Forensic Investigator, Part 07 of 10: Database Forensics

Meet the expert: David Bigger is the lead trainer at Bigger IT Solutions. He has been information technology for a little over 20 years and has been training all over the US. He has worked with companies like US Military, Lockheed Martin, General Dynamics, Dominos Pizza, University of Utah and Expedia

Prerequisites: Recommended:
Understanding of networking; How data flows from source and destination
Computer security basics such as passwords, encryption and physical security
Basic understanding of computing and computer systems
Experience with various operating systems

Runtime: 53:21

Course description: MySQL, Oracle or MS SQL server….which is it running? How do you know? Oracle may be the number one database on the market today, but what does that mean for us as investigators? Coming up, we will be looking at various database management systems and how they work with data. We will dive into Oracle databases, MySQL databases and MS SQL databases so we know where we can look for potential evidence. We will also take a look at some tools and techniques that will allow us to gather the data for our case against the perpetrators. This course is part of a series covering the EC-Council Computer Hacking Forensic Investigator (CHFI).

Course outline:

Database Forensics
- Introduction
- Database Forensics
- Database Review
- Popular DBMS
- Summary

Oracle
- Introduction
- Oracle
- Oracle Logical Structure
- Data Blocks
- System Change Number (SCN)
- Where to Look in Oracle
- System Global Area
- Where to Look in Oracle, Continued
- Oracle Forensic Tools
- Summary

MySQL
- Introduction
- MySQL
- Data Directory
- Log Files for MySQL
- Were to Look in MySQL
- MySQL Forensic Tools
- Summary

Microsoft SQL Server
- Introduction
- Microsoft SQL Server
- Data Storage
- Where to Look on MS SQL Server
- Tools for MS SQL Forensics
- SQL Server Management Studio
- ApexSQL
- Summary