



**XIONGROUP**

**Authorised Training Partner**

34 Circular Road  
Singapore 049390

**opentext™**

# DF320 - Advanced Analysis of Windows Artifacts with EnCase

*Formerly EnCase Advanced Computer Forensics*

## COURSE INFORMATION

Course duration:  
**4 days**

CPE Credits:  
**32**

Delivery method:  
**Group-Live**

Instructor:  
**Frank Butler**

NASBA defined level:  
**Advanced**

Prerequisites:  
**DF210 - Building an Investigation with EnCase**

## CONTACT INFORMATION

Call:  
**+65 6610 3488**

Email:  
**enquiries@xiongroup.com**

Website:  
**www.xiongroup.com/training**

## Syllabus

### Day 1

Day one begins with an overview of SQLite databases and how to query the data they contain followed by a practical exercise allowing the students to exercise these new skills and knowledge. Next, instruction continues with techniques on recovering deleted SQLite data.

The last lesson of the day focuses on to how to use block-based file hash analysis to recover deleted target files even if those files have been fragmented or partially overwritten followed by a practical exercise.

### The main areas covered on day 1 include:

- Documenting the aspects of SQLite that will be most relevant to the forensic investigator
- Using Structured Query Language (SQL) to query SQLite data
- Understanding the structure of SQLite database files and how and why deleted data may be recoverable
- Using block-based hash analysis for file recovery

### Day 2

Day two begins with instruction regarding the structure of the Windows® Registry and the examination techniques of associated artifacts. Students are shown how to extract registry values to facilitate the mounting of them into their own system in support of running applications extracted from the evidence file.

Next, the students are taught how to locate, recognize, and interpret Userassist and ShellBag data within the registry and how to automate decoding of the entries. The students will then be introduced to the Microsoft® Windows® Prefetcher and shows them how to locate and examine the Prefetch files and their value in determining application usage.

Instruction continues with extracting and analyzing various application databases followed by an examination of Windows Timeline, Notification and System Resource Usage Monitor features.

Practical exercises will be administered throughout the day, allowing students to test their newly learned skills.

### The main areas covered on day 2 include:

- Understanding the purpose and structure of the Windows Registry
- Identifying, mounting, and extracting data from registry hive files both in OpenText™
- EnCase™ software and within Windows on a forensic examination machine
- Recreating the registry data necessary to run an extracted application on the examiner's forensic workstation
- Mapping local and domain-level user accounts
- Examining Userassist registry data
- Parsing ShellBag data in conjunction with NTFS USN change-log data
- Understanding the purpose of the Windows Prefetcher and the structure and content of the prefetch files it maintains
- Understanding and accessing various application databases
- Understanding the Windows Timeline feature and how it can be used to demonstrate user activity
- Understand the Windows Push Notifications feature, how it can be configured, and interpreting that information
- Understanding the System Resource Usage Monitor and how it can provide useful information about application usage

### Day 3

Day three begins with a practical exercise focusing on the instruction provided on the Windows Registry. Next, the students learn how to locate, recognize and examine Microsoft Windows event logs. They will explore the Volume Shadow Copy Service (VSS). This function allows volume backups to be created while file system write operations are temporarily frozen. On later versions of Windows, the method of backing up user data is replaced by Windows File History.

The last lesson on day three provides instruction on the history and terminology associated with encrypted data. The students will also learn the principles behind the recognition of encryption software and encrypted data and how they should approach the decryption of such data.

Students participate in practical exercises throughout the day.

### The main areas covered on day 3 include:

- Analyzing Windows event logs
- Learning about VSS operation and how to examine VSS data and the introduction and use of Windows File History under later versions of Windows
- Understanding what encrypted data is and the terminology associated with it
- Learning about the identification of encryption software, encrypted data and exploring the methodology behind decrypting such data

## Day 4

Day four begins with a lesson on decrypting a Windows BitLocker® protected volume. Students learn various techniques for examining RAM and for recovering information from ZIP archives and how this can be used to recover data from the latest type of Microsoft Word documents.

Next, the students will discuss the technology behind hardware and software RAID devices, how these devices should be forensically examined and how the RAID functionality within EnCase functions.

Students will complete relevant practical exercises throughout the day, reinforcing their new knowledge.

### The main areas covered on day 4 include:

- Exploring the recovery options for decrypting Windows BitLocker protected volume
- Learning how to setup and configure the ability to conduct examinations of RAM
- Discussing the ZIP file format and how it affects the ability to locate and recover ZIP data
- Using knowledge of the ZIP file format to recover data from the latest version of Microsoft Word documents
- Understanding RAID configurations and stripe sets
- Understanding how RAID affects forensic examinations
- Discussing options for forensic acquisition of RAID devices and their examination in EnCase software