

P2P FORENSICS TRAINING COURSE

**Techno Security 2009 Pre-Conference Training
May 29-30, 2009, Myrtle Beach, South Carolina**

COURSE COST: \$1,395

INCLUDES V.I.P. ADMISSION TO TECHNO SECURITY CONFERENCE

FOR COURSE REGISTRATION, CLICK HERE

This is an intensive, two-day training course on peer-to-peer computer forensics. The course provides in-depth instruction in investigative techniques for the most frequently seen P2P networks and clients, including the use of P2P Marshal, a product which greatly accelerates P2P investigations.

Digital forensic investigators often find peer-to-peer file sharing software present on the images of hard drives they examine. Investigators must determine what P2P software is present, where the associated information is stored, retrieve the information from the appropriate directories, and then analyze the results. This training course presents information on current and emerging P2P file sharing networks, the structure and behavior of these networks, and techniques for the manual acquisition and analysis of P2P forensic evidence. The course introduces the use of P2P Marshal, an automated tool for detection and analysis of peer-to-peer evidence, and builds investigator proficiency in the use and interpretation of the results generated with this automated product.

The course covers these topics:

- ◆ What is peer-to-peer file sharing, how is it used, and why do I care about it?
- ◆ Overview of current and emerging peer-to-peer file sharing networks
- ◆ Structure and behavior of current P2P networks
 - Gnutella
 - * Leaf-and-supernode architecture
 - * Related networks
 - BitTorrent
 - * Metainfo files and bencoding
 - * BitTorrent extensions
 - DHT networks
- ◆ P2P client features and forensic evidence
 - LimeWire
 - BitTorrent 5 and 6
 - uTorrent
 - Azureus Vuze
 - Ares
- ◆ P2P Marshal
 - P2P Marshal usage and features
 - How P2P Marshal interprets and displays client evidence files
- ◆ Hands-on exercises
 - Manual analysis of LimeWire and BitTorrent forensic evidence
 - Using P2P Marshal to analyze evidence
- ◆ Testing and Silver Certification

Participants will receive P2P Marshal software and reference materials. Documentation will be provided for this course to qualify for law enforcement continuing education credit.