НОВИНИ БЕЗПЕКИ

SECURITY DIRECTOR NEWS
BUSINESS NEWS FOR SECURITY PRACTITIONERS

28 червня, 2011

Подолання розриву між фізичною та інформаційною безпекою

Більшість фахівців з фізичної безпеки не вважають, що інформаційна безпека входить у сферу їх обов'язків, але Джозеф Шоу, старший слідчий з питань загроз MetaNet LLC, каже, що має бути більший взаємозв'язок між двома дисциплінами.

Шоу недавно був найнятий компанією для розслідування потенційно внутрішнього порушення безпеки. Співробітник прийшов в неробочий час, щоб виконати законну роботу, але привів сторонню людину, щоб допомогти йому надолужити згаяне. Шоу використовував різну інформацію від технологій фізичної безпеки, такі як журнали контролю доступу та відеоспостереження, а також цифрову інформацію з комп'ютера підозрюваного.

Шоу зміг точно визначити, коли людина входила в будівлю, як довго вона була там і на чому саме працювала. Використовуючи програмне забезпечення EnCase Forensic з програмного забезпечення Guidance, Шоу зміг визначити, на чому людина працювала, і в той час як було визначено, що її діяльність є легітимною, працівник все одно звільняється через невиконання протоколу. Проводячи це офіційне розслідування, компанія заощадила значну суму грошей, не зобов'язавши повідомляти клієнтів про порушення правил безпеки, що також могло пошкодити їхню репутацію.

http://www.securitydirectornews.com

Тематичне дослідження: Цифровий доказ знижує рівень насильницьких злочинів

У поліцейське управління невеликого містечка на півдні Каліфорнії надійшов дзвінок з повідомленням про нічне пограбування на парковці. Підозрюваний схопив сумочку жертви, коли вона сідала в машину. Поліцейські почали спостерігати за парковкою. Через 48 годин підозрюваний спробував завдати ще одного удару і був заарештований. Його арешт призвів до вилучення комп'ютера.

Використовуючи судово-медичну експертизу EnCase, слідчі знайшли інформацію на жорсткому диску підозрюваного, яка привела до доказів серії пов'язаних з бандою грабежів, наркотиків і використання зброї та критичних нових доказів, що відносяться до декількох пов'язаних з бандою інцидентів в цьому районі. Поліція змогла додати більше звинувачень до первісного звинуваченням у грабежі з більш тривалими термінами через жорстокі закони штату про банду. Використовуючи оперативну інформацію, зібрану з жорсткого диска, поліція змогла вилучити додаткові предмети за кількома звинуваченнями далеко за межами викрадення гаманця.

Особливості EnCase Forensic (продовження)

Розкрийте критичні докази, використовуючи розширені можливості пошуку для ідентифікації даних

Відновлення файлів і розділів, виявлення видалених файлів шляхом аналізу журналів подій, аналізу підписів файлів і аналізу хешу

Збереження даних в форматі файлу доказів з неперевершеним записом про прийняття суду

Перегляд сотень форматів файлів в своєму нинішньому вигляді, вбудований переглядач реєстру, вбудований переглядач фотографій; перегляд результатів на часовій шкалі / календарі

Отримувати дані з диска або оперативної пам'яті, зображень, електронної пошти, артефактів Інтернету, історії веб-пошуку та кешу, стислих файлів, файлів резервних копій, зашифрованих файлів, RAID, робочих станцій, серверів тощо

Особливості судової експертизи EnCase

- Експорт звітів зі списками всіх файлів і папок разом з докладним списком URL, з датами та часом відвідувань
- Виявлення і дешифрування томів, зашифрованих за допомогою Windows 7 BitLocker і Windows 7 BitLocker to Go
- Розшифрування будь-якого зашифрованого вкладення за допомогою служби керування правами до незашифрованого листа за один крок
- Просте управління великим обсягом комп'ютерних доказів
- Можливість передання файлів доказів при необхідності безпосередньо правоохоронним органам або законним представникам
- Параметри огляду дозволяють особам, які не є слідчими, таким як адвокати, переглядати докази з легкістю

EnCase Судові Модулі (продовження)

- EnCase надає безліч програмних модулів, які надають потужні інструменти розслідування в розпорядження судових слідчих
- Ці модулі є доповненнями до програмного забезпечення, і для їх активації потрібні сертифікати на покупку від www.guidancesoftware.com.
- Судові модулі EnCase:

Набір розшифровки EnCase	Емулятор фізичного диска	Віртуальна файлова система
Цей модуль дозволяє розшифровувати зашифровані файли і папки користувачам домену та локальним користувачам, включаючи шифрування диска, шифрування тому і шифрування на основі файлів.	Цей модуль дозволяє слідчим підключати комп'ютерні докази в якості локального диска для перевірки через провідник Windows Explorer	Цей модуль дозволяє слідчим підключати комп'ютерні докази як автономний мережевий диск, доступний тільки для читання, для перевірки через провідник Windows Explorer
		

EnCase Судові Модулі

EnCase Судові Модулі

Програмне забезпечення FastBloc (SE)

- Цей модуль являє собою набір інструментів для управління
- Він призначений для управління операціями читання і запису на диск, підключений до комп'ютера через контролери USB, FireWire, SCSI, IDE і SATA, щоб забезпечити безпечне отримання предметних носіїв з Windows в файл свідоцтв EnCase

Модуль CD-DVD

Цей модуль використовується для запису наступного на CD або DVD:

- Файли доказів і логічних доказів під час придбання
- Файли, папки і звіти з програми EnCase
- Існуючі файли доказів і файли логічних доказів

Мінімальні вимоги

Вимоги до програмного забезпечення EnCase

- Ключ безпеки EnCase
- Сертифікати на всі придбані модулі
- Поточна версія EnCase Examiner
- Останній і найшвидший процесор
- 1 ГБ оперативної пам'яті
- 100 МБ вільного місця на жорсткому диску

Специфічні вимоги до модуля FastBloc SE

- Одна з таких карт контролерів IDE
  - Promise Ultral33 TX2
  - Promise SATA150 TX2plus
  - Promise UltralOOTX2
  - «S1IG UltraATA / 133 PCI
  - «SIIG Ultra ATA 100 PCI RAID

Специфічні вимоги до модуля VFS

- Не менш 100 Мбіт / с мережевої інфраструктури

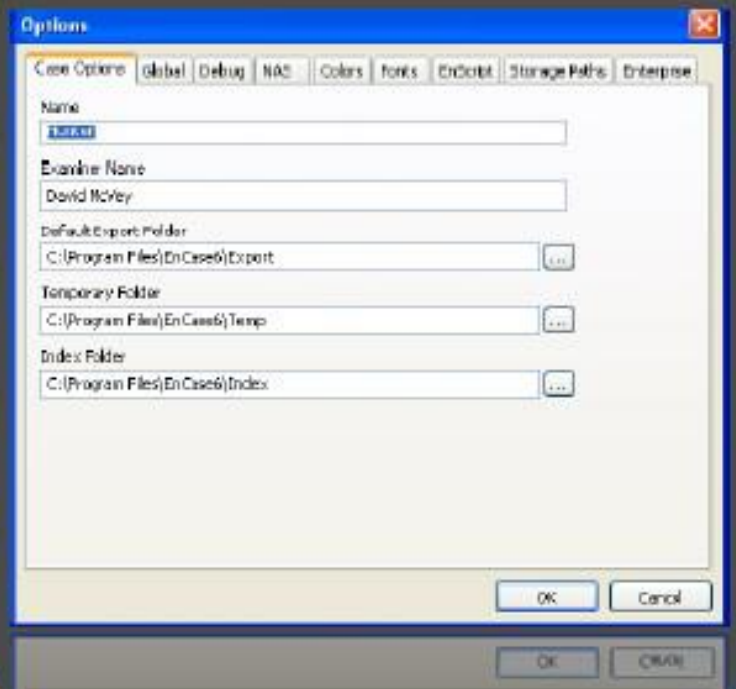
Специфічні вимоги до модуля CD-DVD

- Пальник CD / DVD, що підтримує AOPEN, Plextor 712A, ASUS 0402P, Sony RU-710A, двомісний DVD-диск Memorex, Toshiba R5372layer 16X w / USB шина, та Pioneer DVR-108

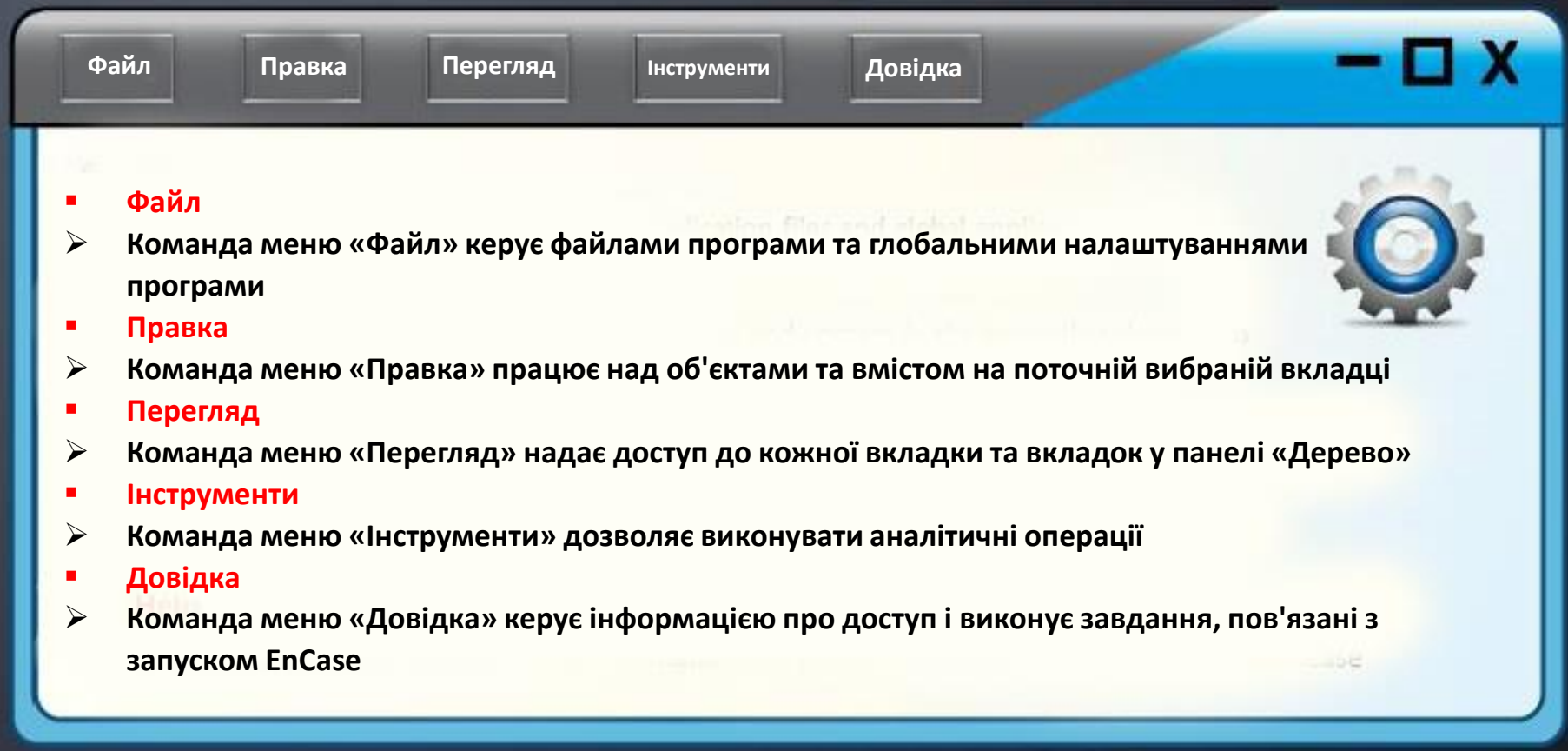
Примітка: Процесори Intel Itanium не підтримуються. FastBloc SE підтримує тільки USB-інтерфейс з 64-розрядною версією

Налаштування EnCase: вкладка «Параметри справи»

- Вкладка «Параметри справи» містить налаштування, що застосовуються до відкритої справи
- Показує інформацію про відкриту справу, таку як назва, назва експорту, папка експорту за замовчуванням, тимчасова папка і папка індексу



Область «Меню системи»



- **Файл**
  - Команда меню «Файл» керує файлами програми та глобальними налаштуваннями програми
- **Правка**
  - Команда меню «Правка» працює над об'єктами та вмістом на поточній вибраній вкладці
- **Перегляд**
  - Команда меню «Перегляд» надає доступ до кожної вкладки та вкладок у панелі «Дерево»
- **Інструменти**
  - Команда меню «Інструменти» дозволяє виконувати аналітичні операції
- **Довідка**
  - Команда меню «Довідка» керує інформацією про доступ і виконує завдання, пов'язані з запуском EnCase

Панель інструментів

Панель інструментів

Панель інструментів з'являється під рядком системного меню і надає опції для часто використовуваних функцій

Доступ до панелі інструментів

Ви можете отримати доступ до багатьох з цих команд, клацнувши правою кнопкою миші і відкривши меню вмісту

Параметри панелі інструментів

На панелі інструментів доступні наступні опції: Новий, Відкрити, Зберегти, Роздрукувати, Додати пристрій, Пошук, Вхід в систему, Вихід із системи, Оновлення та Закриття

Область таблиці: вкладка «Галерея»

Вкладка «Галерея» дає змогу переглядати зображення, вибрані в області Дерево, у вигляді ескізів

Він відображає файли на основі їх розширень

Можна налаштувати перегляд на вкладці «Галерея», щоб показувати більші або менші зображення