



# Создание образов Windows XP Embedded для загрузки с CompactFlash

Станислав Павлов  
Системный аналитик  
Кварта Технологии



# Содержание

- **Обзор**
- **Дизайн**
  - **Enhanced Write Filter**
  - **Выбор подходящей файловой системы**
    - **Disable Last Access Time Stamp**
  - **Отключение дефрагментации диска**
  - **Disable System Restore**
  - **Перенаправление временных файлов на незащищенный том**
  - **Перенаправление файлов Event Log на незащищенный том**
  - **Изменение расположения файла подкачки**
- **Обслуживание**

# Обзор

## ■ За

- Устойчив к промышленным температурам (от  $-40^{\circ}\text{C}$  до  $80^{\circ}\text{C}$ )
- Стандартный интерфейс

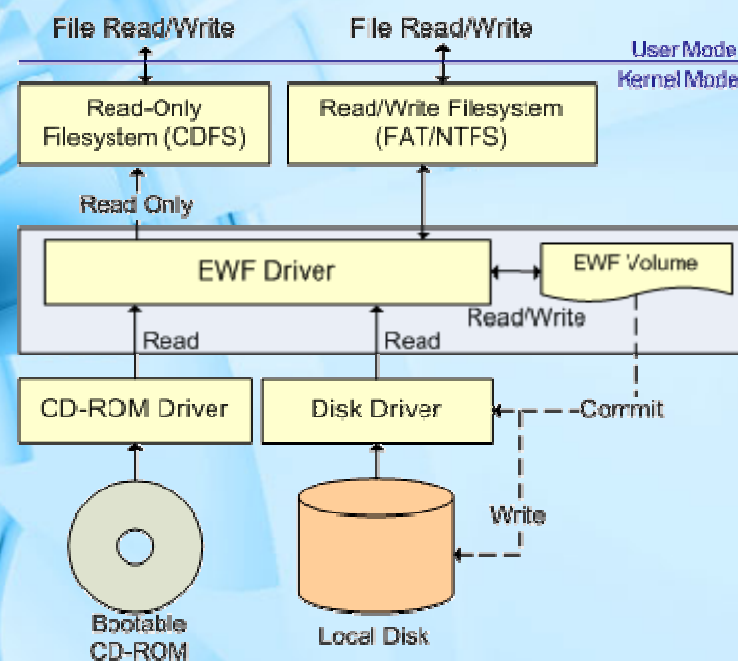
## ■ Против

- Большая скорость изнашивания, чем у жесткого диска
  - 200,000 циклов стирания
- Трудности с разбивкой на разделы
- Помечены “Removable”

# Дизайн

## Enhanced Write Filter - Обзор

- Верхний фильтр в стеке тома
- Защита от записи одной или более разделов
- Позволяет загружать XPc с устройств только для чтения
- Перенаправляет запись в оверлей
- Поддерживает три типа оверлея
  - Disk, RAM и RAM Registry



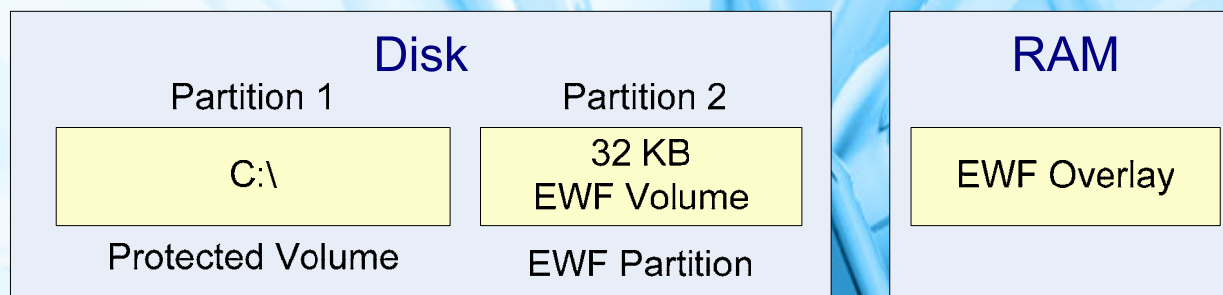
# Дизайн

## Enhanced Write Filter – Развертывание

- **Разбиение диска на разделы**
  - Том EWF считается разделом
  - Необходимо место на диске для создания тома EWF
    - Сразу же за первичным разделом
    - Внутри расширенного раздела
  - Минимум 32К - 8МВ рекомендуется
- **Не более трех первичных разделов**
- **EWF не установится, если том EWF уже присутствует**
- **Полезные утилиты:**
  - Windows PE с diskpart, Bootprep для FAT, Etprep для Bootable CD-ROM

# Дизайн

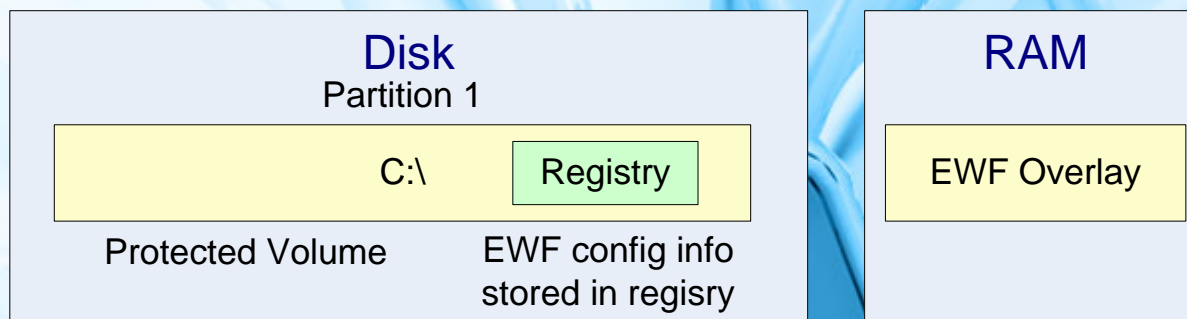
## Enhanced Write Filter - RAM



- Требуется второй раздел (тип 45) для "тома EWF"
  - Мастер-таблица томов
  - Стек оверлея
- "Том EWF" создается в процессе FBA
  - Сразу же за первичным разделом
  - На свободном месте расширенного раздела
- Поддерживается только один оверлей – RAM
  - Память RAM не выделяется заранее
- Перехват чтения/записи к диску
  - Записи перенаправляются в оверлей RAM
  - Читается из оверлея RAM и/или диска

# Дизайн

## Enhanced Write Filter - RAM Reg



- **Вариант оверлея RAM**
- **Используется, если носитель не может быть разбит на разделы**
  - **CD/DVD ROM**
- **Метаданные тома EWF хранятся в реестре**
- **Поддерживает только один оверлей – RAM**
  - **Память RAM не выделяется заранее**
- **Перехват чтения/записи к диску**
  - **Записи перенаправляются в оверлей RAM**
  - **Читается из оверлея RAM и/или диска**
- **Невозможно отключит EWF без сохранения оверлея на раздел (commit)**

# Дизайн

## Выбор подходящей файловой системы

- **Используйте FAT**
  - Минимизирует количество записей на диск
- **Если необходима NTFS, подумайте об использовании сжатия NTFS**
  - Отключите журанлирование времени последнего доступа к файлу NTFS

HKKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem		
Name	Type	Value
NtfsDisableLastAccessUpdate	REG_DWORD	1 (0=disable, 1=enable)

# Дизайн

## Отключите фоновую дефрагментацию диска

- Дефрагментация диска
  - Дефрагментация диска для NTFS
  - Дефрагментация диска для FAT
- Отключите дефрагментацию диска и автоподстройку
  - Background Disk Defragmentation Disable Component

HKEY_LOCAL_MACHINE\Software\Microsoft\Dfrg\BootOptimizeFunction		
Name	Type	Value
Enable	REG_SZ	N (N=disable, Y=enable)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion		
Name	Type	Value
OptimalLayout	REG_DWORD	0 (0=disable, 1=enable)

# Дизайн

## Отключите восстановление системы

- Исключите из конфигурации следующие компоненты
  - System Restore Core
  - System Restore User Interface

# Дизайн

## Перенаправьте временные файлы на незащищенный том

- Перенаправьте временные интернет папки на незащищенный том

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Explorer\User Shell Folders		
Name	Type	Value
Cache	REG_EXPAND_SZ	Path to an unprotected volume

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders		
Name	Type	Value
Cache	REG_EXPAND_SZ	Path to an unprotected volume

- Перенаправьте папки TMP и TEMP на незащищенный том

HKEY_CURRENT_USER\Environment		
Name	Type	Value
TEMP	REG_SZ	Path to an unprotected volume
TMP	REG_SZ	Path to an unprotected volume

# Дизайн

Переместите файлы Event Log на незащищенный том

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Application		
Name	Type	Value
File	REG_EXPAND_SZ	<volume name and path>\AppEvent.evt

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\System		
Name	Type	Value
File	REG_EXPAND_SZ	<volume name and path>\SysEvent.evt

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security		
Name	Type	Value
File	REG_EXPAND_SZ	<volume name and path>\SecEvent.evt

# Конфигурация EWF

Уменьшите кол-во записей на защищенный том

- Измените местоположение файла подкачки

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management		
Name	Type	Value
PagingFiles	REG_MULT_SZ	<path\pagefile.sys minsize maxsize> напр. d:\pagefile.sys 150 500

# Как обслуживать?

- Клиент должен иметь возможность исполнять процесс и/или использовать API
  - Обновление защищенного тома
    - Шаг 1: Отключить EWF
    - Шаг 2: Обновить после перезагрузки
    - Шаг 3: Включить EWF
    - Шаг 4: Перезагрузиться для запуска EWF
  - Обновление для RAM оверлея
    - Шаг 1: Обновить – перенаправится в оверлей RAM
    - Шаг 2: Сбросить оверлей на том (commit)



# Вопросы?

Станислав Павлов  
Системный аналитик  
Кварта Технологии

