

## Windows Data Forensics Using Linux

This course is for those practitioners using Linux on a daily basis who want to be able to analyze a Windows operating system environment using the Linux operating system environment. You will learn how to use and leverage Linux commands and applications to analyze the most common system artifacts of the Windows operating systems.

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

- THE FARMER'S BOOT CD (FBCD) and how to preview Windows systems
- Recycle Bin analysis
- Event Log analysis
- Printer Spool File analysis
- Thumbs.db analysis
- User Login Password analysis
- Alternate Data Stream analysis
- Encrypting File System (EFS) analysis
- LNK File analysis
- File Metadata analysis
- E-mail analysis
- Internet History analysis

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 else whose job duties include acquiring and analyzing electronically stored information. An understanding of basic forensic methodology is a benefit, although not a requirement. 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>