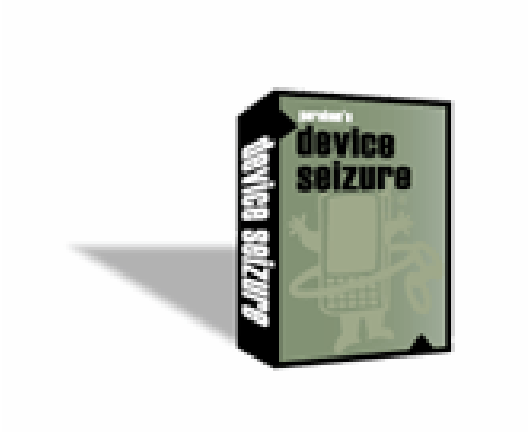
Device Seizure



Цифровая экспертиза, с эволюцией программы Device Seizure, совершила гигантский шаг вперед. Объединив технологии PDA Seizure & Cell Seizure, фирма Paraben предоставила исследователям мощный инструмент экспертизы портативных устройств. В отличие от программ обработки данных, используемых в судебных исследованиях, Device Seizure имеет свои корни в цифровой экспертизе, базируясь на: PDD (Palm DD для командной строки); восстановлении удаленных данных; обеспечивая полное сохранение данных для определенных моделей сотовых телефонов; осуществляя дублирование данных на логическом или физическом уровне; дублирование данных из КПК; доступ к данным, передаваемым по дата-кабелю; расширенной генерацией отчетов; организацией доступа к телефону через инфракрасный порт и Blootooth. Ваш инструментарий не будет полон без Device Seizure, которая поддерживает Symbian 6.0, а также, большинство устройств на других платформах.

В чем отличие между Device Seizure и другими коммерческими или бесплатными продуктами для просмотра данных сотового телефона?

Большинство коммерческих и бесплатных программ разработаны только для просмотра информации в исследуемых устройствах и не предназначены для загрузки данных из них. Это - небезопасный путь для проведения судебного исследования. Фактически все программы, представленные на рынке и маркируемые как программы для судебных исследований, предупреждают о возможности потери данных. Device Seizure не позволяет изменять данные в исследуемом устройстве. Фирма Paraben также может быстро добавить поддержку для неподдерживаемых ранее (новых) моделей сотовых телефонов через службу поддержки пользователей. Сложив все это вместе, мы не сможем найти программу лучше для экспертного перехвата, анализа и составления отчетов для портативных устройств.

Фирма Paraben, в отличие от других компаний, делает упор на физический уровень дублирования данных, предлагая, в основном, физическое дублирование памяти устройства. Логическое дублирование данных из устройства не позволяет захватить данных больше, чем позволено стандартом операционной системы. Уникальный модуль физического дублирования от Paraben позволяет «фотографировать» память большинства устройств, поддерживаемых Device Seizure. Чтобы прочитать подробнее о логическом и физическом дублировании данных для моделей конкретных производителей перейдите по ссылке http://www.paraben-forensics.com/cell_models.html.

- Nokia (GSM and TDMA логические модули) http://www.paraben-forensics.com/cell_models.html#nokia

- LG (LG CDMA and LG GSM логические модули) http://www.paraben-forensics.com/cell_models.html#lg
- Sony-Ericsson (логический модуль) http://www.paraben-forensics.com/cell_models.html#sony
- Motorola (логический и физический модули) http://www.paraben-forensics.com/cell_models.html#motorola
- Siemens (логический и физический модули) http://www.paraben-forensics.com/cell_models.html#siemens
- Samsung (CDMA логический, GSM логический, GSM физический модули) http://www.paraben-forensics.com/cell_models.html#samsung
- Symbian (Psion логический модуль для 16/32 битных устройств) http://www.paraben-forensics.com/cell_models.html#symbian
- GSM SIM Cards (логический модуль) http://www.paraben-forensics.com/cell_models.html#sim

Device Seizure от Paraben поддерживает SIM - карты стандарта GSM, благодаря SIM картридеру, который входит в состав комплекта Device Seizure Toolbox. Device Seizure поддерживает следующие операционные системы:

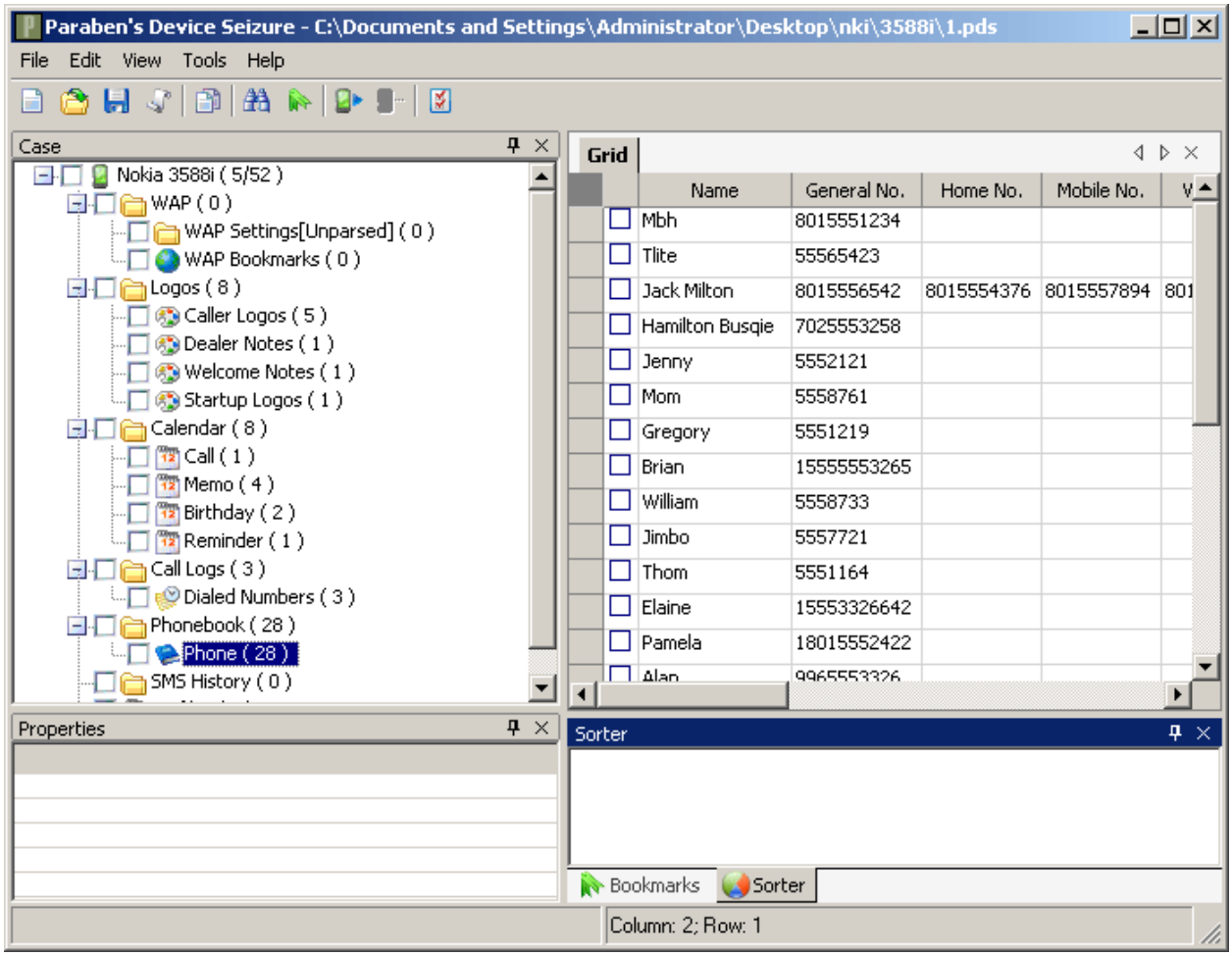
- Palm до 5.4
- Windows CE/Pocket PC/Mobile 5.0 и ранние
- BlackBerry 4.x и ранние
- Symbian 6.0
- EPOC 16/32 (Psion устройства)

ОСНОВНЫЕ ОСОБЕННОСТИ:

- Полнофункциональный, простой в использовании интерфейс
- Поддержка USB и последовательных портов
- Всесторонний доступ к данным: текстовые сообщения, адресные книги, списки вызовов и пр.
- Восстановление удаленных данных
- Проверка целостности файлов с использованием хешей MD5 и SHA1
- Встроенная программа просмотра для основных типов файлов
- Многоязычная поддержка (Unicode) для таких языков, как арабский, русский, китайский и т.д.
- Встроенный поиск и система закладок
- Возможность просмотра данных в текстовом и шестнадцатеричном формате
- Анализ файлов данных КПК, сохраненных в компьютере исследователя
- Встроенное восстановление пароля для Palm (до Palm OS 4.0)
- Программа просмотра реестра Windows CE
- Дублирование доступной информации из GSM SIM карт, включая удаленные данные
- Полное дублирование флэш-памяти для отдельных моделей сотовых телефонов
- Просмотр графической информации, включая форматы мультимедийных файлов, характерных для большинства исследуемых устройств
- Составление подробного отчета в формате HTML
- Шифрование получаемых образов памяти исследуемых устройств гарантирует целостность клонированных данных от преднамеренного изменения
- Текстовый (включая Unicode) и шестнадцатеричный поиск в экспортированных данных
- Экспорт данных в компьютер

- Просмотр экспортированных данных внешними программами просмотра
- Импорт баз данных, клонированных с помощью PDA Seizure, Cell Seizure и SIM Card Seizure
- Сравнение двух баз данных для проверки различий в их структуре
- В стоимость включена 60- ти дневная подписка на получение обновлений программы
- Чтобы прочитать больше информации о Device Seizure и поддерживаемых моделях телефонов перейдите по ссылке http://www.paraben-forensics.com/cell_models.html .

Ограничения демоверсии: 30 дней или 23 запуска, 30 Мб экспортируемых данных для КПК и одна категория экспортируемых данных для мобильного телефона.



Главное окно программы Paraben's Device Seizure.

Помогите Paraben совершенствовать службу поддержки

Paraben постоянно добавляет в программу Device Seizure поддержку новых моделей и производителей. Но остаются еще сотни моделей, поэтому мы нуждаемся в Вашей помощи. Мы не можем получить и протестировать каждый сотовый телефон или КПК. Мы можем бесплатно установить Вам программу в обмен на безвозмездное предоставление нам Вашего телефона. Мы даже подарим Вам фирменную футболку от Paraben в знак нашей благодарности.

Источник: www.paraben-forensics.com

Перевод:
Капинус О.В. (info@computer-forensics-lab.org)
Михайлов И.Ю. (info@computer-forensics-lab.org)
Кузнецов С.М.