

Fundamental Linux Data Forensics

This course will get you up to speed on the Linux operating system from a forensic practitioner perspective. You will learn how to use and leverage Linux for your authentication, acquisition, and analysis needs.

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

- What is Linux and what makes up a Linux distribution
- How to customize the Linux environment for Data Forensics
- What are shells, runlevels, and processes, and what is their importance in Data Forensics
- Users and groups – maintenance and understanding for forensic analysis
- Permissions demystified – what are they, how to analyze them, and how to set them
- Timestamps – what are they, how to interpret them, and pitfalls to avoid
- Linux file system basics
- How to authenticate media using Linux
- How to acquire media using Linux
- How to identify devices and device nomenclature
- How to safely mount image files for forensic analysis
- How to process (analyze) data using system commands and forensic programs
- What forensic programs exist for Linux and what are their pros and cons
- What are the shortcomings of using Linux for Data Forensics

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. No prior 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>