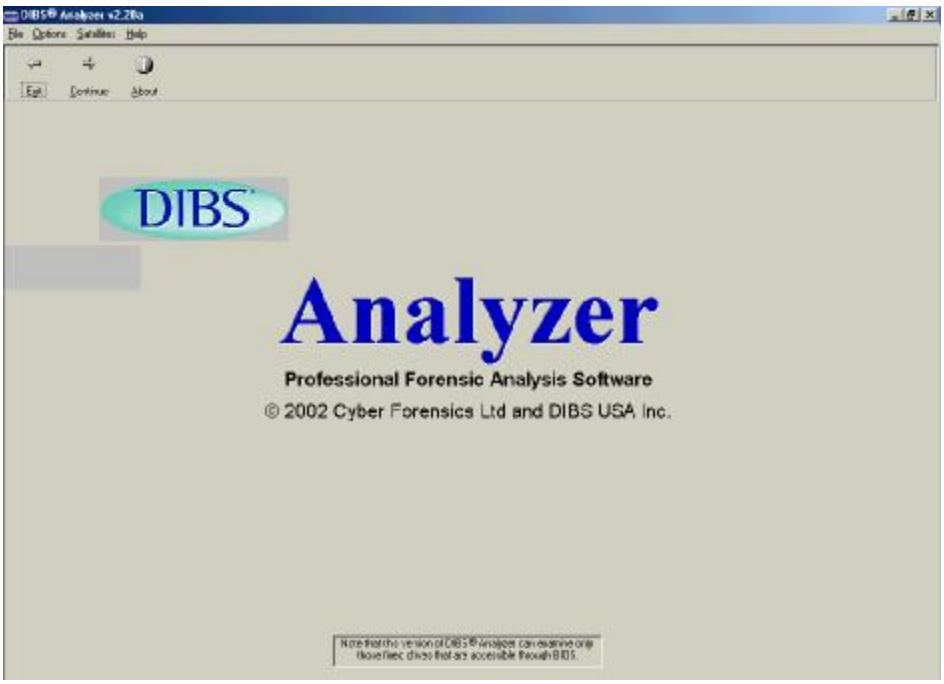
Капинус О.В.
Михайлов И.Ю.

DIBS® Analyzer 2

Эффективный анализ жестких дисков, включая накопители, содержащие ОС Windows 3.11, 95, 98, ME, 2000 и NT (все версии).



Основные характеристики:

- создает полный список файлов, находящихся на различных типах жестких дисков, включая накопители, содержащие ОС: Windows 3.11, 95, 98, ME, 2000 и NT (все версии);
- сортирует списки файлов по атрибутам, включая название, дату, размер, расширение, начальный кластер и т.д.;
- аккуратно производит высокоскоростной поиск по всей поверхности жестких дисков или в их заданных областях по многочисленным критериям;
- обеспечивает быстрое выполнение стандартных команд просмотра, сортировки и распечатки результатов поиска;
- отображает и печатает содержание файлов как в шестнадцатеричном, так и текстовом представлении;
- легко идентифицирует различные типы накопителей;
- автоматически восстанавливает единичные или целые группы файлов;
- распечатывает полученные результаты исследований в формах, предназначенных для предоставления в суд;
- позволяет осуществлять быстрый просмотр и распечатку данных, находящихся в зазорах файловой системы (slack space), свободных кластерах и других областях жесткого диска;
- может использоваться для копирования, поиска и извлечения информации, находящейся на гибких магнитных дисках;
- сохраняет последовательность выполненных в ходе исследования операций.

1.Описание

DIBS® Analyzer 2 (www.dibsusa.com)- профессиональная программа, которая снабжает исследователя мощным и удобным в работе аналитическим инструментом. Высоко эффективная и продуктивная программа **DIBS® Analyzer 2** упрощает и ускоряет занимающую много времени рутинную работу, такую, как восстановление файлов, исследование и распечатка данных, находящихся в зазорах файловой системы, поиск доказательств.

Программный продукт **DIBS® Analyzer 2** был создан практикующими исследователями для обеспечения аналитиков максимальными возможностями в работе. Высоко эффективный программный продукт **DIBS® Analyzer 2** отображает обнаруженные доказательства в форме, приемлемой для предоставления в суд. Списки файлов, создаваемые **DIBS® Analyzer 2,** содержат все детали, необходимые исследователю, в колонках информации, которую можно сортировать индивидуально. Доступно все: дата создания, дата последнего изменения и дата последнего доступа, размер файла, название, начальный кластеры и т.д. Удаленные файлы отображаются красным цветом и могут быть восстановлены как по одному, так и целыми группами с помощью простого клика и перетаскивания мышкой. Поиск можно выполнять, используя надежный и правильный встроенный поисковый механизм. Можно создавать различные варианты проведения поиска и запоминать их, а также поиск можно проводить на различных участках жесткого диска, в зависимости от ваших запросов. Результаты поиска отображаются в форме, легкой для восприятия. Их можно быстро просматривать, удаляя ложноположительные доказательства и сохраняя важные доказательства. Результаты исследований могут быть распечатаны в разных форматах, чтобы соответствовать требованиям конкретного судебного дела.

2.Рекомендуемые области применения

Для использования на месте совершения преступления (в «полевых условиях») или в лаборатории для анализа скопированных подозрительных данных.

3.Прочность судебных доказательств

Когда вы разрабатываете программы, необходимые для проведения компьютерных судебных исследований, то важным фактором является то, чтобы методы проводимых исследований имели твердую научную основу. Особенно это важно для программы, которая должна быть абсолютно точной и должна сохранять полную доказательственную целостность данных в любое время. Единственным способом для достижения этой цели является введение в программу специфической информации, необходимой при ее использовании в ходе проведения расследования. В этом случае, действие каждой строчки кода известно и соответствует поставленной задаче. Все программы, выпущенные DIBS®, созданы и написаны специально для проведения судебных расследований аналитиками мирового уровня, участвующих в судебных процессах.

4.Преимущества

Программа дает уверенность, что проводимая работа соответствует высочайшим стандартам.

Программа создана практикующими профессионалами, которые понимают потребности аналитиков/исследователей (в т.ч. экспертов).

Программа быстро осваивается и легка в применении.

Программа помогает найти доказательства быстро и надежно.

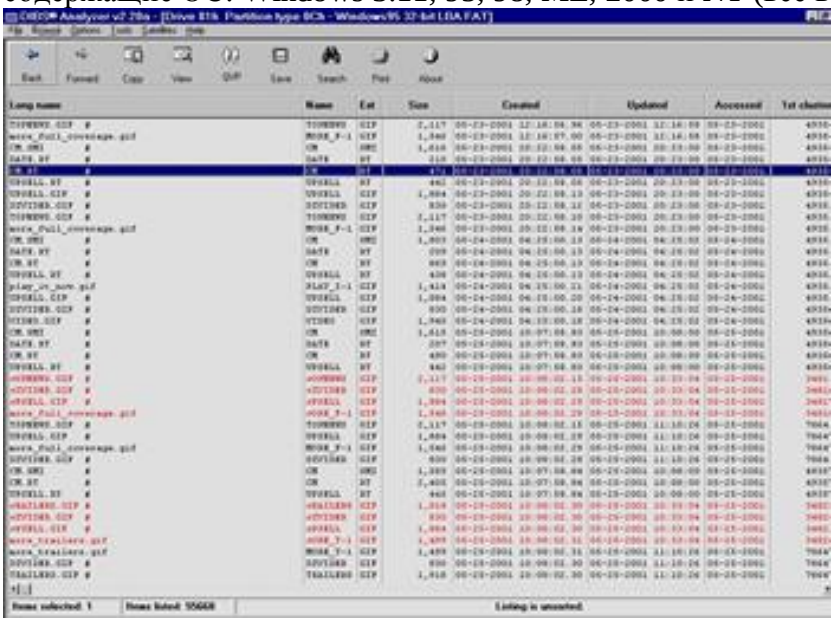
Программа экономит время и повышает продуктивность.

Программа имеет встроенную контекстную справочную систему, которая, в случае необходимости, обеспечивает помощь и совет.

5.Функции

Списки файлов

Создает полные списки файлов для различных жестких дисков, включая накопители, содержащие ОС: Windows 3.11, 95, 98, ME, 2000 и NT (все версии).

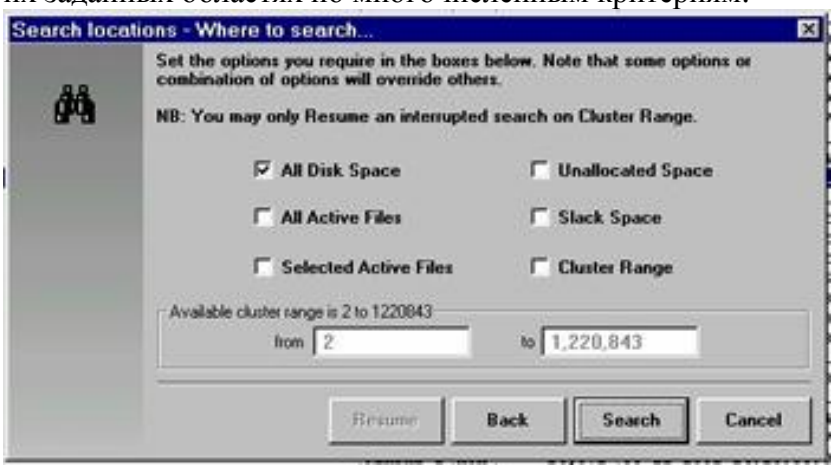


Окно со списком файлов.

Списки файлов могут сортироваться по атрибутам, включая название, дату, название файла, размер, расширение, исходный кластер и т.д. Форма представления может быть изготовлена по техническим условиям заказчика, чтобы соответствовать конкретным требованиям.

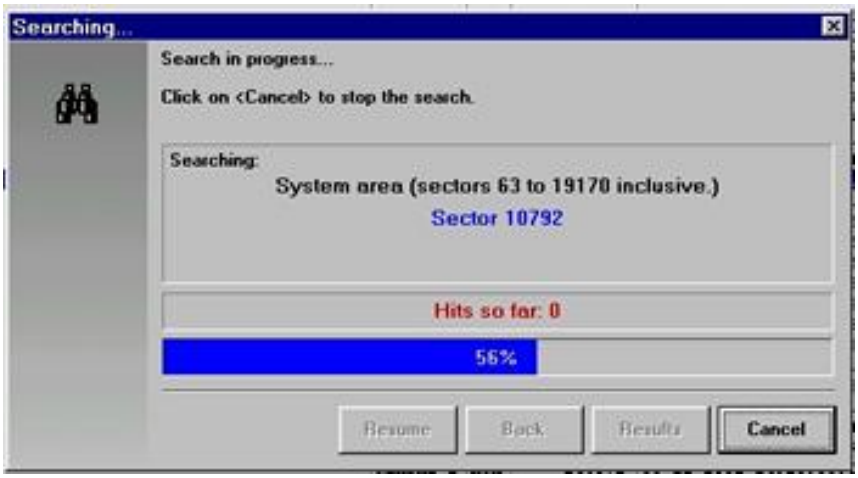
Поиск.

Точно проводит высокоскоростной поиск по всей поверхности жестких дисков или в их заданных областях по многочисленным критериям.

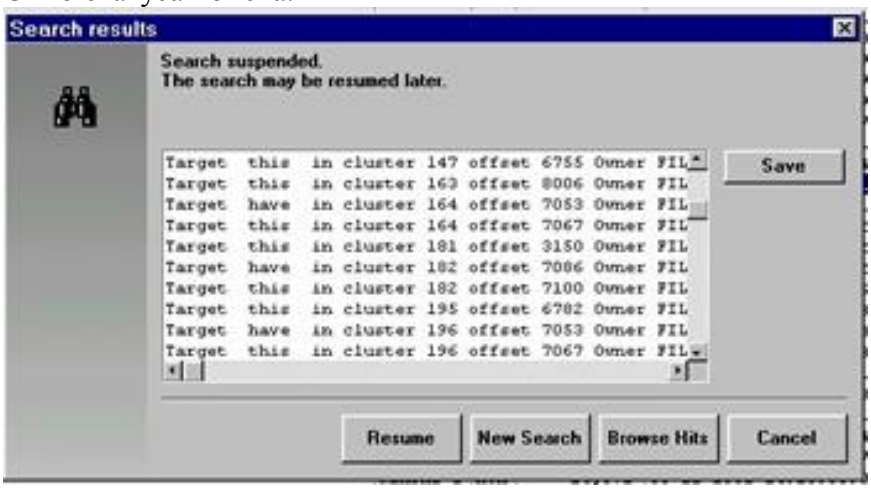


Окно для выбора параметров поиска.

Содержит широкий диапазон параметров поиска. Параметры критериев поиска могут сохраняться пользователем в отдельный файл, который может быть использован для осуществления поиска аналогичных данных на других носителях информации.

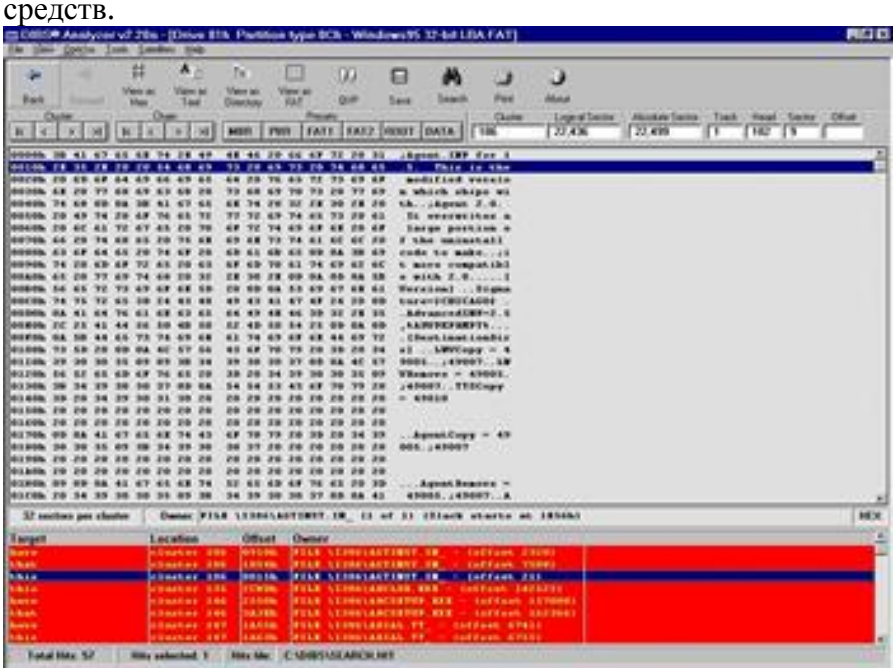


Окно статуса поиска.



Экран с результатами проведенного поиска.

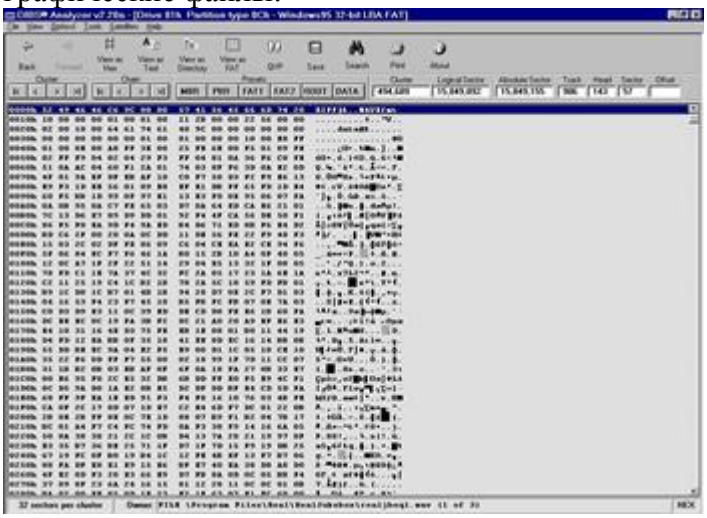
Результаты поиска могут быстро просматриваться, сортироваться, отображаться и распечатываться с применением встроенных в программу специализированных средств.



Окно просмотра данных, обнаруженных во время проведения поиска.

Просмотр и распечатка файлов.

Содержание любого файла можно просмотреть и распечатать как в шестнадцатеричном виде, так и в виде текста. Если инсталлирована программа Quick View Plus™, то файлы можно просматривать в их первоначальном формате, включая и графические файлы.



Окно просмотра данных в шестнадцатеричном виде.

Дополнительная информация:
Оригинал переведенной статьи находится по адресу:
http://www.dibsusa.com/products/dan2.html

Благодарим:
Marat'a, за помощь, оказанную в написании статьи.