Helix3 Pro Live Forensics 1-Day Online Course Syllabus

This course provides students with the knowledge and skills necessary to begin a computer-based investigation using Helix3 Pro. Students will hear lectures regarding common and accepted Incident Response Procedures for previewing, securing and preserving digital evidence at a crime scene. Students will also get a strong understanding of how best practice procedures will enable acquisition of digital content in an accepted and proven format.

This course will be focused on the use of Helix3 Pro, an e-fense developed incident response and forensics tool. Students will learn how to forensically acquire volatile data, and make court accepted forensic images utilizing the Helix3 Pro Acquisition Utility.

This course is intended for first responders and computer forensics investigators, as well as anyone performing activities that have the potential to require seizing digital media and managing an Incident Response initiative while using Helix3 Pro.

1. What is Live Forensics
    - Understanding Volatile Data
    - Traditional Forensics vs. Live Forensics
    - The Live Response Process and the Best Evidence Rule
    - Volatile Data - OS Differences

2. What is Helix3 Pro
    - What is Helix3 Pro
    - Why is Helix3 Pro Different
    - How does Helix3 Pro Work
    - The Helix3 Pro Acquisition Utility

3. Storing the Data
    - Acquisition Destination Options
    - Network Acquisitions
    - Helix3 Pro Receiver
    - Attached Devices
    - Integrity Checks

4. Live Side Collections
    - Acquisitions in a Live Environment
    - System Impact
    - Physical Memory Acquisition
    - API Calls vs. RAM Acquisition
    - Challenges in Acquiring RAM - Windows/Linux/Mac
    - Using Helix3 Pro to Acquire RAM
    - Using the Helix3 Pro Receiver
    - Volatile Data Collection Using APIs
    - Using Helix3 Pro to Acquire Volatile Data

Copyright ©2001-2009 e-fense, Inc. All Rights Reserved

- Storing the Data
- Hard Drive Collection
- Imaging Conditions in a Live Environment
- Encrypted Volumes
- Dynamic Disk Imaging - RAID

5. Bootable Side Background and Collections
    - Why Learn Linux/Helix?
    - Forensic Benefits
    - Understanding Physical and Logical Disks
    - Linux Terminology
    - Commands - What you Must Know
    - How Helix is Organized
    - Mounting Devices
    - Previewing
    - Helix3 Pro Acquisitions

Copyright ©2001-2009 e-fense, Inc. All Rights Reserved