



# ENCASE® EFS MODULE



## EFS (Microsoft Encrypting File System) decryption support for EnCase

### EnCase® EFS Module

The EnCase® EFS Module provides the examiner the ability to automatically decrypt Microsoft Encrypting File System (EFS) encrypted files and folders, for locally authenticated users. Since EFS is key-based, only the user who encrypted the file(s) is able to decrypt and view the file contents, unless the user's password is known. EFS encryption has traditionally posed obstacles for examiners, as the EFS encryption process creates illegible and indecipherable text within files.

The automation and decryption capability of the EnCase® EFS Module allows examiners to concentrate their efforts on investigative analysis, rather than spending excessive time attempting to break EFS encryption. The EnCase® EFS Module supports all Microsoft EFS platforms: Windows 2000 Professional and Server, Windows XP Professional and Windows 2003 Server. However, the decryption capability is slightly different based on the Microsoft platform and the user logon configuration:

### Windows 2000

The EnCase® EFS Module provides automatic decryption capability for EFS encrypted files and folders on target Windows 2000 computers, for locally authenticated users. Windows 2000 EFS decryption is accomplished without any input or password cracking by the examiner, as the EnCase® EFS Module is able to obtain all of the keys necessary to automatically decrypt files and folders.

# ENCRYPTING FILE SYSTEM

## **Windows XP and 2003 Server**

The EnCase® EFS Module provides decryption capability for EFS encrypted files and folders on target Windows XP and Windows 2003 Server operating systems, for locally authenticated users. However, given the enhanced security features of Windows XP and Windows 2003 Server, the user account password must be provided within EnCase® to complete the decryption. EnCase® provides several methods of obtaining the password including; a brute force attack of the password with dictionary files, using EnCase® to recover the encrypted password from a Password Recovery/Reset Disk, and exporting local user accounts from EnCase® to a file importable by specialized NTFS cracking software.

## **User Configured Domain Auto-Login**

The EnCase® EFS Module provides decryption capability for computers that have been configured to use the auto-login feature in Windows 2000, 2000 Server, XP, and 2003 Server. Auto-login automatically logs the computer onto the network domain when the computer is booted. The EnCase® EFS Module automatically recovers the password and decrypts the files for computers utilizing the Windows auto-login feature.

## **Purchasing**

EFS decryption capability is a separate module within EnCase® Version 4. It requires an EFS Certificate to be purchased from Guidance Software and placed on the EnCase® Examiner machine. To order the EFS Certificate, please contact Guidance Software Sales: sales@guidancesoftware.com. When ordering the EFS Certificate, please be prepared to provide the security key serial number (dongle ID#). This number can be located within EnCase by clicking "Help" on the top menu and selecting "About EnCase."

## **About Guidance Software**

Guidance Software is the leader in computer forensics and incident response solutions. Founded in 1997 and headquartered in Pasadena, CA, Guidance Software has offices and training facilities in California, Virginia and the United Kingdom. More than 12,000 corporate and government investigators depend on EnCase® software, while more than 3,500 investigators attend Guidance Software's forensic methodology training annually. Accepted by numerous courts and honored with *eWEEK's* Excellence Award and *SC Magazine's* Annual Award, EnCase® software is considered the standard forensic tool. For more information, visit Guidance Software's Web site at [www.guidancesoftware.com](http://www.guidancesoftware.com).