



Cybercop 401 - Linux File System for Computer Forensic Examiners (LinuxFS)

This 4-1/2 day class is designed for experienced computer forensic examiners who want to gain a better understanding of the unique issues related to Linux based computers.

The class will emphasize Command line usage, interpreting command shell histories, standard environmental variables, the graphic user interface, the native Linux file systems (ext2, ext3 and Reiser), Linux files system metadata, recovering deleted files in ext2, Linux file system journals, the Linux boot process, archiving and compression in Linux and the location of various evidential items on a Linux machine. The student will explore the configuration of a standard Linux computer from install to operation, and default partition layouts. Evidence items to be examined include event logs, email clients, server logs, configuration files and web browser artifacts.

This course requires the student to have previous training in Cybercop 101 (BDRA), Cybercop 201 (IDRA) or equivalent and have at least 1 year of full time processing experience. It is strongly recommended that they also possess prior training in the NT file system and a basic level of experience using the Linux OS.