Режим "Чернового восстановления"

Метод *чернового восстановления* является последним по применимости в ряду средств восстановления информации пользователя предоставляемых комплексом. Основная идея данного метода – восстановление файлов с известными заголовками из предположения их непрерывности, при отсутствующей информации об их размещении и восстановление файлов с известной структурой на основе внутренних закономерностей.

Иначе говоря, если найдены два заголовка файлов известного типа, то с большой долей вероятности можно предположить (если нет точной информации о расположении из таблицы FAT, записи MFT и т.п.), что файл имеет тип, определяемый первым заголовком и размер, определяемый разницей LBA первого и второго.

Это предположение не всегда верно, так как может быть ошибка в идентификации, файл может быть фрагментирован и т.п.

Уменьшить процент подобных ошибок помогает проверка внутренней структуры файла на непротиворечивость. Возможность такой проверки сильно зависит от формата файла. В самых удачных случаях можно точно определить размер и убедиться в отсутсвии каких-либо ошибок. Но в любом случае теряется информация об имени, дате создания, положении (каталоге).

Но, когда нет другого выхода, лучше восстановить хоть что-то, чем ничего. При этом нужно иметь в виду, что конкретный результат восстановления существенно зависит от конкретной ситуации, есть ли в используемом справочнике заголовков соответствующий, насколько фрагментирован диск, велики ли размеры искомых файлов, сколько на диски файлов с известной структурой. В различных случаях процент успешно восстановленных файлов может колебаться от 0 до 70%.

Этот метод нужно применять в случаях, когда логические разрушения очень велики или когда речь идет о файловой системе, для которой у Вас нет средств логического восстановления.

Режим имеет много общего с режимом поиска регулярных выражений.

Основные отличия:

- во время работы происходит поиск не только регулярных выражений, но и анализ известных структур файлов. Для последних в таблице найденных файлов поле GREP пустое (см. Рисунок 1). Чтобы отключить анализ структуры известных файлов, отметить пункт «Использовать только поиск GREP» на панели параметров режима.
- критерии поиска не выбираются, их список определяется *Справочником чернового восстановления* (при этом, критерии поиска могут быть изменены, подробнее см. ниже);
- результатом поиска являются предполагаемые файлы, которые можно скопировать. При этом имя файла - номер сектора начала, расширение определяется критерием. Если копируются все файлы определенного типа (контекстное меню списка критериев), создается подкаталог по имени расширения.
- для файлов с известной структурой отображаются метаданные, которые могут быть сохранены в различных форматах (.html, .rtf, .txt) или скопированы в буфер обмена.

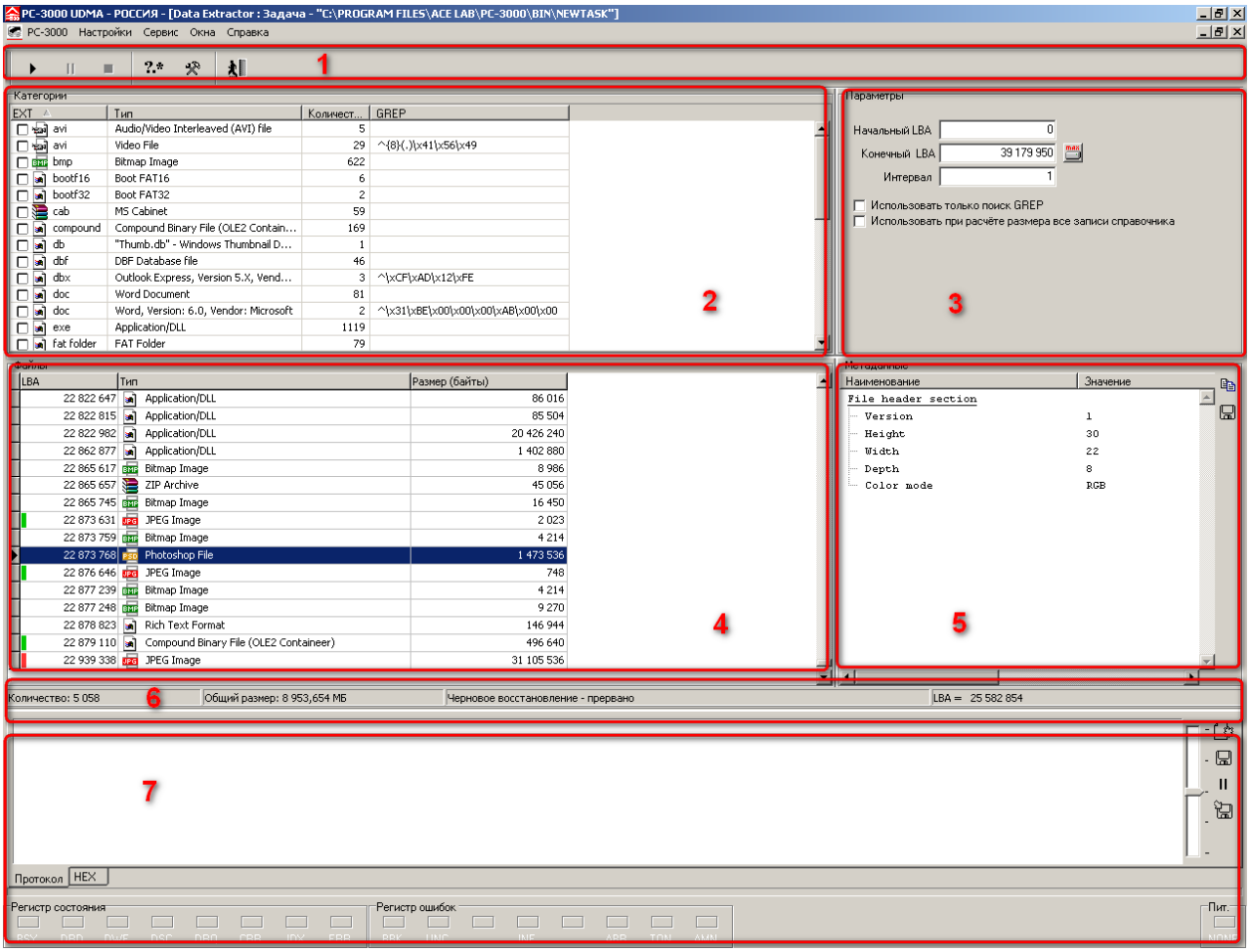

Рисунок 1. Режим чернового восстановления:

1. Оперативная панель
2. Таблица найденных типов файлов (Расширение, Тип, Количество найденных файлов, GREP если найден с помощью регулярного выражения).
3. Панель параметров режима (Начальный LBA, Конечный LBA, Интервал и др.)
4. Таблица найденных файлов (LBA, Тип, Размер в байтах).
5. Панель метаданных файла
6. Строка состояния (Количество найденных файлов, Общий размер, Статус процесса, Текущий LBA)
7. Панель с вкладками «Протокол», «HEX» и индикатором процесса выполнения.

Возможные действия со списком найденных типов файлов, списком найденных файлов и метаданными доступны через контекстные меню, отметим лишь некоторые особенности.

В *таблице найденных файлов* имеется возможность сортировки результатов с помощью щелчка по заголовку столбца. Отметки в левой части каждой строки можно использовать для сохранения или удаления более чем одного типа файлов сразу.

Для некоторых типов файлов с известной структурой выполняется проверка целостности, если такая проверка была выполнена, то ее результат отображается в *таблице найденных файлов* в левой части записи в виде цветного прямоугольника. Зеленым цветом отмечаются целые файлы, красным — поврежденные. Если файл не был проверен, либо был найден с помощью GREP, то отметка не ставится.

Список найденных файлов может быть отфильтрован по признаку целостности файлов и/или по их типу. Настройки фильтра могут быть вызваны из контекстного меню *таблицы найденных файлов* или по щелчку на кнопке 

расположенной на о*перативной панели.* Форма настройки фильтра отображаемых файлов выглядит следующим образом:

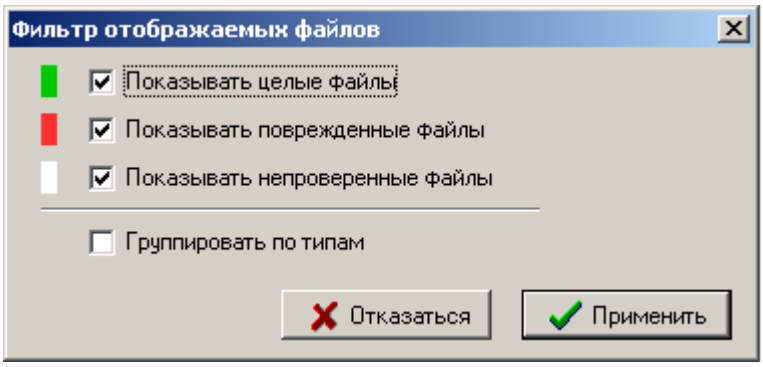

Рисунок 2. Фильтр отображаемых файлов.

Проверка известных структур типов файлов (а вместе с ней и проверка их целостности) может быть отключена с помощью пункта «Использовать только поиск GREP» на *панели параметров режима*.

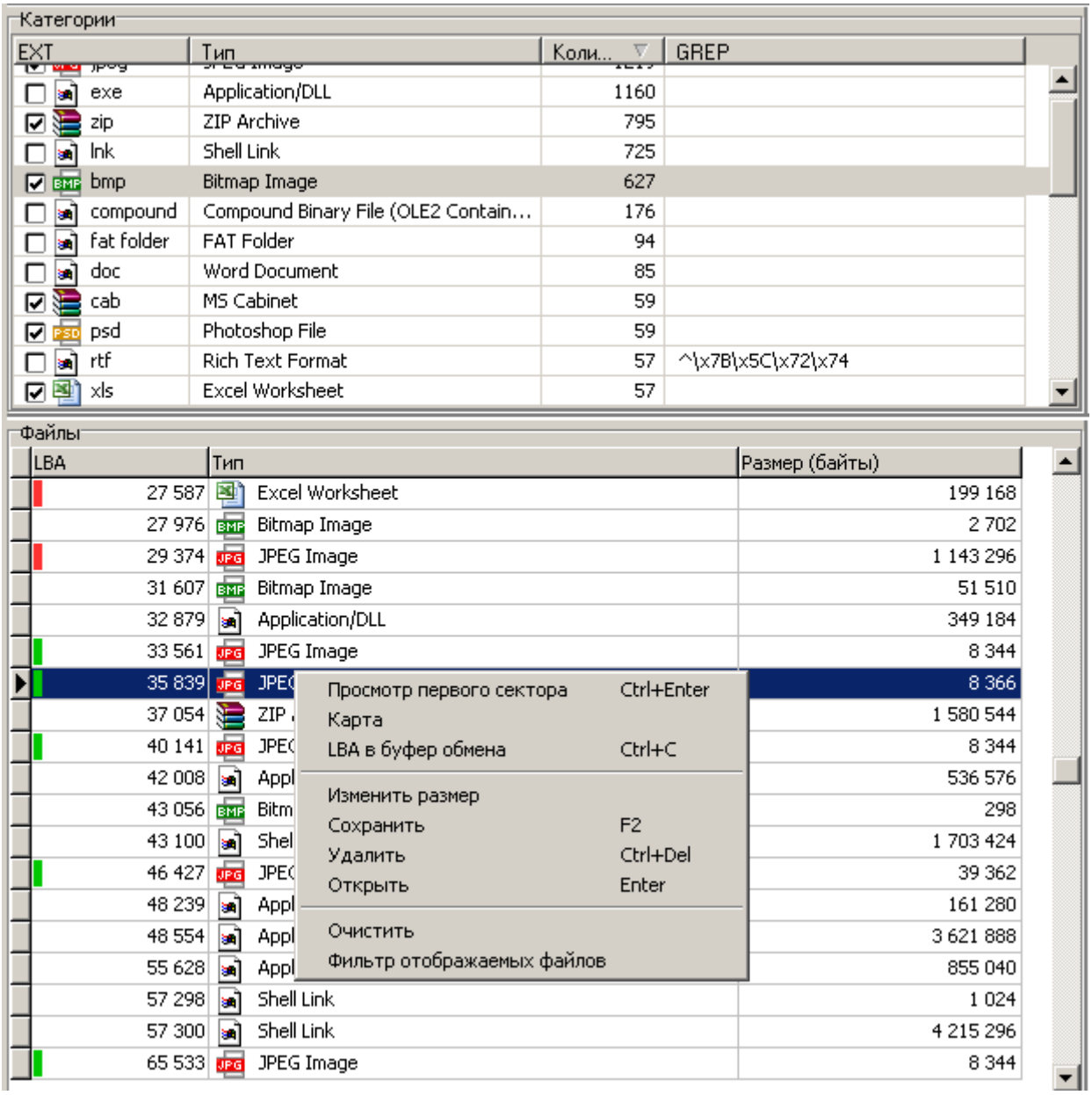

Рисунок 3. Результаты работы режима «Чернового восстановления».

Справочник чернового восстановления. В данном справочнике собраны все регулярные выражения, которые могут быть использованы для идентификации файлов пользователя. Справочник чернового восстановления доступен из меню *Настройки* → *Справочник чернового восстановления* (см. рисунок ниже).

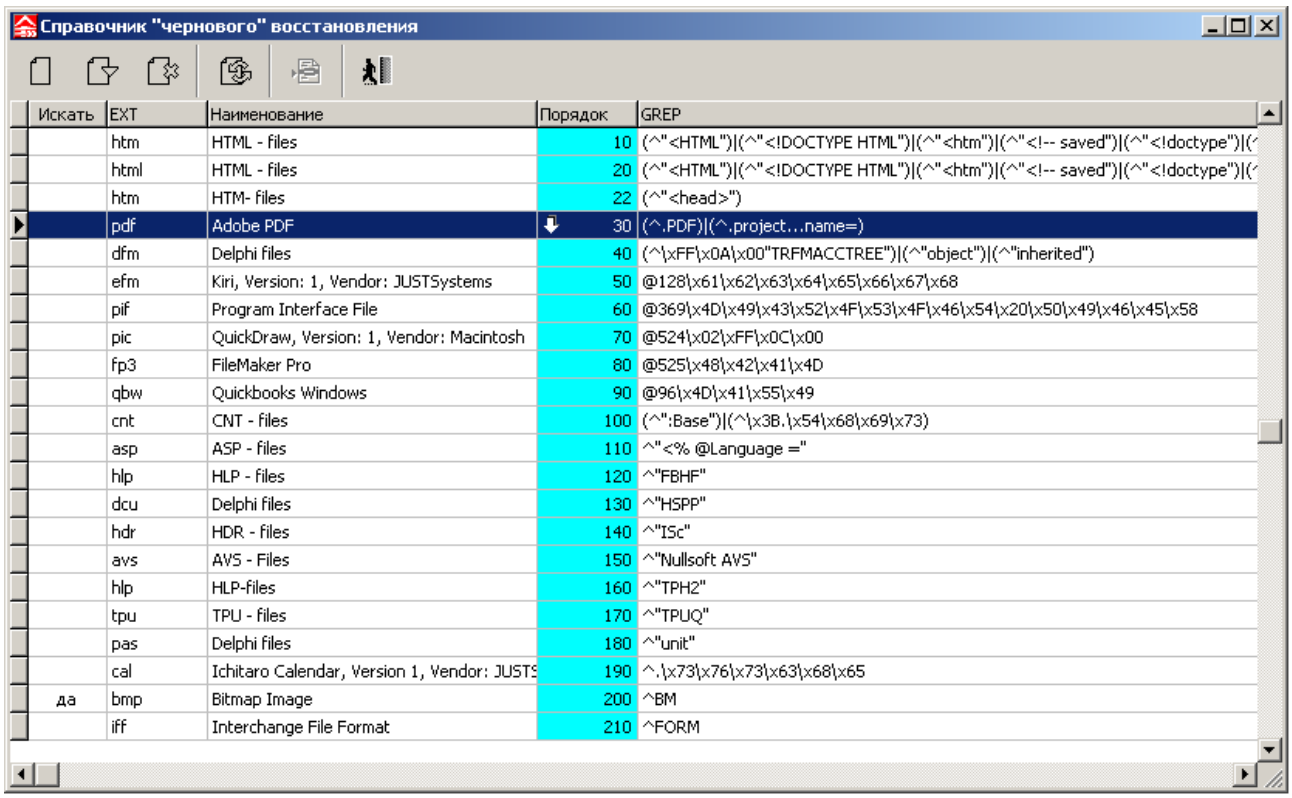

Рисунок 3 Справочник "чернового" восстановления

При выполнении “чернового восстановления”, если не удалось найти файл с известной структурой, то для поиска предполагаемого начала используются регулярные выаражения из справочника, причем не все, а только отмеченные в столбце *Искать*. Для расширения списка используемых при поиске выражений необходимо либо пометить соответствующее выражение из справочника, либо создать новое выражение и установить флажок в поле *Искать*.

При запуске "чернового" восстановления, пользователю предоставляется возможность выбора способа расчета размера найденных данных. Существует два варианта. В первом, при расчете размера используются только регулярные выражения отмеченные в столбце *Искать* справочника. Во втором, используются все регулярные выражения справочника (но только при расчете размера данных). Выбор конкретного способа расчета размера зависит от типа искомых данных, для многих файлов предпочтительнее первый способ, т.к. если размер сохраненного файла будет больше его реального размера, то большинство приложений смогут его корректно открыть. В случае если файл меньше своего реального размера, то это может привести к сбою ассоциированного с ним приложения. Для любого файла есть возможность изменить его размер из контекстного меню таблицы найденных файлов.

Каждая строка справочника задает критерий поиска для файлов определенного типа с помощью поля *GREP*. В процессе чернового восстановления осуществляется поиск этих критериев. Данные поля *GREPEXT* используются для уточнения типа файла в случае наличия нескольких одинаковых GREP для разных типов файлов. Если *GREP* для нескольких типов файлов одинаковый и *GREPEXT* для них не существует, то расширение выбирается с помощью поля *порядок*, точнее по наименьшему порядку.

Дополнительные критерии, задаваемые полем *GREPEXT*, в справочнике не отображаются. Увидеть поле с дополнительными критериями, можно войдя в режим редактирования элемента списка. Например, на рисунке ниже приводятся два окна редактирования элемента списка с одинаковыми *GREP* и различными *GREPEXT*.

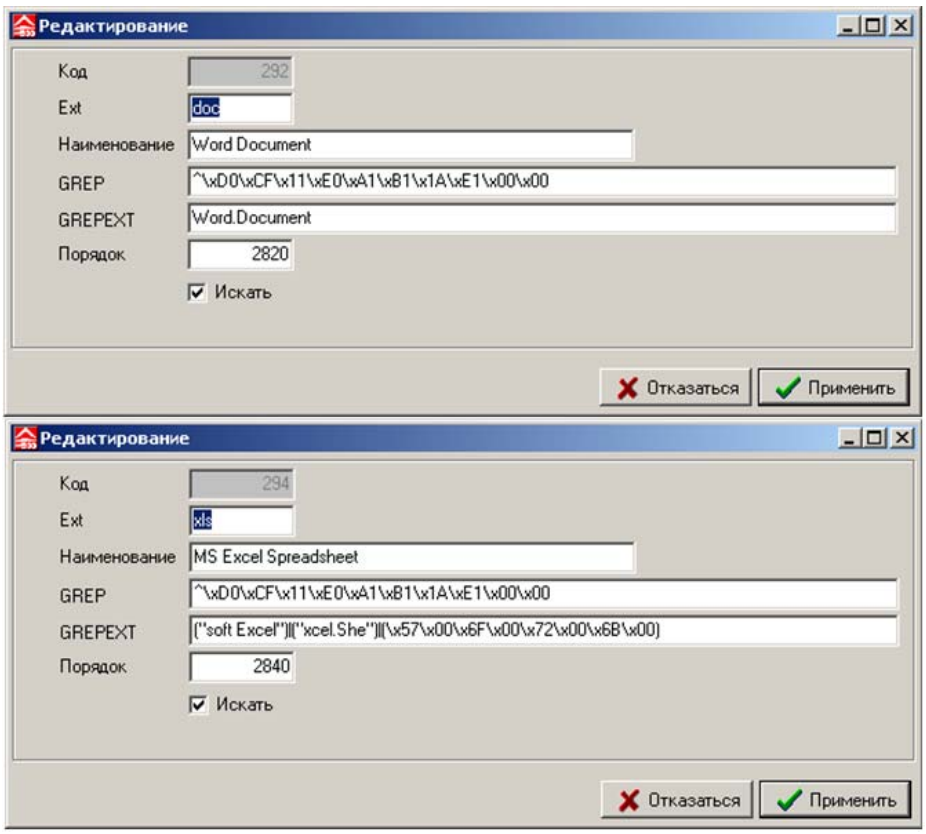

Рисунок 4 Окно редактирования элемента списка чернового восстановления

Существует возможность редактирования данного справочника - это достаточно сложное и ответственное дело. Однако при создании задачи восстановления данных создается копия справочника "чернового" восстановления, с которой и происходит работа в текущей задаче. Соответственно, в случае необходимости справочник можно восстановить. С другой стороны, если Вы хотите, чтобы внесенные изменения были сохранены, то следует редактировать справочник, относящийся не к текущей задаче, а к программе DE.

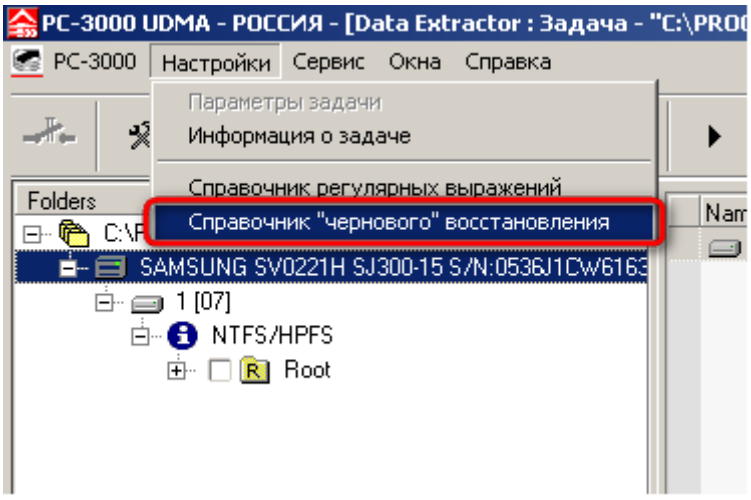

Рисунок 5 Справочник “чернового” восстановления

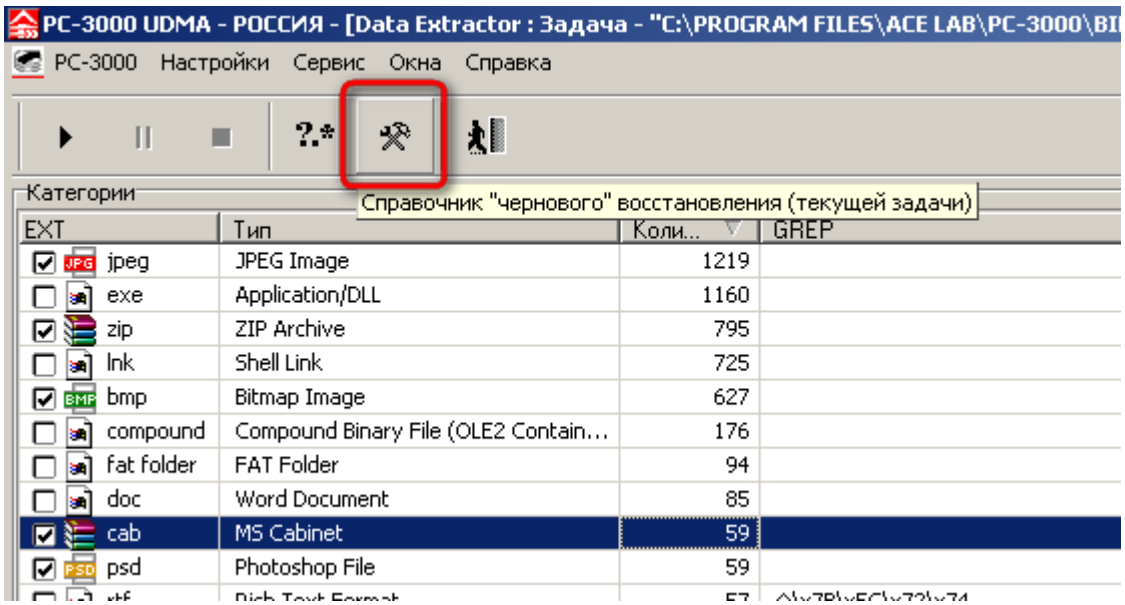

Рисунок 6 Копия справочника “чернового” восстановления в текущей задаче.

Основной справочник "чернового" восстановления DE не используется при выполнении чернового восстановления. При создании задачи создаётся его копия. Редактировать основной справочник можно из меню главной формы. Справочник текущей задачи редактируется в режиме "чернового" восстановления.

Еще одной важной особенностью является то, что для данного режима ошибочная идентификация начала файла может привести к потере данных.

Это можно пояснить на примере - найдено много заголовков файлов определенного типа, имеющего простую и нехарактерную сигнатуру заголовка, а со слов клиента (или Вы сами убеждены) этого типа файлов не должно быть на исследуемом диске. Это означает, что найденные результаты – ошибочные, и они могут привести к неверному расчету размеров других важных файлов.

Правильное определение начала области сканирования и шага может существенно уменьшить количество ошибок и сэкономить время. Надо иметь в виду, что сканирование желательно начинать от известного начала кластеризации и с шагом, равным размеру кластера. Если эта информация отсутствует, то в качестве первого параметра подойдет любой, найденный при поиске с шагом 1, достоверный заголовок файла, а в качестве второго – минимальный размер кластера по умолчанию (например, для FAT - 8).

Режим "чернового" восстановления доступен через пункт меню *Сервис* → *Черновое восстановление*, либо через соответствующие пункты меню объектов проводника с той разницей, что для объектов проводника типа "слот таблицы разделов" установлены границы поиска (раздел), а для "Boot" еще и шаг (размер кластера).