Communications of the Association for Information Systems

Volume 23 Paper

11-2008

# Escaping the Computer-Forensics Certification Maze: A Survey of Professional Certifications

Nena Lim
*Swedish Business School, Örebro University*, nenalim@yahoo.com

Follow this and additional works at: https://aisel.aisnet.org/cais

Recommended Citation
Lim, N. (2008). Escaping the Computer-Forensics Certification Maze: A Survey of Professional Certifications. Communications of the Association for Information Systems, 23, pp-pp. https://doi.org/10.17705/1CAIS.02329

This material is brought to you by the AIS Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in Communications of the Association for Information Systems by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Communications of the Association for Information Systems

CAIS

# Escaping the Computer-Forensics Certification Maze: A Survey of Professional Certifications

Nena Lim

*Swedish Business School, Örebro University*

*nena.lim@oru.se*

Abstract:

With the proliferation of computer crime, the demand for computer-forensics experts continues to increase. Yet with so many computer-forensics certifications currently available, it is not an easy task for those outside the discipline to understand the differences among the various certifications. The objective of this paper is to provide a comprehensive analysis of all the existing computer-forensics certifications for the benefits of non-computer-forensics practitioners. Twenty-six computer-forensics certifications offered by 17 different associations are described and compared based on criteria such as certification requirements and knowledge coverage. The paper is useful to three groups of readers: (1) individuals who want to join the computer-forensics profession; (2) academics who are responsible for curriculum development in computer forensics; and (3) top-level managers who want to recruit computer-forensics professionals.

**Keywords**: practice, secondary source, computer forensics

Volume 23, Article 30, pp. 547- 574, November 2008

## I. INTRODUCTION

John is the owner and managing director of a medium-sized company. Someone broke into his company's IT security system and accessed information from several databases two days ago. It is unclear who was responsible for the attack but credit card information of at least 1,000 customers was stolen. John needs to look for a computer-forensics expert to investigate the incident urgently because the police were busy with other more serious computer crimes and none of his existing staff have any experience in computer crime investigation. The director of human resources gave John a list of potential candidates. John read the resumes of the candidates and immediately realized that he has a problem. All potential candidates have one or more computer-forensics certifications under their belts. But neither he nor the company's security manager knows anything about those certifications. Which candidate should he select to investigate the incident? What does it mean for someone to have a computer-forensics certification such as CCCI or CCFT? Is a CCE more knowledgeable or more experienced than a CIFI? What about CSFA, CFCE, CHFI, EnCE or GCFA?[1] If you were John and needed to select a qualified computer-forensics expert for internal investigations, how would you know which one to choose?

With the proliferation of computer crime and limited resources of the police, more organizations need to recruit security professionals to protect company resources and forensic investigators to conduct internal investigations [Casey 2006; Rogers and Seigfried 2004; Sinangin 2002]. The need for organizations to produce reliable computer evidence should not be underestimated [Kent and Ghavalas 2005]. Yet it is not an easy task for people who want to hire a security/computer-forensics specialist or those who want to join the profession to understand the differences among the various certifications and choose one that suits their needs. While information on security certification is available [Danielyan 2003], such certification information is missing in computer forensics. Outsiders of the computer-forensics discipline, such as company managers or general information systems professionals, often have the following questions:

- What computer-forensics certifications are available in the market?
- What organizations offer computer-forensics certifications?
- What are the requirements of each computer-forensics certification?
- What are the strengths and limitations of each computer-forensics certification?
- Which computer-forensics certifications are trustworthy?
- Which computer-forensics certifications are recognized and accepted by the profession?

The objective of the article is to provide outsiders of the computer-forensics profession a comprehensive analysis of all the certifications in the discipline by addressing the above first four questions. It highlights the diversity of the computer-forensics certification market and provides a comprehensive discussion of computer-forensics certifications currently available. A list of 26 computer-forensics certifications together with their certification requirements are discussed and compared. The information is useful to three groups of readers. The first group is prospective certification applicants, such as information systems professionals, who are interested in pursuing a career in computer forensics. Understanding the knowledge coverage and requirements of each computer-forensics certification will help prospective applicants select certifications that suit their background and experience. The second group is academics responsible for developing curriculum in computer forensics in tertiary institutions. Using information in this paper, they can now develop curricula that prepare students for one or more of the certifications. The third group is top-level managers who need to recruit computer-forensics experts but have problems identifying and appointing appropriate people for particular circumstances. This is the scenario depicted in the opening paragraph.

The remainder of this paper is organized as follows: Section II defines computer forensics and explains its relation with other related disciplines. Section III discusses the importance of having certification in the computer-forensics discipline and the limited literature in this area. Section IV presents a comprehensive discussion of all computer-forensics certifications that are open to the general public. Section V summarizes and compares various certifications based on certification requirements, knowledge areas of certification, examination format, duration of certification, and recertification requirements. Section VI describes training courses that target various computer-forensics certifications. It also briefly presents some computer-forensics education programs that are provided by

[1] A glossary is given at the end of this paper.

tertiary institutions. Section VII provides examples of certification in two disciplines that are closely related to computer forensics. Finally, Section VIII concludes the paper and comments on the current computer-forensics certification environment.

## II. COMPUTER FORENSICS AND OTHER RELATED DISCIPLINES

### Computer Forensics

Computer forensics is sometimes also referred as digital forensics, information technology forensics, or data forensics. It is a process of investigation where investigators identify, preserve, analyze, and present digital evidence of various kinds. Digital evidence is "any data stored or transmitted using a computer that support or refute a theory of how an offence occurred or that address critical elements of the offence such as intent or alibi" [Casey 2004 p. 12]. Because digital evidence often is gathered as a result of crime and is often presented in criminal or civil courts, investigators have to make sure the way they handle the evidence is legally acceptable [McKemmish 1999]. Computer forensics started to appear as a discipline in the 1980s when local and national crime units were set up [Mohay et al. 2003]. Because of its connection to crime investigation and computer technologies, computer forensics overlaps other disciplines such as forensic science, forensic accounting, and information security.

### Forensic Science

Forensic science is a field of science that also involves identification, preservation, analysis and presentation of evidence in crime investigation [Lim 2005]. Forensic science and computer forensics overlap because they are both about crime investigation and presenting legally acceptable evidence in courts. However, the focus of forensic science is physical evidence such as fingerprints and DNA and the focus of computer forensics is digital evidence. General investigative principles, such as chain of custody, are the same for both disciplines but the skills and knowledge required are quite different.

### Forensic Accounting

Forensic accounting is sometimes referred to as forensic auditing, investigative accounting, or fraud examination. Forensic-accounting investigators apply knowledge in accounting, auditing, finance, investigative skills, and legal knowledge to investigate, detect, and prevent fraud or other white-collar crime [Albrecht, et al. 2006]. Forensic accounting and computer forensics overlap because they are both about crime investigation. Although fraud and white-collar crime may or may not be committed through the use of computers, with the increasing use of computer technologies, forensic-accounting investigators often need to handle digital evidence in the process of collecting and analyzing evidence in investigation. However, the knowledge scope required for forensic accounting is wider than that of computer forensics. For example, after retrieving deleted e-mails from different sources, forensic-accounting experts who investigated the collapse of Enron had to make use of their knowledge in areas such as accounting and financial management to piece together all the evidence [Anastasi 2003].

### Information Security

Information security is about protecting information assets of organizations. Organization officials have a responsibility to ensure information of all kinds within the organization is protected from unauthorized access [Canavan 2001]. Information security and computer forensics are both important to the survival of organizations. They are essentially two sides of the same coin. Information security experts implement various security measures to protect information systems and data within organizations. When security measures are compromised, computer-forensics experts investigate incidents by retrieving and analyzing digital evidence. The major difference between the two disciplines is that information security focuses on crime prevention but computer forensics focuses on crime investigation. Information security also overlaps with forensic accounting because internal and external auditing is a common security measure.

## III. CERTIFICATION

Certification implies an individual achieves excellence in certain areas of expertise. Certified individuals typically have to pass examinations and fulfill other requirements such as obtaining a certain number of years of experience or complying with professional codes of ethics. The rigorous certification process applicants have to go through is often the reason that the general public has great confidence in certified professionals. Certification is also beneficial to practitioners because it often means higher salary and prestige. A well-recognized certification is often required for job application these days.

Certification is especially important for computer-forensics professionals who often present and are challenged as "expert witnesses" in courts. Testimonies of computer-forensics investigators are more likely to be found admissible in courts if individuals have certification from some recognized association [Jones 2004; Nelson et al. 2005; Solon



Communications of the Association for Information Systems

and Harper 2004]. Unsurprisingly, certification, together with education and training, was found to be the top issue in computer forensics [Rogers and Seigfried 2004]. As the number of computer-forensics certifications proliferates and certification requirements vary, it is difficult for non-practitioners to distinguish among different certifications and identify those that are recognized and accepted by practitioners. The situation in computer forensics is a big contrast to other disciplines such as accounting. When businesses and individuals look for an accounting expert, they typically look for someone with a CPA (Certified Public Accountant) or a CA (Certified Accountant) certification.

Despite the importance of computer-forensics certification, prior literature in this area is limited. Results of a study that compares computer-forensics certification and forensic-science certification show that certification requirements of computer forensics are not as stringent as those of forensic science. Moreover, computer forensics as a whole does not have a clear identity because of the rather confusing certification situation in the industry [Lim 2008]. It is difficult for nonpractitioners to distinguish among different computer-forensics certifications and select one that suits their needs. The problem with the study is that it is biased because it examines only one computer-forensics certification. The objective of this paper is to fill the gap in the literature by providing a comprehensive analysis of all existing computer-forensics certifications according to criteria such as certification requirements and knowledge coverage.

## IV. COMPUTER-FORENSICS CERTIFICATIONS

This section describes 26 certifications offered by 17 professional organizations (Table 1). It covers all existing computer-forensics certifications that are currently open to the public. However, it excludes government agency-specific certifications such as Computer Investigative Specialist (CIS) of Internal Revenue Service (IRS), Computer Analysis Response Team (CART) Forensic Examiner[2] of Federal Bureau of Investigation (FBI), and Electronic Crime Special Agent Program (ECSAP) of United States Secret Service (USSS). These certifications are tied to specific jobs in specific government agencies and inaccessible to the general public. Because the aim of this paper is to facilitate those who want to recruit suitable computer-forensics personnel and those who want to work in the computer-forensics industry, either in the law enforcement or private sectors, these government agency-specific certifications are excluded.

### AccessData - AccessData Certified Examiner (ACE)

URL: http://www.accessdata.com/index.html

AccessData Certified Examiner (ACE) is a vendor-specific computer-forensics certification. Established in 1987, AccessData is one of the pioneers in the computer-forensics discipline. Holders of ACE are certified to be proficient in using four products of AccessData: Forensic Toolkit (FTK), FTK Imager, Password Recovery Toolkit (PRTK), and Registry Viewer.

Because it is a vendor-specific certification, the prerequisite for anyone to obtain the ACE certification is to possess licensed copies of three of the products (FTK Imager is free). There are no educational requirements but applicants need to have at least six months of computer-forensics examination experience. Certification is granted to applicants who meet the experience requirement and pass both phase 1 and phase 2 examinations. Phase 1 examination is an online “knowledge-based assessment.” Applicants need to complete 60 questions within 90 minutes. The passing score of phase 1 examination is 80 percent. Phase 2 examination is a “practical-based assessment.” Applicants need to complete multiple tasks using the AccessData toolkits. Both examinations are closed-book. Certification applicants are expected to take three specific courses provided by AccessData (AccessData BootCamp, FTK 2 Transition, and Windows Forensics–XP) to help them prepare for the assessments. A study guide is also provided to all applicants.

ACE basically focuses only on how to use the FTK tools efficiently in the Windows environment. Because it is a ‘tool-centric’ certification, this certification does not cover topics such as legal issues or general investigation guidelines. The certification is valid for two years. To obtain recertification, certificate holders need to have at least 40 hours of training every year. Moreover, they need to at least take one course from AccessData, or attend a technical conference organized by AccessData or watch a Web presentation prepared by AccessData. Apart from its own training courses, AccessData recognizes training courses provided by the following organizations:

- Guidance Software Incorporation (GSI)
- International Association of Computer Investigative Specialists (IACIS)

[2] CART Forensic Examiners can use a non-government-agency certification, GIAC Certified Forensics Analyst (GCFA), to fulfill the recertification requirements [National Center for Forensic Science 2004].

- High Tech Crime Institute (HTCI)
- Federal Law Enforcement Training Center (FLETC)
- National White Collar Crime Center
- SEARCH Group
- Defense Computer Investigations Training Program

**Table 1. Computer-Forensics Associations and Certifications**

| Association | Certification |
|---|---|
| 1. AccessData | 1. AccessData Certified Examiner (ACE) |
| 2. American Society for Industrial Security (ASIS) International | 2. Professional Certified Investigator (PCI) |
| 3. Brainbench | 3. Brainbench Computer Forensics (U.S.) (BCF) |
| 4. Cyber Enforcement Resources Incorporated (CERI) | 4. Computer Forensic Examination (CFE)<br>5. Advanced Computer Forensic Examination (ACFE) |
| 5. CyberSecurity Institute (CSI) | 6. CyberSecurity Forensic Analyst (CSFA) |
| 6. Digital Forensic Certification Board (DFCB) | 7. Digital Evidence Practitioner (DEP) |
| 7. E-Business Process Solutions (E-BPS) | 8. Certified Cyber-Crime Expert ($C^3E$) |
| 8. Global Information Assurance Certification (GIAC) | 9. GIAC Certified Forensics Analyst Silver (GCFA)<br>10. GIAC Certified Forensics Analyst Gold (GCFA) |
| 9. Guidance Software Incorporation (GSI) | 11. EnCase Certified Examiner (EnCE) |
| 10. High Tech Crime Institute (HTCI) | 12. Computer Crime Scene Technician (CCST)<br>13. Certified Computer Network Investigator (CCNI)<br>14. Certified Computer Forensic Technician (CCFT)<br>15. Forensic Operating System Specialist (FOSS) |
| 11. High Tech Crime Network (HTCN) | 16. Basic Certified Computer Crime Investigator (CCCI)<br>17. Advanced Certified Computer Crime Investigator (CCCI)<br>18. Basic Certified Computer Forensics Technician (CCFT)<br>19. Advanced Certified Computer Forensics Technician (CCFT) |
| 12. The International Association of Computer Investigative Specialists (IACIS) | 20. Certified Forensic Computer Examiner (CFCE)<br>21. Certified Electronic Evidence Collection Specialist (CEECS) |
| 13. The International Council of Electronic Commerce Consultants (EC-Council) | 22. Computer Hacking Forensic Investigator (CHFI) |
| 14. International Information and Communication Technology Council (IICTC) | 23. Computer Information Forensics Investigator (CIFI) |
| 15. International Information Systems Forensics Association (IISFA) | 24. Certified Information Forensics Investigator (CIFI) |
| 16. The International Society of Forensic Computer Examiners (ISFCE) | 25. Certified Computer Examiner (CCE) |
| 17. Paraben Corporation | 26. Paraben Certified Mobile Examiner (PCME) |

### American Society for Industrial Security (ASIS) International – Professional Certified Investigator (PCI)

URL: http://www.asisonline.org/

Professional Certified Investigator (PCI) is one of three certifications granted by American Society for Industrial Security (ASIS) International. Founded in 1955, ASIS International is a not-for-profit research and educational organization. The PCI certification is not a computer-forensics-specific certification. It covers general investigation skills in case management, evidence collection, and case presentation.

Applicants for PCI need to fulfill four requirements. First, they need to have no criminal records. Second, they need to have a high school diploma or General Education Development (GED) equivalent. Third, they need to have five years of investigation experience, with at least two years in case management. Fourth, they need to take and pass a written examination. The duration of the examination is 2.5 hours. It consists of 125 multiple-choice questions (MCQs).

Knowledge areas covered in PCI include case evaluation, investigative methods, laws and regulations, interview techniques, evidence preservation, case reporting, and witness presentation. A list of reference materials is provided on ASIS Web site. The ASIS provides a two-day review course for the PCI certification but the course is optional.

The certification is valid for three years. Certificate holders need to take 15 hours of training per annum to get recertified. Applicants can earn hours through a number of ways such as attending seminars/conferences, taking accredited college courses, attending chapter meetings, and self-studying.

### Brainbench – Brainbench Computer Forensics (U.S.) (BCF)

URL: http://www.brainbench.com/xml/bb/homepage.xml

Established in 1998, Brainbench offers tests and certifications in more than 600 areas such as information technology, finance, and healthcare. Computer Forensics (U.S.) (BCF) covers general aspects of computer forensics. The only certification requirement for BCF is an online written test. The test is open book and includes 40 MCQs. The passing score of the test is 55 percent. Knowledge areas covered in the test include evidence collection, evidence analysis, forensic tools, and report findings. No training is provided by Brainbench but links to learning resources and practice tests are available to applicants. The certification is valid for three years. Certificate holders need to retake the test to maintain their BCF certification.

### Cyber Enforcement Resources Incorporated (CERI) – Computer Forensic Examination (CFE) and Advanced Computer Forensic Examination (ACFE)

URL: http://www.cyberenforcement.com/ceri.htm

Cyber Enforcement Resources Incorporated (CERI) is a nonprofit corporation established in 2000. Computer Forensic Examination (CFE) and Advanced Computer Forensic Examination (ACFE) are two of three certifications provided by CERI. The third CERI certification is on computer security.

The certification requirements for CFE and ACFE are similar. Both CFE and ACFE applicants need to have at least two years of experience in computer forensics. Both certification applicants need to pass a written examination and complete some online exercises. However, the examination and exercise requirements might be waivered by CERI officials on a case by case basis. CFE applicants need to have at least one year of experience in Microsoft platform analysis and ACFE applicants need to have four years of experience. Regarding non-Microsoft platform analysis, CFE applicants need to have six months of experience and ACFE applicants need to have two years of experience. CFE applicants also need to take at least 40 hours of computer-forensics training. The training requirement for ACFE is 80 hours. CERI does not provide any training courses. Neither certification requires any recertification.

### CyberSecurity Institute (CSI) - CyberSecurity Forensic Analyst (CSFA)

URL: http://www.cybersecurityinstitute.biz/

CyberSecurity Forensic Analyst (CSFA) is offered by CyberSecurity Institute (CSI), an organization that was established in 1997. The certification scope of CSFA covers general computer-forensics skills. CSFAs should be able to conduct a thorough and sound forensic examination of computers and other related devices, interpret digital evidence properly, and communicate examination results effectively and understandably.

Applicants for CSFA need to have a minimum of two years of forensic experience. Moreover, they need to pass a FBI criminal background check. Applicants also need to pass a proctored examination that comprises both written and practical parts. The written part is conducted online and comprises 50 MCQs. The weightings of the written and practical parts are 20 percent and 80 percent respectively. Applicants need to achieve an overall score of at least 85 percent to pass the examination. Applicants for CSFA are highly recommended to hold one of the following certifications:

- AccessData Certified Examiner (ACE)
- Certified Computer Examiner (CCE)
- Certified Forensic Computer Examiner (CFCE)
- Computer Hacking Forensic Investigator (CHFI)
- EnCase Certified Examiner (EnCE)
- GIAC Certified Forensics Analyst (GCFA)

Knowledge areas covered by CSFA include introduction to the Internet, evidence handling, log analysis, Windows forensics, password cracking, and legislation issues. An optional five-day training course is available to CSFA applicants. A list of references is also provided to applicants. The certification is valid for four years. To obtain recertification, certificate holders need to obtain 80 hours of training every two years.

### Digital Forensic Certification Board (DFCB) - Digital Evidence Practitioner (DEP)

URL: http:// http://www.ncfs.org/dfcb/index.html

Digital Evidence Practitioner (DEP) is a certification offered by Digital Forensic Certification Board (DFCB), an organization established in 2004 by National Institute of Justice (NIJ) and administered by National Center of Forensic Science (NCFS). DEP aims at covering four aspects of computer-forensics Investigation: evidence collection, evidence examination, evidence analysis, and evidence presentation.

To become a DEP, applicants need to fulfill four requirements. First, applicants need to have no criminal records. Second, applicants need to have five years of practical experience in handling digital evidence. Third, applicants need to pass an examination. This certification is still under development. DFCB has yet to hold its first certification examination in late 2008. On its Web site, DFCB invites computer-forensics professionals to submit questions to the certification-question bank. Fourth, applicants need to abide by DFCB Ethical Code and Standards of Practices.

All DEPs are expected to demonstrate competencies in five knowledge areas: foundation knowledge, acquisition knowledge, examination knowledge, analysis knowledge, and reporting (written and testimonial) knowledge. Because the certification is still under development, details of other aspects of certification such as duration of certification and recertification requirements are not yet available. However, according to its Web site, DFCB plans to offer specialized certifications in the future. DFCB is associated with the University of Central Florida but computer-forensics courses offered by the university are not tied to or targeted at the DEP certification.

### E-Business Process Solutions (E-BPS) – Certified Cyber-Crime Expert ($C^3E$)

URL: http://www.e-bps.com/outlines/computer_forensic_and_cyber_investigations.htm

Established in 1997, E-Business Process Solutions (E-BPS) is a private management consulting organization. E-BPS offers Certified Cyber-Crime Expert ($C^3E$) certification as part of its training in computer forensics. To obtain the $C^3E$ certification, applicants need to take a four-day course from E-BPS. Upon successful completion of the course, applicants need to pass a practical and a written test. There are no other certification requirements. The certification covers topics such as basic forensic principles, legal issues, search and seizure of computers, forensic imaging and analysis, and investigative techniques. There are no recertification requirements.

### Global Information Assurance Certification (GIAC) – Silver/Gold GIAC Certified Forensics Analyst (GCFA)

URL: http://www.giac.org/

Established in 1999, Global Information Assurance Certification (GIAC) offers a basket of more than 20 certifications in security and computer forensics. GIAC Certified Forensics Analyst (GCFA) focuses on forensic investigation and incident handling. By 2008, GIAC has certified more than 1,100 GCFAs.

The GCFA certification comprises two levels - silver and gold. The only certification requirement for Silver GCFA is a four-hour proctored open-book online examination.[3] The examination comprises 150 MCQs and the passing score is 70 percent. To obtain a Gold GCFA certification, applicants need to be holders of the Silver GCFA. Moreover, they have to complete a 20-page technical report under supervision within six months. Technical reports are assessed according to four criteria: technical accuracy, clear explanation of advanced concepts, extension of ideas beyond courseware, and organization of report. The topics covered in the Silver GCFA include forensic methodology, incident response, evidence gathering, file systems forensics, Windows forensics, network analysis, media analysis, timeline analysis, forensic toolkits.

An optional six-day training course is available for the Silver GCFA certification. The course is provided by SANS (SysAdmin, Audit, Network, Security) Institute. The GCFA certification is valid for four years. Upon expiry of certifications, GCFA holders need to apply again as everyone else.

### Guidance Software Incorporation (GSI) - EnCase Certified Examiner (EnCE)

URL: http://www.guidancesoftware.com/index.aspx

[3] The examination is open book but not open Internet or open computer. Candidates can bring books, reference materials, and printed notes etc. However, electronic devices such as computers, CD-ROM or USB flash drives are not allowed.

EnCase Certified Examiners (EnCE) is offered by Guidance Software Incorporation (GSI). Established in 1997, GSI is the vendor of a leading computer-forensics software, Encase. Similar to other certifications, EnCE certification covers general computer-forensics knowledge. Because it is a vendor-specific certification, EnCE emphasizes the use of EnCase software and methodology. By 2008, GSI has certified more than 750 EnCEs.

Certification requirements of EnCE include three components. First, applicants need to either have 12 months of computer-forensics experience or have attended 64 hours of authorized computer-forensics training (online or classroom). Second, they need to pass an online written examination. The written examination consists of 180 questions and lasts for 2.5 hours. The passing score of the written examination is 80 percent. Third, applicants need to pass a practical examination. The passing score of practical examination is 85 percent. EnCE applicants receive a study guide but they are recommended to take a preparatory course provided by GSI. The duration of the preparatory course, EnCase v6 EnCE Prep Course, is three days. To be eligible to take the preparatory course, applicants need to have already taken two other courses (EnCase Computer Forensics I and II) from GSI.

The knowledge areas covered by EnCE include general computer knowledge, file systems, good forensic practice, the use of EnCase in forensic investigation, and legal issues. The EnCE certification is valid for two years. Certificate holders need to take 64 credit hours of training over two years to obtain recertification.

### High Tech Crime Institute (HTCI) - Computer Crime Scene Technician (CCST), Certified Computer Network Investigator (CCNI), Certified Computer Forensic Technician (CCFT), and Forensic Operating System Specialist (FOSS)

URL: http://www.hightechcrimeinstitute.com/?pg=home

Established in 1995, High Tech Crime Institute (HTCI) offers four certifications - Computer Crime Scene Technician (CCST), Certified Computer Network Investigator (CCNI), Certified Computer Forensic Technician (CCFT), and Forensic Operating System Specialist (FOSS). The four certifications are classified into two levels. CCST is a general Level 1 certification and the other three are Level 2 certifications which focus on specific areas – network, handheld devices, and operating systems respectively.

The only requirement for these four certifications is that applicants successfully complete certain courses provided by HTCI. Applicants for CCST need to successfully complete two courses: Computer Crime Essentials and Forensic Processing Digital Media. Applicants for CCNI need to successfully complete four courses, of which three are compulsory. Same requirements apply for CCFT and FOSS. The three compulsory courses for CCNI, which focuses on network forensics, are Network Investigations, Wireless Investigations, and Home Network Investigations. CCFT focuses on handheld-device forensics and applicants are required to take Cell Phone Forensic Processing, PDA Forensic Processing, and Linux Forensic Processing. The three compulsory courses for FOSS, which focuses on operating systems, are Linux Operating System, Macintosh Apple Operating System, and Advanced Windows Operating System.

The duration of these certifications is only one year. Certificate holders need to take at least 20-26 hours of training every year to get recertified. They can fulfill the requirements by taking computer-forensics courses, participating in computer-forensics meetings, reading books, and so on. Certificate holders can also claim training credits based on their job experience.

### High Tech Crime Network (HTCN) – Basic/Advanced Certified Computer Crime Investigator (CCCI) and Basic/Advanced Certified Computer Forensics Technician (CCFT)

URL: http://www.htcn.org/index.htm

Established in 1991, High Tech Crime Network (HTCN) is a network of law enforcement agencies and security professionals. HTCN offers two certifications: Certified Computer Crime Investigator (CCCI) and Certified Computer Forensics Technician (CCFT).[4] Both certifications have two levels: basic and advanced. Applicants can apply for the advanced certification without having the basic one. The difference between the two certifications is not obvious but according to HTCN officials, CCCI is suitable for non-technical computer crime investigators and CCFT is suitable for technical computer-forensics investigators.

To obtain a basic level CCCI or CCFT certification, applicants are required to submit a detailed application that proves they have at least three years of technical experience and have completed 40 hours of training in computer

[4] The acronym is the same as one of HTCI's four certifications but the spellings are different.

crime. Applicants also need to submit a narrative report of at least 10 cases they have investigated. To obtain an advanced level CCCI or CCFT, applicants have to prove that they have at least five years of technical experience, have completed 80 hours of training in computer crime, have served as a lead investigator in at least 20 cases, and have been involved in a minimum of 40 other cases. Moreover, a detailed narrative report of at least 15 investigated cases is required for advanced level certification applications.

Because of their pure experience requirements, the exact knowledge areas covered by the two certifications are not specified by HTCN. CCCI and CCFT certifications are valid for only one year. The recertification requirements are the same as the ordinary certification requirements.

### The International Association of Computer Investigative Specialists (IACIS) - Certified Forensic Computer Examiner (CFCE) and Certified Electronic Evidence Collection Specialist (CEECS)

URL: http://www.cops.org/

Certified Forensic Computer Examiner (CFCE) and Certified Electronic Evidence Collection Specialist (CEECS) are granted by The International Association of Computer Investigative Specialists (IACIS). IACIS is a nonprofit, volunteer organization which was established in 1990. CFCE covers entire computer-forensics process. Included as part of CFCE certification,[5] CEECS emphasizes best practices of first responders for seizing computers and other related media. By 2008, IACIS has certified more than 600 CFCE and CEECS.

The certification requirements of CFCE and CEECS consist of three parts. First, applicants need to be an active law enforcement officer or an employee of a government agency. Second, applicants need to pass a written test which comprises 100 MCQs. The passing score of the written test is 80 percent. Third, applicants need to pass a practical test which comprises solving six problems involving different media. In most cases, applicants are expected to fulfill the written and practical requirements by successfully completing a two-week training course which is provided by IACIS officials once a year. Applicants who cannot attend the training course can opt for the external CFCE process and take the tests without taking the course. However, applications to go through the external certification process are subject to discretion of IACIS.

Once applicants successfully fulfill all the certification requirements, they can use the certification titles of CFCE and CEECS for three years. Certificate holders need to solve one case in a proficiency examination, complete 60 hours of training, and conduct three forensic examinations of digital evidence within the three-year period to get recertified.

### The International Council of Electronic Commerce Consultants (EC-Council) – Computer Hacking Forensic Investigator (CHFI)

URL: http://www.eccouncil.org/index.htm

Computer Hacking Forensic Investigator (CHFI) is one of the 19 certifications offered by The International Council of Electronic Commerce Consultants (EC-Council), a professional organization established in 2004. CHFI focuses on intruder identification and proper evidence gathering procedures.

Applicants for CHFI need to complete a training course and pass an online proctored written examination. The examination comprises 50 MCQs and lasts for two hours. The passing score of the examination is 70 percent. No working experience is required for CHFI. However, CFHI applicants are recommended to obtain the Certified Ethical Hacker (CEH) certification, which has a requirement of two years of experience in security. CHFI covers a comprehensive set of topics (39 modules) in computer forensics.

CHFI applicants are expected to take a five-day training provided by an authorized training center. Similar to CFCE, special approval is required if CHFI applicants choose to take the written examination without completing the training course. The certification is valid for three years. To obtain recertification, certificate holders need to complete 120 hours of training over the three-year period. To earn the training hours, certificate holders can attend conferences, write research papers, attend webminars, etc. They must complete at least 20 hours of training every year.

### International Information and Communication Technology Council (IICTC) – Computer Information Forensics Investigator (CIFI)

URL: http://www.ictcouncil.org/home/2.html

[5] It is possible to obtain the CEECS separately by attending an IACIS conference or a one-day CEECS course plus passing a written test.



Communications of the Association for Information Systems

Computer Information Forensics Investigator (CIFI) is granted by International Information and Communication Technology Council (IICTC). Established in 2001, IICTC is a nonprofit organization that offers 15 certifications on system administration and software testing. Most certifications offered by IICTC focus on the Linux system.

Applicants for CIFI need to pass a closed-book written examination. Before the examination, applicants are required to read IICTC's code of ethics. The examination duration is three hours and it comprises 100 MCQs. The passing score of the examiantion is 70 percent. Similar to DFCB, IICTC invites professionals to contribute to the certification-question bank. The topics covered in the examination include cybercrime, preparing and planning a computer investigation, computer-forensics tools, and acquiring and handling of computer evidence. A list of reference resources is provided to applicants. IICTC does not provide any training but applicants are recommended to take an optional training course from a registered or accredited training service provider. There are no recertification requirements for this certification.

### International Information Systems Forensics Association (IISFA) - Certified Information Forensics Investigator (CIFI)

URL: http://www.iisfa.org

Established in 2003, International Information Systems Forensics Association (IISFA) is a nonprofit organization that offers a certification titled Certified Information Forensics Investigator (CIFI).[6] CIFI certification covers information investigative process. By 2008, IISFA has certified more than 130 CIFIs.

Applicants for CIFI (IISFA) need to pass a proctored examination. The examination comprises 200 MCQs and covers six categories of knowledge: auditing, incident response, law and investigation, tools and techniques, trackback, and countermeasures. The passing score of the examination is 75 percent. An optional five-day training course is provide by IISFA. There are no recertification requirements for this certification.

### The International Society of Forensic Computer Examiners (ISFCE) - Certified Computer Examiner (CCE)

URL: http://www.isfce.com

Certified Computer Examiner (CCE) certification was first issued in 2003 by The International Society of Forensic Computer Examiners (ISFCE). ISFCE aims to advance the science of computer-forensics examinations. CCE certification covers handling, storage, and examination procedures of digital evidence. By 2008, ISFCE has certified more than 1,000 CCEs.

To obtain a CCE certification, applicants need to fulfill four requirements. First, applicants need to have no criminal records. Second, applicants need to pass an examination that comprises both written and practical parts. Applicants have 45 minutes to complete 75 MCQs in the written examination. For the practical examination, applicants have to write reports after examining three media forensically. The overall passing score is 80 percent. Third, applicants need to either (1) complete a training course from an authorized training center; or (2) have 18 months of forensic experience; or (3) certify completion of self-study. Fourth, applicants need to abide by ISFCE Code of Ethics and Professional Responsibility Standards. Knowledge topics covered in CCE include basic rules of handling evidence, password cracking, and reporting. A list of study materials is provided to applicants.

The CCE certification is valid for two years. To obtain a recertification, all certificate holders need to pass a practical examination. Moreover they need to have either taken at least 50 hours of training or examined digital evidence in at least three cases over the two-year period. If certificate holders fail to meet either the training or the practical experience requirement, they will need to take an online written examination.

### Paraben Corporation - Paraben Certified Mobile Examiner (PCME)

URL: http://www.paraben.com/index.html

Paraben Certified Mobile Examiner (PCME) is granted by Paraben Corporation. Founded in 1999, Paraben Corporation develops software, hardware, and training classes for handheld-device forensics. Similar to HTCI's CCFT, PCME focuses on forensics of handheld devices such as cell phones and personal digital assistants (PDAs).

[6] The acronym of the certification is the same as the one offered by IICTC but different words are used in the certification title.

Certification requirements for PCME consist of four components. First, applicants need to complete and pass three courses (Handheld Forensics, Advanced Cell/SIM Card Forensics, and Cellular/GPS Signal Analysis). The Handheld Forensic course is a Level 1 course which covers operating systems of PDA devices (e.g., Palm, Windows CE, and RIM Blackberry) and the fundamentals of SIM cards. The Advanced Cell/SIM Card Forensics course is a Level 2 course. It is an advanced course on cell phones which covers topics such as network tracing and advanced analysis of data dumps. The Cellular/GPS Signal Analysis course is a Level 3 course which has an in-depth coverage on topics such as historical versus live tracking and legal concepts. The passing score for all three courses is 85 percent. Apart from successfully passing the above three courses, applicants need to pass a proctored written examination. Generally the examination comprises 35 to 45 questions. Applicants also need to pass a practical examination that includes four cases involving handheld devices. Moreover, they need to have at least six months of practical experience in handling handheld devices. The PCME certification is valid for two years. There are no other recertification requirements apart from fees payment.

### Institute of Computer Forensic Professionals (ICFP)

URL: http://www.forensic-institute.org/index.html

Some computer-forensics organizations offer membership but not certification. The Institute of Computer Forensic Professionals (ICFP), which was established in 2004, is one of them. The aim of ICFP is to provide baseline practice standards, educational standards, and testing. The institute does not provide any training courses on computer forensics. Membership of ICFP is classified into two levels. Affiliate members of ICFP are practitioners currently working in the industry. Those who do not work in the computer-forensics industry but are interested in exploring the field can apply for the associate membership. ICFP plans to have additional levels of membership and certifications in the future. Currently, all membership applications are considered on a case by case basis by the ICFP officials. Members need to renew their membership annually.

### High Tech Crime Consortium (HTCC)

URL: http://www.hightechcrimecops.org/index.html

High Tech Crime Consortium (HTCC) is a second example that offers membership only in the area of computer forensics. HTCC is a nonprofit organization founded in 1998. It invites current law enforcement and corporate investigators to join the organization to share information related to computer-forensics. No training courses are available but members have access to a digital library of information. Membership applicants can have a free trial for 90 days after which they need to renew their membership annually.

### High Technology Crime Investigation Association (HTCIA)

URL: http://www.htcia.org/

High Technology Crime Investigation Association (HTCIA) was established in 1999. It is also a nonprofit professional organization that offers membership but not certification in computer forensics. The association focuses on education such as providing training courses but it does not provide any high-tech crime-investigation services. Members of HTCIA are composed of two groups. The first group of HTCIA members comprises investigators and prosecuting attorneys who handle crime associated with computers and other advanced technologies. The second group of HTCIA members is management and security professionals who are responsible for security and computer forensics in private businesses. Similar to ICFP, membership applications for HTCIA are considered on a case by case basis. Members need to renew their memberships annually.

## V. DISCUSSION OF COMPUTER-FORENSICS CERTIFICATION

### Level of Certification and Certification Requirements

Table 2 summarizes all computer-forensics certifications by level of certification and compares their requirements. Most computer-forensics organizations offer one level certification. Only three organizations, GIAC, HTCI, and HTCN, offer two levels of certification. Yet the certification requirements set by these three organizations are quite different. GIAC applicants need to pass a written examination. HTCI applicants need to complete and pass specified training courses. HTCN applicants do not need to take any written examinations or take any specific training courses but they need to fulfill experience and training hour requirements. The question of whether certificate holders of these advanced level certifications are necessarily more competent than those of other one-level certifications is controversial. HTCN's CCCI and CCFT advanced level certifications require applicants to have more practical experience and take more training hours. HTCI's level 2 certifications require applicants to take more courses. Yet GIAC's GCFA Gold level certification only requires applicants to write a technical report.

| Table 2. Computer-Forensics Certification Requirements | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Certification Requirements | | | | | | |
| Certification | Forensic Experience | Report of Investigated Cases | Written Exam | Practical Exam | Training Courses | Criminal Background Check | Note |
| **One-level certification** | | | | | | | |
| ACE | √ 6 months | | √ | √ | | | 1, 2 |
| ACFE | √ 8 years | | √ | | √ 80 hours | | 3, 4, 5 |
| BCF | | | √ | | | | |
| CCE | √ 18 months | | √ | √ | √ 5 days | √ | 6, 7 |
| CFCE (including CEECS) | | | √ | √ | √ 2 weeks | | 8, 9 |
| CFE | √ 3.5 years | | √ | | √ 40 hours | | 3, 4, 10 |
| CHFI | | | √ | | √ 5 days | | 9, 11 |
| CIFI (IICTC) | | | √ | | | | 12 |
| CIFI (IISFA) | | | √ | | | | |
| CSFA | √ 2 years | | √ | √ | | √ | 13 |
| $C^3E$ | | | √ | √ | √ 4 days | | |
| DEP | √ 5 years | | √ | | | √ | 6 |
| EnCE | √ 12 months | | √ | √ | | | 2, 14 |
| PCI | √ 5 years | | √ | | | √ | 15, 16 |
| PCME | √ 6 months | | √ | √ | √ 10 days | | |
| **Two-level certification** | | | | | | | |
| GIAC | | | | | | | |
| Silver GCFA | | | √ | | | | |
| Gold GCFA | | | √ | | | | 17 |
| HTCI | | | | | | | |
| CCST | | | | | √ 8 days | | |
| CCNI/CCFT/ FOSS | | | | | √ 9 days | | |
| HTCN | | | | | | | |
| Basic CCCI / CCFT | √ 3 years | √ 10 cases | | | √ 40 hours | | |
| Advanced CCCI / CCFT | √ 5 years | √ 15 cases | | | √ 80 hours | | 18 |

Note:

1. Must possess licensed copies of AccessData software.
2. Certification examinations are independent of training courses. However, applicants are recommended to take training courses from the certification-granting association.
3. Need to complete certain online exercises.
4. The written examination and exercises may be waivered.
5. Must have at least (i) 2 years of computer-forensics experience; (ii) 4 years of experience in Microsoft platform analysis; and (iii) 2 years of experience in non-Microsoft platform analysis.
6. Abide by code of ethics and professional responsibility standard.
7. Must either have 18 months of experience or complete an approved training course or certify completion of self-study.
8. Must currently work in the industry.
9. It is possible to take the examinations without completing courses but approval to take the examination independently is at the discretion of the certification-granting association.
10. Must have at least (i) 2 years of computer-forensics experience; (ii) 1 year of experience in Microsoft platform analysis; and (iii) 6 months of experience in non-Microsoft platform analysis.
11. Holding of CEH certification is recommended.
12. Must read code of ethics.
13. Holding of other certifications are highly recommended.
14. The experience requirement can be replaced by 64 hours of authorized computer-forensics training.
15. Must include two years of experience in case management.
16. Must have a high school diploma or General Education Requirement (GED) equivalent.
17. Possess Silver GCFA certification plus complete a technical paper.
18. Must have served as a lead investigator in at least 20 cases and be involved in 40 other cases.

Overall, requirements to obtain certifications vary. Most certifications require individuals to pass examinations and have certain relevant experience. HTCN's four certifications (Basic and Advanced CCCI/CCFT) are the only exceptions that do not require applicants to take any specific examination. Most certifications expect applicants to take training courses but the certification examinations are often independent of the courses. However, examinations of HTCI's four certifications are included as part of the specified training courses. Half of the certifications require applicants to have practical computer-forensics or other relevant experience. Individuals who have no prior experience in computer forensics but are interested in embarking on a career in the discipline can pursue certifications such as BCF, CFCE, CHFI, and $C^3E$.

While most certifications include examination requirements, only eight of the certification examinations include a practical component (ACE, CCE, CFCE, CEECS, CSFA, $C^3E$, EnCE, and PCME). Apart from examination and experience requirements, four certifications require applicants to have no criminal records (CCE, DEP, and PCI) or pass a FBI criminal background check (CSFA). Some also require certificate holders to abide by some kind of code of ethics or professional responsibility standard (CCE and DEP). Holding of other computer forensics certifications is also sometimes recommended. For example, ACE, CCE, CFCE, CHFI, EnCE, and GCFA are highly recommended for applicants of CSFA.

## Certification Knowledge Areas

To compare the knowledge scope of various certifications, we classify computer-forensics knowledge areas into 11 categories as shown in Table 3. The categories are developed based on a framework of computer-forensics knowledge that identifies six areas of core computer-forensics knowledge—categories of crime, computer technology, security, legislation, investigation process, and forensic tools [Lim 2005].

1. Introduction to computer forensics
2. Technology
3. Crime
4. Security
5. Legal issues
6. Investigation process
7. Forensic tools
8. Auditing
9. Setting up forensic laboratory
10. Investigating special types of crime
11. Others

The overall picture shown in Table 3[7] confirms the idea that a universal accepted common body of knowledge or curricula in computer forensics is unavailable [Bem and Huebner 2008]. None of the certifications cover all knowledge areas although some certifications (e.g., CHFI, CSFA, and Silver GCFA) appear to be more comprehensive than the others. Most certifications cover legal issues and the investigation process (acquisition, analysis, preservation, and presentation of evidence). However, only seven certifications cover how computer-forensics investigators should behave as an expert witness. Half of the certifications cover network forensics and only three certifications cover forensics of handheld devices (CCFT (HTCI), CHFI, and PCME). Unsurprisingly, the certifications granted by two computer-forensics software vendors, ACE and EnCE, focus on the use of the forensic tools. Despite the overlapping nature of computer forensics with security, only four certifications cover knowledge on security or auditing (BCF, Silver GCFA, CIFI (IICTC) and CIFI (IISFA)). Three certifications also cover knowledge on setting up a forensic laboratory (CHFI, CIFI (IICTC), and CIFI (IISFA)).

## Examination Requirements of Computer-Forensics Certification

Examination requirements of each certification are summarized in Table 4. Passing scores range from 55 percent (BCF) to 85 percent (CSFA, EnCE, and PCME). Most examinations adopt the MCQ format. Two certifications emphasize the practical examination. The weightings of practical examination in CCE and CSFA are 75 percent and 80 percent respectively.

## Certification Duration and Recertification Requirements

Table 5 summarizes the duration and recertification requirements of computer-forensics certifications.[8] The validity period of most certifications vary from one year to four years. However, five certifications have no specified duration.

[7] The summary excludes HTCN's four certifications because they require only practical forensic experience. It also excludes Gold GCFA which requires only report writing. ACFE and CFE of the CERI are also excluded because of insufficient information.
[8] DEP is excluded from the table because the certification is still under construction and information on recertification is not yet available.



Communications of the Association for Information Systems

In all other cases, certificate holders need to pay fees to obtain recertification. Moreover, similar to other certified professionals such as accountants and engineers, computer-forensics professionals often need to fulfill continuous professional development (CPD) requirements to obtain recertification. Such recertification requirements and procedures assure the continued competency of professionals over time.

**Table 3. Certification Knowledge Areas**

| | Certification* | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Knowledge Areas | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1. Introduction to computer forensics | | | | | | √ | √ | | | √ | √ | √ | | | |
| 2. Technology | | | | | | | | | | | | | | | |
| Computer (file systems etc.) | √ | | | √ | √ | √ | √ | √ | √ | √ | √ | √ | | √ | |
| Network | | | | | √ | | √ | | √ | | √ | √ | √ | √ | |
| Media (USB, CD etc.) | | | | √ | | | √ | | | √ | √ | √ | | √ | |
| Handheld devices (cell phone, PDA etc.) | | | | | | | | | √ | | √ | | | | √ |
| Windows systems | √ | | | √ | | | √ | √ | √ | | √ | √ | | √ | |
| Other systems (Linux etc.) | | | | | | | √ | | √ | | √ | √ | | √ | |
| 3. Crime (virus, malware etc.) | | | | √ | √ | √ | | | √ | √ | √ | √ | √ | √ | |
| 4. Security | | | | | | | √ | | | | | √ | √ | | |
| 5. Legal issues | | | | | | | | | | | | | | | |
| Legislations and law enforcement | | √ | √ | √ | | √ | √ | √ | | √ | √ | √ | √ | √ | |
| Becoming an expert witness | | √ | | √ | √ | √ | | | | | √ | √ | √ | | |
| 6. Investigation process | | | | | | | | | | | | | | | |
| Best practices of evidence handling | | √ | | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | |
| Incident response | | | | | √ | | √ | √ | √ | √ | √ | √ | √ | √ | |
| Identification/Searching of evidence | √ | | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | | √ | |
| Acquisition of evidence (imaging, hashing, password cracking etc.) | √ | | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | | √ | |
| Analysis of evidence (e.g., log analysis, timeline analysis) | | | √ | √ | √ | √ | √ | | √ | | √ | √ | | | |
| Preservation of evidence | | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | |
| Presentation of evidence | √ | √ | √ | √ | √ | | | | | | √ | √ | √ | √ | |
| Tracking culprits | | | | | | | √ | | | | √ | √ | √ | | |
| 7. Forensic tools | √ | | √ | | | √ | √ | √ | √ | | √ | √ | √ | | |
| 8. Auditing | | | √ | | | | | | | | | √ | √ | | |
| 9. Setting up forensic laboratory | | | | | | | | | | | √ | √ | √ | | |
| 10. Investigating special types of crime (child pornography, sexual harassment, corporate espionage etc.) | | | | | | | | | | | √ | | | | |
| 11. Others (e.g., insurance, liability issues) | | | | √ | | | | | | | | | | | |

*Certification

1. AccessData Certified Examiner (ACE)
2. Professional Certified Investigator (PCI)
3. Brainbench Computer Forensics (U.S.) (BCF)
4. CyberSecurity Forensic Analyst (CSFA)
5. Digital Evidence Practitioner (DEP)
6. Certified Cyber-Crime Expert ($C^3E$)
7. Silver GIAC Certified Forensics Analyst (GCFA)
8. EnCase Certified Examiner (EnCE)
9. Computer Crime Scene Technician (CCST), Certified Computer Network Investigator (CCNI), Certified Computer Forensic Technician (CCFT), and Forensic Operating System Specialist (FOSS)
10. Certified Forensic Computer Examiner (CFCE) and Certified Electronic Evidence Collection Specialist (CEECS)
11. Computer Hacking Forensic Investigator (CHFI)
12. Computer Information Forensics Investigator (CIFI) (IICTC)
13. Certified Information Forensics Investigator (CIFI) (IISFA)
14. Certified Computer Examiner (CCE)
15. Paraben Certified Mobile Examiner (PCME)

| Table 4. Examination Requirements of Computer-Forensics Certification | | | |
|---|---|---|---|
| | | | |
| Certification | Written Exam | Practical Exam | Note |
| ACE | √ 60 questions | √ | Passing score of written exam is 80% |
| ACFE | √ | | |
| BCF | √ 40 MCQs | | Passing score of written exam is 55% |
| CCE | √ 75 MCQs | √ 3 media | Weighting of written exam is 25%<br>Overall passing score is 80% |
| CFCE (including CEECS) | √ 100 MCQs | √ 6 media | Passing score of written exam is 80% |
| CFE | √ | | |
| CHFI | √ 50 MCQs | | Passing score of written exam is 70% |
| CIFI (IICTC) | √ 100 MCQs | | Passing score of written exam is 70% |
| CIFI (IISFA) | √ 200 MCQs | | Passing score of written exam is 75% |
| CSFA | √ 50 MCQs | √ | Weighting of 2 examinations:<br>20% written exam, 80% practical exam<br>Overall passing score is 85% |
| $C^3E$ | √ | √ | |
| DEP | √ | | Examination is still under construction |
| EnCE | √ 180 questions | √ | Passing score of written exam is 80%,<br>Passing score of practical exam is 85% |
| Silver GCFA | √ 150 MCQs | | Passing score of written exam is 70% |
| Gold GCFA | √ 20-page technical report | | Must complete within 6 months |
| PCI | √ 125 MCQs | | |
| PCME | √ 35 to 45 questions | √ 4 cases | Passing score of written exam is 85% |

Most certifications require certificate holders to take examinations, receive training or have practical forensic experience to get recertified. However, seven certifications (BCF, Basic/Advanced CCCI, Basic/Advanced CCFT (HTCN), and Silver/Gold GCFA) require certificate holders to go through the entire certification process again. Typically certification holders can earn CPD credit points by attending conferences, attending training classes, reading, writing research papers and so on. The number of CPD credit hours of training required ranges from 20 hours (CCST) to 40 hours (ACE, CHFI, and CSFA) per annum. Two certifications (CCE and CFCE) require certificate holders to have practical forensic examination experience in at least three cases during the certification duration. Among all the certifications, CCE has the most flexible arrangement for recertification. Apart from a compulsory practical examination, CCE certificate holders can fulfill the remaining requirements by either having 50 hours of training, having experiences of examining three cases, or passing a written online examination. The CCE is also the only certification that requires holders to take a practical examination in recertification.

## VI. TRAINING AND EDUCATION

Table 6 summarizes information about training courses targeted at specific certification, such as course providers and course duration. Training is typically provided by either the certification-granting association or other approved training providers. In most cases, training courses are part of the certification requirements. Occasionally, applicants can choose to take certification examinations without attending specific training courses but special approval is required (CEECS, CFCE, and CHFI). Sometimes, even if special approval is not required, applicants are expected to take and complete courses specified by the certification-granting association (ACE, EnCE, and Silver GCFA). The duration of training courses targeted at specific certifications ranges from two days to 2 weeks.

Apart from taking certification-specific training courses, individuals who are interested in learning computer forensics can enroll in academic programs at tertiary institutions. Many academic programs on computer forensics have sprung up within the last few years. Some programs are provided as part of a forensic science program. Others are offered separately at different levels—associate degree programs, certificate programs, baccalaureate programs, or graduate programs [Gottschalk et al. 2005]. It should be noted that none of the academic programs in computer forensics are tied to any of the certifications even though in some cases certification-granting associations are associated with certain tertiary institutions[9] or officials of certification-granting associations teach at certain

[9] For example, University of Central Florida is associated with DFCB but its computer-forensics programs are not tied to the DEP certification.



Communications of the Association for Information Systems

institutions.[10] While it is a common practice for professional accounting associations to grant exemptions to graduates of certain tertiary institutions, none of the computer-forensics certification-granting associations grant exemption to students who receive education from tertiary institutions.

Table 5. Certification Duration and Recertification Requirements

| Certification | | Recertification Requirements | | | | | |
|---|---|---|---|---|---|---|---|
| Duration | Title | Complete Retest (1) | Written Exam (2) | Practical Exam (3) | Average Hours of Training PA (4) | Forensic Experience (5) | Note |
| 1-year | Basic/Advanced CCCI | √ | | | | | |
| | CCFT (HTCI) | | | | 26 hours | | |
| | Basic/Advanced CCFT (HTCN) | √ | | | | | |
| | CCNI | | | | 26 hours | | |
| | CCST | | | | 20 hours | | |
| | FOSS | | | | 26 hours | | |
| 2-year | ACE | | | | 40 hours | | Must take one AccessData update (course, technical conference or Web presentation |
| | CCE | | √ | √ | 25 hours | 3 cases over 2 years | ● (3) is compulsory<br>● either (4) or (5) is required<br>● if fails to meet (4) or (5), will need to take (2) |
| | EnCE | | | | 32 hours | | |
| | PCME | | | | | | Only need to pay recertification fees, no other recertification requirements |
| 3-year | BCF | √ | | | | | |
| | CFCE (including CEECS) | | √ | | 20 hours | 3 cases over 3 years | |
| | CHFI | | | | 40 hours | | Must complete at least 20 hours of training per year |
| | PCI | | | | 15 hours | | |
| 4-year | CSFA | | | | 40 hours | | |
| | Silver/ Gold GCFA | √ | | | | | |
| Not specified | ACFE | | | | | | |
| | CFE | | | | | | |
| | CIFI (IICTC) | | | | | | |
| | CIFI (IISFA) | | | | | | |
| | $C^3E$ | | | | | | |

[10] For example, President/CEO of CSI teaches at the Edmonds Community College.



Communications of the Association for Information Systems

**Table 6. Certification-Specific Training**

| Certification | Training Available? | Course Provider | Course Name | Course Duration | Part of Certification Requirement? |
|---|---|---|---|---|---|
| ACE | Yes | AccessData | AccessData Bootcamp | 3 days | No |
| | | | FTK 2 Transition | 1 day | No |
| | | | Windows Forensics–XP | 3 days | No |
| ACFE | No | | | | |
| BCF | No | | | | |
| Basic/Advanced CCCI | No | | | | |
| CCE | Yes | Authorized Training Centers | CCE Bootcamp | 5 days | No |
| CCFT (HTCI) | Yes | HTCI | Cell Phone Forensic Processing | 3 days | Yes |
| | | | PDA Forensic Processing | 3 days | Yes |
| | | | Linux Forensic Processing | 3 days | Yes |
| Basic/Advanced CCFT (HTCN) | No | | | | |
| CCNI | Yes | HTCI | Network Investigations | 3 days | Yes |
| | | | Wireless Investigations | 3 days | Yes |
| | | | Home Network Investigations | 3 days | Yes |
| CCST | Yes | HTCI | Computer Crime Essentials | 3 days | Yes |
| | | | Forensic Processing Digital Media | 5 days | Yes |
| CFCE (including CEECS) | Yes | IACIS | Certified Forensic Computer Examiner Course | 2 weeks | Yes |
| CFE | No | | | | |
| CHFI | Yes | EC-Council Authorized Training Centers | CHFI Exam | 5 days | Yes |
| CIFI (IICTC) | Yes | RSTP or ASTP | Computer Forensic | 2 days | No |
| CIFI (IISFA) | Yes | IISFA | Certified Information Forensics Investigator Training | 5 days | No |
| CSFA | Yes | CSI | Computer Forensics Core Competencies | 5 days | No |
| $C^3E$ | Yes | E-BPS | Computer Forensic and Cyber Investigations | 4 days | Yes |
| DEP | No | | | | |
| EnCE | Yes | GSI | EnCase v6 EnCE Prep Course | 3 days | No |
| | | | EnCase Computer Forensics I | 4 days | No |
| | | | EnCase Computer Forensics II | 4 days | No |
| FOSS | Yes | HTCI | Linux Operating System | 3 days | Yes |
| | | | Macintosh Apple Operating System | 3 days | Yes |
| | | | Advanced Windows Operating System | 3 days | Yes |
| Silver GCFA | Yes | SANS Institute | System Forensics, Investigation & Response | 6 days | No |
| Gold GCFA | No | | | | |
| PCI | Yes | ASIS | Professional Certified Investigator (PCI) Review | 2 days | No |
| PCME | Yes | Paraben Corporation | Handheld Forensics – Level 1 | 4 days | Yes |
| | | | Advanced Cell/SIM Card Forensics – Level 2 | 4 days | Yes |
| | | | Cellular/GPS Signal Analysis – Level 3 | 2 days | Yes |

The number of programs on computer forensics continues to rise both in and outside the U.S. By 2005, Gottschalk et al., [2005] were able to identify 32 computer forensics-related programs in the U.S. Appendix 1 lists some of these programs. Within the U.S., institutions that offer computer-forensics programs include Central Florida University, Champlain College, Dakota State University, Indian Hills Community College, Metropolitan State University, and

Sam Houston State University. [Gottschalk et al. 2005; Kessler and Schirling 2006; Liu 2006]. In Australia, University of Western Sydney in Australia offers a Bachelor of Computer Science degree with a major in Computer Forensics [Bem and Huebner 2008]. In Europe, Northumbria University in the United Kingdom offers a Bachelor of Science degree in Computer Forensics and a Postgraduate Certificate in Digital Forensics. In Germany, computer-forensics courses are part of a postgraduate diploma in computer science at RWTH Aachen University [Anderson et al. 2006].

Because of its multidisciplinary nature and huge amount of preparation work required, computer-forensics programs are often developed and taught as a result of cooperation among different departments such as computer science department and criminology department. Program development often involves additional investments by institutions and requires lengthy planning and preparation [McGuire and Murff 2006]. Moreover, because of its practical nature, a forensic laboratory is often built for a computer-forensics program so that students can have hands-on practice handling digital evidence[11] [Anderson et al. 2006; Yasinsac et al. 2003].

The knowledge areas covered by different academic programs are partly influenced by the length of the program and the extent of cooperation among different departments. Because Champlain College is one of the pioneers in offering computer-forensics programs, its curriculum is used as an example here to demonstrate the knowledge coverage of an academic program [Kessler and Schirling 2006]. The Bachelor of Science in Computer and Digital Forensics at Champlain College requires 120 credit hours. The program comprises four categories of core courses: digital investigation, computer technology, criminal justice, and others. The 24 core courses offered by Champlain College provide a breadth of knowledge. Knowledge taught in courses such as Forensic Accounting, White Collar Crime, Investigative Interviewing, Interpersonal Communication, Critical Thinking and Ethics in Human Services is outside the scope of most computer-forensics certifications.

## VII. CERTIFICATION IN OTHER DISCIPLINES

Because of the overlapping nature of computer forensics with other disciplines, examples of certification in forensic accounting and information security are described below to give readers some ideas how certification in computer forensics compared to other disciplines. An example of certification in forensic science is described in Lim [2008]. Readers who are interested in certifications in forensic accounting and information security can find a list of some of the major certifications in these two disciplines in Appendices 2 and 3.

### Association of Certified Fraud Examiners (ACFE) - Certified Fraud Examiner (CFE)

URL: http://www.acfe.com/

Association of Certified Fraud Examiners (ACFE) offers a popular certification, Certified Fraud Examiner (CFE), in forensic accounting. Established in 1988, ACFE provides anti-fraud training and education. It has certified more than 20,000 CFE by 2008.

Holders of CFE are considered experts in fraud prevention, detection, and deterrence. To become CFEs, applicants need to fulfill six requirements. First they need to be an Associate Member of ACFE. Second, they must have a bachelor's degree. Applicants without a bachelor's degree can substitute each year of academic study by two years of fraud-related professional experience. Third, applicants need to have two years of professional experience in relation to detection or deterrence of fraud. Fourth, they need to pass a written examination which is in CD-ROM format. CFE examination comprises 500 questions and covers four areas: (1) fraudulent financial transactions, (2) legal elements of fraud, (3) investigation methods, and (4) criminology and ethics. The passing score of the examination is 75 percent. Fifth, applicants need to be of high moral character and agree to abide by the bylaws and code of professional ethics. Sixth, three letters of recommendation should also be included in the certification application. Certificate holders need to complete 20 hours of continuing professional education every year to maintain their CFE status. At least 10 hours of the education need to relate directly to fraud detection and deterrence.

### American College of Forensic Examiners Institute (ACFEI) - Certified Forensic Accountant (Cr.FA)

URL: http://www.acfei.com/

Another example of forensic-accounting certification is Certified Forensic Accountant (Cr.FA) which is offered by American College of Forensic Examiners Institute (ACFEI). ACFEI is a professional organization which can be

[11] A computer-forensics course developed in Australia is an exception. The course was developed and taught in a business department by only one academic who has no computer science background. There were no cooperations from other departments. The university had not provided any additional resources. Nor was a forensic laboratory available for the course [Lim 2005].

traced back to 1992 when American Board of Forensic Handwriting Analysts was founded. The Cr.FA certification was first issued in 2001. By 2008, NACVA has certified over 300 Cr.FAs.

Cr.FA applicants need to fulfill four requirements. First, they need to already hold the CPA certification and register with local state board of accountancy. Second, they should not be currently under investigation or have any records of disciplinary action from any certification bodies during the past 10 years. Third, they must have no criminal records. Fourth, they need to complete and pass an online examination. Knowledge areas covered in Cr.FA include expert report writing procedure, challenges related to expert testimony, fraud prevention, and various valuation approaches. Certification holders need to complete 15 hours of continuing professional education every year to maintain their Cr.FA status.

### International Information Systems Security Certification Consortium (ISC)$^2$ - Certified Information Systems Security Professional (CISSP), Systems Security Certified Practitioner (SSCP), Information Systems Security Architecture Professional (ISSAP), Information Systems Security Engineering Professional (ISSEP), and Information Systems Security Management Professional (ISSMP)

URL: https://www.isc2.org/cgi-bin/index.cgi

International Information Systems Security Certification Consortium (ISC)$^2$ is a nonprofit organization established in 1989, which aims at educating and certifying information security professionals. Its Certified Information Systems Security Professional (CISSP) certification is one of the most widely recognized certifications in the security industry. ISC$^2$ also offers Systems Security Certified Practitioner (SSCP) certification for people with less experience in security and three other certifications that focus on different areas. The three specialized certifications are Information Systems Security Architecture Professional (ISSAP), Information Systems Security Engineering Professional (ISSEP), and Information Systems Security Management Professional (ISSMP). The total number of ISC$^2$ certificate holders is more than 60,000.

CISSP applicants need to fulfill the following three requirements. First, they need to have five years of direct full-time security work experience. If applicants have a college degree or another approved certification,[12] the experience requirement is reduced by one year. Second, they must pass a written test. The test is six hours long and comprises 250 MCQs. The passing score of the test is 70 percent. Third, they must subscribe to (ISC)$^2$'s code of ethics.

The CISSP certification covers 10 knowledge areas and focuses on managerial instead of technical aspect. They include security management practices, security architecture and models, application development security, and business continuity planning. An optional five-day review seminar on CISSP certification examination is provided by (ISC)$^2$. The CISSP certification is valid for three years. Certificate holders need to obtain 120 hours of continuing professional education over three years.

## VIII. CONCLUSIONS

This paper aims to guide nonpractitioners of computer forensics through the certification maze of the discipline. It surveys all the computer-forensics certifications that are open to the public and provides a detailed description of the certification-granting associations, certification requirements, knowledge areas, and recertification requirements. It also describes three professional associations that offer membership but not certification in computer forensics. Unlike certification, membership of such organizations does not imply expertise in computer forensics. Analysis of 26 certifications shows that there is no uniform standard of certification or recertification in the industry. The large number of certifications and the mixture of certifications and memberships, together with the wide continuum of certification requirements, which range from pure examination to pure experience, create a confusing image of the discipline in the eyes of outsiders.

The confusing situation gets worse when different certification titles clash and have the same acronyms. For example, the acronym of one of the computer-forensics certifications, CFE, overlaps with two other certifications in forensic accounting. The situation gets even messier when the clash happens within the discipline. One example is the CCFT certification, which is granted by both HTCI and HTCN. Apart from different spellings of the their titles, the two certifications are at the opposite ends of the requirement-continuum (pure courses/examinations for HTCI and experience plus training for HTCN). Another example is the CIFI certification, which is granted by both IICTC and IISFA. The two CIFI certifications use different words but their certification requirements are similar. Both CIFI certifications only have the examination requirement. With such multiple use of the same acronyms it is doubtful

[12] The following certifications in computer forensics are recognized by (ISC)$^2$: CCE, CCCI (Advanced), CFCE, CFE, and GCFA.



Communications of the Association for Information Systems

whether many computer-forensics professionals, let alone outsiders, are fully aware of the differences among various certifications.

Apart from the clash of certification titles, confusion also arises when overlapping certifications are offered by the same organization but differences among the certifications are not obvious (e.g., CCCI and CCFT). Why should there be a separate certification title if one certification is part of another certification (e.g., CEECS is part of CFCE)? The overlapping situation gets worse when one considers certifications in both computer-forensics and information security disciplines. We believe all the confusion prevents computer forensics from building a clear image and could potentially hamper the general public's trust in the discipline.

It is difficult to say which of the 26 certifications is considered the most trustworthy by practitioners and non-practitioners. The fact that computer-forensics professionals tend to obtain at least three or four certifications, whose knowledge areas overlap, is evident that even the practitioners themselves do not know which certification is better than the others. Such a multiple-certification approach is not necessarily good for the discipline as it further creates confusion for the outsiders.

The level of trust in certifications could be affected by factors such as transparency of the certification process, rigor of the certification and recertification requirements, frequency of certification requirement updates (e.g., revised requirement for a new version of forensic software), and association with government agencies. Regarding the number of certificate holders, only two certifications (GCFA and CCE) have more than 1,000 certificate holders by 2008. We believe the DEP certification is likely to attract applicants because of its association with the NIJ and NCFS. Further research should be done to investigate the trustworthiness and general acceptance issues of each certification. For example, one might conduct a survey of all practitioners to gather their opinions on different certifications.

The results of this study show that certification requirements in computer forensics do not differ too much from those in forensic accounting and information security. However, the results confirm the findings of an earlier study which show that the certification and recertification requirements of the computer-forensics discipline are not as stringent as those of forensic-science discipline [Lim 2008]. Many computer-forensics certifications require only a one-off examination. Only half of the certifications require applicants to have practical experience. None require peer reviews for recertification. No single computer-forensics certification has certification and recertification requirements as comprehensive as the forensic-science certification described in Lim [2008].

Computer forensics is a fast-changing discipline. It is important for certifications to keep their certificate holders abreast of the developments in new technologies. It is also important for certifications to establish a clear image of the discipline. Perhaps different certification-granting associations could work together to build a strong brand image of the discipline. Practitioners should work together to build up outsiders' trust of the discipline. They can perhaps try enhancing the transparency of the certification process and tightening the certification requirements. Currently, training and education of computer forensics are independent of each other. Perhaps certification-granting associations could consider cooperating with tertiary institutions to strengthen the training and education in the computer-forensics discipline. Yet before the discipline matures, potential employers of computer-forensics professionals and prospective certification applicants will have to exercise care in selecting an appropriate certification that suits their needs.

## ACKNOWLEDGMENTS

The author thanks Åke Grönlund, Peter Seddon, and the associate editor for their helpful comments.

## REFERENCES

*Editor's Note*: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Albrecht, W. S., C. C. Albrecht, and C. O. Albrecht. (2006). *Fraud Examination*, London, U.K.: Thomson South-Western.

Anderson, P. et al. (2006). "A Comparative Study of Teaching Forensics at a University Degree Level," Proceedings of the International Conference on IT-Incident Management & IT-Forensics, Stuggart, Germany, pp. 116-127.

Anastasi, J. (2003). *The New Forensics: Investigating Corporate Fraud and the Theft of Intellectual Property*, John Wiley & Sons, New Jersey.

Bem, D. and E. Huebner. (2008). "Computer Forensics Workshop for Undergraduate Students," Proceedings of the Tenth Conference on Australasian Computing Education - Volume 78, Wollongong, NSW, Australia, Australian Computer Society, Inc., pp. 29-33.

Canavan, J. E. (2001). *Fundamentals of Network Security*, Norwood, MA: Artech House.

Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. London, UK: Elsevier Academic Press.

Casey, E. (2006). "Investigating Sophisticated Security Breaches," *Communications of the ACM* (49)2, pp. 48-54.

Danielyan, E. (2003). *Information Security Qualifications: An In-Depth Coverage of Vendor and Vendor-Neutral Qualifications*, Swiss Federal Institute of Technology Zurich.

Gottschalk, L. et al. (2005). "Computer Forensics Programs in Higher Education: A Preliminary Study," *ACM SIGCSE Bulletin* 37(1), pp. 147-151.

Jones, R. (2004). "Your Day in Court - The Role of the Expert Witness," *Digital Investigation* (1)4, pp. 273-278.

Kent, J., and B. Ghavalas. (2005). "The Unique Challenges of Collecting Corporate Evidence," *Digital Investigation* (2)4, pp. 239-243.

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

Lim, N. (2005). "Crime Investigation: A Course in Computer Forensics," *Communications of the Association for Information Systems* (18), pp. 205-225.

Lim, N. (2008). "Digital Forensic Certification Versus Forensic Science Certification," ADFSL Conference on Digital Forensics, Security and Law, Oklahoma City, USA, pp. 7-13.

Liu, J. (2006). "Developing an Innovative Baccalaureate Program in Computer Forensics," 36th ASEE/IEEE Frontiers in Education Conference, San Diego, CA, pp. 1-6.

McGuire, T. J. and K. N. Murff. (2006). "Issues in the Development of a Digital Forensics Curriculum," *Journal of Computing Sciences in Colleges* 22(2), pp. 274-280.

McKemmish, R. (1999). “No. 118 What Is Forensic Computing?” *Australian Institute of Criminology Trends and Issues in Crime and Criminal Justice*, http://www.aic.gov.au/publications/tandi/ti118.pdf (current Apr. 1, 2006).

Mohay, G. et al. (2003). *Computer and Intrusion Forensics*, Norwood, MA: Artech House.

National Center for Forensic Science. (2004). “Draft Final Report: The Certification Roundtable Meeting,” May 5-6 2004, pp. 1-10, http://www.ncfs.org/dfcb/CERT%20ROUNDTABLE%20REPORT%20(DRAFT%20V%206-07-04).pdf (current Sept. 24, 2008).

Nelson, B. et al. (2005). *Guide to Computer Forensics and Investigations*, 2nd edition, Boston, Massachusetts: Thomson Course Technology.

Rogers, M. K. and K. Seigfried. (2004). "The Future of Computer Forensics: A Needs Analysis Survey," *Computers & Security* (23)1, pp. 12-16.

Sinangin, D. (2002). "Computer Forensics Investigations in a Corporate Environment," *Computer Fraud & Security*, (2002)6, pp. 11-14.

Solon, M. and P. Harper. (2004). "Preparing Evidence for Court," *Digital Investigation* (1)4, pp. 279-283.

Yasinsac, A. et al. (2003). "Computer Forensics Education," *IEEE Security & Privacy* 1(4), pp. 15-23.

## APPENDIX 1: EXAMPLES OF ACADEMIC PROGRAMS IN COMPUTER FORENSICS

**Appendix 1. Examples of Academic Programs in Computer Forensics**

| Country | Institution | Level* | Program Title | Program Duration |
|---|---|---|---|---|
| Australia | Melbourne University | P | Graduate Certificate in Digital Forensics | 2 years part-time |
| | University of Western Sydney | U | Bachelor of Computer Science (major in Computer Forensics) | 3 years |
| Germany | RWTH Aachen University | U | Computer Science Diploma (specialize in Computer Forensic) | 1 year |
| United Kingdom | Cranfield University | P | Master of Science/Postgraduate Diploma/Postgraduate Certificate in Forensic Computing | 1-3 years part-time |
| | Leeds Metropolitan University | U | BSc(Hons) Computer Forensics | 3 years |
| | Northumbria University | U | BSc(Hons) Computer Forensics | 3 years full-time<br>4 years sandwich |
| | | P | Postgraduate Certificate in Digital Forensics | 1 year |
| U.S.A. | Central Florida University | P | Graduate Certificate in Computer Forensics | 1 year |
| | | | Master of Science in Digital Forensics | 2 years |
| | Champlain College | U | Bachelor of Science in Computer and Digital Forensics | 4 years |
| | Dakota State University | U | Bachelor degree (minor in Computer Forensics) | 4 years |
| | Indian Hills Community College | U | A.A.S. in Computer Forensics | 2 years |
| | Metropolitan State University | U | B.A.S. in Computer Forensics | 4 years |
| | Sam Houston State University | P | Master of Science in Digital Forensics | 2 years |

* U: Undergraduate program, P: Postgraduate program

## APPENDIX 2: EXAMPLES OF CERTIFICATION IN FORENSIC ACCOUNTING

| Appendix 2. Examples of Certification in Forensic Accounting | | |
|---|---|---|
| Year Established | Certification-Granting Association and Web site | Certification |
| 1992 | American College of Forensic Examiners Institute (ACFEI)<br><br>http://www.acfei.com/ | Certified Forensic Accountant (Cr.FA) |
| 1999 | Association of Certified Forensic Investigators of Canada (ACFI)<br><br>http://www.acfi.ca/ | Certified Forensic Investigator (CFI) |
| 1988 | Association of Certified Fraud Examiners (ACFE)<br><br>http://www.acfe.com/ | Certified Fraud Examiner (CFE) |
| 1993 | Association of Certified Fraud Specialists (ACFS)<br><br>http://acfsnet.org/index.htm | Certified Fraud Specialists (CFS) |
| 1992 | Association of Insolvency and Restructuring Advisors (AIRA)<br><br>http://www.airacira.org/ | Certified Insolvency and Restructuring Advisor (CIRA) |
| 1991 | Financial Forensics Institute (FFI) of National Association of Certified Valuation Analysts (NACVA)<br><br>http://www.nacva.com/ | Certified Forensic Financial Analyst (CFFA) |
| 1973 | Society of Financial Examiners (SOFE)<br><br>http://www.sofe.org/ | • Accredited Financial Examiner (AFE)<br>• Certified Financial Examiner (CFE)<br>• Automated Examiner Specialist (AES) |

## APPENDIX 3: EXAMPLES OF CERTIFICATION IN INFORMATION SECURITY

| Appendix 3. Examples of Certification in Information Security | | |
|---|---|---|
| Year Established | Certification-Granting Association and Web site | Certification |
| 1989 | CERT Coordination Center<br><br>http://www.cert.org/cert/ | CERT-Certified Computer Security Incident Handler (CSIH) |
| 2000 | Certified Internet Web Professional (CIW)<br><br>http://www.ciwcertified.com/ | • CIW Security Analyst<br>• CIW Security Professional |
| 1993 | Check Point Software Technologies Ltd.<br><br>http://www.checkpoint.com/index.html | • Check Point Certified Master Architect (CCMA)<br>• Check Point Certified Managed Security Expert (CCMSE)<br>• Check Point Certified Security Expert (CCSE)<br>• Check Point Certified Security Administrator (CCSA)<br>• Check Point Certified Security Principles Associate (CCSPA) |
| 2002 | Computing Technology Industry Association (CompTIA)<br><br>http://certification.comptia.org/default.aspx | Computer Technology Industry Association Security+ (CompTIA Security+) |
| 1999 | Global Information Assurance Certification (GIAC)<br><br>http://www.giac.org/ | • GIAC Security Essentials Certification (GSEC)<br>• GIAC Certified Windows Security Administrator (GCWN)<br>• GIAC Certified UNIX Security Administrator (GCUX)<br>• GIAC Information Security Fundamentals (GISF)<br>• GIAC Security Leadership Certificate (GSLC)<br>• GIAC Security Engineer (GSE) |
| 1969 | Information Systems Audit and Control Association (ISACA)<br><br>http://www.isaca.org/ | Certified Information Security Manager (CISM) |
| 1989 | International Information Systems Security Certification Consortium (ISC)[2]<br><br>https://www.isc2.org/cgi-bin/index.cgi | • Certified Information Systems Security Professional (CISSP)<br>• Information Systems Security Architecture Professional (ISSAP)<br>• Information Systems Security Engineering Professional (ISSEP)<br>• Information Systems Security Management Professional (ISSMP)<br>• Systems Security Certified Practitioner (SSCP) |
| 1999 | Security Certified Program (SCP)<br><br>http://www.securitycertified.net/index.htm | • Security Certified Network Specialist (SCNS)<br>• Security Certified Network Professional (SCNP)<br>• Security Certified Network Architect (SCNA) |

## GLOSSARY

| | |
|---|---|
| A.A.S. | Associate of Applied Science |
| ACE | AccessData Certified Examiner |
| ACFE | 1. Advanced Computer Forensic Examination (A certification offered by CERI.) |
| | 2. Association of Certified Fraud Examiners (A forensic accounting association.) |
| ACFEI | American College of Forensic Examiners Institute |
| ACFI | Association of Certified Forensic Investigators of Canada |
| ACFS | Association of Certified Fraud Specialists |
| AES | Automated Examiner Specialist |
| AFE | Accredited Financial Examiner |
| AIRA | Association of Insolvency and Restructuring Advisors |
| ASIS International | American Society for Industrial Security International |
| ASTP | Accredited Training Service Provider |
| B.A.S. | Bachelor of Applied Science |
| BCF | Brainbench Computer Forensics (U.S.) |
| BSc | Bachelor of Science |
| CA | Certified Accountant |
| CART | Computer Analysis Response Team |
| CCCI | Certified Computer Crime Investigator |
| CCE | Certified Computer Examiner |
| CCFT | 1. Certified Computer Forensic Technician (A certification offered by HTCI.) |
| | 2. Certified Computer Forensics Technician (A certification offered by HTCN.) |
| CCMA | Check Point Certified Master Architect |
| CCMSE | Check Point Certified Managed Security Expert |
| CCNI | Certified Computer Network Investigator |
| CCSA | Check Point Certified Security Administrator |
| CCSE | Check Point Certified Security Expert |
| CCSPA | Check Point Certified Security Principles Associate |
| CCST | Computer Crime Scene Technician |
| CEECS | Certified Electronic Evidence Collection Specialist |
| CEH | Certified Ethical Hacker |
| CERI | Cyber Enforcement Resources Incorporated |
| CFCE | Certified Forensic Computer Examiner |
| CFE | 1. Certified Financial Examiner (A certification offered by SOFE.) |
| | 2. Certified Fraud Examiner (A certification offered by ACFE.) |
| | 3. Computer Forensic Examination (A certification offered by CERI.) |
| CFFA | Certified Forensic Financial Analyst |
| CFI | Certified Forensic Investigator |
| CFS | Certified Fraud Specialists |
| CHFI | Computer Hacking Forensic Investigator |

| | |
|---|---|
| CIFI | 1. Certified Information Forensics Investigator (A certification offered by IISFA.)<br>2. Computer Information Forensics Investigator (A certification offered by IICTC.) |
| CIRA | Certified Insolvency and Restructuring Advisor |
| CIS | Computer Investigative Specialist |
| CISM | Certified Information Security Manager |
| CISSP | Certified Information Systems Security Professional |
| CIW | Certified Internet Web Professional |
| CompTIA | Computing Technology Industry Association |
| CPA | Certified Public Accountant |
| CPD | Continuous Professional Development |
| Cr.FA | Certified Forensic Accountant |
| CSFA | CyberSecurity Forensic Analyst |
| CSI | CyberSecurity Institute |
| CSIH | CERT-Certified Computer Security Incident Handler |
| $C^3E$ | Certified Cyber-Crime Expert |
| DEP | Digital Evidence Practitioner |
| DFCB | Digital Forensic Certification Board |
| E-BPS | E-Business Process Solutions |
| ECSAP | Electronic Crime Special Agent Program |
| EnCE | EnCase Certified Examiner |
| EC-Council | The International Council of Electronic Commerce Consultants |
| FBI | Federal Bureau of Investigation |
| FFI | Financial Forensics Institute |
| FLETC | Federal Law Enforcement Training Center |
| FTK | Forensic Toolkit |
| FOSS | Forensic Operating System Specialist |
| GCFA | GIAC Certified Forensics Analyst |
| GCUX | GIAC Certified UNIX Security Administrator |
| GCWN | GIAC Certified Windows Security Administrator |
| GED | General Education Requirement |
| GIAC | Global Information Assurance Certification |
| GISF | GIAC Information Security Fundamentals |
| GSE | GIAC Security Engineer |
| GSEC | GIAC Security Essentials Certification |
| GSI | Guidance Software Incorporation |
| GSLC | GIAC Security Leadership Certificate |
| HTCC | High Tech Crime Consortium |
| HTCI | High Tech Crime Institute |
| HTCIA | High Technology Crime Investigation Association |
| HTCN | High Tech Crime Network |

| | |
|---|---|
| IACIS | The International Association of Computer Investigative Specialists |
| ICFP | Institute of Computer Forensic Professionals |
| IICTC | International Information and Communication Technology Council |
| IISFA | International Information Systems Forensics Association |
| IRS | Internal Revenue Service |
| ISACA | Information Systems Audit and Control Association |
| $(ISC)^2$ | International Information Systems Security Certification Consortium |
| ISFCE | The International Society of Forensic Computer Examiners |
| ISSAP | Information Systems Security Architecture Professional |
| ISSEP | Information Systems Security Engineering Professional |
| ISSMP | Information Systems Security Management Professional |
| MCQ | Multiple-Choice Question |
| NACVA | National Association of Certified Valuation Analysts |
| NCFS | National Center of Forensic Science |
| NIJ | National Institute of Justice |
| PCI | Professional Certified Investigator |
| PCME | Paraben Certified Mobile Examiner |
| PDA | Personal Digital Assistant |
| PRTK | Password Recovery Toolkit |
| RSTP | Registered Training Service Provider |
| SANS Institute | SysAdmin, Audit, Network, Security Institute |
| SCNA | Security Certified Network Architect |
| SCNP | Security Certified Network Professional |
| SCNS | Security Certified Network Specialist |
| SCP | Security Certified Program |
| SOFE | Society of Financial Examiners |
| SSCP | Systems Security Certified Practitioner |
| USSS | United States Secret Service |

## ABOUT THE AUTHOR

**Nena Lim** joined the Swedish Business School at Örebro University, Sweden in January 2008. She received her Ph.D. from The University of Queensland, Australia. She also has an M.S. in Computer Information Systems from Georgia State University and an M.A. in Accounting and Finance from Lancaster University, United Kingdom. Her work focuses on Internet security, computer forensics, and digital piracy. She has published in *Communications of the ACM*, *Communications of the Association for Information Systems*, *Electronic Commerce Research and Applications*, *Australian Journal of Information Systems*, *Communications of the IBIMA*, and *Digital Investigation*. She can be contacted at nena.lim@oru.se.

Copyright © 2008 by the Association for Information Systems. 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 full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712 Attn: Reprints or via e-mail from ais@aisnet.org

Communications of the Association for Information Systems

ISSN: 1529-3181

**EDITOR-IN-CHIEF**
Joey F. George
Florida State University

**AIS SENIOR EDITORIAL BOARD**

| | | |
|---|---|---|
| Guy Fitzgerald<br>Vice President Publications<br>Brunel University | Joey F. George<br>Editor, CAIS<br>Florida State University | Kalle Lyytinen<br>Editor, JAIS<br>Case Western Reserve University |
| Edward A. Stohr<br>Editor-at-Large<br>Stevens Inst. of Technology | Blake Ives<br>Editor, Electronic Publications<br>University of Houston | Paul Gray<br>Founding Editor, CAIS<br>Claremont Graduate University |

**CAIS ADVISORY BOARD**

| | | | |
|---|---|---|---|
| Gordon Davis<br>University of Minnesota | Ken Kraemer<br>Univ. of Calif. at Irvine | M. Lynne Markus<br>Bentley College | Richard Mason<br>Southern Methodist Univ. |
| Jay Nunamaker<br>University of Arizona | Henk Sol<br>University of Groningen | Ralph Sprague<br>University of Hawaii | Hugh J. Watson<br>University of Georgia |

**CAIS SENIOR EDITORS**

| | | |
|---|---|---|
| Steve Alter<br>U. of San Francisco | Jane Fedorowicz<br>Bentley College | Jerry Luftman<br>Stevens Inst. of Tech. |

**CAIS EDITORIAL BOARD**

| | | | |
|---|---|---|---|
| Michel Avital<br>Univ of Amsterdam | Dinesh Batra<br>Florida International U. | Indranil Bose<br>University of Hong Kong | Ashley Bush<br>Florida State Univ. |
| Erran Carmel<br>American University | Fred Davis<br>U of Arkansas, Fayetteville | Gurpreet Dhillon<br>Virginia Commonwealth U | Evan Duggan<br>Univ of the West Indies |
| Ali Farhoomand<br>University of Hong Kong | Robert L. Glass<br>Computing Trends | Sy Goodman<br>Ga. Inst. of Technology | Mary Granger<br>George Washington U. |
| Ake Gronlund<br>University of Umea | Ruth Guthrie<br>California State Univ. | Juhani Iivari<br>Univ. of Oulu | K.D. Joshi<br>Washington St Univ. |
| Chuck Kacmar<br>University of Alabama | Michel Kalika<br>U. of Paris Dauphine | Claudia Loebbecke<br>University of Cologne | Paul Benjamin Lowry<br>Brigham Young Univ. |
| Sal March<br>Vanderbilt University | Don McCubbrey<br>University of Denver | Fred Niederman<br>St. Louis University | Shan Ling Pan<br>Natl. U. of Singapore |
| Kelly Rainer<br>Auburn University | Paul Tallon<br>Loyola College, Maryland | Thompson Teo<br>Natl. U. of Singapore | Craig Tyran<br>W Washington Univ. |
| Chelley Vician<br>Michigan Tech Univ. | Rolf Wigand<br>U. Arkansas, Little Rock | Vance Wilson<br>University of Toledo | Peter Wolcott<br>U. of Nebraska-Omaha |

**DEPARTMENTS**

| | |
|---|---|
| Global Diffusion of the Internet.<br>Editors: Peter Wolcott and Sy Goodman | Information Technology and Systems.<br>Editors: Sal March and Dinesh Batra |
| Papers in French<br>Editor: Michel Kalika | Information Systems and Healthcare<br>Editor: Vance Wilson |

**ADMINISTRATIVE PERSONNEL**

| | | |
|---|---|---|
| James P. Tinsley<br>AIS Executive Director | Robert Hooker<br>CAIS Managing Editor<br>Florida State Univ. | Copyediting by Carlisle<br>Publishing Services |



Communications of the Association for Information Systems