DEPARTMENT OF DEFENSE CYBER CRIME CENTER (DC3)

Operating since 1998, DC3 provides digital and multimedia (D/MM) forensics, cyber investigative training; research, development, test and evaluation (RDT&E); and cyber analytics to DoD computer network defense (CND), law enforcement (LE), intelligence community (IC), counterintelligence (CI) and counterterrorism (CT) agencies. DC3 is recognized as a national cyber center in NSPD 54/HSPD 23 and serves as the operational focal point for the Defense Industrial Base (DIB) Cybersecurity and Information Assurance DIB CS/IA Program.

Mission Statement

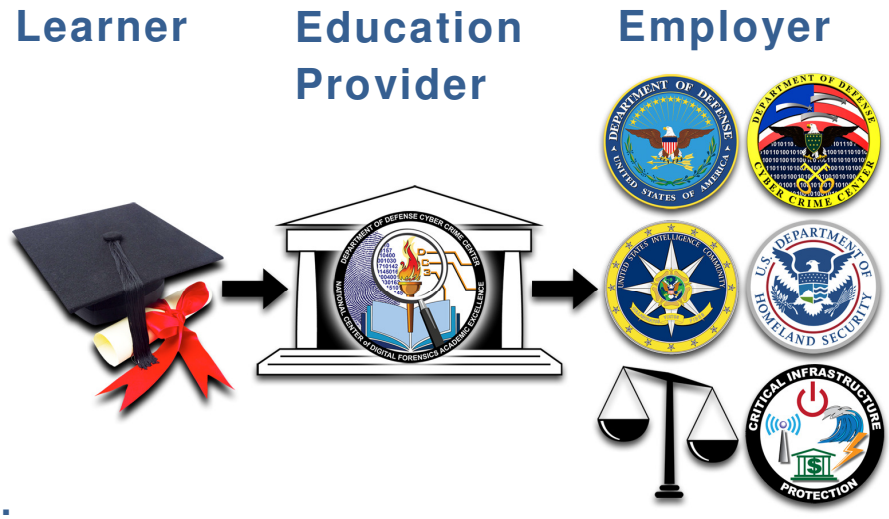
Develop a partnership between academia, standards bodies, and the US Government to establish standards and best practices for digital forensics practitioners, educators, and researchers to advance the discipline of Digital Forensics and increase the number of qualified professionals to meet the needs of law enforcement, counterintelligence, national defense and legal communities.

Value Added

- Establish a common core curriculum and development of standards for education and training in Digital Forensics studies.
- CDFAE designation requires in-course peer reviews of curriculum and practicum within a three year period.
- Education model based upon core learning objectives progressing to topic driven research.
- Provides an opportunity for students to demonstrate their knowledge and skills in Digital Forensics
- Provides employers capacity to confirm a candidate's capability to apply their knowledge.
- Develops a certifiable path to meet National Cyber needs.
- Strengthens bonds between Government, Academia, Professional Organizations, and Industry.

Why CDFAE?

The United States is in a Science, Technology, Engineering, and Mathematics (STEM) skills deficit. More than ever, organizations need to plan for the future as significant shifts in cyber operations accelerate globally. Digital Forensics skill sets provide cross-cutting application to multiple fields. Digital Forensics, in its strictest connotation, the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony. Beyond traditional legal purposes, the same techniques, scientific rigor, and procedural precision now support the range of military operations and courses of action (e.g., computer network operations as well as CI objectives). CDFAE serves as a prime avenue for cultivating leaders to meet evolving objectives across the digital forensics and cyber communities, and is vital to protect, investigate, and serve public, private and national goals.



Students:

- Accredited skill set and awareness of current issues facing Digital Forensics investigators and examiners.
- Opportunity to be recognized where their skills can be of the greatest value.
- Valued for highly desirable and unique skill sets.
- The capability to use the current techniques, skills, and tools necessary for digital forensic examination of digital media, files, operating systems, devices, networks, and applications for discovery and recovery of evidence.
- The aptitudes to design, implement, and evaluate a system, process, component, or program to meet digital forensic needs.
- An appreciation of professional, ethical, legal, security, social, and continuing education and development responsibilities.

Education Providers:

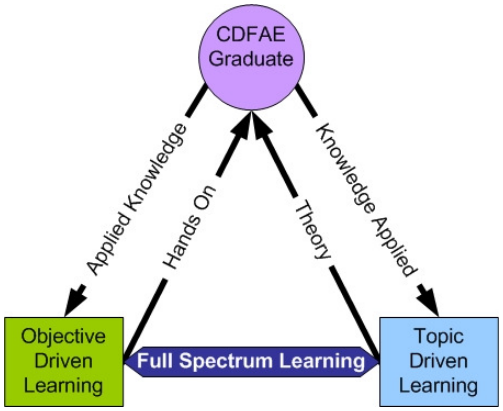
- Access to advanced digital forensic resources.
- Educators are recognized as being capable of effectively delivering theory, and practicum.
- Provide students greater access to unique internship or employment opportunities.

Employers:

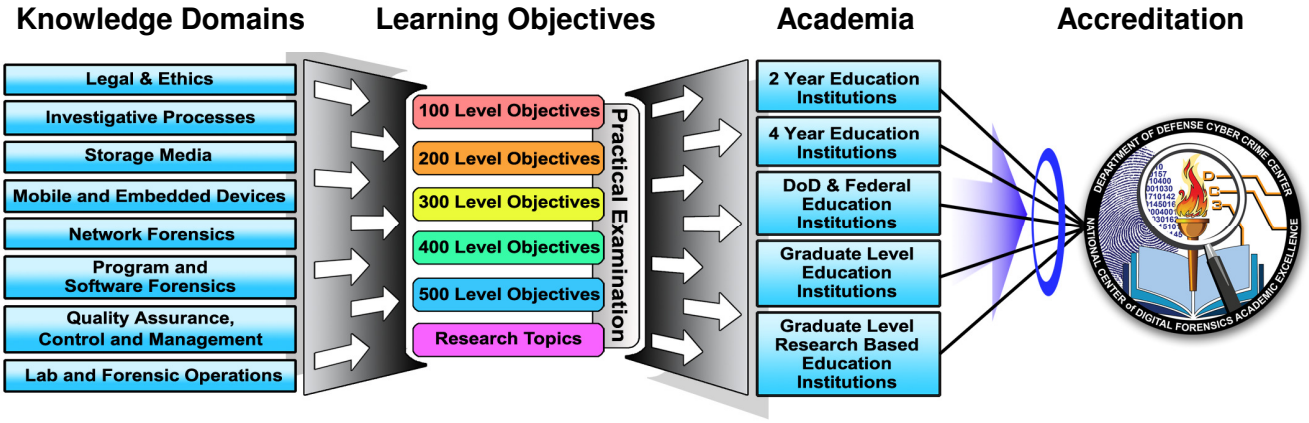
- Hire employees with validated skill sets capable of being on task day 1.
- Understand exactly what skills the employee brings to bear.
- Be able to diversify geographical hires without compromising quality.

How CDFAE is designed?

CDFAE focuses upon building core Knowledge Domains at multiple Skill and Ability levels across the education spectrum. CDFAE accredits DoD and Federal education organizations, and Academia to a Digital Forensic Education standard based upon Knowledge, Skills, and Abilities (KSA) utilized in field. It is an objective driven program which progresses to topic based research and problem solving. The CDFAE program is designed to create an applied knowledge (Hands-On) to knowledge applied (theoretical and research) educational mechanism with a clear progression between the training and education dichotomy in workforce development.



The eight Knowledge Domains represent well rounded digital forensics education topics field and the Learning Objective Levels are indicative elements of those topics. The program must provide structured advanced academic, research, and development capabilities in any or all of the digital forensics knowledge domain areas under the LOF at a level appropriate for the current curriculum of participating educational institutes while enhancing and providing supplemental support towards digital forensic objectives. This is accomplished by transitioning general knowledge areas to a specific topic application.



Institutions desiring CDFAE accreditation will fall into four main categories based upon the type of institution. These categories are:

- United States Federal or Defense Institutions
- 2-year programs such as community colleges
- 4-year bachelor's degree-granting institutions
- Graduate schools

Each subsequent category either includes or assumes the requirement of knowledge from the preceding categories and/or levels.

CDFAE Contact Information: *Email:* CDFAE@dc3.mil *Office:* 410-981-3121