EC-Council

Digital Forensics Essentials (DFE)

Exam Blueprint v1

Digital Forensics Essentials

Exam Blueprint

S. No.	Domains	Sub Domains	Domain %
1	**Computer Forensics Fundamentals**	Fundamentals of Computer Forensics	8
		Digital Evidence	
		Forensic Readiness	
		Roles and Responsibilities of a Forensic Investigator	
		Legal Compliance in Computer Forensics	
2	**Computer Forensics Investigation Process**	Forensic Investigation Process and its Importance	6
		Forensic Investigation Process - Pre-investigation Phase	
		Forensic Investigation Process - Investigation Phase	
		Forensic Investigation Process - Post-investigation Phase	
3	**Understanding Hard Disks and File Systems**	Different Types of Disk Drives and their Characteristics	10
		Logical Structure of a Disk	
		Booting Process of Windows, Linux, and Mac Operating Systems	
		File Systems of Windows, Linux, and Mac Operating Systems	
		File System Examination	

4	**Data Acquisition and Duplication**	Data Acquisition Fundamentals	**8**
		Types of Data Acquisition	
		Data Acquisition Format	
		Data Acquisition Methodology	
5	**Defeating Anti-forensics Techniques**	Anti-forensics and its Techniques	**8**
		Anti-forensics Countermeasures	
6	**Windows Forensics**	Volatile and Non-Volatile Information	**12**
		Windows Memory and Registry Analysis	
		Cache, Cookie, and History Recorded in Web Browsers	
		Windows Files and Metadata	
7	**Linux and Mac Forensics**	Volatile and Non-Volatile Data in Linux	**8**
		Analyze Filesystem Images Using The Sleuth Kit	
		Memory Forensics	
		Mac Forensics	
8	**Network Forensics**	Network Forensics Fundamentals	**8**
		Event Correlation Concepts and Types	
		Identify Indicators of Compromise (IoCs) from Network Logs	
		Investigate Network Traffic	
9	**Investigating Web Attacks**	Web Application Forensics	**8**
		IIS and Apache Web Server Logs	
		Investigating Web Attacks on Windows-based Servers	
		Detect and Investigate Attacks on Web Applications	
10	**Dark Web Forensics**	Dark Web	**6**
		Dark Web Forensics	
		Tor Browser Forensics	
11	**Investigating Email Crimes**	Email Basics	**8**
		Email Crime Investigation and its Steps	

12	**Malware Forensics**	Malware, its Components and Distribution Methods	**10**
		Malware Forensics Fundamentals and Recognize Types of Malware Analysis	
		Static Malware Analysis	
		Analyze Suspicious Word Documents	
		Dynamic Malware Analysis	
		System Behavior Analysis	
		Network Behavior Analysis	