E103: Live Forensics & Incident Response (Featuring Helix3 Pro) Intermediate Level Course 2-Day Syllabus

This course provides students with the knowledge and skills necessary to begin a computer-based investigation. Students will use common and accepted Incident Response Policies and 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.

A strong emphasis will be 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.

This hands-on intensive 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.

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
    - Network Shares and Samba
    - 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

- Hands-On Exercises
- Volatile Data Collection Using APIs
- Using Helix3 Pro to Acquire Volatile Data
- Storing the Data
- Hands-On Exercises
- Hard Drive Collection
- Imaging Conditions in a Live Environment
- Encrypted Volumes
- Dynamic Disk Imaging - RAID

5. Bootable Side Details
    - Why Learn Linux/Helix?
    - Forensic Benefits
    - Understanding Physical and Logical Disks
    - Linux Terminology
    - The Boot Process
    - How Helix is Organized
    - Files and File Systems
    - Permissions
    - Commands - What you Must Know
    - Mounting Devices
    - Helix Hardware Issues
    - Device Detection and Boot Problems
    - Cheat Codes
    - Other Issues

6. Bootable Side Collections
    - Preparing the Harvest Drive
    - Mounting Devices
    - dd Acquisitions
    - dc3dd Acquisitions
    - aff Acquisitions
    - Linen Acquisitions
    - Helix3 Pro Acquisitions
    - Using Helix to Acquire a Forensic Image
    - Hands-On Exercises
    - Previewing Devices
    - Mounting Devices
    - Using loop
    - iSCSI - Previewing and Imaging with Helix3 Pro
    - iSCSI and Helix3 Pro bootable environment
    - iSCSI Initiators - Windows, Mac and Linux
    - Additional Tricks and Useful Utilities

7. Memory Analysis
    - What's in Memory?
    - Simple Tools and Techniques
    - Strings, grep, foremost, scalpel
    - Advanced Tools and Techniques
    - ptfinder, volatility
    - Hands-On Exercises