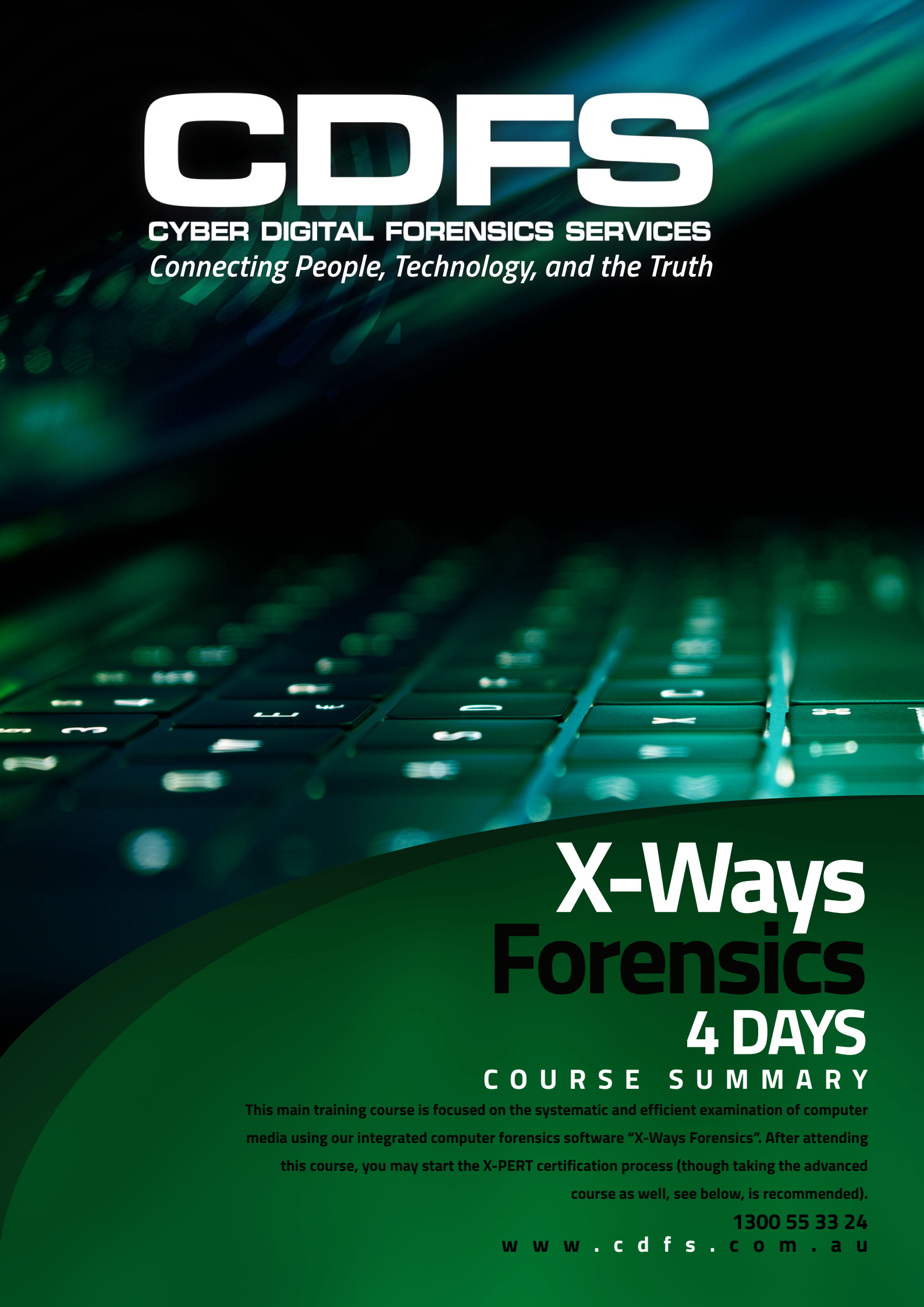


CDFS

CYBER DIGITAL FORENSICS SERVICES

Connecting People, Technology, and the Truth

X-Ways Forensics

4 DAYS

COURSE SUMMARY

This main training course is focused on the systematic and efficient examination of computer media using our integrated computer forensics software "X-Ways Forensics". After attending this course, you may start the X-PERT certification process (though taking the advanced course as well, see below, is recommended).

1300 55 33 24

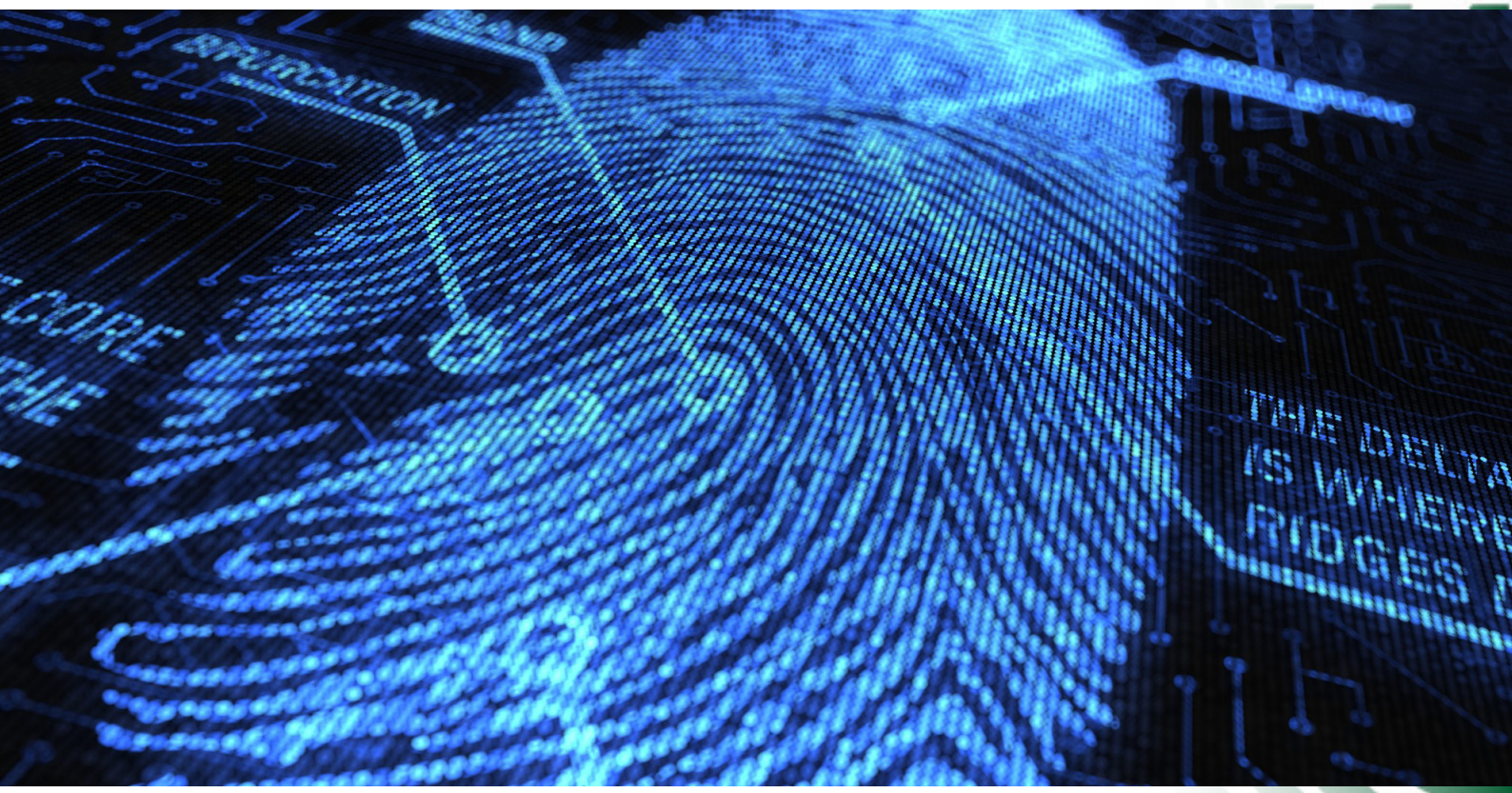
www.cdfs.com.au

CDFS
CYBER DIGITAL FORENSICS SERVICES
Connecting People, Technology, and the Truth

This main training course is focused on the systematic and efficient examination of computer media using our integrated computer forensics software "X-Ways Forensics". After attending this course, you may start the X-PERT certification process (though taking the advanced course as well, see below, is recommended).

Complete and systematic coverage of most 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 space, partially initialized space, how hash databases are internally structured, how deleted partitions are found automatically, with what methods X-Ways Forensics finds deleted files, etc. etc.). Other topics are forensically sound disk imaging and cloning, data recovery, search functions, dynamic filtering, report creation, ... You will receive complete printed 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, etc. There will be a practical exam at the end of the course, which you can regard as just another exercise for yourself or that you can take more seriously and get scored by the instructor if you like. The exam recapitulates the most important functions of the software and helps you to gauge your proficiency. The results will not be recorded by us in any way. Note that the instructor will present the answers to the test during the final 20 minutes.



- **Basic setup of the software**
- Key folder paths
- Read-only vs Edit vs. In-Place mode - WinHex vs. X-Ways Forensics
- Start-up options
- Alternative disk access methods
- Viewer programs

- **Learning the user interface components**
- 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

- **Navigating disks and file systems**
- Understanding offsets and sectors
- Absolute, relative and backwards positioning
- Directly navigating to specific file system structures (e.g. FILE records in NTFS, Inodes in Ext*)

- **Understanding the Data Interpreter**
- Available conversion options
- How to get the value you actually want

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

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

- **Creating a case/adding evidence objects**
- **Hash calculation and checking**
- **Using the gallery view and skin color detection efficiently**
- **Detecting data hiding methods like alternate 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**
- Recursive listing of directories and entire drives
- Column visibility and arrangements
- Copying cell values
- Selecting, tagging, hiding, viewing, opening files
- Recovering/copying files
- Identifying duplicates based on hash
- Efficient navigation of the file systems' data structur

- **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
- By size
- By one or more timestamps
- By attributes: ADS, compression, encryption, e-mail (unread, with attachment), video still, ...

- **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:**
- File system specific thorough data structure search for previously existing data
- Signature search for previously existing data not identifiable via file system metadata
- Verifying file types based on signatures on algorithms
- Extracting metadata from a variety of file types
- Analyzing browser history for Internet Explorer, Firefox, Safari, Chrome
- Analyzing Windows Event Logs (evt and evtx)
- 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.
- Creating video stills from movie files
- Skin color percentage calculation and black and white detection
- Identifying file type specific encryption and running statistical encryption tests

- **The Hash Database**
- Importing single or multiple hash sets
- Creating your own hash sets
- Matching files against existing hash sets via Refine Volume Snapshot

CDFS
CYBER DIGITAL FORENSICS SERVICES
Connecting People, Technology, and the Truth

- **Various methods of file recovery**
- **Customizing file signatures**
- **Using search functions effectively**
- Practically unlimited numbers of keywords simultaneously
- Multiple encodings (Windows codepages, MAC encodings, Unicode: UTF-16, UTF-8) simultaneously
- The many 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
- **Decoding Base64, Uuencode, etc.**

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?"

Price

$6000 ex GST
Per Participant

Or

4 Vouchers
ex GST Per Participant