EnCase Forensic

Version 8.07

Release Notes

EnCase Forensic Version 8.07

Thank you for using Guidance Software products.

Guidance Software recommends that you read the EnCase Forensic *Release Notes* prior to installing your product. This document provides the most current list of new features, fixed items, compatibility details, and supported platforms.

SAFE Version

The Guidance Software SAFE and Configuration Tool version for this release is a.07.

New Features

macOS APFS Support

EnCase Forensic now supports APFS, the file system used in the Apple High Sierra operating system (macOS 10.13).

The following APFS features are not yet supported in this release: snapshots, crash protection, checkpoints, fast directory sizing, and encryption support.

Support for Symantec PGP Version 10.3

EnCase Forensic now supports Symantec PGP Version 10.3.

Support for Dell Data Protection 8.17

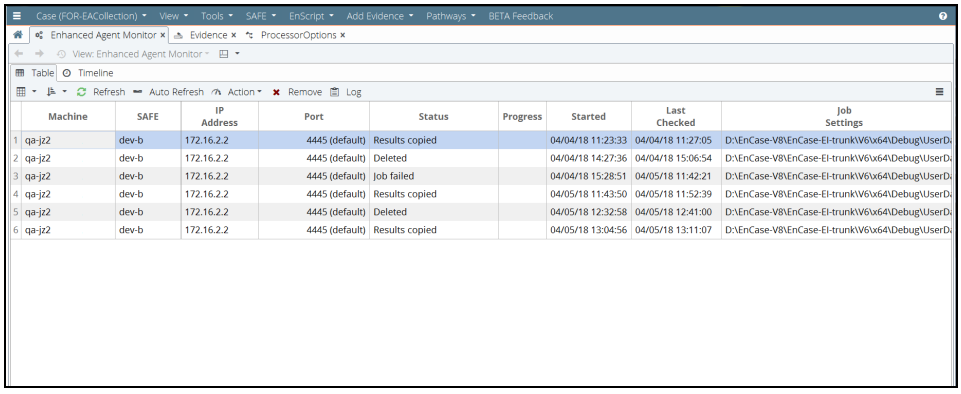
EnCase Forensic now supports Dell Data Protection Version 8.17.

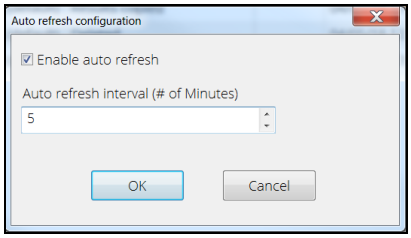
Support for Microsoft BitLocker XTS-AES

EnCase Forensic now supports decryption of the Microsoft BitLocker XTS-AES encryption algorithm.

Auto Refresh Added to Enhanced Agent Monitor Tab

The Enhanced Agent Monitor tab in EnCase Forensic now has auto refresh functionality and will refresh jobs every five minutes by default. You can manually refresh from the title bar using the Refresh button, or you can change settings by clicking the Auto Refresh button in the Enhanced Agent Monitor tab title bar and making changes in the dialog box that displays.





Add Word Delimiters to Search Index

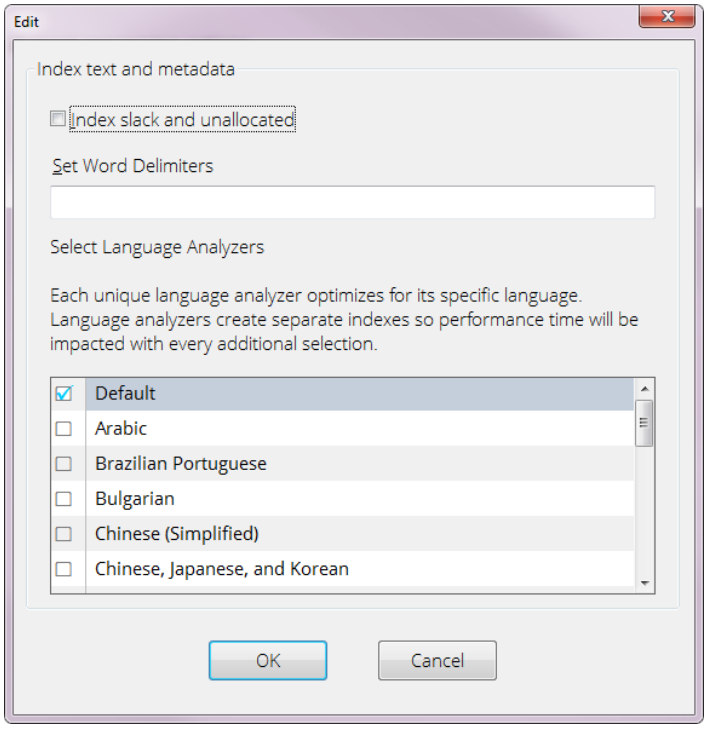
You can now add word delimiters to your search index in addition to the default delimiters used with each language analyzer. Word delimiters are used to identify breaks between words in indexed data. Each Language analyzer has one or more standard delimiters it uses by default. There is no need to enter a delimiter if the language you are indexing uses that delimiter by default.

The indexing engine in EnCase Forensic uses the following delimiters for all analyzers by default. There is no need to add a delimiter if it is in this list.

```
!#$%&()*+,-\/;<=>?@[]^`{|}~
```

To add word delimiters for indexing:

1. From the Evidence tab, select the evidence you want to process, then select **Process Evidence** > **Process** from the menu bar of the Evidence tab. The EnCase Processor Options dialog displays.
2. Click the **Index text and metadata** link to display the Edit Index text and metadata dialog.
3. Enter one or more word delimiters without spaces in the text box.



4. Click **OK**.

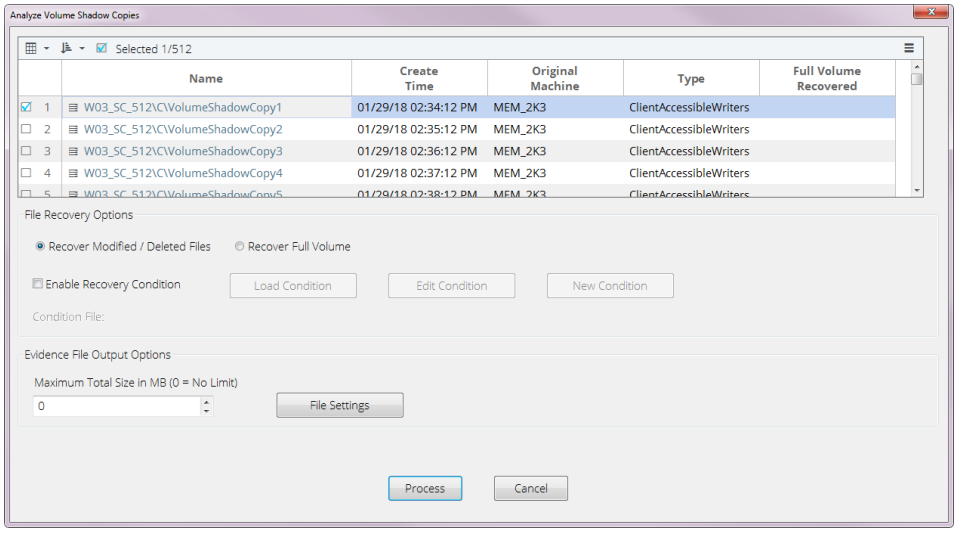
Once your evidence is processed, all data will be indexed with the default word delimiters for the language analyzer as well as any additional delimiters added during processing. Any additional word delimiters entered during processing can be viewed by right-clicking on **Index text and metadata** link in the EnCase Processor Options dialog. The table that displays lists all current processing options.

Windows Volume Shadow Copy Support

You can now use EnCase Forensic to analyze Volume Shadow Snapshot (VSS) backups (also known as volume shadow copies). Using the new Analyze Volume Shadow Copies module, you can use a recovery condition to select and recover specific modified or deleted files, or you can recover a full volume. Volume shadow copies enable volume analysis over time. Volume shadow copy functionality requires the file system to be NTFS.

To view or restore a volume shadow copy:

1. Select **Tools** > **Analyze Volume Shadow Copies**. A dialog displays a table of shadow copy volumes and file recovery options.



2. Select the checkboxes next to the volume or volumes you want to process from the table.
3. Select **Recover Modified / Deleted Files** to recover a portion of a shadow copy volume or **Recover Full Volume** to recover an entire volume.
4. Check **Enable Recovery Condition** and a condition button to apply a condition during file recovery.
    - **Load Condition** - load a pre-existing condition from the default EnCase Conditions folder or browse to locate another condition.
    - **Edit Condition** - edit an existing condition using the Conditions editor.
    - **New Condition** - create a new condition in the default EnCase Conditions folder.

    Note: Conditions cannot be applied to a full volume recovery.

5. Select the maximum total size of the evidence file or use the default `0` value for no file size limit.
6. Click the **File Settings** button to change output file settings. The Default Output Options dialog displays.
    - A partial shadow copy volume outputs to `.Lx01` logical evidence files.
        - Change the file name, evidence number, case number, examiner name, output path, or alternative path on the Location tab.
        - Change the evidence file format, compression, file segment size, or encryption settings on the Format tab.
    - A full shadow volume recovery outputs to `.Ex01` evidence files.
        - Change the file name, evidence number, case number, examiner name, output path, or alternative path on the Location tab.
        - Change the evidence file format, verification hash, compression, file segment size, or encryption settings on the Format tab.
        - Change additional settings on the Advanced tab.

7. Click **Process** to begin the volume recovery.

EnCase Forensic recovers and adds the volume shadow copies to your case as evidence files.

Mobile Acquisition Enhancements

Mobile Data Triage

Mobile Data Triage has been added for cases acquired from Android devices and iPhone devices, and imported from iPhone backups.

Android File System Acquisition Improvements

File system acquisition for Android devices has been improved. File systems from more devices can now be acquired.

iCloud Imports

EnCase Forensic can now import iCloud backups.

Data Parsing Added for More Applications

Application data parsing for Android devices has been added for the following applications:

- Firefox
- WeChat

WhatsApp Application Parsing Improvements

WhatsApp application data parsing for Android devices has been improved.

Items Fixed

FOR-8964: Previously, EnCase Forensic had difficulty detecting some hard drives larger than 2 TB when connected via UASP hot-swap docks. This issue has been resolved.

FOR-8990: An issue in EnCase Forensic was identified that prevented the use of backup volume boot record data to rebuild file structures. This issue has been resolved.

FOR-9811: EnCase Forensic now displays the correct logical size of files larger than 4 GB in UDF file systems.

FOR-9904: An issue that prevented the decryption of drives encrypted using PGP in EnCase Forensic v8.x has been resolved.

FOR-9951: When entering Syskey or encrypted password files in the secure storage tab, EnCase Forensic now directs the user to select the path to the file. Previously, EnCase Forensic attempted to access a floppy drive.

FOR-10779: Parsing issues with the Tinder application on Android and iOS have been fixed.

Known Limitations

Found in Version 8.07

AGENT-2808: When EnCase Forensic parses a live acquisition of Apple macOS devices that use APFS, it is possible that parts of the acquisition may be incomplete or contain inaccuracies. This occurs because devices that use APFS can modify file system objects during acquisition. A greater number of artifacts can result when acquiring large volumes, or when there is increased system activity on the machine.

AGENT-2859: Users logged into their SAFE user account can delete their own SAFE user record.

FOR-10826: Due to the structure of APFS containers and volumes, navigation of APFS devices in disk view can appear confusing when moving across clusters.

FOR-11087: Items in quick search pane do not match items in the table pane.

FOR-10958: When dropping APFS evidence into EnCase Forensic, the data fails to load if you process the evidence before opening it. The workaround is to open the evidence first and then process it.

FOR-11089: Because EnCase Forensic parses macOS APFS volumes directly, the timestamp values of files match those found in the terminal command line rather than the corresponding timestamp values displayed in the Finder.

Found in Version 8.06

AGENT-2554: macOS agents deployed on High Sierra (10.13) targets can only parse evidence from HFS+ devices. macOS High Sierra (10.13) devices using Apple File System (APFS) are not supported.

FOR-8181: The ability to index personally identifiable information (PII) is not supported in this version of EnCase Forensic.

FOR-9360: When you process evidence with the **Expand compound files** option selected, file transcripts can not be directly viewed within the compound file. You must select an individual file within the archive file to view a transcript of that file.

FOR-9507: Compound words containing any of the following three stop words (period/dot, underscore, single quote) do not highlight the entire word in highlight view. For example, a search for the word, `primary`, would only highlight the word `primary` in `primary.user@email.com`, but not the text after the period, `.user@email.com`. This issue only affects highlighting. Search and indexing are unaffected by this highlighting issue.

FOR-9612: Indexing is performed in English by default, and the term, Default, will display in the Query Actions Bar of the Indexed Items tab unless another language analyzer is chosen instead of English. The term, English, should display instead of Default where English is the chosen language.

Found in Version 8.04

AGENT-771: When running a 32-bit Windows operating system, the .NET 4.5.1 runtime must be installed before running the combined SAFE/License Manager installer. If it is not present, the SAFE will not be installed successfully.

FOR-6647: Parsed 7-Zip files do not display physical size, initialized size, or file extents. Instead, they display the default value of 0.

FOR-6432: EnCase Forensic does not run on Windows Nano Server 2016.

FOR-6352: When using the Evidence Processor and running Expand Compound files, .odf (Math) and .odb (Base) OpenOffice files are mounted, but other OpenOffice files are not. All other OpenOffice files are indexed and available as transcripts.

DOC-1501: EnCase Forensic does not support Mac OS X compression types LZVN and LZFSE. Currently, files compressed with the use of these algorithms cannot be decompressed.

Found in Version 8.02.01

FOR-5348: When running EnCase Forensic on a Microsoft Windows 10 operating system, foreign language word breaking may cause the indexing to not work correctly. Windows 10 does not include a word breaker so some languages can be processed correctly, but others (such as Hebrew, Chinese, and other languages that have different roots and other structural differences from English) have inconsistent results.

DOC-1797: EnCase Forensic requires Open Sans font to be installed when working on Microsoft Windows 10 operating systems.

Found in Version 8.01

DOC-1654: The **Is Bookmarked** column does not show True when bookmarking a thumbnail artifact. The bookmark is created and can be seen in the Bookmarks tab, but does not update in the **Artifacts** tab.

DOC-1650: The **Is Bookmarked** column does not show True for items that are bookmarked in the Table view.

DOC-1647: If you reprocess an evidence file with Overwrite Evidence Cache selected, clicking the green refresh button does not refresh the page. To refresh the page, you must exit Entry view and return.

DOC-1609: The screenshots in the *EnCase Forensic User Guide* do not reflect the current extensive changes to the interface. Unless otherwise noted in these release notes, the functionality is the same, but the design and format may be different from what is displayed on your screen.

DOC-1533: EnScript cannot currently call the **Isbookmarked** function; therefore, the new bookmarked column in Entry view does not display correctly for custom EnScript programs.

FOR-3189: You cannot move a folder between the User and Shared folders while in the fourth pane.

Found in Version 7.11

DOC-1217: After selecting a specific process memory entry from the network preview pane and drilling into the corresponding item in EnCase, the only entry shown is the unused disk area. The memory event representing the memory of the process is not shown. This issue is specific to Windows 10.

DOC-1215: Running System Info Parser with the checkbox **Live Registry** cleared returns a folder in the **Records** tab with the label "xxxxxx (Live Registry)." This is misleading, because the live registry option is disabled.

Found in Version 7.10

CORE-1527: The 32 and 64-bit EnCase servlet requires the Windows Management Interface (WMI) service for installation and operation on Windows 10, Windows 8, Windows 8.1, Windows Server 2012, and Windows 2012 R2.

TS-141: File Carver may display a status of 100 percent complete, but continue to process or crash EnCase. This situation is caused by File Carver searching for numerous file types, including headers leading with "..." Guidance Software recommends that you perform file carving for file types with "..." leading headers separately.

CORE-1322: When exporting items in Search Results, if **Add to existing evidence file** is selected, EnCase crashes.

CORE-895/69792: The index uses all caps by default; so, for example, DOBBS is the only hit for a search on <c>DOBBS. <c>dobbs, <c>Dobbs, and all other case variations are in a different set.

Found in Version 7.09.04

69649: After several iterations of running Case Analyzer and bookmarking, when clicking on a bookmark created with Case Analyzer, EnCase may crash.

Found in Version 7.09.02

68889: Outside In: EnCase hangs while viewing some .mif files.

Supported File Systems

APFS	HFS	SOLZFS
CDFS	HFS+	SUN
EXFAT	HFSX	UDF
EXT2	HPFS	UFS
EXT3	HPUXFS	UFS2
EXT4	JFS	VXFS
FAT	JFS2	XFS
FAT12	NETWARE	YAFFS2
FAT16	NTFS	ZFS
FAT32	REISER	

Third Party Systems

Vendor	Version
Project VIC data model	1.2

Vendor	Version
NetWare	No longer supported
Windows XP	No longer supported
Windows Server 2003	No longer supported

Encryption Support

EnCase Forensic supports the following encryption products.

Vendor	Product	Supported Versions	64-bit Support
Check Point	Check Point Full Disk Encryption (formerly Pointsec PC)	6.3.1 up to 7.4, 8.0 (for Windows and Macintosh computers)	Yes
Credant	Mobile Guardian (subsumed by Dell)	5.2.1, 5.3, 5.4.1, 5.4.2, 6.1 through 6.8, 7.3	Yes
Dell	Data Protection Enterprise Edition	8.3, 8.5, 8.12, 8.13, 8.15, 8.16, 8.17	Yes
GuardianEdge	Encryption Plus/Anywhere	7 and 8	No
GuardianEdge	Hard Disk Encryption	9.1.5, 9.2.2, 9.3.0, 9.4.0, 9.5.0, 9.5.1	Yes
McAfee	EndPoint Encryption (formerly SafeBoot)	4, 5, 6, 7 (for Windows and Macintosh computers)	Yes

Vendor	Product	Supported Versions	64-bit Support
Microsoft	BitLocker and BitLocker To Go	Windows Vista (Enterprise and Ultimate), Windows 7, 8, 10, Windows Server 2008	Yes
Sophos	SafeGuard Easy and Enterprise (formerly Utimaco)	4.5, 5.5, 5.6, 6.0	Yes (only for SafeGuard Easy, not for Enterprise)
Symantec	PGP Whole Disk Encryption	9.8, 9.9, 10, 10.1, 10.2, 10.3	Yes
Symantec	Endpoint Encryption	7.0.2, 7.0.3, 7.0.4, 7.0.5, 7.0.6, 7.0.7, 7.0.8, 8.0, 8.2, 8.2.1, 9.1, 11.1.1	Yes
WinMagic	SecureDoc Full Disk Encryption and Self-Encrypting Drives	4.5, 4.6, 5.x, 6.x	Yes

USGCB Compliance

EnCase Forensic has been validated as USGCB compliant using the following version of NIST VHD images:

2/27/17 (for Windows 7 only)

EnCase Forensic was tested using Retina Network Security Scanner, which is a NIST validated USGCB scanner (http://usgcb.nist.gov/usgcb/microsoft_content.html).

SAFE and License Manager Upgrade Instructions

The Guidance Software SAFE was introduced with EnCase Forensic Version 8.02.

With the release of Guidance Software SAFE, license management functionality was removed from the SAFE and packaged as the License Manager. The License Manager permits administrators to manage and serve licenses to authorized users of Guidance Software investigative applications without need of a SAFE.

When you should upgrade

You do not need to install or upgrade the Guidance Software SAFE or License Manager if you are currently using EnCase SAFE v7m or earlier, and do not centralize the management of your Guidance Software licenses using NAS.

You do not need to install or upgrade the Guidance Software SAFE if you are upgrading from EnCase Forensic Version 8.01 or later. If you were using EnCase SAFE/NAS to manage your software licenses, your software licenses have already been moved from your old SAFE to License Manager.

IF YOU ARE USING ENCASE SAFE V7M OR EARLIER:

If you are upgrading from EnCase Forensic prior to Version 8.01 and are using EnCase SAFE v7m or earlier with a NAS License server, you must install the new License Manager

Before you begin, you need access to a Guidance Software MyAccount online account and the email from Guidance Software with the subject line, "Guidance Software Electronic Software Delivery for Your Order."

You also need to activate an electronic license or security key (dongle) for License Manager. If you have an electronic license, you must activate it before installing License Manager. See Activating a License for License Manager in the *Guidance Software SAFE User Guide*.

Guidance Software recommends continuing to run the License Manager on the same machine as the SAFE.

To install the License Manager:

1. If you are going to install License Manager on the same machine as your existing SAFE/NAS you can bypass resubmission of the `.keymaster` and `.machine` files to Guidance Software by creating a copy of the SAFE folder (`C:\Program Files\Guidance Software\SAFE`) in the same parent folder and naming it `EnCase LM`. If you are going to install License Manager on a different machine from the existing SAFE/NAS, follow the License Manager installation instructions found in the *Guidance Software SAFE User Guide*.
2. Run the `EnCase License Manager Setup` or `EnCase License Manager Setup (x64)` installer.
3. The License Manager installer opens.
4. Point the License Manager installer to the `EnCase LM` installation folder.
5. The installer will use your existing `.setup` file to complete the installation process.

Note: There is no need to resubmit your `.machine` or `.publickey` files if you have copied your original files from your old SAFE/NAS installation.

6. Upon completion of the installation process, you will have a `.nas` file in the NAS folder and a `.SAFE` file in the license manager directory. Distribute these files to any examiners using licenses from this server. License Manager runs on port 4446 by default unless you have chosen a different port.

To configure desktop investigative applications to use License Manager, see Configuring Desktop Clients to use License Manager in *Guidance Software SAFE User Guide*.

Support

Guidance Software is committed to providing our customers with the best user experience possible. There are a variety of ways for you to get the help you need, when you need it.

Guidance Software provides a wide array of resources to help you find answers to your questions online.

To access online support, navigate to www.guidancesoftware.com and click **Support**.

Contact Technical Support

Guidance Software provides telephone technical support 24 hours a day, excluding weekends and holidays, through the regional support numbers listed below. All technical support inquiries are automatically routed to either our US or UK office, depending on the time of day.

UNITED STATES:

Phone: +1 (866) 973-6577 or (626) 229-9191
Fax: +1 (626) 229-9199
1055 E. Colorado Blvd.
Pasadena, CA 91106

UNITED KINGDOM:

Phone: +44 (0) 1753-552252, Option 4
Fax: +44 (0) 1753-552232
Thames Central, 5th Floor
Hatfield Road
Slough, Berkshire UK SL1 1QE

EMEA AND APAC:

+800-4843-2623

For customers in the following countries, use your country's local exit code and call: +800-GUIDANCE (4843-2623). Do not dial US country code 1.

- Australia
- Belgium
- China-North
- China-South
- Denmark
- Finland
- France
- Germany
- Hong Kong
- Italy
- Japan
- Malaysia
- Netherlands
- New Zealand
- Norway
- Poland
- Singapore
- South Korea
- Spain
- Sweden

If you do not know your exit code, refer to http://www.howtocallabroad.com/codes.html. Dial your country's exit code, then dial 800-4843-2623.

Contact Customer Service

BY TELEPHONE:

626-463-7964 (Monday through Friday, 7 am to 5 pm, Pacific Time)
866-229-9199

BY ONLINE REQUEST:

Navigate to www.guidancesoftware.com and click **Support** > **Customer Service** > **Contact**.