

Advanced Linux Data Forensics

This course is for those using Linux on a daily basis who want to further their understanding of Linux and how to leverage it for advanced forensic applications. You will learn how to build your own custom Linux kernel, how to build your own Trusted Media Toolkit for live analysis, and how to handle non-standard storage devices.

What can you expect to learn by working through this course?

- The importance of customizing the Linux kernel for Data Forensics
- How to cleanly apply patches to the Kernel source tree
- The importance of using a Trusted Media Toolkit for live analysis
- Identify key programs and libraries to include in your Trusted Media Toolkit
- Learn how to statically link programs and the importance of static linking
- Identify the potential benefits and pitfalls to performing live analysis
- Learn how to access and use your Trusted Media Toolkit for live analysis
- Learn the seven steps to successful live analysis
- Learn how to acquire media over a network communication channel (LAN/WAN)
- Learn how to identify and acquire RAID arrays
- Learn how to identify and acquire non-standard storage devices (digital cameras, etc.)

Throughout this course you will be presented with real world scenarios and expected to work through exercises and answer end-of-module review questions that illustrate key topic areas. There is a cumulative practical exam at the completion of this course.

Prerequisites

This course is intended for forensic practitioners, incident response team members, disaster recovery professionals, and anyone whose job duties include acquiring and analyzing electronically stored information. An understanding of basic forensic methodology is a benefit, although not a requirement. Strong, hands-on experience with Linux is required.

Dates

Anytime you have the time!

Location

In your home, office, or anywhere you have the materials!

Registration

<http://www.onlineforensictraining.com/register.html>