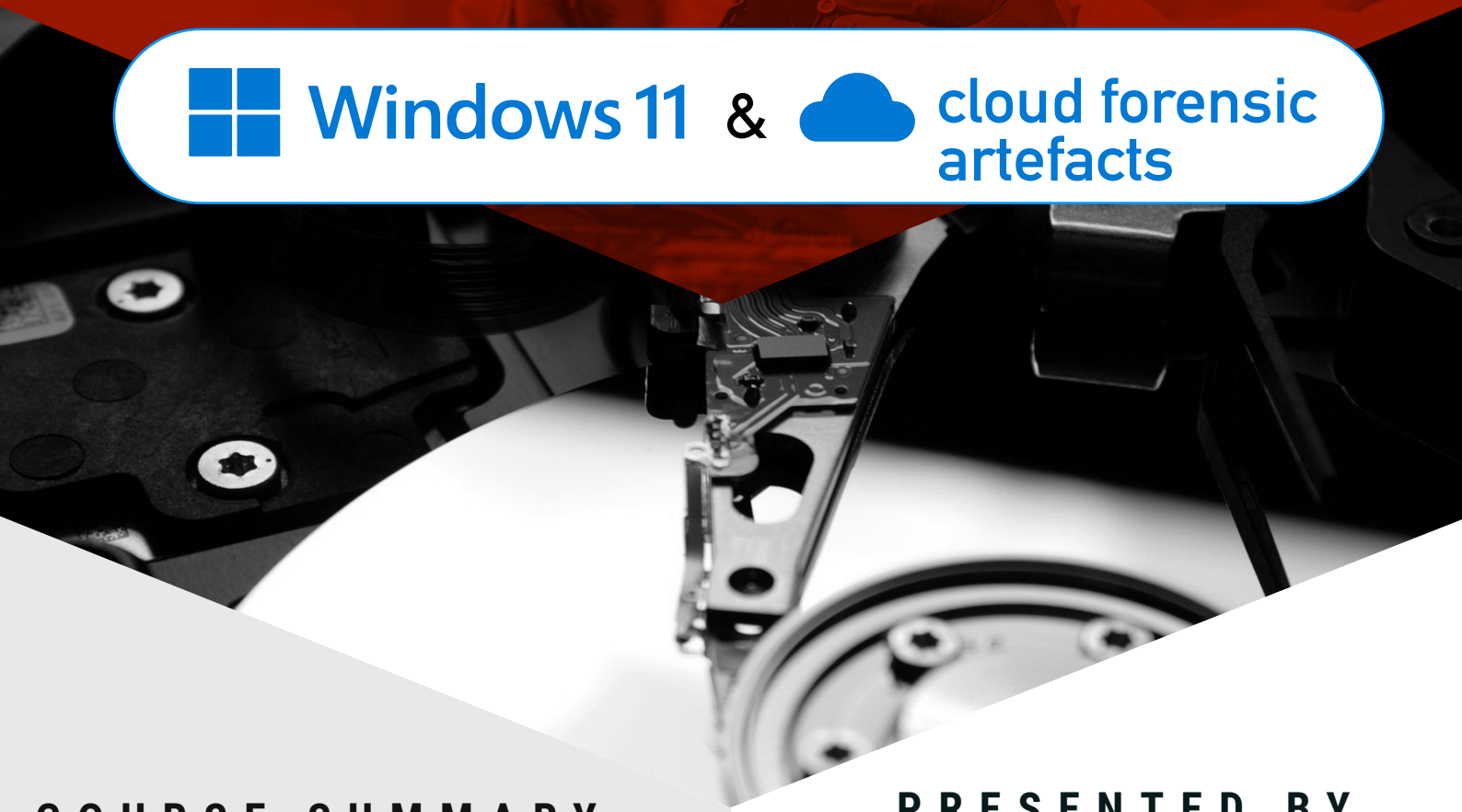
CDFS

CBIT DIGITAL FORENSICS SERVICES

CCE BootCamp VERSION 6

NOW INCLUDING

Windows 11 & cloud forensic artefacts



COURSE SUMMARY

This is the Official CCE BootCamp® that will teach you what you need to know to successfully take the Certified Computer Examiner (CCE)® certification examination.

PRESENTED BY

Zoran Iliev

CCE Instructor

Master of eForensics and Enterprise Security

NEW CCE BOOTCAMP V6

NOW INCLUDING

Windows 11 & cloud forensic artefacts

An intensive 5-day course, the Bootcamp will teach you how to conduct forensically sound computer examinations across a wide range of systems and devices. This latest version comes with the addition of new material covering both Windows 11 and cloud artefacts. You will learn additional material on topics such as jump lists and LNK files, the Windows Timeline and event logs, volume shadow copies, shellbags, and cloud storage such as OneDrive, O365, Dropbox, Google Drive and the iCloud.

Equipment

Students will use the Guardonix USB3.0 writeblocker and stabilizer in many practical hands-on activities. This device is made by DeepSpar, a leader in data recovery hardware since 2004.

Updated Training Material

Many updates to the training manuals include:

- Windows 11 operating system
- New training exercises including the latest file systems

CCE BOOTCAMP

Module 1

Introduction to Computer Forensics

- What makes a good computer forensic examiner?
- Computer forensics vs. e-Discovery
- Dealing with clients or employers
- Examination scope and client contracts
- Legal and privacy issues
- Ethical conduct
- Cases that may include digital evidence
- Forensic examination procedures
- Hardware and imaging issues
- USB and optical media examination
- Limited examinations and e-Discovery
- Forensic sterilisation processes
- Documentation and reporting
- The ASCII table
- A general overview of the boot process and Operating Systems
- BIOS history
- Networked computers
- Media acquisition and documentation
- Chain of custody

Module 2

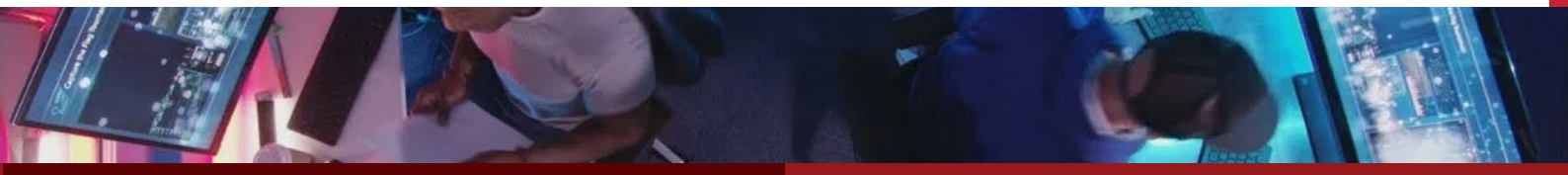
Imaging

- Imaging theory and process
- Imaging methods
- Write blocking
- Imaging USB devices
- Wiping, hashing, validation, image restoration, cloning, and unallocated space
- Drive partitioning

Module 3

File Signatures, Data Formats & Unallocated Space

- File identification
- File headers
- General file types
- File viewers
- Examination of compressed files
- Data carving



Module 4
FAT File System

- Logical structures of DOS and the Windows operating systems
- The Master Boot Record
- The File Allocation Table
- 16-Bit FAT
- 32-Bit FAT
- Directory entries
- Clusters
- Unallocated space
- Sub-directories
- File recovery and fragmentation

WHY DO WE STILL TEACH THE DOS FAT FILE SYSTEM?

You may be wondering why we still teach the DOS FAT file system? A sound understanding of the FAT file system is essential, as it is still a very common file system widely used in portable devices such as USB thumb drives, and memory cards found in digital cameras and mobile phones. These types of portable media can often hold valuable forensic evidence, and for this reason a solid understanding the FAT file system is an important part of becoming a qualified digital forensic examiner.

Module 5
NTFS

- Introduction and overview
- Basic terminology
- Basic boot record information
- Time stamps
- The root directory
- The Recycle Bin
- File attributes, creation and deletion
- Examining NTFS drives

Module 6
Registry & Artifacts

- BitLocker
- Windows Spool, Swap and Page Files
- Analysis of the Windows Registry
- Browser artifacts
- Windows Mail
- Common situations encountered during examinations
- Password protection and defeating passwords
- Compound documents
- Examining optical media

Module 7

Forensic Policy, Case Writing, Legal Process & Forensic Tool Kits

- Use of policy and checklists in forensic practice
- Data presentation to the client
- Case report writing
- The legal process
- Expert admission
- Going to court

Approximately 40% of the CCE BootCamp® consists of hands-on, comprehensive practical exercises that will guide you through best practice forensic skills. Successful course completion requires the submission of at least three written reports based on the results of specific practical exercises. These reports may be submitted to the instructors during the training class or within the 6 weeks of additional instructor support provided at the conclusion of the training class. Students must have strong computer skills, including the ability or desire to work outside the Windows GUI interface and handle computer hardware. The online multiple-choice portion of the CCE certification test is administered at the end of each CCE BootCamp®.

PRICE

$7,500
per person ex GST

OR

5 VOUCHERS
per person ex GST

* Vouchers can only be used for courses delivered by CDFS at our training facility or via Virtual Instructor-Led Training.

CDFS

CBIT DIGITAL FORENSICS SERVICES

Please contact the CDFS team to discuss your requirements.

1300 553 324

contact@cdfs.com.au