

CC 250	Linux Open Source Forensics (LOSF)
Cybercop	<p>This course teaches students how to use free and open-source software to conduct digital forensic examinations of Windows OS platforms. Students learn to locate and install free Linux-based forensic software. After covering key forensic concepts as applied to open source software, basic forensic analysis techniques are covered. Topics include imaging and mounting, review and examination of live and deleted files, hash analysis, keyword searching, Windows Registry, report creation, and identification and extraction of file metadata, scripting, local and environmental variables.</p>
Classroom course	
2 days	
Prerequisite: CC 201	



Linux forensic suites

Autopsy, Bulk Extractor.

Linux basics

The Virtual File system. Referencing objects. Linux and NTFS metadata.

Hands-on experience

Many tools and best practices.