EC-Council

CHFI Exam Blueprint v2.1

Categories	Topics Covered	A minimally competent candidate will be able to:	Weightage	Items
1. Forensic Science			15%	22
	01. Computer Forensics Objective and Need	1. Understand computer forensics, and explain the objectives and benefits of computer forensics		
		2. Apply the key concepts of Enterprise Theory of Investigation (ETI)		
	02. Cyber Crime	1. Fuse computer network attack analyses with criminal and counterintelligence investigations and operations		
	03. Web Applications and Webservers Attacks	1. Identify elements of the crime		
	04. Email Crimes	1. Understand various types of Web attacks		
	05. Network Attacks	1. Understand various types of email attacks		
	06. Forensics on Mobile Devices	1. Understand various types of network attacks		
	07. Cyber Crime Investigation	1. Understand mobile based operating systems, their architectures, boot process, password/pin/pattern lock bypass mechanisms.		
	08. Computer Forensics Investigation Methodology	1. Understand the importance of cybercrime investigation		
	09. Reporting a Cyber Crime	1. Understand the methodology involved in Forensic Investigation		
	10. Expert Witness	1. Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.		
	11. Expert Witness	1. Understand the role of expert witness in computer forensics		
2. Regulations, Policies and Ethics			10%	15
	1. Searching and Seizing Computers with and without a Warrant	1. Idenify legal issues and reports related to computer forensic investigations		
	2. Laws and Acts against Email Crimes	1. Idenify legal issues and reports related to computer forensic investigations		
	3. Laws pertaining to Log Management	1. Idenify legal issues and reports related to log management		
	4. Pertaining to Mobile Forensics	1. Idenify internal BYOD and information security policies of the organization		
	5. Laws and Acts against Email Crimes	1. Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action		
	6. General Ethics While Testifying	1. Idenify legal issues and reports related to computer forensic investigations		

3. Digital Evidence			20%	30
	01. Digital Evidence	1. Apply the key concepts of Enterprise Theory of Investigation (ETI)		
	02. Types of Digital Evidence	1. Undersand various types and nature of digital Evidence		
	03. Rules of Evidence	1. Understand the best evidence rule		
	04. Electronic Evidence: Types and Collecting Potential Evidence	1. Secure the electronic device or information source, Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence		
	05. Electronic Crime and Digital Evidence Consideration by Crime Category			
	06. Computer Forensics Lab	1. Create a forensically sound duplicate of the evidence (forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes HDD, SSD, CD/DVD, PDA, mobile phones, GPS, and all tape formats.		
	07. Understanding Hard Disks	1. Perform MAC timeline analysis on a file system		
	08. Disk Partitions and Boot Process	1. Undersatnd the Windows and Macintosh boot process, and handling volatile data		
	09. Understanding File Systems	1. Understand File Systems and help in digital forensic investigations		
	10. Windows File Systems	1. Understand Windows File Systems and help in digital forensic investigations		
	11. Linux File Systems	1. Understand Linux File Systems and help in digital forensic investigations		
	12. Mac OS X File Systems	1. Understand Mac OS X File Systems and help in digital forensic investigations		
	13. RAID Storage System	1. Understand RAID Storage System and help in digital forensic investigations		
	14. File Carving	1. Understand Carving Process and help in digital forensic investigations		
	15. Image Files	1. Understand Image File Formats		
	16. Analyze Logs	1. Understand Computer Security Logs		
	17. Database Forensics	1. Perform MSSQL Forensics		
		2. Perform MySQL Forensics		
	18. Email Headers	1. Perform various steps involved in investigation of Email crimes		
	19. Analyzing Email headers	1. Perform analysis of email headers and gather evidential information		
	20. Malware Analysis	1. Perform static and dynamic malware analysis		

	21. Mobile Operating Systems	1. Understand the hardware and software characteristics of mobile devices		
		2. Understand the different precautions to be taken before investigation		
		3. Perform various processes involved in mobile forensics		
4. Procedures and Methodology			20%	30
	01. Investigating Computer Crime	1. “Exploit information technology systems and digital storage media to solve and prosecute cybercrimes and fraud committed against people and property		
		2. Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations “		
	02. Computer Forensics Investigation Methodology	1. Write and publish Computer Network Defense guidance and reports on incident findings to appropriate constituencies,		
		2. Determine and develop leads and identify sources of information in order to identify and prosecute the responsible parties to an intrusion investigation,		
		3. Process crime scenes,		
		4. Track and document Computer Network Defense incidents from initial detection through final resolution,		
		5. Develop an investigative plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the internet,		
		6. Identify outside attackers accessing the system from Internet or insider attackers, that is, authorized users attempting to gain and misuse non-authorized privileges,		
		7. Coordinate with intelligence analysts to correlate threat assessment data		
	03. Digital Evidence Examination Process	1. Ensure chain of custody is followed for all digital media acquired (e.g., indications, analysis, and warning standard operating procedures)		
		2. Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration		
		3. Assist in the gathering and preservation of evidence used in the prosecution of computer crimes		
		4. Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures)		
		5. Prepare reports to document analysis		

	4. Encryption	1. Decrypt seized data using technical means		
	5. First Responder	1. Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals)		
		2. Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents		
	6. First Response Basics	Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations which enable expeditious remediation		
	7. Roles of First Responder	1. Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.)		
		2. Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems		
		3. Perform real-time Computer Network Defense Incident Handling (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs)		
		4. Provide technical assistance on digital evidence matters to appropriate personnel		
		5. Conduct interviews and interrogations of victims, witnesses and suspects		
		6. Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence		
		7. Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.)		
		8. Independently conducts large-scale investigations of criminal activities involving complicated computer programs and networks		
	8. Data Acquisition and Duplication	1. Examine recovered data for items of relevance to the issue at hand		
		2. Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation		
		3. Perform static media analysis		
		4. Review forensic images and other data sources for recovery of potentially relevant information		

		5. Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration		
		6. Identify data of intelligence of evidentiary value to support counterintelligence and criminal investigations		
		7. Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise		
	9. Defeating Anti-forensics Techniques	1. Identify Anti-Forensics Techniques		
		2. Recover Deleted Files and Partitions		
		3. Bypass Windows' and Applictions' Passwords		
		4. Detect steganography and identify the hidden content		
	10. Log Management and Event Correlation	1. Perform command and control functions in response to incidents		
		2. Analyze computer generated threats		
	11. Network Forensics (Intrusion Detection Systems (IDS)	1. Perform Computer Network Defense trend analysis and reporting		
		2. Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis		
	12. Computer Forensics Reports and Investigative Report Writing	1. Develop reports which organize and document recovered evidence and forensic processes used		
		2. Write and publish Computer Network Defense guidance and reports on incident findings to appropriate constituencies		
5. Digital Forensics			25%	37
	01. Recover Data	1. Perform file signature analysis, Perform tier 1, 2, and 3 malware analysis		
	02. File System Analysis	1. Analyze the file systems contents in FAT, NTFS, Ext2, Ext3, UFS1, and UFS2		
	03. Windows Forensics	1. Collect Volatile and Non-Volatile Information		
		2. Perform Windows registry analysis		
		3. Perform Cache, Cookie, and History Analysis		
		4. Peform Windows File Analysis		
		5. Perform Metadata Investigation		
		6. Analyze Windows Event Logs		

	4. Linux Forensics	1. Collect Volatile and Non-Volatile Information		
		2. Use Various Shell Commands		
		3. Examine Linux Log files		
	5. MAC Forensics	1. Examine MAC Forensics Data		
		2. Examine MAC Log Files		
		3. Analyze MAC Directories		
	6. Recovering the Deleted Files and Partitions	1. Examine MAC Forensics Data		
		2. Examine MAC Log Files		
		3. Analyze MAC Directories		
	7. Steganography and Image File Forensics	1. Detect steganography		
		2. Process images in a forensically sound manner		
	8. Steganalysis	1. Perform steganalysis to recover the data hidden using steganography		
	9. Application Password Crackers	1. Undersatnd various password cracking techniques		
		2. Crack the password to recover protected information and data		
	10. Investigating and Analyzing Logs	1. Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion		
		2. Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion		
	11. Investigating Network Traffic	1. Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts		
	12. Investigating Wireless Attacks	1. Investigate wireless attacks		
	13. Web Attack Investigation	1. Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security		
	14. Investigating Email Crime and Violation	1. Perform various steps involved in investigation of email crimes		
	15. Mobile Forensic Process	1. Perform various processes involved in mobile forensics		
	16. Cloud Forensics	1. Perform investigation on cloud storage services such as Google Drive and Dropbox.		
	17. Malware Forensics	1. Understand and perform static and dynamic malware analysis		
	18. Defeating Anti-Forensic Techniques	1. Bypass anti-forensic techniques and access the required resources		

6. Tools/Systems/ Programs			10%	16
	01. First Responder Toolkit	1. Maintain deployable Computer Network Defense toolkit (e.g., specialized Computer Network Defense software/hardware) to support incident response team mission		
	02. Windows Forensic Tools (Helix3 Pro, X-Ways Forensics, Windows Forensic Toolchest (WFT), Autopsy, The Sleuth Kit (TSK), etc.)	1. Recognize and accurately report forensic artifacts indicative of a particular operating system		
		2. Perform live forensic analysis (e.g., using Helix in conjunction with LiveView)		
		3. Perform dynamic analysis to boot an "image" of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment		
		4. Use data carving techniques (e.g., Autposy) to extract data for further analysis		
		5. Decrypt seized data using technical means		
	03. Data Acquisition Software Tools UltraKit Forensic Falcon, etc.)	1. Perform data acquisition (using UltraKit, Active@ Disk Image, DriveSpy, etc.)		
	04. Tools to defeat Anti-Forensics	1. Use File Recovery Tools (e.g., Recover My Files, EaseUS Data Recovery Wizard, etc.), Partition Recovery Tools (e.g., Active@ Partition Recovery, 7-Data Partition Recovery, Acronis Disk Director Suite, etc.), Rainbow Tables Generating Tools (e.g., rtgen, Winrtgen), Windows Admin Password Resetting Tools (e.g., Active@ Password Changer, Windows Password Recovery Bootdisk, etc.).		
		2. Understand the usage of Application Password Cracking Tools (e.g., Passware Kit Forensic, SmartKey Password Recovery Bundle Standard, etc.), Steganography Detection Tools (e.g., Gargoyle Investigator™ Forensic Pro, StegSecret, etc.)		
	05. Steganography Tools	1. Use tools to locate and recover image files		
	06. Database Forensics Tools	1. Use tools to perform database forensics (e.g., Database Forensics Using ApexSQL DBA, SQL Server Management Studio, etc.)		
	07. Password Cracking Tools	1. Use tools to recover obstrcted evidence		
	8. Network Forensics Tools	1. Use network monitoring tools to capture real-time traffic spawned by any running malicious code after identifying intrusion via dynamic analysis		
		2. Understand the working of wireless forensic tools (e.g., NetStumbler, NetSurveyor, Vistumbler, WirelessMon, Kismet, OmniPeek, CommView for Wi-Fi, Wi-Fi USB Dongle: AirPcap, tcpdump, KisMAC, Aircrack-ng Suite AirMagnet WiFi Analyzer, MiniStumbler, WiFiFoFum, NetworkManager, KWiFiManager, Aironet Wireless LAN,		

	9. Web Security Tools, Firewalls, Log Viewers, and Web Attack Investigation Tools	1. Understand the working of web Security Tools, Firewalls, Log Viewers, and Web Attack Investigation Tools (e.g., Acunetix Web Vulnerability Scanner, Falcove Web Vulnerability Scanner, Netsparker, N-Stalker Web Application Security Scanner, Sandcat, Wikto, WebWatchBot, OWASP ZAP, dotDefender, IBM AppScan, ServerDefender, Deep Log Analyzer, WebLog Expert, etc.)		
	10. Cloud Forensics Tools	1. Use Cloud Forensics Tools (e.g., UFED Cloud Analyzer, WhatChanged Portable, WebBrowserPassView, etc.)		
	11. Malware Forensics Tools	1. Use Malware Analysis Tools (e.g., VirusTotal, Autoruns for Windows, RegScanner, MJ Registry Watcher, etc.)		
	12. Email Forensics Tools	1. Use email forensic tools (e.g.,Stellar Phoenix Deleted Email Recovery, Recover My Email, Outlook Express Recovery, Zmeil, Quick Recovery for MS Outlook, Email Detective, Email Trace - Email Tracking, R-Mail, FINALeMAIL, eMailTrackerPro, Paraben's email Examiner, Network Email Examiner by Paraben, DiskInternal's Outlook Express Repair, Abuse.Net, MailDetective Tool, etc.)		
	13. Mobile Forensics Software and Hardware Tools	1. Use mobile forensic software tools (e.g., Oxygen Forensic Suite 2011, MOBILedit! Forensic, BitPim, SIM Analyzer, SIMCon, SIM Card Data Recovery, Memory Card Data Recovery, Device Seizure, Oxygen Phone Manager II, etc.)		
		2. Use mobile forensic software tools		
	14. Report Writing Tools	1. Create well formatted computer forensic reports		