



ЭТАЛОН

В области компьютерных судебных расследований

Правоохранительные органы, правительство, военные следователи и следственные органы используют программу EnCase Forensic для проведения тщательного компьютерного мониторинга, который нередко имеет определяющее значение.

Правоохранительные органы, правительство, военные следователи и следственные органы используют программу EnCase Forensic для проведения тщательного компьютерного мониторинга, который нередко имеет определяющее значение.

Так как компьютерные данные и другие цифровые улики приобрели решающее значение для разрешения судебных дел, работа судебных лабораторий расписана на недели или даже месяцы вперед, что откладывает разрешение вашего судебного дела на еще более долгий срок.

EnCase Forensic предоставляет вам инструменты для успешного проведения расследований и документирования большинства бытовых правонарушений: детской порнографии, домашнего насилия, злоупотребления наркотиками, азартными играми, а также «краж личности». EnCase

Forensic предотвращает потерю ценных улик содержащихся на компьютере, а также избавит Вас от необходимости ждать своей очереди в лабораторию. Решение позволяет эксперту работать с найденными уликами в рамках простого графического интерфейса, используя набор простых и эффективных инструментов, что в значительно уменьшает количество времени, обычно затрачиваемое на расследование одного дела.

Будучи разработанной специалистами в области судебных криминалистических расследований, программа EnCase Forensic признана судебными органами по всему миру. Услугами EnCase Forensic пользуются такие организации, как ФБР, Министерство национальной безопасности США, Министерство обороны США, Нью-Скотленд-Ярд и тысячи других агентств правоохранительных органов и криминалистических лабораторий по всему миру.

Расширенные функциональные возможности экономят ваше ценное время и повышают продуктивность...

EnCase Forensic предлагает Вам расширенные функциональные возможности, которые экономят время и повышают продуктивность работы сотрудников следственных органов. Теперь они получают возможность просматривать уже полученные данные, параллельно получать новую информацию с других накопителей. После создания образов файлов вы можете анализировать данные с многочисленных накопителей, осуществлять поиск необходимой информации по ключевым словам, при помощи анализа значений хэш-функций, анализа сигнатур файлов, а также используя различные фильтры файлов.

Предоставление надежных сведений...

EnCase Forensic предоставляет возможность получать надежные доказательства. Программа создает точную копию оригинального накопителя или носителя данных, затем осуществляет ее верификацию, генерируя значения хэш-функции MD5 для родственных файлов. В дополнение к этому, программа устанавливает значение CRC (ЦИК) для данных, чтобы выявить, когда доказательства были повреждены или изменены. Данный подход одобрен Национальным институтом стандартов и технологий США и применялся в ходе многочисленных судебных расследований.

Гибкость программы позволяет лучше отвечать вашим запросам...

Программы EnCase построены на базе Enscript® программирования, язык макропрограммирования, который позволяет пользователям создавать собственные сценарии (scripts) с целью автоматизировать занимающие много времени операции, такие как поиск и анализ документов особого типа. В основе Enscript® программирования лежат языки JAVA и C + +.

Новая 64-битовая версия

Обеспечивает более высокую производительность, расширенные возможности обработки данных и возможность более эффективного использования имеющейся свободной памяти.

Encase® Forensic

облегчает работу с большими

объемами найденной информации.

Позволяет просматривать важные для поиска документы, включая «удаленные» файлы, заполнители файлов и свободное пространство.

Возможности

Создание поисковых запросов

Создание при помощи новой, заявленной на патент, технологии подробных поисковых запросов, включающих слова, как английского, так и других языков, позволяет пользователям осуществлять быстрый и простой поиск по ключевым словам. Поисковые запросы могут быть сгруппированы чтобы впоследствии можно было осуществлять поиск одинаковых ключевых слов в отдельных расследованиях. Поисковые запросы с поддержкой Unicode создаются на основе содержимого персональных документов, удаленных файлов, артефактов файловой системы, заполнителей файлов, файлов подкачки, свободного пространства, электронной почты и веб-страниц.

Возможность просматривать более 400 файлов в родном формате

Родной формат просмотра файлов позволяет просматривать файлы в рамках программы EnCase в таком виде, в каком они выглядят в своих родных приложениях. И больше нет необходимости экспортировать файлы и пользоваться инструментами сторонних производителей. Вы можете печатать, помещать в избранное, копировать и вставлять более 400 форматов файлов. Это в значительной степени помогает снизить вероятность ошибочных результатов поиска.

Расширенная поддержка файловых систем

Программа поддерживает широкий ряд файловых систем, включая Windows FAT12 (Floppy), FAT 16, FAT32, NTFS; Macintosh HFS, HFS+; Sun Solaris UFS; Linux EXT2/3; Reiser; BSD FFS; FreeBSD's Fast File System 2 (FFS2) и FreeBSD's UFS2; Novell's NSS и NWFS; IBM's AIX jfs, JFS и JFS с Lvm8; TiVo Series One и Two; CDFS; Joliet; DVD; UDF; ISP 9660; и Palm. В скором времени: HP-UX (vxfs).

Расширенная поддержка электронной почты

Программа распознает большое количество форматов электронной почты, включая Outlook PSTs/OSTs ('97-'03), Outlook Express DBXs; Microsoft Exchange EDB Parser; Lotus Notes v6.0.3, v6.5.4 b v 7; AOL 6.0, 7.0, 8.0 и 9.0 PFCS; базирующиеся на интернет технологиях форматы, включая Yahoo, Hotmail, Netscape Mail и MBOX архивы (реальный стандарт, используемый практически каждой популярной программой чтения электронной почты, установленной на UNIX, Windows и Mac). Недавно усовершенствованная функция поддержки электронной почты теперь позволяет отображать удаленные послания электронной почты, заметки, записи ежедневника для PSTs и OSTs. В дополнение к этому теперь вы можете копировать и восстанавливать сообщения электронной почты в широко распространенном формате для просмотра сообщений в других приложениях.

Поддержка интернет браузеров

Программа также декодирует интернет историю и показывает файлы кэш страниц HTML и сопутствующие изображения. Программа поддерживает Microsoft Internet Explorer, Mozilla Firefox, Opera и Apple Safari (Mac OS X default).

Гибкие возможности сбора данных

Программа предоставляет возможность графически отображать медиа файлы используемые различными операционными системами, экономя время и устраняя сложности с которыми сталкиваются эксперты при сборе данных. Программа позволяет графически отображать медиа файлы систем Windows, DOS и Linux, а также обладает рядом функций, позволяющих управлять компрессией, скоростью и ошибками.

Расширенные возможности отображения временных промежутков

Программа предоставляет «Календарь» всех процессов, происшедших с файлами, показывая, когда файлы были созданы, последний раз перезаписаны или когда последний раз к ним осуществлялся доступ. Календарная шкала захватывает месяцы и годы, предоставляя эксперту полный обзор активности файлов.

Детальные отчеты

Программа создает детальные отчеты о специфических файлах, папках, томах, физических дисках и событиях, а также позволяет просматривать информацию о процессах сбора данных, конфигурациях подключаемых или стационарных накопителей, структурах папок, избранных файлах и изображениях. Отчеты экспортируются в форматы RTF или HTML.

Guidance Software предлагает дополнительные инновационные решения для более эффективного использования возможностей EnCase Forensic...

Модуль FastBloc[®] SE (ПО версия) (FastBloc[®] (Software Edition) Module)

FastBloc SE – новое программное решение предотвращающее запись на диск для гарантии сохранности исследуемой информации. Блокируются устройства подключаемые по USB, FireWire, IDE и SCSI на базе Windows. Данный модуль позволяет без использования дополнительных внешних устройств блокировать изменение данных на исследуемом накопителе. Это гарантирует что данные на исследуемом носителе не были изменены в ходе расследования экспертом или сотрудником службы безопасности. В дополнение к этому, программа позволяет проникать в защищенные области данных (Host Protected Areas – HPA) и уровни конфигурации устройства (Device Configuration Overlays – DCO) на жестких накопителях IDE и SATA.

Модуль дешифрования EnCase (EnCase Decryption Suite (EDS) Module)

Позволяет экономить время и повышает продуктивность в процессе работы с дешифрованием и восстановлением паролей. Эксперт получает доступ к зашифрованным файлам и папкам на базе системы шифрования файлов NTFS (NTFS Encrypting File System) и извлекает информацию о сохраненных паролях из системного реестра Windows.

Эмулятор физического диска EnCase (EnCase Physical Disk Emulator (PDE) Module)

Избавляет от долгих часов рутинной работы переписывания данных с одного жесткого диска на другой. Модуль позволяет представлять компьютерные улики в качестве виртуального локального диска для последующей работы с ними с использованием VMware и других инструментов сторонних производителей.

Виртуальная файловая система EnCase (EnCase Virtual File System (VFS) Module)

Позволяет представлять компьютерные улики доступными «только для чтения» в качестве сетевого диска, для последующей работы с данными с использованием Windows Explorer и других инструментов сторонних производителей, например, детекторов взломщиков паролей, вирусов, вредоносных программ и стеганографии.

CD/DVD модуль

Данный модуль упрощает процесс архивирования найденных доказательств и исходных данных. Позволяет сохранить полученные данные совместно с результатами исследования данного носителя как логический диск, верифицировать их и создать архив на CD или DVD. Отчеты, избранное и записи, сделанные в EnCase, также могут напрямую помещаться на CD или DVD.

Примечание:

Продукты EDS, PDE и VFS могут быть приобретены отдельно, в качестве отдельных модулей к EnCase Forensic Professional Suite, или же поставяться в составе Premium License Support Program.

O Guidance Software

Основанная в 1997 году, компания Guidance Software завоевала всемирное признание в качестве лидера на рынке компьютерных решений в области компьютерных расследований. Ее продукт EnCase[®] предоставляет базу для проведения расследований, как для правоохранительных органов, так и для организаций и позволяет осуществлять эффективные компьютерные расследования всех типов, оперативно реагировать на запросы eDiscovery, а также осуществлять оперативные и тщательные внутренние расследования, подразумевающие поиск цифровых улик, соблюдая принцип сохранности доказательств, что необходимо при судебных расследованиях. Более чем 20.000 сотрудников следственных органов пользуются услугами EnCase, и почти 4.000 сотрудников ежегодно посещают тренинги Guidance Software по проведению судебных расследований. Получившее одобрение многочисленных судебных органов по всему миру, программное обеспечение EnCase также нередко удостоивается наград в номинации «совершенно секретно» от таких изданий, как eWEEK, SC Magazine, Network Computing и других.

Дальнейшую информацию о наших продуктах и услугах вы сможете получить по адресу:

<http://www.guidancesoftware.ru>