Hewlett Packard Enterprise

CCFP—Certified Cyber Forensics Professional H0DU6S

This course provides a comprehensive review of cyber forensic concepts and industry best practices, covering the six domains of the CCFP CBK: Legal and ethical principles, investigations, forensic science, digital forensics, application forensics, hybrid and emerging technologies.

HPE course number	H0DU6S
Course length	5 Days
Delivery mode	ILT
View schedule, local pricing, and register	**View now**
View related courses	**View now**

Why HPE Education Services?

- IDC MarketScape leader 4 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and (ISC)²
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, January 2016

Audience

The course is intended for intermediate to advanced cyber forensics professionals who have at least three years of recent full-time digital or IT security experience in cyber forensics. The CCFP CBK defines the work experience as pertaining to cyber/digital forensics, legal investigation, or application forensics. It builds on and brings together the holistic view of the cyber forensics topics covered in the everyday environment of corporate, legal, law enforcement, and government occupations. Forensics experience is highly recommended for the successful completion of the course.

Examples of work experience may include:

- Digital forensic examiners in law enforcement supporting criminal investigations
- Cybercrime and cybersecurity professionals working in the public or private sectors
- Computer forensic engineers and managers working in corporate information security
- Digital forensic and e-discovery consultants focused on litigation support
- Cyber intelligence analysts working for defense/intelligence agencies
- Computer forensic consultants working for management or specialty consulting firms

Course description

The course is a combination of instructor lecture, hands-on lab exercises, instructor demonstrations, and practicum exam with after-exam review. The course instructors are (ISC)²-qualified cyber forensics professionals from law enforcement, academia, government service, and the private sector. The lab exercises include computer forensics using commercial tools, network forensics and Internet forensics. Such areas as email, applications, forensic timeliners, social media, and mobile devices will be addressed in addition to the traditional computer forensics examinations. Outside of the laboratory exercises, students address legal and ethical considerations, the foundations of digital forensic science within the context of the forensic sciences, and emerging and hybrid technologies as they impact the digital forensic investigator.

Course objectives

After completing this workshop, participants will be able to:

- Analyze the nature of evidence, chain of custody, rules of procedure, and the role of expert witness as they pertain to the legal and ethical principles, concepts, methodologies, and their implementation within centralized and decentralized environments across an organization's computing environment

- Demonstrate an understanding of investigations as they relate to data communications in local area and wide area networks, remote access, and Internet/intranet/extranet configurations
- Analyze fundamental principles, forensic methods, forensic analysis, and examination planning, and evaluate report writing and presentations as they relate to forensic science, applying a broad spectrum of science and technologies to investigate and establish facts in relation to criminal or civil law
- Analyze media and file systems, computer and operating systems, network, mobile devices, embedded devices, multimedia and content, virtual system forensics, and the techniques and tools used in the collection of any digital evidence that can be defined as data or transmitted via electronic means
- Apply software forensics to file formats and metadata, analyze web, email, and messaging forensics; and understand database forensics and malware forensics
- Describe the developing technologies and the practice of applying comprehensive and rigorous methods for collecting evidence within the hybrid and emerging technologies of cloud forensics, social networks, the big data paradigm, controls systems, critical infrastructure, and online gaming and virtual/augmented reality

Benefits to you

This course will help candidates review and refresh their cyber forensic and help identify areas they need to study for the CCFP exam and features:

- Official (ISC)² courseware
- Taught by an authorized (ISC)² instructor
- Student handbook and laboratory handbook
- Collaboration with classmates
- Real-world learning activities and scenarios
- Live, hands-on labs

Detailed course outline

Domain 1: Legal and ethical principles	Addresses ethical behavior and compliance with regulatory frameworks • Analyze the nature of evidence and its characteristics • Analyze the chain of custody • Analyze the significance of rules of procedure • Analyze the role of expert witness • Apply codes of ethics
Domain 2: Investigations	Encompasses the investigative measures and techniques required to gather digital evidence • Analyze the investigative process • Analyze evidence management • Analyze criminal investigations • Analyze civil investigations • Analyze administrative investigations • Analyze forensic response to security incidents • Analyze electronic discovery • Analyze Intellectual Property (IP) investigation
Domain 3: Forensic science	Entails applying a broad spectrum of sciences and technologies to investigate and establish facts in relation to criminal or civil law • Analyze fundamental principles • Analyze forensic methods • Analyze forensic analysis and examination planning • Evaluate report writing and presentation • Analyze quality assurance, control, management, and accreditation procedures
Domain 4: Digital forensics	Refers to the collection of any digital evidence which can be defined as data stored or transmitted via electronic means • Analyze media and file system forensics • Analyze computer and operating systems forensics • Analyze network forensics • Apply mobile device forensics • Understand embedded device forensics • Apply multimedia and content forensics • Apply virtual system forensics • Analyze forensic techniques and tools • Understand anti-forensic techniques and tools
Domain 5: Application forensics	Addresses the forensics complexities of the many application types that a CCFP candidate may encounter during a forensic investigation • Apply software forensics • Analyze web, email, and messaging forensics • Understand database forensics • Understand malware forensics
Domain 6: Hybrid and emerging technologies	Contains the ever evolving technologies that the CCFP candidate is expected to have a sound understanding of • Understand cloud forensics • Understand social networks • Understand the big data paradigm • Understand control systems • Understand critical infrastructure • Understand online gaming and virtual/augmented reality

Learn more at
hpe.com/ww/learnsecurity

Follow us:

© Copyright 2015–2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. The OpenStack Word Mark is either a registered trademark/service mark or trademark/service mark of the OpenStack Foundation, in the United States and other countries and is used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation or the OpenStack community. Pivotal and Cloud Foundry are trademarks and/or registered trademarks of Pivotal Software, Inc. in the United States and/or other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other third-party trademark(s) is/are property of their respective owner(s).

c04755692, October 2016, Rev. 3

Hewlett Packard
Enterprise