Computer Technology
Investigators Northwest
is sponsoring

Computer Forensics:

X-Ways Forensics & File Systems Revealed

X-Ways Forensics
Complete and systematic demonstration of all computer forensics features in WinHex . Practical, hands-on exercises with sample media, simulating the complete computer forensics process. Covers forensically sound cloning under DOS and Windows, evidence acquisition, data recovery, and report creation.

Topics include:
• Understanding all options of X-Ways Replica • Basic setup of the software • Learning the user interface components • Understanding the data interpreter • Preparing media for cloning • Cloning media/Image creation • Creating a case/adding evidence objects • Hash calculation and checking • Using the gallery view and skin color detection efficiently • Creating drive contents tables systematically • Creating hash sets and matching against existing hash sets • Detecting data hiding methods like alternate data streams, host-protected areas (HPA), misnamed files • Adding annotations/bookmarks • Working with the directory browser • Working with the Access button menu • Various methods of file recovery • Customizing file signatures • Extraction and analysis of free space, slack space, etc. • Using search functions effectively • Efficient navigation of the file systems' data structures • Data profiles • Decoding Base64, Uuencode, etc. • Viewing RAM • Automated report generation • Optionally other topics like template and script programming

File Systems Revealed
Extensive introduction to the file systems FAT12, FAT16, FAT32, NTFS, and Ext2/Ext3. Immediate application of newly gained knowledge by examining data structures on a practical example with WinHex. These exercises will ensure you will remember what you have learned. By the end you will be able to navigate almost intuitively on a hard disk and to identify various sources of information with relevance to forensics. You will be enabled to recover data manually in several cases even where automated software fails and to verify the results computer forensics software reports automatically. You will receive a complete documentation of all the filesystems discussed in this course, with all the training material for later repetition. Prerequisite: some general computer science knowledge recommended.

Basics:
• Binary data storage concepts • Data types • Date formats

FAT:
• Structure of FAT file systems • Boot record • File Allocation Table (FAT) • Directory entries

NTFS:
• Boot sector • Master File Table (MFT) • FILE records structure • FILE record attributes • Directory organisation in NTFS • INDX record structure • NTFS system files • Consistency in NTFS • Alternate data streams • ...

Ext2/3:
• Structure of Ext file systems • Superblocks, group descriptors, block groups, bitmap blocks • Inodes
• Concept of block addressing • Concept of directory structure

http://www.x-ways.net/signup_ext.html

This is a rare training event in the United States!

Tuition:
$1650.00, which includes a licensed version of X-Ways Forensic Edition software and 12 months of updates.

Dates:
January 25-28, 2005

Location:
Burien CJTC

Register:
Apply Online to
X-Ways Forensics:
http://www.x-ways.net
/signup_ext.html

Questions:
http://www.x-ways.net

This course is sponsored by the Computer Technology Investigators Northwest with support from the Washington State Criminal Justice Training Commission.