

P2P Marshal



a computer forensic tool to detect and analyze peer-to-peer/file sharing use

P2P FORENSICS & P2P MARSHAL TRAINING COURSE

May 5, 2010

9:00 AM – 5:00 PM

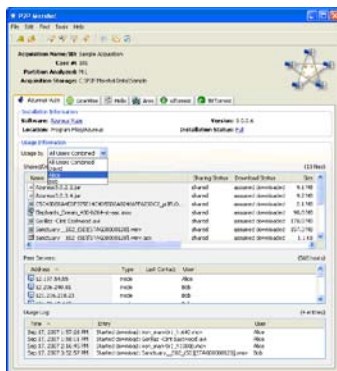
Minnesota Dept. of Human Services Building, St. Paul, MN

The one-day training course on peer-to-peer forensics and P2P Marshal includes:

- Overview of the architecture of peer-peer file sharing systems: networks and clients
- Legitimate and illegitimate uses of peer-to-peer systems
- Forensic details of peer-to-peer software commonly seen in criminal investigations
- Forensic analysis of client evidence
- Potential pitfalls of evidence analysis
- Hands-on exercises using manual analysis techniques
- Detailed instruction for using P2P Marshal in forensic investigations
- Hands-on exercises using P2P Marshal
- Certification

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 manual techniques for P2P investigations and introduces the use of P2P Marshal, a new, automated tool for the detection and analysis of peer-to-peer usage.

P2P Marshal automatically detects and analyzes peer-to-peer client use on a disk. P2P Marshal determines what clients currently are or have been installed on a machine and then extracts per-user usage information, specifically a list of peer servers contacted and files that were shared and downloaded. The tool performs its actions in a forensically-sound way and maintains a detailed audit trail of all actions.



Features:

- Discovers and analyzes peer-to-peer file sharing usage
- Supported targets: Images of Windows 2000, XP, 2003, Vista and Windows 7 systems (English and non-English, 32- and 64-bit)
- Forensically sound
- Automatically maintains detailed log
- Extensive search capabilities
- Produces reports in CSV, RTF, PDF, and HTML formats
- Performs full analysis for: Ares, BitTorrent, FrostWire, LimeWire, uTorrent, and Azereus Vuze
- Detects and shows default download locations for Kazaa

Cost: FREE to US state & local law enforcement; includes P2P Marshal software.

For more information and registration:
(607) 257-1975 x7119 or training@p2pmarshal.com

www.P2PMarshal.com

