Database Fundamentals and Forensic Analysis

Description

This training program delves into the foundational principles of databases with a special focus on forensic analysis. Participants will gain an in-depth understanding of various database types, such as SQLite, Chromium, LevelDB, and Apple Plist files. The training emphasizes hands-on learning, enabling participants to extract and analyze data, recover deleted information, and perform forensic investigations using advanced query techniques. The program culminates in a capstone project, allowing participants to apply their knowledge to real-world scenarios.

Duration : 3 days(24 hours)

Target Audience

- Forensic investigators and cybersecurity professionals seeking specialized database analysis skills.
- IT professionals interested in understanding database fundamentals and structures.
- Data analysts and scientists keen on exploring database types and forensic techniques.
- Students and educators in computer science or information technology fields.

Prerequisites

- Basic knowledge of databases and SQL.
- Familiarity with general computer forensics concepts is beneficial but not mandatory.
- Understanding of file systems and operating system basics.
- Proficiency in using Windows or macOS environments.

Table of Contents :

Introduction to Databases

- Overview of Relational Databases
- Key Database Terminologies
- The Importance of Forensic Database Analysis

SQLite Databases

- Understanding SQLite
    - SQLite's Architecture and Use Cases
    - File Format and Structure
- Analyzing SQLite Databases
    - B-tree Pages and Data Organization
    - Overflow and Freelist Pages
    - Rollback Journals and WAL (Write-Ahead Logs)
- Practical Analysis
    - Extracting Data from SQLite
    - Case Studies in SQLite Forensics

Chromium Databases

- Introduction to Chromium Databases
    - History and Relevance
    - Use in Web Browsing and Applications
- Forensic Exploration Techniques
    - Identifying Patterns in Chromium Storage
    - Recovering Deleted or Hidden Data
- Hands-On Activities
    - Analyzing Chromium Databases using Tools
    - Data Interpretation Exercises

LevelDB Databases

- Overview of LevelDB
    - Design Principles and Key-Value Storage
    - Differences Between SQLite and LevelDB
- Forensic Techniques
    - Investigating Metadata and Compression

    - Extracting and Visualizing Stored Values
- Real-Life Applications
    - Examples of LevelDB Usage in Forensic Cases

Apple Plist Files

- Fundamentals of Plist Files
    - XML and Binary Plists
    - Common Fields and Structures
- Methods for Analysis
    - Converting Binary Plists to Readable Formats
    - Decoding Timestamps, Preferences, and Settings
- Forensic Use Cases
    - Apple Ecosystem Investigations
    - Real-World Analysis Scenarios

SQLite Query Language

- Introduction to SQLite Query Syntax
    - Basic Commands: SELECT, INSERT, UPDATE, DELETE
- Advanced Query Features
    - Joins, Subqueries, and Index Optimization
- Hands-On Exercises
    - Writing Queries for Forensic Analysis
    - Real-World Data Analysis Challenges