CDFS

CBIT Digital Forensics Services

X-Ways Forensics

Computer Forensics Training

This course is focused on the systematic and efficient examination of computer media using the integrated computer forensics software 'X-Ways Forensics'.

The students will learn e.g. how to get the most thorough overview conceivable of existing and deleted files on computer media, how to scan

X-Ways Forensics

Presented by:

Zoran Iliev

X-Ways Forensics Instructor
Master of eForensics and Enterprise Security

CDFS
CBIT Digital Forensics Services

X-Ways
Forensics

X-WAYS FORENSICS (4-DAY INSTRUCTOR-LED COURSE)

This course is focused on the systematic and efficient examination of computer media using the integrated computer forensics software "X-Ways Forensics".

Complete and systematic coverage of all computer forensics features in WinHex and X-Ways Forensics. Hands-on exercises, simulating most aspects of the complete computer forensics process. Attendees are encouraged to immediately try newly gained insights as provided by the instructor, with sample image files. Many topics are explained along with their theoretical background (slack: beyond the usual, how hash databases are internally structured, how deleted partitions are found automatically, with what methods X-Ways Forensics finds deleted files). Other topics are forensically sound disk imaging and cloning, data recovery, search functions, dynamic filtering, report creation, ... Emphasis can be put on any aspect suggested by the participants. You will receive reference training material for later repetition. Prerequisite: basic knowledge of computer forensics.

The students will learn e.g. how to get the most thorough overview conceivable of existing and deleted files on computer media, how to scan for child pornography in the most efficient way, or how to manually recover deleted files compressed by NTFS which would not even be found by conventional file carving techniques.

TOPICS INCLUDE:

- Basic setup of the software
- Learning the user interface components
- Navigating disks and file systems
- Understanding the Data Interpreter
- Creating disk images
- Creating a case/adding evidence objects
- Hash calculation and checking
- Using the gallery view and skin color detection efficiently
- Detecting data hiding methods
  (eg data streams, host-protected areas (HPA), misnamed files)
- Previewing file contents
- Calendar view and event list (timeline)
- Registry Viewer and Registry Reports, Registry Report definition files
- Working with the directory browser
- Filtering files
- Creating report tables and report table associations
- Using report tables for filtering and classification
- Report creation: Basic reports, report tables and activity log
- Refining Volume Snapshots:
- The Hash Database
- Various methods of file recovery
- Customizing file signatures
- Using search functions effectively
- Decoding Base64, Uuencode, etc.

Goal:
It is the goal to be able to draw sustainable conclusions from the data and metadata stored on or seemingly deleted from media to answer to specific problems while documenting the proceedings in a manner acceptable in court.

Examples:
"What documents were altered on the evening of January 12, 2012?"
"What pictures were hidden with what method, where and by whom?"
"Who viewed which web pages on what day?"
"Which MS Excel documents saved by Alan Smith contain the word 'invoice'?"
"Which USB sticks were attached to the computer at what time?"

trainer

Zoran Iliev
X-Pert | X-Ways Forensics Instructor

X-WAYS FORENSICS