

DIGITAL FORENSICS CERTIFICATION BOARD

RECERTIFICATION POLICY

DFCB Board Policy

Every holder of a certificate issued by the Digital Forensics Certification Board must renew their certification every 36 months.

DFCB Board Requirements For Recertification

Every holder of a Digital Forensics Certified Practitioner certificate must satisfy the following requirements every 36 months. These requirements encompass a linear three step process:

- (1) The certificate holder must be current with their annual membership fees over the last 36 months,
- (2) Over the last 36 months the certificate holder must have been actively involved in the field of digital forensics and/or eDiscovery, and
- (3) The certificate holder must have accumulated a total of at least 36 CPE professional development credits over the previous 36 months.

The specifics of each of these three areas are detailed in the pages below. Note that the individual certificate holder is responsible for maintaining the documentation that establishes their compliance with items (2) and (3) above. The certificate holder will not be required to produce this documentation for review by the Board unless specifically requested by the recertification audit and compliance committee.

All certificate holders who are compliant with the above three requirements are granted the privilege of using the "DFCP" moniker and emblem as an indication of professional achievement in the field of digital forensics.

DFCB Board Oversight

The Executive Board reserves the right to review at its discretion and on-demand the supporting documents maintained by certificate holders that substantiate their compliance with the recertification process described above.

Failure to comply with these requirements will result in the suspension of the certification until such time as the Executive Board is satisfied that the process of reinstatement has been completed to the specifications described above. The reinstatement process is discussed on the last page of this document.

The Executive Board also reserves the right to establish a renewal date by which all re-certifications must be submitted and current.

Policy Parameter Definitions

CPE: One CPE credit is the equivalent of one hour of professional development. Fractional accumulations of CPE credit hours are permitted where necessary.

Membership fees: Membership fees are set by the Executive Board. As of 2011 annual dues are \$40 and due during the Month of January. The January payment covers membership fees for the remainder of that calendar year.

Recertification fees: There are no recertification fees.

Personal Attestation: It is the desire of the DFCB board to keep the paperwork associated with the recertification process to a minimum. As a result, certificate holders will be asked to attest to their active participation in the field and compliance with the 36 CPE credits without direct oversight by the Executive Board. This approach is also designed to compensate for those situations where the recertification requirements would require the disclosure of classified information and/or information covered by non-disclosure agreements.

Recertification Requirement #1: Membership Fees Must Be Current

There are no fees directly associated with the recertification process. There are no charges or fees that the certificate holder must pay to become recertified. Membership fees are required on an annual basis and must be paid during the month of January. Annual membership fees are \$40. Dues are delinquent after March 31 and a Reinstatement fee \$20.00 will apply. All fees are non-refundable once paid.

Recertification Requirement #2: Active Participation In The Field

To standardize the recertification process the Executive Board will provide a spreadsheet that certificate holders can download from the DFCB Web site that can be used to calculate if the hours of experience accumulated over the past 36 months to meet the requirements of this section.

The certificate holder must personally attest that their experience in the fields of Digital Forensics and/or eDiscovery (over the last 36 months) qualifies under one or more of the following three categories:

- (1) Over the last 36 months the certificate holder has accumulated at least 48 hours performing digital acquisitions and 144 hours analyzing digital evidence. Analysis includes but is not limited to forensic assessments, research, report writing, case management, testimony and briefings conducted. 192 hours in total are required to satisfy this requirement at the 100% level.¹
- (2) Over the last 36 months the certificate holder has directly supervised at least 96 hours of digital acquisitions and 288 hours analyzing digital evidence. Hours accumulated in this category can be acquired concurrently during the supervision of multiple staff. Supervisory analysis includes but is not limited to creating action plans, monitoring project goals and deliverables, monitoring employee performance, supervising forensic assessments, research, report writing, case management, testimony and briefings conducted. . 384 hours in total are required to satisfy this requirement at the 100% level²

¹ Assume 8 cases every two years as an average for most practitioners. Further assume that an average case lasts three days, of which 25% of the time is spent performing digital acquisitions at some level and 75% is spent performing some form of forensic analysis or case management. The numbers provided are then based on: 8 cases x 3 days x 8 hours per day = 192 hours, 192 x 25% = 48 hours, 192 x 75% = 144 hours.

² Assumes that the supervisor is supervising at least two staff members. As a result, the hours required are two times greater than that of the individual practitioner.

DFCB Recertification Policy (Version 2.6)

- (3) Over the last 36 months the certificate holder has spent at least 96 hours in a classroom environment instructing formal training classes on topics related to digital forensics or eDiscovery. 96 hours in total are required to satisfy this requirement at the 100% level.³
- (4) If certificate holders are aware that they will be unable to accumulate the “experience” hours required during the 36 month recertification period they can substitute the time lacking with hours spend developing a “test” case image that other DCFB members can use for training purposes. The time spent developing these test case(s) should be approximately equal to the time they were not able to accumulate under the experience hours. Certificate holders will be required to submit their test case images to the recertification committee, along with a description of the case and a list of items that should be discovered by the analyst during their examination. Once the test case is accepted by the recertification committee and approved by the Executive Board the hours spent creating the test case images(s) will be applied as “experience” hours.
- (5) The DFCB Executive Board recognizes that it cannot realistically anticipate all the different job responsibilities that a certificate holder may have in the area of digital evidence or eDiscovery. It further realizes that a certificate holder may be actively involved in the practice of digital evidence or eDiscovery that may not fall within the work "experience" parameters outlined above. If a certificate holder believes that their work "experiences" are unique and not a currently recognized category of "experiences" they may petition the recertification committee for consideration and request that their unique work "experiences" be applied towards their recertification requirements. Such petitions must be in writing and filed with the recertification committee at least six months prior to the end of the certificate holder's 36 month recertification period. The recertification committee will review all such petitions within 45 days of filing and issue a finding within 60 days of such filing. Findings approved by the Board will allow the petitioner to apply their unique “experiences” as qualifying hours for the current 36 month recertification period, as well as all future recertification periods.”

Satisfying the requirements of the above five categories can be completed by partially satisfying the hours required in each category as long as the total hours accumulated represent 100%. For example, a certificate holder may accumulate the following: 9.6 hours of individual acquisitions, 28.8 hours of individual analysis, 19.2 hours of supervised acquisitions, 57.6 hours of supervised analysis and 19.2 hours of classroom training.

Breaking these hours into a percentage of required hours results in: $(9.6 / 48 = 20\%)$, $(28.8 / 144 = 20\%)$, $(19.2 / 96 = 20\%)$, $(57.6 / 288 = 20\%)$ and $(19.2 / 96 = 20\%)$. Since the percentages add up to 100% the certificate holder has demonstrated that he/she is an active participant in the digital forensics arena by partially satisfying each of the three experience categories.

Recertification Requirement #3: Accumulation Of 36 CPE Credits

To standardize the recertification process the Executive Board will provide a spreadsheet that certificate holders can download from the DFCB Web site and use to track the CPE credits they have accumulated over the past 36 months.

³ Informal briefings do not qualify as formal training sessions. Assumes that the training class instructed lasted 3 days with 8 hours of scheduled training per day and the training is conducted once every 6 months. The numbers provided are based on: 4 courses over two years x 3 days each x 8 hours per day = 96 hours

DFCB Recertification Policy (Version 2.6)

In addition to the above professional experience requirements the certificate holder must be able to demonstrate that they have earned at least 36 CPE credit hours over the last 36 months by any combination of the following:

- One CPE credit for each hour of training attended in the Digital Forensics or eDiscovery field, subject to the review and approval of the Recertification Committee and the Executive Board. Training may include;
 - Attendance at Digital Forensics or eDiscovery conferences or seminars regularly associated with the field such as but not limited to: HTCIA, ISSA, CEIC, LegalTech, DOJ CyberCrime and conferences hosted by forensic vendors.
 - Attendance at formal training classes in the Digital Forensics or eDiscovery field such as but not limited to: SEARCH, National White Collar Crime Center, Local, Federal or State sponsored training for Law Enforcement or Private Investigators.
 - Attendance at training meetings of professional organizations such as but not limited to: HTCIA, ISSA, IACIS, and (ISC)2.
 - Completion of on-line training courses or seminars relevant to the field.
- 72 CPE credits for being the primary author of a new book published by a recognized publisher that furthers the literature in the field of digital forensics. The 36 credits which are not required for this period's certification carry-over into to the next 36 month recertification cycle.
- 36 CPE credits for being the co-author of a new book published by a recognized publisher that furthers the literature in the field of digital forensics.
- 36 CPE credits for participation in a DCFB research project involving 3-5 members and which produces a relevant research paper or technical article of at least 20 pages (12 pt) on a topic relevant to Digital Forensics or eDiscovery matters.
- 36 CPE credits for successfully completing a formal college course related to digital forensic taught on a semester level basis.⁴ Certificate holder must be able to demonstrate that he/she received a "B" or better in the course.
- 18 CPE credits for successfully completing a formal college course related to digital forensic taught at the quarter level basis.⁵ Certificate holder must be able to demonstrate that he/she received a "B" or better in the course.
- 18 CPE credits for participation in a DCFB research paper or technical article involving 3-5 members and which produces a relevant research paper of at least 10 pages (12 pt) on a topic relevant to Digital Forensics or eDiscovery matters.
- 8 CPE credits for being the sole author of an article published in a peer reviewed journal that furthers the literature in the field of digital forensics.
- 4 CPE credits for being the co-author of an article published in a peer reviewed journal that furthers the literature in the field of digital forensics.

⁴ Assumes course meets 3 times a week for 16 weeks.

⁵ Assumes class meets 3 times a week for 12 weeks.

DFCB Recertification Policy (Version 2.6)

- ☐ 0.25 CPE credits for every 15 minutes a certificate holder participates as a listener in a podcast event related to the field of digital forensics.
 - ☐ One CPE credits for each hour of instruction provided to practitioners in the field on topics relevant to Digital Forensics or eDiscovery.
 - ☐ One CPE credits for each hour of instruction development in the field on topics relevant to Digital Forensics or eDiscovery.
 - ☐ One CPE for every hour of testimony or deposition on Digital Forensic or eDiscovery matters. ☐
- One CPE credit for each hour of participation on a DFCB committee.

Reinstatement Policy

If the holder of a DFCB Certification allows his/her certification currency to lapse, he/she must satisfy the following requirements to reinstate it:

1. Bring their membership fees, from the last point in time when their dues were current, to the current time period where reinstatement is being requested from the Executive Board.⁶
2. Document and attest to having currency in the field over the preceding 36 months as required under “Recertification Requirement #2” above.
3. Document and attest to having completed at least 36 CPE requirements as required under “Recertification Requirement #3” above.

Once the reinstatement requirements are met and the Board has no objections, the holder of a DFCB Certification is deemed recertified and may again exercise the privileges and responsibilities of the DFCB certification.

⁶ Example: If a member lets their membership dues lapse for two years and in Feb. of the third year requests reinstatement from the Board, that individual will be required to pay the fees for the last two years as well as the current year.