Skillmine
Technology • Consulting • Services

infosec
Miners

July 2023

Digital Forensics

According to Future Market Insights the global digital forensics market is poised to increase at a CAGR of 11.2%, reaching US$ 23.62 Bn by 2030 from a market valuation of US$ 10.07 Bn in 2022. Digital forensics accounted for 8% share of the global cybersecurity market value in 2021. Digital forensics is a process that involves the storage, analysis, retrieval, and preservation of electronic data for investigative purposes. It encompasses a wide range of devices such as computers, mobile phones, smart appliances, vehicle navigation systems, electronic door locks, and other digital devices.

Various Types of Digital Forensics:

Computer Forensics
Examining digital evidence collected from computers, laptops, and storage media to assist with investigations and judicial actions.

Mobile Device Forensics
Gathering evidence from small electronic devices like mobile phones, tablets, sim cards, and gaming consoles.

Network Forensics
Analyzing data obtained from monitoring and examining cyber network activities, such as attacks, breaches, and abnormal network traffic.

Digital Image Forensics
Focusing on the extraction and analysis of digital images to verify authenticity, examine metadata, and determine their history and information.

Digital Video/Audio Forensic
Examining audio-visual evidence to determine authenticity and extract additional information, such as location and time intervals.

Memory Forensics
Recovering information from a running computer's RAM, also known as live acquisition.

Objectives of Digital Forensics:

- Recovery, analysis, and preservation of computers and related materials to present them as evidence in a court of law.
- Determining the motive for the crime and identifying the primary perpetrator.
- Establishing procedures at a suspected crime scene to ensure that digital evidence is not contaminated.
- Data duplication and acquisition, which entails extracting and verifying evidence from digital media by recovering erased files and partitions.
- Assisting in quickly identifying evidence and assessing the potential impact of malicious activity on the victim.
- Creating a comprehensive computer forensic report that provides detailed information about the investigation process.
- Safeguarding the evidence by adhering to the chain of custody.

Digital Forensics tools are developed to examine data on devices without causing damage. They can assist investigators in analyzing and identifying risk areas in information and communications technology (ICT) environments. These tools can be classified as digital forensic open-source tools, digital forensic hardware tools, and others. Popular tools in this field include:

- **FTK Imager**
- **OSForensic**
- **Bulk Extractor**
- **The SleuthKit**
- **Hex Editor Neo**

Steps Involved in Digital Forensics:

- **Identification:** This initial stage focuses on identifying the individuals or devices that are likely to provide significant evidence for the investigation.
- **Preservation:** In this step, the goal is to preserve the relevant electronically stored information (ESI) by capturing and securing the crime scene. This includes documenting visual images and how the information was obtained.
- **Analysis:** The analysis stage entails a thorough evaluation of the acquired data. This investigation generates data objects, such as user- and system-generated files, and looks for particular solutions and points of departure for making judgements.
- **Documentation:** Procedures are followed to document the analysis findings in a manner that allows other competent examiners to read and reproduce the results.
- **Presentation:** This step involves collecting digital information, which may require removing electronic devices from the crime/incident scene and making copies or printing them for further investigation.

Challenges Faced by Digital Forensics include:

1. Extracting data from locked or damaged computing devices.
2. Locating specific data entries within vast amounts of stored data.
3. Maintaining a reliable digital chain of custody.
4. Ensuring data integrity throughout the investigation.

Advantages of Digital Forensics:

- Enabling digital evidence analysis.
- Aiding in the identification of criminals.
- Recovering deleted data.
- Providing insights into how crimes are committed and helping prevent future crimes.

Disadvantages of Digital Forensics:

- A lengthy procedure.
- The need for specialized knowledge and skills.
- Potential costs involved.
- The requirement for a court order to obtain evidence, and the susceptibility of evidence to destruction or manipulation.

Digital forensics is a crucial process for storing, analyzing, and preserving electronic data in investigations. It helps identify perpetrators, recover deleted data, and present evidence in legal proceedings. Despite challenges, digital forensics offers advantages like evidence analysis and crime prevention. Specialized tools enhance the effectiveness of investigations. Overall, digital forensics is an evolving field that contributes significantly to criminal investigations.

SKILLMINE CYBER SECURITY TEAM

Skillmine
Technology • Consulting • Services
India | KSA | UK | USA

#46/4, Novel Tech park,
Kudlu Gate, Bangalore
Karnataka-560 068

+91 9920663515
www.Skill-mine.com
info@Skill-mine.com

Follow us on