Перевод: Михайлов И.Ю.
Капинус О.В.

SMART
(Storage Media Analysis Recovery Toolkit)

Что такое SMART?

SMART – это программное обеспечение, которое было разработано и оптимизировано для автоматизации работы судебных экспертов, специализирующихся на проведении компьютерно-технических экспертиз и сотрудников служб информационной безопасности предприятий.

Технология и методология SMART были созданы с намерением объединения технических, методологических и юридических требований к программному инструменту исследования компьютерных систем.

SMART – более чем программа для автономного использования. Особенности SMART позволяют применять ее в различных приложениях:

1. Решение специализированных, узконаправленных задач.
2. Локальный или удаленный просмотр исследуемой компьютерной системы.
3. Исследование поврежденной компьютерной системы.
4. Тестирование и проверка других программных продуктов для экспертного исследования компьютерных систем.
5. Установление соответствия данных, находящихся в файле, его расширению.
6. Определение основных параметров системы.

Кто использует SMART?

SMART в настоящее время используется:

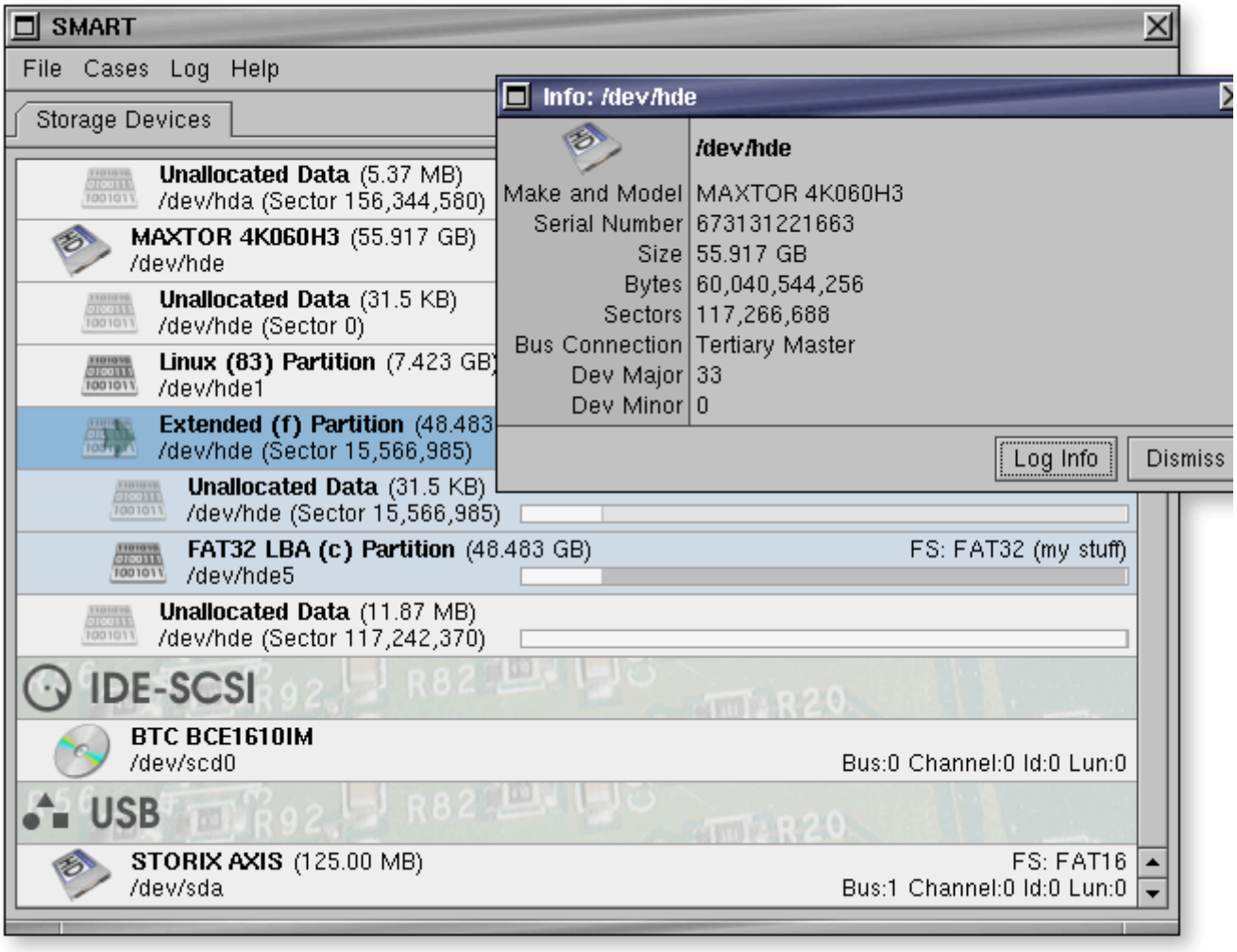
- В государственных и правительственных учреждениях.
- Специализированными подразделениями армии США и правоохранительными органами.
- Фирмами, специализирующимися на исследованиях компьютерных систем.
- Судебными экспертами.
- Частными детективами.
- Специалистами по восстановлению данных.
- Системными администраторами и специалистами в области информационной безопасности.

SMART широко используется правоохранительными органами и крупными корпорациями.

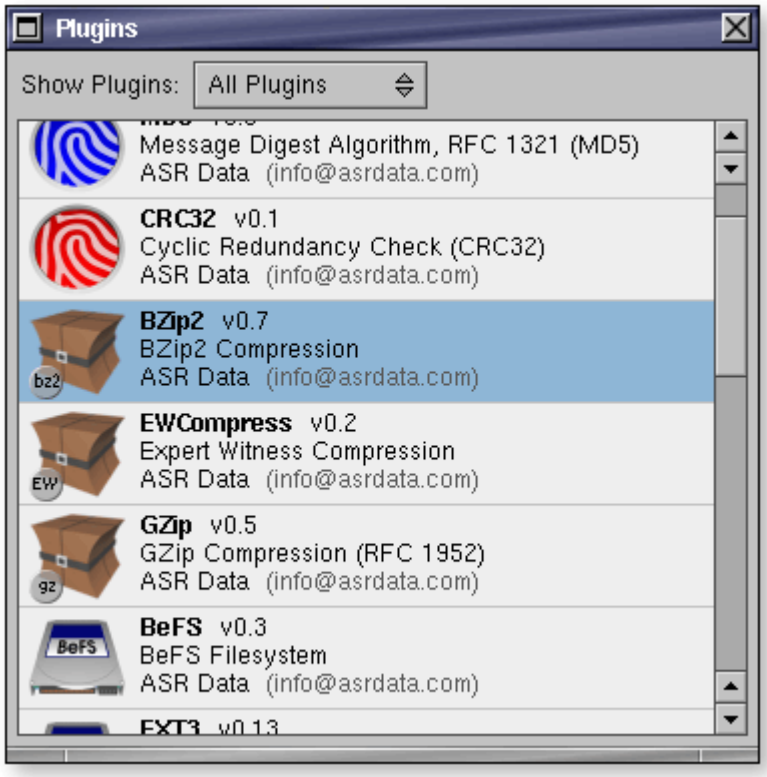
Базовая информация о SMART.

Далее, будут представлены скриншоты, на которых показана работа SMART. Вы увидите, что SMART обладает мощным, интуитивно понятным интерфейсом. Возможности, заложенные в SMART, позволяют назвать ее экспертной системой следующего поколения.

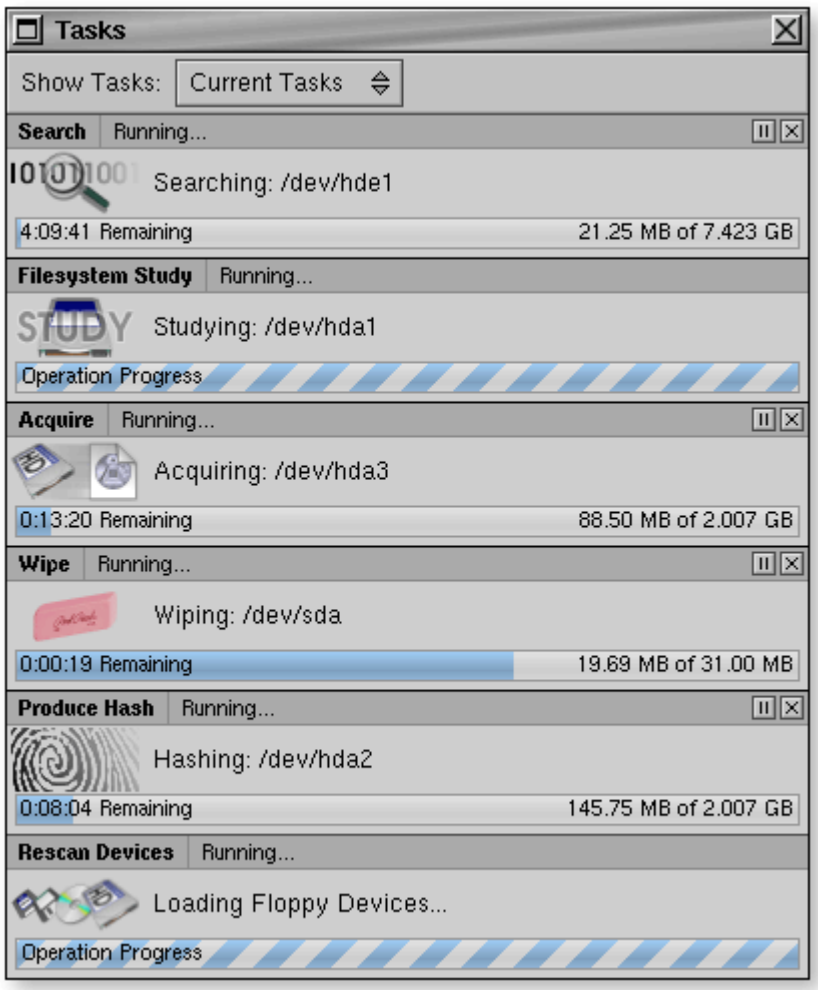
В главном окне программы отображены подключенные накопители. Устройства внесены в список согласно их типу связи с аппаратными средствами компьютера. Все логические диски и неразделенные области внесены в список, как соответствующие подпункты, для устройства, на котором они находятся. Кроме того, в этих же окнах отображается информация о модели устройства, емкости диска, файловой системе. Более подробную информацию можно получить, вызвав информационное окно нажатием правой кнопки манипулятора мышь на выбранном устройстве.


SMART
File Cases Log Help
Storage Devices
Unallocated Data (5.37 MB)
/dev/hda (Sector 156,344,580)
MAXTOR 4K060H3 (55.917 GB)
/dev/hde
Unallocated Data (31.5 KB)
/dev/hde (Sector 0)
Linux (83) Partition (7.423 GB)
/dev/hde1
Extended (f) Partition (48.483
/dev/hde (Sector 15,566,985)
Unallocated Data (31.5 KB)
/dev/hde (Sector 15,566,985)
FAT32 LBA (c) Partition (48.483 GB)
/dev/hde5
FS: FAT32 (my stuff)
Unallocated Data (11.87 MB)
/dev/hde (Sector 117,242,370)
IDE-SCSI
BTC BCE1610IM
/dev/scd0
Bus:0 Channel:0 Id:0 Lun:0
USB
STORIX AXIS (125.00 MB)
/dev/sda
FS: FAT16
Bus:1 Channel:0 Id:0 Lun:0
Info: /dev/hde
/dev/hde
Make and Model MAXTOR 4K060H3
Serial Number 673131221663
Size 55.917 GB
Bytes 60,040,544,256
Sectors 117,266,688
Bus Connection Tertiary Master
Dev Major 33
Dev Minor 0
Log Info
Dismiss

В SMART используются вспомогательные программные модули для выполнения рутинной работы. В целом, программа имеет высокомодульную философию. Это позволяет легко исправлять ошибки, обнаруженные в программе, и не влияет на основные функциональные возможности SMART.



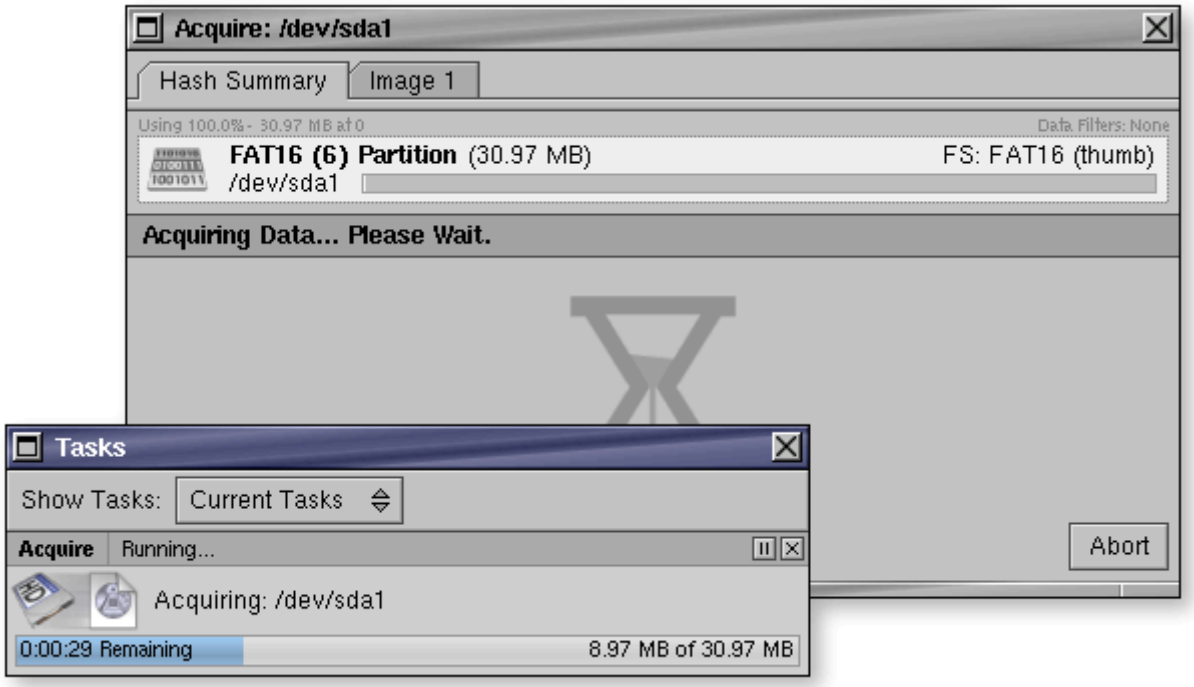
SMART поддерживает многозадачность. Вы можете управлять работой параллельных задач, наиболее эффективно используя аппаратные возможности Вашего компьютера. Вы можете запускать, приостанавливать или прерывать запущенные процессы.



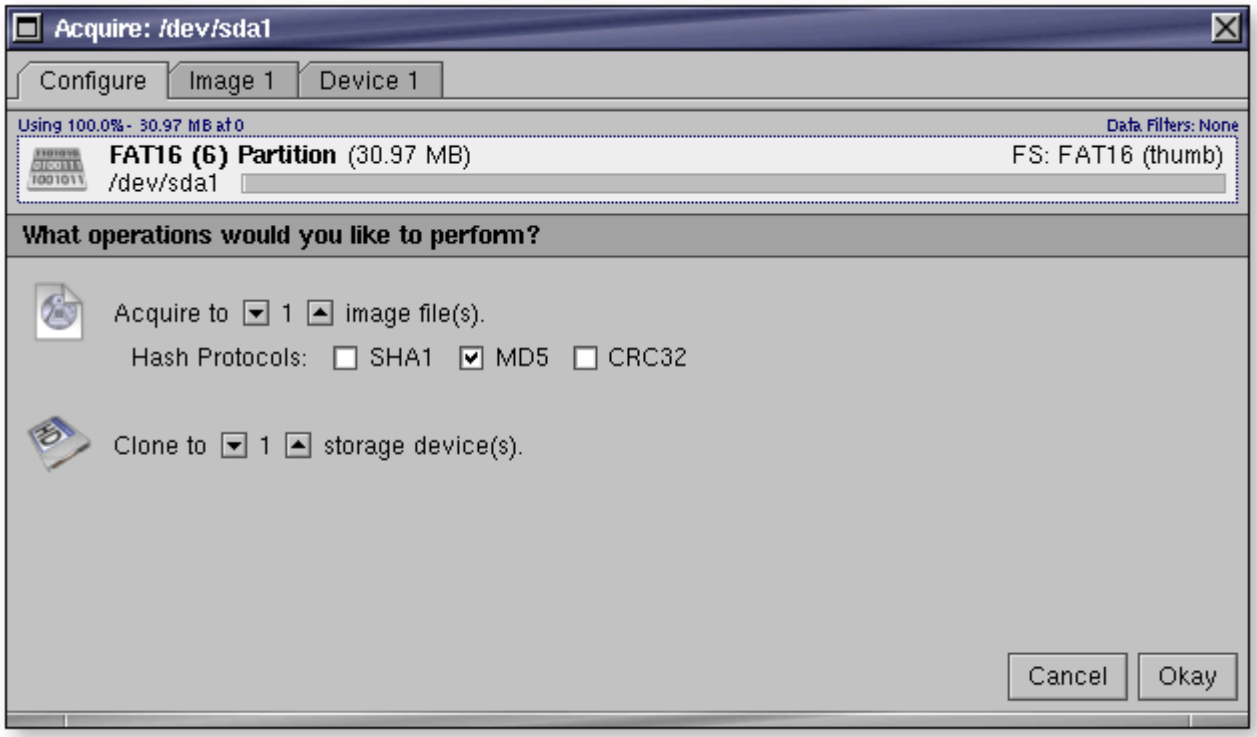
Создание образов исследуемых накопителей в SMART.

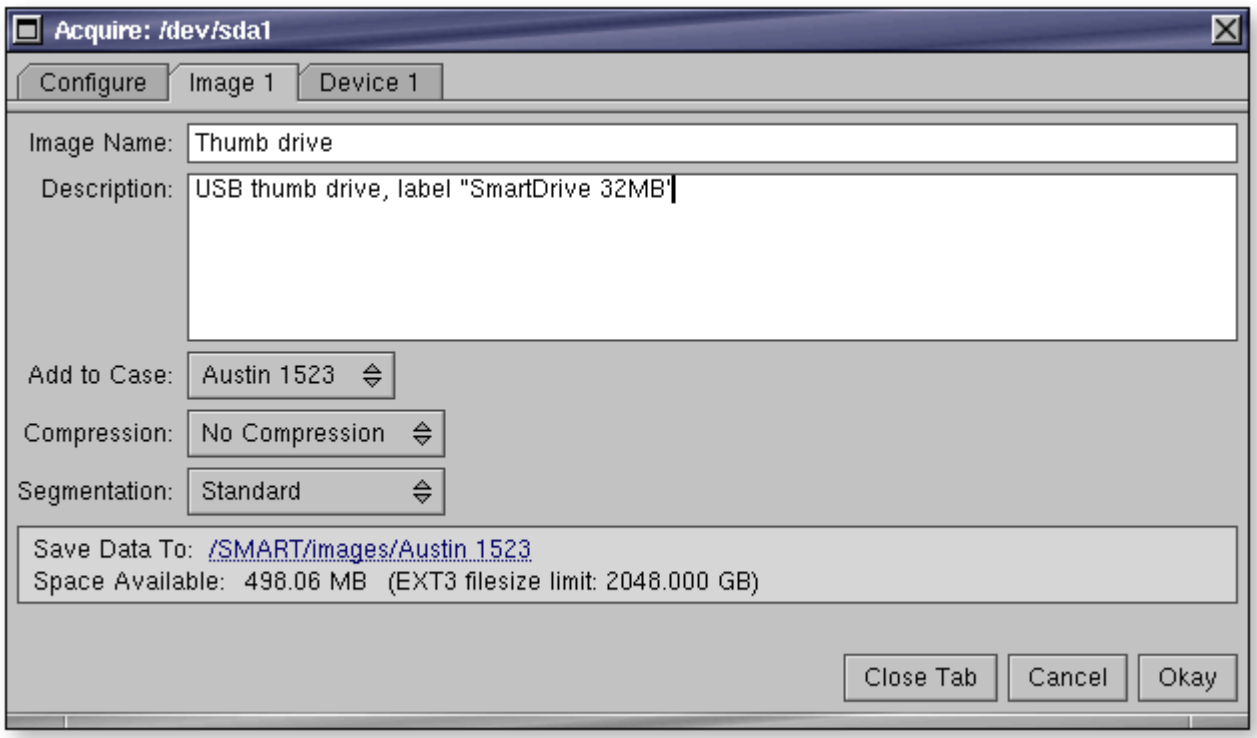
Мощные и гибкие возможности SMART позволяют Вам создавать полные образы исследуемых накопителей или их логических разделов. Поддерживается функция компрессии создаваемого образа. На самом деле, не многие программы, за исключением SMART, способны создавать точную побитовую копию накопителя.

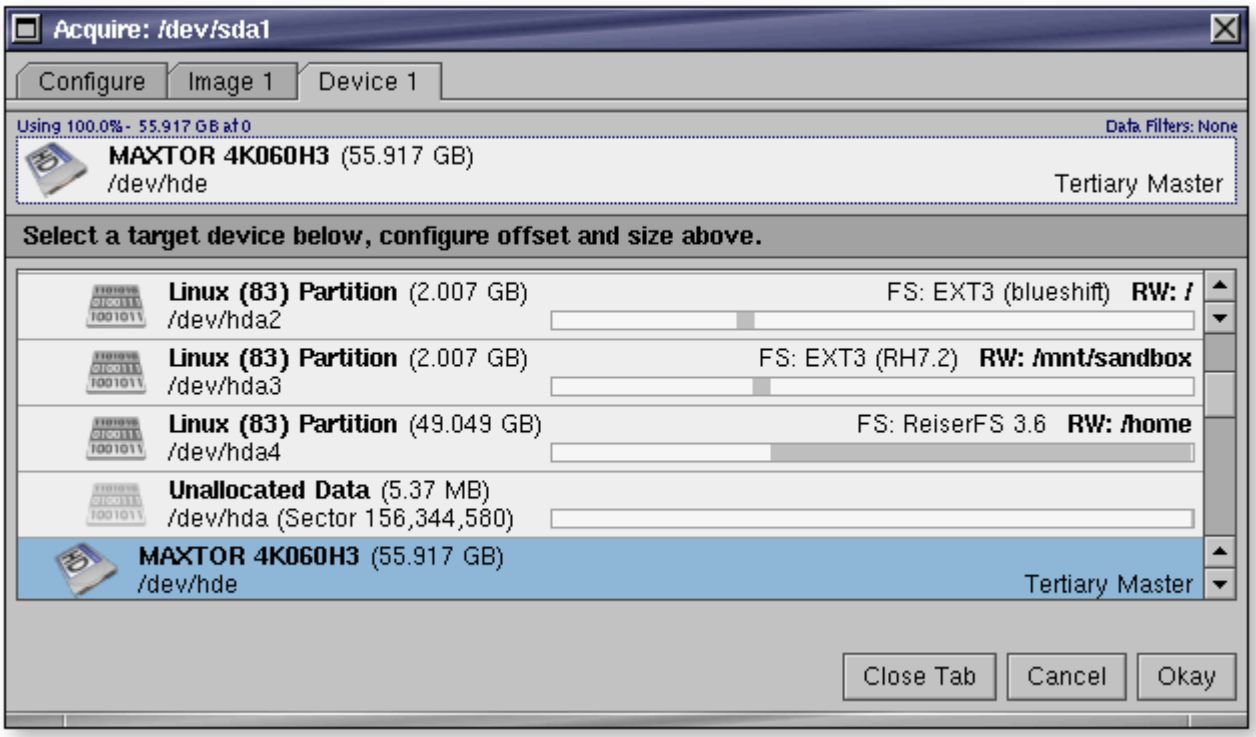
На рисунке, в информационном окне, отображаются все детали процесса создания образа накопителя.



SMART может создавать одновременно несколько копий исследуемого накопителя. Это позволяет создать «эталонную» и «рабочую» копии исследуемого накопителя одновременно. На рисунках показан процесс конфигурирования программы для создания образа устройства /dev/sda/ при его клонировании на жесткий диск.



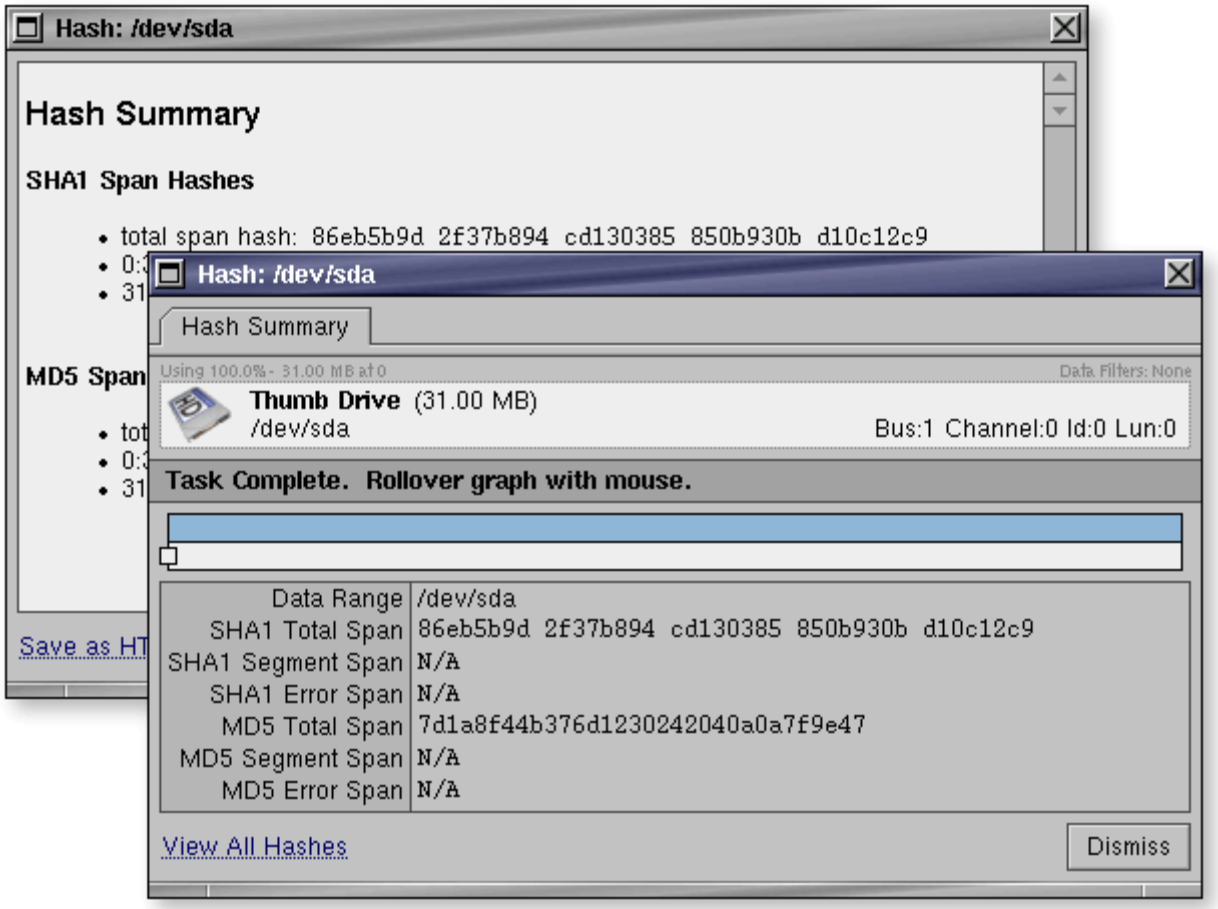



Acquire: /dev/sda1
Configure
Image 1
Device 1
Using 100.0% - 55.917 GB at 0
Data Filters: None
MAXTOR 4K060H3 (55.917 GB)
/dev/hde
Tertiary Master
Select a target device below, configure offset and size above.
Linux (83) Partition (2.007 GB)
/dev/hda2
FS: EXT3 (blueshift) RW: /
Linux (83) Partition (2.007 GB)
/dev/hda3
FS: EXT3 (RH7.2) RW: /mnt/sandbox
Linux (83) Partition (49.049 GB)
/dev/hda4
FS: ReiserFS 3.6 RW: /home
Unallocated Data (5.37 MB)
/dev/hda (Sector 156,344,580)
MAXTOR 4K060H3 (55.917 GB)
/dev/hde
Tertiary Master
Close Tab
Cancel
Okay

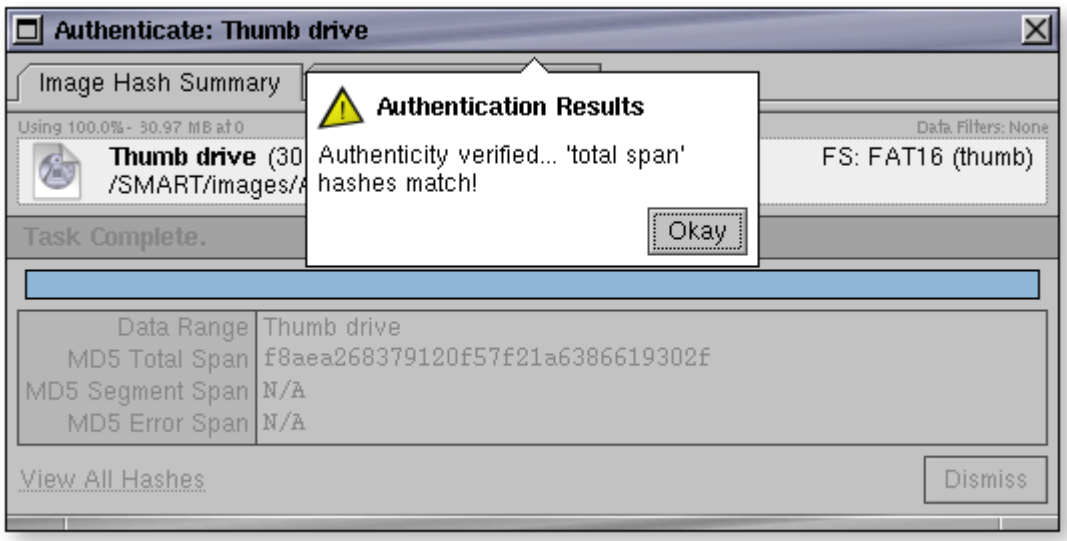
SMART-аутентификация (подтверждение подлинности).

SMART показывает большое количество информации о клонируемом носителе. Отображаются контрольные суммы для всего носителя, его разделов и подразделов, неразделенных областей. Обработка ошибок в SMART, в ходе процесса клонирования носителей и расчета контрольных сумм, более точная и обеспечивает лучшую степень детализации, чем любой другой экспертный инструмент.

Информация о носителе выводится в виде последовательных уровней, визуально отображающих структуру исследуемого носителя.



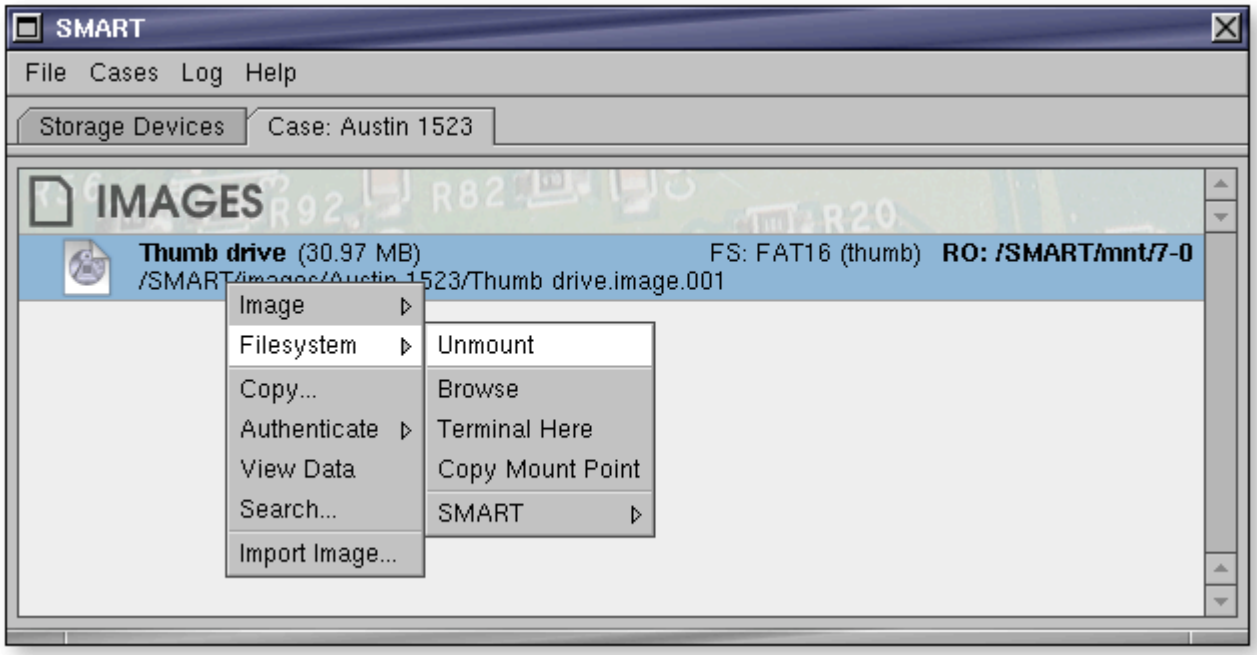
С помощью SMART возможно установить соответствие образа накопителя и его контрольных сумм реальному накопителю.



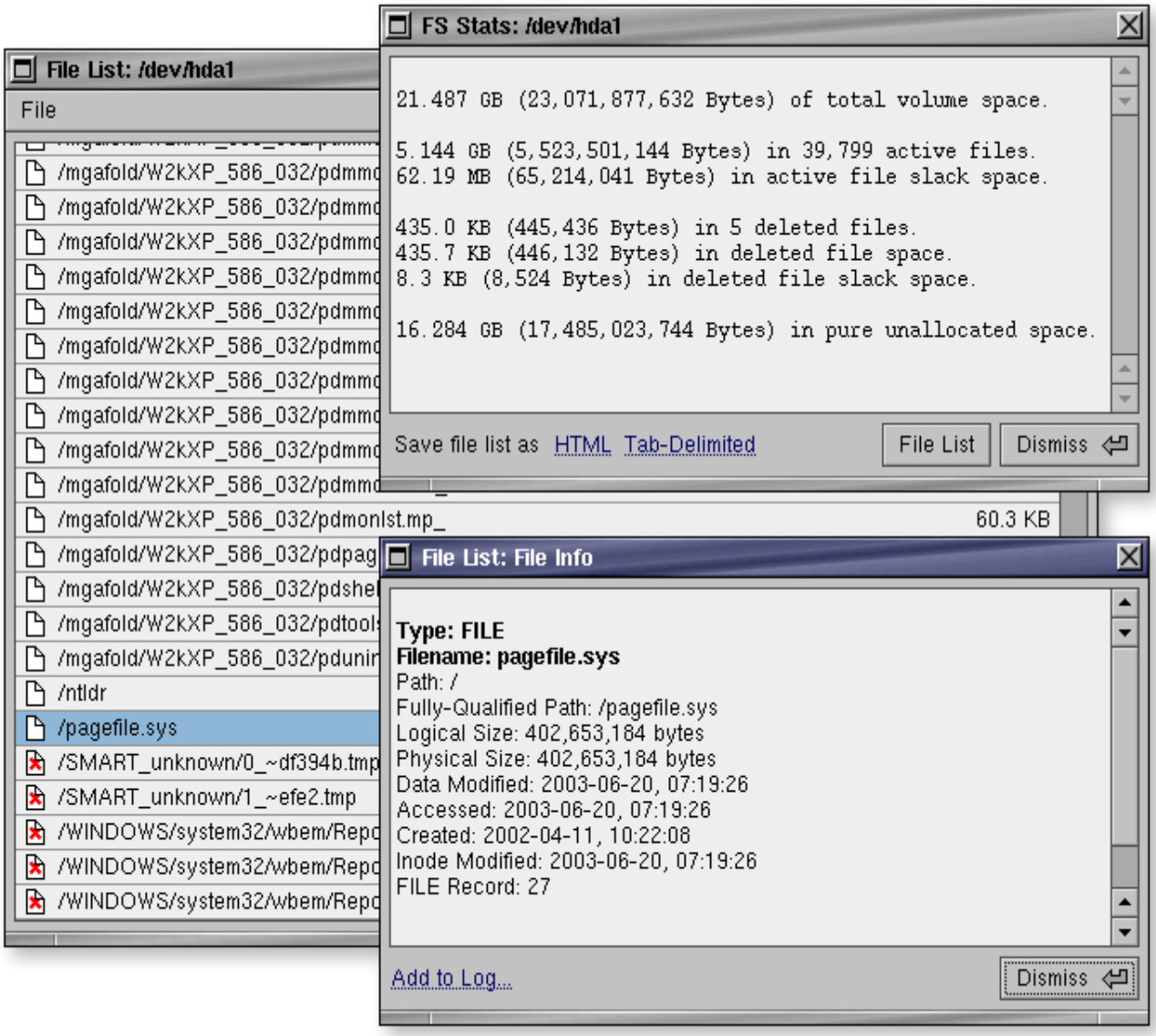
SMART и файловые системы.

SMART функционирует в операционных системах, реализованных на базе Linux/GNI в графических оболочках KDE и GNOME. SMART позволяет безопасно осуществлять предпросмотр данных практически любого типа.

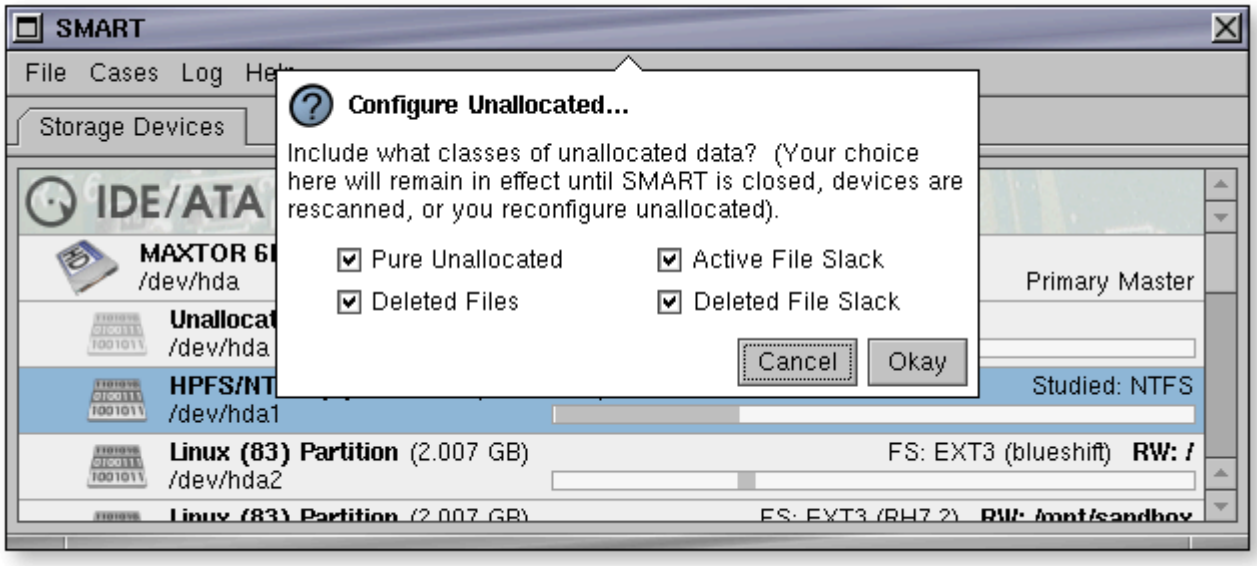
SMART позволяет подключать любые накопители, разделы и образы накопителей. Журналируемые файловые системы подключаются в режиме «только чтение». На момент написания статьи, SMART являлся единственным экспертным инструментом, который не повреждал информацию на носителе при исследовании журналируемой файловой системы. Вы можете легко определить тип файловой системы, содержащейся в подключаемом образе накопителя, даже если образ накопителя сегментирован.



SMART обеспечивает дополнительные возможности при исследовании распространенных файловых систем. При исследовании файловых систем определяются параметры и атрибуты файлов, их расположение на носителе, детектируются служебные области файловой системы, проводится сбор статистической информации и многое другое.

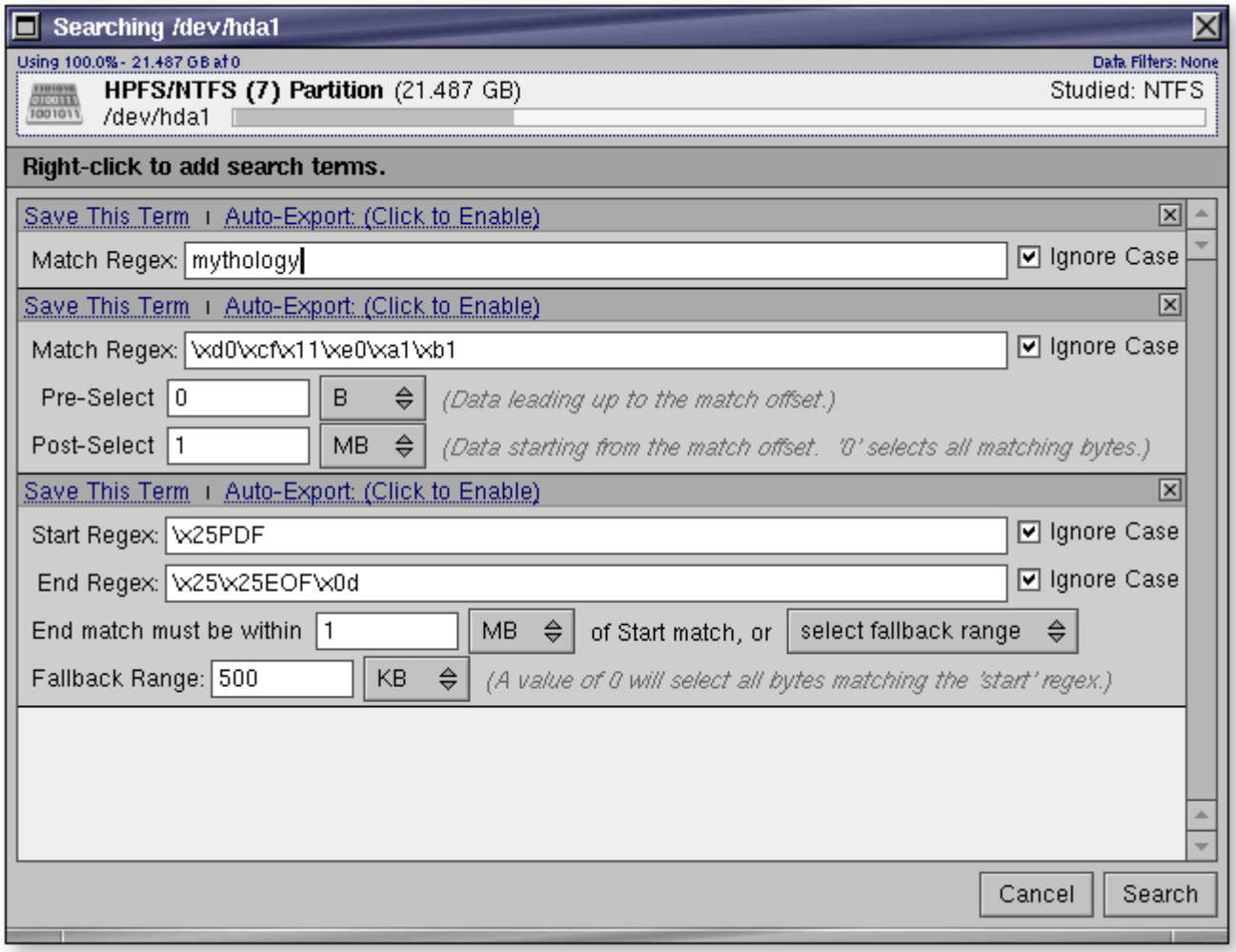


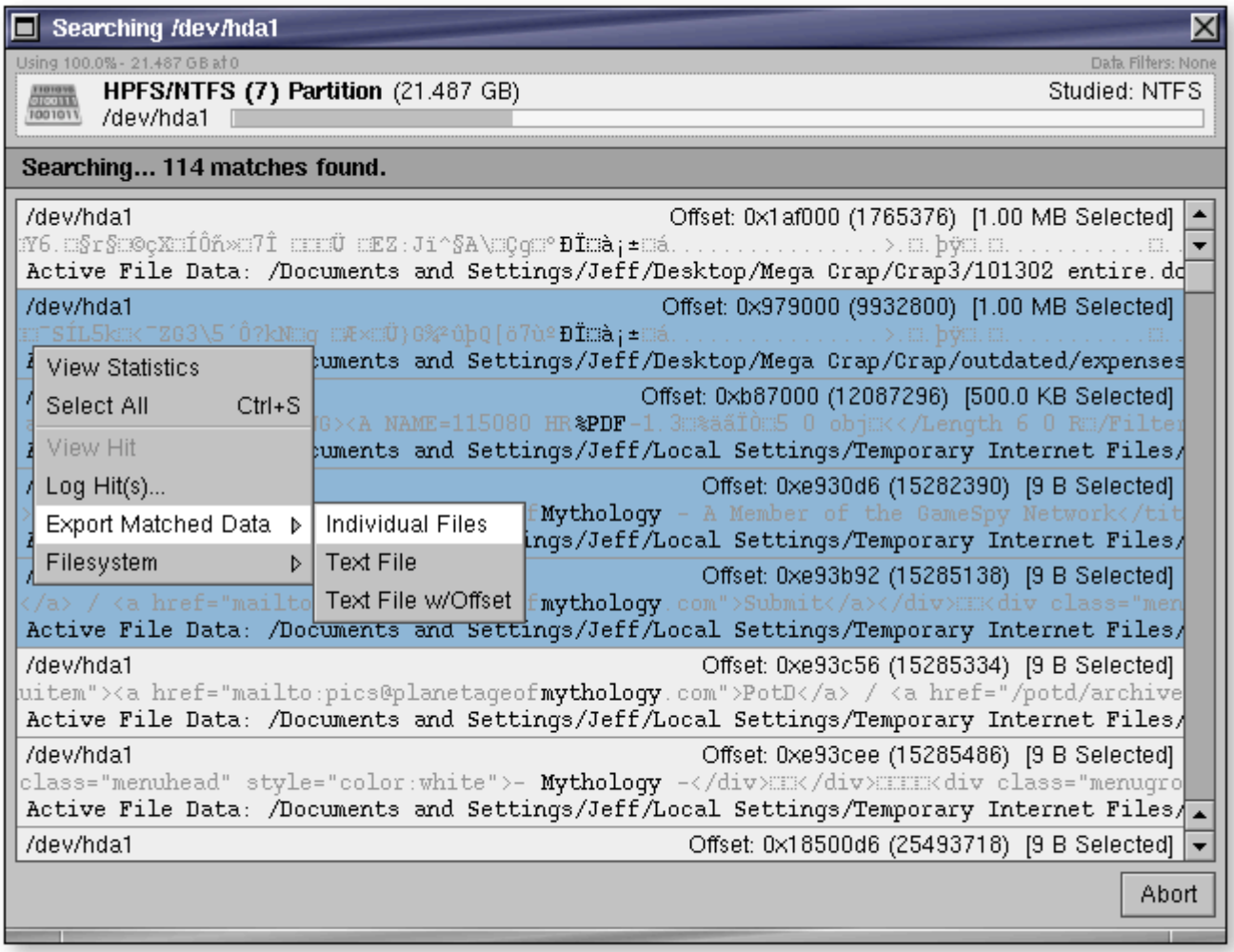
В ходе исследования файловой системы, в зависимости от параметров анализа, проводится исследование данных, находящихся в свободных и неразделенных областях (не отнесенных к определенным логическим разделам) накопителя. Обнаруженные данные сортируются по соответствующим категориям.



Поиск в SMART.

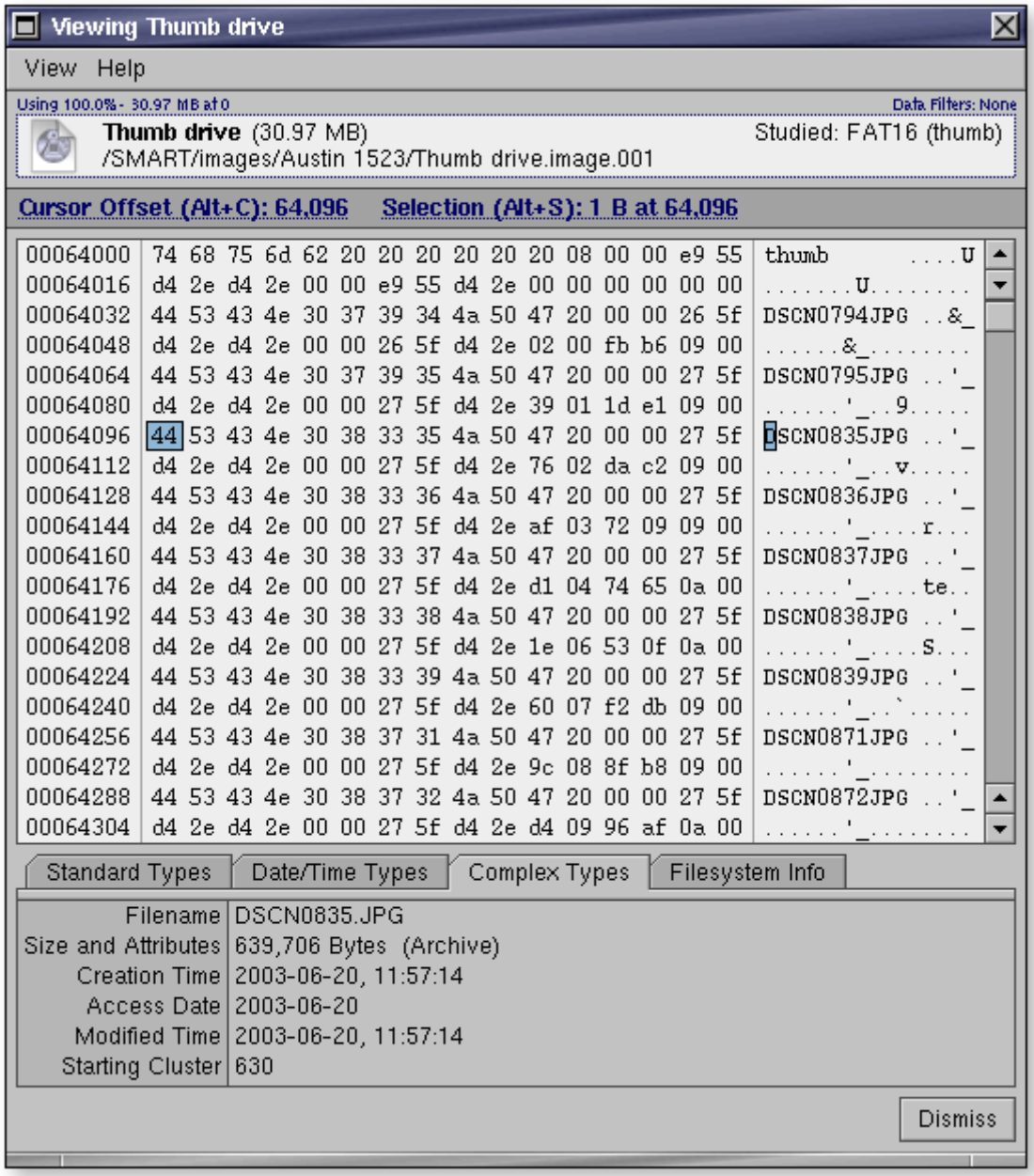
В SMART реализован мощный, гибкий и интуитивно понятный механизм поиска. Большое число настроек позволяет оптимально подобрать его параметры. Встроенный шестнадцатеричный редактор позволяет осуществлять предварительный просмотр обнаруженных данных. С файлами, в которых находятся найденные данные, возможно проведение различных действий. В том числе, они могут быть отсортированы, экспортированы, для них могут быть определены контрольные суммы и т.д. Все действия по поиску файлов могут быть зарегистрированы и использованы в дальнейшем при составлении отчета об исследовании.



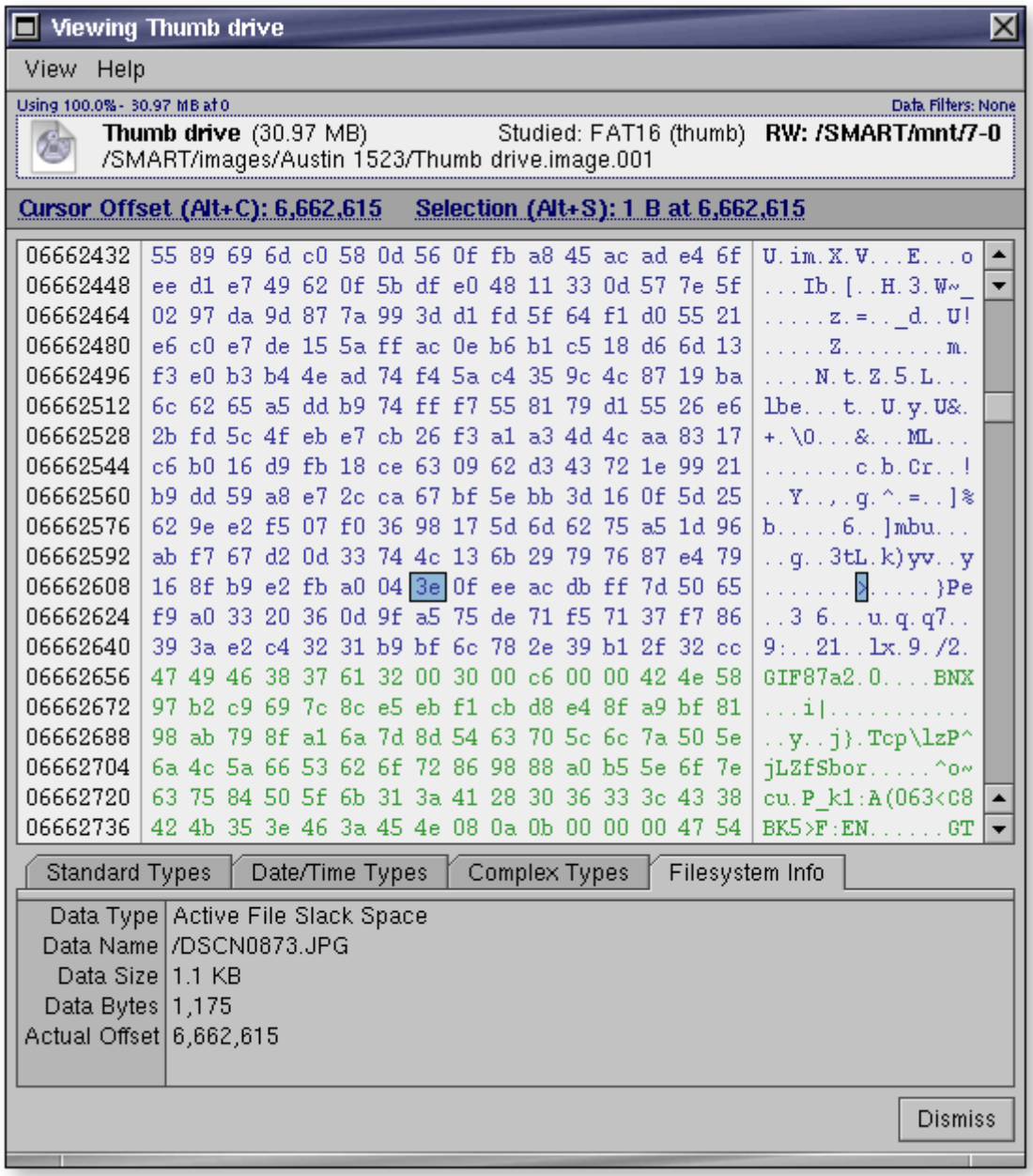

Searching /dev/hda1
Using 100.0% - 21.487 GB at 0
Data Filters: None
HPFS/NTFS (7) Partition (21.487 GB)
Studied: NTFS
/dev/hda1
Searching... 114 matches found.
/dev/hda1
Offset: 0x1af000 (1765376) [1.00 MB Selected]
Active File Data: /Documents and Settings/Jeff/Desktop/Mega Crap/Crap3/101302 entire.do
/dev/hda1
Offset: 0x979000 (9932800) [1.00 MB Selected]
View Statistics
Select All Ctrl+S
View Hit
Log Hit(s)...
Export Matched Data
Filesystem
Individual Files
Text File
Text File w/Offset
Offset: 0xb87000 (12087296) [500.0 KB Selected]
Offset: 0xe930d6 (15282390) [9 B Selected]
Offset: 0xe93b92 (15285138) [9 B Selected]
Active File Data: /Documents and Settings/Jeff/Local Settings/Temporary Internet Files/
/dev/hda1
Offset: 0xe93c56 (15285334) [9 B Selected]
Active File Data: /Documents and Settings/Jeff/Local Settings/Temporary Internet Files/
/dev/hda1
Offset: 0xe93cee (15285486) [9 B Selected]
Active File Data: /Documents and Settings/Jeff/Local Settings/Temporary Internet Files/
/dev/hda1
Offset: 0x18500d6 (25493718) [9 B Selected]
Abort

SMART – обработка данных.

Встроенный просмотрщик SMART может автоматически распознавать некоторые структуры данных файловой системы. На рисунке показана интерпретация программой SMART фрагмента FAT таблицы.



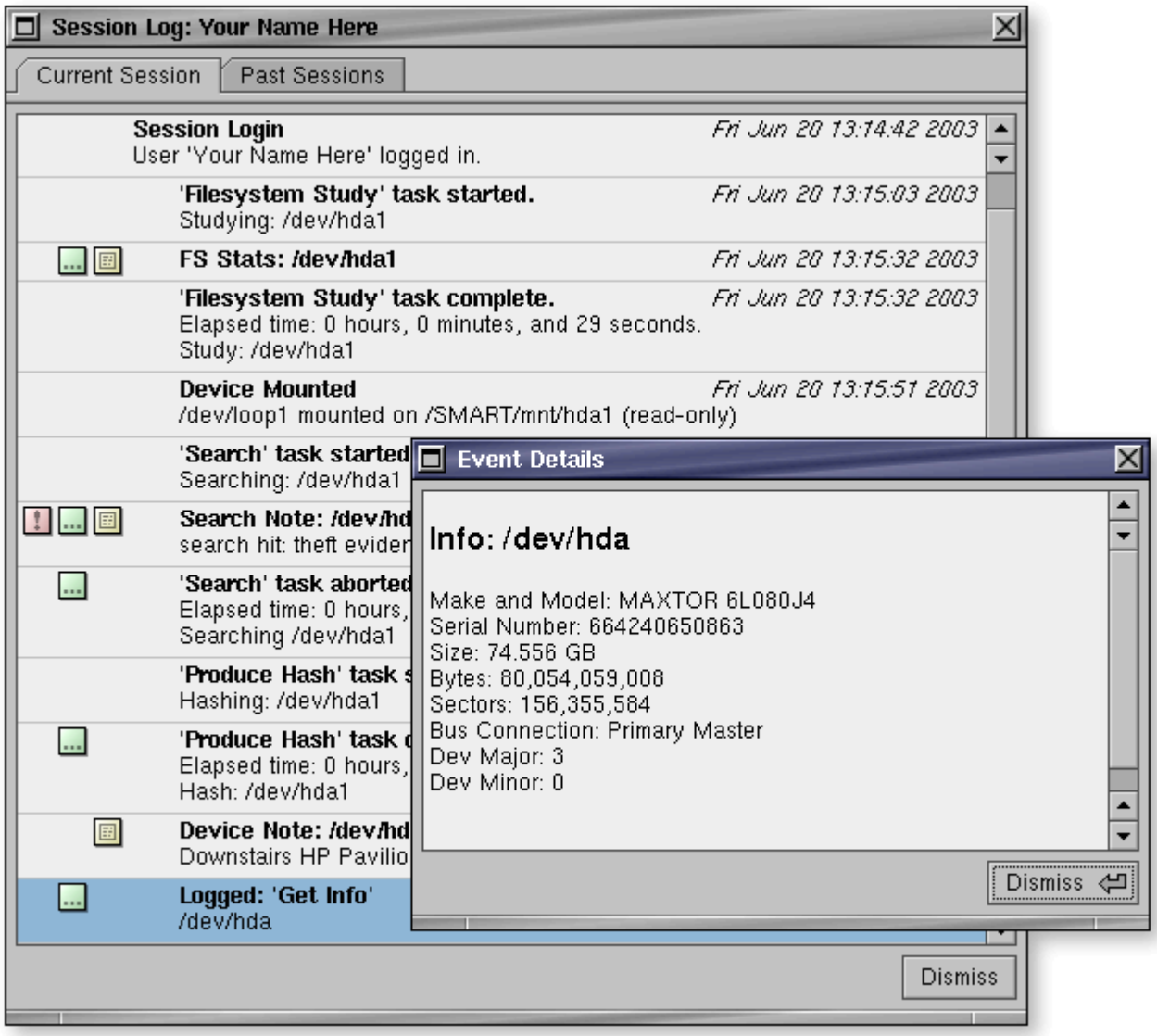
Расширенное изучение файловой системы с использованием SMART проводится с применением специализированного пользовательского интерфейса. Здесь исследуемые объекты файловой системы выделяются разным цветом. На рисунке: синяя область – окончание данных одного файла; зеленая область – начало данных другого файла (GIF-файла, о чем свидетельствует его заголовок).



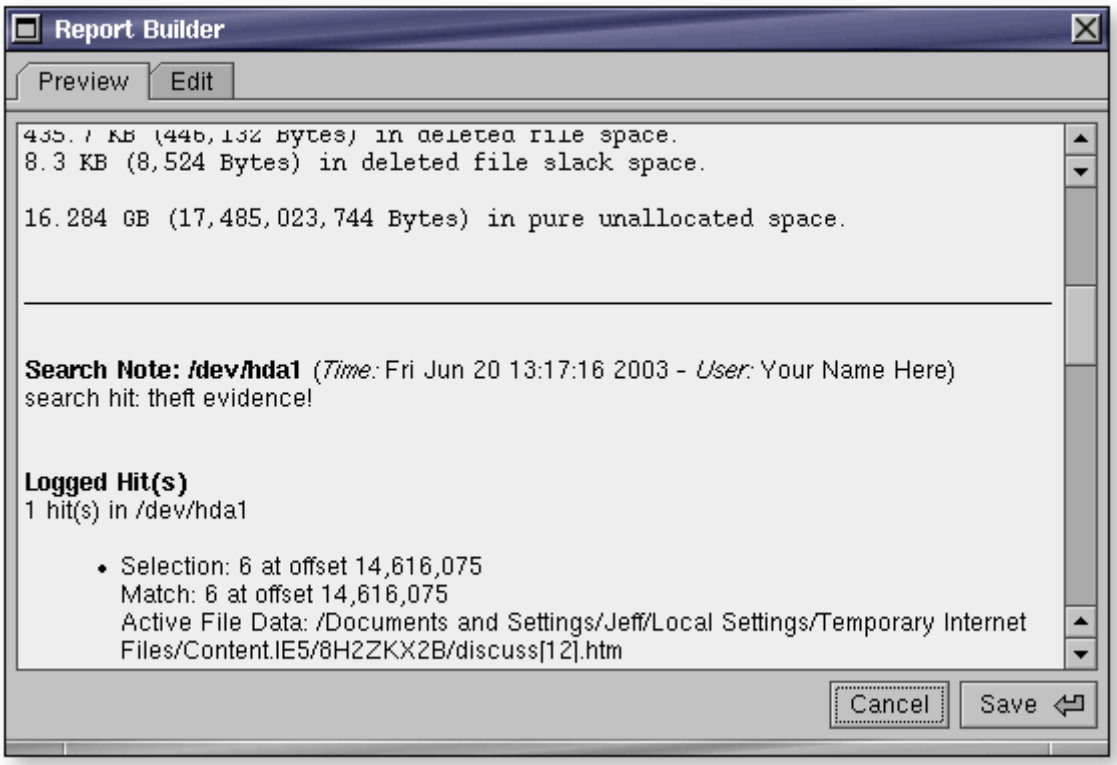
Отчеты SMART.

Все действия в SMART могут быть зафиксированы и, в дальнейшем, в полном объеме или выборочно сведены в «финальный» отчет, который выводится в формате HTML.

Отчет имеет древовидную структуру. Так, отчеты о конкретных действиях исследователя находятся в отчете сессии проведения исследования. Подробную информацию о конкретном событии можно просмотреть, кликнув правой кнопкой мыши по зеленой кнопке соответствующего отчета. Красным цветом отмечены наиболее важные части отчета.



Выбранные Вами отчеты могут быть добавлены к «финальному» отчету.



Очистка носителей в SMART.

SMART имеет настраиваемую систему очистки носителей. В зависимости от настроек, могут быть очищены: весь накопитель, логический раздел, определенная область и т.д.

Дополнительная информация:

Оригинал переведенной статьи находится по адресу: http://www.asrdata.com/SMART/

Сайт производителя SMART: http://www.asrdata.com/

Демонстрационная версия SMART находится по адресу: http://smartforensics.net/SMART-2004-10-05E.tar.bz2

Форум, посвященный использованию SMART, расположен по адресу: http://smartforensics.net/