



E103: Live Forensics & Incident Response (Featuring Helix₃[™]) Intermediate Level Course 3-Day Syllabus

This course provides students with the knowledge and skills necessary to begin a computer based investigation. Using common and accepted Incident Response Policies and Procedures for previewing, securing and preserving digital evidence at a network crime scene, students will 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 Helix, an e-fense developed incident response and forensics tool. Students will learn how to forensically acquire volatile data, and make court accepted forensics backups.

The hands-on intensive course, intended for first responders and computer forensics investigators, as well as anyone performing activities that have the potential to require seized digital media and managing an Incident Response initiative.

Cost for this course:

Corporate - \$1995.00

Law Enforcement - \$1495.00

DAY 1

1. Primer
 - Brief understanding of network basics
 - Brief re-education on the command line
2. What is Helix
 - Understanding what Helix is and how it works
 - Helix CD interaction within a Live Environment
 - Helix tools for incident response and acquisition
3. Understanding volatile data
 - What is considered evidence
 - Determining the steps and process to preserve evidentiary integrity
 - Learning what comprises volatile data and how to view it
 - Hands on exercises
4. Obtaining volatile data
 - How to collect volatile data
 - Using specific tool sets to collect volatile data
 - Chain of custody and relevant issues
 - Hands on exercises

DAY 2

5. Storing volatile data
 - Using the power of a network to gather your data
 - Using attached devices
 - Options for storage
 - Hands on exercises
6. Bootable Helix
 - Helix boot process
 - Learning about devices
 - Boot issues and hardware problems
7. Helix navigation
 - File system Structure and file systems
 - Command shell and common commands
 - Working with files, directories and permissions
 - Mounting devices
 - Hands on exercises
8. Traditional acquisitions
 - Understanding partitions and drives in Helix
 - Making a forensic image using dd
 - Playing with Adepto
 - Using EnCase Linen
 - HPA's and DCO's
 - Hands on exercises

DAY 3

9. Previewing and Other Tricks
 - Using Retriever to locate files
 - Understanding the Helix file manager
 - Using the loopback filesystem
 - Using CDFS / CHNTPW / Anti-Virus
 - Hands on exercises
10. Imaging the Live OS
 - Acquiring the live OS over a network
 - Issues with acquiring the live OS
 - Operating Systems other than Windows
11. All about RAIDS
 - Understanding RAID levels
 - Large corporate systems
 - Handling dynamic disks and RAIDS



12. Advanced Information

- Problematic Live systems
- Looking at memory
- Advanced memory

13. Practical Exercise