

EC-Council Computer Hacking Forensics Investigator (CHFI) v9.0

Prehľad

This course will provide participants the necessary skills to identify an intruders footprints and to properly gather the necessary evidence to prosecute in the court of law.

Vzdelávacie ciele

Computer forensics enables the systematic and careful identification of evidence in computer related crime and abuse cases. This may range from tracing the tracks of a hacker through a client's systems, to tracing the originator of defamatory emails, to recovering signs of fraud.

Computer Forensics and Investigations as a Profession

- Understanding Computer Forensics
- Comparing Definitions of Computer Forensics
- Exploring a Brief History of Computer Forensics
- Developing Computer Forensics Resources
- Preparing for Computing Investigations
- Understanding Enforcement Agency Investigations
- Understanding Corporate Investigations
- Maintaining Professional Conduct

Understanding Computer Investigations

- Preparing a Computer Investigation
- Examining a Computer Crime
- Examining a Company-Policy Violation
- Taking a Systematic Approach
- Assessing the Case
- Planning Your Investigation
- Securing Your Evidence
- Understanding Data-Recovery Workstations and Software
- Setting Up Your Workstation for Computer Forensics
- Executing an Investigation
- Gathering the Evidence
- Copying the Evidence Disk
- Analyzing Your Digital Evidence
- Completing the Case
- Critiquing the Case

[Online registrácia](#)

Termíny

Trvanie kurzu (v dňoch): 5 Days

G2R = "Garantovaný termín" | OLL = "Online LIVE"
ILT = "Kurz vedený inštruktorom"

06/10/19	G2R	3:00PM - 11:00PM	Bratislava, Slovakia	OLL	€ 2300.00
10/21/19	G2R	3:00PM - 11:00PM	Bratislava, Slovakia	OLL	€ 2300.00

Working with Windows and DOS Systems

- Understanding File Systems
- Understanding the Boot Sequence
- Examining Registry Data
- Disk Drive Overview
- Exploring Microsoft File Structures
- Disk Partition Concerns
- Boot Partition Concerns
- Examining FAT Disks
- Examining NTFS Disks
- NTFS System Files
- NTFS Attributes
- NTFS Data Streams
- NTFS Compressed Files
- NTFS Encrypted File Systems (EFS)
- EFS Recovery Key Agent
- Deleting NTFS Files
- Understanding Microsoft Boot Tasks
- Windows XP, 2000, and NT Startup
- Windows XP System Files
- Understanding MS-DOS Startup Tasks
- Other DOS Operating Systems

Macintosh and Linux Boot Processes and Disk Structures

- Understanding the Macintosh File Structure
- Understanding Volumes
- Exploring Macintosh Boot Tasks
- Examining UNIX and Linux Disk Structures
- UNIX and Linux Overview
- Understanding modes
- Understanding UNIX and Linux Boot Processes
- Understanding Linux Loader
- UNIX and Linux Drives and Partition Scheme
- Examining Compact Disc Data Structures
- Understanding Other Disk Structures
- Examining SCSI Disks
- Examining IDE/EIDE Devices

The Investigators Office and Laboratory

Understanding Forensic Lab Certification Requirements
Identifying Duties of the Lab Manager and Staff
Balancing Costs and Needs
Acquiring Certification and Training
Determining the Physical Layout of a Computer Forensics Lab
Identifying Lab Security Needs
Conducting High-Risk Investigations
Considering Office Ergonomics
Environmental Conditions
Lighting
Structural Design Considerations
Electrical Needs
Communications
Fire-suppression Systems
Evidence Lockers
Facility Maintenance
Physical Security Needs
Auditing a Computer Forensics Lab
Computer Forensics Lab Floor Plan Ideas
Selecting a Basic Forensic Workstation
Selecting Workstations for Police Labs
Selecting Workstations for Private and Corporate Labs
Stocking Hardware Peripherals
Maintaining Operating Systems and Application Software Inventories
Using a Disaster Recovery Plan
Planning for Equipment Upgrades
Using Laptop Forensic Workstations
Building a Business Case for Developing a Forensics Lab
Creating a Forensic Boot Floppy Disk
Assembling the Tools for a Forensic Boot Floppy Disk
Retrieving Evidence Data Using a Remote Network Connection

Current Computer Forensics Tools

Evaluating Your Computer Forensics Software Needs
Using National Institute of Standards and Technology (NIST) Tools
Using National Institute of Justice (NIJ) Methods
Validating Computer Forensics Tools
Using Command-Line Forensics Tools
Exploring NTI Tools
Exploring Ds2dump
Reviewing DriveSpy
Exploring PDBlock
Exploring PDWipe
Reviewing Image
Exploring Part
Exploring SnapBack DatArrest
Exploring Byte Back
Exploring MaresWare
Exploring DIGS Mycroft v3
Exploring Graphical User Interface (GUI) Forensics Tools
Exploring AccessData Programs
Exploring Guidance Software EnCase
Exploring Ontrack
Using BIAProtect
Using LC Technologies Software
Exploring WinHex Specialist Edition
Exploring DIGS Analyzer Professional Forensic Software
Exploring ProDiscover DFT
Exploring DataLifter
Exploring ASRData
Exploring the Internet History Viewer
Exploring Other Useful Computer Forensics Tools
Exploring LTOOLS
Exploring Mtools
Exploring R-Tools
Using Explore2fs
Exploring @stake
Exploring TCT and TCTUTILs
Exploring ILook
Exploring HashKeeper
Using Graphic Viewers
Exploring Hardware Tools
Computing-Investigation Workstations
Building Your Own Workstation
Using a Write-blocker
Using LC Technology International Hardware
Forensic Computers
DIGS
Digital Intelligence
Image MASSter Solo
FastBloc
Acard
NoWrite
Wiebe Tech Forensic DriveDock
Recommendations for a Forensic Workstation

Digital Evidence Controls

- Identifying Digital Evidence
- Understanding Evidence Rules
- Securing Digital Evidence at an Incident Scene
- Cataloging Digital Evidence
- Lab Evidence Considerations
- Processing and Handling Digital Evidence
- Storing Digital Evidence
- Evidence Retention and Media Storage Needs
- Documenting Evidence
- Obtaining a Digital Signature

Processing Crime and Incident Scenes

- Processing Private-Sector Incident Scenes
- Processing Law Enforcement Crime Scenes
- Understanding Concepts and Terms Used in Warrants
- Preparing for a Search
- Identifying the Nature of the Case
- Identifying the Type of Computing System
- Determining Whether You Can Seize a Computer
- Obtaining a Detailed Description of the Location
- Determining Who Is in Charge
- Using Additional Technical Expertise
- Determining the Tools You Need
- Preparing the Investigation Team
- Securing a Computer Incident or Crime Scene
- Seizing Digital Evidence at the Scene
- Processing a Major Incident or Crime Scene
- Processing Data Centers with an Array of RAIDS
- Using a Technical Advisor at an Incident or Crime Scene
- Sample Civil Investigation
- Sample Criminal Investigation
- Collecting Digital Evidence

Data Acquisition

- Determining the Best Acquisition Method
- Planning Data Recovery Contingencies
- Using MS-DOS Acquisition Tools
- Understanding How DriveSpy Accesses Sector Ranges
- Data Preservation Commands
- Using DriveSpy Data Manipulation Commands
- Using Windows Acquisition Tools
- AccessData FTK Explorer
- Acquiring Data on Linux Computers
- Using Other Forensics Acquisition Tools
- Exploring SnapBack DatArrest
- Exploring SafeBack
- Exploring EnCase

Computer Forensic Analysis

- Understanding Computer Forensic Analysis
- Refining the Investigation Plan
- Using DriveSpy to Analyze Computer Data
- DriveSpy Command Switches
- DriveSpy Keyword Searching
- DriveSpy Scripts
- DriveSpy Data-Integrity Tools
- DriveSpy Residual Data Collection Tools
- Other Useful DriveSpy Command Tools
- Using Other Digital Intelligence Computer Forensics Tools
- Using PDBlock and PDWipe
- Using AccessDatas Forensic Toolkit
- Performing a Computer Forensic Analysis
- Setting Up Your Forensic Workstation
- Performing Forensic Analysis on Microsoft File Systems
- UNIX and Linux Forensic Analysis
- Macintosh Investigations
- Addressing Data Hiding Techniques
- Hiding Partitions
- Marking Bad Clusters
- Bit-Shifting
- Using Steganography
- Examining Encrypted Files
- Recovering Passwords

E-mail Investigations

- Understanding Internet Fundamentals
- Understanding Internet Protocols
- Exploring the Roles of the Client and Server in E-mail
- Investigating E-mail Crimes and Violations
- Identifying E-mail Crimes and Violations
- Examining E-mail Messages
- Copying an E-mail Message
- Printing an E-mail Message
- Viewing E-mail Headers
- Examining an E-mail Header
- Examining Additional E-mail Files
- Tracing an E-mail Message
- Using Network Logs Related to E-mail
- Understanding E-mail Servers
- Examining UNIX E-mail Server Logs
- Examining Microsoft E-mail Server Logs
- Examining Novell GroupWise E-mail Logs
- Using Specialized E-mail Forensics Tools

Recovering Image Files

- Recognizing an Image File
- Understanding Bitmap and Raster Images
- Understanding Vector Images
- Metafile Graphics
- Understanding Image File Formats
- Understanding Data Compression
- Reviewing Lossless and Lossy Compression
- Locating and Recovering Image Files
- Identifying Image File Fragments
- Repairing Damaged Headers
- Reconstructing File Fragments
- Identifying Unknown File Formats
- Analyzing Image File Headers
- Tools for Viewing Images
- Understanding Steganography in Image Files
- Using Steganalysis Tools
- Identifying Copyright Issues with Graphics

Writing Investigation Reports

- Understanding the Importance of Reports
- Limiting the Report to Specifics
- Types of Reports
- Expressing an Opinion
- Designing the Layout and Presentation
- Litigation Support Reports versus Technical Reports
- Writing Clearly
- Providing Supporting Material
- Formatting Consistently
- Explaining Methods
- Data Collection
- Including Calculations
- Providing for Uncertainty and Error Analysis
- Explaining Results
- Discussing Results and Conclusions
- Providing References
- Including Appendices
- Providing Acknowledgments
- Formal Report Format
- Writing the Report
- Using FTK Demo Version

Becoming an Expert Witness

Comparing Technical and Scientific Testimony
Preparing for Testimony
Documenting and Preparing Evidence
Keeping Consistent Work Habits
Processing Evidence
Serving as a Consulting Expert or an Expert Witness
Creating and Maintaining Your CV
Preparing Technical Definitions
Testifying in Court
Understanding the Trial Process
Qualifying Your Testimony and Voir Dire
Addressing Potential Problems
Testifying in General
Presenting Your Evidence
Using Graphics in Your Testimony
Helping Your Attorney
Avoiding Testimony Problems
Testifying During Direct Examination
Using Graphics During Testimony
Testifying During Cross-Examination
Exercising Ethics When Testifying
Understanding Prosecutorial Misconduct
Preparing for a Deposition
Guidelines for Testifying at a Deposition
Recognizing Deposition Problems
Public Release: Dealing with Reporters
Forming an Expert Opinion
Determining the Origin of a Floppy Disk

Computer Security Incident Response Team

Incident Response Team
Incident Reporting Process
Low-level incidents
Mid-level incidents
High-level incidents
What is a Computer Security Incident Response Team (CSIRT)?
Why would an organization need a CSIRT?
What types of CSIRTs exist?
Other Response Teams Acronyms
What does a CSIRT do?
What is Incident Handling?
Need for CSIRT in Organizations
Best Practices for Creating a CSIRT?

Logfile Analysis

- Secure Audit Logging
- Audit Events
- Syslog
- Message File
- Setting Up Remote Logging
- Linux Process Tracking
- Windows Logging
- Remote Logging in Windows
- ntsyslog
- Application Logging
- Extended Logging
- Monitoring for Intrusion and Security Events
- Importance of Time Synchronization
- Passive Detection Methods
- Dump Event Log Tool (Dumpel.exe)
- EventCombMT
- Event Collection
- Scripting
- Event Collection Tools
- Forensic Tool: fwanalog
- Elements of an End-to-End Forensic Trace
- Log Analysis and Correlation
- TCPDump logs
- Intrusion Detection Log (RealSecure)
- Intrusion Detection Log (SNORT)

Recovering Deleted Files

- The Windows Recycle Bin
- Digital evidence
- Recycle Hidden Folder
- How do I undelete a file?
- e2undel
- O&O UnErase
- Restorer2000
- BadCopy Pro
- File Scavenger
- Mycroft v3
- PC ParaChute
- Search and Recover
- Stellar Phoenix Ext2,Ext3
- Zero Assumption Digital Image Recovery
- FileSaver
- VirtualLab Data Recovery
- R-Linux
- Drive & Data Recovery
- Active@ UNERASER - DATA Recovery

Application Password Crackers

Advanced Office XP Password Recovery
AOXPPR
Accent Keyword Extractor
Advanced PDF Password Recovery
APDFPR
Distributed Network Attack
Windows XP / 2000 / NT Key
Passware Kit
How to Bypass BIOS Passwords
BIOS Password Crackers
Removing the CMOS Battery
Default Password Database

Investigating E-Mail Crimes

E-mail Crimes
Sending Fakemail
Sending E-mail using Telnet
Tracing an e-mail
Mail Headers
Reading Email Headers
Tracing Back
Tracing Back Web Based E-mail
Microsoft Outlook Mail
Pst File Location
Tool: R-Mail
Tool: FinaleMail
Searching E-mail Addresses
E-mail Search Site
abuse.net
Network Abuse Clearing House
Handling Spam
Protecting your E-mail Address from Spam
Tool: Enkoder Form
Tool: eMailTrackerPro
Tool: SPAM Punisher

Investigating Web Attacks

- How to Tell an Attack is in Progress
- What to Do When You Are Under Attack?
- Conducting the Investigation
- Attempted Break-in
- Step 1: Identifying the System(s)
- Step 2: Traffic between source and destination
- How to detect attacks on your server?
- Investigating Log Files
- IIS Logs
- Log file Codes
- Apache Logs
- Access_log
- Log Security
- Log File Information
- Simple Request
- Time/Date Field
- Mirrored Site Detection
- Mirrored Site in IIS Logs
- Vulnerability Scanning Detection
- Example of Attack in Log file
- Web Page Defacement
- Defacement using DNS Compromise
- Investigating DNS Poisoning
- Investigating FTP Servers
- Example of FTP Compromise
- FTP logs
- SQL Injection Attacks
- Investigating SQL Injection Attacks
- Web Based Password Brute Force Attack
- Investigating IP Address
- Tools for locating IP Address
- Investigating Dynamic IP Address
- Location of DHCP Server Logfile

Investigating Network Traffic

- Network Intrusions and Attacks
- Direct vs. Distributed Attacks
- Automated Attacks
- Accidental Attacks
- Address Spoofing
- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Preventing IP Spoofing
- Preventing ARP Spoofing
- Preventing DNS Spoofing
- VisualZone
- DShield
- Forensic Tools for Network Investigations
- TCPDump
- Ethereal
- NetAnalyst
- Ettercap
- Ethereal

Investigating Router Attacks

DoS Attacks
Investigating DoS Attacks
Investigating Router Attacks

The Computer Forensics Process

Evidence Seizure Methodology
Before the Investigation
Document Everything
Confiscation of Computer Equipment

Data Duplication

Tool: R-Drive Image
Tool: DriveLook
Tool: DiskExplorer for NTFS

Windows Forensics

Gathering Evidence in Windows
Collecting Data from Memory
Collecting Evidence
Memory Dump
Manual Memory Dump (Windows 2000)
Manual Memory Dump (Windows XP)
PMDump
Windows Registry
Registry Data
Regmon utility
Forensic Tool: InCntrl5
Backing Up of the entire Registry
System State Backup
Forensic Tool: Back4Win
Forensic Tool: Registry Watch
System Processes
Process Monitors
Default Processes in Windows NT, 2000, and XP
Process-Monitoring Programs
Process Explorer
Look for Hidden Files
Viewing Hidden Files in Windows
NTFS Streams
Detecting NTFS Streams
Rootkits
Detecting Rootkits
Sigverif
Detecting Trojans and Backdoors
Removing Trojans and Backdoors
Port Numbers Used by Trojans
Examining the Windows Swap File
Swap file as evidence
Viewing the Contents of the Swap/Page File
Recovering Evidence from the Web Browser
Locating Browser History Evidence
Forensic Tool: Cache Monitor
Print Spooler Files
Steganography
Forensic Tool: StegDetect

Linux Forensics

- Performing Memory Dump on Unix Systems
- Viewing Hidden Files
- Executing Process
- Create a Linux Forensic Toolkit
- Collect Volatile Data Prior to Forensic Duplication
- Executing a Trusted Shell
- Determining Who is logged on to the System
- Determining the Running Processes
- Detecting Loadable Kernel Module Rootkits
- LKM
- Open Ports and Listening Applications
- /proc file system
- Log Files
- Configuration Files
- Low Level Analysis
- Log Messages
- Running syslogd
- Investigating User Accounts
- Collecting an Evidential Image
- File Auditing Tools

Investigating PDA

- Parabens PDA Seizure

Enforcement Law and Prosecution

- Freedom of Information Act
- Reporting Security Breaches to Law Enforcement
- National Infrastructure Protection Center
- Federal Computer Crimes and Laws
- Federal Laws
- The USA Patriot Act of 2001
- Building the Cybercrime Case
- How the FBI Investigates Computer Crime
- Cyber Crime Investigations
- Computer-facilitated crime
- FBI
- Federal Statutes
- Local laws
- Federal Investigative Guidelines
- Gather Proprietary Information
- Contact law enforcement
- To initiate an investigation

Investigating Trademark and Copyright Infringement

Trademarks

Trademark Eligibility

What is a service mark?

What is trade dress?

Internet domain name

Trademark Infringement

Conducting a Trademark Search

Using Internet to Search for Trademarks

Hiring a professional firm to conduct my trademark search

Trademark Registrations

Benefits of Trademark Registration

Copyright

How long does a copyright last?

Copyright Notice

Copyright Fair Use Doctrine

U.S. Copyright Office

How are copyrights enforced?

SCO vs IBM

What is Plagiarism?

Turnitin

Plagiarism Detection Tools
