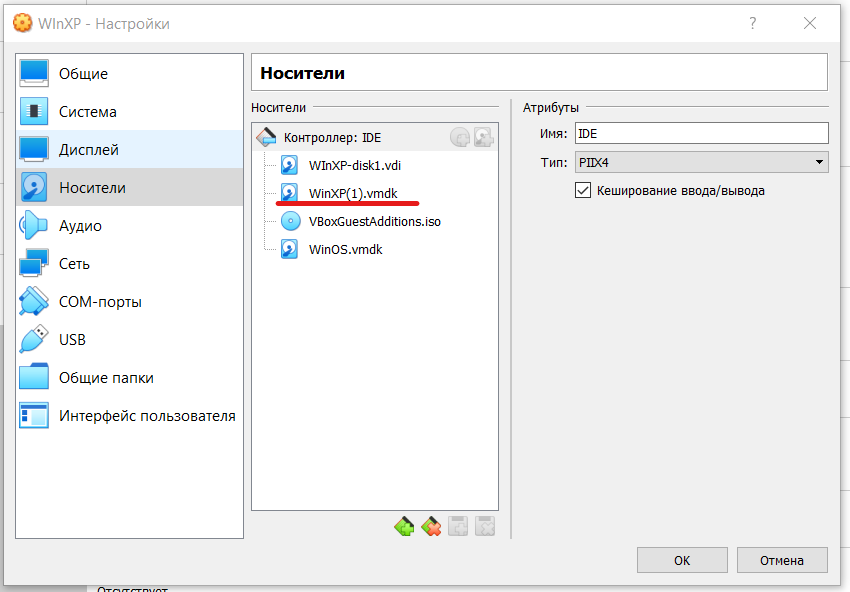
**Вариант №2**

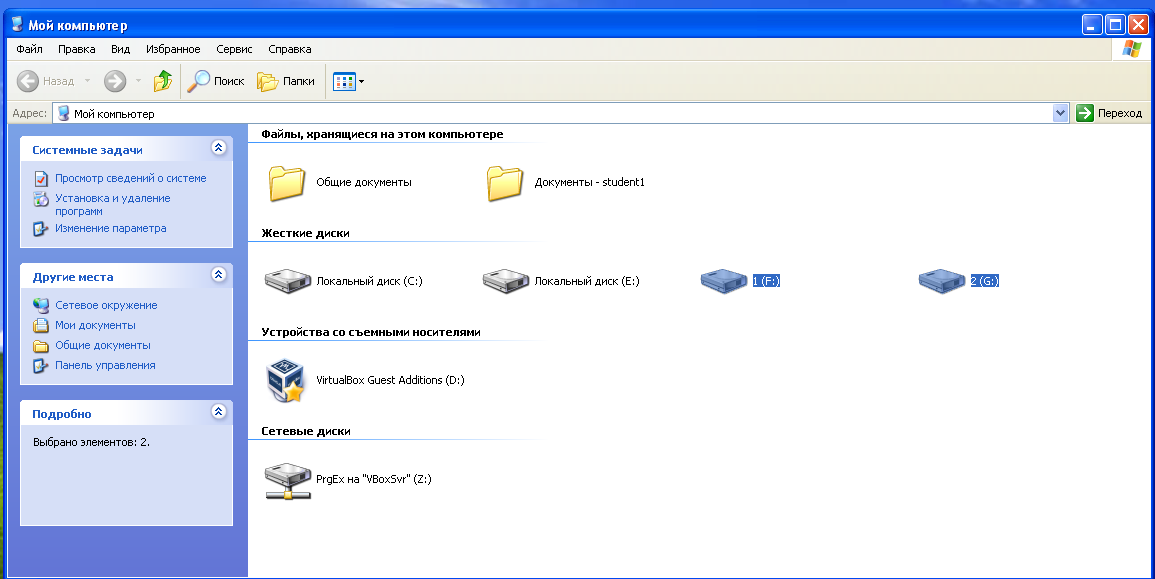
Работу выполнил студент 431гр. Никитин А.В.

**WinXP(1)**

Перед началом работы подключил исследуемый носитель к виртуальной машине:

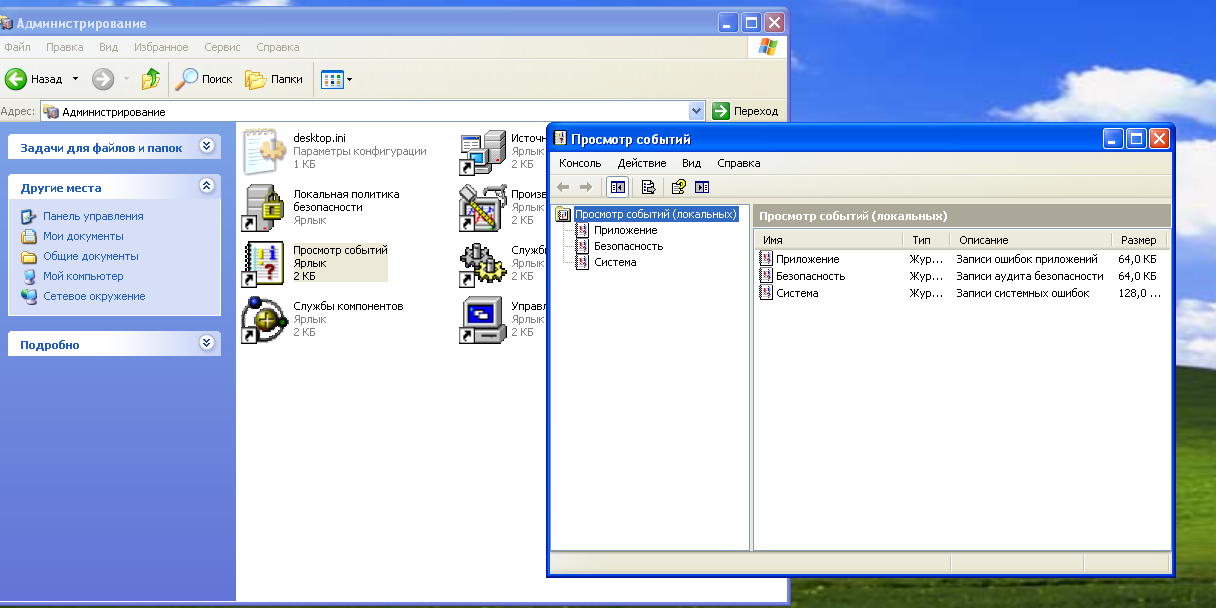


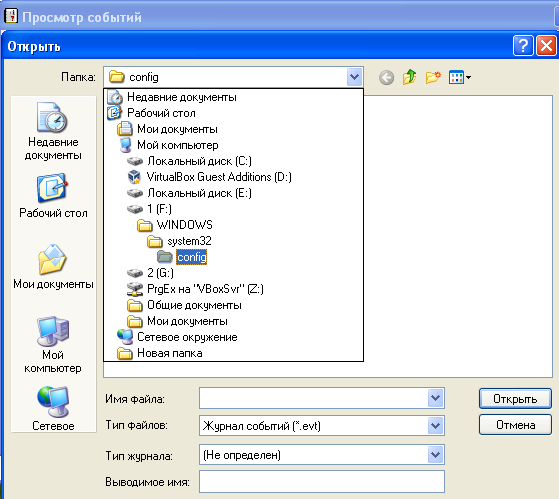
Носитель успешно инициализировался системой:



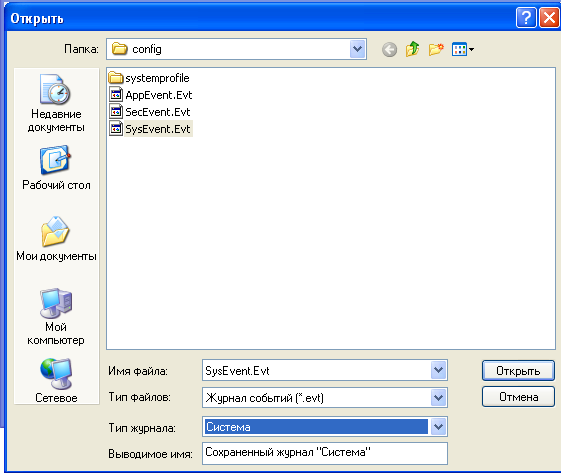
1. **Когда производился последний запуск представленного экземпляра ОС?**

Для выполнения данного задания буду использовать встроенную в виндовс оснастку (Просмотр событий):

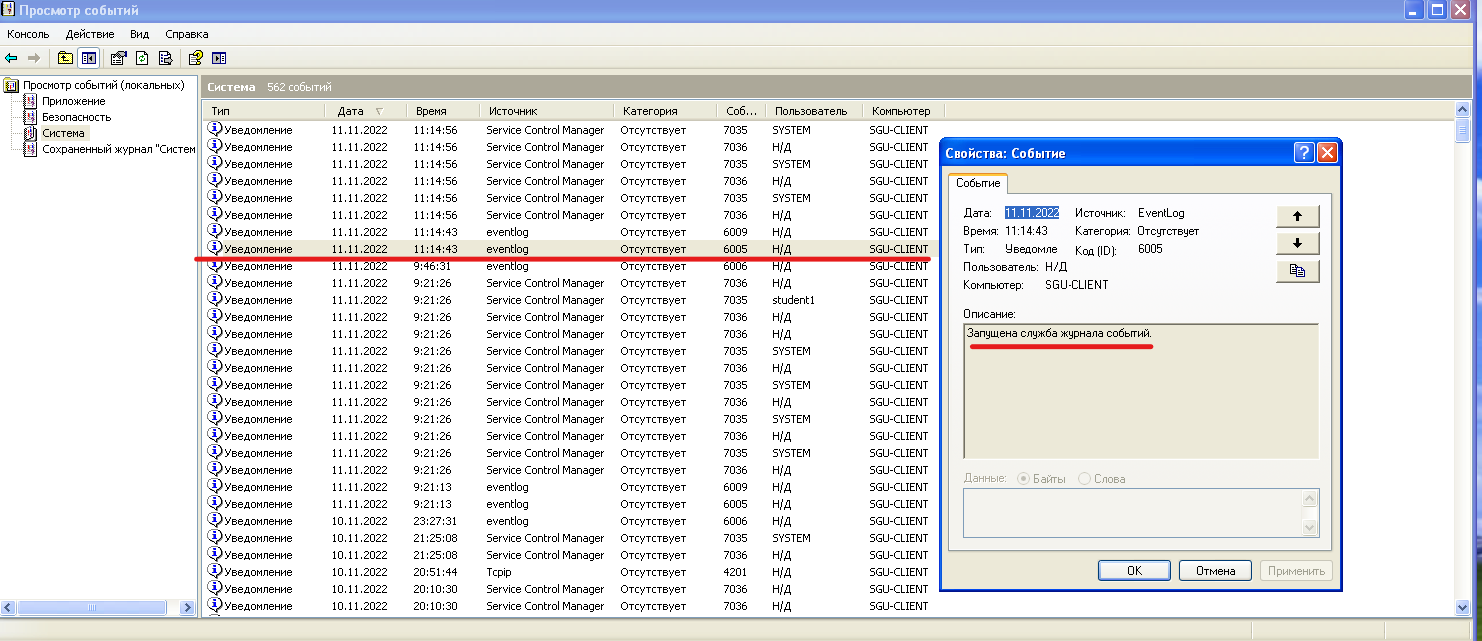
Подключаю к приложению файл журнала событий системы с представленного носителя:



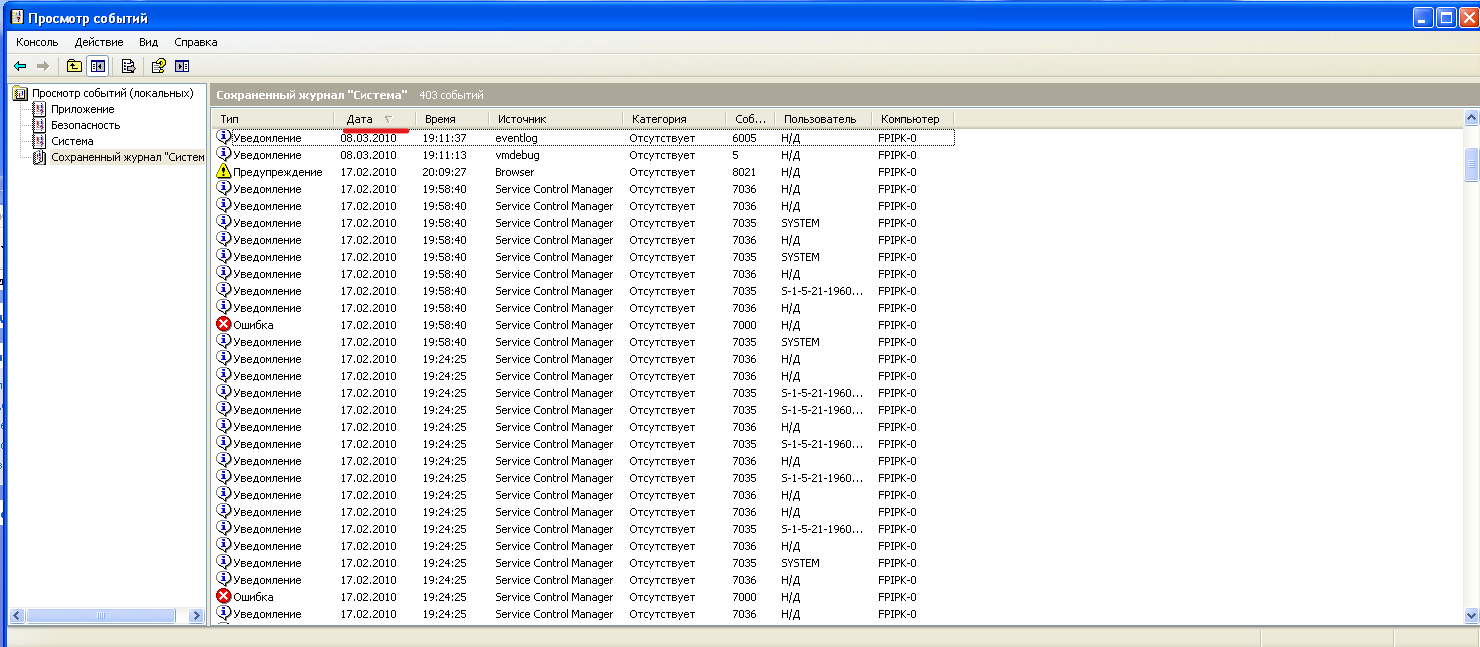
Сам журнал называется SysEvent.evt:



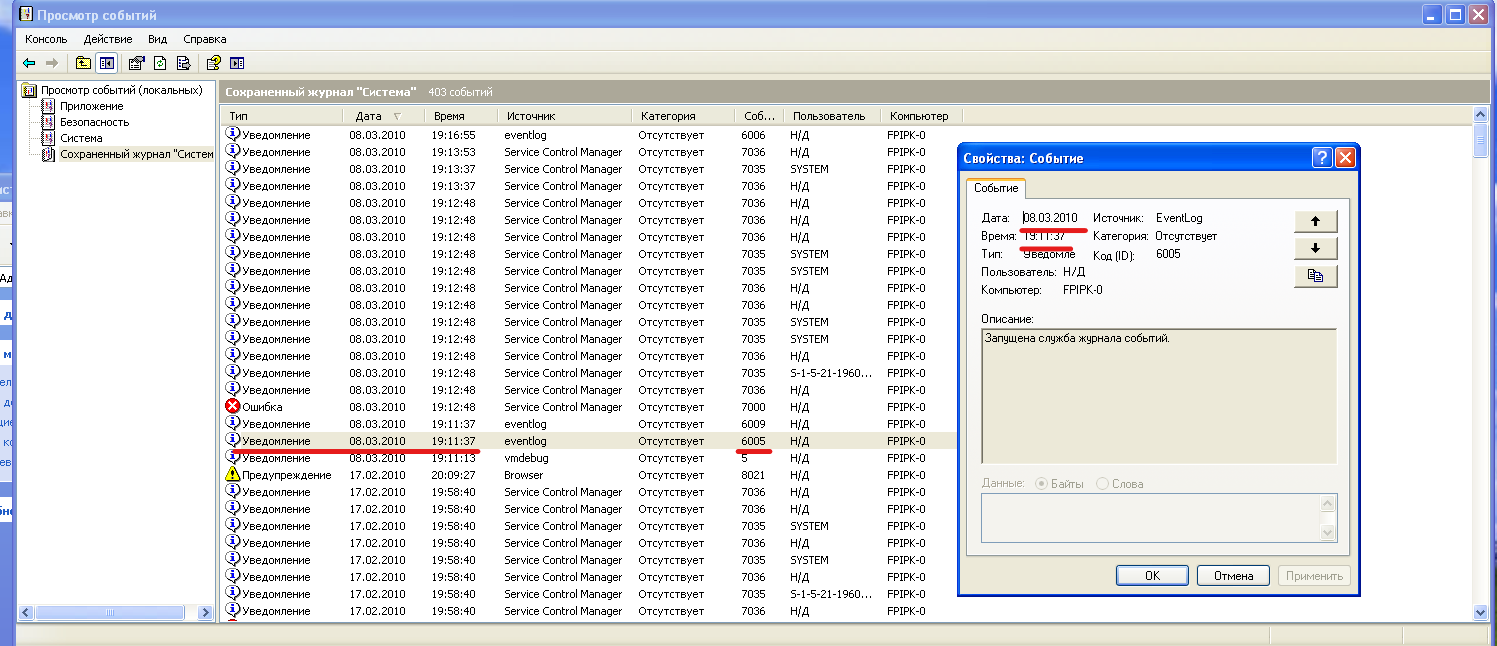
Запуск текущей сессии системы моего компьютера отображается как событие с кодом 6005 в моем журнале системы (отметил красным цветом):



Теперь рассмотрим журнал исследуемой системы. Для этого отсортировал журнал по дате и начал поиск интересующего события :



Первое найденное событие с кодом **6005** (запуск службы журнала событий):



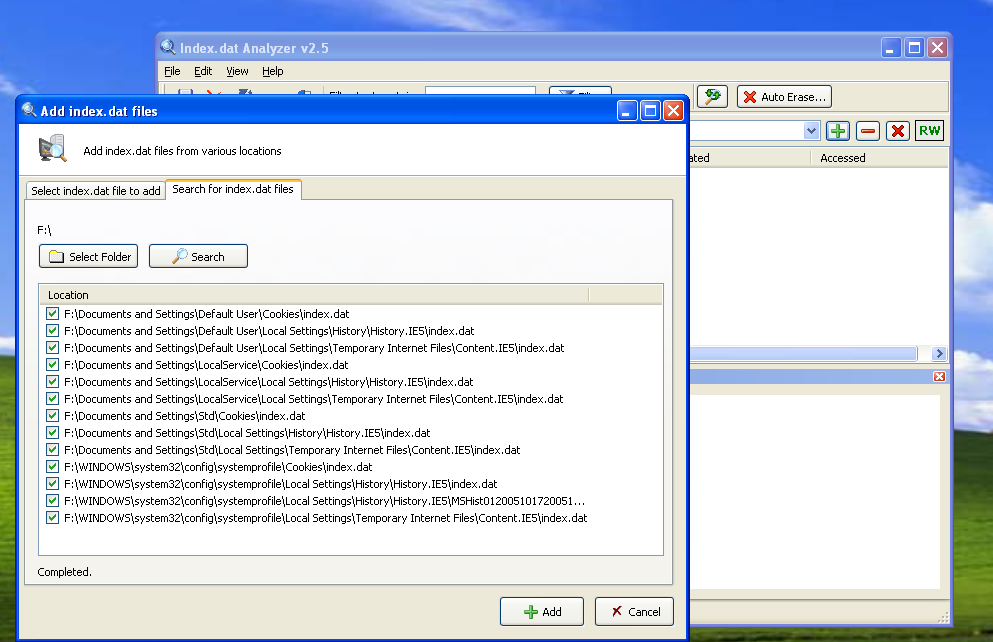
Значит делаю вывод, что **система в последний раз была запущена 08.03.2010 в 19:11:37.**

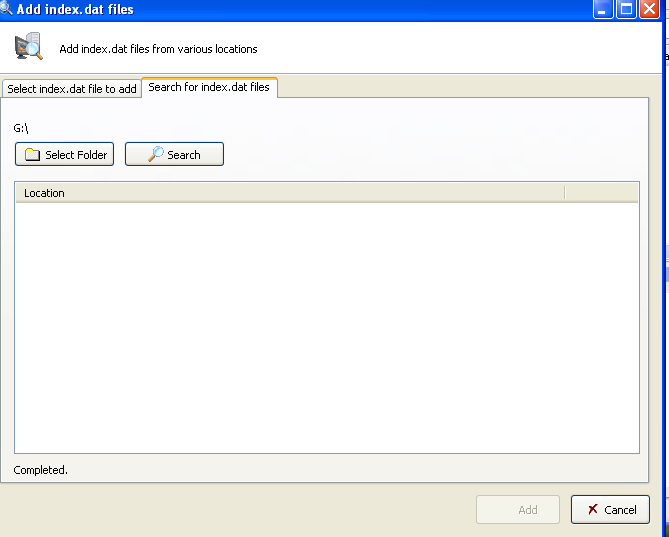
1. Осуществлялся ли выход в Internet в представленном экземпляре ОС (следы программного и аппаратного обеспечения)?

Для поиска следов использования Internet буду использовать программу IndexDat

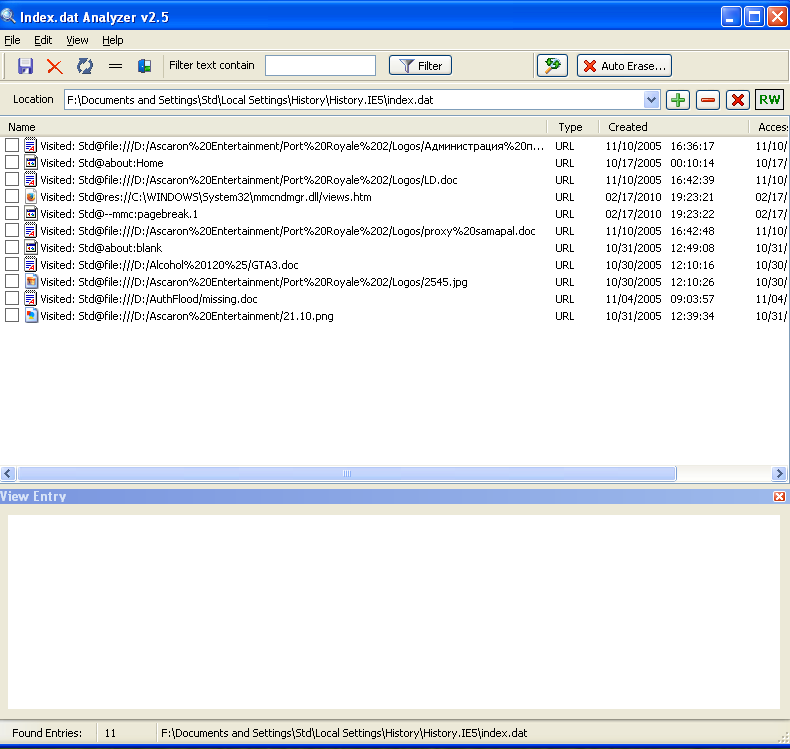
Analizer, в которой выполню поиск всех Index.dat файлов в обоих разделах диска:

На разделе 1 были найдены следующие файлы, в которых могут быть следы:

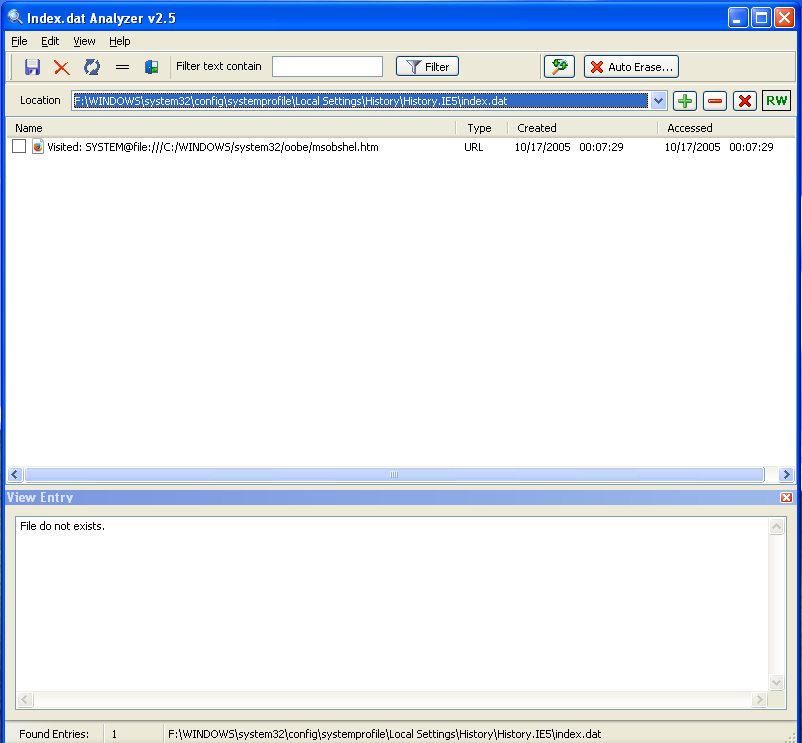


На втором разделе файлы, в которых могут быть следы, отсутствовали:

В файле History.IE5 свидетельства посещения интернет ресурсов не обнаружено:



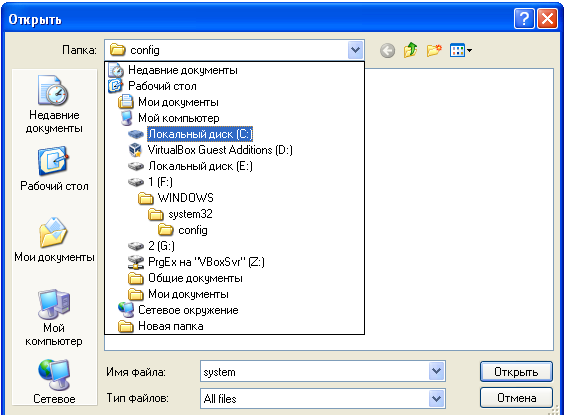
В другом файле также никаких следов:

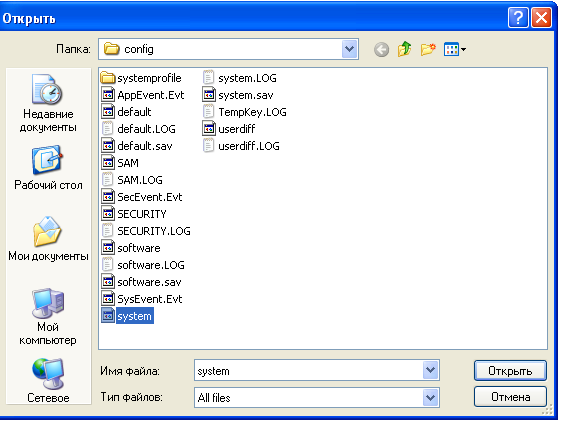


Также отмечу, что в других файлах вообще не было никакой информации.

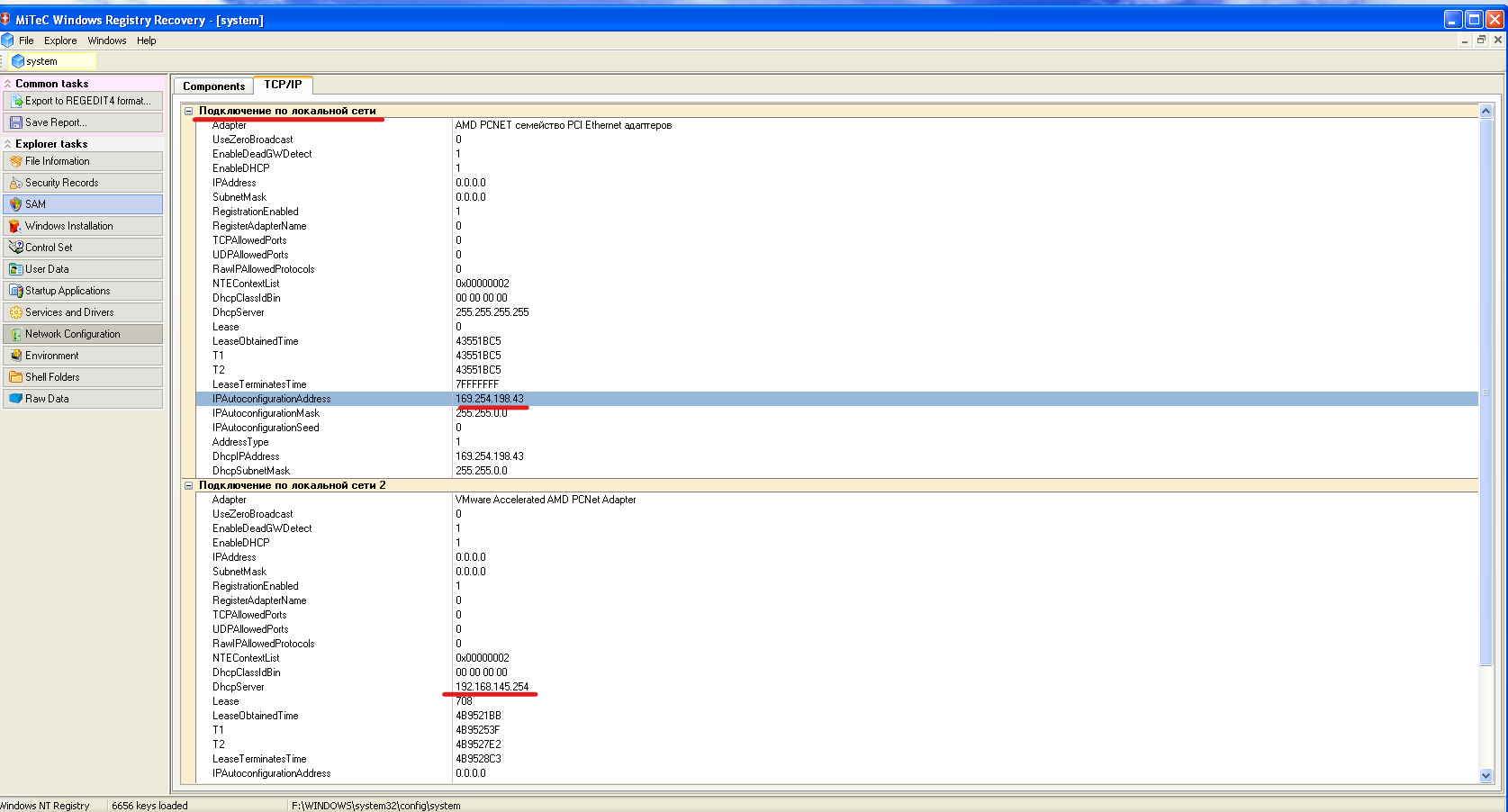
Затем попробовал найти хотя бы одну базу данных SQLite, содержащую какую-либо информацию о посещениях интернет ресурсов, но ни одна база данных найдена не была.

Что касается аппаратного обеспечения, то воспользуюсь программой Windows Registry Recovery и подключусь к реестру исследуемого диска:

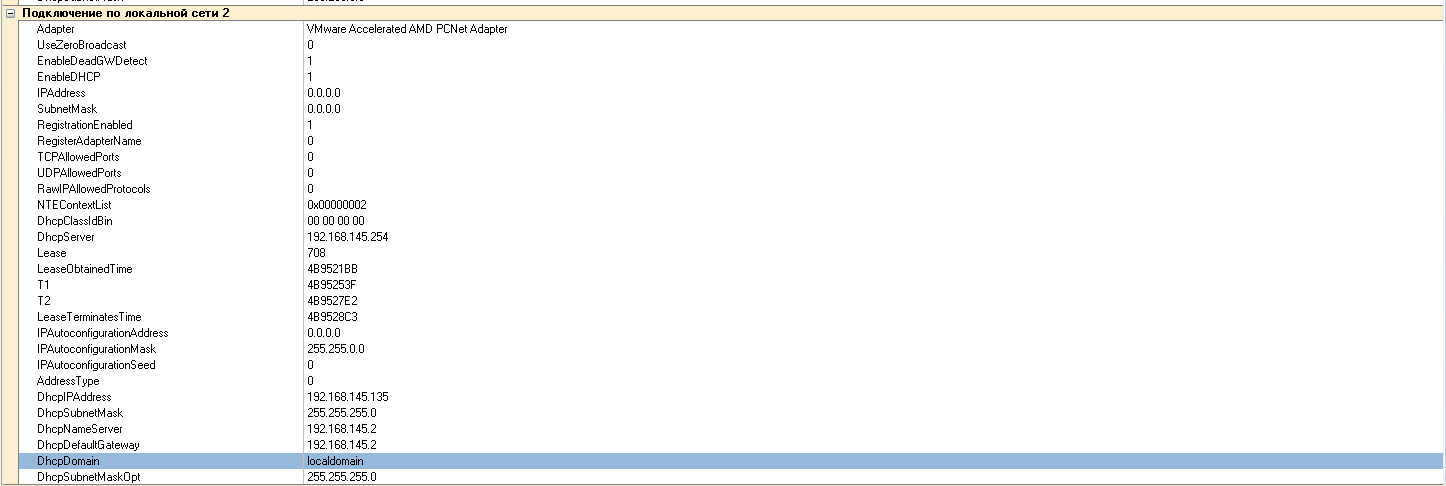




Далее выполнил просмотр сетевой конфигурации и обнаружил два подключения, одно из которых, видимо, являлось для выхода в сеть, а другое для подключения к домену:



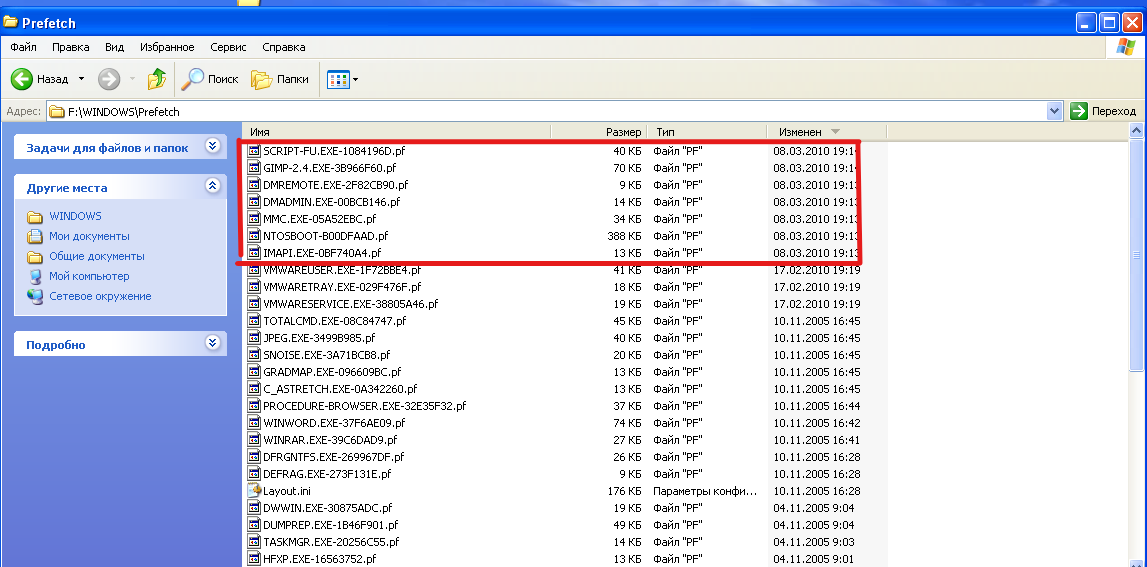
Информация о том что компьютер в домене:



1. Какие программы запускались последними на этом экземпляре ОС?

MRU в реестре найти не удалось, поэтому перешел по каталогу F:\WINDOWS\Prefetch

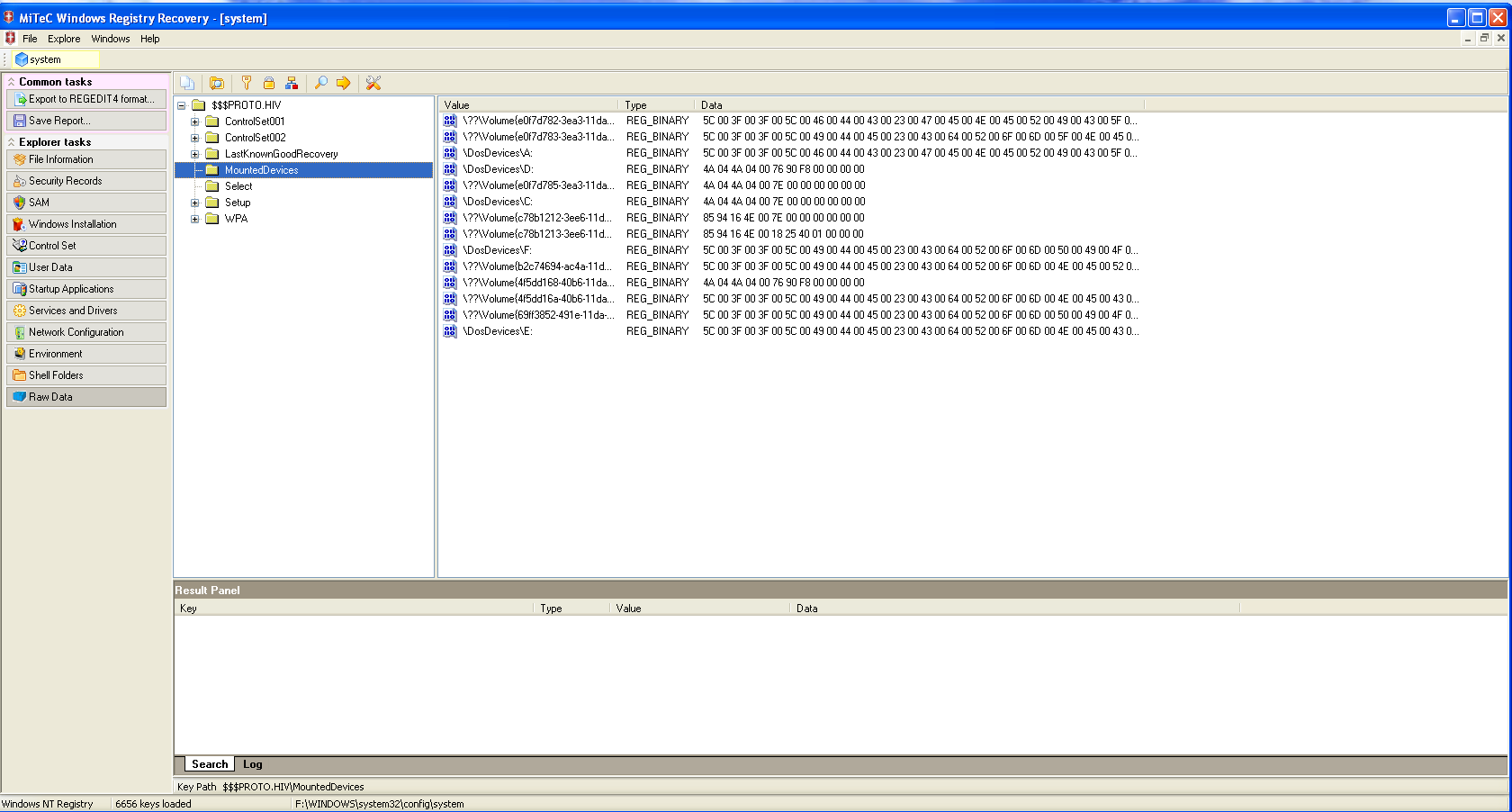
и отсортировал список запущенных программ по дате:



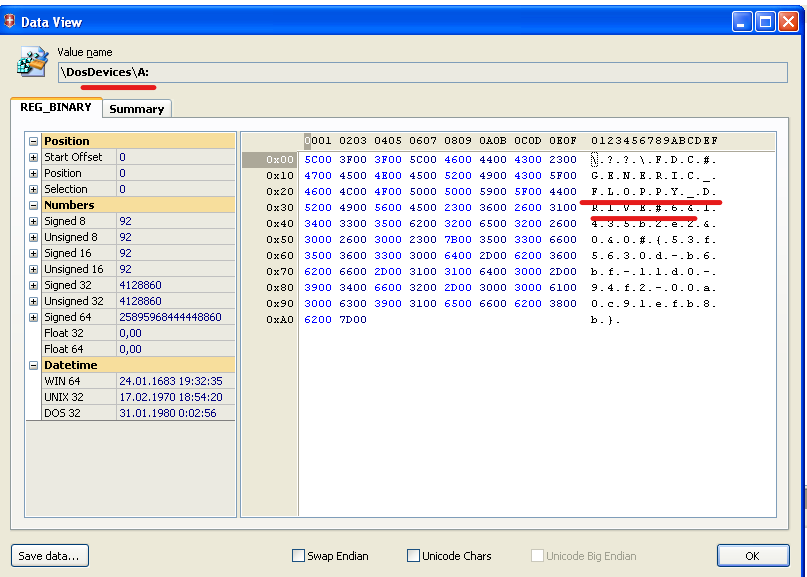
Итак, программы, которые запускались на данном компьютере последними: **SCRIPT-FU, GIMP v2.4** (в последнюю минуту) и другие (ранее в тот день) выделены красной рамкой на скриншоте.

1. Устанавливались ли в системе носители, отличные от представленного, если ДА, то какого типа?

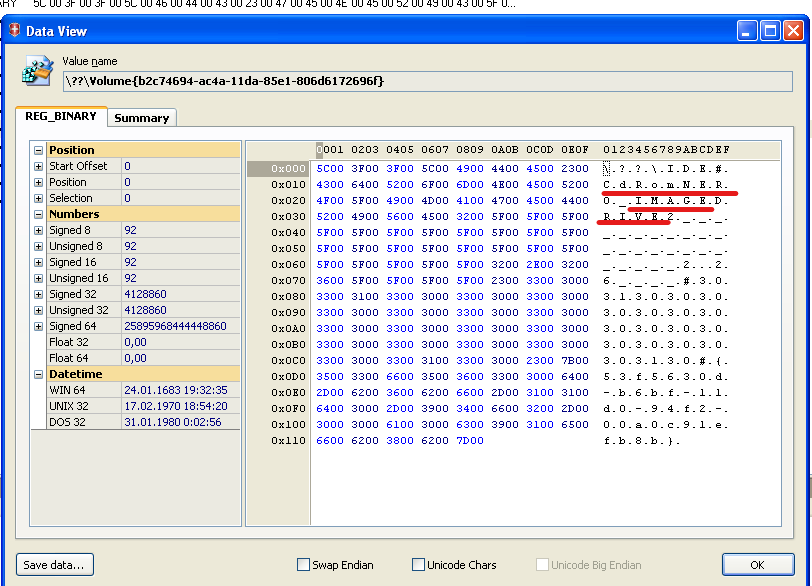
Опять подключился к реестру к файлу system и перешел во вкладку MountedDevices:



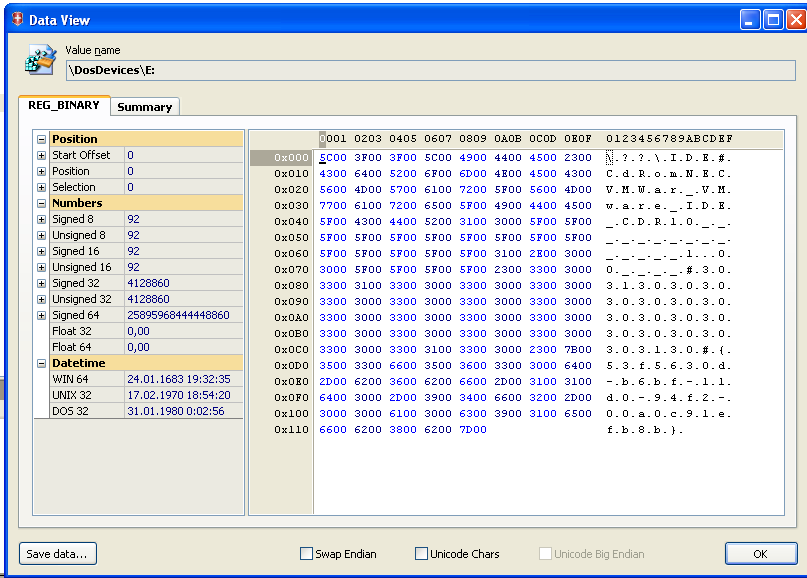
Обнаружил, что был подключен FloppyDisk (дискета) (A):



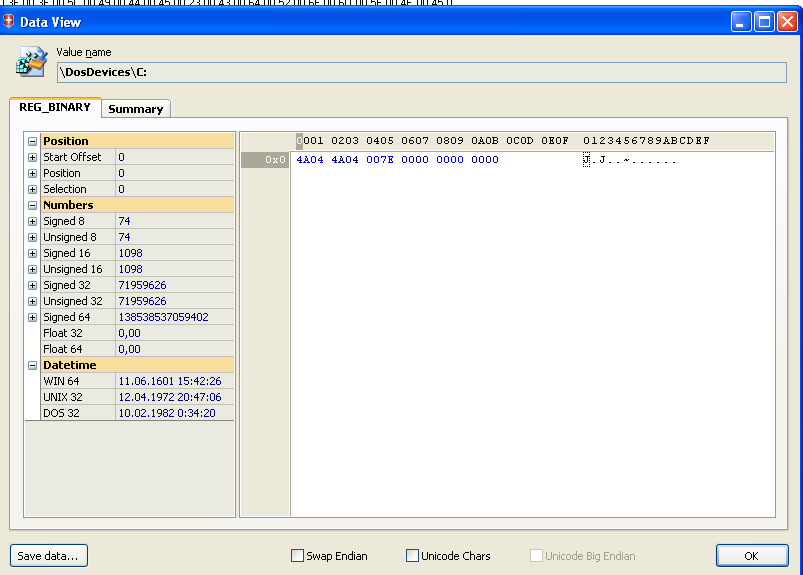
Также были подключены образы обычных DVD дисков, один из них представлен на скриншоте ниже:

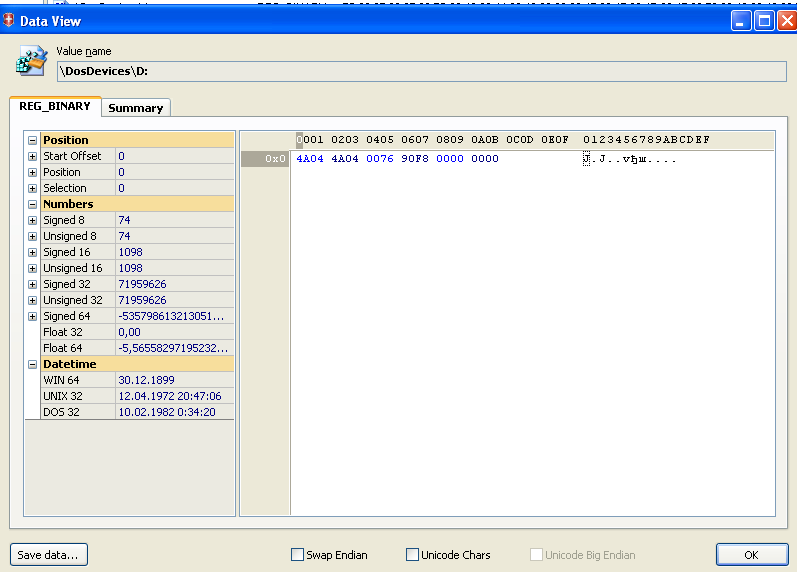


Также был обнаружен еще один носитель информации, который подключался к системе:



Другие 2 диска (D и C) изначально были в системе:

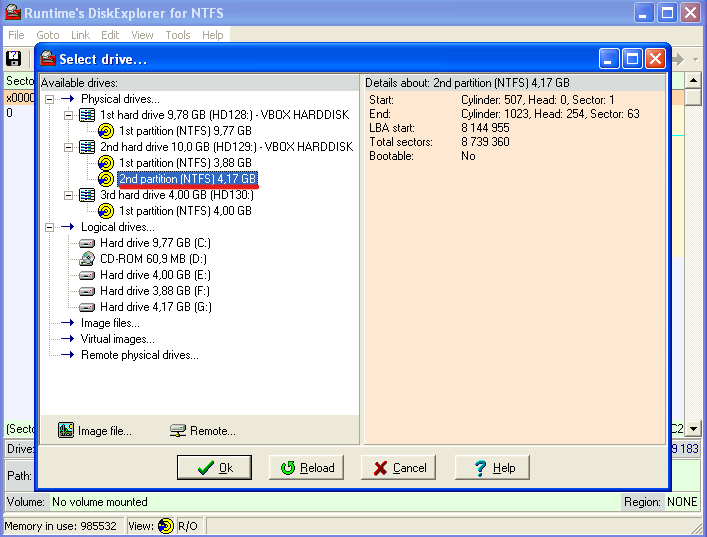




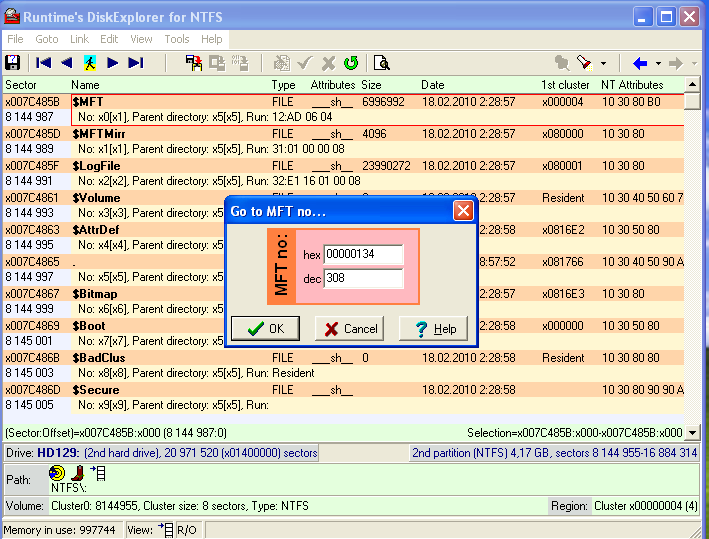
1. WinXP(1) 2-й раздел. Определить дату и время последнего доступа к файлу, который описан в файловой записи №308

Для выполнения данного задания буду использовать программу DiskExp for NTFS.

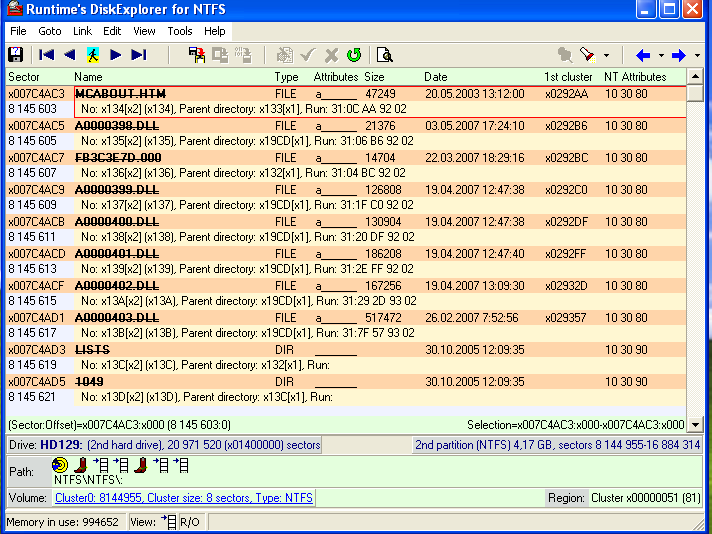
Подключился ко второму разделу исследуемого носителя:



Найдем интересующий нас файл с MFT #308:



Это файл **MCABOUT.HTM** и он был удален в системе:



Информация о доступе к файлу хранится в атрибуте $10$ (Standard Information):

Видим, что последний доступ к файлу был **20.10.2005 в 8:19:18**

