filename:comptia-secplussy0601-9-6-1-digital-forensics-concepts
Showname: Security+ (SY0-601)
Topic: Operational Security and Incident Response
Episode: Digital Forensics Concepts
Learner Objectives:

Explain the key aspects of digital forensics.

Description:In this episode, the viewer will identify key aspects of digital forensics such as documentation and evidence gathering, chain of custody, information acquisition and preservation concepts like order of volatility and location, maintaining integrity through hashing, checksums and more.

- Legal Hold
- Digital Forensics Concepts
    - Right-to-audit clauses
    - Regulatory and Jurisdiction
    - Data breach notification
- Order of Volatility
- Data Preservation and Documentation
    - Time stamps
    - Time offset
    - Reports and event logs
    - Integrity
        - Hashing
        - Checksums
        - Provenance
- Chain of Custody
- Digital Forensics Tools
    - dd

- memdump / coupled with Volatility
- FTK Imager
- WinHek
- Autospy
- EnCase