Introduction to Digital Evidence

Module 01: Introduction to Digital Evidence

The importance of digital evidence in modern investigations.

a. Brief history of digital evidence.
b. Types of digital evidence.
c. Methods for storing digital evidence.

Module 02: Risks of Improper Evidence Handling

a. Digital evidence disasters: Case studies and examples.
    i. LA County Sheriff and Fire (Kobe Bryant case)
    ii. Rittenhouse Trial
    iii. Dallas Police

Module 03: File Types and Surveillance Video

a. Overview of standard vs. proprietary file types.
b. Growth of video.
    i. Surveillance Video
    ii. BWC & In-Car Camera Video
    iii. Citizen Shared Video
    iv. Video Canvassing & Collection

Module 04: Evidence Lifecycle

a. Digital evidence lifecycle from collection to disposal.
b. Digital evidence vs public records.
c. Public disclosure considerations for evidence retention.

Module 05: Preserving Data Integrity

a. Synthetic Media
b. Verification and Authentication
c. Original vs Copies
d. Chain of Custody
e. File Hashing

Module 06: DEMS Overview

a. Benefits of centralized digital evidence storage.
b. On-Premises vs Cloud
c. Access Control
d. Integrating with an existing system (case management, BWC, etc.).

Module 07: Real-World Scenario

a. Walkthrough of an arson case.
b. Review of arson evidence managed in DigitalOnQ.

Module 08: Summary and Resources

a. Final Thoughts
b. Downloadable Resources
    i. Organizations and Training
    ii. Video Authenticity Statement
    iii. Video Retrieval Notes
c. Contact Information for Follow Up