LIST OF TERMS

Terms	Definition
Web Server Seizure	Legal and forensic process of capturing digital evidence from a web server used in criminal activities.
Digital Forensics Framework	Structured set of procedures to guide the collection, preservation, and analysis of digital evidence.
Live Acquisition	Collecting evidence from a running server without shutting it down to preserve volatile data.
Remote Acquisition	Collecting data from servers hosted remotely, especially in cloud environments.
Volatile Data	Data that is lost when a system is powered off, such as RAM contents and active session logs.
Hashing	Process of generating a unique fixed-size hash value from data to verify its integrity.
Chain of Custody (CoC)	Documentation process that records the handling of evidence from collection to presentation in court.
Cloud Forensics	Branch of digital forensics focused on evidence collection from cloud computing environments.
Hybrid Server Environment	Infrastructure combining both Virtual Private Server (VPS) and cloud-based servers.
Forensic Tools	Software and hardware used in the acquisition, preservation, and analysis of digital evidence.
Integrity Validation	Ensuring that digital evidence remains unchanged and authentic during forensic processing.
Legal Authorization	Court-issued permission required to perform seizures or searches involving digital evidence.
Subject Matter Expert (SME)	Individual with specialized knowledge who validates the forensic process or framework.
Multi-Tenant Cloud	Cloud architecture where multiple customers share the same physical infrastructure while keeping data isolated.
Snapshot	Captured state of a server or disk at a specific point in time, used for forensic analysis.
Seizure	The use of legal authority to take something from somebody; an amount of something that is taken in this way.

Continued on next page...

Terms	Definition
Seizure Framework	A procedural model that guides the legal and technical aspects of server seizure and evidence acquisition.
Data Contamination	Alteration or damage to digital evidence, compromising its validity for legal proceedings.
Write Blocker	Device or software ensuring no modifications occur to a storage medium during acquisition.
Volatility Framework	Open-source tool for memory forensics, used to capture and analyze volatile data.
Secure Evidence Storage	Process of protecting acquired digital evidence against tampering, typically involving encryption and access control.