EC-Council – Computer Hacking Forensic Investigator Certification (CHFI)

EC-Council – Computer Hacking Forensic Investigator Certification (CHFI v10)

За Курса

Computer hacking forensic investigation is the process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks.

Computer crime in today’s cyber world is on the rise. Computer Investigation techniques are being used by police, government, and corporate entities globally and many of them turn to EC-Council for our Digital Forensic Investigator CHFI Certification Program.

Computer Security and Computer investigations are changing terms. More tools are invented daily for conducting Computer

Investigations, be it computer crime, digital forensics, computer investigations, or even standard computer data recovery. The tools and techniques covered in EC-Council’s CHFI program will prepare the student to conduct computer investigations using ground-breaking digital forensics technologies.

Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. CHFI investigators can draw on an array of methods for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information known as computer data recovery.

Цели – Какво ще научите (Course Goals):

What You Will Learn ?

Perform incident response and computer forensics	Identify data, images and/or activity which may be the target of an internal investigation
Perform electronic evidence collections	Establish threat intelligence and key learning points to support pro-active profiling and scenario modelling
Perform digital forensic acquisitions as an analyst	Search file slack space where PC type technologies are employed

Perform bit-stream Imaging/acquiring of the digital media seized during the process of investigation.	File MAC times (Modified, Accessed, and Create dates and times) as evidence of access and event sequences
Examine and analyze text, graphics, multimedia, and digital images	Examine file type and file header information
Conduct thorough examinations of computer hard disk drives, and other electronic data storage media	Review e-mail communications including web mail and Internet Instant Messaging programs
Recover information and electronic data from computer hard drives and other data storage devices	Examine the Internet browsing history
Follow strict data and evidence handling procedures	Generate reports which detail the approach, and an audit trail which documents actions taken to support the integrity of the internal investigation process
Maintain audit trail (i.e., chain of custody) and evidence integrity	
Work on technical examination, analysis, and reporting of computer-based evidence	Recover active, system and hidden files with date/time stamp information
Prepare and maintain case files	Crack (or attempt to crack) password protected files
Utilize forensic tools and investigative methods to find electronic data, including	Perform anti-forensics detection

Internet use history, word processing documents, images, and other files	Maintain awareness and follow laboratory evidence handling, evidence examination, laboratory safety, and laboratory security policy and procedures
Gather volatile and non-volatile information from Windows, MAC, and Linux	Play a role of the first responder by securing and evaluating a cybercrime scene, conducting preliminary interviews, documenting a crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, reporting of the crime scene
Recover deleted files and partitions in Windows, Mac OS X, and Linux	Perform post-intrusion analysis of electronic and digital media to determine the who, where, what, when, and how the intrusion occurred
Perform keyword searches including using target words or phrases	Apply advanced forensic tools and techniques for attack reconstruction
Investigate events for evidence of insider threats or attacks	Perform fundamental forensic activities and form a base for advanced digital forensics
Support the generation of incident reports and other collateral	Identify and check the possible source/incident origin
Investigate and analyze all response activities related to cyber incidents	Perform event co-relation

Plan, coordinate and direct recovery activities and incident analysis tasks	Extract and analyze logs from various devices such as proxies, firewalls, IPSs, IDSes, Desktops, laptops, servers, SIM tools, routers, switches, AD servers, DHCP servers, Access Control Systems, etc.
Examine all available information and supporting evidence or artifacts related to an incident or event	Ensure that reported incident or suspected weaknesses, malfunctions and deviations are handled with confidentiality
Collect data using forensic technology methods in accordance with evidence handling procedures, including a collection of hard copy and electronic documents	Assist in the preparation of search and seizure warrants, court orders, and subpoenas
Conduct reverse engineering for known and suspected malware files	Provide expert witness testimony in support of forensic examinations conducted by the examiner
Perform detailed evaluation of the data and any evidence of activity in order to analyze the full circumstances and implications of the event	

Формат на курса (Course Format):

[table id=1 /]

Език на курса (Course Language Option)

[table id=2 /]

Може да изберете Език на който да се проведе обучението – български или английски. Всичките ни инструктори владеят свободно английски език.

Учебни Материали (Student Guides):

Учебните материали са достъпни в електронен формат. Могат да се ползват online/offline на всяко устройство. Доживотен достъп.

Лабораторна среда (Lab Environment):

Всеки курсист разполага със собствена лаб среда, където се провеждат упражненията, част от курса.

Не е необходимо да инсталирате софтуер на компютър или специални изисквания за хардуер.

Участниците в присъствен формат в Учебния ни център разполагат с индивидуален компютър по време на обучението.

След завършване получавате (At Course Completion):

[table id=3 /]

Доживотен достъп до видео архив с запис на всяка отделна лекция.

Официален международно признат сертификат за завършен курс на обучение.

Продължителност (Course Duration):

- 5 работни дни (понеделник – петък 09:00 – 17:00)

или

- **40 уч.ч. обучение (теория и практика) в извънработно време с продължителност 1 седмици**
- събота и неделя 10:00 – 14:00, 14:00 – 18:00, 18:00 – 22:00
- понеделник и сряда 19:00 – 23:00

- вторник и четвъртък 19:00 – 23:00

Плащане

Заявка за издаване на фактура се приема към момента на записването на съответния курс.

Фактура се издава в рамките на 7 дни от потвърждаване на плащането.

Предстоящи Курсове

[tribe_events_list category=”ceh”]

За повече информация използвайте формата за контакт.

Ще се свържем с Вас за потвърждаване на датите.

Предпоставки (Изисквания) за Участие (Prerequisites):

- If a candidate have completed an official EC-Council training either at an Accredited Training Center, via the iClass platform, or at an approved academic institution, the candidate is eligible to attempt the relevant EC-Council exam without going through the application process.

Курсът подготвя за следните сертификационни нива

- CHFI (Exam Voucher Included). IT-Training.pro is an authorized EC-Council Test Center. You can take the exam with us, after the training.
- The CHFI certification is awarded after successfully passing the exam EC0 312-49. CHFI EC0 312-49 exams are available at ECC exam center around the world. In order to maintain the high integrity of our certifications exams, EC-Council Exams are provided in multiple forms (I.e. different question banks). Each form is carefully analyzed through beta testing with an appropriate sample group under the purview of a committee of subject matter experts that ensure that each of our exams not only has academic rigor but also has “real world” applicability. We also have a process to determine the difficulty rating of each question. The individual rating then contributes to an overall “Cut Score” for each exam form. To ensure each form has equal assessment standards, cut scores are set on a “per exam form” basis. Depending on which exam form is challenged, cut scores can range from 60% to 78%.