Научно-технические средства и методы цифровой криминалистики

Холопов Алексей Васильевич
Заведующий криминалистической лабораторией
Санкт-Петербургского юридического института (филиал)
Университета прокуратуры Российской Федерации
кандидат юридических наук, доцент, советник юстиции

Окинавская хартия глобального информационного общества принята 22 июля 2000 года лидерами стран «Большой восьмёрки»

РОССИЯ

Владимир Путин

Президент Российской Федерации

ЯПОНИЯ

Йосиро Мори

Премьер-министр Японии

ФРАНЦИЯ

Жак Ширак

Президент Французской Республики

ГЕРМАНИЯ

Герхард Шрёдер

Федеральный канцлер ФРГ

США

Билл Клинтон

Президент Соединенных Штатов Америки

КАНАДА

Жан Кретьен

Премьер-министр Канады

ВЕЛИКОБРИТАНИЯ

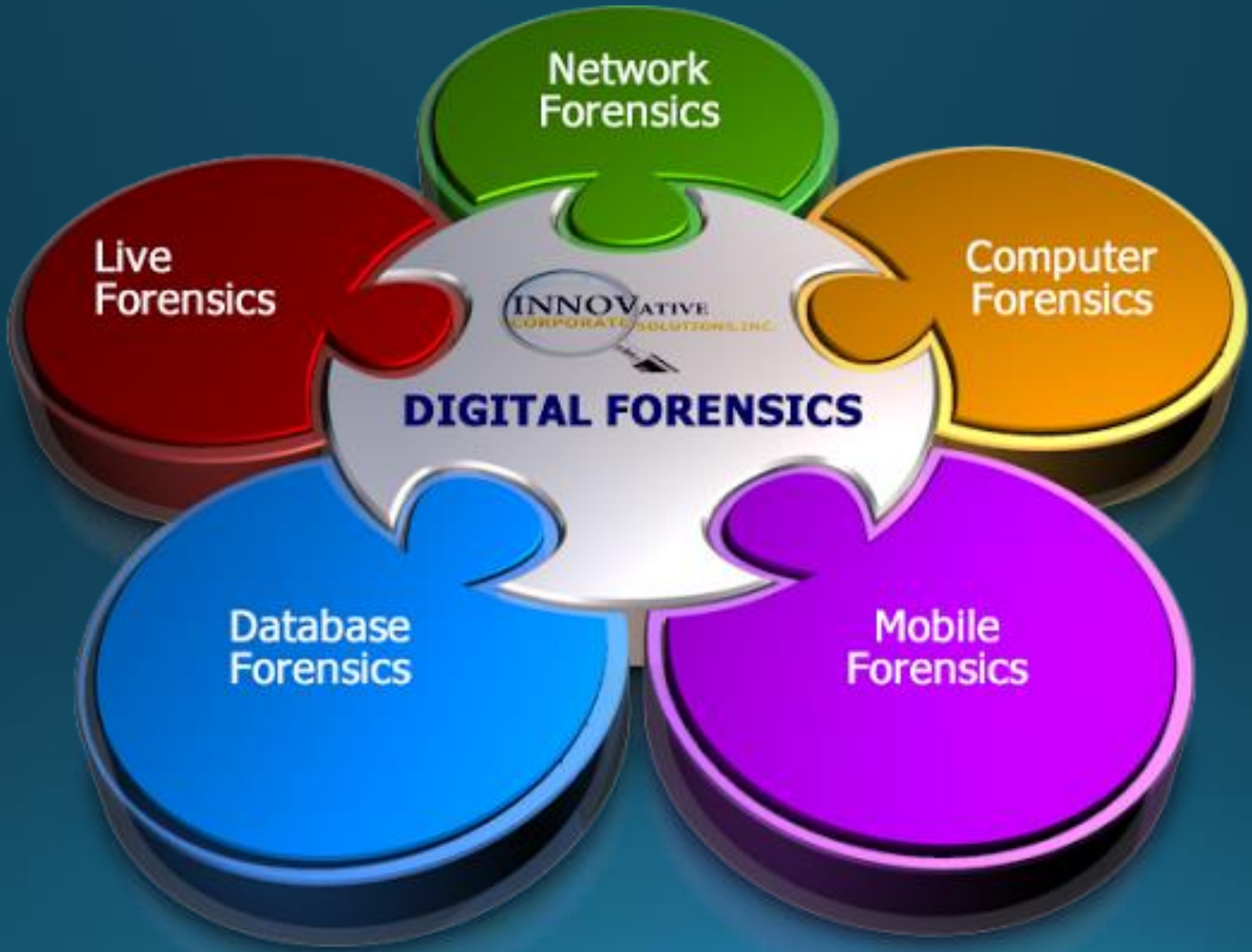
Энтони Чарльз Линтон (Тони) Блэйр

Премьер-министр Великобритании

ИТАЛИЯ

Джулиано Амато

Председатель Совета министров Итальянской республики


Network Forensics
Live Forensics
Computer Forensics
INNOVative
DIGITAL FORENSICS
Database Forensics
Mobile Forensics

Киберпреступление – это общественно опасное деяние, совершаемое в киберпространстве, посягающее на общественную безопасность, собственность, права человека, другие охраняемые законом отношения, необходимым элементом механизма подготовки, совершения, сокрытия и отражения которого является компьютерная информация, выступающая в роли предмета или средства преступления.

Основные виды киберпреступлений

- Кардинг(carding)
- Крекинг (cracking)
- Спаминг (spamming)
- Фишинг (phishing)
- Фарминг (pharming)
- Нюкинг (nuking)
- Хакинг(hacking)

кракеры – (cracker) ломают программные защиты от серийных номеров до аппаратных ключей;

фрикеры – (fricker) занимаются телефонией;

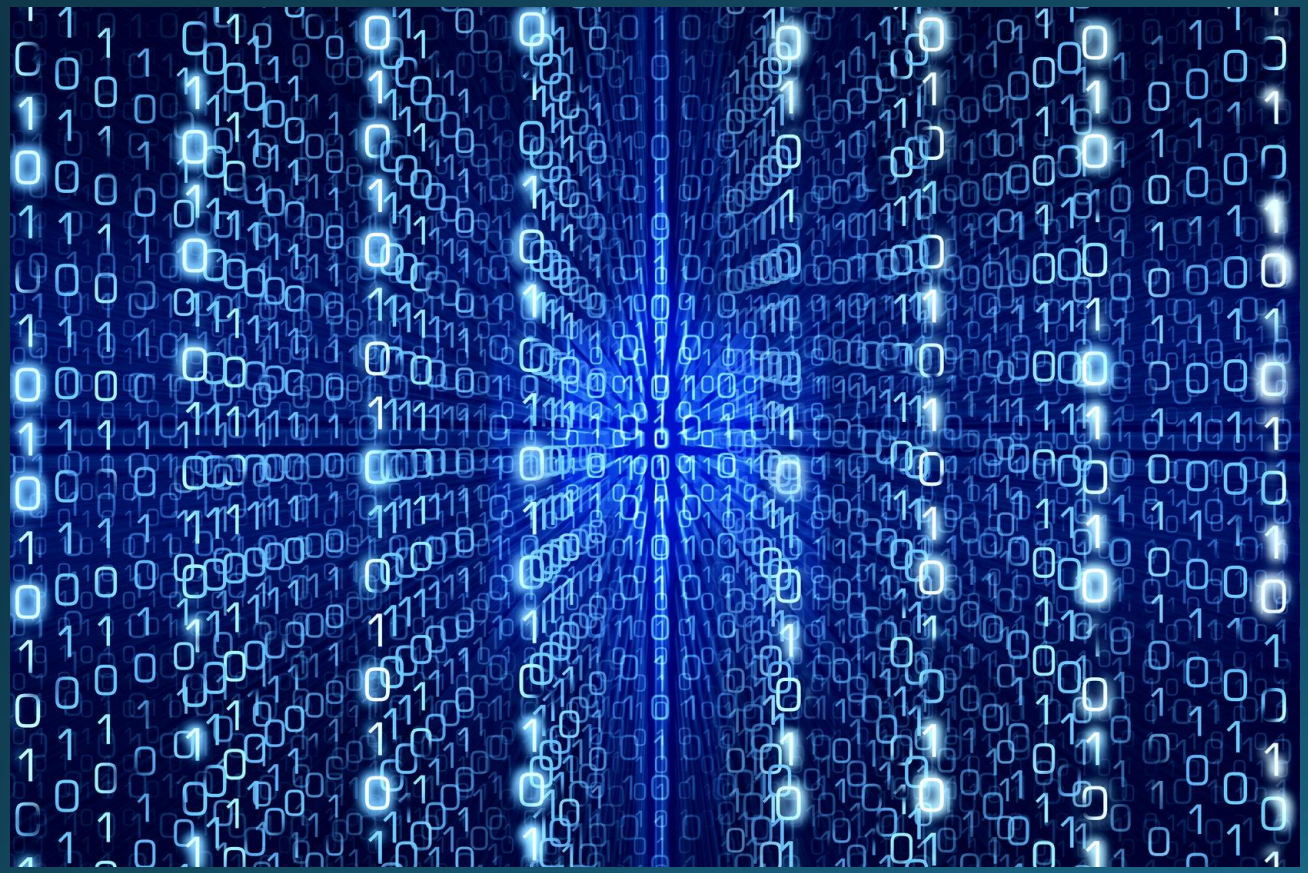
сетевые хакеры – их цель глобальные и локальные сети.

Классификация по уровню квалификации пользователя (субъекта преступления) и его возможности в выборе «криминальных информационных технологий» :

1) Преступления, **совершённые пользователем с применением простейших информационных технологий**, когда информационно-телекоммуникационные технологии используются примитивно. Противоправное деяние может быть совершено даже «случайным» пользователем, т. е. не требует наличия у преступника криминальных навыков и профессиональных знаний в области информационно-телекоммуникационных технологий.

2) Преступления, **совершённые опытным пользователем с применением информационных технологий среднего уровня**. Преступление способен совершить профессиональный непрограммирующий пользователь.

3) Преступления, **совершённые пользователем-специалистом с применением сложных информационных технологий**, предполагающие использование информационно-телекоммуникационных технологий и методов: их адаптация либо модификация применительно к целям преступной деятельности при наличии у преступников высокой квалификации, глубоких профессиональных знаний, умений и навыков в рассматриваемой сфере.



Киберпространство – это область взаимодействия информационных систем различного уровня, включающих следующие элементы: компьютерные системы, сети (как глобальные, так и локальные), компьютерные программы пользователей, а также данные, циркулирующие в перечисленных элементах.

Структура «кибернетического пространства»:

1. Глобальная информационная сеть (например, Интернет)
2. Локальная сеть (система ЭВМ)
3. Средства вычислительной техники (персональный компьютер, большая ЭВМ, специализированное вычислительное устройство)
4. Элемент средства вычислительной техники как отдельный носитель информации
5. Информационная структура первого уровня (логический носитель информации)
6. Информационная структура второго уровня (файл)
7. Информационная структура третьего уровня (запись файла)
8. Элементарная информационная группа (слово - 16, 32, 64 или более бит, размещенных рядом друг с другом, байт, бит).

Особенности преступлений, совершаемых в киберпространстве

– **повышенная скрытность** совершения преступлений, что становится возможным благодаря специфике сетевого информационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т. п.);

– **трансграничный характер сетевых преступлений**, когда преступник, объект криминального посягательства, потерпевший могут находиться на территориях разных государств;

– **высокая квалификация преступников** в области компьютерных технологий, интеллектуальный характер преступной деятельности;

– **нестандартность, сложность, многообразие** и динамичное обновление способов совершения преступлений и применяемых специальных средств;

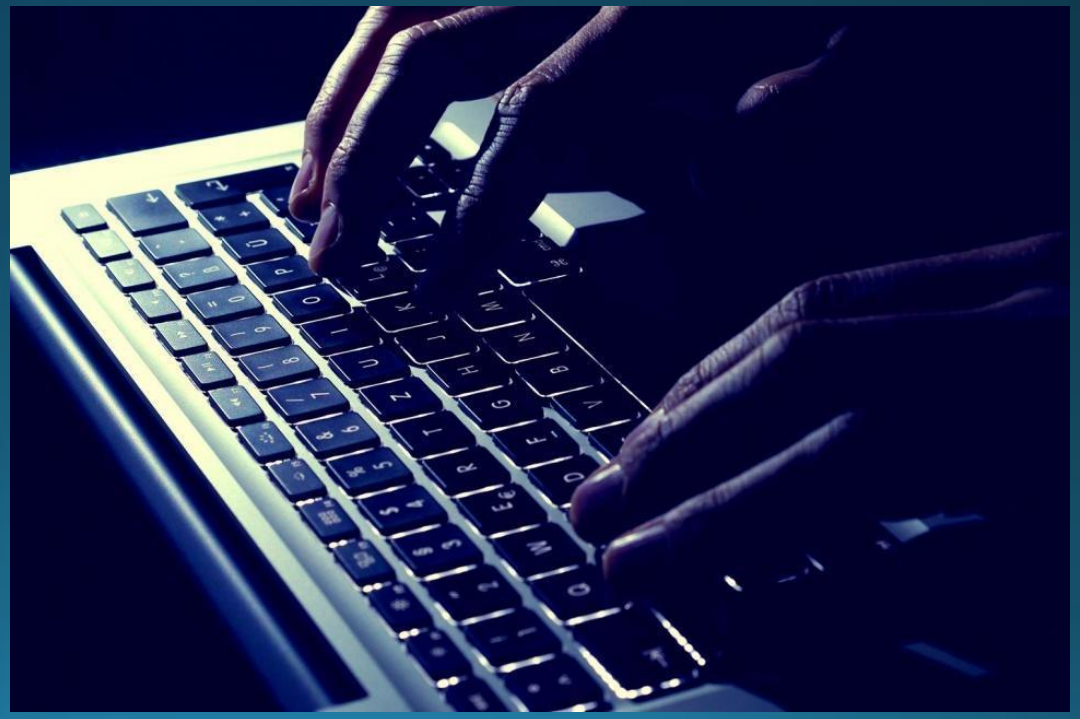
– возможность **совершения преступления в автоматизированном режиме в нескольких местах одновременно**, возможность объединять относительно слабые ресурсы многих отдельных компьютеров в мощное орудие совершения преступления;

– **многоэпизодичный характер** криминальных действий с множеством потерпевших;

– **неосведомлённость потерпевших** о том, что они подверглись преступному посягательству (воздействию);

– **дистанционный характер преступных посягательств**, отсутствие физического контакта преступника и потерпевшего; невозможность предотвращения и пресечения преступлений данного вида традиционными криминалистическими средствами

Виртуальные следы – это данные о совершении действий в информационном пространстве технических устройств, их сетей и систем, такие как: создание, включение, удаление, внесение изменений, активация, открывание.



Виды виртуальных (кибер) следов

1. Сетевые виртуальные следы – это данные, сохраненные провайдером (информация о сеансе связи, статистические или динамические IP-адресные журналы регистрации провайдера в сети Интернет, телефонные номера, скорость передачи сообщения, исходящие сеансы связи, типы использованных протоколов и т. д.), LOG-файлы.

2. Локальные виртуальные следы – следы, остающиеся на компьютерах, используемых для совершения преступных действий, либо через которые проходит или поступает информация (таблицы размещения файлов FAT, NTFS и др., системные реестры операционных систем, отдельные кластеры магнитного носителя информации, файлы и каталоги хранения сообщений электронной почты, файлы конфигурации программ удаленного доступа и иное).

Источники виртуальных следов

1. **Электронный почтовый ящик.** Здесь могут быть оставлены виртуальные следы в виде переписки по вопросам финансирования терроризма.

2. **Интернет-сайт.** Обычно это популярные ресурсы в сети Интернет.

3. **Профиль в социальных сетях**. В ходе анализа уголовных дел по финансированию терроризма было выявлено, что информация, находящаяся в социальной сети («ВКонтакте», «Одноклассники» и др.), чаще становится объектом преступного посягательства по мотивам мести, из хулиганских побуждений, нежели в корыстных целях. Это выделяет ее среди остальных видов.

4. **Счет в электронных платежных системах** («Qiwi-кошелек», «Яндекс.Деньги», Perfect Money и др.).

5. **База данных** (абонентов операторов связи и др.).

6. **Локальная сеть.** Возможность доступа к ресурсам (программам, файлам, папкам и др.) всех соединенных между собой посредством кабелей (телефонных линий, радиоканалов) компьютеров.

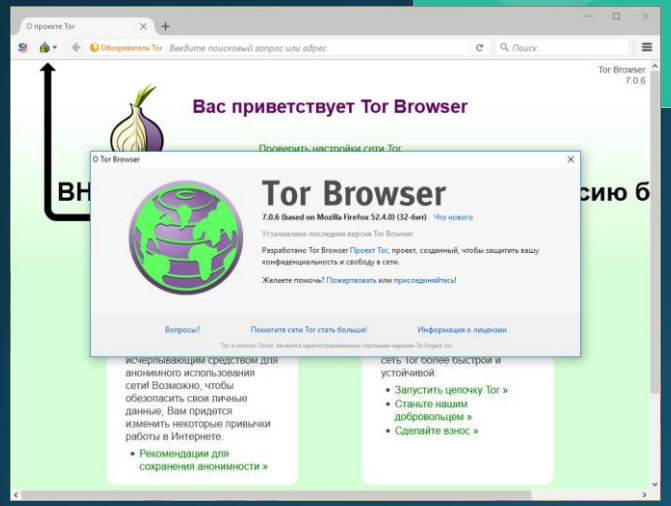
7. **Сетевые устройства** (роутеры, маршрутизаторы и т.д.).

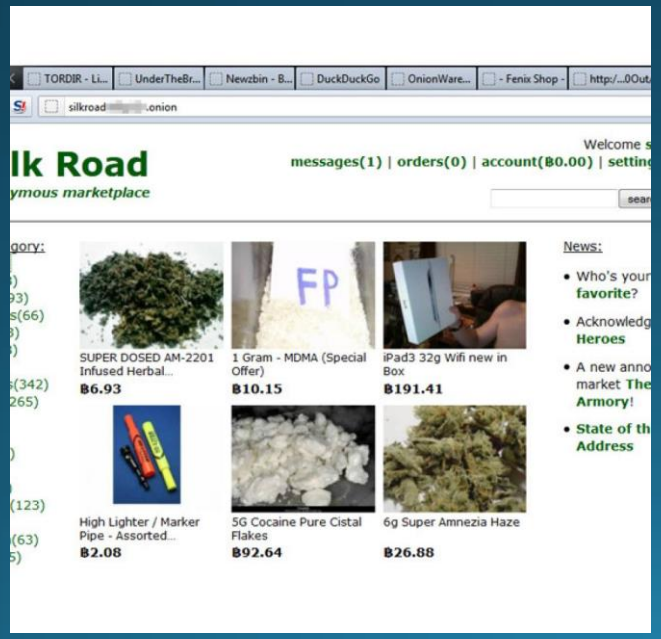
8. **Компьютер.** Жесткий диск содержит информацию о его включении, применении разных материалов, отправке счетов, выполнении иных манипуляций. Благодаря работе памяти компьютера сведения об активности ресурсов операционной системы сохраняются, поэтому их можно использовать как источник доказательств в уголовном процессе.

9. **Устройства хранения компьютерной информации** (флешки, мобильные винчестеры и т.д.)

10. **Средства мобильной связи** (как правило, применяются операционные системы Android и Apple в силу обширной распространенности). Лица, причастные к финансированию терроризма, могут оставить следы использования мобильных устройств в виде информации о соединениях между абонентами и (или) абонентскими устройствами .

Сокрытие виртуальных следов





Анонимайзеры - работа с интернет-сервисами через прокси-серверы.

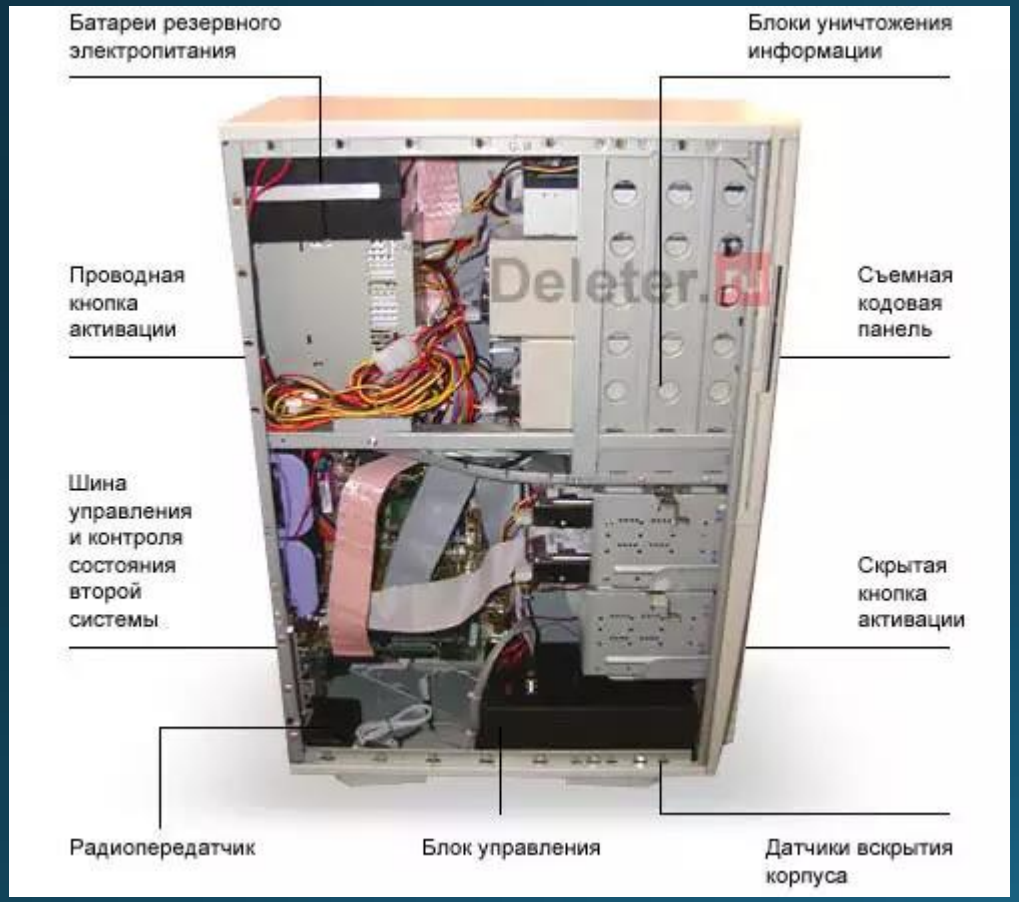
VPN Whoer.net лишен всех перечисленных выше недостатков анонимайзера: VPN работает быстро, не режет скорость вашего провайдера, не показывает рекламу, стабильно работает, обладает списком IP-адресов разных стран, шифрует весь трафик в обе стороны и не записывает логи.

Tor, децентрализованная сеть прокси-серверов.

Дарк нет (англ. DarkNet, с англ. — «скрытая сеть», «тёмный интернет», «теневой интернет», также — Dark Web) — скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов.

Программно-аппаратные комплексы экстренного удаления данных с физических носителей компьютерной информации

Система уничтожения информации Цунами



Импульс-EUSB 3.5

Мобильный уничтожитель информации с внешних магнитных носителей

УСТРОЙСТВА ЭКСТРЕННОГО УНИЧТОЖЕНИЯ ДАННЫХ НА SSD-НАКОПИТЕЛЯХ «РАСКАТ» (МОДУЛЬ-СЛОТ SSD).

Магма-4
Экстренное уничтожения информации с USB-накопителей с флеш-памятью

Flash-накопитель подключается к изделию "Магма-4" через выделенный USB-порт. Уничтожение информации производится специальным импульсом высокого напряжения. Для предотвращения замыкания напряжения через контроллер, воздействие производится непосредственно на элемент памяти, чем достигается гарантированное уничтожение информации.

При необходимости транспортировки изделие "Магма-4" обеспечивает готовность к уничтожению информации в течение 24 часов без дополнительной зарядки аккумуляторной батареи.

Импульс NB для экстренного уничтожения информации на жестких дисках ноутбука

Виды активации и управления.

Периферийные устройства позволяют производить дистанционное (в том числе беспроводное) управление устройством.

Дистанционная активация - радиоканал (дальность 40, 1000м), GSM контроллер с дополнительной возможностью получения обратной связи о активации и состоянии устройства.

Защита периметра – механические, герконовые датчики, управление охраной – бесконтактные ключи.

Импульс Сейф–
для безопасного хранения дисков или дисковых хранилищ

Виды активации и управления

Периферийные устройства позволяют производить дистанционное (в том числе беспроводное) управление устройством, организацию защиты периметра компьютерного корпуса, помещения.

Локальная активация устройства – проводные кнопки до 300м.

Дистанционная активация - радиоканал (дальность 40, 1000м), GSM контроллер с дополнительной возможностью получения обратной связи о активации и состоянии устройства.

Защита периметра – механические, герконовые датчики, управление охраной – бесконтактные ключи.

ЛВС модуль активации/мониторинга системы по локальной сети.

Paraben Data Shredder Stick

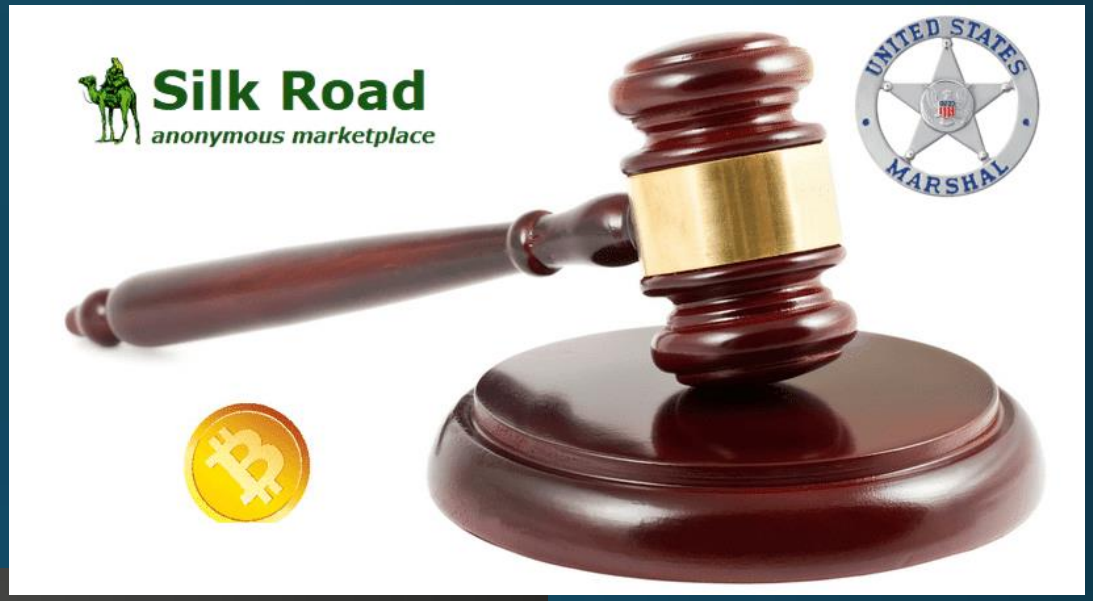
Устройство в виде флэш-накопителя, которое выступает в качестве портативного «шреддера» цифровых документов.

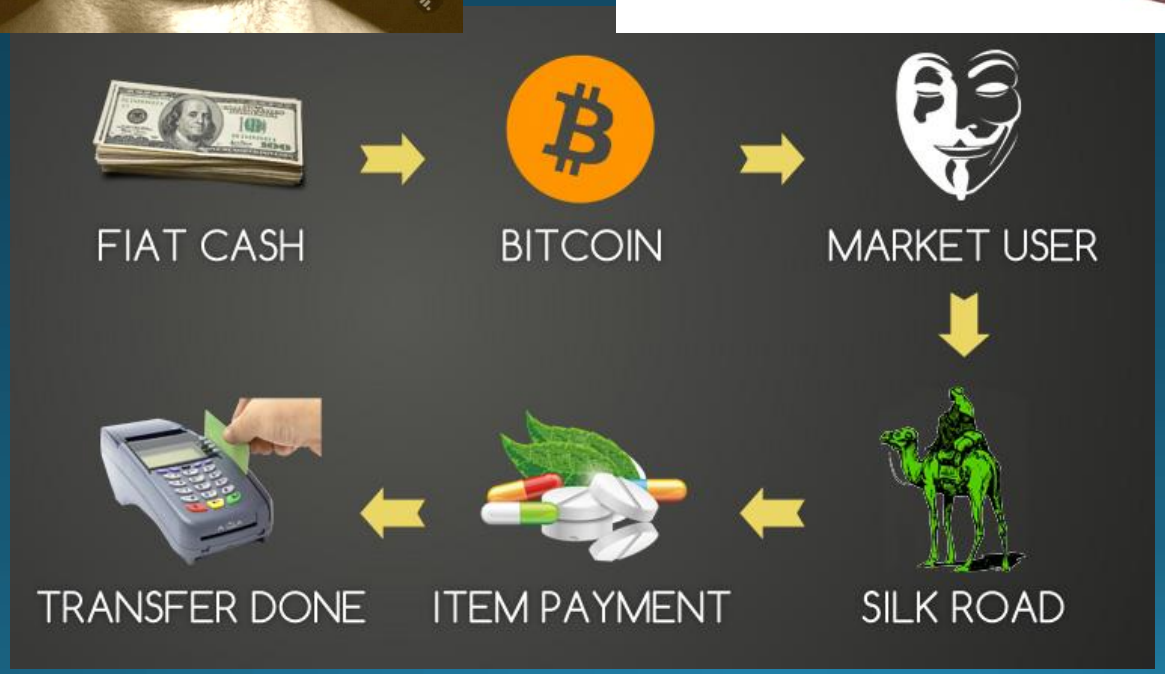
Когда удаляются файлы на компьютере, на самом деле они остаются доступными, даже если вы очистите вашу корзину. Файлы могут быть восстановлены с помощью инструментов восстановления данных, пока они не будут перезаписаны новыми данными. Data Shredder Stick позволяет удалить навсегда отдельные файлы и папки или уничтожить все ранее удаленные данные целого диска.

Противодействие анонимайзерам

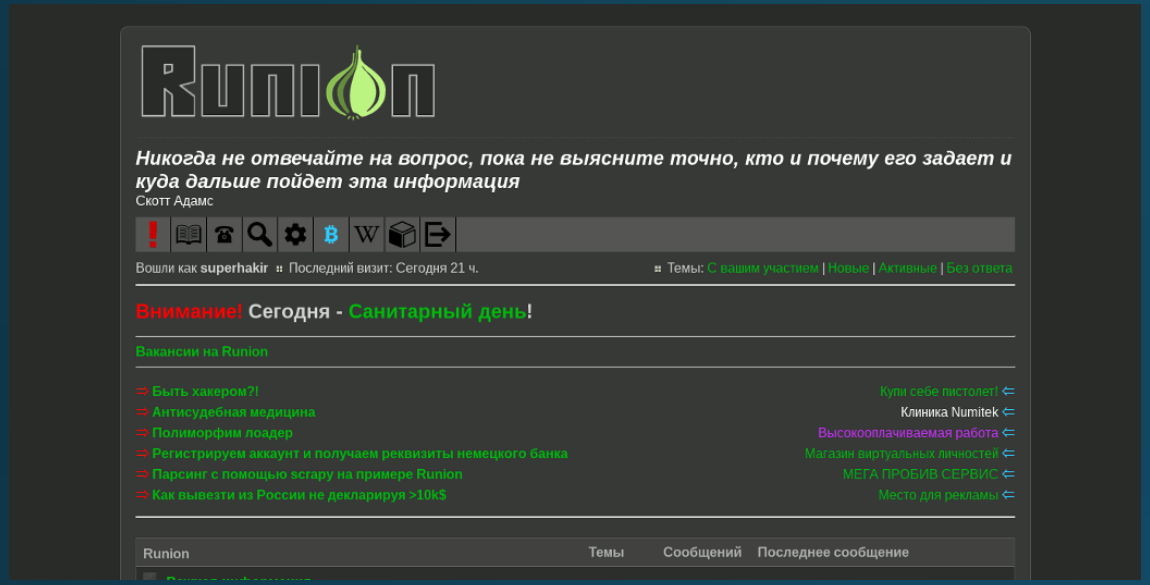
Осенью 2016 года полиция Швеции совместно с коллегами из других стран провела международную операцию «Титан». Результат? Поймано 3000 покупателей наркотиков в сети Tor.

Противодействие анонимайзерам

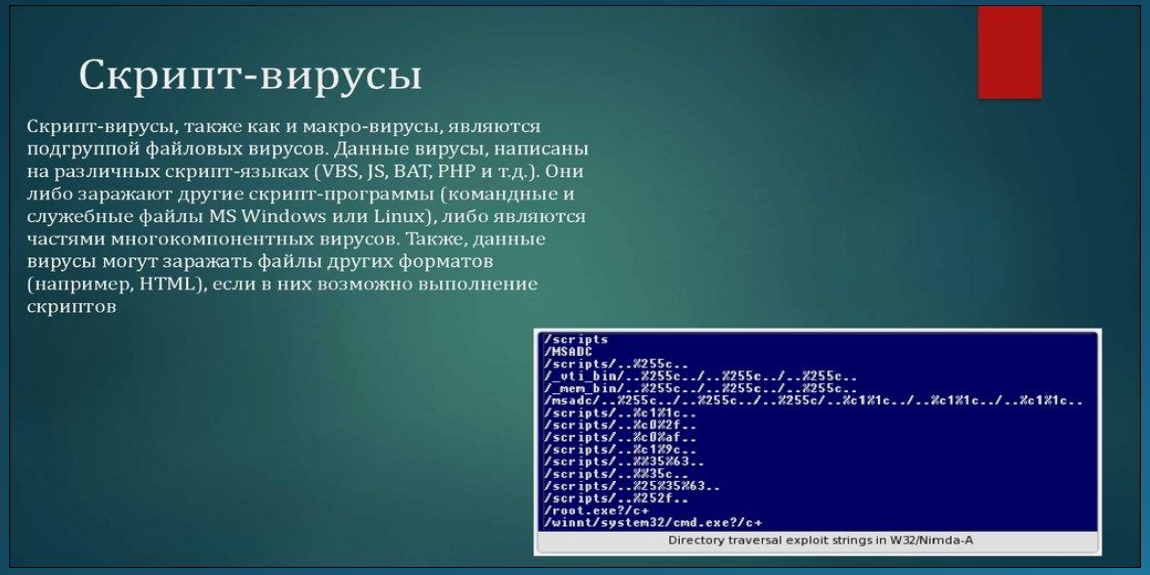




Противодействие анонимайзерам



Взлом аккаунтов на сайтах даркнета

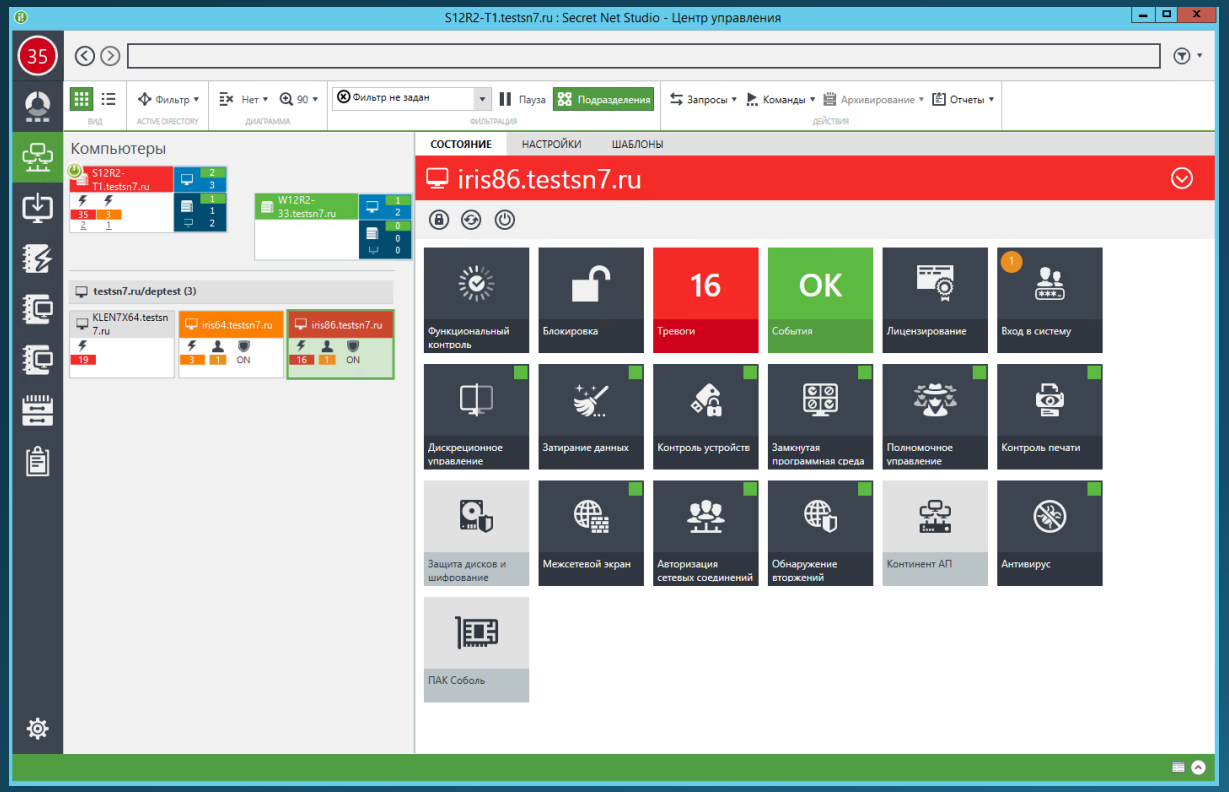


Загрузка вирусов и вредоносных скриптов

Методы выявления незаконных действий в киберпространстве

- Перехват и исследование трафика
- Исследование статистики трафика
- Исследование логов веб-сервера
- Исследование системных логов
- Исследование логов мейл-сервера и заголовков электронной почты
- Установление принадлежности и расположения IP-адреса
- Установление принадлежности доменного имени
- Принадлежность адреса электронной почты
- Кейлогеры

Первоначальный этап обнаружения незаконных действий в киберпространстве должен обнаруживаться и фиксироваться специальным программами, обеспечивающими кибербезопасность страны, предприятия и т.д.



ForensicTools
инструменты для компьютерных расследований

Аппаратные средства

Устройства для клонирования жестких дисков и других носителей (в том числе в полевых условиях)

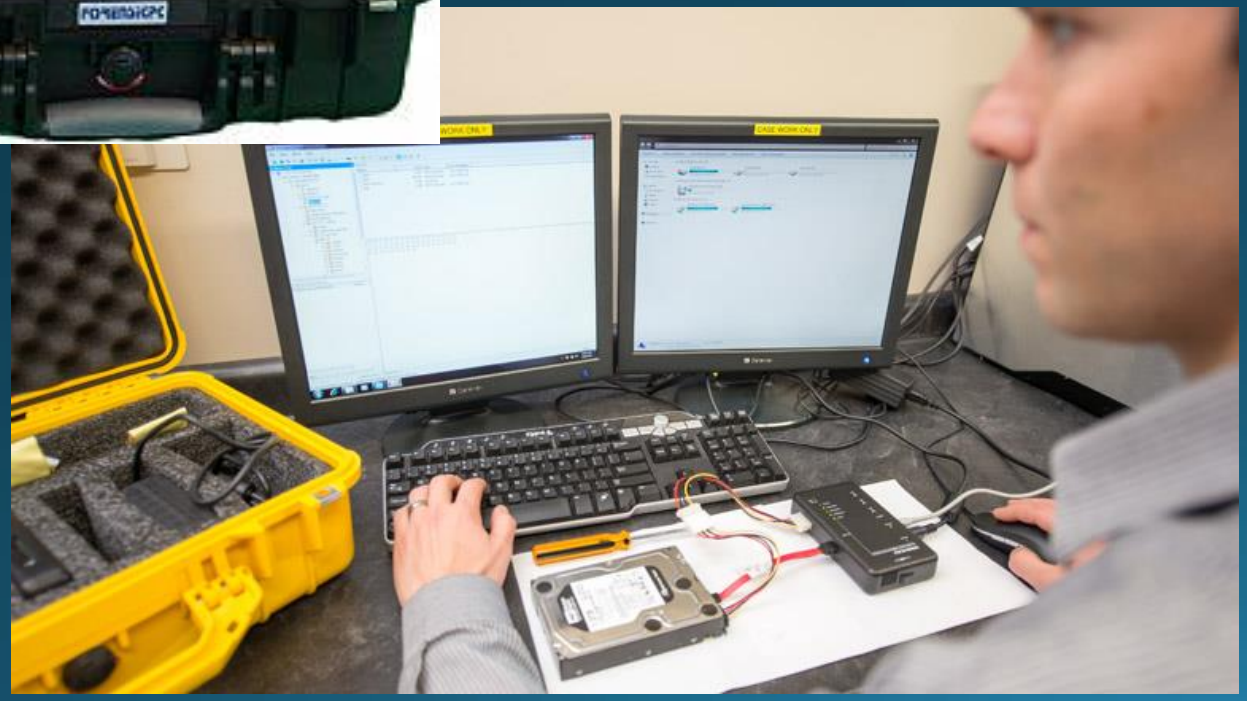
Мобильная лаборатория RoadMASSter-3

Мобильная лаборатория RoadMASSter-3 предназанчена для извлечения, дублирования и анализа информации. Она позволяет быстро и надежно создавать образ и проводить анализ данных. Эта компьютерная система спроектирована для работы в полевых условиях с такими интерфейсами как FireWire 1394A/B, USB, IDE, SATA, SAS и SCSI. RoadMASSter-3 является мощным и универсальным инструментом для экперта-криминалиста благодаря поддержке разлинчых типов медиа носителей, нескольким методам извлечения информации с возможностью хэширования и мощным процессором для проведения анализа.

ImageMASSter Solo-3 Forensic Kit

Комплект технических средств для копирования данных.

ForensicPC Ultimate Write Block Kit



Специально разработанный портативный комплект аппаратных блокираторов записи, используемых при проведении судебного дублирования различных накопителей.

Переносные компьютеры с комплексом программных и аппаратных средств, ориентированных на исследование компьютерной информации в полевых условиях.

Специализированная переносная лаборатория FREDDIE

Сервер для криминалистов FREDDIE снабжен устройством UltraBay 3 Write Protected Imaging Bay для получения образа исследуемого диска в режиме "защиты от записи". Комплекс FREDDIE представляет из себя гибкую масштабируемую систему для получения и анализа компьютерных улик.

Аппаратные и программные средства для исследования мобильных телефонов (SIM-карт), навигаторов, плееров и т.д.

UFED 4PC

Универсальный аппаратно-программный комплекс для криминалистических исследований, дающий возможность извлекать, декодировать и анализировать цифровые данные, полученные из мобильных устройств, на существующем ПК или ноутбуке. Комплекс поставляется с набором приложений UFED, периферийными устройствами и принадлежностями, нужными для успешного проведения исследований. UFED 4PC может работать как автономно, так и со сторонним программным обеспечением.

UFED Touch Ultimate

Решение для извлечения, декодирования, анализа данных и составления отчетов, специально сконструированное с учетом поддержки высокопроизводительных устройств. Комплекс позволяет выполнить извлечение данных на физическом, логическом уровнях и на уровне файловой системы, а также восстановление паролей (даже удаленных) с самых разнообразных устройств, включая устаревшие и мобильные телефоны, смартфоны, портативные устройства GPS и планшетные компьютеры. Благодаря собственному аппаратному оборудованию, встроенному аккумулятору, интуитивно понятному графическому интерфейсу и сенсорному экрану, UFED Touch Ultimate ускоряет процесс расследования и полностью отвечает требованиям мобильной криминалистики.

XRY

Комплекс исследования информации с мобильных устройств, таких как мобильные телефоны, смартфоны различных производителей, GPS навигаторы, планшеты и 3G модемы.

Eclipse Screen Capture Kit

Предназначен для фиксации пользовательской информации с экранов мобильных телефонов, GPS навигаторов, Tablet PC и других портативных устройств, экраны которых могут быть сфотографированы.

Аппаратные средства для исследования локальных сетей

Fluke Networks WiFi AirCheck - анализатор Wi-Fi сети

Функциональные возможности WiFi AirCheck:

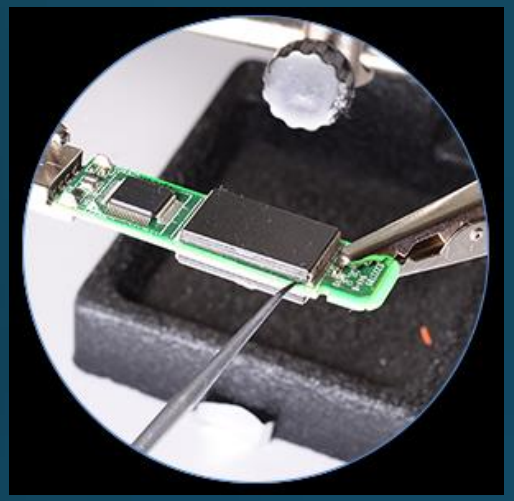
- Автоматическое тестирование одной кнопкой
- Вывод списка точек доступа в каждом канале в полосах частот 2,4 и 5 ГГц
- Сведения о точке доступа
- Статус авторизации точки доступа
- Обнаружение местонахождения точек доступа и клиентов по уровню сигнала
- Вывод списка сетей
- Тестирование возможности подключения к беспроводной сети
- Проверка соединений
- Использование канала и помехи в нем
- Подробности о клиенте
- Программное обеспечение менеджера AirCheck
- Поддержка многих языков

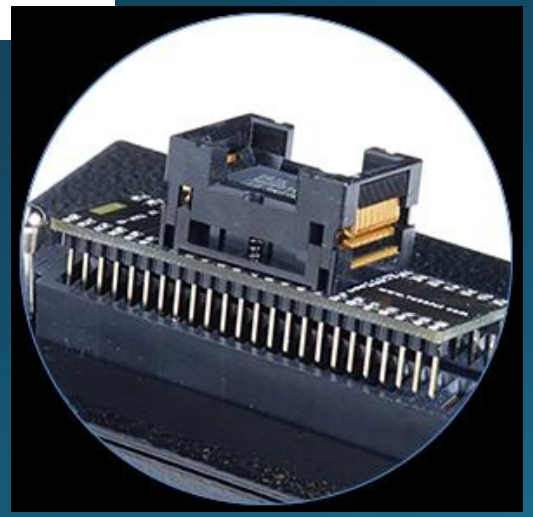
Стационарные программно-аппаратные комплексы Forensic Workstation

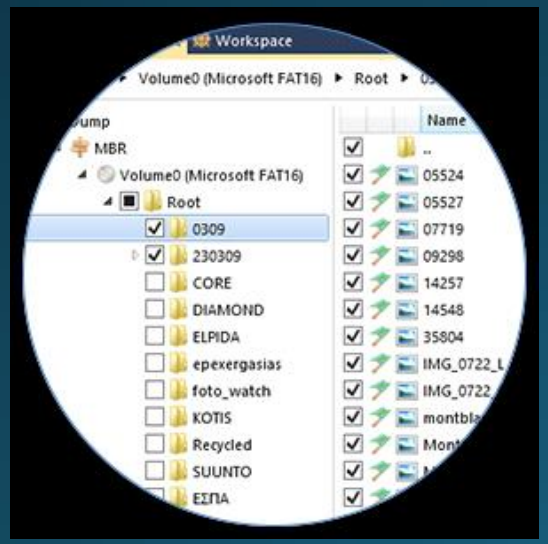
Программно-аппаратный комплекс для компьютерно-технических исследований.

- представляет мощную вычислительную систему, построенную на базе новейших компьютерных технологий, с широким набором интерфейсов для съема информации с блокировкой записи (IDE/SATA, SAS, USB), с встроенным RAID-массивом большой емкости;
- используется для криминалистического исследования компьютерных носителей информации, и мобильных устройств специализированным программным обеспечением, таким как Encase, Passware Kit Forensic и и многое другое.

Аппаратные средства восстановления данных Visual NAND Reconstructor







Универсальная платформа для Chip-Off восстановления данных и криминалистического анализа информации с поврежденных накопителей с флэш памятью.

Программные средства

Программы поиска и обнаружения виртуальных следов в киберпространстве

Paraben Phone Recovery Stick

Восстановление удаленных данных

Phone Recovery Stick базируется на проверенных технологиях мобильной криминалистики от Paraben. Он восстанавливает удаленные данные непосредственно с телефона и SD-карты. Он может не только восстановить текстовые сообщения, контакты и интернет-историю, также он может восстанавливать удаленные данные из приложений, таких как Facebook, Chrome, TextFree и многих других.

Получение всех пользовательских данных

Иногда вам нужно больше, чем восстановление удаленных данных. Иногда, вы должны видеть, что происходило на вашем устройстве. Phone Recovery Stick загружает данные пользователя и отображает их в удобном для чтения формате. Вы можете проверить все, от интернет-истории, до друзей в Facebook, Skype-переписки, закладок и многое другое.

Безопасность источника

Первым правилом криминалистики является сохранение исходных данных. Так как Phone Recovery Stick построен на базе инструмента мобильной криминалистики, вы можете быть уверены, что данные исследуемого телефона – в безопасности. Нет необходимости получать ROOT-права на телефоне.

Обход паролей

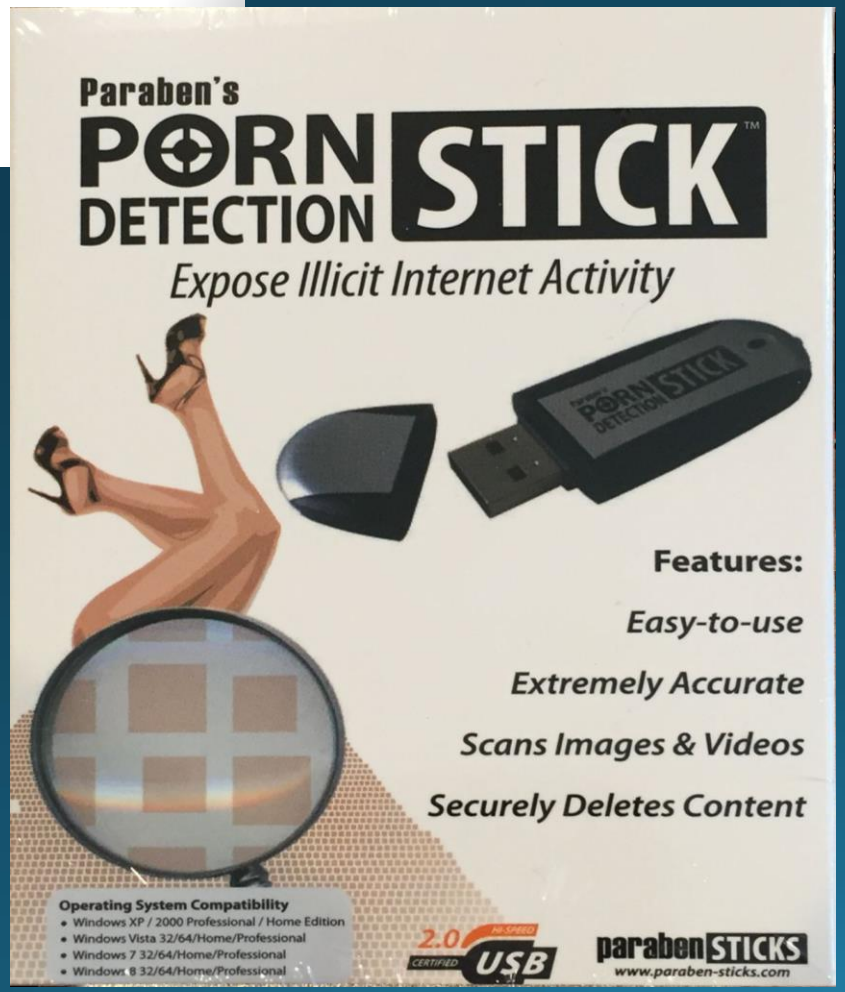
Если телефон имеет графический ключ или PIN-код блокировки на него, и он работает под управлением Android 4.1 или ниже, Phone Recovery Stick сможет обойти защиту для восстановления данных.

Paraben Fact Finder Stick

Персональный инструмент для проведения компьютерных криминалистических экспертиз, предназначен для тех, кто собирается обращаться в инстанции гражданского судопроизводства, чтобы иметь возможность собрать ценные цифровые доказательства.

Предназначен для работы с ОС Windows, и поставляется с бесплатным ПО анализа и просмотра извлеченных данных - Evidence Reviewer. Инструмент полезен для того, чтобы проанализировать данные самостоятельно или с адвокатом и определить, необходимо ли обратиться за более полной экспертизой к специалистам по криминалистике. Позволяет сэкономить время и деньги, делая первоначальный анализ данных.

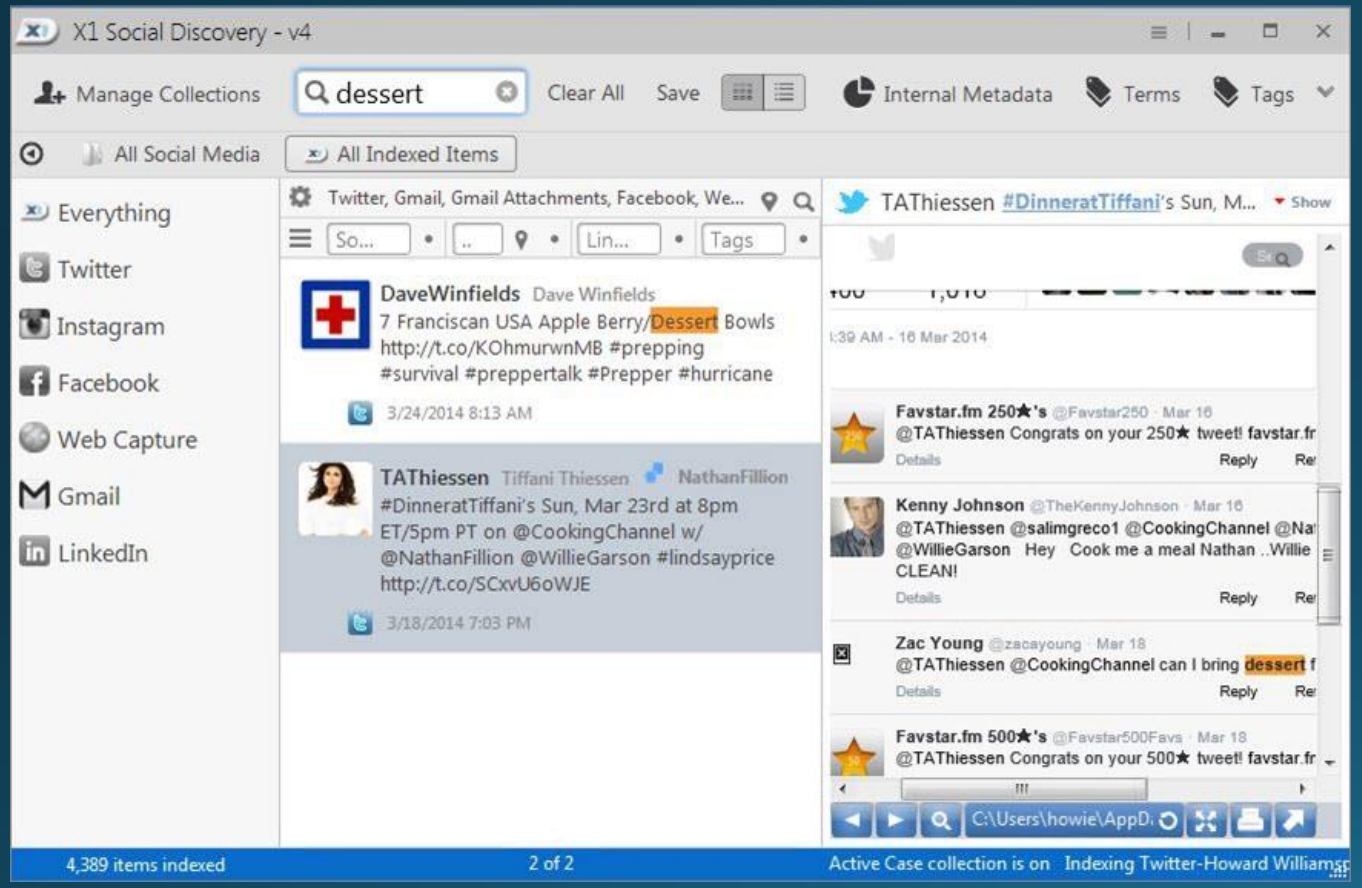
Porn Detection Stick



Флэш-накопитель, с помощью которого происходит поиск картинок и видео порнографического содержания на вашем компьютере. По окончании процесса сканирования создается отчет с перечнем файлов с предполагаемым порнографическим содержанием. Porn Detection Stick также сканирует удаленные картинки и

удаленную кэш память интернет-браузеров, поэтому не удастся скрыть какую-либо интернет активность.

X1 Social Discovery

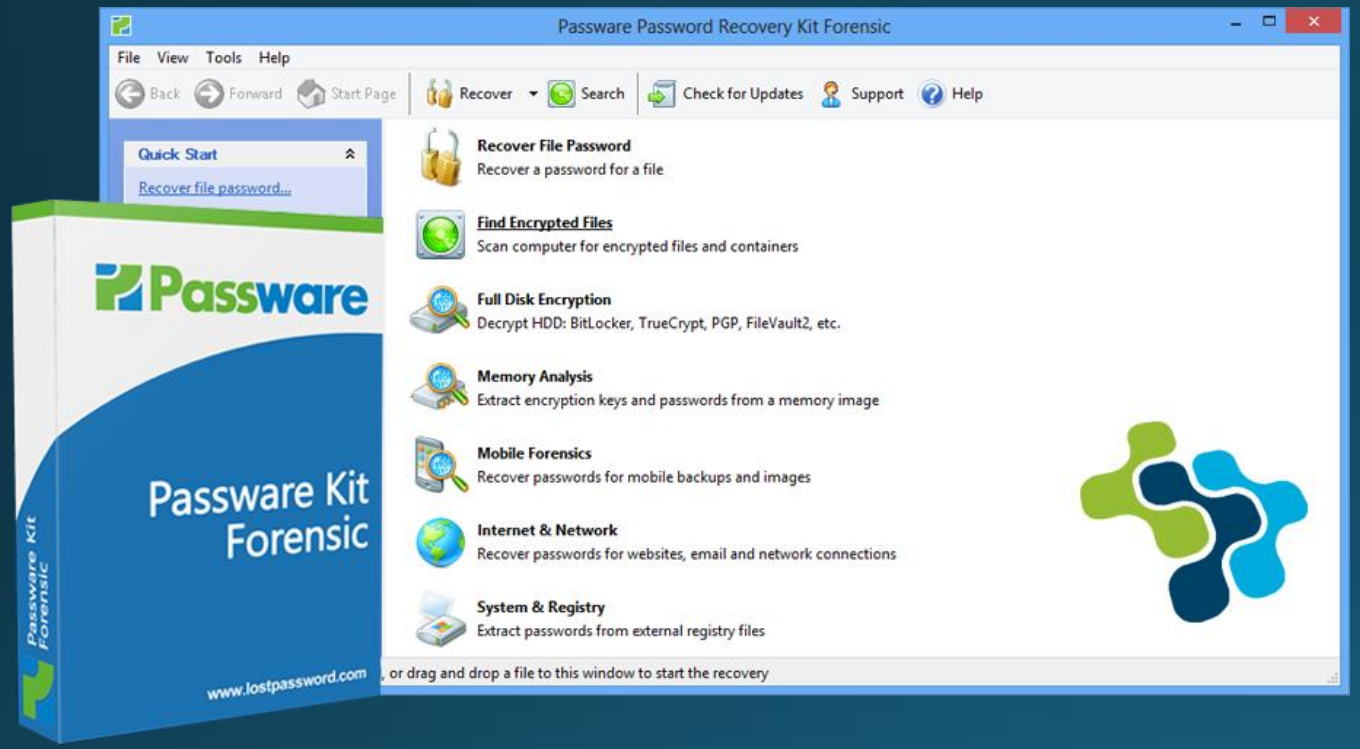


Программный продукт собирает вместе в одно целое детальный медиа контент из соц.сетей и Web данные. Решение X1 Social Discovery экономит экспертам огромное количество времени благодаря автоматизированной и одновременной работе по сбору информации из различных акканутов в социальных сетях.

Работает со следующими ресурсами:

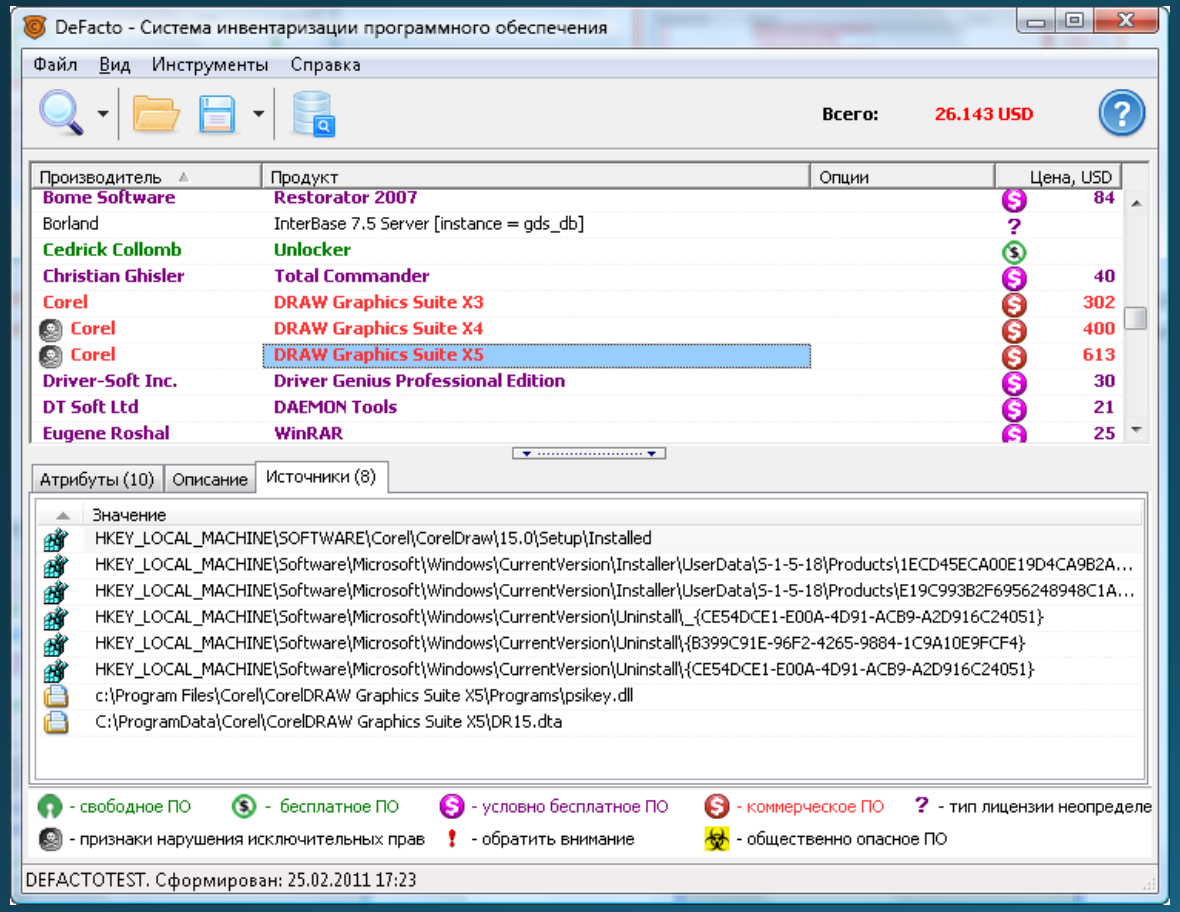
Facebook, Twitter, Instagram, YouTube, Tumblr, Web pages & websites, Gmail, YahooMail, Outlook.com, AOL Mail, Internet Message Access Protocol (IMAP).

Passware Recovery Kit Forensic



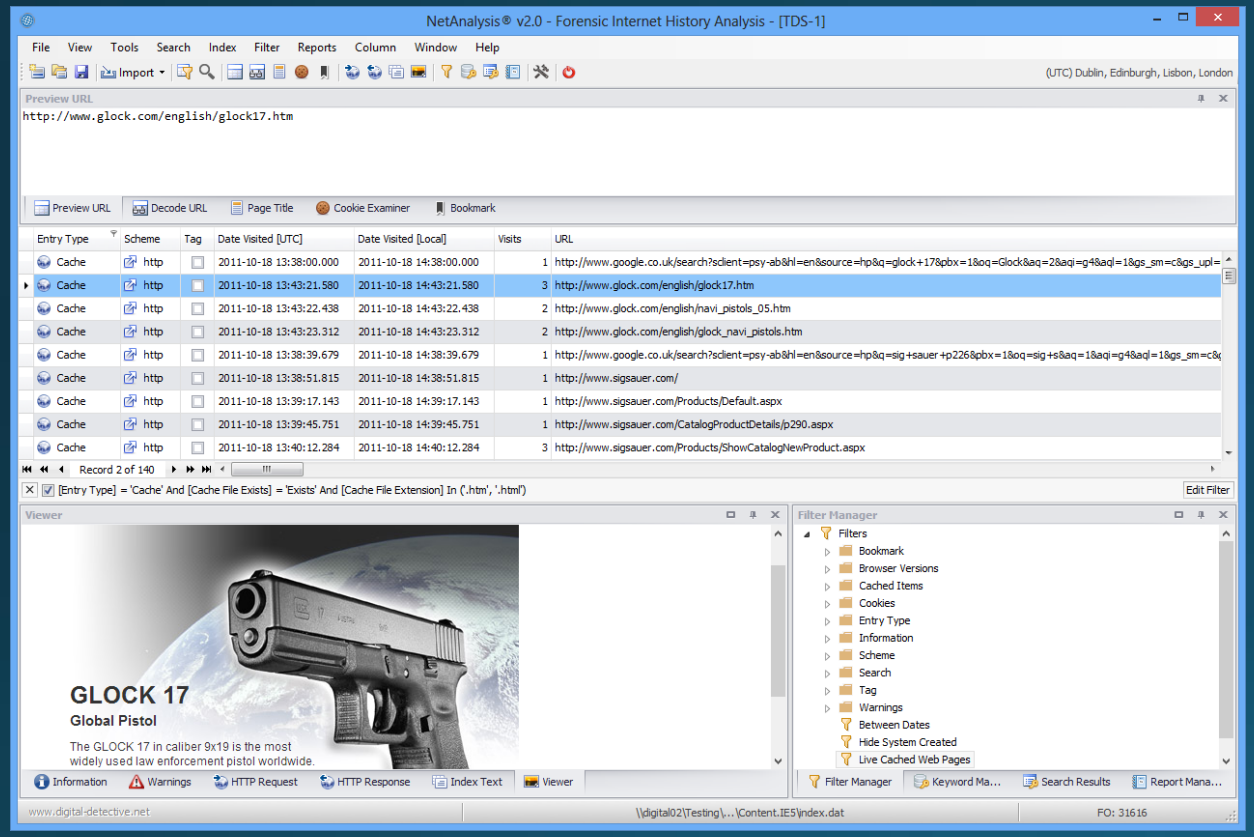
Программа включает в себя более 30 модулей восстановления паролей, объединённых в единый пользовательский интерфейс. Для восстановления сложных паролей используются передовые методы ускорения.

Defacto



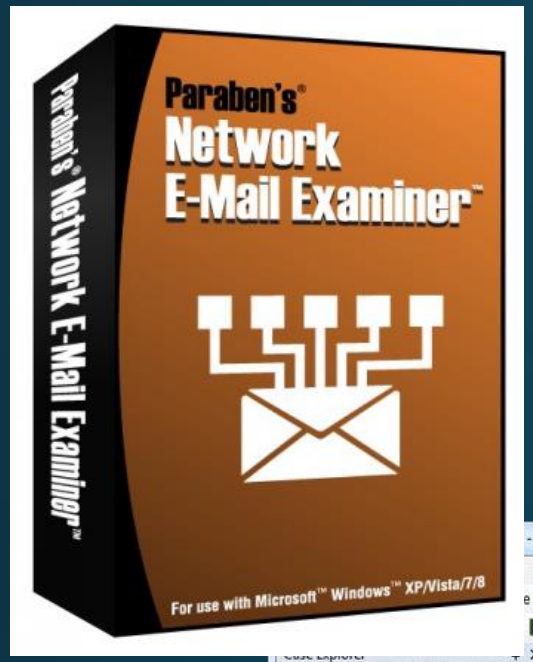
Решение предназначенное для экспресс-инвентаризации программного обеспечения, фактически установленного на жестком диске компьютера. Результаты представляются в виде таблицы, в которую сведены сведения об авторе, названии программы, ее рыночной стоимости, статусе (коммерческая, условно-бесплатная, бесплатная). Бесплатные программы отображаются зеленым цветом, платные — красным, пробные (shareware) — фиолетовым.

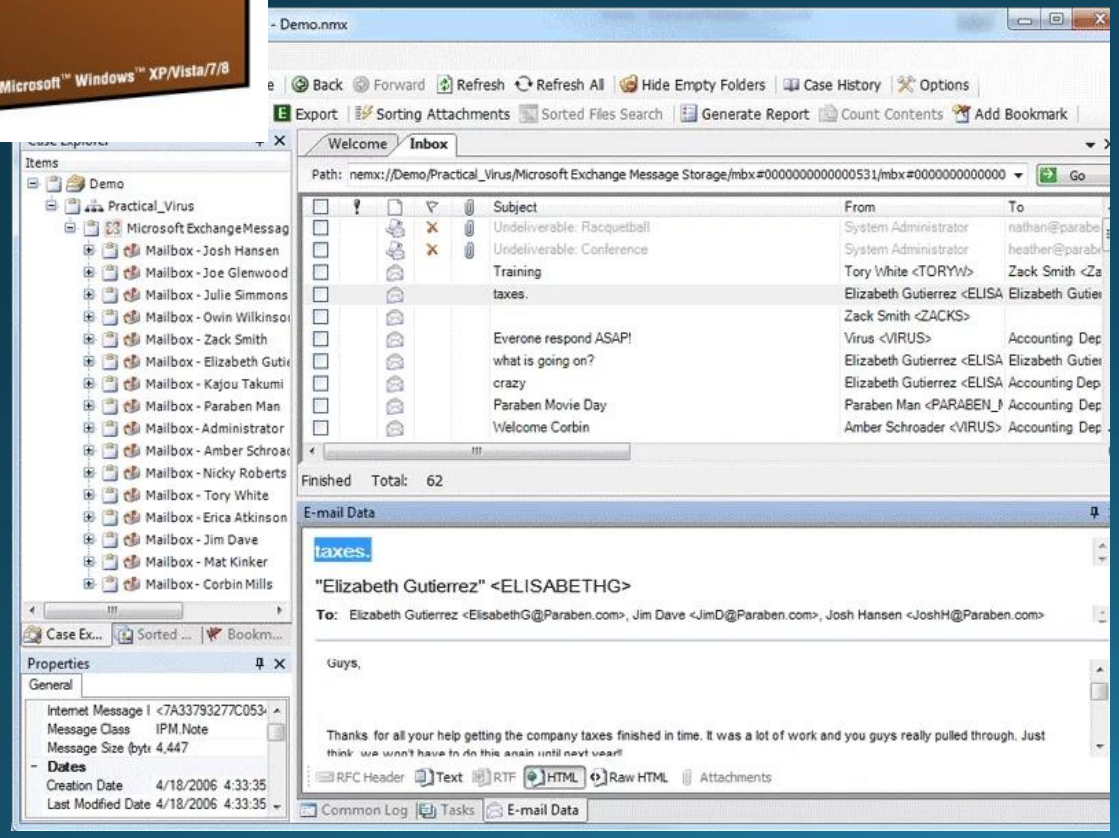
NetAnalysis



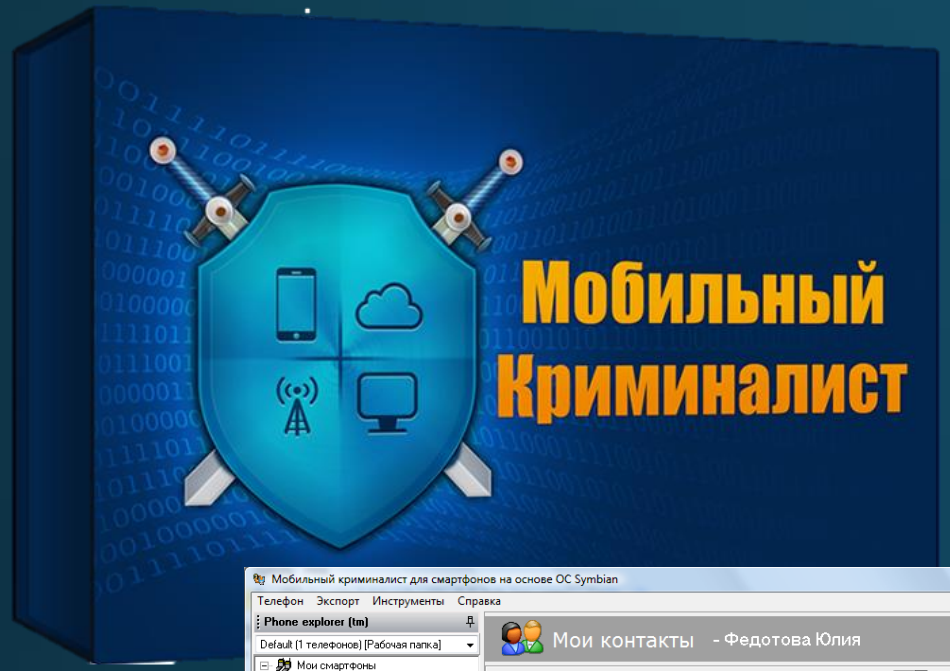
Программа для восстановления и анализа артефактов интернет-браузера. NetAnalysis также имеет уникальную функцию для быстрой идентификации возможных сайтов детской порнографии, критерии поиска, введенные пользователем, паролями и именами пользователей и доступом к онлайн-хранилищу.

Network E-mail Examiner



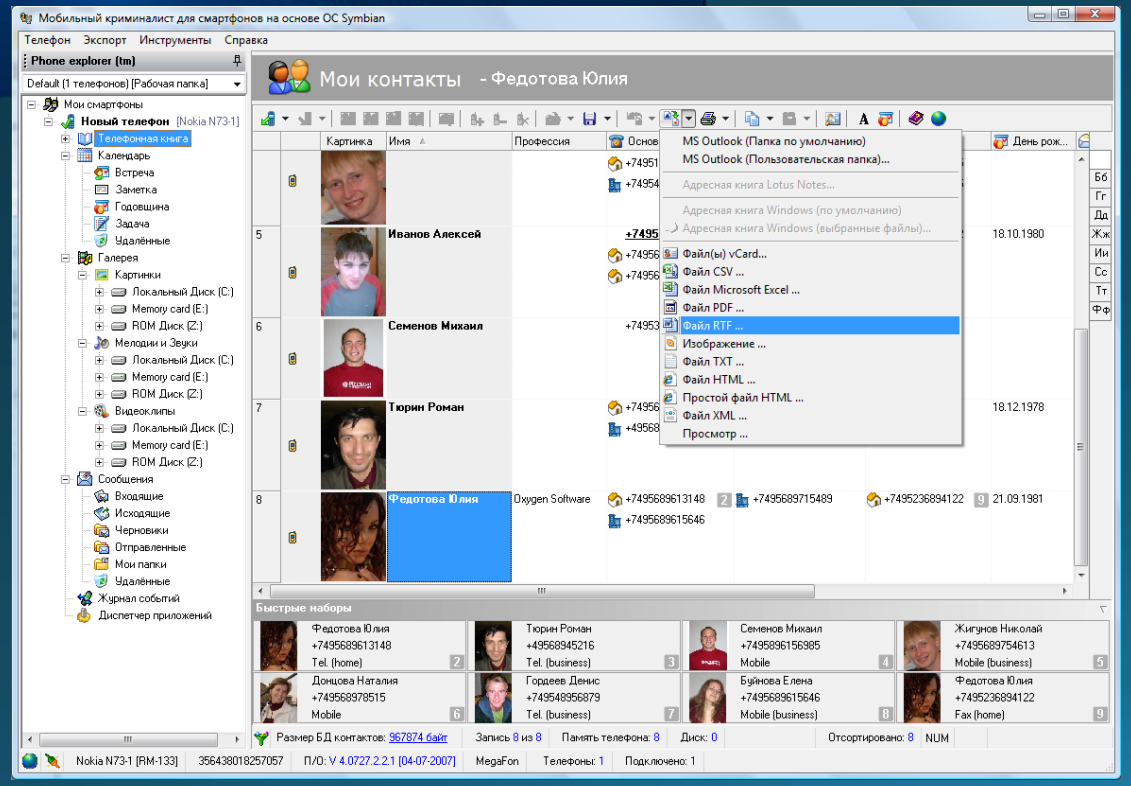


Программный продукт предназначен для экспертного анализа архивов электронной почты в корпоративной сети.

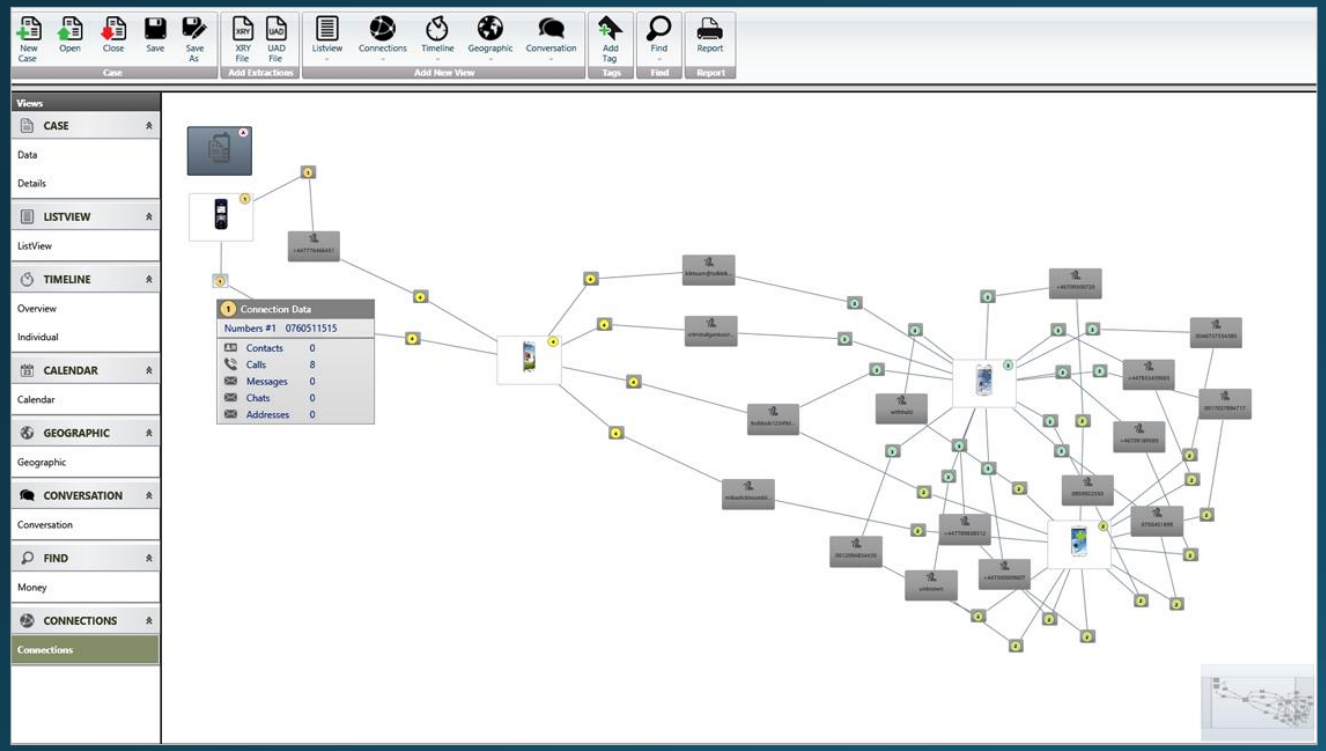


Мобильный криминалист

Универсальный программный комплекс для исследования мобильных устройств, извлечения данных из облачных хранилищ и анализа биллингов операторов сотовой связи. Программа позволяет обходить блокировку экрана, находить пароли на зашифрованные резервные копии, извлекать данные из самых надежных приложений, а также восстанавливать удаленную информацию. Данные из мобильных устройств, облачных хранилищ и биллинги операторов показаны вместе в удобном для использования интерфейсе с возможностью их глубокого анализа во встроенных аналитических секциях программы.

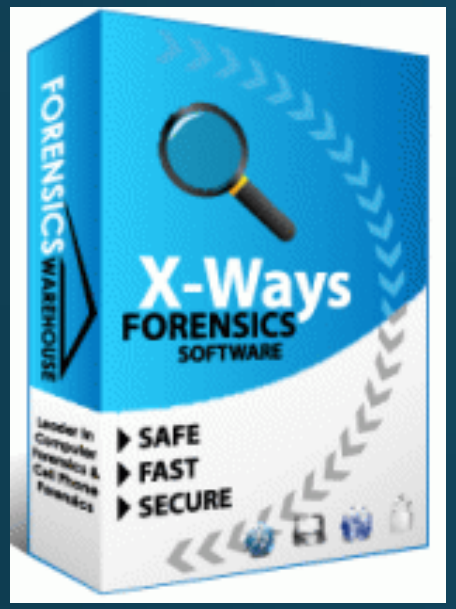


XAMN



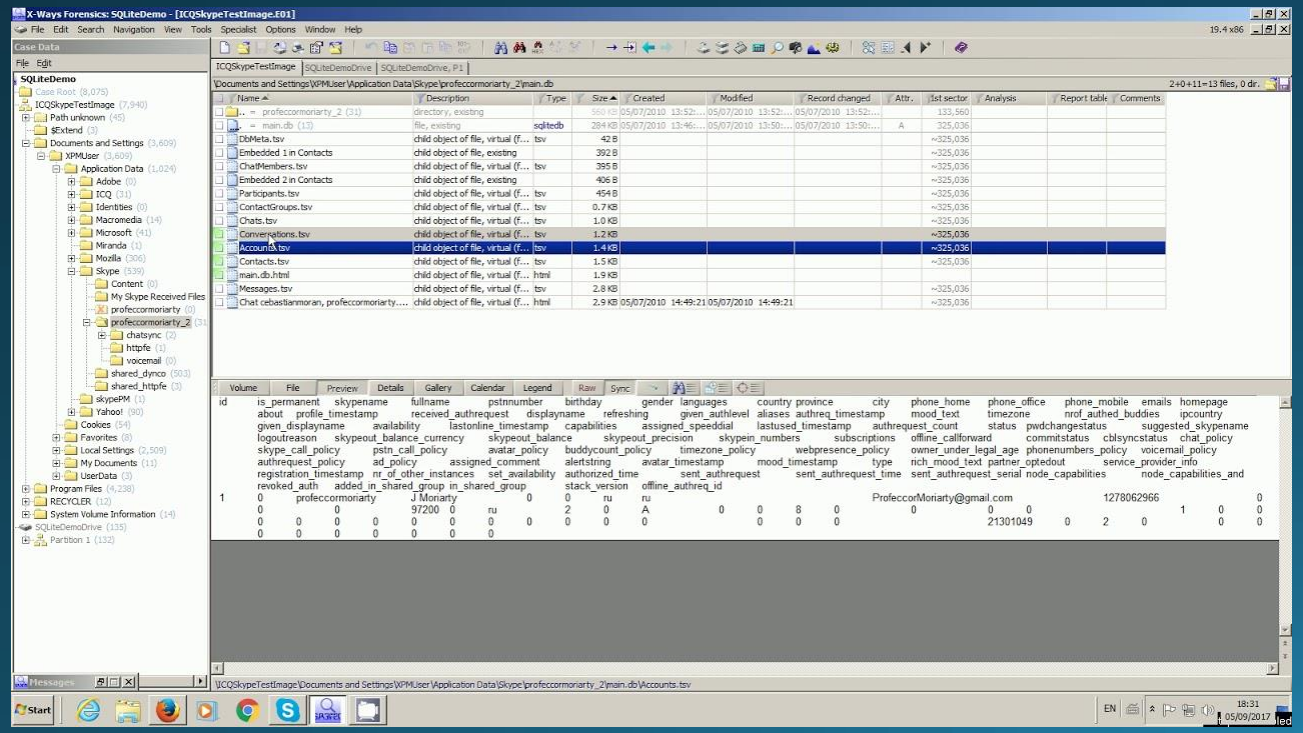
Аналитическое программное обеспечение для выявления взаимосвязей между данными, извлеченными из мобильных устройств Это комплект аналитического программного обеспечения, разработанный исключительно для сопоставления данных, извлеченных из смартфонов, планшетов и других мобильных устройств посредством экспертных инструментов. Дает возможность распознавания соединений, объединения отчетов и предоставления их в хронологическом формате, создания логических схем и нанесения геопозиционных данных на карту.

Программы для проведения компьютерно-технических экспертиз



X-Ways Forensics

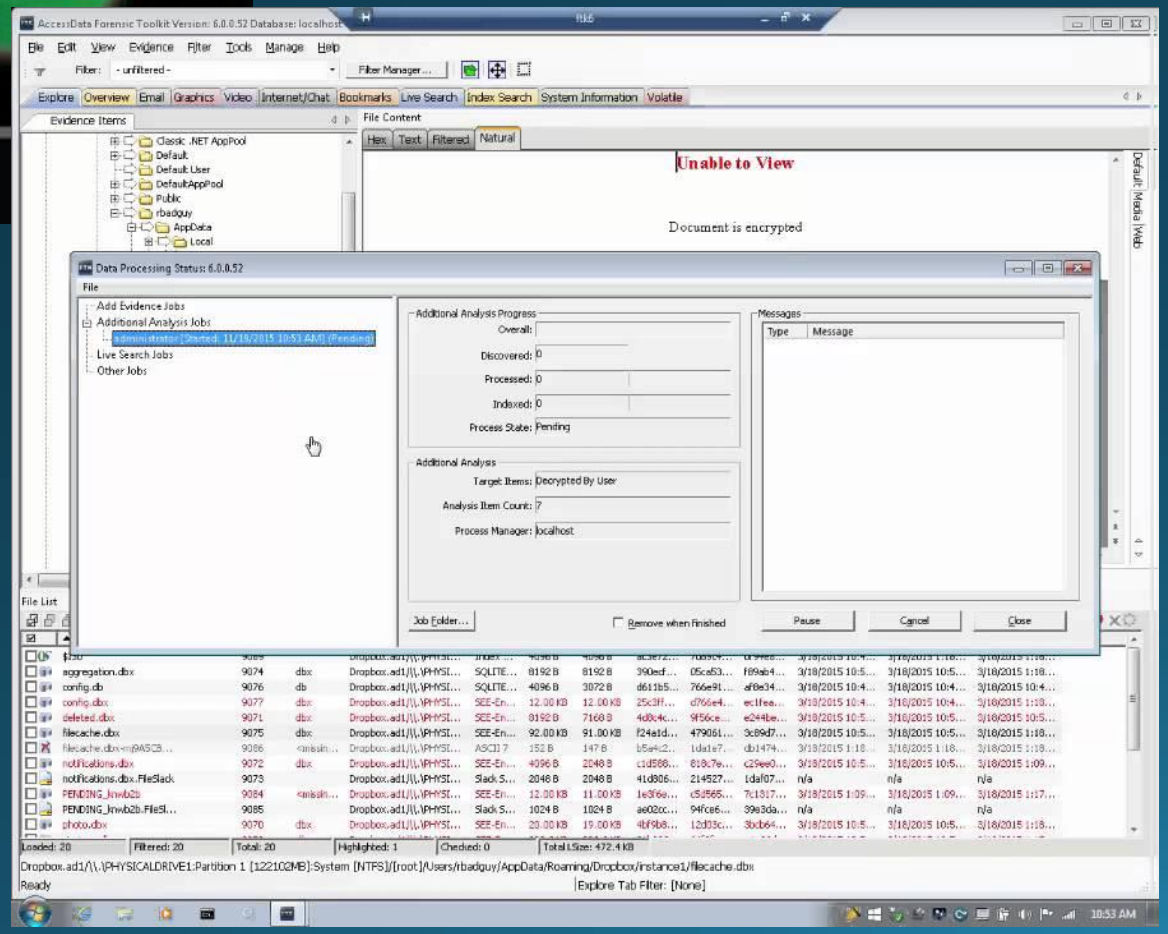
Программный комплекс, позволяющий оперативно решать практически весь спектр задач компьютерной экспертизы и расследования ИТ инцидентов, от съема данных до составления отчетов. Благодаря этому повышается эффективность работы экспертов, существенно сокращаются сроки проведения исследований.



Основные функции и возможности X-Ways Forensics

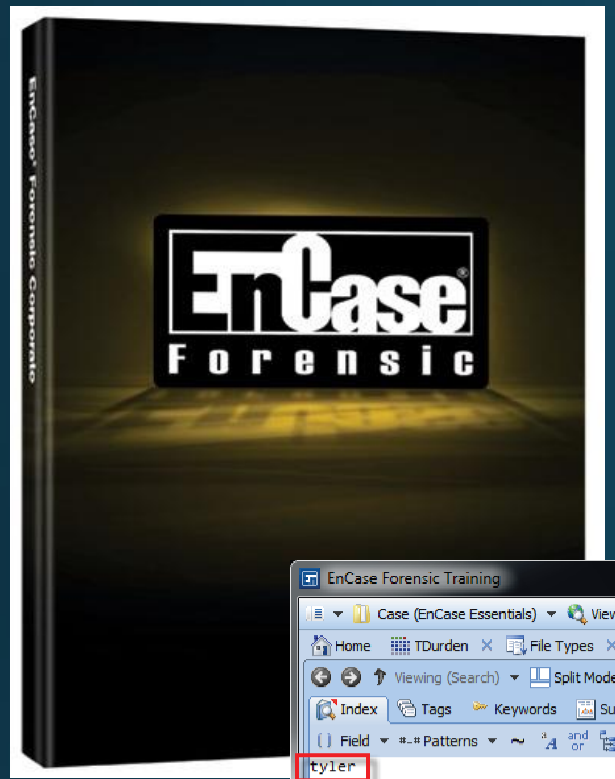
- Съем и восстановление данных
- Просмотр и анализ данных
- Поиск и индексирование
- Хэширование

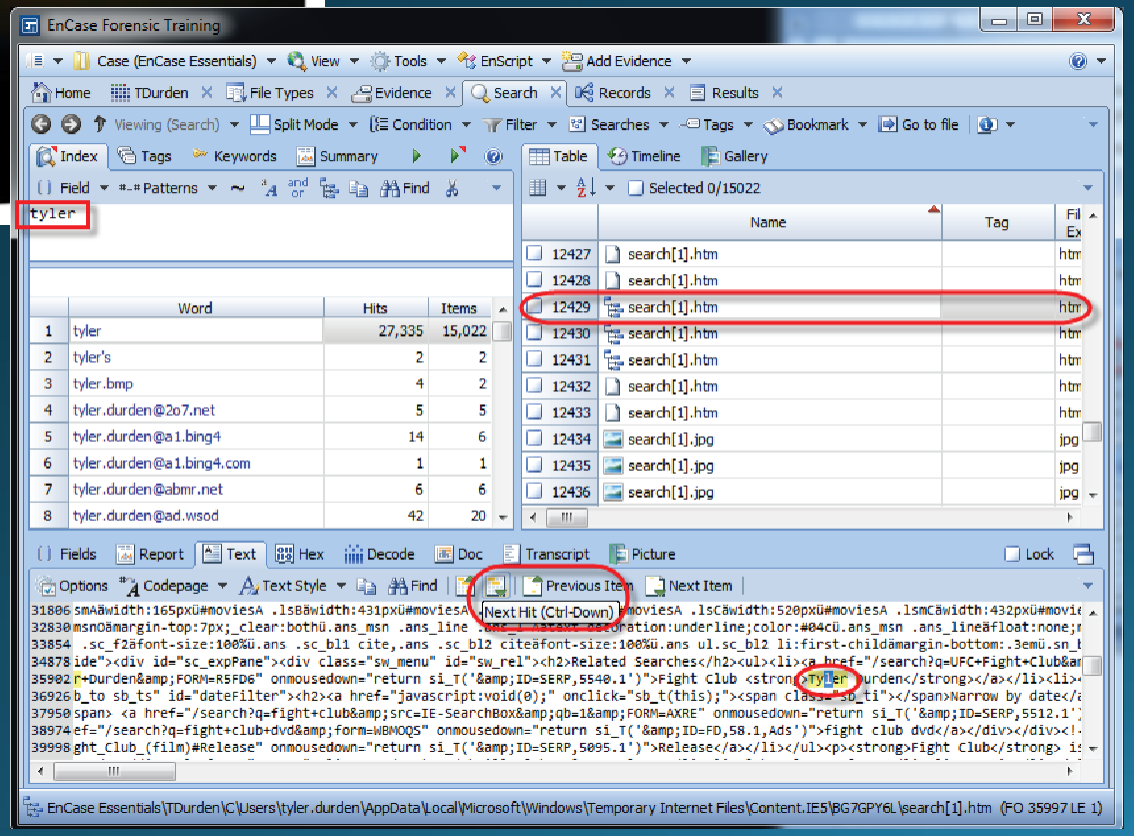
ForensicToolkit®



Программное обеспечение для проведения компьютерно-технической экспертизы, являющееся по сути международным стандартом поиска цифровых улик и предоставления данных в суд. EnCase ® Forensic позволяет экспертам получать данные с помощью широкого спектра готовых фильтров и модулей, выявлять потенциальные доказательства путем криминалистического анализа информации, содержащейся на жестком диске, и подготавливать полные отчеты о полученных результатах, сохраняя при этом надежность и целостность полученных доказательств.

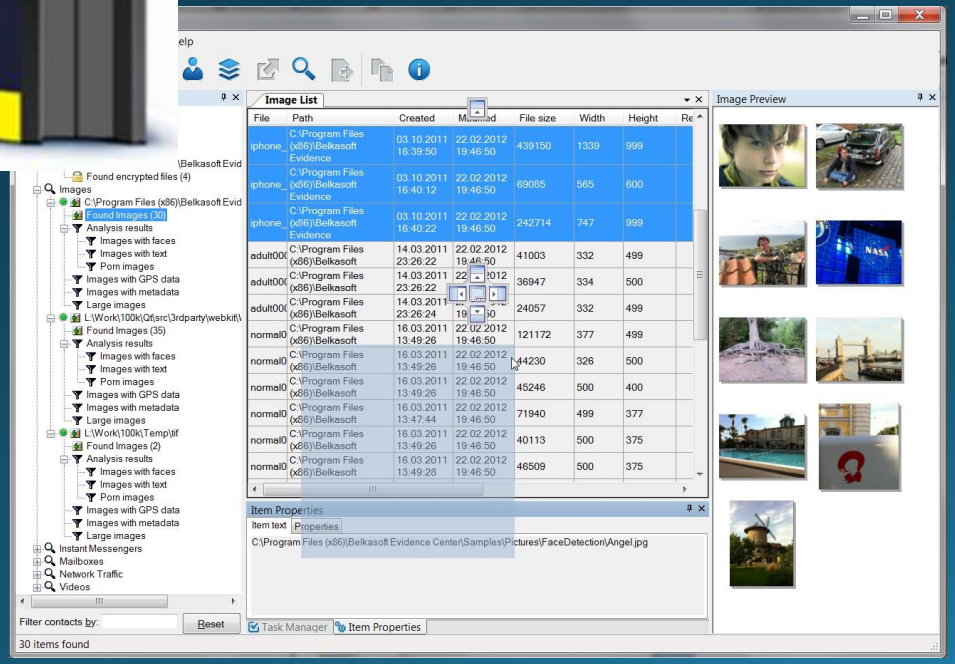
EnCase ® Forensic





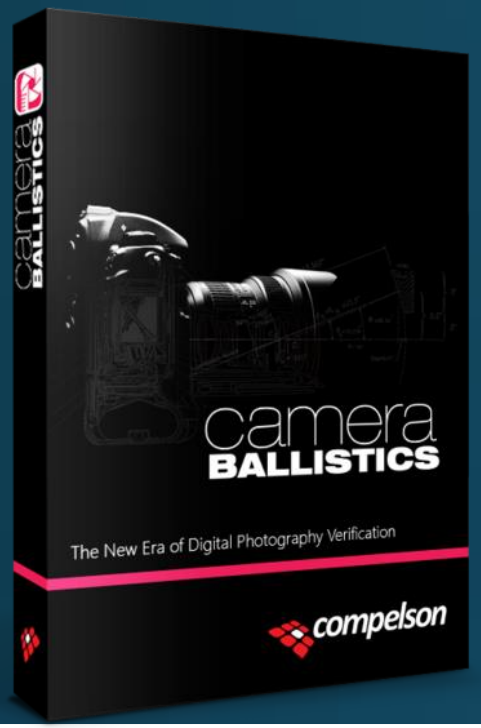
Программная платформа для проведения расследования киберинцидентов. Осуществляет расширенный анализ информации с криминалистической точностью, дешифрует и взламывает пароли. Программа FTK создана для проведения быстрого анализа данных с возможностью масштабирования для использования в больших компаниях.

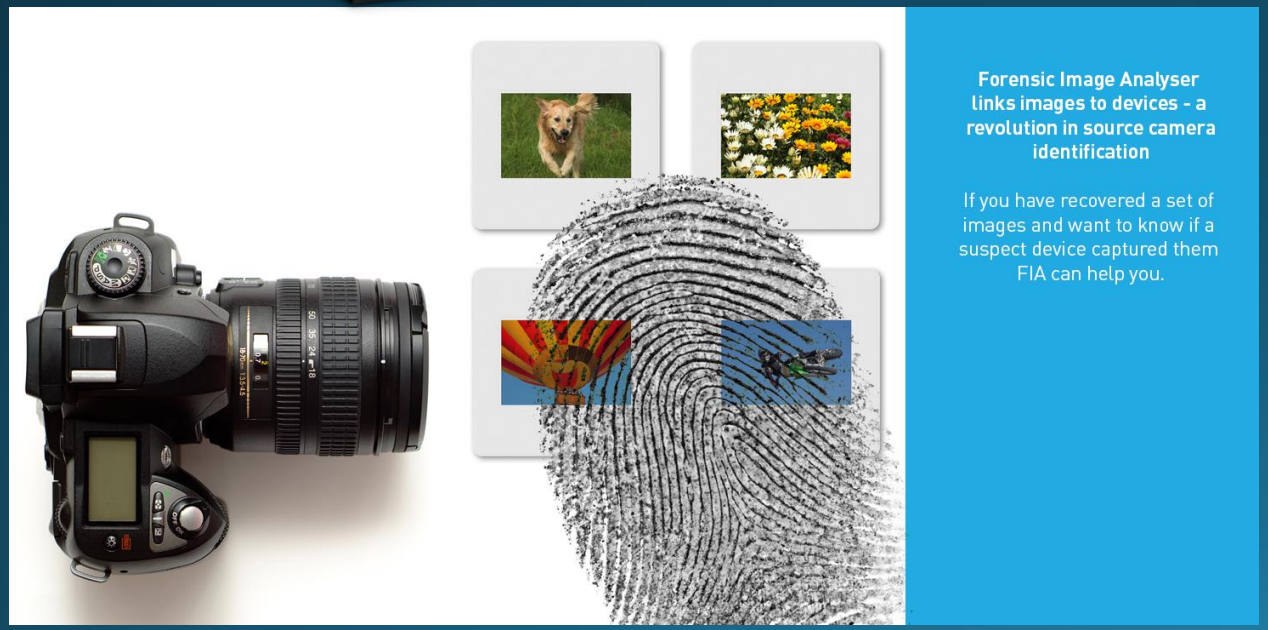
Belkasoft Evidence Center



Программа облегчает получение, поиск, анализ, хранение и передачу цифровых улик, находящихся внутри компьютеров и мобильных устройств. Программа быстро извлечет цифровые улики из различных источников путем анализа жестких дисков, образов, облачных приложений, содержимого рабочей памяти, резервных копий iOS, Blackberry и Android, UFED, JTAG и chip-off дампов. Evidence Center автоматически проанализирует источник данных и представит наиболее значительные улики для обзора, подробного изучения или включения в отчет.

Camera Ballistics





Программа выявляет аномалии в каждом изображении и использует эту информацию для создания описания сенсора устройства. Сенсор является частью каждой цифровой камеры, собирая свет в миллионы пикселей и преобразуя его в изображение. Из-за различий в размерах и материале, каждый пиксель может вести себя по-разному, делая каждый датчик уникальным. Это верно даже между устройствами той же марки и модели. Именно эти различия, генерируемые сенсором, позволяют создать неповторимый отпечаток и связать его с конкретной камерой.

Спасибо за внимание.