# Encase Forensic Edition. Быстрый старт.

Капинус Ольга Валерьевна

Михайлов Игорь Юрьевич

## Введение.

Encase Forensic Edition ( далее, Encase) – специализированное программное обеспечение, предназначенное для исследования ЭВМ и компьютерных носителей информации, разрабатываемое Guidance Software Inc. с 1997 года. Encase используется в ходе проведения исследований и экспертиз, при расследовании преступлений в сфере высоких технологий по всему миру. В настоящее время продано более 14000 копий программы. Несмотря на наличие локализованных ( переведенных на русский язык) версий программы Encase и подробнейших Руководств пользователя на русском языке (для версий программы Encase Forensic Edition 4, Encase Forensic Edition 5) неподготовленному пользователю, не прошедшему обучение на специализированных курсах Guidance Software Inc., сложно начать применять программу Encase в экспертной практике. Этой работой мы хотим начать цикл статей, посвященных описанию использования Encase в судебной экспертной практике и выполнения, с ее помощью, рутинных операций ( например, поиск по ключевым словам, поиск и просмотр графических изображений и т.д.), которые выполняет эксперт в ходе проведения судебной экспертизы.

## 1. Подготовка к производству исследования.

Для начала нового исследования рекомендуется создать каталог (например, case), в котором будут находиться все материалы исследования и, дополнительно, создать в нем три подкаталога:

Evidence – используется для хранения образов исследуемых накопителей;

Export – в данный каталог помещаются данные, экспортируемые из накопителей (или их образов) в ходе производства исследования;

Temp – каталог используется для хранения временных файлов.

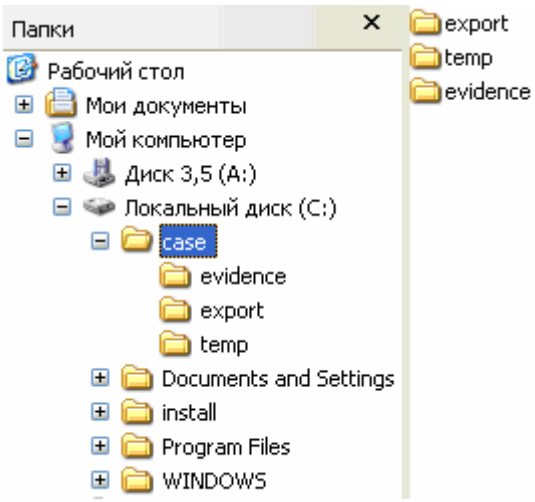


Иллюстрация №1. Создание подкаталогов: Evidence, Export, Temp в каталоге Case Проводника Windows.

После старта программы Encase необходимо выбрать опцию «New»

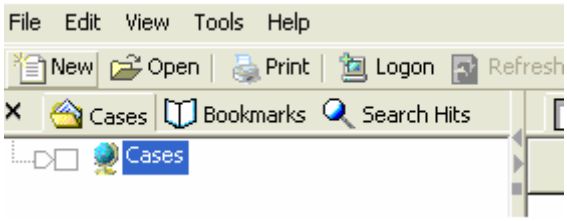


Иллюстрация №2. Фрагмент главного окна программы Encase.

и, в появившемся окне, настроить параметры нового дела:

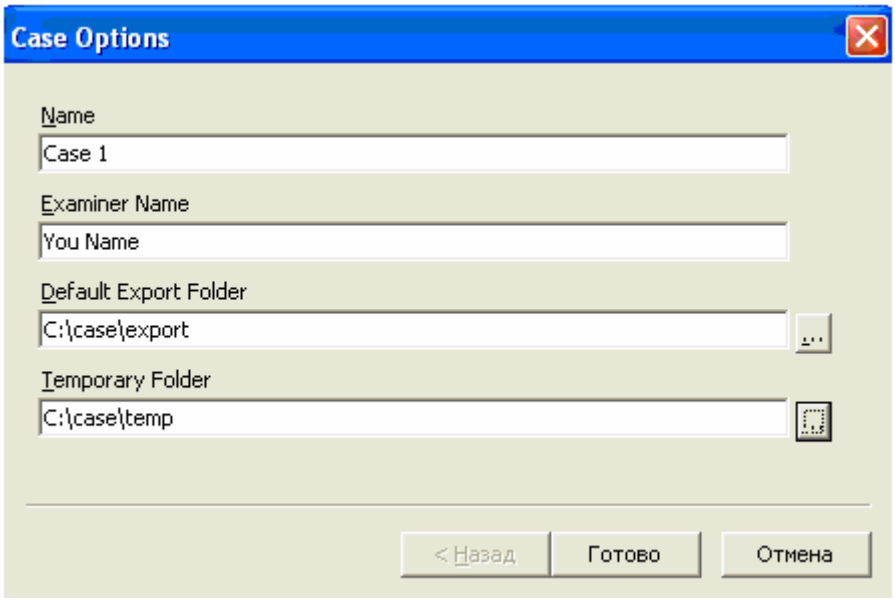


Иллюстрация №3. Окно настройки опций нового дела программы Encase.

При этом, в строках «Default Export Folder» и «Temporary Folder» прописываются пути до соответствующих подкаталогов каталога case (где будут храниться все материалы исследования). В строке «Examiner Name» указываются данные исследователя. Как правило, это имя и фамилия.

2.Подключение накопителей.

Для подключения новых накопителей необходимо кликнуть по опции «Add Device».

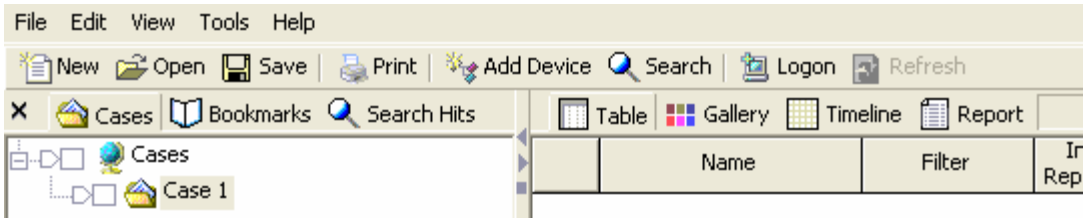


Иллюстрация №4. Фрагмент главного окна программы Encase.

В появившемся окне установить галочку в окошке напротив «Local Drives».

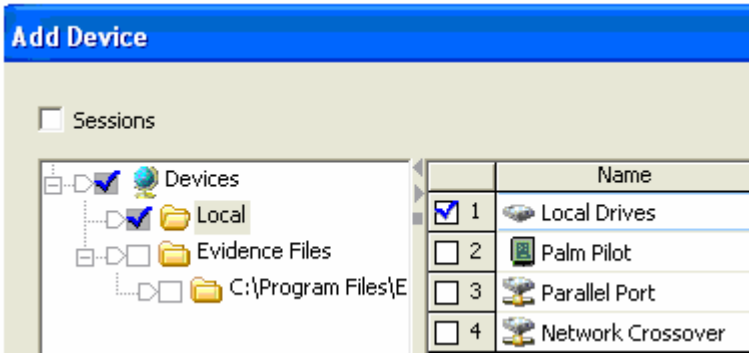


Иллюстрация №5. Фрагмент окна для выбора подключаемых устройств или образов накопителей программы Encase.

После сканирования, проводимого с целью обнаружения подключенных накопителей, программа откроет окошко с доступными, для подключения в программе Encase, накопителями:

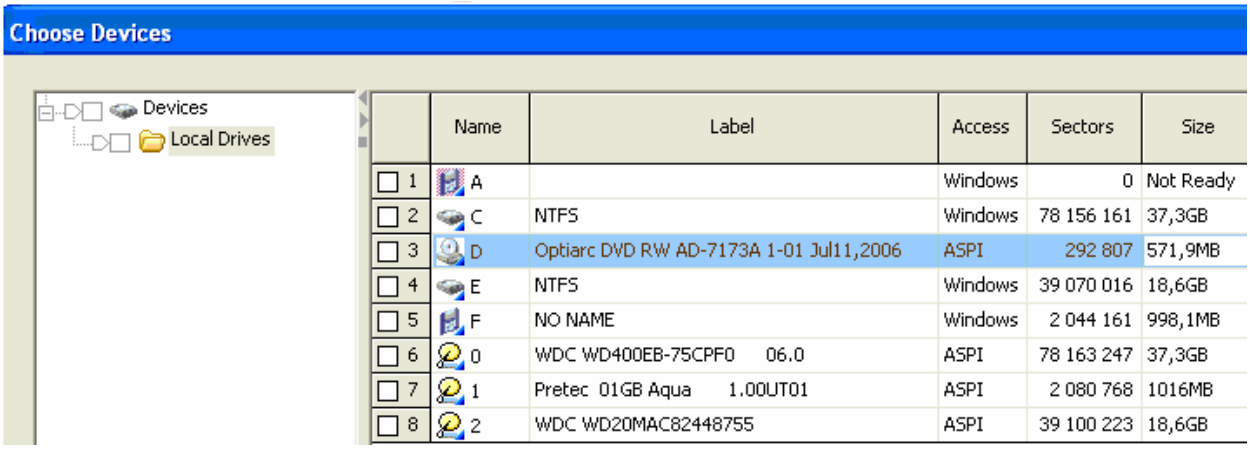


Иллюстрация №6. Фрагмент окна для выбора подключаемых накопителей в программе Encase.

В данном случае, в системе присутствуют:

- НГМД (логический накопитель A), в накопителе отсутствует дискета;

- Привод компакт-дисков «Optiarc DVD», в котором находится компакт диск (мы видим, что Encase отображает для установленного в привод компакт- диска размер «Size» и число секторов «Sectors»);

- НЖМД WDC WD400EB-75CPF0 ( позиция в списке - 6) и НЖМД WDC WD20MAC82448755 ( позиция в списке - 8), на этих НЖМД присутствуют логические разделы C и E;

- Флэш - накопитель «Pretec 01Gb Aqua» ( позиция в списке - 7) на котором, скорее всего, присутствует логический раздел F.

Т.е. можно исследовать на выбор или логические разделы накопителей, или всю доступную поверхность накопителя целиком, включая логические разделы и неразмеченную область. Рекомендуем исследовать накопители целиком, не ограничиваясь анализом логических разделов.

В проводнике Windows видим:

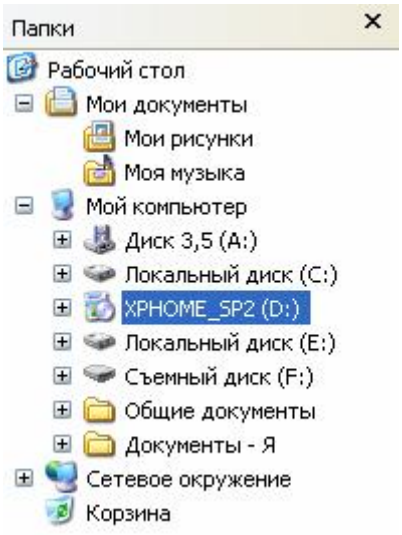


Иллюстрация №7. Фрагмент окна Проводник Windows с отображаемыми в нем накопителями (которые были представлены в Encase (Иллюстрация №6 )).

Т.е. наши предположения о том, что в приводе компакт – дисков ПЭВМ находится оптический диск и то, что логический раздел F является логическим разделом флэш-накопителя, - подтвердились.

Особенностью Encase является использование собственных драйверов для работы с накопителями. Это, например, позволяет исследовать файловые системы NTFS и EXT в среде Windows 98 без использования дополнительных программ или драйверов.

Для подключения накопителя необходимо выбрать накопитель, который необходимо исследовать, установив напротив него галочку, и нажать кнопку « Далее», затем кнопку «Готово».

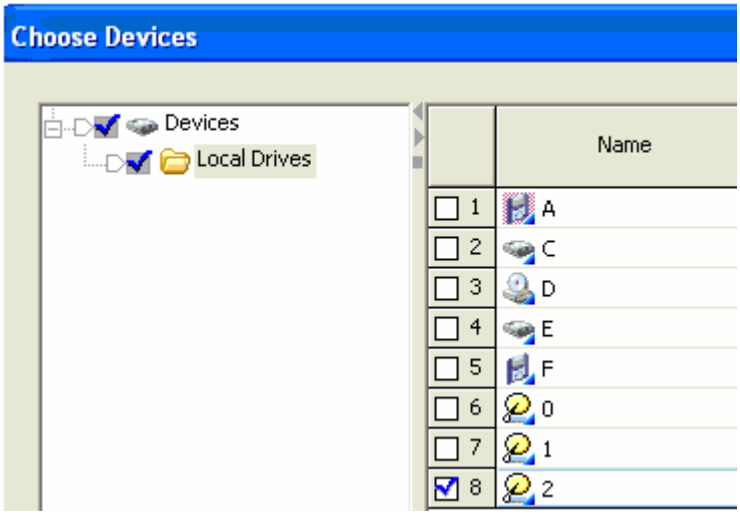


Иллюстрация №8. Фрагмент окна для выбора подключаемых накопителей в программе Encase с выбранным накопителем.

Важно: Значок показывает, что в Encase подключен накопитель. Значок показывает, что в Encase подключен образ накопителя.

3.Монтирование образов накопителей.

Для подключения образов накопителей необходимо кликнуть по опции «Add Device»

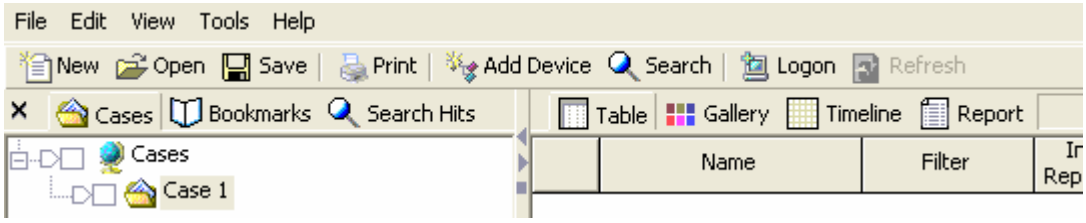


Иллюстрация №9. Фрагмент главного окна программы Encase.

В появившемся окне выбрать значение «Evidence Files»,

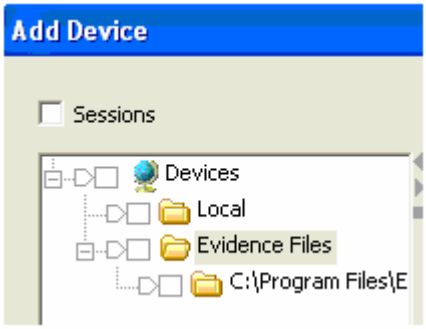


Иллюстрация №10. Фрагмент окна для выбора подключаемых устройств или образов накопителей программы Encase.

кликнув правой кнопкой мыши. В появившемся меню выбрать опцию «New»

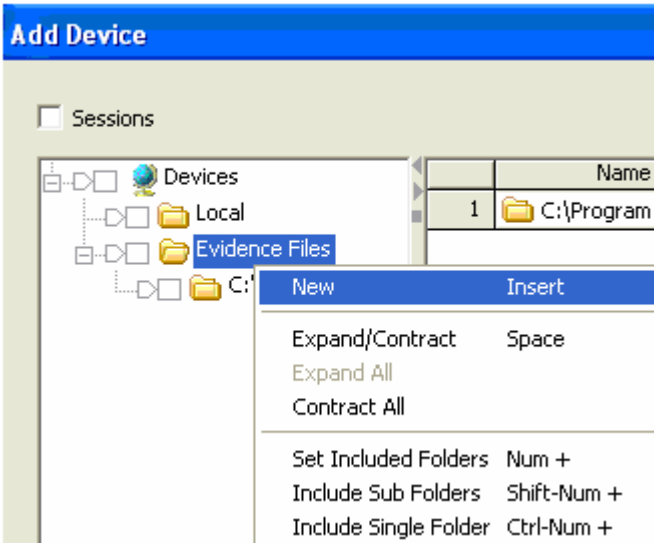


Иллюстрация №11. Указание нового пути расположения образов накопителей в программе Encase.

и указать путь до местонахождения образа накопителя. После чего нажать на кнопку «ОК».

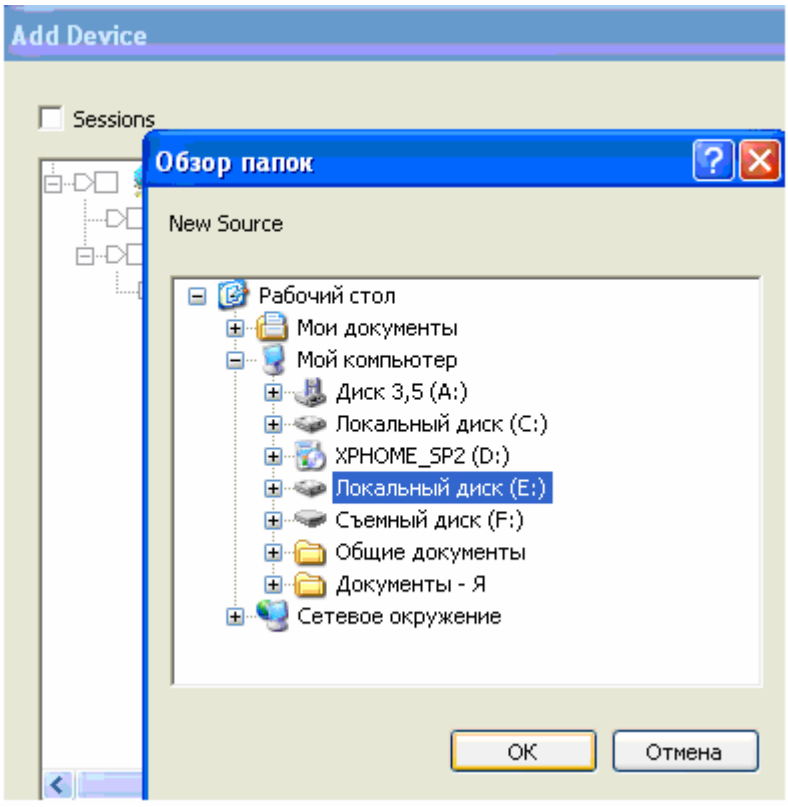


Иллюстрация №12. Указание пути расположения образов накопителей в программе Encase.

Encase просканирует накопитель и выдаст список доступных для монтирования образов накопителей.

Для подключения образа накопителя необходимо выбрать нужный образ накопителя (установить напротив него галочку), который будет исследоваться, и нажать кнопку «Далее», затем еще раз кнопку «Далее», затем кнопку «Готово».

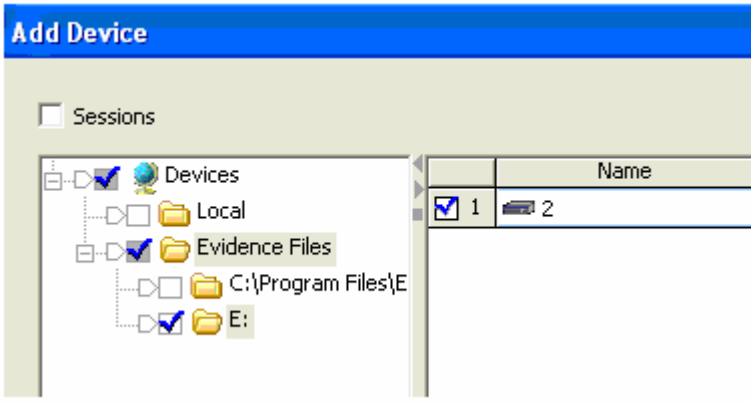


Иллюстрация №13. Фрагмент окна для выбора подключаемых образов накопителей в программе Encase с выбранным образом накопителем.

При этом, Encase смонтирует образ накопителя.

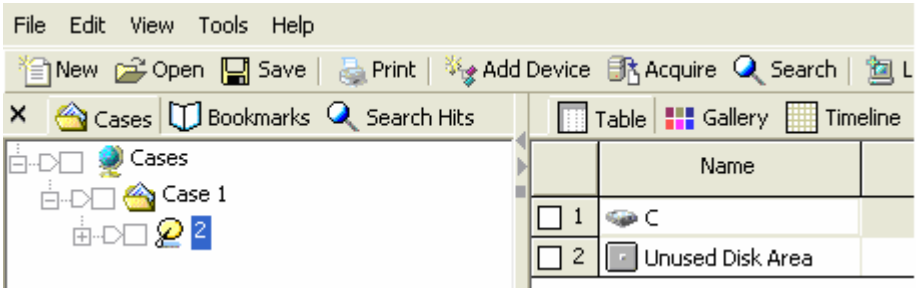


Иллюстрация №14. Главное окно программы Encase с подключенным образом накопителя.

При монтировании образа накопителя автоматически происходит проверка его целостности. При этом в правом нижнем углу программы Encase отображается ход прохождения процесса верификации и примерное время оставшееся до его окончания.


Иллюстрация №15. Отображение хода прохождения процесса верификации.

Если в ходе процесса верификации будет установлено, что образ накопителя поврежден, об этом будет выдано соответствующее сообщение.

4.Подключение флэш-накопителя и создание его образа.

(рекомендуется предварительно ознакомиться с содержанием Руководства пользователя Encase Forensic Edition 4 страницы 76,77).

Для подключения флэш-накопителя в Encase необходимо проделать последовательно шаги, описанные в разделах 1. Подготовка к производству исследования и 2. Подключение накопителей. После этого, мы увидим в Encase подключенный флэш-

накопитель. Для того чтобы получить его образ, необходимо кликнуть на накопителе правой клавишей мыши и в появившемся меню выбрать «Acquire…».

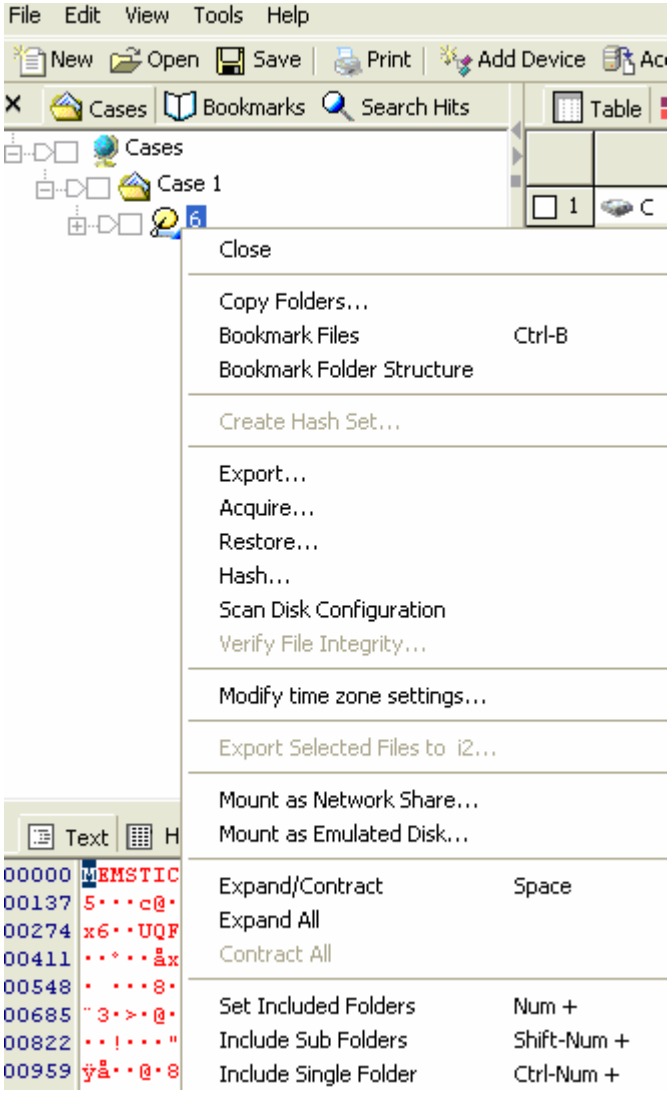


Иллюстрация №16. Опции доступные для подключенного носителя в программе Encase.

В появившемся окне «Option» необходимо задать параметры создаваемого образа

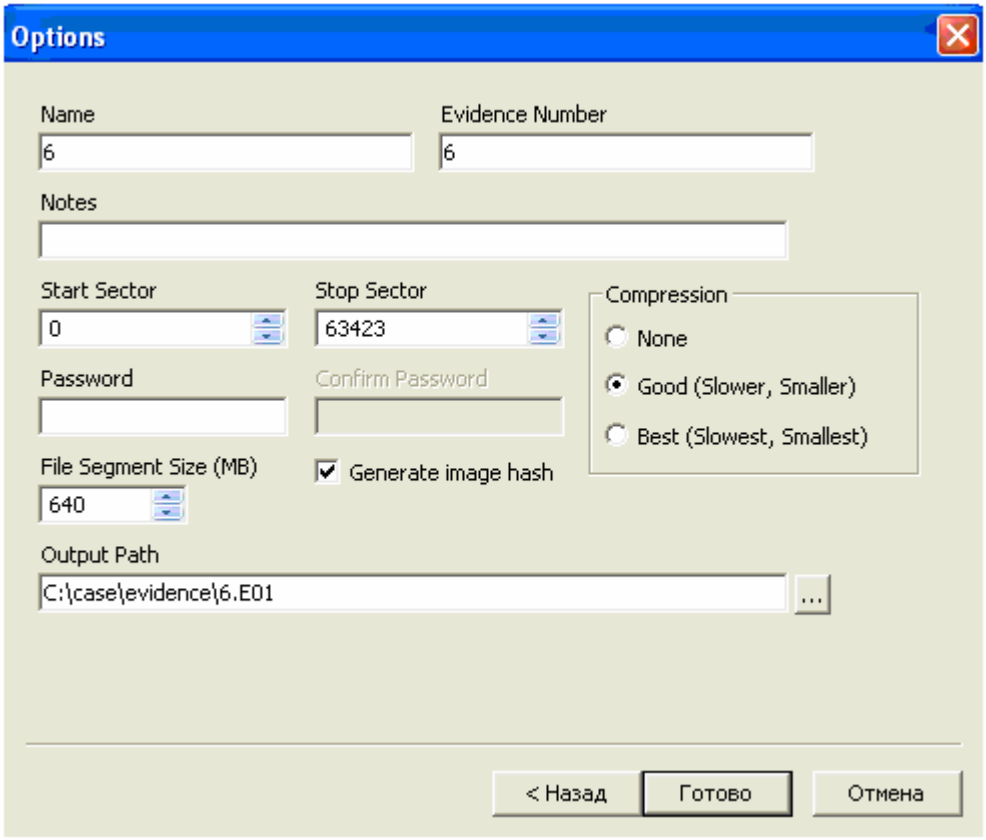


Иллюстрация №17. Окно «Option» программы Encase.

Наиболее значимые:

Compression – степень сжатия создаваемого образа (рекомендуется «Good»);

File Segment Size – размер фрагмента файла образа накопителя (рекомендуется установить значение 2000);

Output Path - путь до подкаталога evidence каталога case (6.E01 – имя и расширение создаваемого образа).

5.Работа с делом.

Для того, чтобы просмотреть: какие логические разделы и файлы находятся на исследуемом накопителе, необходимо кликнуть на значке «+», расположенном возле него. Выбрав нужный логический раздел, можно просмотреть файлы и папки, расположенные на нем.

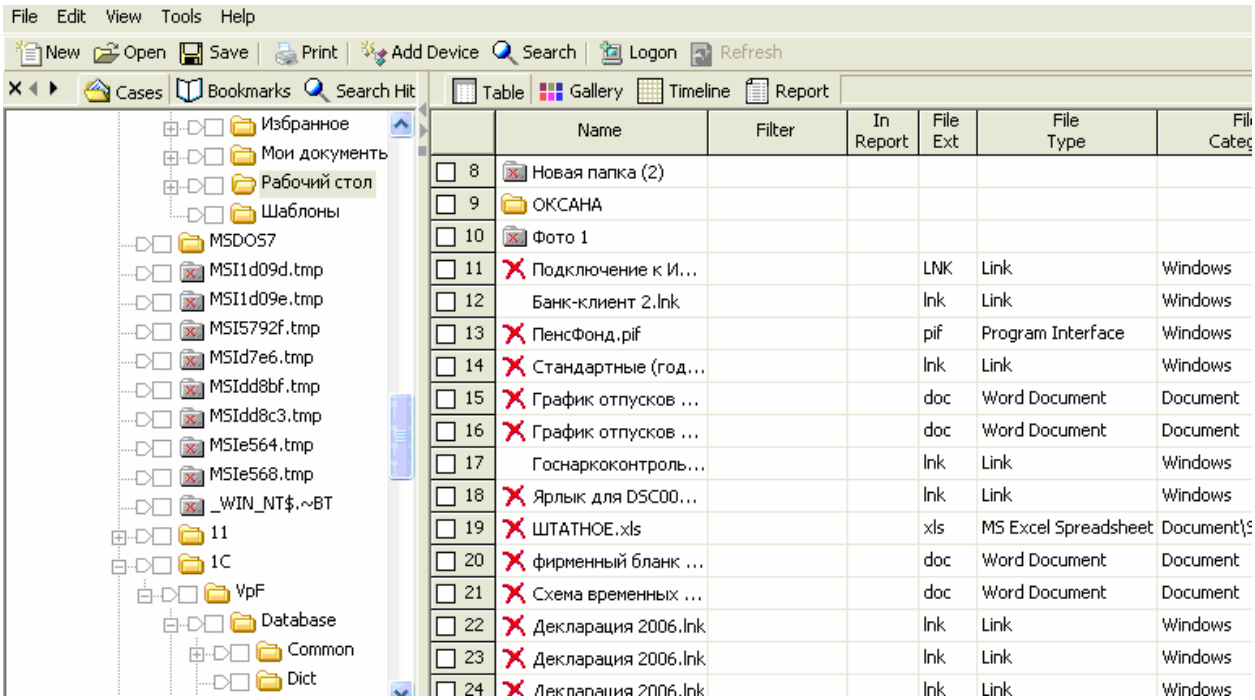


Иллюстрация №18. Фрагмент главного окна программы Encase в котором отображаются: слева – каталоги, находящиеся в логическом разделе исследуемого накопителя, справа – файлы, находящиеся на исследуемом накопителе.

При отображении файлов, encase использует систему условных обозначений (см.также страницу 107 Руководства пользователя Encase Forensic Edition 4). Так:

- значок ⊘ показывает исследователю, что файл удален, но, тем не менее, файл может быть восстановлен;

- значок ✕ показывает исследователю, что файл удален и частично перезаписан.

Тем не менее, возможно получить частичный доступ к данным, находившимся в нем. Так в примере показано, что хотя файл autoexec.bat помечен как удаленный, можно просмотреть текстовые данные, находившиеся в нем:

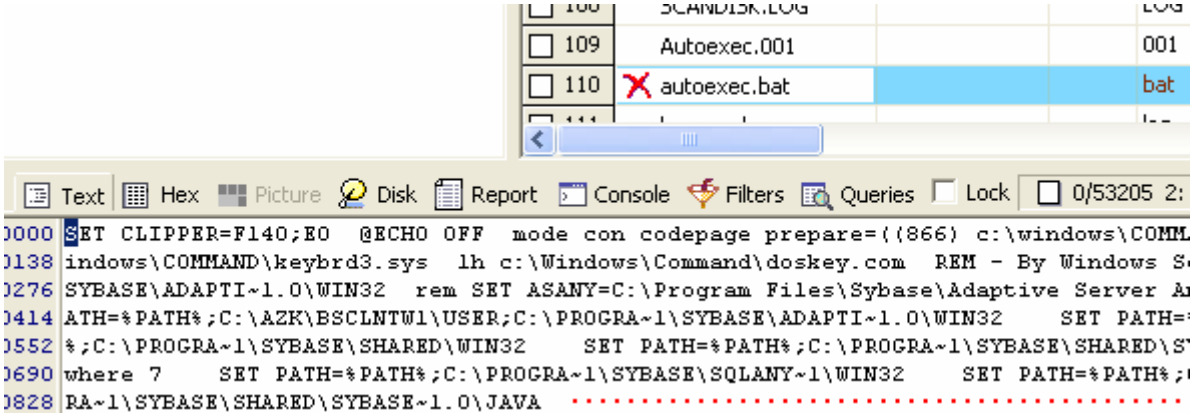


Иллюстрация №19. Просмотр содержимого удаленного и частично перезаписанного файла в программе Encase.

- значок  показывает исследователю, что удаленный файл восстановлению не подлежит.

6.Работа с графикой.

Для того чтобы просмотреть все графические файлы, присутствующие на накопителе необходимо сделать следующее:

Установить зеленый значок рядом с обозначением накопителя и выбрать вкладку «Gallery» в главном окне программы Encase.

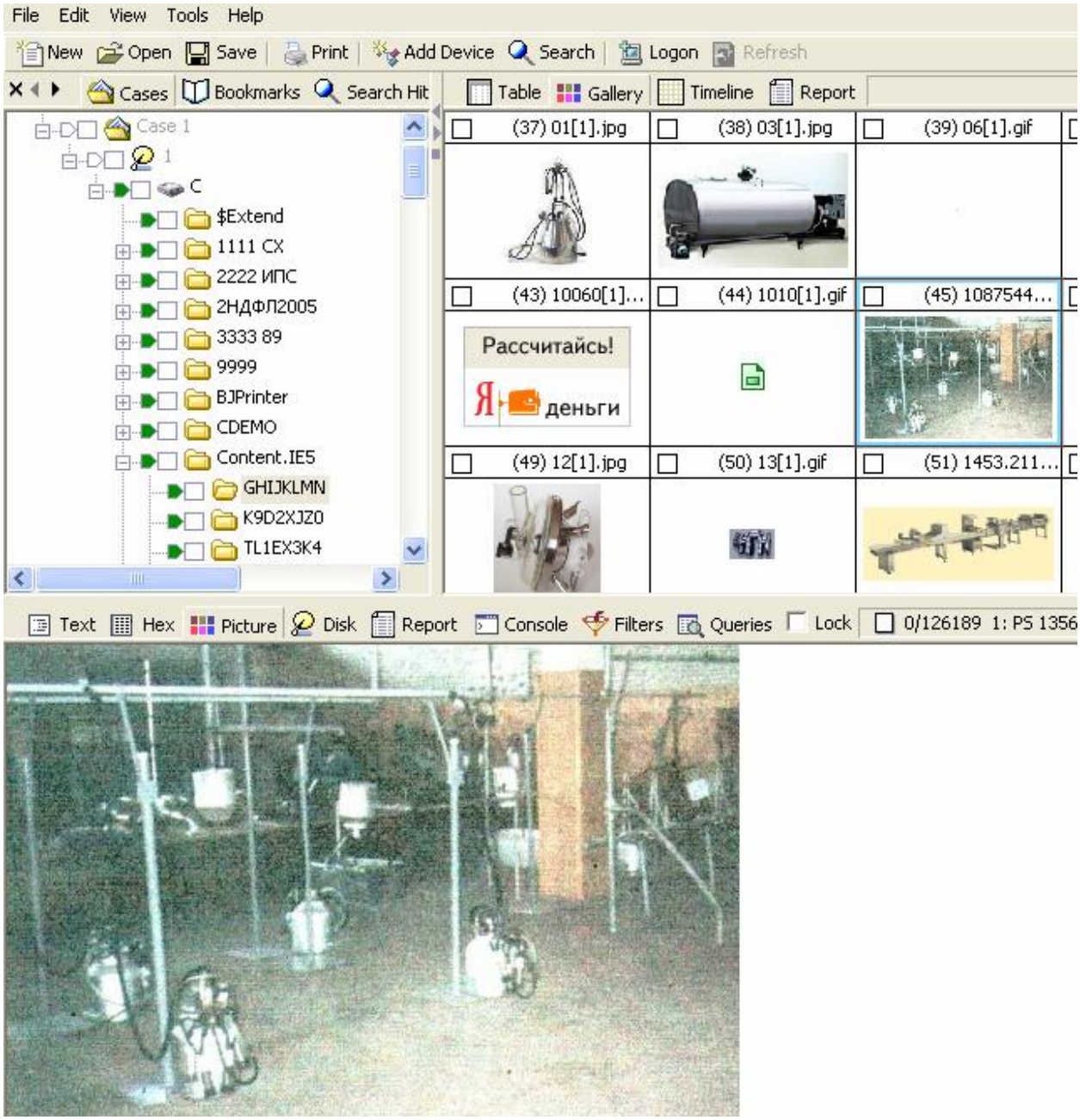


Иллюстрация №20. Просмотр графических изображений, в программе Encase, на исследуемом носителе.

При этом Encase в правом верхнем окне отобразит все присутствующие на накопителе графические изображения ( в том числе и удаленные) в виде эскизов. Само изображение, в случае выбора, отображается в нижнем окне. В Encase версий 6.3 и выше доступен просмотр векторных изображений и файлов Corel Draw.

7.Восстановление графических изображений.

7.1.Экспорт графических файлов из дела.

Выбранные графические изображения могут быть экспортированы из дела. Для этого необходимо выбрать интересующие изображения, которые находятся в явном или удаленном виде, установив галочку в левом верхнем углу эскиза изображения. Затем нужно кликнуть правой клавишей мыши и в появившемся меню выбрать опцию «Copy/UnErase».

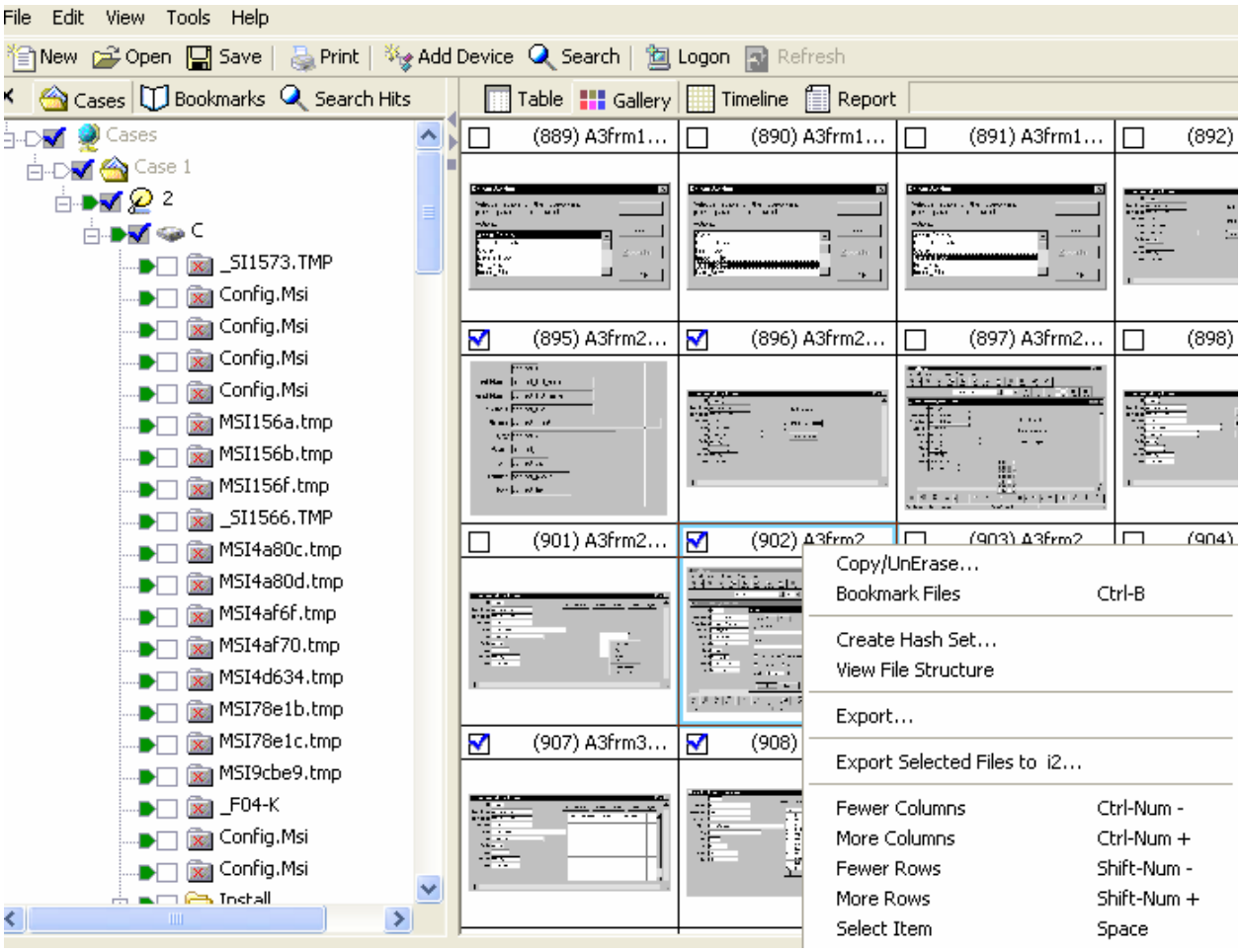


Иллюстрация №21. Экспорт графических изображений из программы Encase.

В появившемся окне нужно нажать кнопку « Далее», затем еще раз « Далее». В окне «Destination» прописать путь до подкаталога export каталога case. И нажать кнопку «Готово».

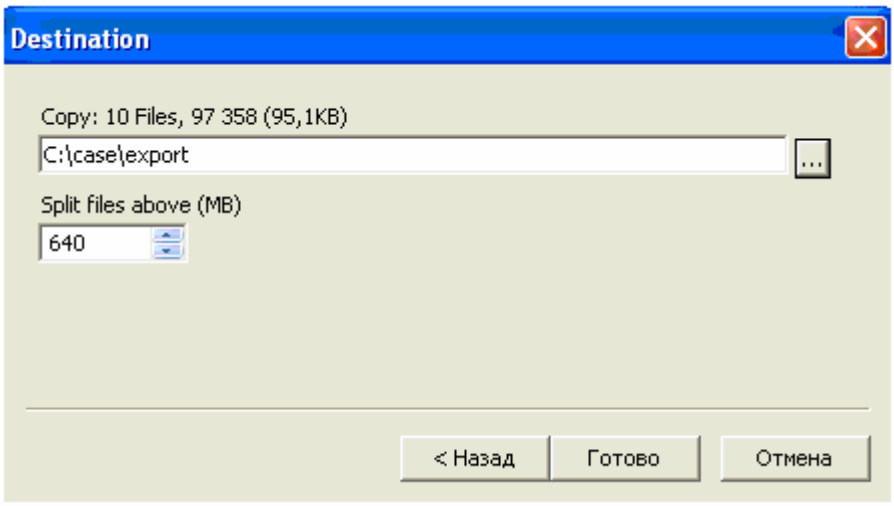


Иллюстрация №22. Опции экспорта графических изображений из программы Encase.

Для экспорта свойств копируемых/восстанавливаемых файлов нужно: кликнуть правой клавишей мыши и в появившемся меню выбрать опцию «Export».

В появившемся окне необходимо указать: какие сведения о файлах необходимо экспортировать, путь и имя файла, в который будут экспортированы данные (созраняются в формате txt).

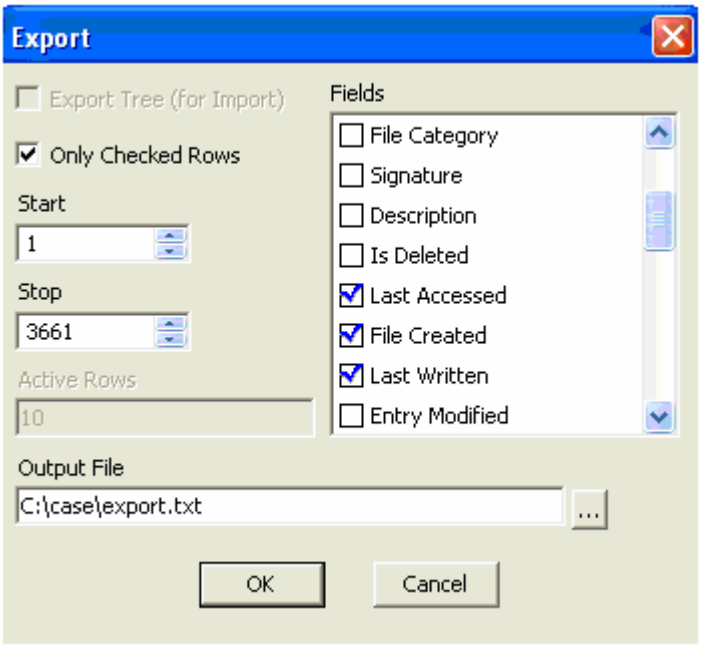


Иллюстрация №23. Опции экспорта свойств файлов из программы Encase.

Наиболее значимые позиции:

Only Checked Rows – экспортировать данные только для выбранных файлов;

Name - имя файла;

Last Accessed –дата/время последнего доступа к файлу;

File Created – дата/время создания файла;

Last Written - дата/время последней записи в файл;

Logical Size – логический размер (в байтах);

Full Path – полный путь до файла (включая имя файла).

Важно: При повторном экспорте данных о файлах, содержимое файла export.txt перезаписывается без предупреждения.

7.2.Восстановление графических файлов из свободных областей.

Для восстановления графических файлов из свободных областей (т.е. файлов, о которых отсутствуют сведения в файловой системе) используется подпрограмма, написанная на языке Enscript - File Finder.

Кликните «View» и установите галочку напротив «Scripts».

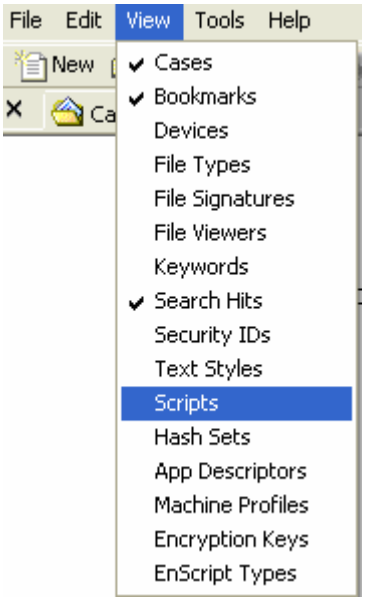


Иллюстрация №24. Выбор «Scripts» в меню «View» программы Encase.

При этом в программе появится вкладка «Scripts». Необходимо развернуть список находящихся в ней подпрограмм и дважды кликнуть на названии подпрограммы «File Finder»:

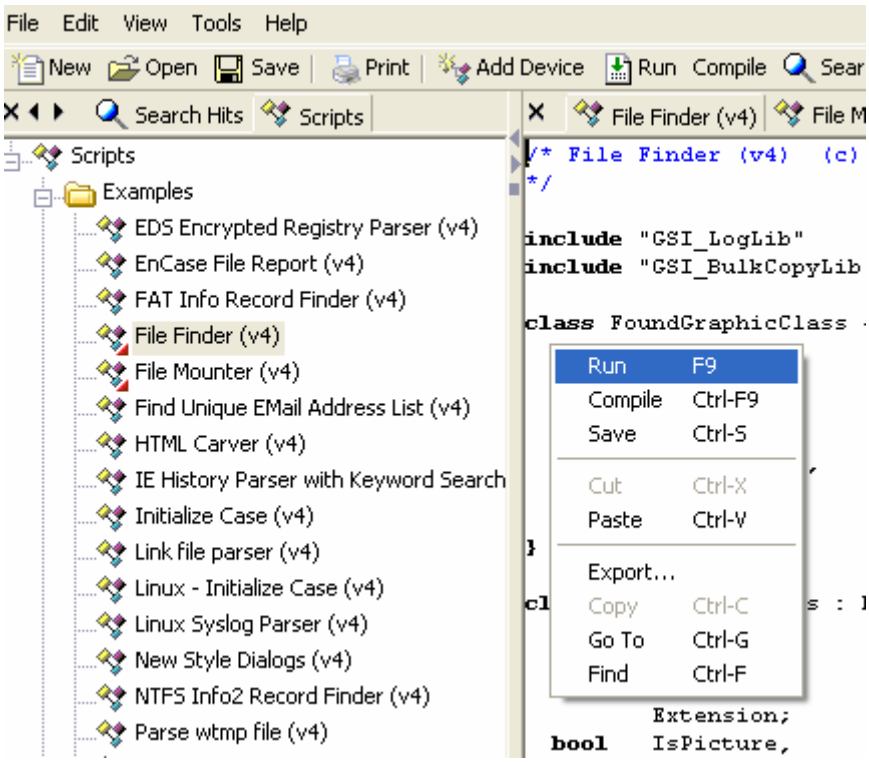


Иллюстрация №25. Запуск подпрограммы File Finder.

Затем кликнуть на тексте подпрограммы правой клавишей мыши и в появившемся меню кликнуть по опции «Run». Откроется окно настройки параметров поиска. В разделе «File Types» необходимо указать: какой тип файлов будет нужно найти. Необходимо установить галочку напротив «Export Files» для экспорта найденных файлов в подкаталог Export каталога case. Затем нажать кнопку «ОК».

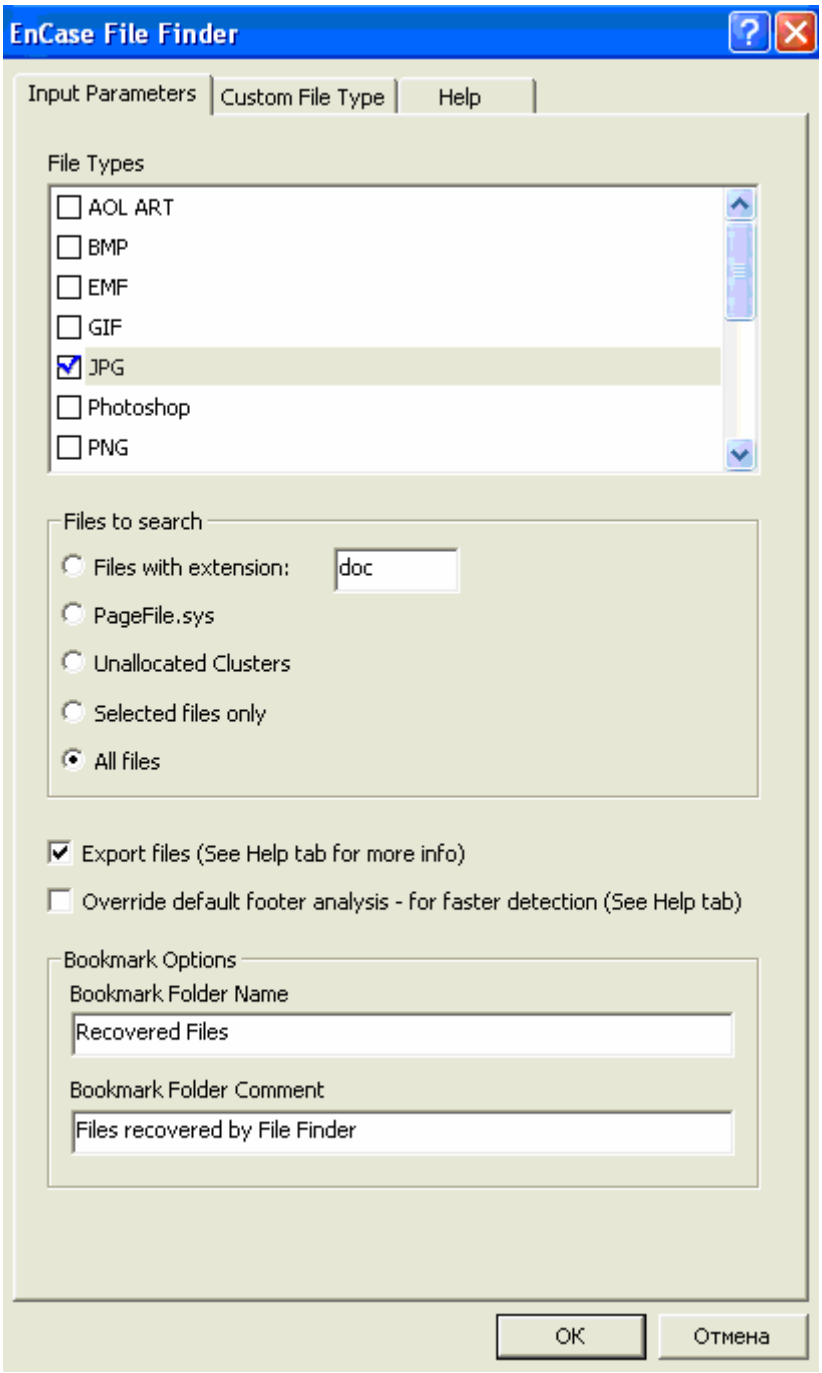


Иллюстрация №26. Установка параметров извлекаемых данных в подпрограмме File Finder.

В следующем окне устанавливаем параметры:

Auto-export size – т.е. если программа найдет сигнатуру начала файла (header), но не найдет сигнатуру окончания файла (footer), она «отрежет» от сигнатуры начала файла фрагмент, равный значению, указанному в этой строке ( для графических файлов рекомендуется выставлять значение не менее 10Мб);

Directory to copy to – путь до подкаталога «Export» каталога case куда будут экспортироваться найденные файлы;

Max size of a dir - размер директории, в которую помещаются извлекаемые файлы. Максимальное значение 1024 Мб. При извлечении файлов, объем которых превышает указанный параметр, создается несколько директорий (с названиями: Export-1, Export-2 … и т.д.), размер каждой из которых не превышает заданный параметр «Max size of a dir».

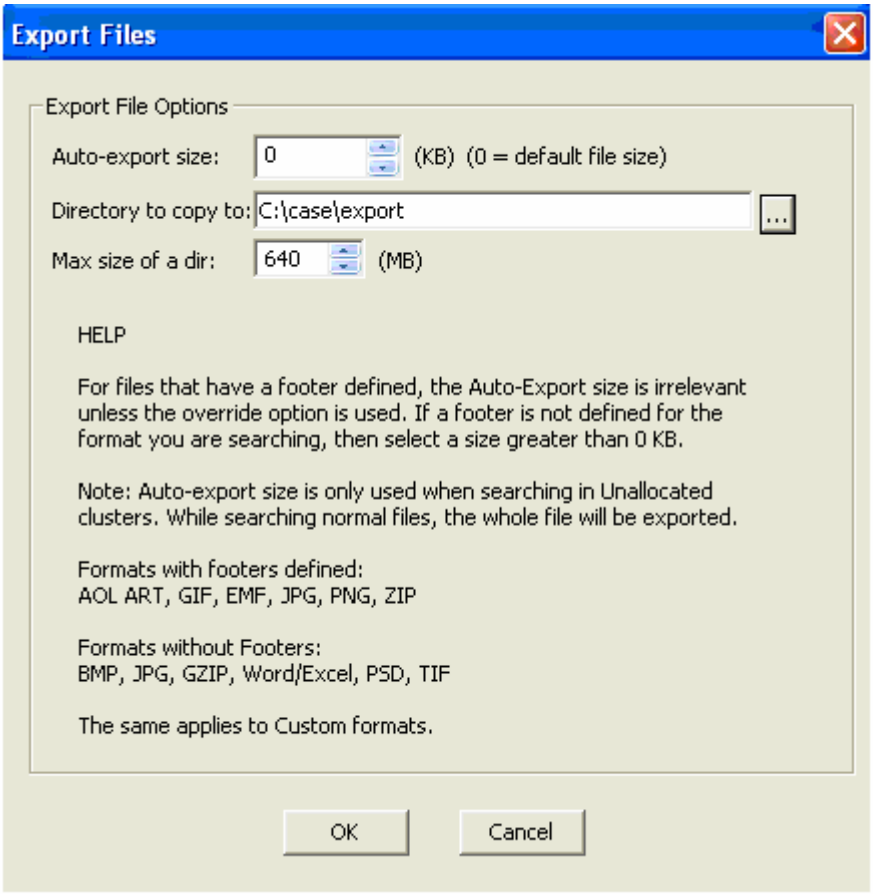


Иллюстрация №27. Установка параметров куда должны быть извлечены данные подпрограммой File Finder.

8.Поиск текста.

Для поиска фрагмента текста по ключевым словам, необходимо сначала задать список ключевых слов ( поиск производится по всем заданным ключевым словам одновременно).

Кликните View и установите галочку напротив Keywords

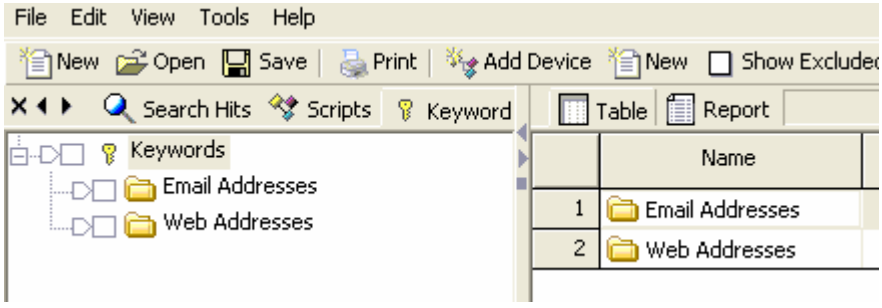

Иллюстрация №28. Выбор «Keywords» в программе Encase.

Затем во вкладке Keywords, необходимо кликнуть правой клавишей мыши и задать новые ключевые слова.

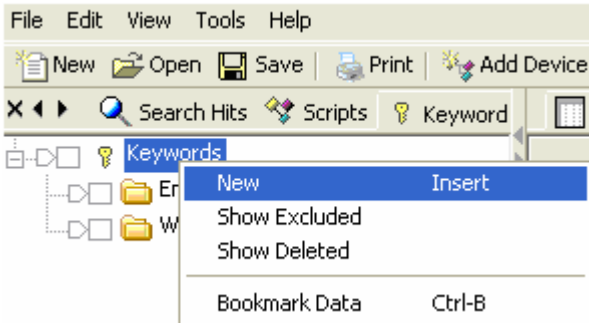


Иллюстрация №29. Создание нового ключевого слова в программе Encase.

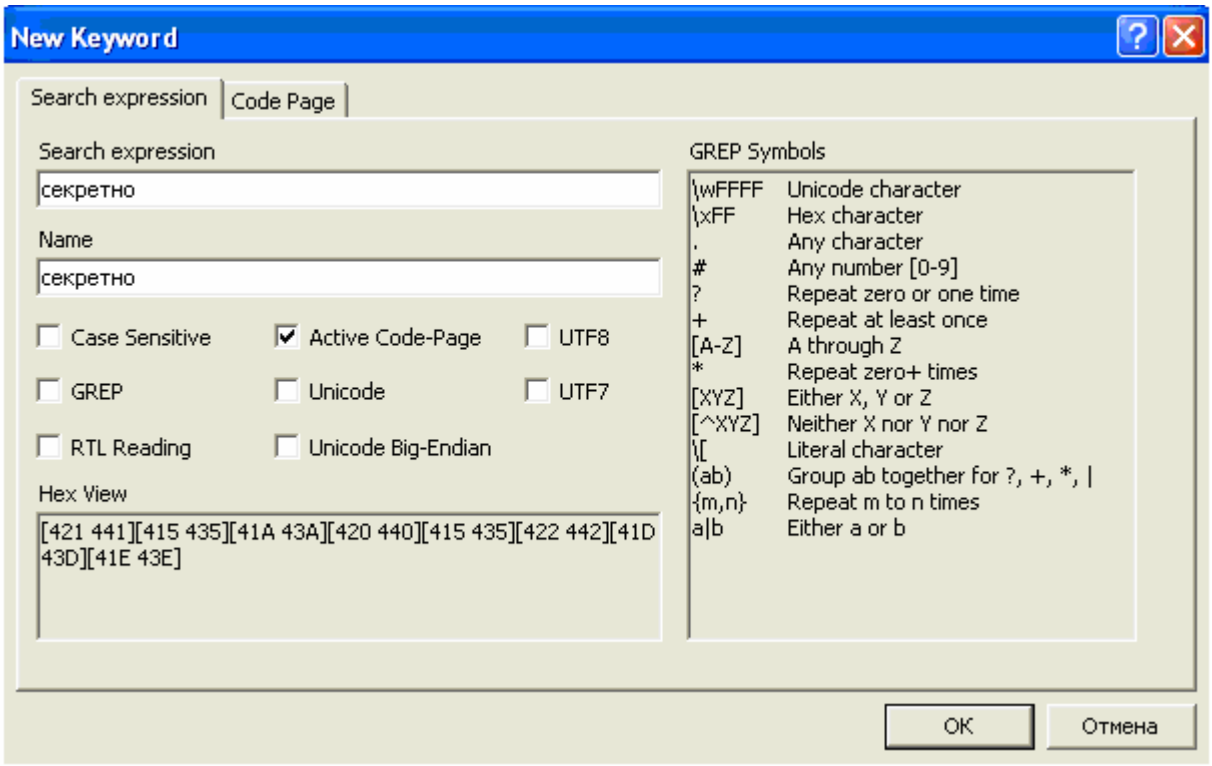


Иллюстрация №30. Установка параметров нового ключевого слова в программе Encase.

Затем необходимо выбрать ключевые слова, по которым необходимо произвести поиск,

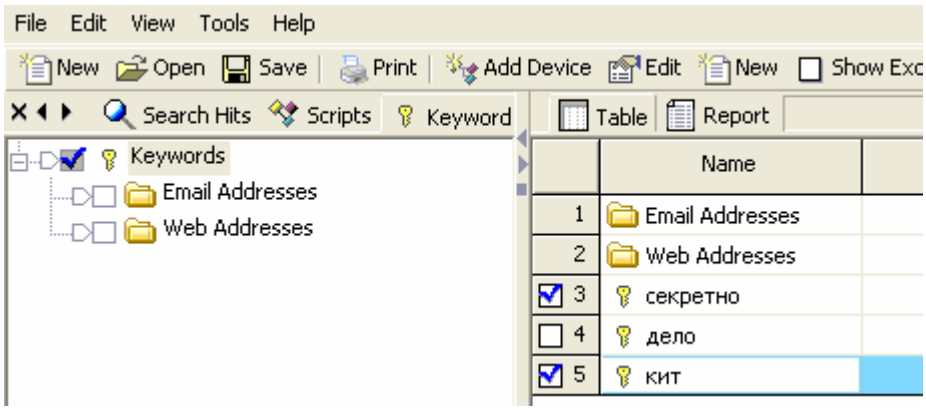


Иллюстрация №31. Выбор ключевых слов, по которым будет произведен поиск.

и кликнуть «Search»


Иллюстрация №32. Панель инструментов программы Encase.

В появившемся окне необходимо установить галочку напротив «Selected keywords only» (провести поиск только по выбранным ключевым словам) и нажать кнопку «Start».

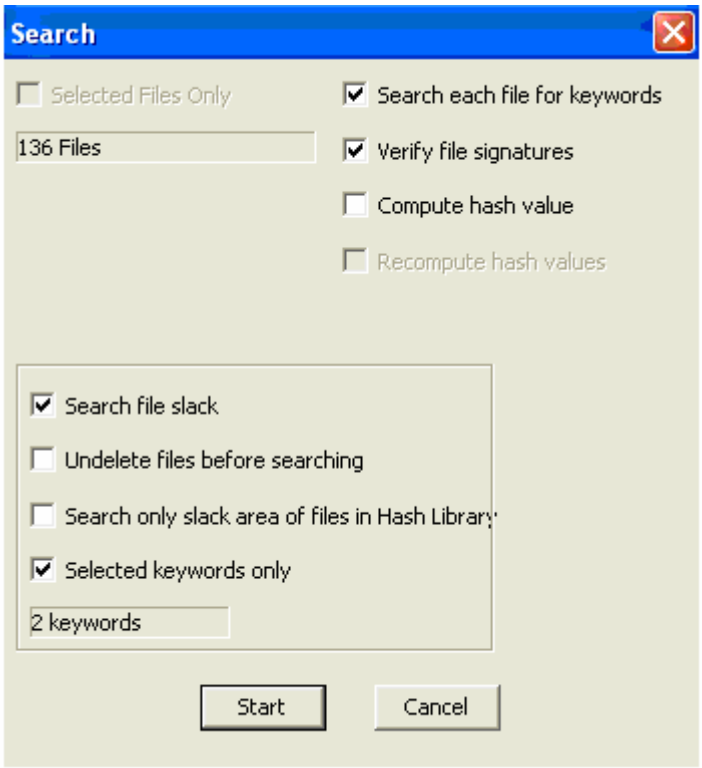


Иллюстрация №33. Задание параметров поиска по ключевым словам в программе Encase.

После производства поиска, результаты поиска можно просмотреть во вкладке «Search Hits».

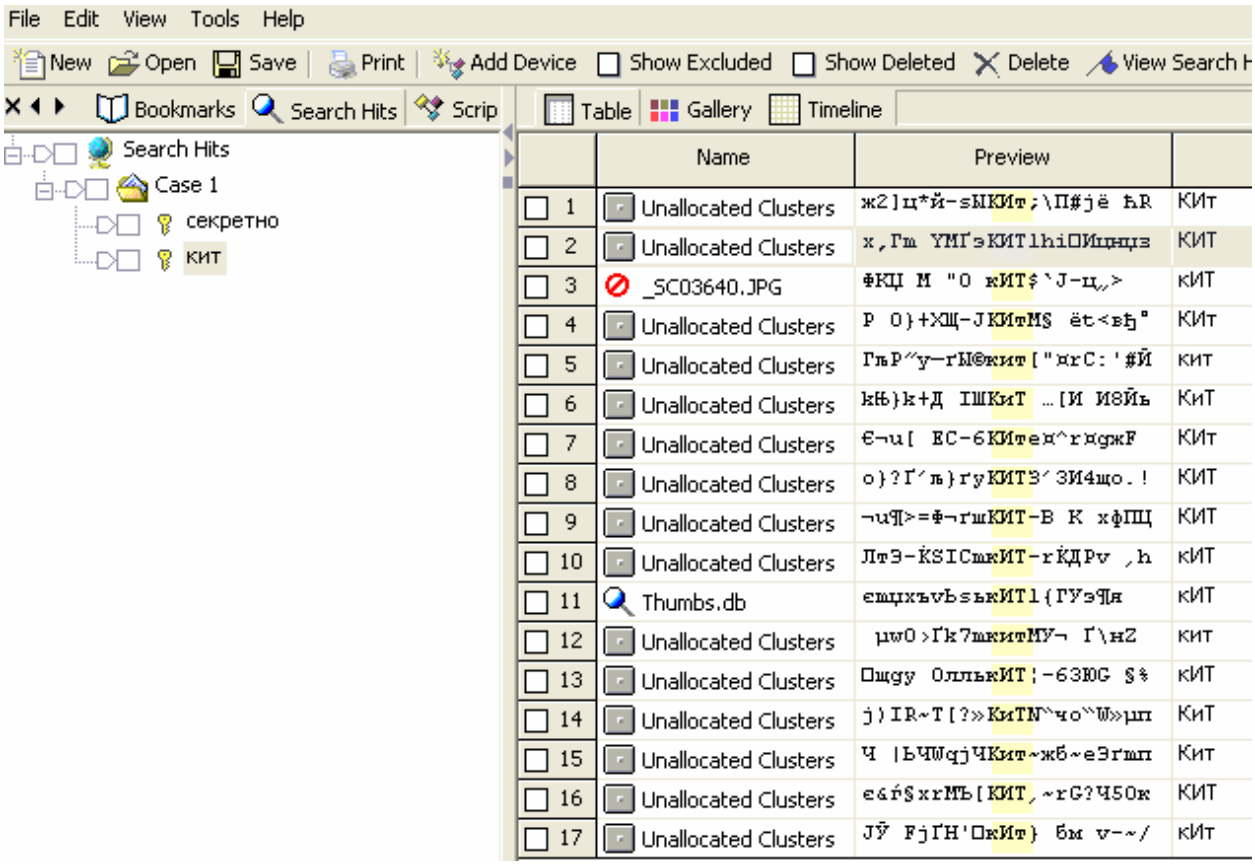


Иллюстрация №34. Просмотр результатов поиска по ключевым словам в программе Encase.

Часто наблюдается ситуация, когда в строке «Preview» отображается искомый текст на русском языке,а в окне просмотра ( нижнее окно) кириллица отображается не верно.

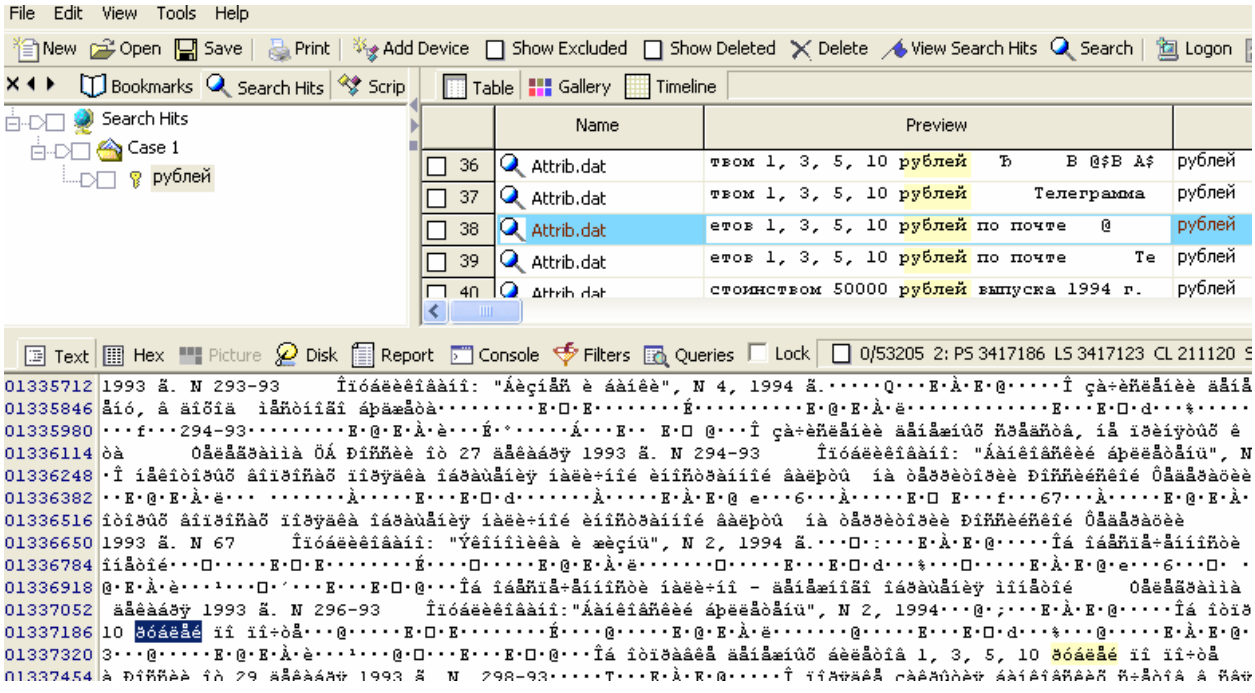


Иллюстрация №35. Неверное отображение кириллических символов в программе Encase.

Это происходит из-за того, что в программе, установленной по умолчанию, не подключены кириллические шрифты. Для их подключения нужно кликнуть «View» и установить галочку напротив «Text Styles». В левом верхнем окне кликнуть правой клавишей мыши и в появившемся меню выбрать New.

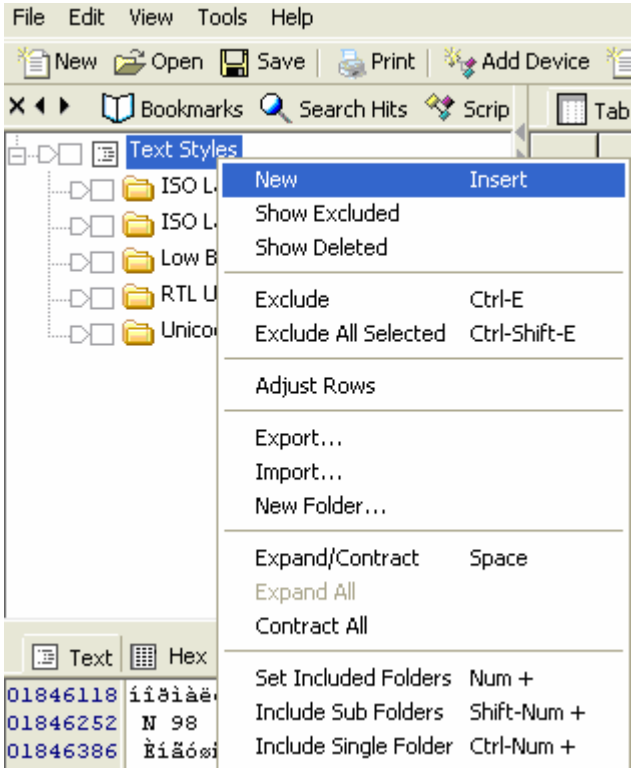


Иллюстрация №36. Подключение нового шрифта в программе Encase.

В появившемся окне «New Test Style» открыть вкладку «Code Page», выбрать «Other». В активировавшемся окне выбрать «ANSI – кириллица 1251», нажать кнопку «ОК».

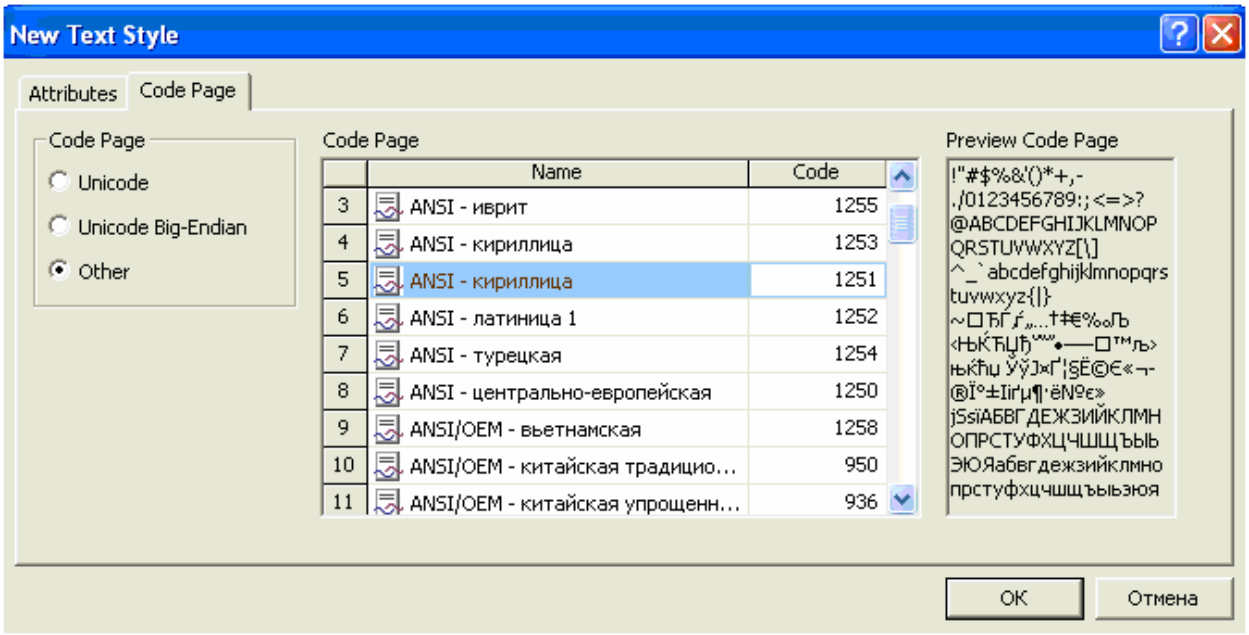


Иллюстрация №37. Выбор нового шрифта.

При этом текст в нижнем окне будет отображаться на кириллице.

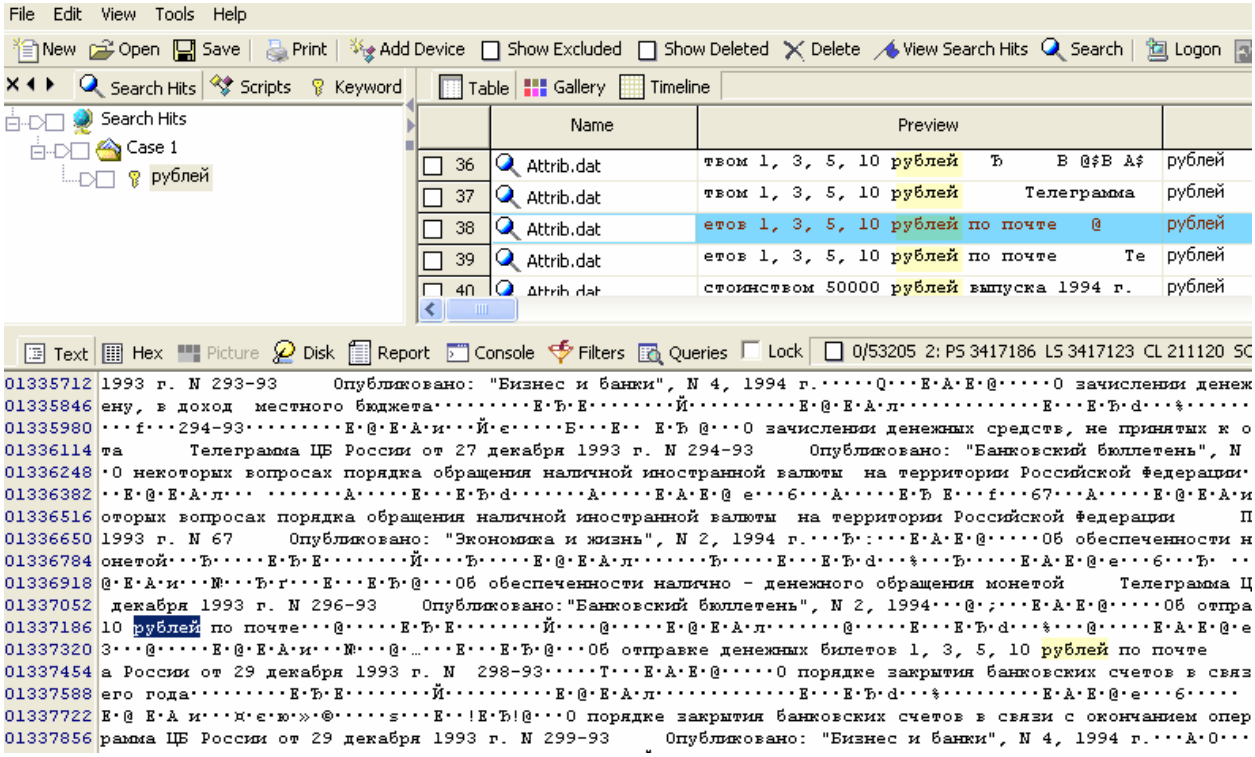


Иллюстрация №38. Верное отображение кириллических символов в программе Encase.

Заключение.

На этом мы хотим закончить нашу первую статью, посвященную описанию использования программы Encase в экспертной практике. Надеемся, что сведения, изложенные в работе, позволят экспертам максимально быстро приступить к работе с этой программой и максимально полно использовать ее возможности при производстве судебных экспертиз и исследований.