Development of a Graduate Certificate Program in Computer Forensics

Alfredo Cruz, PhD

Polytechnic University of Puerto Rico, Hato Rey, PR, alcruz@pupr.edu

Jeff Duffany, PhD

Universidad del Turabo, Gurabo, PR, jeduffany@suagm.edu

ABSTRACT

The Graduate School at the Polytechnic University of Puerto Rico (PUPR) proposes the creation of a Graduate Certificate Program in Computer Forensics (GCCF). The Certificate is primarily for students who are pursuing a Master Degree in Computer Science and Computer Engineering or who are working in the area of Information Technology (IT) and wish to broaden their skills and knowledge base in computer forensics. The GCCF will be the first in Puerto Rico; and a great opportunity for local and federal employees, as well as the private sector. The primary goal of the Graduate Certificate in Computer Forensics is to help meet the current and future needs of local and national industry and government by providing a talent pool of professionals with expertise in the areas of computer forensics and information assurance. With the Certificate there is no doubt that PUPR will strengthen their role as a Center for Academic Excellence in Information Assurance Education (CAE/IAE). The main goal of the Center of Information Assurance for Research and Education (CIARE) at PUPR is to develop Information Assurance (IA) professionals in areas that are important to national security.

Keywords: CAE/IAE, Information Assurance, Computer Forensics, GPU, Cyber-security

1. INTRODUCTION

The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information. Because technology changes rapidly, computer specialists must continue to acquire the latest skills (Casey, 2011; Farmer, 2005; Kruse & Heiser, 2001). IA professionals can enhance their skills and employment opportunities by earning certifications, which are offered through academic institutions, product vendors, computer associations, and other training institutions. Many organizations offer intermediate and advanced certification programs that pertain to the most recent technological advancements. The GCCF prepares IT professionals to master critical capabilities such as advanced digital investigative techniques and state-of-the-art computer forensics technologies.

2. PROGRAM JUSTIFICATION

As society at large becomes more dependent on technology, the vulnerability to data-driven theft and corruption is greater than ever. We operate in a world where cyber criminals constantly invent sophisticated techniques to threaten and defeat the security of organizations; making it important to track threats as they change and evolve. Organizations need to be informed and prepared to minimize current risks and increase their capacity to recover from incidents that threaten and affect information assets.

Through formal education and certified training, organizations and Information Assurance (IA) professionals have the opportunity to learn about the many options for improving the cyber protection of intellectual property, and the recovery of customer data, services, and critical infrastructures; as well as the development of new computer

forensics tools and practices.

PUPR was designated a National Center of Academic Excellence in Information Assurance Education (CAE/IAE) by the National Security Agency and Department of Homeland Security (NSA/DHS) in June, 2009. PUPR is proud to be the first CAE/IAE in Puerto Rico. With the Certificate there is no doubt that PUPR will strengthen their role as a Center for Academic Excellence in Information Assurance Education (CAE/IAE). The main goal of the Center of Information Assurance for Research and Education (CIARE) at PUPR is to develop IA professionals in areas that are important to national security.

2.1 STUDENT SURVEY

The study included an internal survey questionnaire administered to eighty one (81) students at Polytechnic University of Hato Rey. The questionnaire was administered at random to Electrical Engineering, Computer Engineering and Computer Science students enrolled in Baccalaureate and Master degree studies. It contained a total of eighteen (18) questions that revealed the student's personal profile (sex, age, academic status, work status, income, etc.); included a series of questions about their work experience or knowledge on Computer Forensics (CF) and Information Assurance (IA); and their interest in the area. Student data is obtained from the sample on: gender, age, academic and employment status, last degree obtained, years of work experience, current program enrollment, exposure and or interest in the field, and others. The student survey was done to measure the acceptance of the GCCF in the campus among students, and to obtain a profile of the students that are actually studying at Polytechnic University, in related areas. The purpose of the survey was to conclude if students who were enrolled in related Bachelors' or Masters' programs at the PUPR were interested in obtaining skills in computer forensics and information assurance by enrolling in the Graduate Certificate in Computer Forensics (GCCF) to complement an undergraduate degree or graduate studies.

Certifications have become very important for IT professionals as the need to up-date their knowledge and skills is constantly required. In the survey, students were asked if they were interested in enhancing their IT professional skills with certificate programs that are in great demand. A total of 92.59% of the students surveyed were interested in enhancing professional skills with certifications in IT. By genre, 69.23% of female and 97.06% of male students showed interest (see Figure 1).

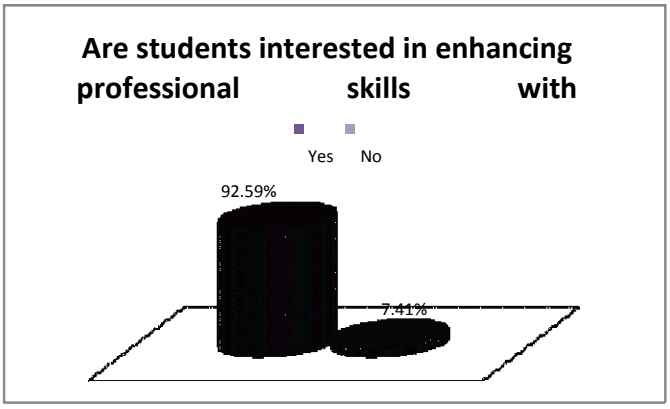

Figure 1. Percentage of Students Interviewed Interested in Enhancing Their Professional Skills With Certifications

In Figure 2, we can observe that a very significant percentage of the students interviewed (93.83%) consider information assurance and computer forensics important IT issues (69.23% of the females and 98.53% of male students).

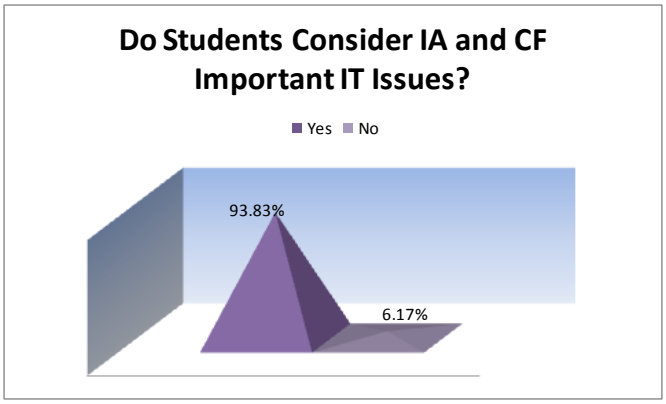

Figure 2. Percentage of Students Interviewed that Consider IA and CF Important IT Issues.

Almost 77% of the females interviewed as well as 85.29% percent of the males consider that obtaining additional skills in Computer Forensics and Information Assurance will help them excel in their careers. This represents almost 84% of the students interviewed, as can be observed in Figure 3 below.

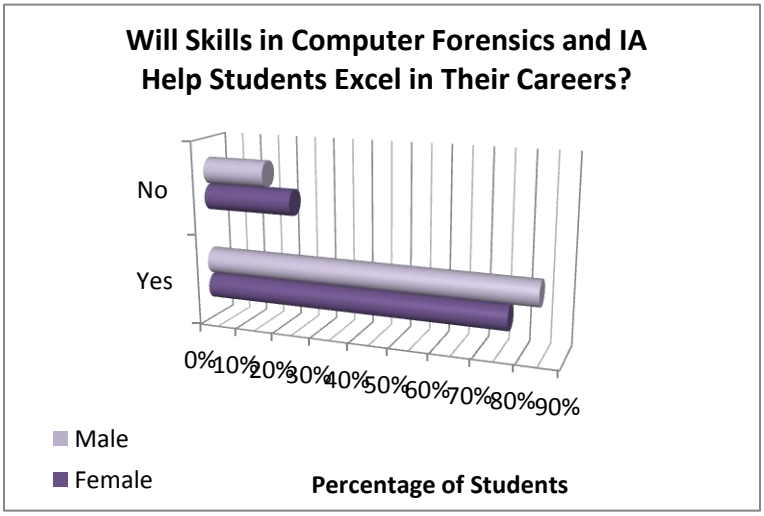

Figure 3. Percentage of Students that Consider Skills in Computer Forensics and IA Will Help Them Excel in Their Careers (by gender)

2.2 BUREAU OF LABOR STATISTICS (BLS) OCCUPATIONAL OUTLOOK

According to the U.S. BLS, the IT security workforce had an increase of 27 percent in six months this year (2011). According to the government statistics, the number of IT security analysts is steadily growing, but not as fast as employers want. This need arises from a variety of sources including industry, government, law enforcement, FBI, and Secret Service.

Salaries and Growth Outlook for some of the IT careers that require knowledge in Computer Forensics (Yansisac, 2003) and Information Security are listed below in Table 1, as reported by the BLS and the 2011 Occupational Outlook for 2010-18. All require at least a Bachelors Degree in related areas:

Table 1. Expected Growth and Salaries for IA Occupations 2010-2018

Occupation	Percentage of Growth	Salaries
Security Architect	+23.23%	$115,000
Security Engineer	+23.23%	$110,000
Infrastructure Architect	+13.14%	$110,000
Network Security Engineer	+23.23%	$103,210
Infrastructure Engineer	+13.14%	$98,800
Telecommunications Engineer	+53.36%	$82,000
Infrastructure Manager	+16.90%	$80,000
Network Analyst	+53.36%	$72,000
Software Quality Assurance Analyst	+13.14%	$70,000
Infrastructure Analyst	+20.31%	$66,000
Firewall Engineer	+23.23%	$65,000
Software Quality Assurance Tester	+13.14%	$65,000
Telecommunications Analyst	+53.36%	$65,000
Server Manager	+23.23%	$62,920
Telecom Analyst	+53.36%	$62,400
Server Administrator	+23.23%	$60,000
Telecommunications Specialist	+53.36%	$55,000

(Sources: Career Igniter 2011; BLS Occupational Outlook 2010-18)

Due to this progressive growth, there is an urgent need to supply the demand for IA professionals at the local and national level. Currently there is no Certificate in Computer Forensics at any other institution in Puerto Rico, creating a great opportunity to strengthen the local workforce and capacitate faculty and students from PUPR and other universities.

As stated by the BLS: "The demand for increasing efficiency in areas such as networking technology, computing speeds, software performance, and embedded systems will lead to employment growth. In addition, the growing emphasis on information security will lead to new jobs." Another significant fact is that many occupations associated to IA and Computer Forensics such as Information Security Analysts and others have an unemployment rate of zero percent. Eric Chabrow, Executive Editor of GovInfoSecurity.com shares this information in the article written on July 9, 2011: "Infosec Joblessness Remains Steady, at 0%". It acknowledges that none of the Information Security Analysts interviewed by the BLS in the United States were out of a job!

Even though the sample size was too small to be completely considered statistically reliable, the government numbers strongly suggests a critical shortage of skilled IT security personnel. There is an urgent need for more professionals with skills and knowledge in the area of IA and Computer Forensics in IT and Computer Science related positions.

There is also an urgent need to promote information security skills among women, minorities, and other underrepresented groups. As stated by Eric Chabrow, Executive Editor, GovInfoSecurity.com in his article "Women, Minorities Scarce in IT Security Field Profession Does Not Mirror Rest of American Workforce" (October 11, 2011): "Despite virtually no unemployment among IT security pros, the scarcity of women, African Americans, Latinos and women is highly evident." Information reported by the U.S. Bureau of Labor and Statistics (BLS) in 2011 states "Whites make up 70 percent of the IT security workforce. Latinos make up about 5 percent of the IT security labor force and women also are underrepresented in the IT security workforce

representing about 8 percent".

We recognize that minority serving colleges are a prime resource for IT professionals in the area of Networking and Systems Security, and Forensics. According to Dr. Ricardo Fernandez's written testimony for submission to the Record on H.R. 2183 and H.R. 2272: the Minority-Serving Institution Digital and Wireless Network Technology Opportunity Act of 2003, "HSIs and other Minority-Serving Institutions have the expertise, proximity, and commitment to their students and communities to provide front-line leadership and support in the effort to close the information gap. However, these institutions cannot succeed without the support of Congress and its endorsement of a substantial investment in federal dollars."

There is an urgent need for academia, the government, and private industries to promote academic programs and certificates in IA such as the GCCF, for underrepresented groups.

3. GCCF CURRICULUM, GRADUATE PROFILE AND FACULTY

3.1 CURRICULUM

The program will provide an in-depth introduction to key topics of computer forensics and provides a balanced teaching philosophy that contains both theory and hands-on practice. To complete the certificate program the student must take a total of 5 graduate courses of three (3) credits each:

1. Computer Security
2. Network Security
3. Computer Forensics
4. Advanced Computer Forensics
5. Law, Investigation, and Ethics

3.1.1 COURSE DESCRIPTIONS

CECS 7570 Computer Security. Three (3) credit hours
The fundamental tools and techniques for computer security are discussed in the context of the pervasive role and impact that computer technology has over the individual, the enterprise and on society-at-large. Topics include confidentiality, integrity, availability, computer viruses, operating systems, program and database security.

CECS 7230 Network Security. Three (3) credit hours
Major topics covered are symmetric encryption (DES and AES), public key encryption (RSA and Diffie-Hellman), message authentication and hash functions. A general introduction to number theory, prime numbers and discrete logarithms is provided as mathematical background. The course concludes by illustrating these techniques in network security applications including electronic mail, IP security, wireless and web security.

CECS 7235 Computer Forensics. Three (3) Credits
This course is an introduction to digital forensics in the context of the Microsoft windows operating system. Overview of evidence collection and archiving, order of volatility (RFC 3227) and Locard's Exchange Principle. Preservation of volatile and non-volatile data. Analysis of data including windows memory and registry analysis, log file and executable file analysis. The course will use case studies and open source tools.

CECS 7237 Advanced Computer Forensics. Three (3) Credits. Prerequisites: CECS 7235 Computer Forensics
Advanced topics in computer forensics concerned mainly with file system forensics. Hard drives, USB drives, removable media, CD-ROMs and flash drives. Accessing data from cell phones and PDA's. Recovery of deleted data from DOS, NTFS, MAC, and other widely used file systems. Data carving techniques. Case studies and open source tools.

CECS 6045 Law, Investigation, and Ethics. Three (3) Credits
This course is intended for students of computer science and other related fields of study who are interested in the IT social and ethical issues that arise from computationally intense environments in the workplace and in society. It addresses computer crime laws and regulations, the measures and technologies used to investigate computer crime incidents and the ethics involved in the use of computers, information systems and technology. Controversies and alternate points of view are addressed on social, legal, philosophical, political, constitutional and economic issues related to computers.

Through this certificate, participants gain vital insight into obtaining and documenting digital information, determining the source of information compromises and delivering expert testimony concerning digital crime related to data in computers, networks and hand-held devices. In addition, the program addresses recovery of corrupted, encrypted and hidden information, providing a comprehensive preparation for assisting in the prevention and prosecution of malicious information theft and other criminal activity.

These are the skills that PUPR wants to offer graduate students in the Graduate Certificate in Computer Forensics (GCCF) that will benefit both faculty and students.

3.2 GRADUATE PROFILE

Individuals who complete the program will have a thorough understanding of Computer Forensics principles which they will be able to apply to a wide variety of situations in management, technical areas, or research and development. If the student specializes in providing evidence of computer crimes to law-enforcement agencies, then knowing the legalities of search and seizure, and the approved techniques for collecting and preserving evidence will be mandatory (Nelson, 2009; Noblett & et al., 2000; Pfleeger, 2006; Stallings, 2011). Students who complete the certificate are expected to have the following skills:

- Experience in computer/digital forensics
- Proficient with forensic techniques and the most commonly used forensic toolsets, such as dtSearch, EnCase, and FTK Suite
- Familiarity with Windows, Macintosh, and Linux Operating Systems
- Familiarity with computer system hardware and software installation and troubleshooting.
- Experience with programming languages (e.g. Python)
- Thorough understanding of chain of custody procedures, forensic lab practices, and evidence handling
- Preserve, harvest, and process electronic data according to the firm's policies and practices
- Perform digital forensic analysis
- Provide creative and innovative solutions for client matters
- High quality oral and writing skills that can present and document complex technical matters clearly and concisely
- Form and articulate expert opinions based on analysis
- Draft expert reports, affidavits, and other expert testimony
- Provide expert testimony in depositions, trials, and other proceedings
- Consult with (and take direction from) supervisors, engagement managers, and clients regarding case investigation and status

3.3 FACULTY

The program will rely on both Polytechnic University of Puerto Rico faculty plus adjunct faculty, which are knowledgeable in the field of Computer Forensics. Table 2 lists faculty that has been identified for teaching in the Computer Forensics Certificate program. This list will be expanded as additional qualified personnel are identified.

Table 2. Faculty Available for the Graduate Certificate in Computer Forensics

Name	Degree
Dr. Jeffrey L. Duffany CISSP, MSCE, MCSA,CEH	Ph.D. Computer and Information Engineering
Dr. Juan Sola	PhD Computer Information Science and Engineering
Dr. Alfredo Cruz	PhD Computer Engineering PhD Computer Information System
Fernando Cervoni, Esq.	Juris Doctor (JD)
Dr. Juan Torres	PhD Electrical and Computer Engineering

4. FACILITIES FOR GCCF STUDENTS

PUPR has modern equipment for research and education currently available for students from the Graduate School and undergraduate Electrical & Computer Engineering and Computer Science (ECECS) Department programs. These laboratories have been established in the last six years with grants from the DoD, NSF, NSA, DHS, DE, and PRIDCO. Some are used for classroom activities and others for graduate research and studying. The established laboratories are:

- The Data Communication Laboratory and Advanced Network Laboratory
- The High Performance Computing Laboratory (HPC) that includes three PC Clusters and an Altix 350 Supercomputer
- The Windows to the Caribbean Laboratory
- The Turing Laboratory for Graduate Studies
- The Cyber Information Assurance Wireless Lab (CIAW)
- The Cyber Digital Forensics Investigation Laboratory (CDFIL)

All the mentioned laboratories also support research in other basic sciences requiring sophisticated computing facilities. These resources are key components in PUPR's goal to provide IA students and faculty with state-of-the-art infrastructure for their academic endeavors in research and education.

The Cyber Digital Forensics Investigation Laboratory (CDFIL) is used for analyzing financial frauds, telecommunication frauds, cyber crime, and terrorism investigation, among other activities. This laboratory will encourage other institutions to adopt similar models that provide high quality training and further increase the available supply of practitioners prepared in this critical discipline. The laboratory provides real and simulated analysis by gathering digital evidence from computer systems using legally established procedures of computer forensic science. The activities done include: ensuring evidence is not altered, impacting learning of how investigations in forensically sterile environments can be conducted, documenting chains of custody, and logging investigative actions. In addition, this equipment stimulates students to develop new research in computer forensic science.

Polytechnic University of Puerto Rico, through various grants for over $150,000.00 from the DOD, DHS, DE, and NSA increased their infrastructure in computer forensics by establishing the Cyber Digital Forensics Investigation Laboratory (CDFIL). We host two FRED SC (Super Computer) at the CDFIL facilities. The FRED

SC is the first commercially available Super Computer designed and optimized for parallel processing with four NVIDIA® CUDA™ Graphic's Processing Units (GPU's). The FRED-SC system has four liquid cooled NVIDIA GTX480 Video cards (each with one onboard GPU consisting of 480 stream processors per GPU). A total of 1,920 CUDA processors are available on this system for massive parallel processing and computation.

Figure 4. The FRED Super Computer

The Compute Unified Device Architecture (CUDA) is particularly useful to the forensic community for brute force password cracking. This specialized platform is capable of about 4.769 TeraFlops of performance (4,769 GigaFlops). The technology leverages the massive parallel processing power of GPUs. The CUDA architecture is a revolutionary parallel computing architecture that delivers the performance of graphics processor technology to general purpose GPU Computing. Applications that run on the CUDA architecture can take advantage of an installed base of over one hundred million CUDA-enabled GPUs in desktop and notebook computers, professional workstations, and supercomputer clusters.

With the CUDA architecture and tools, developers are currently achieving dramatic speedups in fields such as medical imaging and natural resource exploration, and creating breakthrough applications in areas such as image recognition and real-time HD video playback and encoding.

Currently there are 12 FRED (Forensic Recovery of Evidence Device) in the CDFIL, and it is planned to add 6 more micro FRED devices which would bring the total to 18. Therefore the laboratory will be able to accommodate up to 18 students. There are no equipment limitations for the other classes. The low ratio of students to equipment will ensure a quality educational experience which is designed to fully integrate the classroom and laboratory to maximize the individual learning experience. The curriculum and the laboratory were simultaneously co-designed so that classroom teaching and lab experiments would be coordinated.

5. CONCLUSIONS

In the survey a very good percent of the students revealed their interest in continuing additional certificate studies and strongly consider the GCCF as a promising means for obtaining additional know-how and technical skills in IA and Computer Forensics (CF) that could significantly enhance their IT careers. Graduate and undergraduate students surveyed acknowledge that IA and Computer Forensics are fields of great demand in today's workplace in both industry and government. An overall interest was observed in obtaining IA and CF skills, recognizing that these skills will give them a competitive edge in their fields of study (which are of great demand). The study clearly reflects that PUPR students acknowledge the importance and have the intention of obtaining additional certification and skills. Student awareness of the need for these skills in the workplace was noticeable among the sample interviewed. We are completely convinced of the success and the benefits that this certificate could

represent to students and faculty throughout Puerto Rico and the Caribbean. These findings reassure us that the GCCF certificate program will be a success and another important asset to PUPR as a Center for Information Assurance Research and Education of Puerto Rico. We are actually the first and only CAE/IAE in Puerto Rico and the Caribbean as of this moment.

The GCCF is anticipated to attract people from local and national law enforcement agencies who need the background in this area to enhance their job skills and overall performance. The certificate is intended to provide exposure to current problems in a rapidly changing field and to encourage participants to experiment and learn firsthand innovative ideas and approaches.

6. ACKNOWLEDGMENTS

This work was supported by the DoD AFOSR under the grant # W911NF-11-1-0174. The authors also thank Mr. Alexander Lopez, Administrative Assistant for this grant, for his dedication and work in the development of the proposal for the Graduate Certificate in Computer Forensics.

REFERENCES

Casey, E. (2011). *Digital Evidence and Computer Crime*, 3rd edition, Academic Press, ISBN 0-12-374268-4.

Farmer, D. and Venema, W. (2005). *Forensic Discovery*, Addison-Wesley Professional, ISBN 0-32-170325-1.

Kruse, W.G. and Heiser, J.G. (2001). *Computer Forensics: Incident Response Essentials*, Pearson Education, ISBN 0-20-170719-5.

Nelson, B. (2009). *Guide to Computer Forensics and Investigations*, Thomson Course Technology, ISBN 1-43-549883-6.

Noblett, M.G., Pollitt, M.M., and Presley, L.A. (2000). "Recovering and Examining Computer Forensic Evidence", *Forensic Science Communications*, Vol. 2, No. 4.

Pfleeger, C. (2006). *Security in Computing*, 4th edition, Prentice Hall, ISBN 0-13-2390779.

Stallings, W. (2011). *Cryptography and Network Security*, 5th edition, Prentice Hall, ISBN 0-13-609704-9.

Yasinsac, A., Erbacher, R.F., Marks, D.G., and Pollitt, M.M. (2003). "Computer Forensics Education". *IEEE Security & Privacy*, Vol. 03.

Authorization and Disclaimer

Authors authorize LACCEI to publish the paper in the conference proceedings. Neither LACCEI nor the editors are responsible either for the content or for the implications of what is expressed in the paper.