

# EnCase® ProSuite

Powerful tools to help reduce time, costs and complexity

## EnCase® ProSuite Modules:

### VFS (Virtual File System)

- Mounts evidence virtually

### PDE (Physical Disk Emulator)

- Emulates subject's environment

### EDS (EnCase Decryption Suite)

- Suite of decryption tools

## What You Get:

- Powerful, integrated tools
- Convenient way to review forensic data with non-EnCase users
- Ability to integrate third-party applications to expand analysis
- Decryption of encrypted files

EnCase® ProSuite is bundle of tools that extends analysis capabilities for EnCase® Forensic.

Expand review and analysis of EnCase evidence!

Forensic Examiners are faced with the challenges associated with working evidence that may be encrypted, or require the use of tools outside the scope of EnCase, or need an investigator or legal representative to review it. Sometimes just looking at the evidence with a different perspective or tool can provide valuable information to an investigation.

EnCase ProSuite gives the investigator maximum flexibility with a powerful combination of integrated tools for use with EnCase Forensic. Seamless integration of tools is key to taking advantage of expanded capabilities. It helps reduce potential corruption of evidence and uses a single interface to launch programs.

### Efficient Investigations

Something as simple as running a virus scanner or other third-party Microsoft® Windows® applications on a piece of evidence can take hours and resources. With ProSuite there is no need to restore your evidence on a clean drive to run utilities. Just mount the drive and proceed. This will save a lot of time and the cost of stocking hard drives.

In addition, the decryption capabilities will allow examiners to concentrate efforts on investigative analysis, rather than spending excessive amounts of time trying to decrypt data.

### Add Simplicity

Examiners rely on EnCase Forensic to provide in-depth analysis of subject data. Once the relevant data is produced, it may need to be reviewed by investigators or legal staff who may not be trained in computer forensics. Adding EnCase ProSuite will provide a vehicle to give non-EnCase users evidence to review in a more familiar environment.

## VFS - Virtual File System

EnCase evidence is served virtually to Windows in a read-only format and placed on a local or network share drive. Further analysis can now be accomplished using Windows Explorer, third-party Windows utilities or other analytical tools.

- **Mounts evidence at the case, device, volume or folder level**
- **Provides an easy platform for evidence review in a read-only state, outside EnCase for investigators or non-forensic examiners**
- **Captures file system artifacts contained in the EnCase environment, including all allocated files, deleted files, internal system files, alternate data streams and unallocated space**
- **Potential support tools include: file carving utilities, antivirus, antispyware, trojan detectors, steganography detectors, word indexers, undelete software and encryption detection software**
- **File systems supported: DOS (FAT12/16/32, NTFS), Linux (EXT2, EXT3, Reiser), UNIX® (Solaris UFS), Macintosh® (HFS, HFS+), BSD (FFS), CD/DVD (Joliet, ISO 9660, UDF, DVD) and Palm® (Palm OS)**
- **Easily mounts Windows RAIDS, dynamic disks rebuilt by EnCase software and drives compressed or encrypted by NTFS**
- **VFS server mounts the evidence on the network share drive**

## PDE - Physical Disk Emulator

EnCase evidence is served to a local drive in a read-only state. Using VMware to boot Windows or some other operating systems, examiners can view applications or other functions in the same manner as a user may have done.

- **Mounts images of hard drives or CDs**
- **Enables the use of third-party analysis tools**
- **Emulates the subject's environment in the same state as it was in when the evidence was captured**
- **Provides a platform for review for non-EnCase users**
- **VMware bootable file systems include: Windows (DOS, FAT 12/16/32, NTFS), Linux® (SuSE, Red Hat and Mandrake), Free BSD and NetWare**
- **Does not capture some file system artifacts such as deleted files or unallocated space**

## EDS - EnCase® Decryption Suite

EDS enables decryption of encrypted files and folders by domain users and local users by leveraging the encryption's native authentication systems. It can quickly decrypt encrypted information from either the registry or the attached devices.

### Decryption capabilities include:

#### Disk and volume encryption

- Microsoft BitLocker™
- GuardianEdge® Encryption Anywhere
- GuardianEdge Plus
- Ultimaco® SafeGuard Easy
- McAfee® SafeBoot

#### File Based encryption

- Microsoft Encrypting File System (EFS)
- CREDANT Mobile Guardian

#### Mounted files

- PST (Microsoft Outlook®)
- S/MIME encrypted email in PST
- NSF (Lotus Notes®)
- Protected Storage (ntuser.dat)
- Security hive
- Active Directory 2003 (ntds.dit)



Guidance Software, Inc. is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be addressed to the National Registry of CPE sponsors, 150 Fourth Avenue North, Nashville, TN, 37219-2417. Web site: [www.nasba.org](http://www.nasba.org)

### About Guidance Software (GUID)

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organizations to conduct thorough, network-enabled, and court-validated computer investigations of any kind, such as responding to eDiscovery requests, conducting internal investigations, responding to regulatory inquiries or performing data and compliance auditing - all while maintaining the integrity of the data. There are more than 30,000 licensed users of the EnCase technology worldwide, and thousands attend Guidance Software's renowned training programs annually. Validated by numerous courts, corporate legal departments, government agencies and law enforcement organizations worldwide, EnCase has been honored with industry awards and recognition from *eWEEK*, *SC Magazine*, *Network Computing*, and the *Socha-Gelbmann survey*. For more information about Guidance Software, visit [www.guidancesoftware.com](http://www.guidancesoftware.com).

©2009 Guidance Software, Inc. All Rights Reserved. EnCase and Guidance Software are registered trademarks or trademarks owned by Guidance Software in the United States and other jurisdictions and may not be used without prior written permission. All other marks and brands may be claimed as the property of their respective owners.