- Review data from cloud backups, email accounts, and other remote storage for evidence of unauthorized access or activities.

Network Forensic Analysis

- Capture and analyze network traffic, logs, and communications to identify evidence of data exfiltration, malware attacks, or unauthorized access.
- Investigate data flows, track cyberattacks, and uncover key evidence for digital forensics investigations.
- Review firewall logs, router data, and server traffic to understand attack vectors and data breach methods.

Cloud Forensic Analysis

- Analyze data stored in cloud environments, including public and private clouds (e.g., Google Drive, Dropbox, AWS, etc.).
- Investigate access logs, file shares, and cloud storage for evidence of unauthorized access or data manipulation.
- Recover cloud-based data for evidence of malicious or criminal activity.

Email and Communication Forensics

- Perform analysis of email records and other communication data to uncover hidden or deleted messages.
- Review email headers, attachments, timestamps, and metadata for evidence of fraud, harassment, or corporate espionage.

Metadata Analysis

- Examine metadata associated with documents, images, videos, and other digital files to uncover timestamps, author information, and file history.
- Reveal the true origin and authenticity of files to support your investigation.

Malware and Incident Analysis

- Identify and analyze malware, trojans, ransomware, or other malicious software that has compromised devices, networks, or systems.
- Trace the origin and behavior of malware to identify perpetrators and uncover attack methods.