EnCase Forensic

Version 8.05

Release Notes

EnCase Forensic Version 8.05

Thank you for using Guidance Software products.

Guidance Software recommends that you read these 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 version for this release is a.05.

There were no changes to License Manager in this release.

New Features

Mobile Acquisition

EnCase Forensic now has expanded mobile acquisition capabilities. In addition to mobile device support, you can now import mobile device backup files and Cellebrite UFED case files, and acquire data from cloud services, such as Facebook, Twitter, Gmail, and Google Drive.

Before beginning acquisition on a mobile device, you will need to download and install the Mobile Driver Pack from the Guidance Software Download Center.

> **Note:** If you are running Windows 7, you will need to install two security updates before you can install the Mobile Driver Pack. Windows 7 needs to be upgraded to SP1 before installing the security updates.

To acquire mobile data, click **Add Evidence** on the **Home** tab and select one of the options under **Acquire Smartphone**. Select **Acquire from Device** to acquire a mobile device, such as a smartphone, tablet, PDA, or GPS device. To acquire data from a device backup file, select **Acquire from File**. Use **Acquire from Cloud** to import data from one of the supported cloud services.

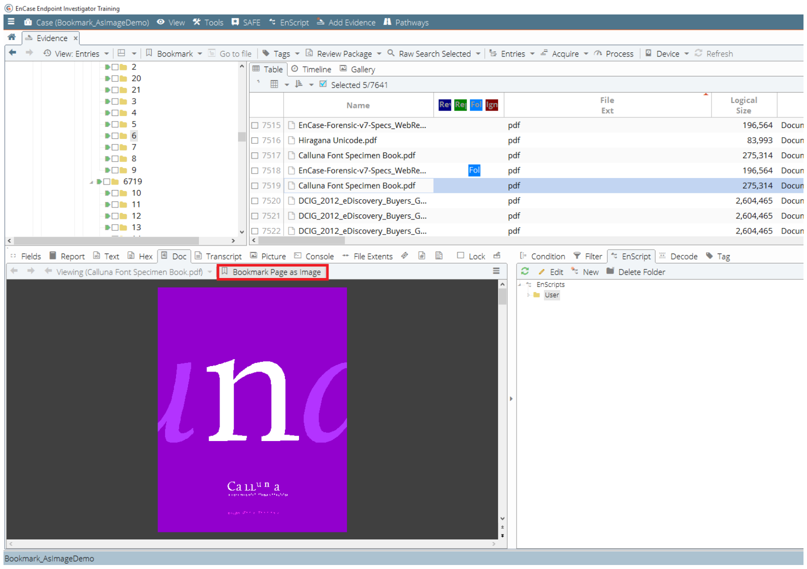
The mobile acquisition process will create an EnCase Logical Evidence File (LEF) in the folder you specify in the Output File Settings.

Bookmarking a Document as an Image

You can bookmark Microsoft Office, PDFs, or OpenOffice documents as images that can be inserted into reports with formatting and pagination intact. Microsoft Excel spreadsheet pages and orientation cannot be modified.

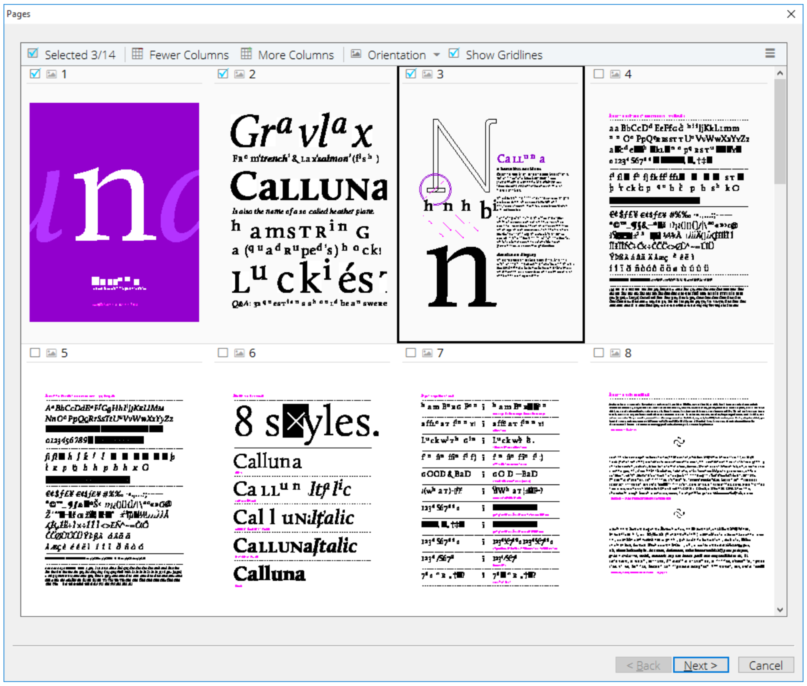
To bookmark a document as an image:

1. While in the Evidence tab, select the document you want to bookmark from your evidence list and click the **Doc** tab in the lower view pane.

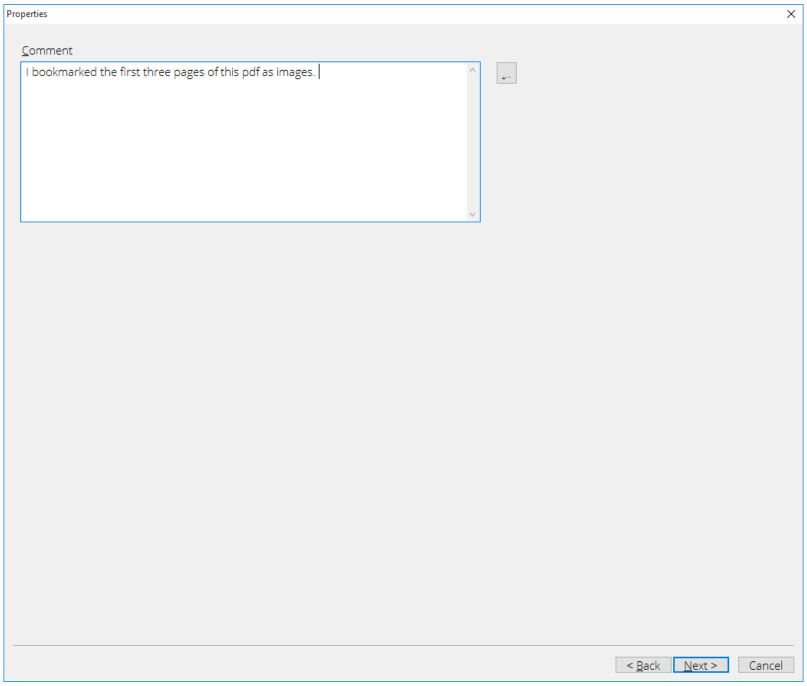


	Name	Re Re Fol Ign	File Ext	Logical Size	
□ 7515	EnCase-Forensic-v7-Specs_WebRe...		pdf	196,564	Docun
□ 7516	Hiragana Unicode.pdf		pdf	83,993	Docun
□ 7517	Calluna Font Specimen Book.pdf		pdf	275,314	Docun
□ 7518	EnCase-Forensic-v7-Specs_WebRe...	Fol	pdf	196,564	Docun
□ 7519	Calluna Font Specimen Book.pdf		pdf	275,314	Docun
□ 7520	DCIG_2012_eDiscovery_Buyers_G...		pdf	2,604,465	Docun
□ 7521	DCIG_2012_eDiscovery_Buyers_G...		pdf	2,604,465	Docun
□ 7522	DCIG_2012_eDiscovery_Buyers_G...		pdf	2,604,465	Docun

2. In the Doc tab, select Bookmark Page as Image. A dialog opens, displaying all the pages in the selected document.



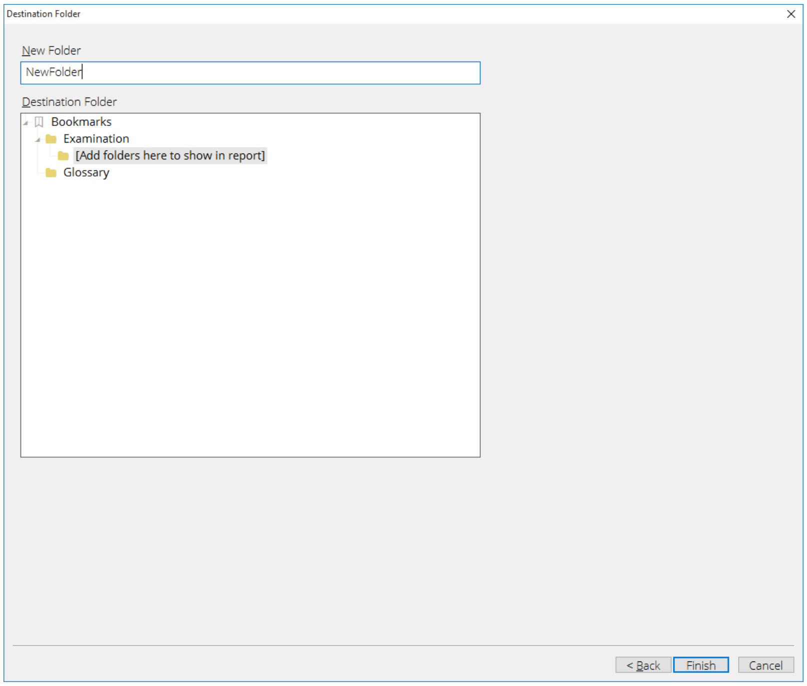
3. Select the page(s) you want to create as an image, and click **Next**.



Comment

I bookmarked the first three pages of this pdf as images.

4. Add an optional comment, and click **Next**.



New Folder

NewFolder

Destination Folder

5. Select a folder in which to add the image and click **Finish**.

The image is added to all appropriate reports automatically. Original formatting and pagination, when available, is preserved.

Items Fixed

FOR-7563: When running scan LVM on a Linux disk, a buffer overflow vulnerability has been fixed.

TS-2276: Symantec Endpoint Encryption (SEE) drives that have been upgraded from Symantec Endpoint Encryption v8.x to v11.1 now decrypt successfully.

TS-2329: The BinderClass in EnScript has been fixed to retain image quality in extracted images.

Known Limitations

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

- CDFS
- EXFAT
- EXT2
- EXT3
- EXT4
- FAT
- FAT12
- FAT16
- FAT32
- HFS
- HFSPLUS
- HFSX
- HPFS
- HPUXFS
- JFS
- JFS2
- NETWARE
- NTFS
- REISER
- SOLZFS
- SUN

- UDF
- UFS
- UFS2
- VXFS
- XFS
- YAFFS2
- ZPS

Third Party Systems

Vendor	Version
Project VIC data model	1.2
NetWare	No longer supported
Windows XP	No longer supported
Windows Server 2003	No longer supported

Encryption Support

EnCase 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	5.2.1, 5.3, 5.4.1, 5.4.2, 6.1 through 6.8, 7.3	Yes
Dell	Data Protection	8.3 and 8.5	Yes
GuardianEdge	Encryption Plus/Anywhere	7 and 8	No

Vendor	Product	Supported Versions	64-bit Support
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
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	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) 463-7977
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**.