 4, April 2007.
- [6] Garfinkel, S., “Lessons learned writing digital forensics tools and managing a 30TB digital evidence corpus,” Journal of Digital Investigation, Vol. 9, 2012, pp80 - 89.
- [7] Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., and Stein, M., “Computer Forensics Programs in Higher Education: A Preliminary Study,” the proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education, St. Louis, Missouri, USA, Feb. 23-27, 2005, pp147 - 151
- [8] Goodison, S. E., Davis, R. C., and Jackson, B. A., “Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence,” last accessed June 21, 2016 at <https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf>
- [9] Gunsch, G. H., “The Defiance College Undergraduate Major in Digital Forensic Science: Setting the Bar Higher,” the proceedings of the ADFSL 2010 International Conference on Digital Forensics, Security and Law, St. Paul, MN, May 10 – 12, 2010, pp131-140
- [10] Hankins, R., Uehara, T. and Liu, J., “A Comparative Study of Forensic Science and Computer Forensics,” in the proceedings of the 3rd IEEE International Conference on Secure Software Integration and Reliability Improvement,” Shanghai, China, July 8-10, 2009, pp230 - 239
- [11] Kessler, G. C. and Schirling, M. E., “The Design of an Undergraduate Degree Program in Computer & Digital Forensics,” the Journal of Digital Forensics, Security and Law, 1(3), 2006, pp37 - 50
- [12] Lang, A., Bashir, M., Campbell, R., and DeStefano, L., “Developing a New Digital Forensics Curriculum,” Digital Investigation 11 (2014), pp76 - 84
- [13] Liu, J., “Developing an Innovative Baccalaureate Program in Computer Forensics,” the proceedings of the 36th ASEE/IEEE Frontiers in Education Conference (FIE2006), San Diego, CA, Oct. 28 – 31, 2006, pp1 - 6
- [14] Liu, J., Gottschalk, L., Jian, K., “Textbooks for Computer Forensic Courses: A Preliminary Study,” the proceedings of ADFSL 2007 Annual Conference on Digital Forensics, Security, and Law, Arlington, Virginia, USA, April 18-20, 2007, pp 141 - 146
- [15] Liu, J., “Implementing a Baccalaureate Program in Computer Forensics,” the Journal of Computing Sciences in Colleges, Vol. 25, No. 3, January, 2010, pp 101-109
- [16] Liu, J., “An Analysis of the students’ academic background in a computer forensics program,” the Journal of Computing Sciences in Colleges, Volume 28, Issue 2, Dec., 2012, pp 32 - 39
- [17] Liu, J., “Baccalaureate Programs in Computer Forensics,” the proceedings of the 2016 IEEE International Conference on Electro/Information Technology, Grand Forks, North Dakota, May 19 to 21, 2016, pp 615 - 620
- [18] McCraw, T. K., “Prophet of Innovation: Joseph Schumpeter and Creative Destruction,” Harvard University Press, 719 pages, March 2010, ISBN 9780674034815
- [19] National Science Foundation, *Federal Cyber Service: Scholarship for Service (SFS)*, NSF 12-531, 2012
- [20] Oriwih, E., Jazani, D., Epiphaniou, G., and Sant, P., “Internet of Things Forensics: Challenges and Approaches,” the proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Work-sharing, 2013
- [21] Pollitt, M. M., “Who is SWGDE and what is the history?” last accessed on April 27, 2016 at <https://www.swgde.org/pdf/2003-01-22%20SWGDE%20History.pdf>
- [22] Riley, Jr. J. H., “Developing a Baccalaureate Digital Forensics Major,” the proceedings of the ADFSL 2010 International Conference on Digital Forensics, Security and Law, St. Paul, MN, May 10 – 12, 2010, pp123 - 130
- [23] Rhodes, K. A., “‘ILOVEYOU’ Computer Virus Emphasizes Critical Need for Agency and Government-wide Improvements,” Testimony before the Subcommittee on Technology, Committee on Science, House of Representatives, United States General Accounting Office, May 10, 2000
- [24] Scientific Working Group on Digital Evidence, last accessed on April 24, 2016 at <https://www.swgde.org>
- [25] Troell, L., Pan, Y., and Stackpole, W., “Forensic Course Development,” Proceeding of the 4th conference on Information technology Curriculum, Lafayette, IN, USA, October 16-18, 2003
- [26] Troell, L., Pan, Y., and Stackpole, W., “Forensic Course Development – One Year Later,” SIGITE’04, Salt Lake City, Utah, USA, October 28–30, 2004
- [27] US-CERT, “Computer Forensics,” last accessed on June 21, 2016 at http://www.us-cert.gov/reading_room/forensics.pdf
- [28] U.S. Supreme Court, *Amendment to the Federal Rules of Civil Procedure*, April 12, 2006, last accessed on June 21, 2016 at <http://www.supremecourt.gov/orders/courtorders/frcv06p.pdf>
- [29] Whitcomb, C. M., “The Evolution of Digital Evidence in Forensic Science Laboratories,” The Police Chief,” vol.74 no 11, November 2007
- [30] Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., and Sommer, P. M., “Computer Forensics Education,” IEEE Security and Privacy, The IEEE Computer Society, July/August 2003, pp15 - 23