Meta Insight

Info@metainsight.us

402-576-5220

Types of Digital Forensics

1. E-discovery: Digital data capturing, analysis and processing. E-discovery is used in a regulatory or legal context to capture and/or preserve information electronically.
2. Forensic data analysis: The type of cyber forensics that deals explicitly with organized data. Forensic analysis involves data analysts combing through troves of data to arrive at usable evidence. It mainly affects the financial fraud space.
3. Incident Response: Digital forensics from a corporate point of view. This type of forensics aims to ensure business continuity and reduce the impact of an event (such as a data breach or technology failure). Internal teams in an organization can be trained to handle, review, and maintain the incident response procedures.
4. Computer forensics: Digital forensics that deals with accessing, gathering, and analyzing information on computer systems that operate in a computing or storage capacity. Computer forensics covers any mobile device, Personal Computers (PC), servers, and external media (like thumb drives).
5. Network Forensics: Standalone computers are rare today. Almost all digital devices are connected to each other and the internet using computer networks. Network forensics involves the analysis of network traffic patterns and incriminating payloads.
6. Database Forensics: Involves the analysis and extraction of data and metadata from databases. This includes data stored by third-party services in a contract with the suspect. These might even be SaaS vendors when we consider incidents in organizations.
7. Disk Forensics: Another subset of computer forensics, disk forensics, specializes in data retrieval and recovery from nonvolatile devices.
8. Memory Forensics: While disk forensics focuses on persistent storage, memory forensics focuses on RAM. Memory forensics is also called live acquisition since it presents the ‘crime scene’ as it is.
9. Cloud Forensics: Most systems on the cloud now, cloud forensics deals with cloud-hosted information. It requires the analysis of configuration, security, and the geolocation of cloud-based assets. Cloud forensics requires cooperation from cloud vendors (such as AWS and Google Cloud).
10. Email Forensics: Involves retrieving and scanning all email communication, including the deleted ones. Forensic analysts look for identities, content, time stamps, and other metadata attached to the emails. Email forensics looks for forged emails and malicious content, such as phishing emails.
11. Malware Forensics: The type of forensics dealing with tracing the source of malware that has already been injected into the system. It is sometimes a part of incident response. Malware forensic analysts investigate the extent of damage and try to trace it back to the code used to build the malware. Most digital forensic investigators specialize in more than one of these types. The type of digital forensics used in a case depends on the evidence present and the nature of the crime (or incident) that investigators must solve.