

## Advanced Data Extraction and Acquisitions in Cyber Forensics

The H-11 Advanced Data Extraction and Acquisitions in Cyber Forensics is a certified 5-day course where students learn how to collect, acquire, extract, and then analyze digital forensic evidence. Students will learn various methods to extract data from computers using MS-Windows, Apple iOS, Android OS, Cloud Data, and IoT devices.

This hands-on course helps students understand the best methods and tools to use when collecting data from computers, smartphones, cloud, and IoT devices. Students will learn what IoT and Cloud data is available and to gain access to said data.

This advanced course will include various data duplication tools, methods, and techniques. Looking at data from several perspectives and tools. It includes an in-depth look at Disk Storage technologies, smartphones, cloud data, and IoT devices.

The following topics will be covered during this 5-day training course:

### Digital Extraction Forensics Overview

#### Processes to Consider:

- Acquisition
- Authentication
- Preservation
- Carving
- Analysis
- Reporting
- Presenting

#### History of Hard Disk Drives

#### Hard Disk Structure

- IDE
- SATA
- SCSI
- PCI
- USB
- Solid State Drives (SSD)
- M.2 drive
- Non-Volatile Memory Express (NVMe)
- NAND technology
- Other Technologies

#### RAID technology

#### Extraction Methods

- Write Blocking Devices
- Disk Duplication Devices
- FTK Imager
- DI - Field Triage
- DI - Media Acquisition
- DI - Mobile
- Other triage tools

### Cloud Extractions Overview

#### What is IoT?

- Wearable
- IoT Hub Devices
- Home Uses
- Office Uses
- Cars and other Vehicle Uses

#### Concerns on IoT

What is IoT Forensics and How is it Different from Digital Forensics?

What are challenges to IoT forensics?

Gaining access to IoT devices

Extracting Router Data

Extracting Drone Data

Extracting Data from Smart Devices

Finding evidence on Amazon Echo devices

Collecting Data from the cloud

- Tools to use to preserve evidence
- Tools to analyze evidence
- Collecting from Social Networks

Analyzing the evidence

Smart Device Extractions Overview

What is a SQLite Database?

- Structures
- Schemas
- Journals

SQLite Forensics

Hands-on Labs

Written Exams

Final Hands-on Test

Final Written Examination