

EnCase® ProSuite

Reduce investigation complexity, time and costs with a powerful suite of tools

EnCase ProSuite is a powerful combination of tools that facilitates the seamless sharing of evidentiary information to third-party applications and solves the resource drain of encrypted data.

- Powerful, integrated tool suite delivers convenience and maximum flexibility during investigations
- A convenient way to review forensic data with non-EnCase users
- Facilitates the use of third-party applications to view and analyze forensic data served by EnCase software
- Decrypt EFS encrypted files and display passwords stored in the Windows® Registry

Although most investigative challenges can be solved with EnCase Forensic, sometimes it's necessary to further examine forensic data outside of the EnCase environment or use additional tools on data served by EnCase software.

Evidence may need to be reviewed by legal representatives or other non-users of EnCase software, and it is easier to present that information to those people in an environment familiar to them. Also, investigators often want to use third-party Microsoft® Windows® applications to further analyze exposed data. Finally, another challenge to viewing and sharing data is the time spent by investigators in their attempts to decrypt and unlock protected files. This diverts focus from the investigation at hand.

EnCase ProSuite solves these challenges with a powerful combination of integrated tools. It gives investigators maximum flexibility during investigations, and the ProSuite helps mask the complexity of forensic data when it's shared with untrained individuals.

HOW IT WORKS

Forensic data is served from EnCase software to Windows as read-only and can then be further analyzed with common applications, such as Windows Explorer, third-party Windows utilities or other analytical tools. This allows evidence to be viewed and analyzed in a format that may be more familiar to non-investigators and non-users of EnCase Forensic.

Examiners are able to boot Windows and other operating systems from EnCase data, using VMware. This allows the examiner to interact with the operating system as the user does or as the application did, but in a read-only state.

EnCase ProSuite also provides a method to easily decrypt Microsoft EFS encrypted files, as well as Utimaco and PC Guardian encrypted devices. This decryption capability allows examiners to concentrate efforts on investigative analysis, rather than spending excessive amounts of time trying to decrypt data. By leveraging the encryption's native authentication systems, ProSuite makes it possible to quickly decrypt encrypted information either from the registry or the devices.

EnCase ProSuite consists of...

EnCase® Virtual File System

- Mounts evidence at the case, device, volume or folder level as a read-only network share.
- Provides an easy platform for information for evidence review in a read-only state, outside of the EnCase environment.
- Files contain the same file system artifacts as contained in the EnCase environment, including all allocated files, deleted files, internal system files, as well as alternate data streams and unallocated space.
- Once mounted, the read-only media is available to any native application:
Windows Explorer and third-party Windows applications or computer forensic tools, such as file carving utilities, virus checkers, spyware detectors, trojan detectors, steganography detectors, word indexers, undelete software and encryption detection software.
- Review evidence with anyone, not just those running EnCase 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.

EnCase® Physical Disk Emulator

- Mounts images of hard drives or CDs as read-only local drives.
- Enables the use of third-party tools on forensic data exposed by EnCase software.
- When using VMware, it enables the examiner to boot and interact with the computer in the same state as it was when the evidence was captured.
- Provides a platform for juries to view digital evidence in a way that they may better understand.
- Reduces the number of drive restores, saving time and money needed to stock hard drives.
- Mounts a number of file systems not recognized by Windows Explorer, but still recognized and bootable by VMware. While Windows does not read the Linux and Free BSD formats, the following file system formats are still bootable with VMware: Windows (DOS, FAT 12/16/32, NTFS), Linux (SuSE, Red Hat and Mandrake), Free BSD and NetWare.

EnCase® Decryption Suite

- Support for Microsoft® Encrypting File System (EFS) encrypted files and folders, including domain-authenticated accounts.
- Support for decryption of PC Guardian and Utimaco disk-based encryption products.
- Support for Outlook® PST passwords, (Except Outlook 2004).
- Enables the automatic decryption and analysis of the Windows registry protected storage area for Internet Explorer®.

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 and effective computer investigations of any kind, such as intellectual property theft, incident response, compliance auditing and responding to eDiscovery requests—all while maintaining the forensic integrity of the data. There are more than 20,000 licensed users of the technology, and thousands of investigators and corporate security personnel attend Guidance Software's forensic methodology training annually. Validated by numerous courts worldwide, EnCase is also frequently honored with top security awards and recognition from *eWEEK*, *SC Magazine* and *Network Computing*, as well as the *Socha-Gelbmann* survey.