EC-Council

CHFI Exam Blueprint v4

Domains	Sub Domain	Description	Number of Questions	Weightage (%)
1. Forensic Science	Understand Different Types of Cybercrimes and List Various Forensic Investigation Challenges	▪ Types of Computer Crimes ▪ Impact of Cybercrimes at the Organizational Level ▪ Cyber Attribution ▪ Cyber Crime Investigation ▪ Challenges Cyber Crimes Present for Investigators ▪ Indicators of Compromise (IoC) ▪ Network and Web Application Threats and Attacks ▪ Challenges in Web Application Forensics ▪ Indications of a Web Attack ▪ What is Anti-Forensics? ▪ Anti-Forensics Techniques ▪ Challenges to Forensics from Anti-Forensics	**5**	**15%**
	Understand the Fundamentals of Computer Forensics and Determine the Roles and Responsibilities of Forensic Investigators	▪ Understanding Computer Forensics ▪ Need and Scope of Computer Forensics ▪ Why and When Do You Use Computer Forensics? ▪ Forensic Readiness and Business Continuity ▪ Forensics Readiness Planning and Procedures ▪ Computer Forensics as part of the Incident Response Plan ▪ Overview of Incident Response Process Flow ▪ Role of SOC in Computer Forensics ▪ Role of Threat Intelligence in Computer Forensics ▪ Integration of Artificial Intelligence with Digital Forensics ▪ GitOps and its Impact on Digital Forensics ▪ Forensics Automation and Orchestration ▪ Need for Forensic Investigator ▪ Roles and Responsibilities of Forensics Investigator	**6**	

		▪ What makes a Good Computer Forensics Investigator? ▪ Code of Ethics ▪ Managing Clients or Employers during Investigations ▪ Accessing Computer Forensics Resources ▪ Other Factors that Influence Forensic Investigations ▪ Web Applications and Network Forensics ▪ Postmortem and Real-Time Analysis ▪ Forensics-as-a-Service (FaaS)		
	Understand Data Acquisition Concepts and Rules	▪ Data Acquisition ▪ Live Acquisition ▪ Order of Volatility ▪ Dead Acquisition ▪ Rules of Thumb for Data Acquisition ▪ Types of Data Acquisition ▪ Determine the Data Acquisition Format	**5**	
	Understand the Fundamental Concepts and Working of Databases, Cloud Computing, Emails, IOT, Malware (file, fileless, and .NET), and Dark Web	▪ Dark Web ▪ TOR Relays and TOR Bridge Node ▪ How the TOR Browser works ▪ Risks of Investigating the Dark Web ▪ Internal Architecture of MySQL ▪ Structure of Data Directory ▪ Types of Cloud Computing Services ▪ Cloud Deployment Models ▪ Cloud Computing Threats and Attacks ▪ Fundamentals of Amazon Web Services (AWS) and Google Cloud ▪ Components Involved in Email Communication ▪ How Email Communication Works ▪ Understanding Parts of an Email Message ▪ Malware and its Components	**6**	

		▪ Common Techniques Attackers Use to Distribute Malware Across Web ▪ Types of Malware and their Characteristics ▪ Coordination and Management in Addressing Malware ▪ Fileless Malware ▪ Infection Chain of Fileless Malware ▪ How Fileless Attack Works via Memory Exploits, Websites, Documents, and Containers ▪ Detecting Linux memfd_create() Fileless Malware with Command Line Forensics ▪ Infection Chain of .NET Malware ▪ Analyzing .NET Malware ▪ IoT Architecture ▪ IoT Security Problems ▪ OWASP Top 10 IoT Vulnerabilities ▪ IoT Threats and Attack Surface Areas ▪ Understand OT and OT Security Problems ▪ OT Threats ▪ Understand Multimedia Basics		
2. Regulations, Policies and Ethics	Understand Rules and Regulations Pertaining to Search and Seizure of the Evidence and Evidence Examination	▪ Rules of Evidence ▪ Best Evidence Rule ▪ Federal Rules of Evidence ▪ ACPO Principles of Digital Evidence ▪ Computer Forensics vs. eDiscovery ▪ ChatGPT-4's Role in Evidence Processing, Analysis, and Production ▪ Best Practices for Handling Digital Evidence ▪ Seeking Consent ▪ Obtaining Witness Signatures ▪ Obtaining a Warrant for Search and Seizure ▪ Searches Without a Warrant ▪ Initial Search of the Scene ▪ Preserving Evidence	**5**	**10%**

		▪ Chain of Custody ▪ Sanitize the Target Media ▪ Records of Regularly Conducted Activity as Evidence ▪ Division of Responsibilities		
	Understand Different Laws and Legal Issues that Impact Forensic Investigations	▪ Legal and IT Team Considerations for eDiscovery ▪ Role of Local/International Agencies during Cybercrime Investigation ▪ Legal Issues, Privacy Issues and Legal Compliance ▪ Other Laws that May Influence Computer Forensics ▪ Legal Challenges in Dealing with Malware ▪ U.S. Laws Against Email Crime: CAN-SPAM Act	**5**	
	Understand Various Standards and Best Practices Related to Computer Forensics	▪ ISO Standards ▪ ENFSI Best Practices for Forensic Examination of Digital Technology	**5**	
3. Digital Evidence	Understand the Fundamental Characteristics and Types of Digital Evidence	▪ Types of Digital Evidence ▪ Characteristics and Role of Digital Evidence ▪ Sources of Potential Evidence ▪ Understanding Hard Disk and Solid State Drive (SSD) ▪ Logical Structure of Disks ▪ RAID Storage System ▪ RAID and Virtualization ▪ NAS/SAN Storage ▪ Disk Interfaces ▪ Logical Structure of Disks	**5**	**18%**
	Understand the Fundamental Concepts and Working of Desktop and Mobile Operating Systems	▪ Booting Process ▪ Essential Windows System Files ▪ Windows Boot Process: BIOS-MBR Method and UEFI-GPT ▪ Macintosh and Linux Boot Processes ▪ Windows, Linux, and macOS File Systems ▪ MAC Forensics Data, Log Files, and Directories	**6**	

		▪ Architectural Layers of Mobile Device Environment ▪ Android Architecture Stack and Boot Process ▪ iOS Architecture and Boot Process ▪ Mobile Storage and Evidence Locations ▪ Mobile Phone Evidence Analysis ▪ Data Acquisition Methods ▪ Components of Cellular Network ▪ Different Cellular Networks ▪ Cell Site Analysis: Analyzing Service Provider Data ▪ CDR Contents ▪ Subscriber Identity Module (SIM) ▪ Android and iOS File Systems ▪ Rooting of Android and Jailbreaking of iOS Devices ▪ Different Types of Network-based Evidence		
	Understand Different Types of Logs and their Importance in Forensic Investigations	▪ Types of Logon Events ▪ Event Log File Format ▪ Organization of Event Records ▪ ELF_LOGFILE_HEADER structure ▪ EventLogRecord Structure ▪ Windows 11 Event Logs and Other Audit Events ▪ Evaluating Account Management Events ▪ Log Files as Evidence ▪ Legal Criteria for Admissibility of Logs as Evidence ▪ Guidelines to Ensure Log File Credibility and Usability ▪ Ensure Log File Authenticity and Maintain Log File Integrity ▪ Implement Centralized Log Management ▪ IIS Web Server Architecture and Logs ▪ Analyzing IIS Logs ▪ Apache Web Server Architecture and Logs ▪ Apache Access and Error Logs	**6**	

	Understand Various Encoding Standards and Analyze Various File Types	▪ Character Encoding Standard: ASCII and UNICODE ▪ OFFSET ▪ Understanding Hex Editors and Hexadecimal Notation ▪ Image File Analysis: JPEG and BMP ▪ Understanding EXIF data ▪ Hex View of Popular Image File Formats ▪ PDF, Word, PowerPoint, and Excel File Analysis ▪ Hex View of Other Popular File Formats	**5**	
	Understand the Fundamental Workings of WAF and MySQL Database	▪ Web Application Firewall (WAF) ▪ Benefits and Limitations of WAF ▪ Data Storage in SQL Server ▪ Database Evidence Repositories ▪ MySQL Forensics ▪ Viewing the Information Schema ▪ MySQL Utility Programs for Forensic Analysis	**5**	
4. Procedures and Methodology	Understand the Forensic Investigation Process	▪ Forensic Investigation Process ▪ Importance of the Forensic Investigation Process ▪ Setting Up a Computer Forensics Lab ▪ Building the Investigation Team ▪ Understanding the Hardware and Software Requirements of a Forensic Lab ▪ Validating Laboratory Software and Hardware ▪ Ensuring Quality Assurance ▪ Building Security Content, Scripts, Tools, or Methods to Enhance Forensic Processes ▪ First Response and First Responder ▪ First Response Basics ▪ First Response by Non-forensics Staff, System/Network Administrators, and Laboratory Forensics Staff ▪ First Responder Common Mistakes ▪ Health and Safety Issues	**5**	**17%**

		▪ Documenting the Electronic Crime Scene ▪ Search and Seizure ▪ Evidence Preservation ▪ Data Acquisition and Data Analysis ▪ Case Analysis ▪ Reporting ▪ Testify as an Expert Witness ▪ Generating Investigation Report ▪ Electron Applications and Chat Application Forensics ▪ Mobile Forensics Process ▪ Mobile Forensics Report Template ▪ Sample Mobile Forensic Analysis Worksheet ▪ Social Media Forensics ▪ Social Engineering Forensics ▪ Insider Threat and Identity Theft Forensics ▪ Cryptocurrency and Blockchain Forensics ▪ Virtualization Forensics ▪ Cloud Forensics ▪ Forensic Methodologies for Containers and Microservices ▪ Bluetooth Forensics ▪ IoT Forensics ▪ OT Forensics ▪ Multimedia Forensics		
	Understand the Methodology to Acquire Data from Different Types of Evidence	▪ Data Acquisition Methodology ▪ Step 1: Determine the Best Data Acquisition Method ▪ Step 2: Select the Data Acquisition Tool ▪ Step 4: Acquire Volatile Data ▪ Step 5: Enable Write Protection on the Evidence Media ▪ Step 6: Acquire Non-Volatile Data ▪ Step 7: Plan for Contingency ▪ Step 8: Validate Data Acquisition ▪ Data Acquisition Guidelines and Best Practices ▪ Collecting Volatile Information and Non-Volatile Information	**5**	

		▪ Live Mac Data Collection - Imaging, RAM and Volatile Data ▪ Collecting Volatile Database Data ▪ Collecting Primary Data Files and Active Transaction Logs Using SQLCMD ▪ Collecting Primary Data Files and Transaction Logs ▪ Collecting Active Transaction Logs Using SQL Server Management Studio ▪ Collecting Database Plan Cache ▪ Collecting Windows Logs ▪ Collecting SQL Server Trace Files and Error Logs ▪ Data Acquisition in the Cloud ▪ Data Acquisition on OT Systems		
	Understand the eDiscovery Process	▪ eDiscovery Process Flow ▪ Electronic Discovery Reference Model (EDRM) Cycle ▪ Monitor and Maintain Accurate Metrics and Detailed Tracking Information Related to eDiscovery ▪ eDiscovery Collections/Methodologies ▪ eDiscovery Best Practices to Mitigate Costs and Risk	**5**	
	Illustrate Image/Evidence Examination and Event Correlation	▪ Getting an Image Ready for Examination ▪ Viewing an Image on Windows, Linux, and Mac Forensic Workstations ▪ Windows Memory Analysis and Registry Analysis ▪ Extracting Additional Windows OS Artifacts ▪ File System Analysis Using Autopsy and The Sleuth Kit (TSK) ▪ File System Timeline Creation and Analysis ▪ Types of Event Correlation ▪ Event Deconfliction ▪ Timeline and Kill Chain Analysis ▪ Prerequisites of Event Correlation ▪ Event Correlation Approaches	**6**	

		▪ Collecting and Analyzing macOS Artifacts ▪ Analyzing macOS User Activities ▪ Cloud Digital Evidence Analysis		
	Explain Dark Web and Malware Forensics	▪ Dark web forensics ▪ Information Found on the Dark Web ▪ Safety Precautions while Exploring the Dark Web ▪ Identifying TOR Browser Artifacts: Command Prompt, Windows Registry, and Prefetch Files ▪ Malware Forensics ▪ Why Analyze Malware? ▪ Malware Analysis Challenges ▪ Identifying and Extracting Malware ▪ Malware Forensic Artifacts and Indicators ▪ Prominence of Setting up a Controlled Malware Analysis Lab ▪ Preparing Testbed for Malware Analysis ▪ Supporting Tools for Malware Analysis ▪ General Rules for Malware Analysis ▪ Documentation Before Analysis ▪ Types of Malware Analysis	**5**	
5. Digital Forensics	Review Various Anti-Forensic Techniques and Ways to Defeat Them	▪ Anti-Forensics Technique: Data/File Deletion ▪ What Happens When a File is Deleted in Windows? ▪ Recycle Bin in Windows ▪ File Carving ▪ Anti-Forensics Techniques: Password Protection, Steganography, Alternate Data Streams, Trail Obfuscation, Artifact Wiping, Overwriting Data/Metadata, Encryption, Program Packers, Exploiting Forensics Tools Bugs and Detecting Forensic Tool Activities ▪ Anti-Forensics Countermeasures and Tools	**5**	**29%**

	Analyze Various Files Associated with Windows, Linux, and Android Devices	▪ Windows File Analysis ▪ Metadata Investigation ▪ Windows ShellBags ▪ Analyze LNK Files and Jump Lists ▪ Event logs ▪ File System Analysis using The Sleuth Kit (TSK) ▪ Linux Memory Forensics ▪ Viewing Log Messages in Mac ▪ APFS File System Analysis: Biskus APFS Capture ▪ Parsing metadata on Spotlight ▪ Logical Acquisition of Android and iOS Devices ▪ Physical Acquisition of Android and iOS Devices ▪ Android and iOS Forensic Analysis ▪ SQLite Database Extraction ▪ Challenges in Mobile Forensics	**6**	
	Analyze Various Logs and Perform Network Forensics to Investigate Network Attacks	▪ Analyzing Firewall, IDS, Honeypot, Router, and DHCP Logs ▪ Analyzing Cisco Switch, VPN, and DNS Server Logs ▪ Investigating SSH Logs ▪ Network Protocols and Packet Analysis ▪ Why Investigate Network Traffic? ▪ Gathering Evidence via Sniffers ▪ Sniffing Tools ▪ Analyze Traffic for TCP SYN and SYN-FIN Flood DOS Attack ▪ Analyze Traffic for UDP and HTTP Flood Attacks ▪ Analyze Traffic for FTP and SMB Password Cracking Attempts ▪ Analyze Traffic for Sniffing Attempts ▪ Analyze Traffic to Detect Malware Activity ▪ Analyze SMTP and SNMP Traffic ▪ Centralized Logging Using SIEM Solutions ▪ SIEM Solutions	**6**	

		▪ Examine Brute-Force Attacks, DoS Attacks, and Malware Activity ▪ Examine Data Exfiltration Attempts made through FTP ▪ Examine Network Scanning Attempts and Ransomware Attacks ▪ Detect Rogue DNS server (DNS Hijacking/DNS Spoofing) ▪ Wireless Network Security Vulnerabilities ▪ Performing Attack and Vulnerability Monitoring ▪ Detect a Rogue Access Point and Access Point MAC Spoofing Attempts ▪ Detect Misconfigured Access Points, Honeypot Access Points, and Signal Jamming Attack ▪ Investigate Wireless Network Traffic		
	Analyze Various Logs and Perform Web Application Forensics to Examine Various Web-Based Attacks	▪ Investigating Cross-Site Scripting, SQL Injection, and Directory Traversal Attacks ▪ Investigating Command Injection, Parameter Tampering, and XML External Entity Attacks ▪ Investigating Brute Force Attack and Cookie Poisoning Attack	**6**	
	Perform Forensics on Databases, Dark Web, Emails, Cloud and IoT devices	▪ Database Forensics Using SQL Server Management Studio and ApexSQL DBA ▪ Common Scenario for Reference ▪ MySQL Forensics for WordPress Website Database ▪ Tor Browser Forensics: Memory Acquisition ▪ Collecting Memory Dumps ▪ Memory Dump Analysis: Bulk Extractor ▪ Forensic Analysis of Memory Dumps to Examine Email Artifacts (Tor Browser Open and Tor Browser Closed) ▪ Forensic Analysis of Storage to Acquire the Email Attachments (Tor Browser Open and Browser Closed)	**6**	

		▪ Forensic Analysis: Tor Browser Uninstalled ▪ Dark Web Forensics Challenges ▪ Steps to Investigate Email Crimes ▪ Division of Responsibilities ▪ Where Is the Data Stored in Azure? ▪ Logs in Azure ▪ Acquiring a VM in Microsoft Azure ▪ Acquiring a VM Snapshot Using Azure Portal and PowerShell ▪ AWS Forensics ▪ Cloud Storage Forensics ▪ Google Workspace Forensics ▪ Google Cloud Forensics ▪ Wearable IoT Device: Smartwatch ▪ IoT Device Forensics: Smart Speaker-Amazon Echo		
	Perform Static and Dynamic Malware Analysis in a Sandboxed Environment	▪ Malware Analysis: Static and Dynamic ▪ Analyzing Suspicious Word, Excel, and PDF Documents	**5**	
	Analyze Malware Behavior on System and Network Level, Analyze Malware Persistence, and Analyze Fileless Malware	▪ Registry-Based Malware Persistence Mechanisms ▪ Identifying Malware Persistence ▪ System Behavior Analysis: Monitoring Registry Artifacts, Processes, Services, Startup Programs, Windows Event Logs, API Calls, and Device Drivers ▪ System Behavior Analysis: Installation and System Calls Monitoring ▪ System Behavior Analysis: Monitoring Files and Folders, Monitoring Network Activities, Port, and DNS ▪ Artifact Analysis for Suspicious or Malicious Content ▪ Fileless Malware Analysis: GOOTLOADER ▪ Perform Timeline Analysis	**5**	

	Perform Digital Forensics using Python	▪ Python Digital Forensics Basics ▪ Data Acquisition using Python ▪ Windows and Linux Forensics using Python ▪ Malware Forensics using Python ▪ Web Application and Cloud Forensics using Python ▪ Email Forensics using Python ▪ Mobile Device and IoT Forensics using Python ▪ Multimedia Forensics using Python	**5**	
6. Tools/ Systems/Programs	Identify Various Tools to Investigate Operating Systems, Including Windows, Linux, Mac, Android, and iOS	▪ File System Analysis Tools ▪ File Format Analyzing Tools ▪ Volatile and Non-Volatile Data Acquisition Tools ▪ Data Acquisition Validation Tools ▪ eDiscovery Tools ▪ Digital Forensic Imaging Solutions ▪ Tools for Examining Images on Windows, Linux, and macOS ▪ Tools for Carving Files on Windows, Linux, and macOS ▪ Partition Recovery Tools ▪ Using Rainbow Tables to Crack Hashed Passwords ▪ Password Cracking Tools ▪ Tool to Reset Admin Password ▪ Steganography Detection Tools ▪ Detecting Data Hiding in File System Structures Using OSForensics ▪ ADS Detection Tools ▪ Detecting File Extension Mismatch using Autopsy ▪ Tools to Detect Overwritten Data/Metadata ▪ Program Packers Unpacking Tools ▪ USB Device Enumeration using Windows PowerShell ▪ Tools to Collect Volatile and Non-Volatile Information on Windows and Linux	**6**	**11%**

		▪ Tools to Perform Windows Memory and Registry Analysis ▪ Tools to Examine the Cache, Cookie, and History Recorded in Web Browsers ▪ Private Browsing and Browser Artifact Recovery ▪ Tools to Examine Windows Files, Metadata, ShellBags, LNK files, and Jump Lists ▪ Linux File system Analysis Tools ▪ Tools to Perform Linux Memory Forensics ▪ APFS File System Analysis ▪ Parsing Metadata on Spotlight ▪ MAC Forensic Tools ▪ Network Traffic Investigation Tools ▪ Incident Detection and Examination with SIEM Tools ▪ Detect and Investigate Various Attacks on Web Applications by Examining Various Logs ▪ Tools to Identify TOR Artifacts ▪ Tools to Acquire Memory Dumps ▪ Tools to Examine the Memory Dumps ▪ Tools to Perform Static and Dynamic Malware Analysis ▪ Tools to Analyze Suspicious Word and PDF Documents ▪ Tools to Analyze Malware Behavior on a System and Network ▪ Tools to Perform Logical and Physical Acquisition on Android and iOS Devices ▪ Mobile Forensic Tools		
	Determine the Various Tools to Investigate MSSQL, MySQL, Azure, AWS, Emails, and IoT Devices	▪ Tools to Collect and Examine the Evidence Files on MSSQL Server and MySQL Server ▪ Tools for Investigating Microsoft Azure and AWS ▪ Tools to Acquire Email Data and Deleted Emails ▪ Tools to Perform Forensics on IoT devices	**5**	

	Identify Various Tools to Perform Network, Web Application, Cloud, Social Media, and Insider Threat Forensics	▪ Network Log Analysis Tools ▪ Tools for Investigating Network Traffic ▪ Social Media Forensic Tools ▪ Insider Threat Tools ▪ Tools for Analyzing IIS Logs and Apache Logs ▪ Blockchain Forensic Tools ▪ AWS Forensic Tools	**5**	