X-Ways Forensics Training

X-Ways Forensics is a 4-Day training course focused on the systematic and efficient examination of computer media using the integrated computer forensics software X-Ways Forensics. Students will learn complete and systematic methods of the computer forensics features in both WinHex and X-Ways Forensics. This includes: forensically sound disk imaging and cloning, data recovery, thorough overview of existing and deleted files on computer media, theoretical background on slack space, partially initialized space, how to find deleted partitions, what methods X-Ways Forensics finds evidence, search functions, dynamic filtering, report creation, and more! The Hands-on Exercises and the Final Practical Exam will gauge students' proficiency, skills, and knowledge, preparing them for the X-PERT certification.

DAY 1

Module 1: Getting Started with X-Ways Forensics

- Introductions
- Course Overview and X-PERT certification
- Structure, components and functionality
- Key folder paths
- Read-only versus Edit versus In-Place mode
- WinHex versus X-Ways Forensics
- Start-up options
- Alternative disk access methods
- Viewer programs
- Exercise: Installing X-Ways Forensics

Module 2: X-Ways User Interface

- Menus and toolbars
- Directory browser (icons, sorting, navigation, ...)
- Virtual files and directories
- Case data window with directory tree
- The case root
- Modes: Disk/Partition/Volume vs File
- Info panel
- Exercise: Using X-Ways Forensics

Module 3: Creating Disk Images

- Raw images and evidence files
- Fast, adaptive compression
- In-built encryption

Module 4: Creating a Case/Adding Evidence Objects

- Previewing file contents
- Working with the directory browser
- Recursive listing of directories and entire drives
- Column visibility and arrangements
- Efficient navigation of the file systems' data structures

DAY 1 – Continued

Module 4: Creating a Case/Adding Evidence Objects

- Filtering files
    - existing, previously existing
    - tagged, not tagged
    - viewed, not viewed
    - non-hidden, hidden
    - By name, including multiples: by exact name, using wildcards, searching within name, using GREP
    - By path, including multiples
    - By type - exact type, multiple types, entire category, multiple categories

DAY 2

Module 4: Creating a Case/Adding Evidence Objects

- Revision Exercise: Filtering

Module 5: The Various Timestamps Available

- Timestamp filter
- Exercise: Timestamp filtering

Module 6: Recovering/Copying Files

- Original names or names derived from other details
- Groupings vs original paths
- Exporting file lists
    - HTML, TSV, XML, JSON
- Creating report tables and report table associations
- Report creation: Basic reports, report tables and activity log
- Using report tables for filtering and classification
- Exercise: Report table filtering

X-PERT

X-Ways – Professional in Evidence Recovery Techniques

Learn more at: http://www.x-ways.net/x-pert/

DAY 2 – Continued

Module 7: Refining Volume Snapshots

Part 1

- File system specific thorough data structure search for previously existing data
- Signature search for previously existing data not identifiable via file system metadata

DAY 3

Module 7: Refining Volume Snapshots

Part 2

- Verifying file types based on signatures and algorithms
- Exercise: Type mismatch filtering

Part 3

- Exploring ZIP, RAR, etc. archives
- Extracting e-mails from PST, OST, Exchange EDB, DBX, mbox (Unix mailboxes, used e.g. by Mozilla Thunderbird), AOL PFC, etc.
- Finding pictures embedded in documents, etc.
- Exercise: Hidden Pictures

Part 4

- Extracting metadata from a variety of file types
- Analyzing browser history for Internet Explorer, Firefox, Safari, Chrome, Opera
- Analyzing Windows Event Logs (evt and evtx)

DAY 4

Module 8: The Hash Database

- Importing single or multiple hash sets
- Creating your own hash sets

Module 9: Refining Volume Snapshots

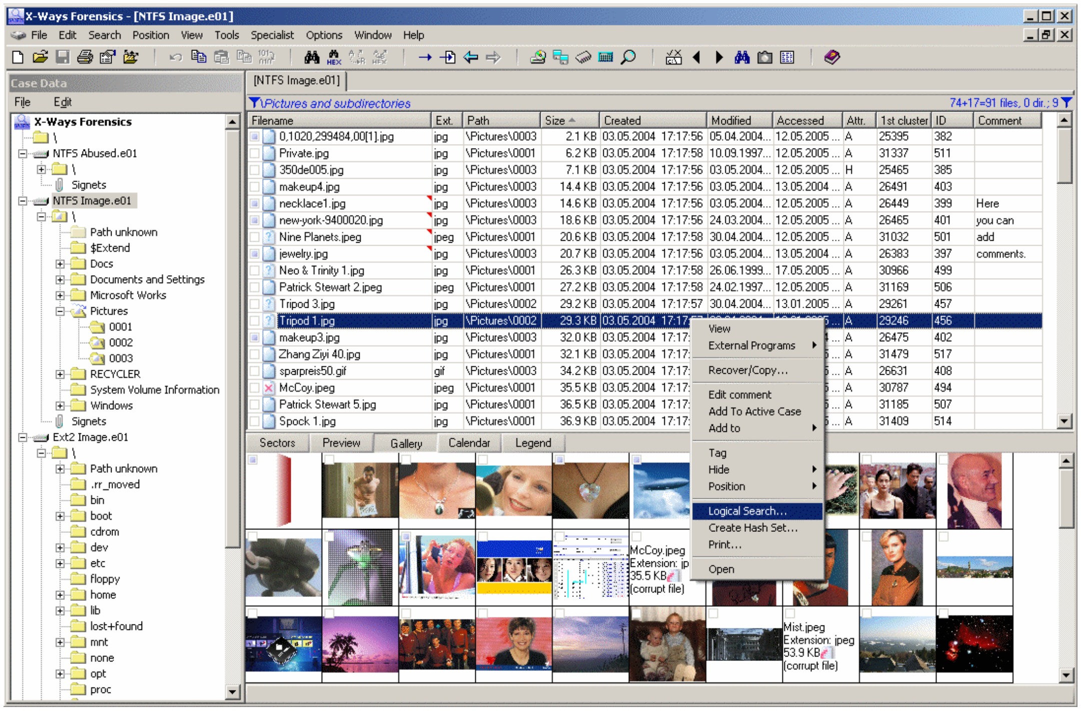
Part 5

- Matching files against hash sets in Hash Database
- Creating video stills from movie files
- Skin color percentage calculation and black and white detection
- PhotoDNA
- Identifying file type specific encryption and running statistical encryption tests

Module 10: Using Search Functions Effectively

- Practically unlimited numbers of keywords simultaneously
- Multiple encodings (Windows codepages, MAC encodings, Unicode: UTF-16, UTF-8) simultaneously
- Advantages of logical over physical search
- Searching inside archives, e-mail archives, encoded data (e.g. PDF documents)
- GREP search
- Logical combination of multiple keywords while evaluation results
- Filtering keywords based on the files they are contained in
- Exercise: Search

http://x-ways.com/forensics/index-m.html



Filename	Ext.	Path	Size	Created	Modified	Accessed	Attr.	1st cluster	ID	Comment
0,1020,299484,00[1].jpg	jpg	\Pictures\0003	2.1 KB	03.05.2004 17:17:56	05.04.2004...	12.05.2005 ...	A	25395	382	
Private.jpg	jpg	\Pictures\0001	6.2 KB	03.05.2004 17:17:58	10.09.1997...	12.05.2005 ...	A	31337	511	
350de005.jpg	jpg	\Pictures\0003	7.1 KB	03.05.2004 17:17:56	03.05.2004...	12.05.2005 ...	H	25465	385	
makeup4.jpg	jpg	\Pictures\0003	14.4 KB	03.05.2004 17:17:56	03.05.2004...	13.05.2004 ...	A	26491	403	
necklace1.jpg	jpg	\Pictures\0003	14.6 KB	03.05.2004 17:17:56	03.05.2004...	12.05.2005 ...	A	26449	399	Here
new-york-9400020.jpg	jpg	\Pictures\0003	18.6 KB	03.05.2004 17:17:56	24.03.2004...	12.05.2005 ...	A	26465	401	you can
Nine Planets.jpeg	jpeg	\Pictures\0001	20.6 KB	03.05.2004 17:17:58	30.04.2004...	12.05.2005 ...	A	31032	501	add
jewelry.jpg	jpg	\Pictures\0003	20.7 KB	03.05.2004 17:17:56	03.05.2004...	13.05.2004 ...	A	26383	397	comments.
Neo & Trinity 1.jpg	jpg	\Pictures\0001	26.3 KB	03.05.2004 17:17:58	26.06.1999...	17.05.2005 ...	A	30966	499	
Patrick Stewart 2.jpeg	jpeg	\Pictures\0001	27.2 KB	03.05.2004 17:17:58	24.02.1997...	12.05.2005 ...	A	31169	506	
Tripod 3.jpg	jpg	\Pictures\0002	29.2 KB	03.05.2004 17:17:57	30.04.2004...	13.01.2005 ...	A	29261	457	
Tripod 1.jpg	jpg	\Pictures\0002	29.3 KB	03.05.2004 17:17:		5 ...	A	29246	456	
makeup3.jpg	jpg	\Pictures\0003	32.0 KB	03.05.2004 17:17:		4 ...	A	26475	402	
Zhang Ziyi 40.jpg	jpg	\Pictures\0001	32.1 KB	03.05.2004 17:17:		5 ...	A	31479	517	
sparpreis50.gif	gif	\Pictures\0003	34.2 KB	03.05.2004 17:17:		5 ...	A	26631	408	
McCoy.jpeg	jpeg	\Pictures\0001	35.5 KB	03.05.2004 17:17:		5 ...	A	30787	494	
Patrick Stewart 5.jpg	jpg	\Pictures\0001	36.5 KB	03.05.2004 17:17:		5 ...	A	31185	507	
Spock 1.jpg	jpg	\Pictures\0001	36.9 KB	03.05.2004 17:17:		5 ...	A	31409	514	

Contact us today!