



Cybercop 201 - Intermediate Data Recovery and Analysis (IDRA)

This 5-day course is designed to be the “sequel” to the Cybercop 101 (BDRA) course. It covers the forensic examination of Windows based operating systems on FAT File System, and includes processing the Recycle Bin, the swap file, the registry, long file names and other windows features. Topical areas include detailed partition table entries and recovering data from the registry. In addition, the student will learn to process slack space, unallocated space, print spool files, and application metadata for additional evidence that may be overlooked. The class is scenario based giving an opportunity for the students to examine 5 separate “suspect” hard drives. This will be accomplished throughout the course of the week using manual tools as well as the automated forensic tools by FTK and EnCase.

This course requires the student to have previous training in Cybercop 101 (BDRA) within the last 12 months.