

Recursos e funcionalidades do EnCase® Forensic

Todas as investigações são importantes



Investigadores digitais precisam de uma solução que capture facilmente dados relevantes para sustentar uma investigação ou requisito de conformidade e que tenha recursos de análise técnica sofisticada para localizar dados enterrados e/ou ocultos. O EnCase® Forensic é uma potente plataforma de investigação que coleta dados digitais, realiza análises, informa as descobertas e as preserva em um formato validado e legalmente aceito.

Como o EnCase® Forensic funciona:

1) Obtenha aquisições legalmente aceitas

O EnCase® Forensic produz uma cópia binária exata da unidade de disco ou da mídia original, depois a verifica gerando valores de hash MD5 para os arquivos de imagem relacionados e atribuindo valores de CRC aos dados. Essas verificações e balanços revelam quando provas foram falsificadas ou alteradas, mantendo todas as provas digitais legalmente válidas para os processos judiciais.

2) Economize um tempo valioso com recursos avançados de produtividade

Os analistas podem visualizar dados enquanto as unidades ou outras mídias estão sendo adquiridas. Assim que os arquivos de imagem são criados, os analistas podem pesquisar e analisar várias unidades e outras mídias simultaneamente. O EnCase Forensic também oferece um indexador de casos. Essa potente ferramenta elabora um índice completo em vários idiomas, permitindo consultas rápidas e fáceis. Os índices também podem ser vinculados para localizar palavras-chave comuns a outras investigações. Esse índice com suporte para Unicode contém documentos pessoais, arquivos excluídos, artefatos do sistema de arquivos, espaços entre arquivos, espaços não alocados, e-mails e páginas da web. Além disso, o EnCase tem amplo suporte para o sistema de arquivos, para que as organizações possam analisar todos os tipos de dados.

3) Personalize o EnCase® Forensic com o EnScript® Programming

O EnCase Forensic oferece os recursos de programação do EnScript®. O EnScript, é uma linguagem de programação orientada para objetos, semelhante ao Java ou C++, que permite que os usuários criem programas personalizados para ajudá-los a automatizar tarefas investigativas demoradas, como a pesquisa e análise de tipos específicos de documentos ou outros processos e procedimentos que exigem muito trabalho. Esse recurso pode ser aproveitado por qualquer investigador por meio do uso de ferramentas de computação forense, como o "Case Developer" ou um dos numerosos filtros e condições integradas.

4) Forneça dados relevantes, crie relatórios desses dados e passe para o próximo caso

Assim que os investigadores marcarem os dados relevantes, poderão criar um relatório adequado para apresentação em um tribunal, para a administração ou para outra autoridade legal. Os dados também podem ser exportados em vários formatos de arquivo para análise.

Lista de verificação de recursos e funcionalidades do EnCase Forensic

Aquisição

- Granularidade da aquisição:
 - o Erros: especifica o número de setores que serão zerados quando um erro for encontrado.
 - o Blocos de aquisição: define o tamanho do bloco.
- Reinício da aquisição: dá sequência a uma aquisição baseada em Windows a partir do ponto em que ela foi interrompida.
- Arquivos de evidências lógicas: um recipiente de evidências somente com os arquivos ou pastas que você precisa.
- CRC: imagem confirmada por soma de verificação cíclica de redundância (CRC) e MD5
- Utilitário LinEn: adquire provas por meio do disco de inicialização
- Utilitário WinEn: adquire provas na RAM

Ferramentas de automação - aceleram o processo de investigação.

- EnScript: crie scripts ou use scripts pré-integrados
- Filtros e condições: mais de 150 disponíveis
- Combina filtros para criar consultas complexas usando lógica simples "OR" ou "AND"
- Extrator de informações do Active Directory
- Análise de hardware: examina automaticamente o registro e os arquivos de configuração
- Recuperação de partições: reconstrói automaticamente a estrutura de volumes formatados NTFS e FAT
- Recuperação de arquivos/pastas excluídos

Recursos de análise

- Analisador do registro de eventos do Windows
- Analisador de arquivos de vínculos (link): localiza em espaços não alocados
- Documento e arquivo composto (por exemplo, compactado)
- Análise de assinatura de arquivo
- Análise de hash
- Localizador de arquivos: localiza arquivos em espaços não alocados

Visualizadores

- Visualização original para aproximadamente 400 formatos de arquivo
- Visualizador de registro integrado
- Visualizadores de arquivos externos
- Visualizador integrado de imagens com modo de exibição de galeria
- Visualizador de cronograma/calendário

Pesquisa

- Pesquisa de índice Unicode: pesquisa textos extraídos de documentos
- Pesquisa binária: pesquisa dados binários não processados
- Pesquisa de proximidade
- Pesquisa na internet e em e-mails
- Diferencia maiúsculas e minúsculas • GREP • Leitura da direita para a esquerda

- Página de código ativo: palavras-chave em vários idiomas
- Big Endian/Little Endian, UTF-8/UTF-7
- Pesquisa de espaços entre arquivos e espaços não alocados

Relatórios - Relatórios automáticos

- Listagem de todos os arquivos e pastas de um caso
- Listagem detalhada de todos os URLs e datas correspondentes e horários de visita aos sites
- Documentação de relatórios de resposta a incidentes
- Registros
- Registro do computador
- Informações detalhadas do disco rígido sobre partições físicas e lógicas
- Exibição de dados sobre a aquisição, geometria da unidade de disco, estruturas de pastas e arquivos e imagens marcados
- Exportação de relatórios em formato RTF ou HTML

Recursos de marcação

- Dados destacados
- Notas
- Informações das pastas
- Arquivos que podem receber anotações
- Grupos de arquivos

Investigação da internet e de e-mails

Análise do histórico do navegador

- Artefatos da internet
- Histórico da Web e análise do cachê
- HTML carver (busca e exporta arquivos HTML)
- Reconstrução de páginas em HTML
- Kit de ferramentas Kazaa
- Kit de ferramentas de mensagens instantâneas: Microsoft® Internet Explorer, Mozilla Firefox, Opera e Apple Safari

Suporte para e-mail inclui

- Outlook PSTs/OSTs ('97-'03)
- Outlook Express DBXs
- Microsoft Exchange EDB Parser
- Lotus Notes v6.0.3, v6.5.4 e v7
- PFCs AOL 6.0, 7.0, 8.0 e 9.0
- Yahoo
- Hotmail
- Netscape Mail
- Arquivos MBOX

Suporte do sistema

- Hardwares e softwares RAIDs
- Suporte dinâmico de disco para Windows 2000/XP/2003 Server
- Interpretação e análise dos formatos de imagem VMware, Microsoft Virtual PC, DD e SafeBack v2
- Sistemas de arquivos: Windows FAT12/16/32, NTFS; Macintosh HFS, HFS+; Sun Solaris UFS, ZFS; Linux EXT2/3; Reiser; BSD FFS, FreeBSD's Fast File System 2 (FFS2) e FreeBSD's UFS2; Novell's NSS e NWFS; IBM's AIX jfs, JFS e JFS com LVm8; TiVo Series One e Two; CDFS; Joliet; DVD; UDF; ISO 9660; e Palm

Sobre a Guidance Software (GUID)

A Guidance Software é mundialmente reconhecida como líder do setor em soluções investigativas digitais. Sua plataforma EnCase® fornece a base para que organizações governamentais, corporativas e reguladoras realizem investigações completas, habilitadas para rede e legalmente válidas, de qualquer tipo, como resposta a solicitações de investigação eletrônica (eDiscovery), realização de investigações internas, resposta a inquéritos regulamentares ou auditorias de conformidade e de dados, mantendo a integridade legal dos dados periciais. Existem mais de 30 mil usuários licenciados para a tecnologia EnCase em todo o mundo e milhares participam dos renomados programas de treinamento da Guidance Software anualmente. Validado por inúmeros tribunais, departamentos jurídicos corporativos, órgãos governamentais e organizações reguladoras em todo o mundo, o EnCase foi homenageado com prêmios do setor, com o reconhecimento das publicações eWEEK, SC Magazine e Network Computing e também da pesquisa da Socha-Gelbmann. Para obter mais informações sobre a Guidance Software, visite www.guidancesoftware.com.

©2009 Guidance Software, Inc. Todos os direitos reservados. EnCase e Guidance Software são marcas registradas ou marcas comerciais de propriedade da Guidance Software nos Estados Unidos e em outras jurisdições e não podem ser usadas sem permissão prévia por escrito. Todas as outras marcas podem ser reivindicadas como propriedade de seus respectivos detentores.