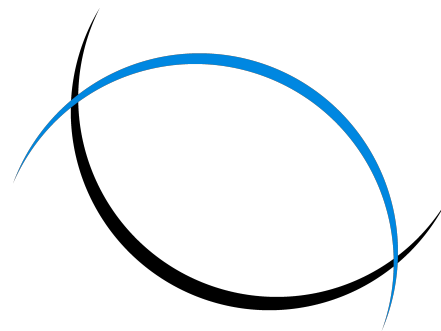


Introduction to Digital Forensics

for Law Enforcement
and Government Investigators



Digital evidence is playing an increasingly important part of law enforcement investigations. Nearly every case has some form of digital evidence associated with it, be it cellular phones, video footage, computers, internet evidence, or other forms of storage media. This evidence often requires extraction and examination by individuals trained in digital forensic concepts, methodologies, and tools.

Digital forensics is a field that both challenging and rewarding, but approaching the topic can be daunting. There is a vast wealth of knowledge that must be learned before one can properly examine digital evidence, with decades of technological advancement and best practices to learn.

Introduction to Digital Forensics is a one-day (8 hours) long introductory training course designed to assist law enforcement personnel who have been assigned or aspire to be assigned to a position where they will conduct digital forensic examinations.

The content will introduce underlying concepts and terminology used in the digital forensic world, which in turn provides a foundational knowledge that attendees can leverage when attending more advanced training topics.

This course will cover the following concepts:

- The components of computer systems and what purposes they fulfill
- How data is stored, including how to read binary, hex, and ASCII
- Cellphone and mobile device technology and extractions
- The forensic process, data extraction, and device imaging types
- Forensic report writing
- Modern and historic operating systems
- The fundamentals of network infrastructure
- Common forensic tools
- Tool and data validation
- Court testimony for forensic practitioners

This class is open to any law enforcement personnel or government investigator, whether sworn or civilian, who may be tasked with forensically extracting and examining digital evidence. It may also benefit any investigative personnel who handle data that has been provided to them by a digital forensic examiner.

The course is designed and taught by active law enforcement personnel who have an expertise in digital forensics. Students will receive a certificate upon completion of the course. This class may be taught either virtually or in-person.

Prerequisites: Attendance to our [Digital Evidence Basics](#) course or some similar training. In lieu of such training, we ask that attendees have knowledge and experience with digital evidence best practices relating to the identification, seizure, and overall handling of digital evidence items.

Price: \$275 per student (discounts for multiple registrations)

(Michigan) MCOLES 302 Funds Approved

Dates and Times:

Friday, September 22nd, 2023 from 8 a.m. to 4 p.m. (Eastern)

Location:

Virtual

Live, Instructor-Led

Register at penumbra-training.com

Contact: training@penumbra-training.com