




Apr 24th, 10:30 AM

## Digital Forensic Certification Versus Forensic Science Certification

Nena Lim  
Örebro University, Sweden, nenalim@yahoo.com

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

---

### Scholarly Commons Citation

Lim, Nena, "Digital Forensic Certification Versus Forensic Science Certification" (2008). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 8.  
<https://commons.erau.edu/adfsl/2008/thursday/8>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact [commons@erau.edu](mailto:commons@erau.edu).

**EMBRY-RIDDLE**  
Aeronautical University™  
SCHOLARLY COMMONS

(c)ADFSL



# **Digital Forensic Certification versus Forensic Science Certification**

**Nena Lim**  
Örebro University  
Sweden  
nena.lim@oru.se

## **ABSTRACT**

Companies often rely on certifications to select appropriate individuals in disciplines such as accounting and engineering. The general public also tends to have confidence in a professional who has some kinds of certification because certification implies a standard of excellence and that the individual has expert knowledge in a specific discipline. An interesting question to the digital forensic community is: How is a digital forensic certification compared to a forensic science certification? The objective of this paper is to compare the requirements of a digital forensic certification to those of a forensic science certification. Results of the comparison shed lights on the maturity level of the digital forensic discipline and reveal what can be improved to enhance the confidence and trust of the general public on the digital forensic profession.

**Keywords:** certification, recertification, digital forensics, computer forensics, forensic science

## **1. INTRODUCTION**

The general public has confidence in professionals with certification because certification is a proof that individuals meet a minimum standard and are capable of doing their jobs properly. Such qualification is particularly important to digital forensic professionals because they often need to present as expert witnesses in courts where both their work, such as the methodology and tools used, and their qualifications are under close scrutiny (Nelson et al., 2005). It is noteworthy that collecting and analyzing digital evidence appropriately represent only part of a forensic investigation process. The expertise and qualification of the digital forensic investigators often could have a significant impact on the reliability of the findings in the eyes of judges and juries.

Despite the importance of certification to digital forensic professionals, no prior study has examined this issue. The objective of this paper is to compare the requirements of one of the digital forensic certifications to those of a closely related discipline -- forensic science. Results of the comparison shed lights on the maturity level of the digital forensic discipline and reveal what can be improved to enhance the confidence and trust of the general public on the digital forensic profession.

## **2. DIGITAL FORENSIC CERTIFICATION**

Digital forensic is the “process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable” (McKemmish, 1999). It emerged as a discipline in 1980s (Mohay et al., 2003). Unlike well-established disciplines such as accounting and engineering, digital forensics discipline has many certifications available. The variety of certification could be quite confusing even to the digital forensic professionals themselves. Some of the certifications include Certified Information Forensics Investigator (CIFI), Certified Computer Examiner (CFE), GIAC Certified Forensics Analyst (GCFA), just to name a few. With so many digital forensic certifications available, choosing a representative one is not an easy task. In this paper, we decided to use the number of certificate holders as an objective indicator of the representativeness of a certification. Unfortunately, most computer forensic certification granting bodies do not indicate their numbers of certificate holders on their web-sites. Based on the limited available information, we chose GIAC Certified Forensics Analyst (GCFA) because it has more than 1100 certificate holders and GIAC has certified

over 20,000 professionals.

GCFA is one of the certifications granted by Global Information Assurance Certification (GIAC). GIAC is a professional body established in 1999. It offers a suite of more than 20 certifications which cover expertise in computer security and digital forensics (Frisk, 2008). All GIAC certifications are structured across four levels (level 3 to level 6). As the coverage of each GIAC certification is rather specific, information systems or security professionals will have to obtain different certifications from GIAC to show they have knowledge in different areas. GCFA is a level 5 certification and it provides assurance that a certified individual has the knowledge and skills necessary to undertake forensic analysis and incident investigation.

### 3. FORENSIC SCIENCE CERTIFICATION

Similar to digital forensic, forensic science is the application of science to identify, preserve, analyze, and present evidence in a legally acceptable manner. The main difference between the two disciplines is that forensic science emphasizes physical evidence instead of digital evidence. The forensic science certification is chosen for comparison purposes because forensic science is closely related to digital forensics. It will be interesting to see how closely the certification requirements of these two relatively new disciplines match up to each other. Among the various forensic science certifications, the certification provided by the Board of Forensic Document Examiners (BFDE) is included in the comparison in this study because it is one of the six accredited boards under the Forensic Specialties Accreditation Board, Inc. (FSCB). (None of the FSCB accredited boards is related to digital forensic.) As the FSCB is sponsored by the American Academy of Forensic Sciences (AAFS), the National Forensic Science Technology Center (NFSTC), and the National Institute of Justice, certifications granted by the accredited boards under FSCB are likely to gain more confidence from the general public. We believe the BFDE was established around 2005 but the exact date is unclear.

### 4. CERTIFICATION COMPARISON

Table 1 summarizes the information of the GCFA and BC-BFDE certifications. According to their websites, in early 2008 the number of certificate holders of GCFA and BC-BFDE are 1134 and 15 respectively. Apart from the relatively longer history of GIAC, we believe the big discrepancy in number of certificate holders is also due to greater demand of digital forensic professionals and more stringent certification requirements of the BFDE.

Table 1: GCFA versus BC-BFDE

Discipline	Digital Forensic	Forensic Science
Certification Granting Association	Global Information Assurance Certification (GIAC)	Board of Forensic Document Examiners (BFDE)
URL	<a href="http://www.giac.org/">http://www.giac.org/</a>	<a href="http://www.bfde.org/">http://www.bfde.org/</a>
Certification title	GIAC Certified Forensics Analyst (GCFA)	Board Certified by the Board of Forensic Document Examiner (BC-BFDE)
Number of Certificate holders	1134	15
Levels of certification	Two (Silver and Gold)	One

*ADFSL Conference on Digital Forensics, Security and Law, 2008*

Application fee	None	\$100
Certification fee	Silver: \$899 (\$499 with SANS training, \$325 for recertification) Gold: \$299	\$500
Annual fee	None	None
Certification requirement	<p>Silver level:</p> <ul style="list-style-type: none"> <li>● Pass an online examination</li> </ul> <p>Gold level:</p> <ul style="list-style-type: none"> <li>● Silver certification</li> <li>● Complete a written technical report</li> </ul>	<ul style="list-style-type: none"> <li>● Baccalaureate degree (can be substituted by professional experience)</li> <li>● Basic training in forensic document examination including attendance as a spectator at a trial where a forensic document examiner presented expert witness testimony</li> <li>● Good moral character</li> <li>● Sign an agreement to abide by Code of Ethics and Code of Professional Responsibility</li> <li>● Two letters of recommendation</li> <li>● Satisfactorily pass a background check</li> <li>● Pass all examinations</li> <li>● Currently employed in the profession</li> </ul>
Examination structure	<p>Silver level:</p> <ul style="list-style-type: none"> <li>● A proctored open book online examination consisting of 150 multiple choice questions</li> <li>● 4 hours is allocated for the examination</li> <li>● Passing score is 70%</li> <li>● Must pass within 4 months upon account activation</li> </ul> <p>Gold level:</p> <ul style="list-style-type: none"> <li>● A satisfactory 20-page technical report</li> <li>● Must complete within 6 months</li> </ul>	<ul style="list-style-type: none"> <li>● A proctored written exam consists of around 250 multiple choice questions covering 9 sections of knowledge</li> <li>● A proctored performance examination</li> <li>● A total of 8 hours allocated for all examination</li> <li>● Study guide provided</li> <li>● No fixed passing score but applicants must pass all 9 sections</li> </ul>
Valid period	4 years	5 years

<p>Continuous professional development (CPD) requirement for recertification</p>	<p>No CPD, requires complete retesting after 4 years</p>	<ul style="list-style-type: none"> <li>● 60 credits of continuing forensic education (50 minutes education = 1 credit)</li> <li>● Undertake proficiency testing twice within 5 years (can be substituted by approved lab work)</li> <li>● Contributions to the profession (e.g., publication, presentation, participation in research)</li> <li>● Peer review audit</li> <li>● Currently working in the document examination profession</li> <li>● Renew pledge of Code of Ethics and Code of Professional Responsibility</li> </ul>
--	--	--

#### 4.1 Certification Requirements

GCFA offers two levels of certification (Silver and Gold) whereas BFDE offers only one level of certification. To obtain a GCFA Silver certification, applicants do not need to have any prior experience in digital forensic. All they have to do is pass an online examination. Certificate applicants have four months to complete the examination requirement upon their application submission for the certification. Certificate holders of GCFA Silver certification can advance to the Gold level if they complete a technical report under an advisor within 6 months.

The requirements set for a BC-BFDE certification are more comprehensive than those of GCFA. Apart from passing all examinations, certificate applicants generally need to have a baccalaureate degree although such educational requirement sometimes can be substituted by professional experience. BC-BFDE applicants need to show that they had basic training in forensic document examination prior to their application. This includes an attendance as a spectator at a trial where a forensic document examiner presented expert witness testimony. Moreover, applicants are expected to have good moral character and are required to sign an agreement to abide themselves by the Code of Ethics and Code of Professional Responsibility. All applicants need to pass a background check. They should also currently be employed in the profession and submitted two letters of recommendation.

#### 4.2 Examination Structure

Candidates of GIAC certification generally are expected to take training courses provided by the SANS (SysAdmin, Audit, Network, Security) Institute before they take certification examinations. For the GCFA certification, candidates are expected to take a course titled "System Forensics, Investigation & Response." Certificate applicants who obtain the GCFA certification without attending the SANS training are said to have passed the challenge certification. The certification fee for challenge applicants is \$899 but it is reduced to \$499 for applicants who have completed the SANS training. Topics covered in the SANS course include the following:

- Forensic definitions
- Incident response and volatile evidence gathering
- Core forensic methodology
- File system essentials and forensics

- Network forensics
- Timeline analysis
- Forensic toolkits
- Media analysis using the Sleuthkit
- Hash comparisons
- Autopsy forensic browser
- Windows forensic
- NTFS/FAT examination
- Application foot printing and analysis
- Legal consideration

The GCFA Silver level examination is a four-hour proctored online examination. The examination is open book and consists of 150 multiple choice questions. The passing score is 70 percent. The prerequisite for obtaining a GCFA gold certification is a GCFA silver certification. GCFA Gold level applicants are required to complete a 20-page technical report covering in digital forensic under the supervision of an adviser. Technical reports are evaluated using four criteria: technical accuracy, clear explanation of advanced concepts, extension of ideas beyond courseware, and organization of report.

The BFDE examination includes a proctored written examination and a proctored performance examination. The written examination lasts for four hours and includes around 250 multiple choice questions from the following nine sections. Certificate applicants need to pass all sections to obtain an overall pass but there is not a fixed passing score.

- Foundation skills
- Gathering evidence
- Analyzing handwriting
- Analyzing falsified documents
- Analyzing features of paper and media
- Analyzing impact and non-impact images
- Use of laboratory instruments
- Evaluating evidence and presenting case findings
- Demonstrating knowledge of legal procedures

In addition to the written examination, certificate applicants of BFDE also need to undertake a practical examination which requires candidates to conduct examination in a simulated case. During the practical examination, applicants are required to examine case documents, render an opinion, and provide an argument to support the opinion. The practical examination also lasts for four hours. Unlike GCFA, no course is provided specifically for the BFDE applicants. However, all BFDE applicants receive a study guide.

#### **4.3 Recertification Requirement**

To maintain the confidence of the general public and employers in their work, certified professionals in many disciplines these days are expected to keep abreast of the latest development and keep their skills and knowledge current. As a result, certification granting bodies often require its certificate holders to undergo some kinds of recertification process.

The validity period of the two certifications is similar. A GCFA certification is valid for four years whereas a BC-BFDE certification is valid for five years. Nevertheless, GCFA and BFDE adopt different approaches toward recertification as shown in Table 1. A certificate holder of GCFA needs to retake the complete certification examination every four years. Similar to its certification requirements, the BFCF has a comprehensive list of requirements for recertification. Certificate holders of BC-BFDE seek for recertification need to be currently working in the document examination profession. Moreover, they are required to take 60 credit hours of continuing forensic education and undertake proficiency test twice within five years. (It is, however, unclear how the proficiency examination is related to the normal certification examinations.) Recertification applicants need to show they have contributed to the profession through publication, presentation, or participation in research. More importantly, the BFDE has additional recertification requirements which involve monitoring the behavior of its certificate holders. First, BFDE certificate holders need to submit a transcript of two complete case files for a peer review audit. Second, if they render an opposite opinion in trial against another forensic expert in more than five occasions within a five-year period, the Board will appoint a review committee to review the certificate holders' work.

## **5. CONCLUSION**

The objective of the above certification comparison is to provide a glimpse of the current certification situation in digital forensic as well as a closely related discipline. For both digital forensic professionals and the other stakeholders in digital forensic such as employers, the above comparison results provide them with some ideas how the digital forensic discipline compared against other disciplines. Of course, with the variety of digital forensic certifications currently available, the comparison results are not meant to be definite. For example, while GCFA applicants do not need to have any relevant digital forensic experience, some digital forensic certifications such as Cyber Security Forensic Analyst (CSFA) and EnCase Certified Examiner (EnCE) have such requirements (Lim, 2008).

Overall, the comparison results show that certification requirements for a forensic science certification such as BC-BFDE are more stringent than those of a digital forensic certification both in terms of practical experience and practical examination. Moreover, the numerous specific digital forensic certifications could be quite confusing for other stakeholders of the discipline. For example, while GCFA covers incident response, GIAC offers a specific certification in that area titled GIAC Certified Incident Handler (GCIH). In fact, such an overlap can be confusing even for the security and digital forensics professional who do not hold those certifications. We believe that it might not be a bad idea for the digital forensic community to consider following an overall certification approach. That is, it might want to consider offering an overall certification but allowing its certificate holders to specialize in a specific area. In this way, the digital forensic certification might have a clearer identity. The general public might have more confidence in the discipline if more rigorous requirements on practical experience are set.

## **6. REFERENCES**

- Frisk, J. (2008) 'GIAC Program Overview,' <http://www.giac.org/overview/brief.pdf> (current Mar. 2, 2008)
- Lim, N. (2008) 'How to select a digital forensic certification: A difficult task made easy' Örebro University, Örebro, Working paper.
- 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., Anderson, A., Collie, B., de Vel, O., and McKemmish, R. (2003) *Computer and Intrusion Forensics*, Artech House, Norwood, MA.

Nelson, B., Phillips, A., Enfinger, F., and Steuart, C. (2005) *Guide to Computer Forensics and Investigations*, 2<sup>nd</sup> edition, Thomson Course Technology, Boston, Massachusetts.



