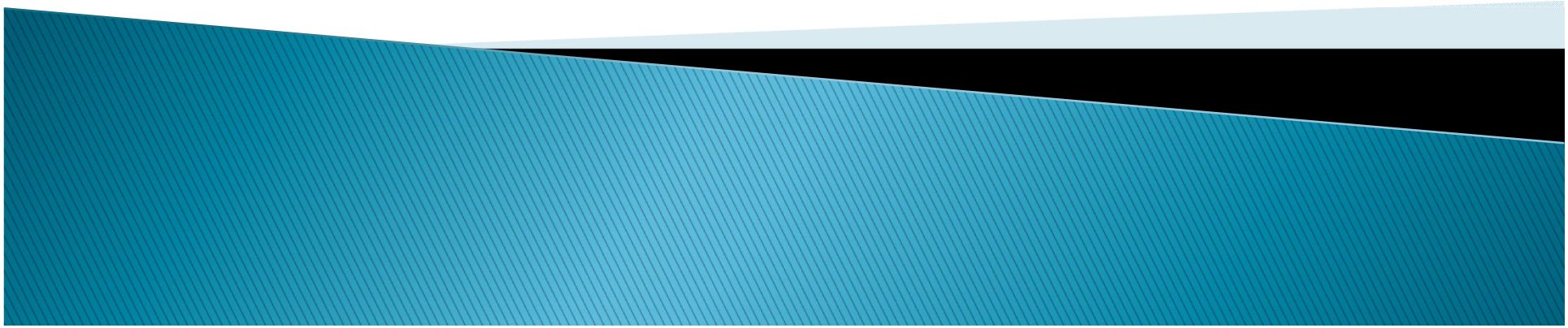
Password Recovery and Forensic Software

Алгоритмические и инженерные аспекты анализа защищенных данных

Алексей Чиликов

Апрель 2010

Конференция РусКрипто’2010



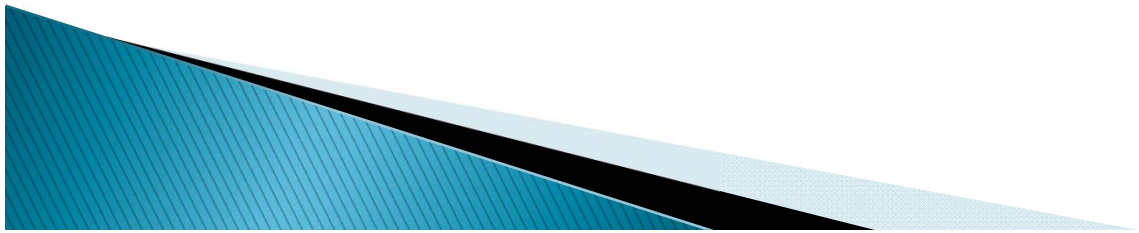
Коротко о нас

- Passware
  - На рынке с 1998 года
  - Отделения в США и России

- Passware Kit Forensic
  - Восстановление данных для 180+ типов файлов
  - Быстрый поиск защищённых объектов на компьютере
  - Поддержка аппаратного ускорения (Tableau TACC, GPU) для восстановления паролей/ключей
  - Переносимая версия для работы на месте инцидента
  - Анализ данных в памяти

Обзор

- Парольная защита и шифрование
  - Типы защиты
  - История вопроса
- Как работать с защищёнными данными?
  - Поиск защищённых данных
  - Анализ и снятие защиты



Типы защиты

- Сохранённые пароли
  - Internet-браузеры, email-аккаунты, etc.
- Защита файлов
  - Пароли
- Защита дисков
  - Full Disk Encryption (FDE)
    - Software
      - BitLocker
      - PGP
      - TrueCrypt
    - Hardware

Немного истории

- Увеличение стойкости шифрования
  - Microsoft Office
    - До Office 97 – мгновенное восстановление пароля
    - Office 97–2003 – 40bit encryption – гарантированное расшифрование (Passware Decryptum, 2003)
    - Office 2007 – AES
  - ZIP
    - 96-битное шифрование – plaintext attack ([Biham, Kocher, 1991])
    - AES

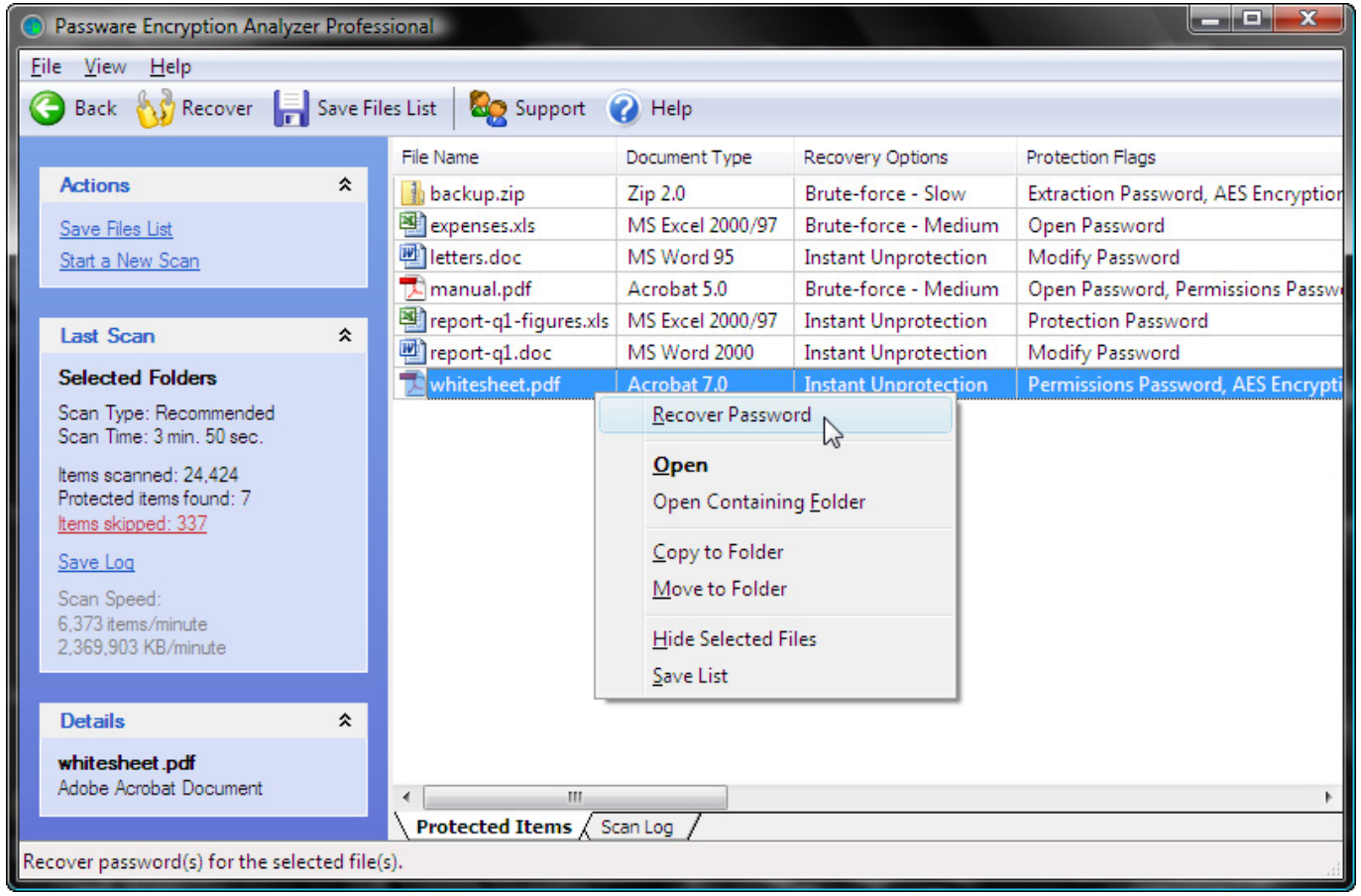
Passware

Что сейчас?

- Почти нет «доморощенных» алгоритмов
- Используются проверенные стандарты шифрования
- Ключ – не пароль, а хэш (SHA-1, etc)
- «Усиление ключа» через многократное хэширование. Не имеет значение при проверке одного пароля, но существенно усложняет перебор
- Office 2007, WinZip – используют SHA-1/AES
- Высокая стойкость!

Поиск защищённых данных

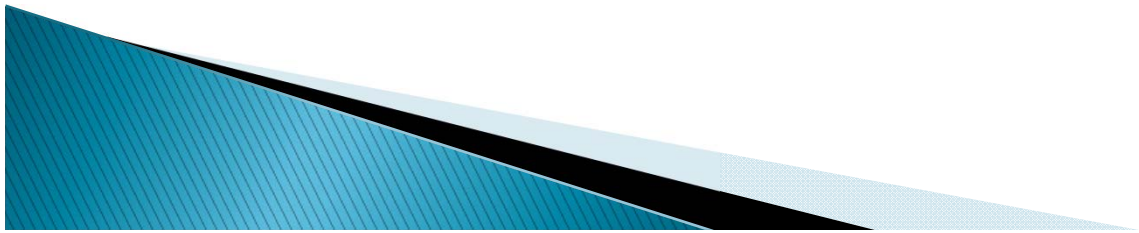
Passware Encryption Analyzer



Поиск защищённых данных

Passware Encryption Analyzer

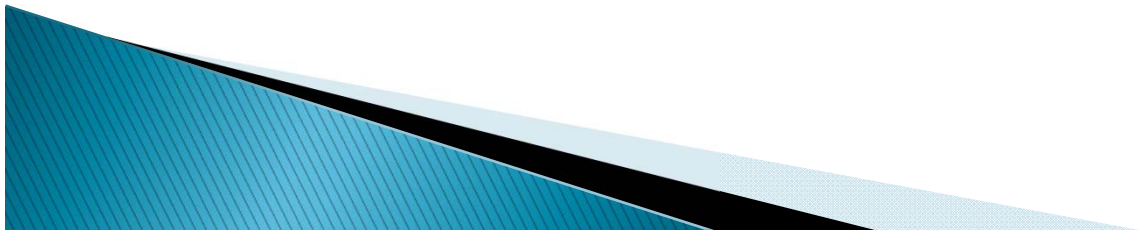
- Скорость – более 4000 файлов в минуту
- Поддержка более 180 типов файлов
- Есть бесплатная версия
- Выход: Список защищённых объектов, с оценками ресурсоёмкости атаки



Снятие защиты

Методы:

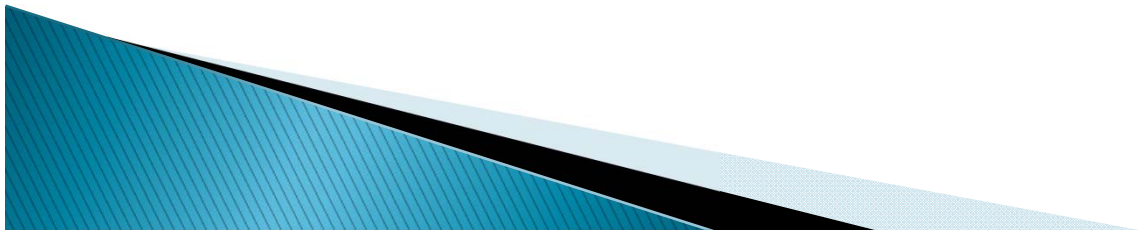
- Атака на пароль
- Использование физического доступа
- Сбор информации во время работы



Снятие защиты

Для успешной атаки на пароль нужно найти слабейшее звено.

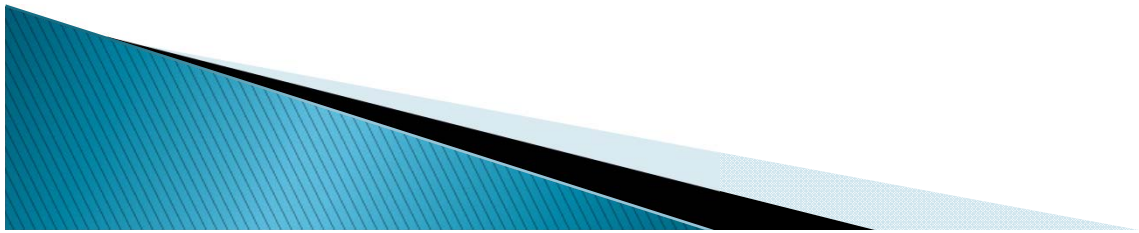
- Часто используются одинаковые (или похожие) пароли
- Разные объекты защищены с различной степенью стойкости



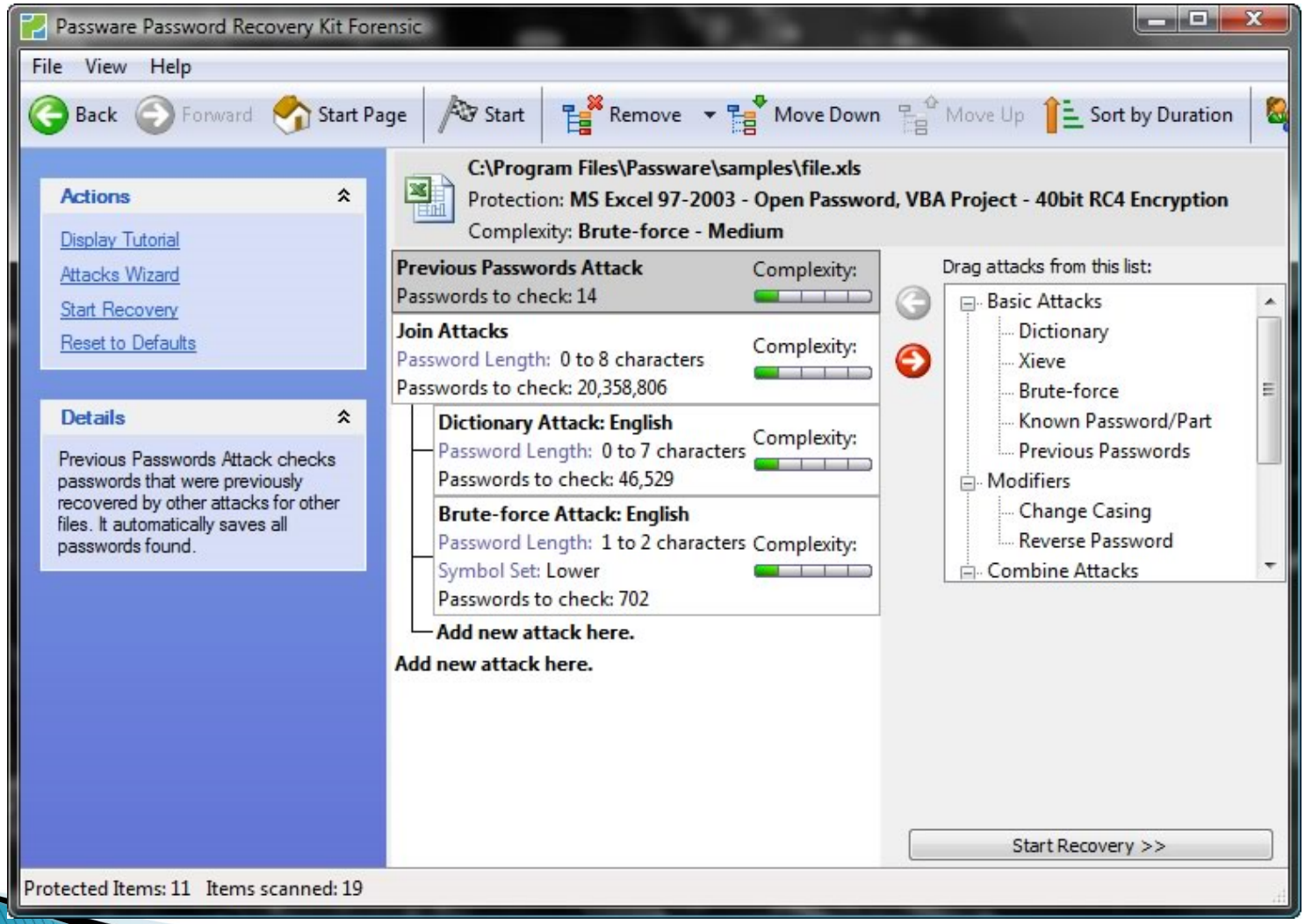
Увеличьте шансы

Поиск слабого звена:

- Начните с «лёгких» типов файлов
- Используйте ранее найденные пароли
- Используйте хороший словарь
- Сконструируйте подходящие шаблоны для поиска пароля



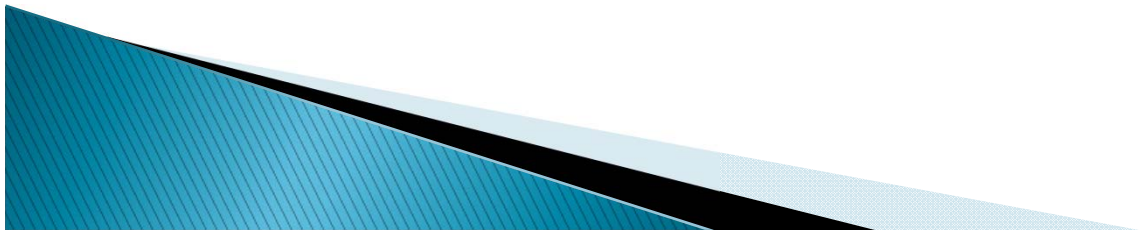
Атаки на пароль



Passware

Экономьте время

- Многоядерные CPU
- Распределённые вычисления
- Вычисления на GPU – >20x
- Аппаратное ускорение (FPGA) – >25x

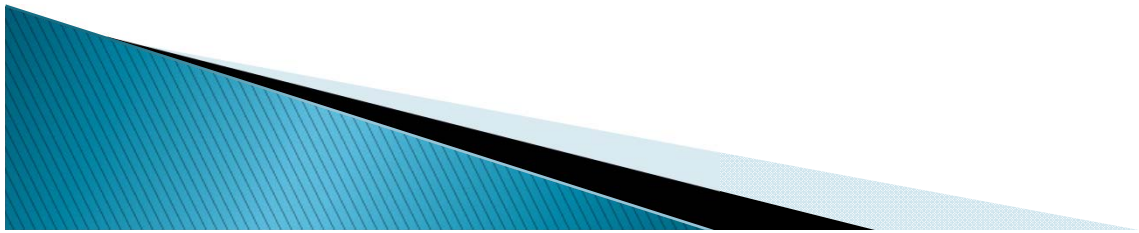


Используйте физический доступ

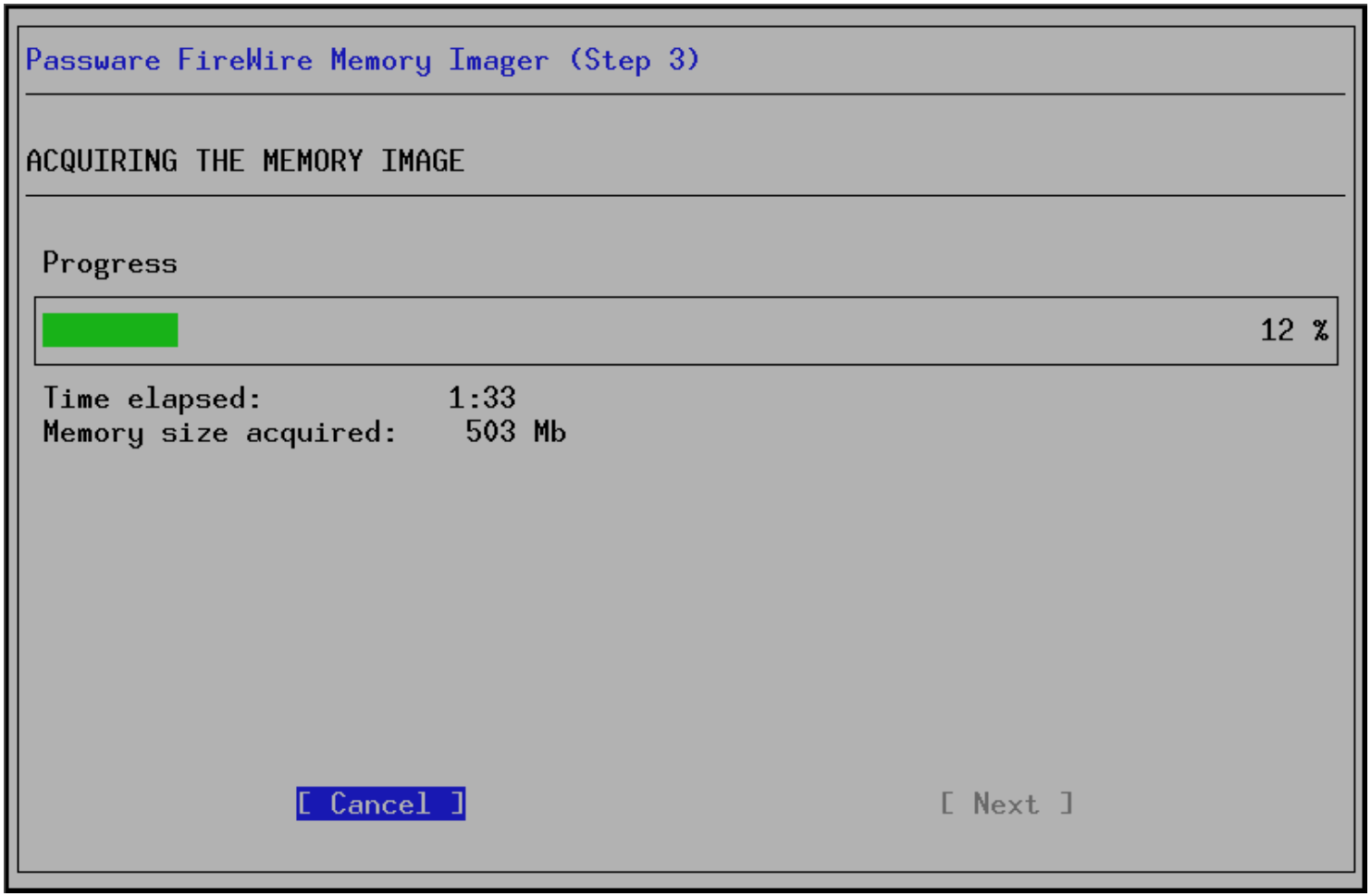
- Сохранение состояния – не выключайте компьютер!
- Ключи шифрования сохраняются в памяти
  - BitLocker
  - TrueCrypt
  - etc
- Прямой доступ к RAM

Доступ к памяти

- Предустановленный драйвер
  - Широкий выбор инструментов
- FireWire + DMA
  - Passware FireWire Memory Imager
- ColdBoot
  - [D. MacIver, 2006]

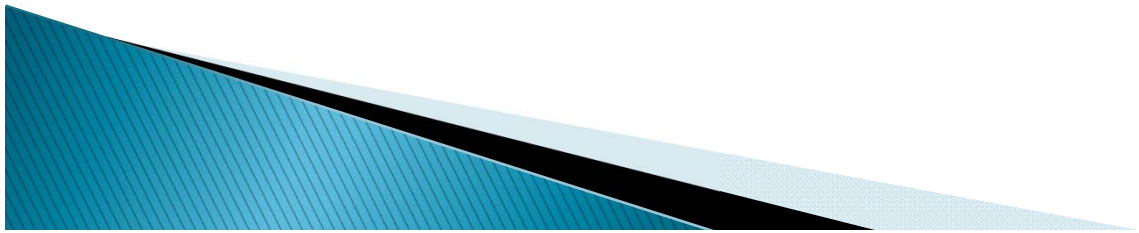


Passware FireWire Memory Imager



Анализ RAM

- Поиск возможных ключей
  - Энтропийные тесты
  - Формат структур данных
  - Избыточность
  - Точная проверка
- Получение доступа к данным
  - Восстановление оригинального пароля/ключа
  - Непосредственное расшифрование
- Выход: Открытые данные, доступные для анализа



Выводы

- Найдите слабое звено
- Экономьте время
- Используйте физический доступ
- Воспользуйтесь эффективным инструментом

Вопросы?

- chilikov@lostpassword.com
- http://www.lostpassword.com