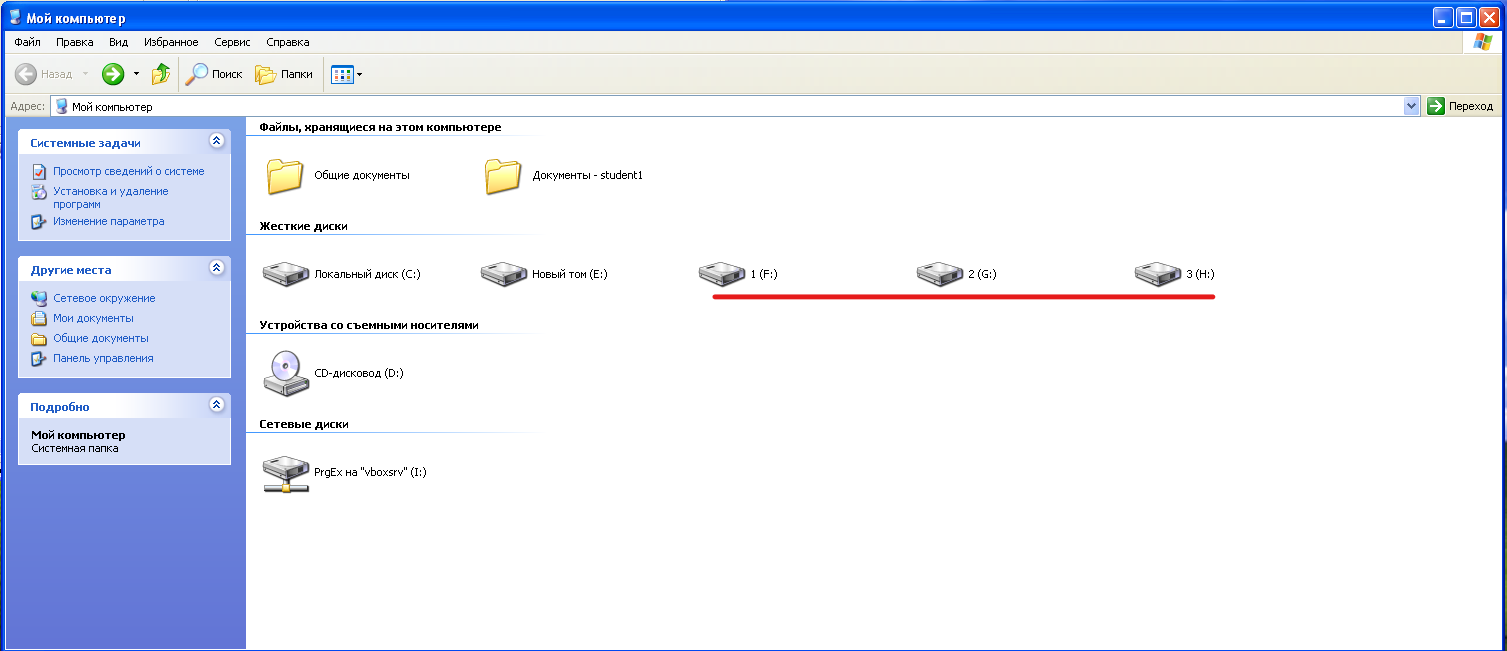
Установление программной среды расследуемого события по следам в файловой системе системного устройства

Работу выполнил студент 431гр. Никитин А.В.

Произвел подготовку исследовательской машины, выполнив установку необходимого для исследования ПО:



Подключил исследуемый образ жесткого диска:

Проанализировав представленные на исследование материалы,

**Исследование информации на НЖМД**

При исследовании НЖМД, обнаружено, что имеет три логических раздела, один из которых является системным, т.е. загружаемым.

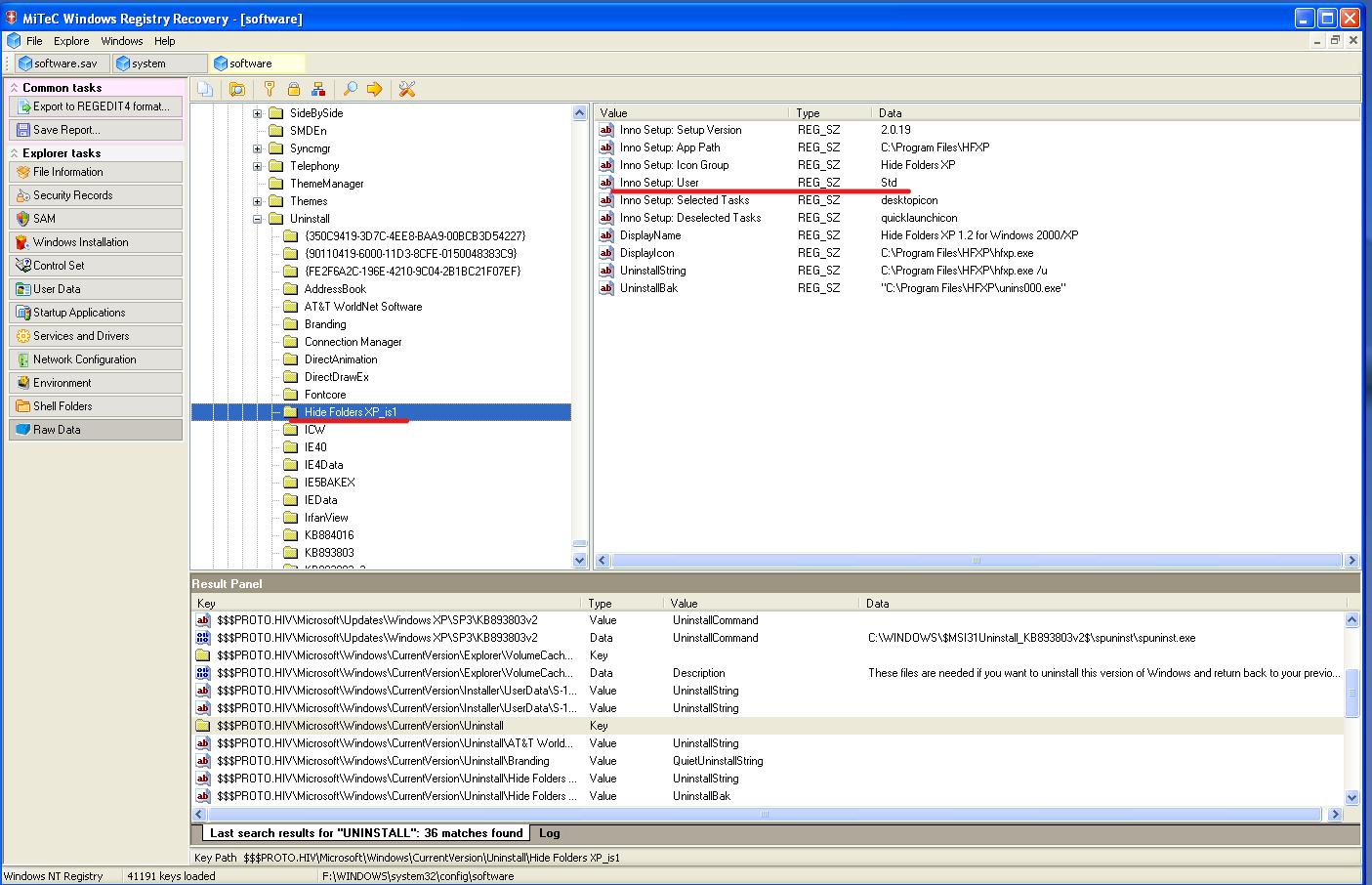
Далее на основе представленных на исследование материалов представлена работа по поиску следов использования ПО для работы с текстовыми документами, растровой графикой, сокрытия информации и защиты КС от нежелательного доступа, найдены конфигурационные файлы программ, базы данных с использованными при работе с миниатюрами изображений (thumbnail-ы) , а также временные файлы, создаваемые конкретными приложениями, выявлены логические цепочки использования программ и, на основе этого, выполнен поиск следов. Также выполнен анализ точек восстановления.

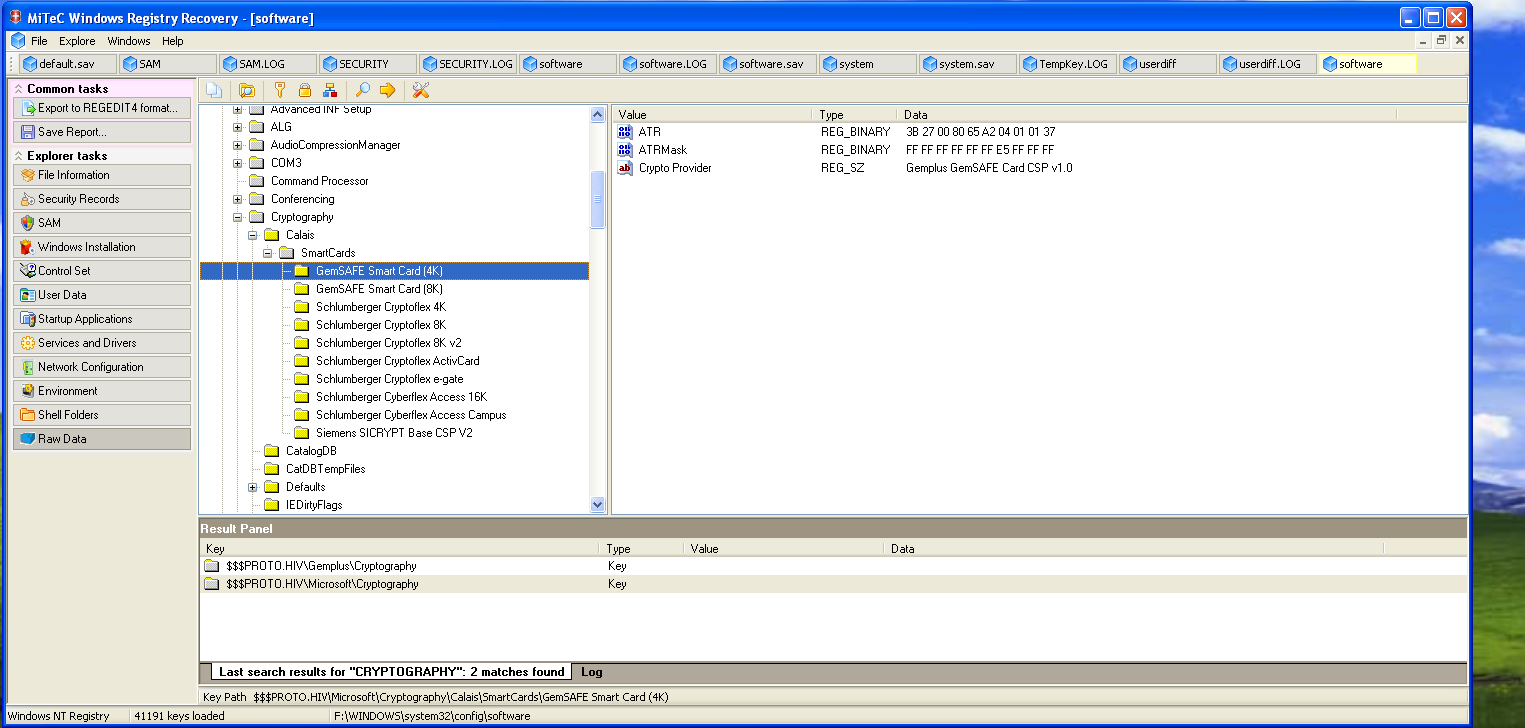
Исследовательская часть разделена на 2 составляющие:

1. ПО, находящееся на данном НЖМД, благодаря которому могли создаваться, редактироваться и просматриваться текстовые и графические файлы.
2. Следы использования ПО и аппаратных средств для создания, редактирования и просматривания и печати текстовых и графических файлов.

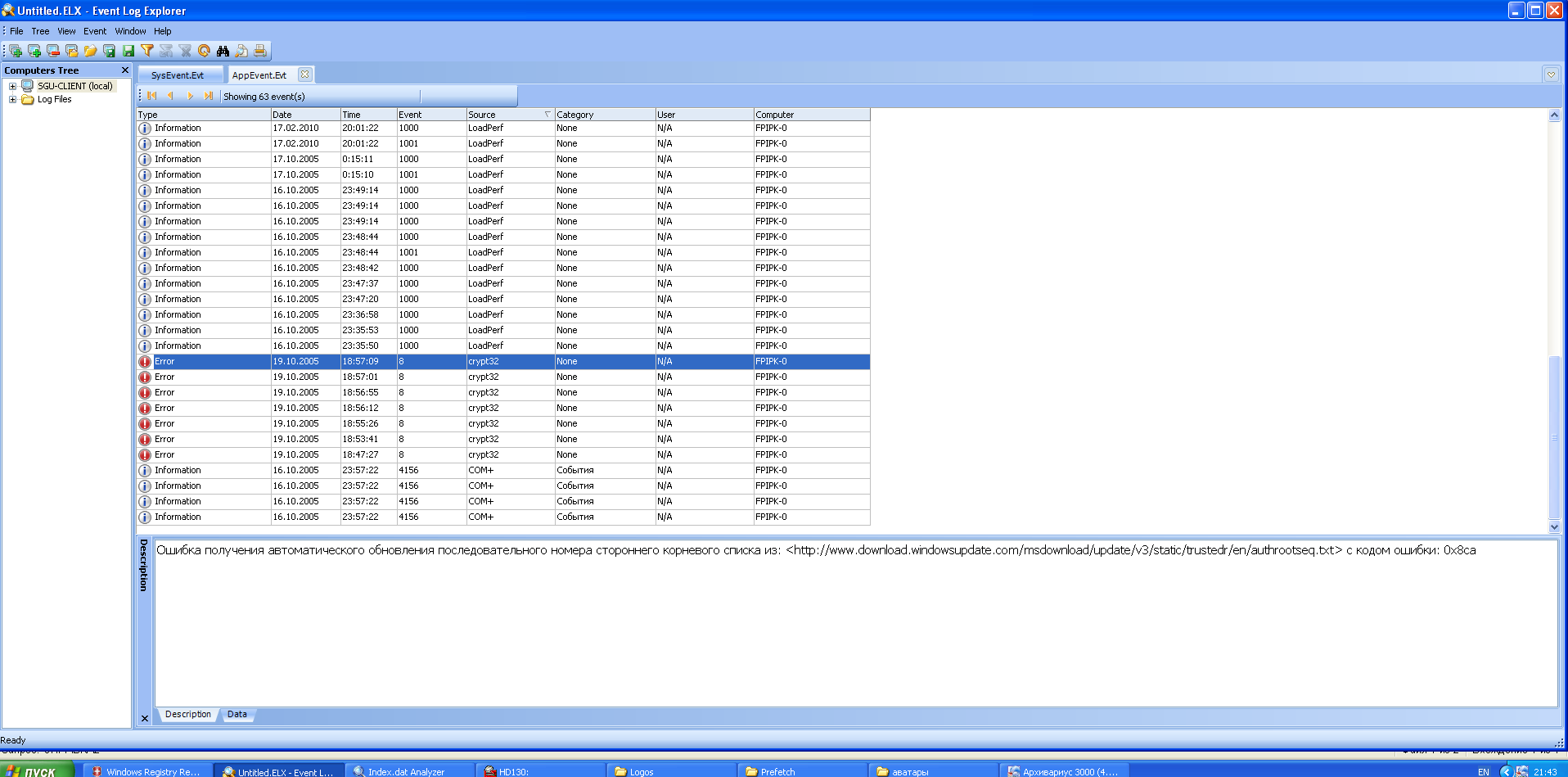
**ПО, находящееся на данном НЖМД, благодаря которому могли создаваться, редактироваться и просматриваться текстовые и графические файлы.**

**Средства сокрытия информации и защиты КС от нежелательного доступа:**

С помощью программы просмотра пассивного реестра MiTec Windows Recovery, в файле software в Uninstall была найдена программа HideFolders (используется для разграничения доступа и сохранения конфиденциальности файлов и папок):

В качестве аппаратной защиты были найдены присутствующие в системе по умолчанию смарт-карты:

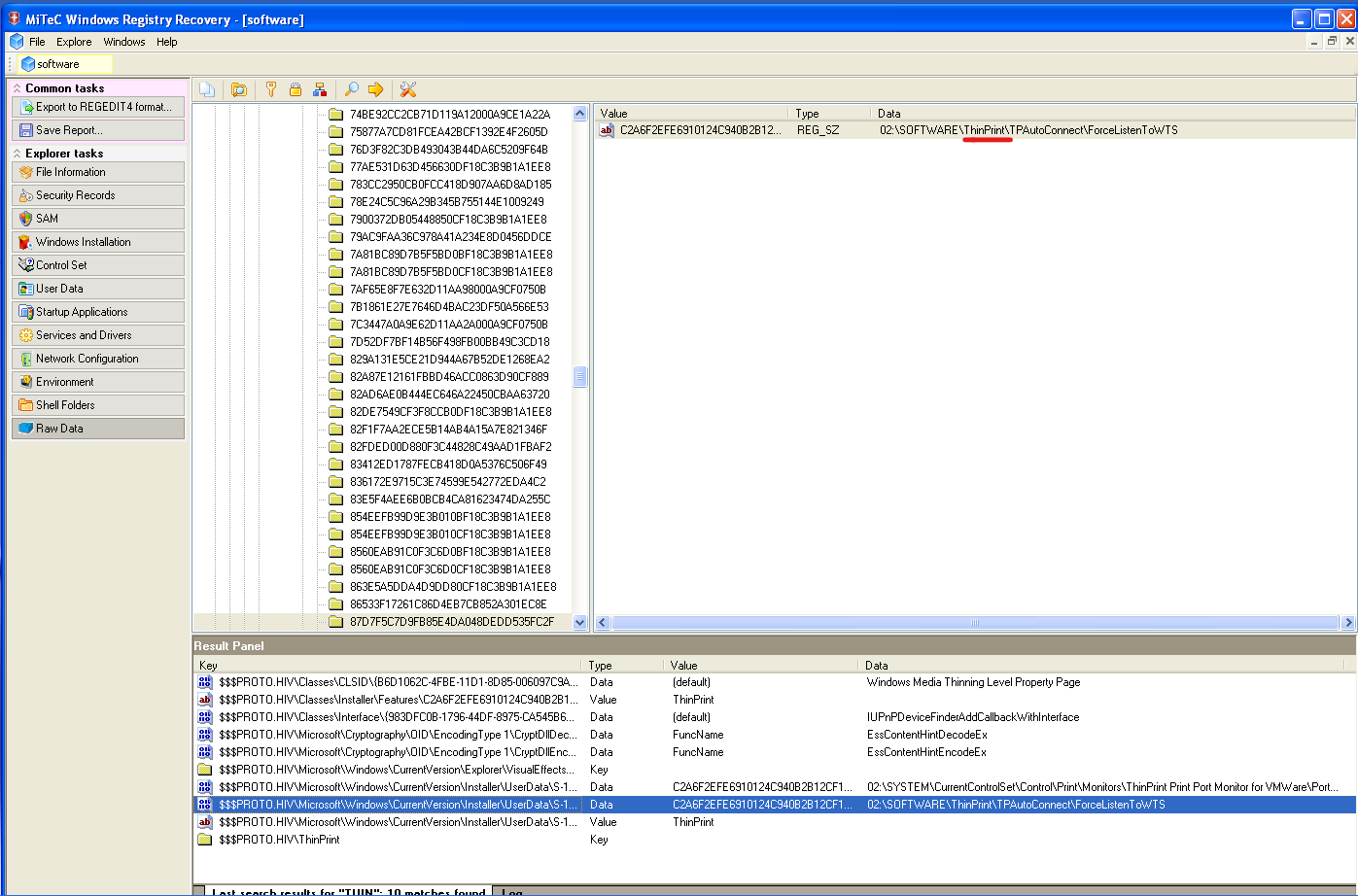
Далее с помощью программы Event Log Explorer, которая используется для просмотров пассивных журналов событий, в журнале AppEveуnt.Evt была найдена ошибка одной из служб CryptoAPI, а именно crypt32:



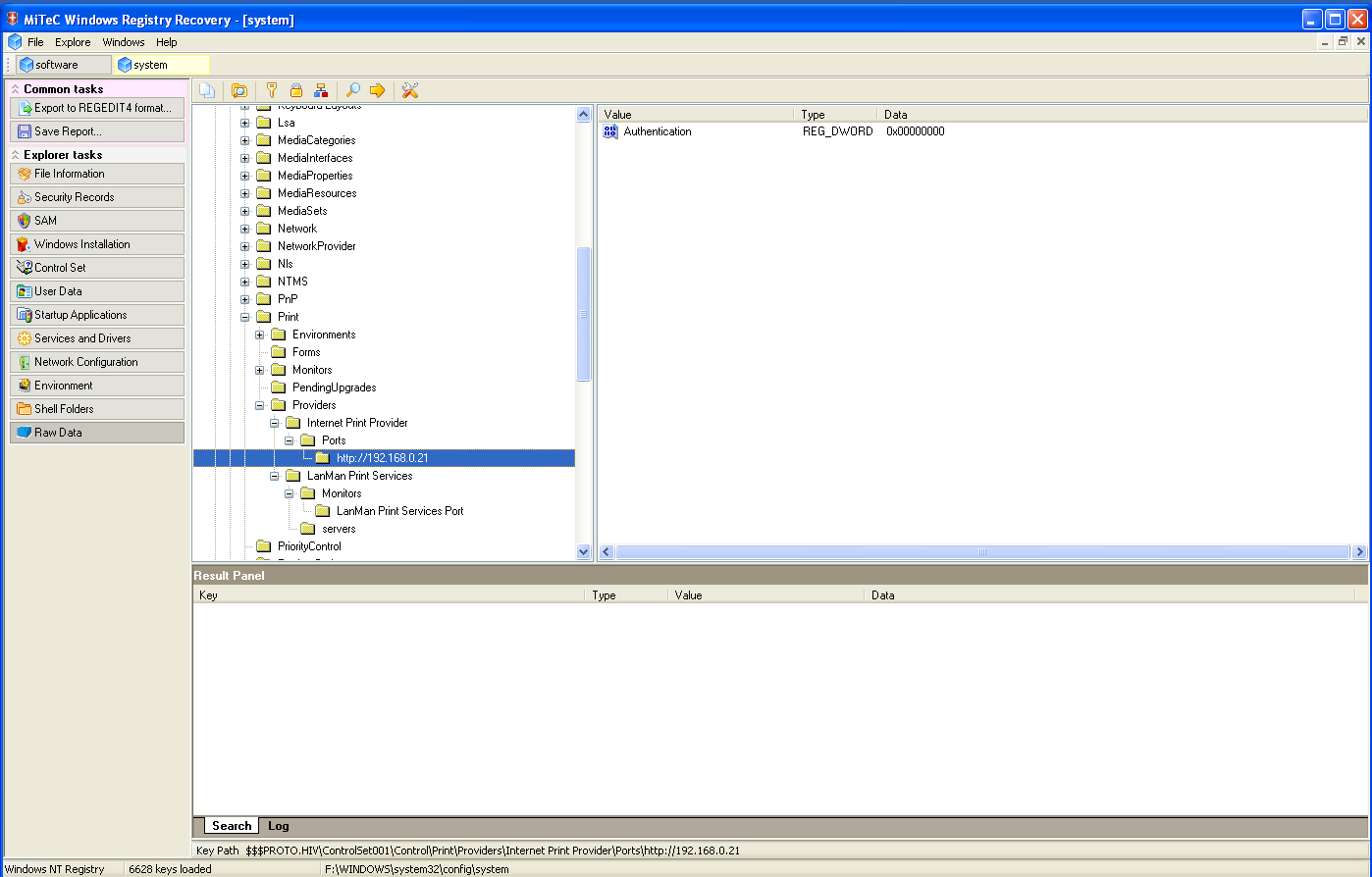
**Программы создания и редактирования файлов, средства печати:**

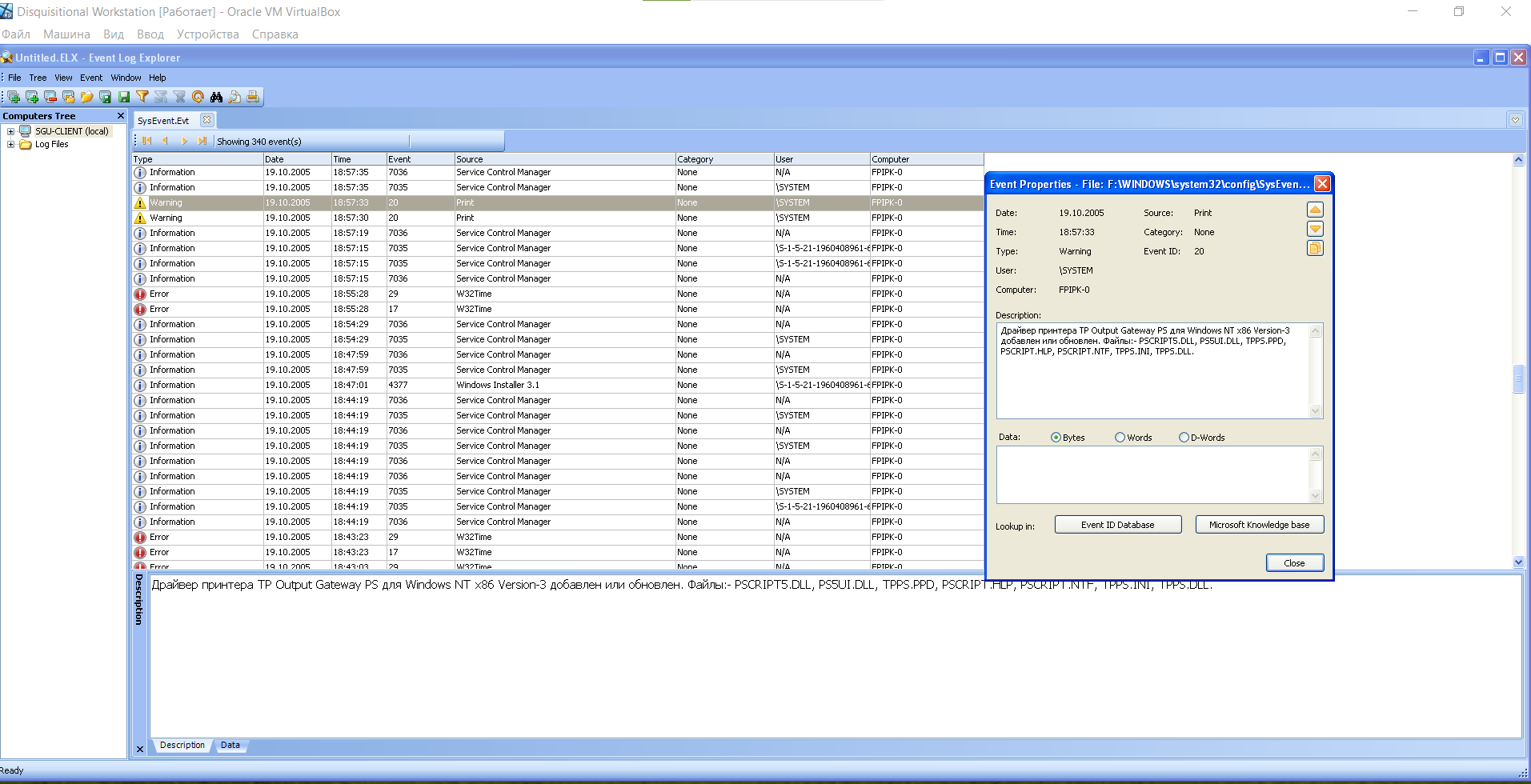
С помощью программы MiTec Windows Registry Recovery были найдены установленные в системе принтеры, которые могли использоваться для печати твердых копий документов:

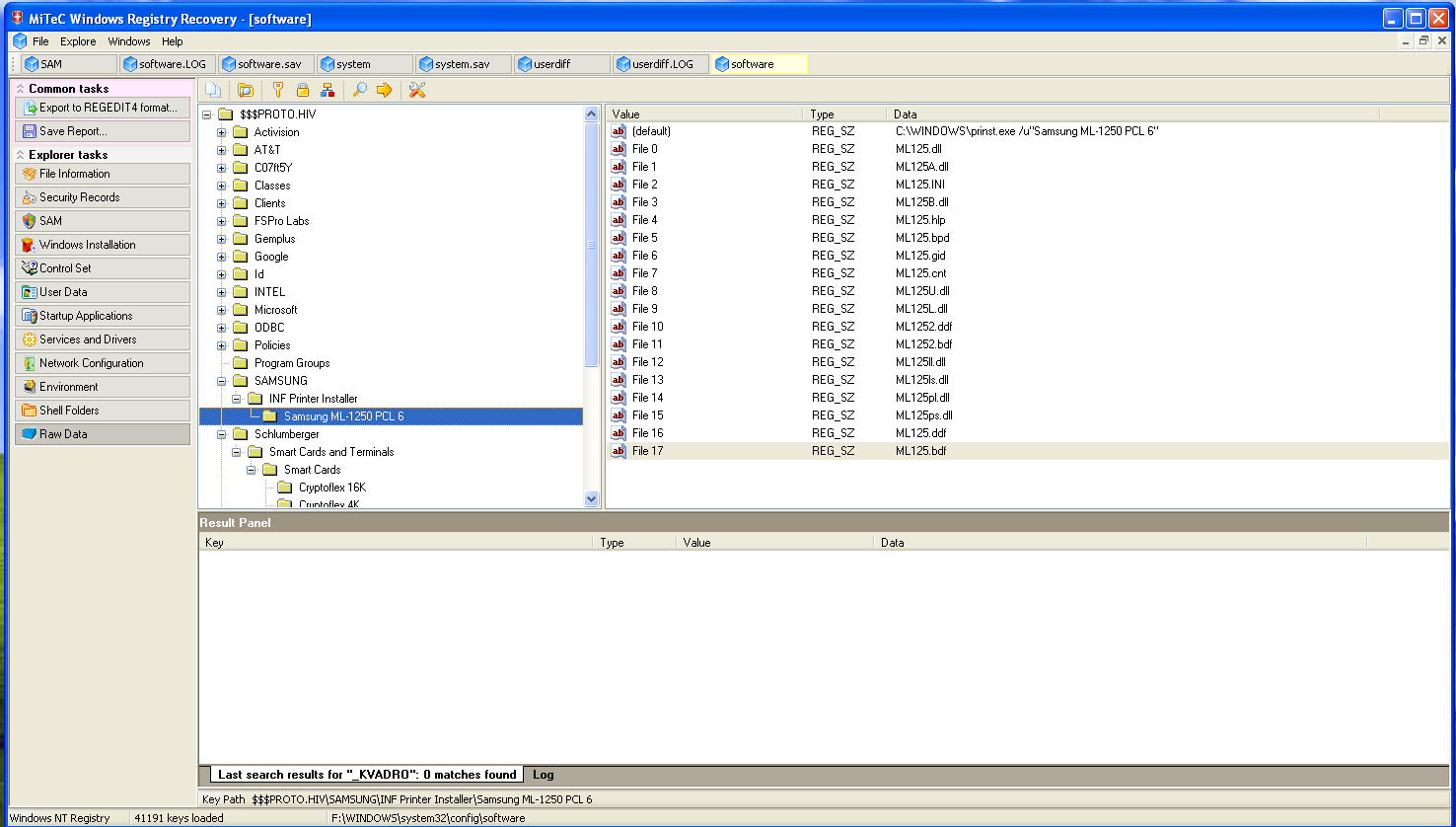
* Драйвера для сервиса удаленной печати ThinPrint:



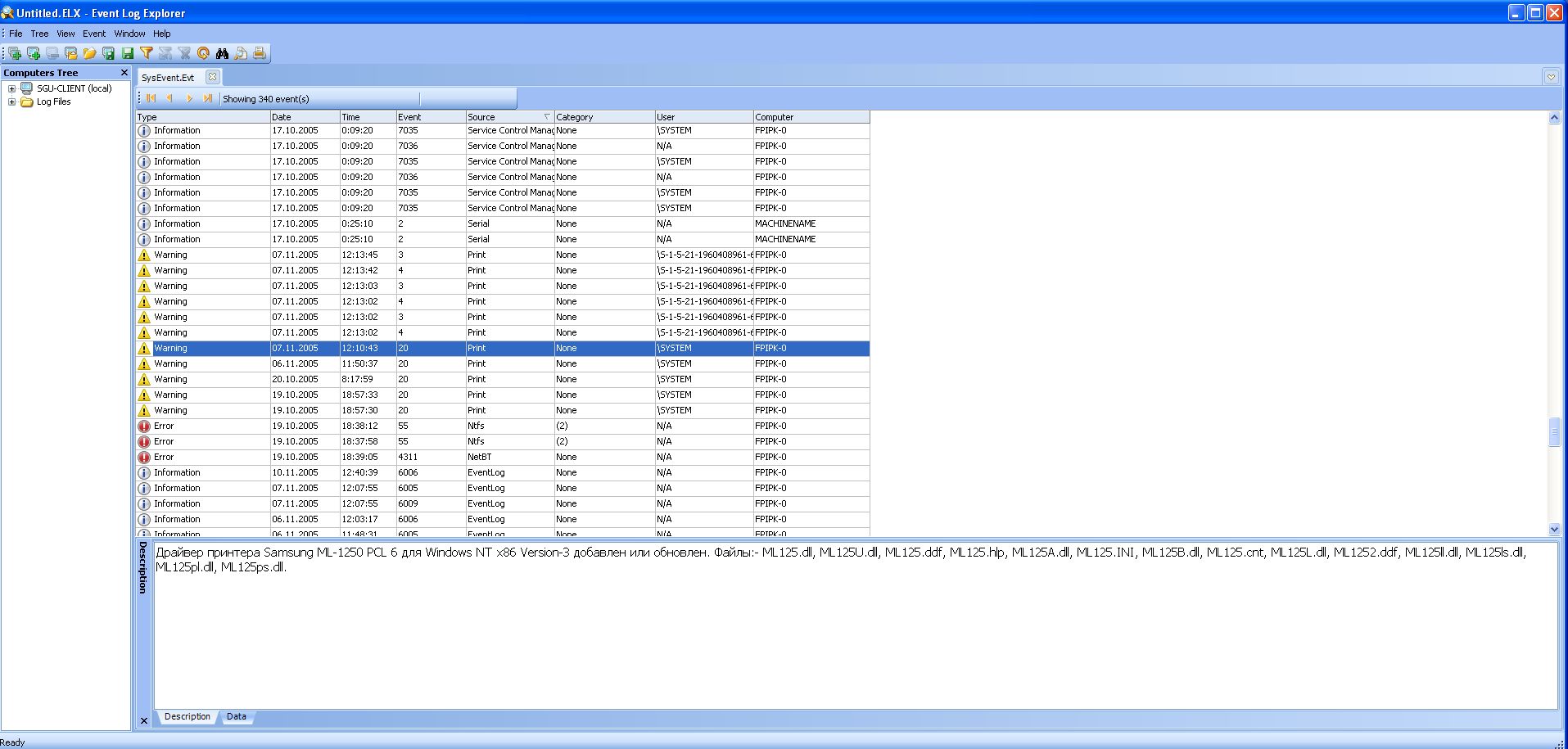
Был найден ip-адрес, по которому, возможно, производилась интернет-печать документов. Также, возможно, данный ip-адрес использовался для принтера Xerox:

В журнале системы добавлен драйвер принтера сетевой печати:

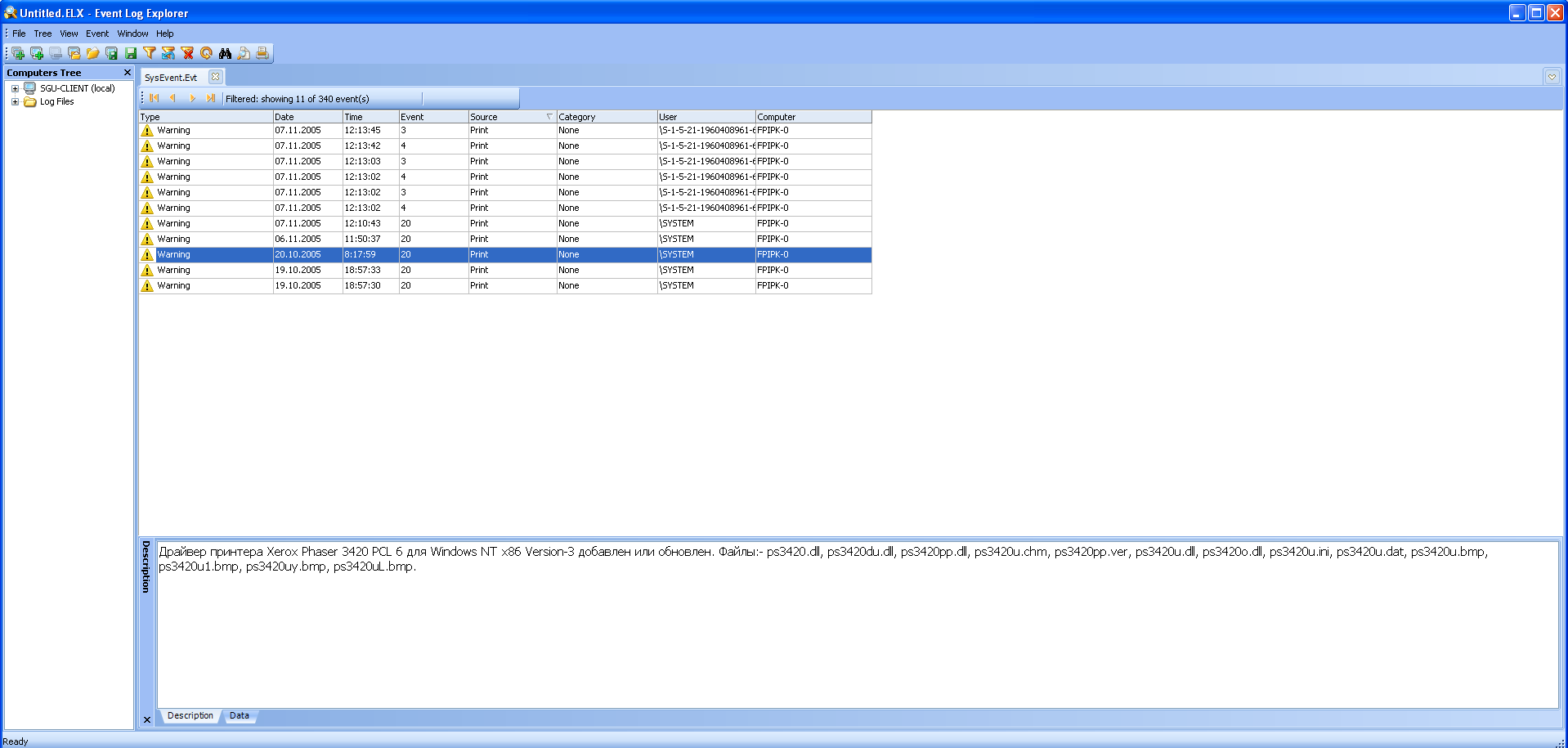


* Установлен драйвер для принтера **Samsung ML-1250 PCL 6** (далее имя принтера будет использовано для поиска по контексту возможных следов использования:

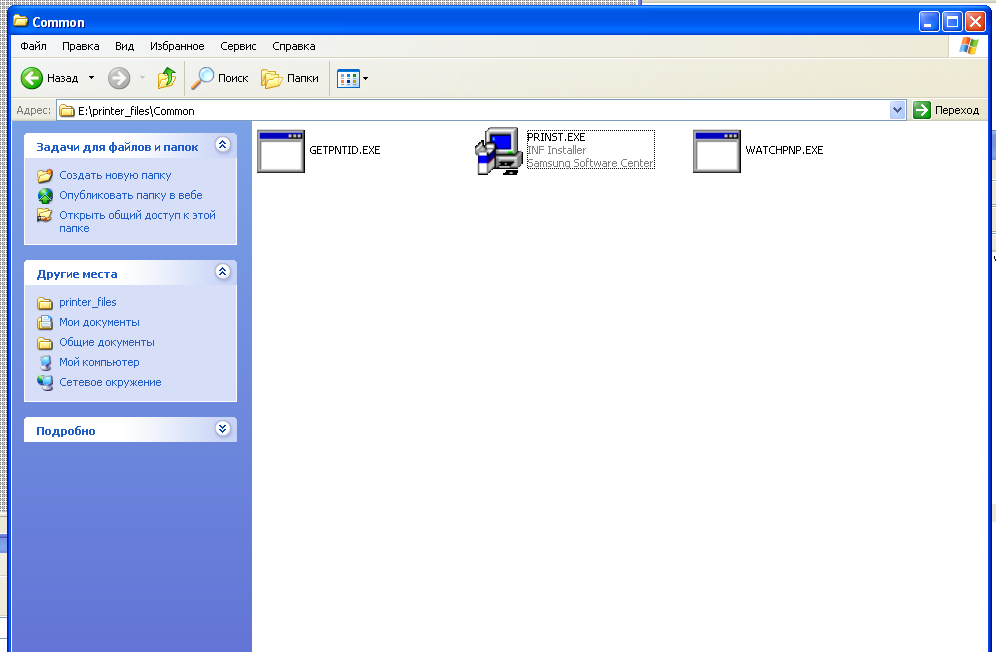
Факт установки также подтвердился и журналом событий (выше расположены события также и для сетевой печати с вышеуказанным ip:



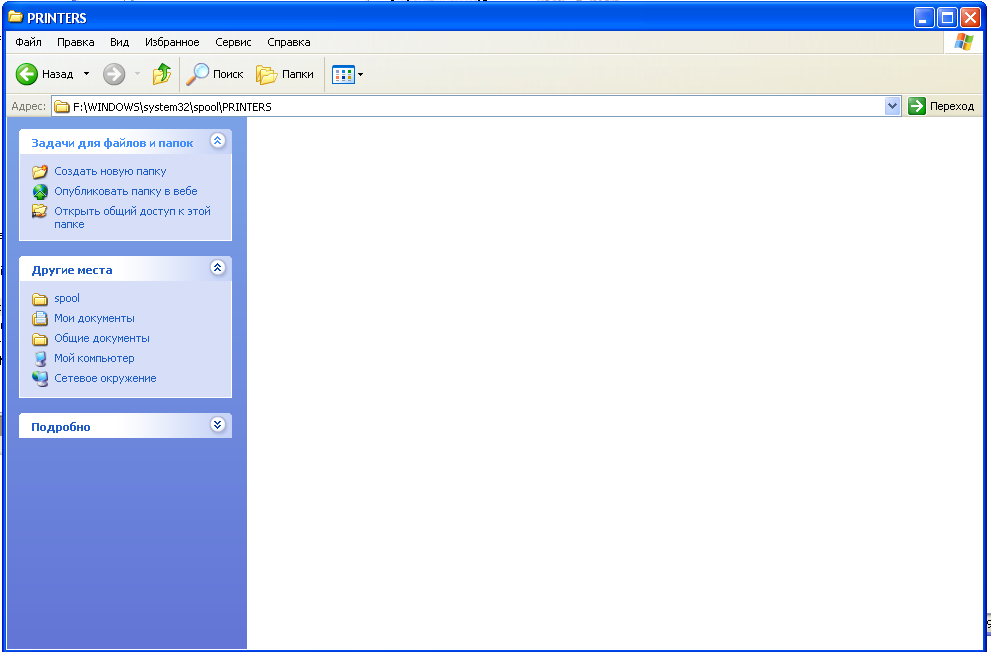
* Также была найдена информация об установке драйверов для принтера **Xerox Phaser 3420** в SysEvt (название принтера также будет использовано для поиска по контексту):



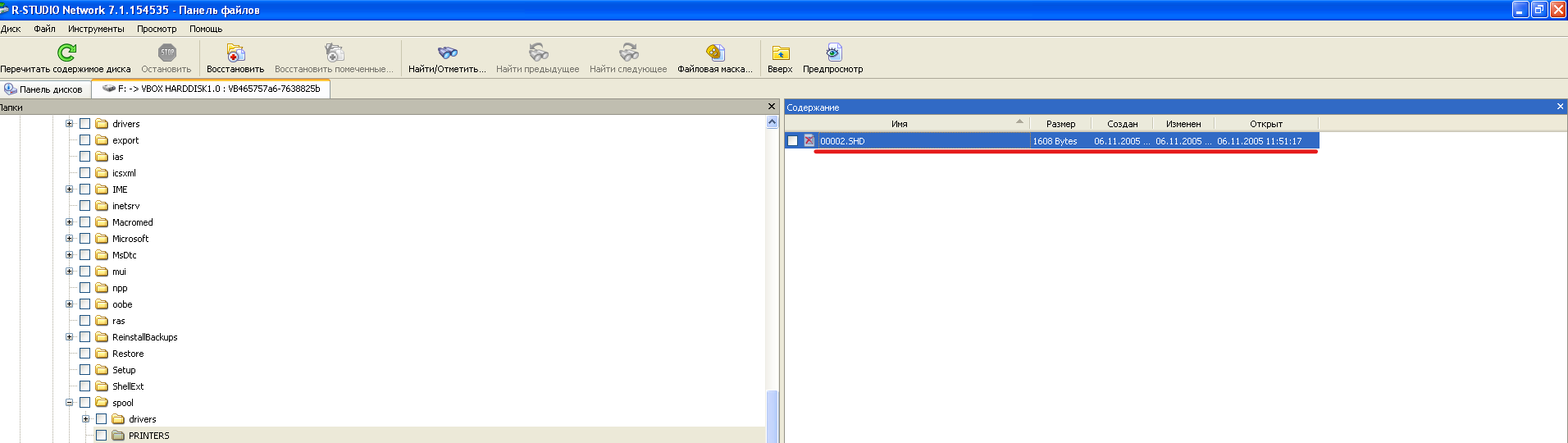
Был найден файл драйвера принтера:



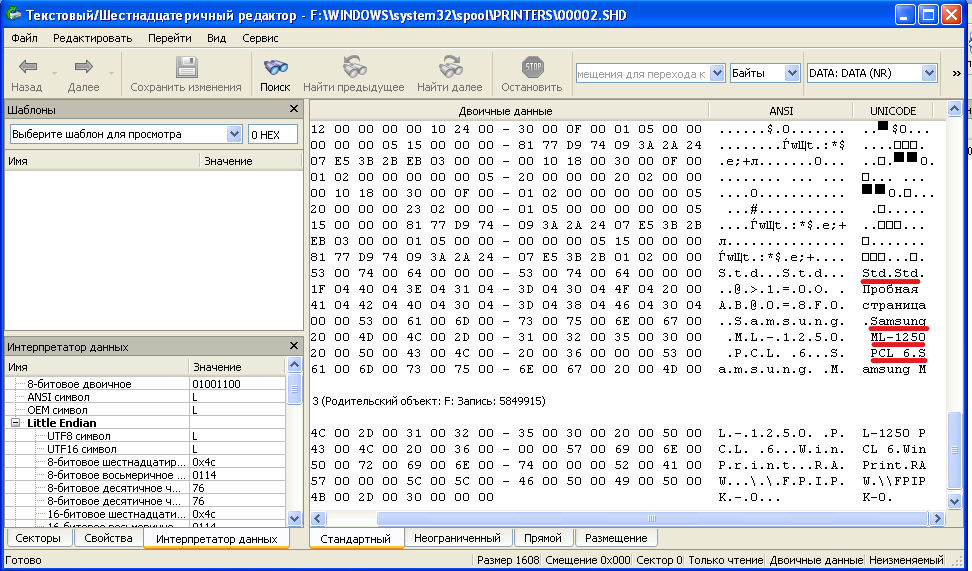
На скриншоте ниже представлена очередь печати, которая находится по адресу \WINDOWS\system32\spool\PRINTERSа:



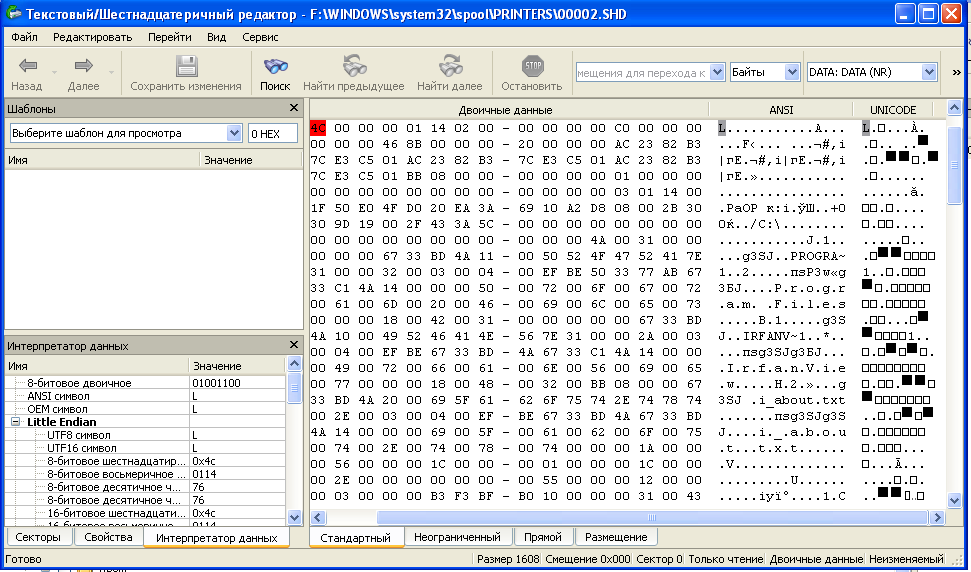
С помощью программы R-Studio выяснилось, что в очереди печати находилась как минимум одна запись, что свидетельствует о распечатке:



Далее просмотрел содержимое файла из очереди печати: во-первых, использовался принтер Samsung ML 1250 PCL, также он использовался пользователем Std:



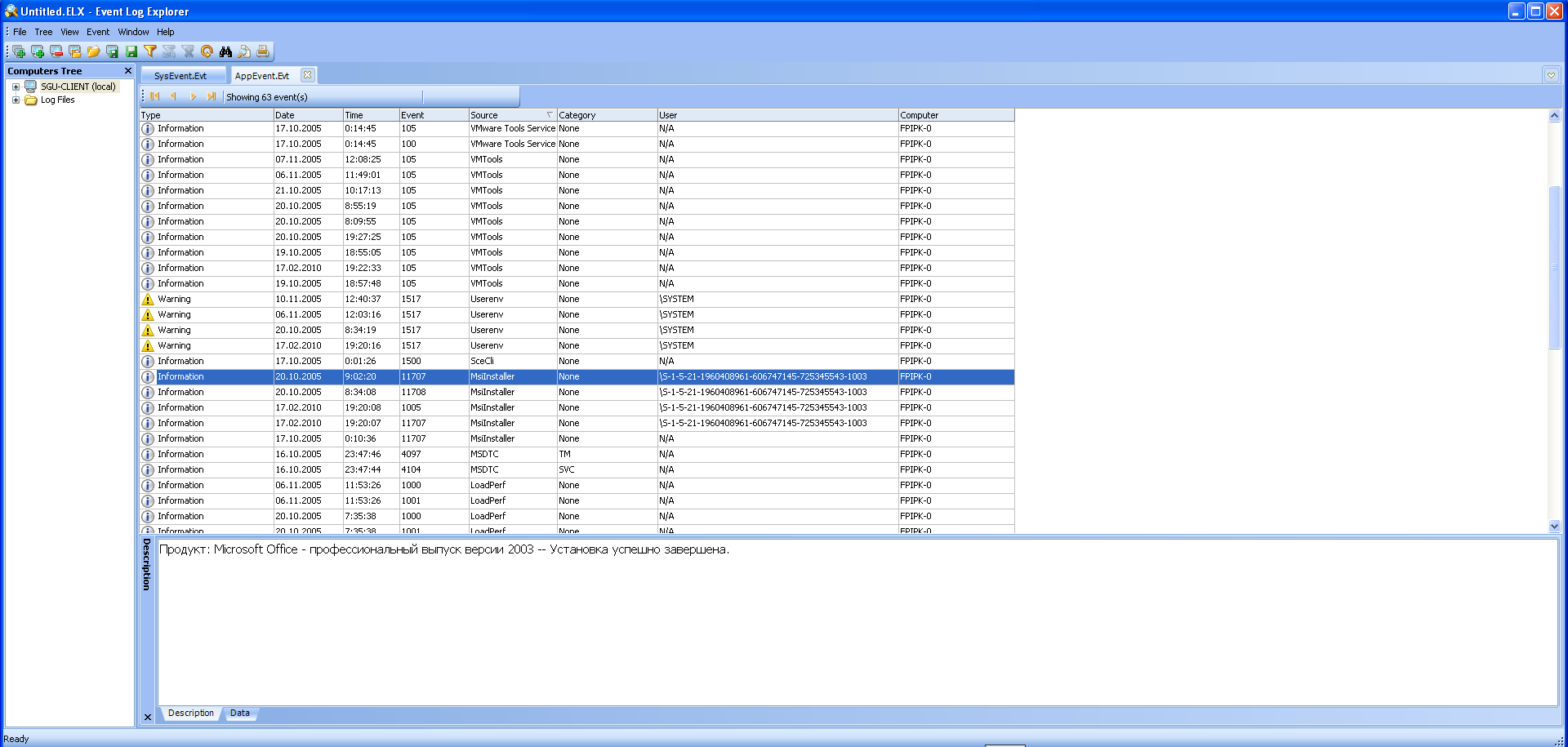
В том же файле была найдена информация о факте использования программы IrfanView (данная программа является аналогом программы GIMP, которая, в свою очередь используется как редактор файлов с растровой графикой):



**Средства работы с текстовыми документами:**

Был просмотрен системный журнал AppEvent.Evt для поиска фактов, свидетельствующих об установке рассматриваемого ПО:

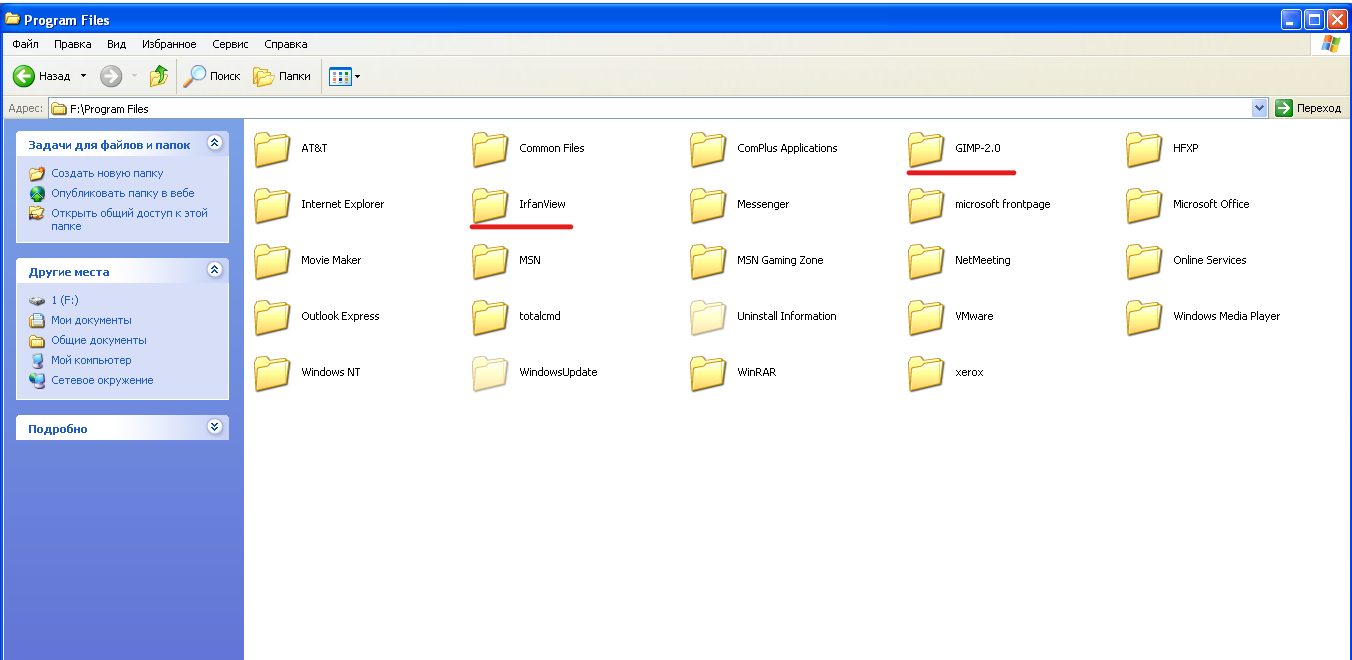
Была найдена информация, что **MS Office 2003 (**набор программ, среди которых есть программа для работы с текстовыми документами --- Word**)** был установлен для пользователя с SID **S-1-5-21-1960408961-606747145-725345543-1003**:



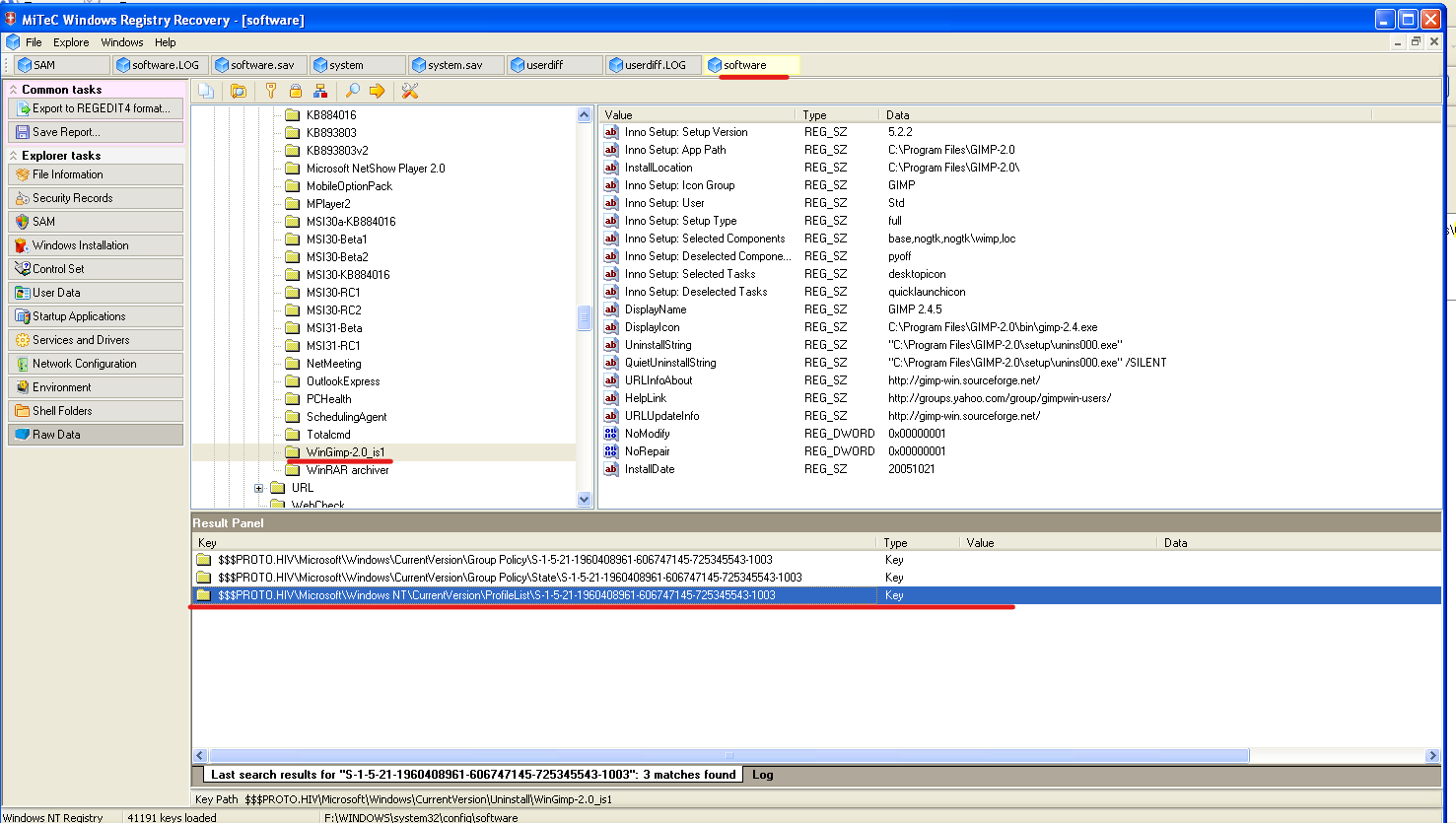
Средства работы с растровой графикой:

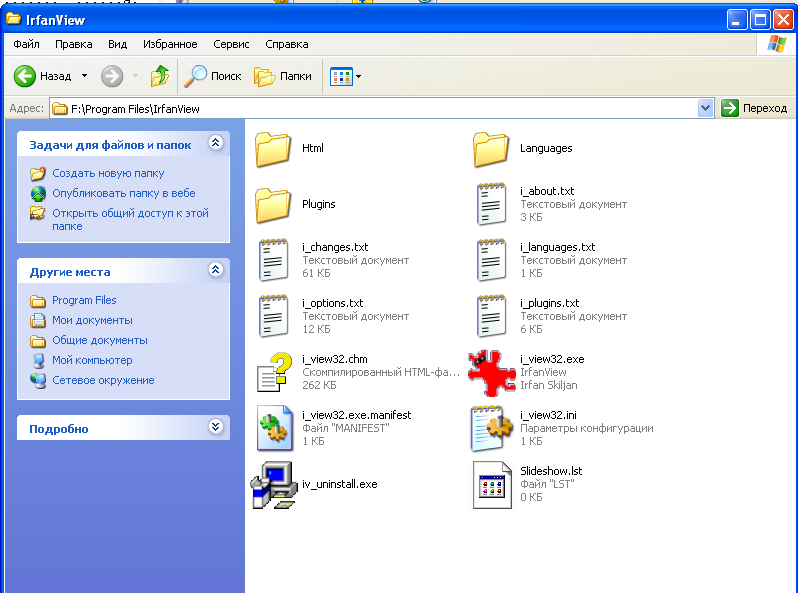
В папке ProgramFiles на системном разделе были найдены 2 установленных программы:

1. IrfanView
2. GIMP v2.0.

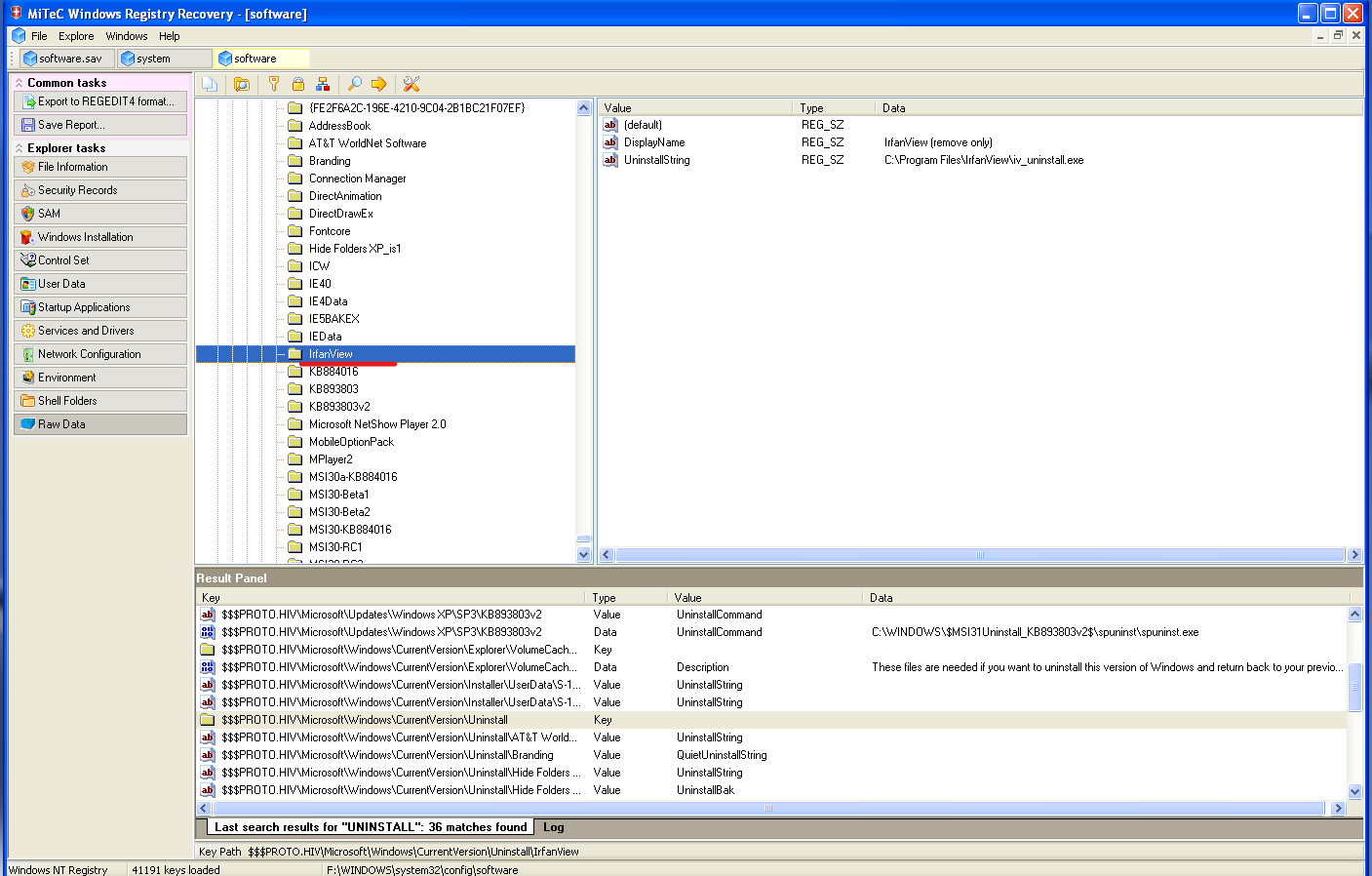


В программе просмотра пассивного реестра была найдена программа GIMP:



Ранее был найден след использования программы IrfanView (в очереди печати принтера производителя Samsung). В следе был указан адрес расположения программы, перешел по нему и программа оказалась действительно установленной:

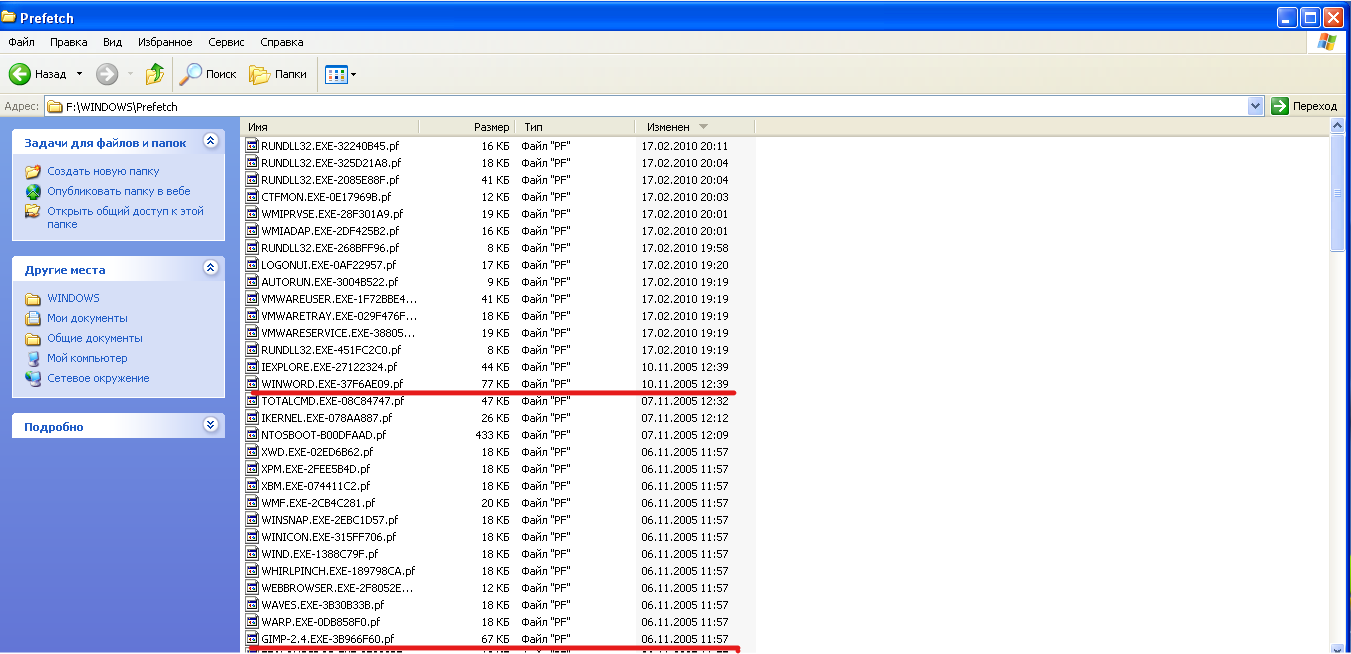
Та же программа, след в пассивном реестре:



2 **Следы использования ПО и аппаратных средств для создания, редактирования и просматривания и печати текстовых и графических файлов.**

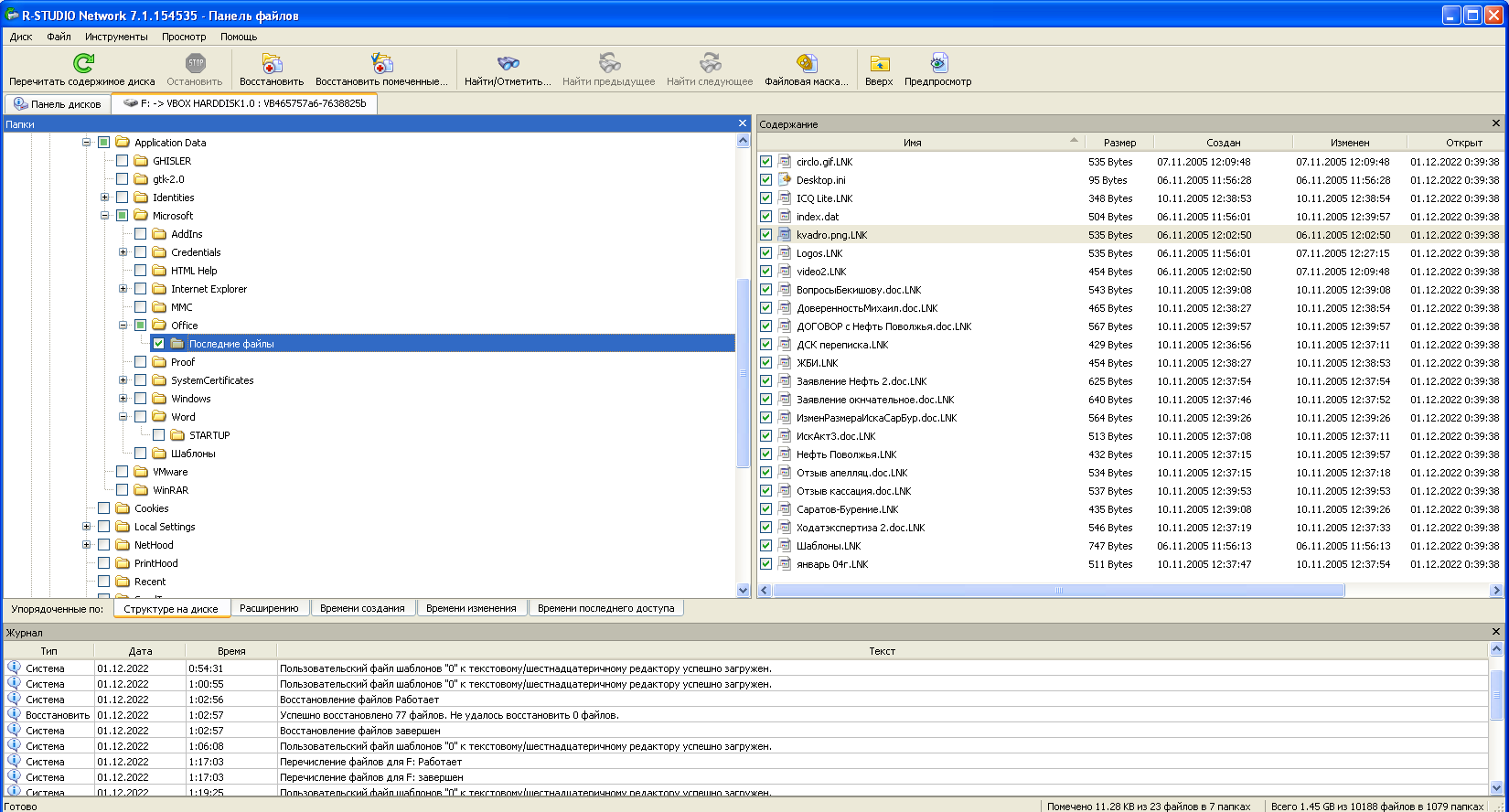
Далее представлен каталог Prefetch, содержащий информацию о недавно запущенных программах.

Отсортируем список файлов по дате изменения. На скриншоте ниже отмечены представляющие интерес программы Word и GIMP:

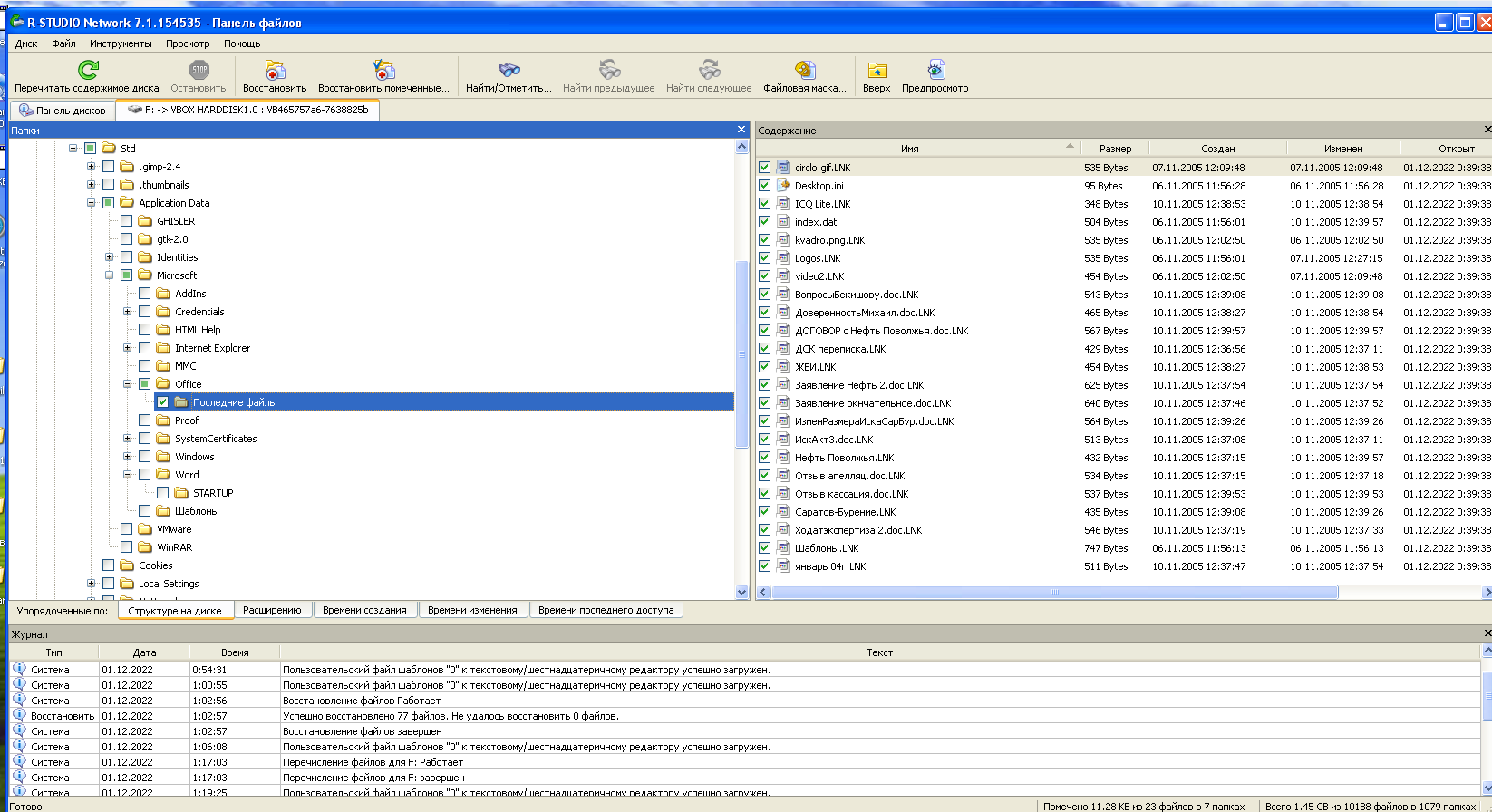


Так как последней программой, используемой для работы с текстовыми документами, являлась программа Word и так как известно имя пользователя, который работал с текстовыми файлами, то с помощью программы R-Studio были просмотрены файлы которые были использованы программой Word.

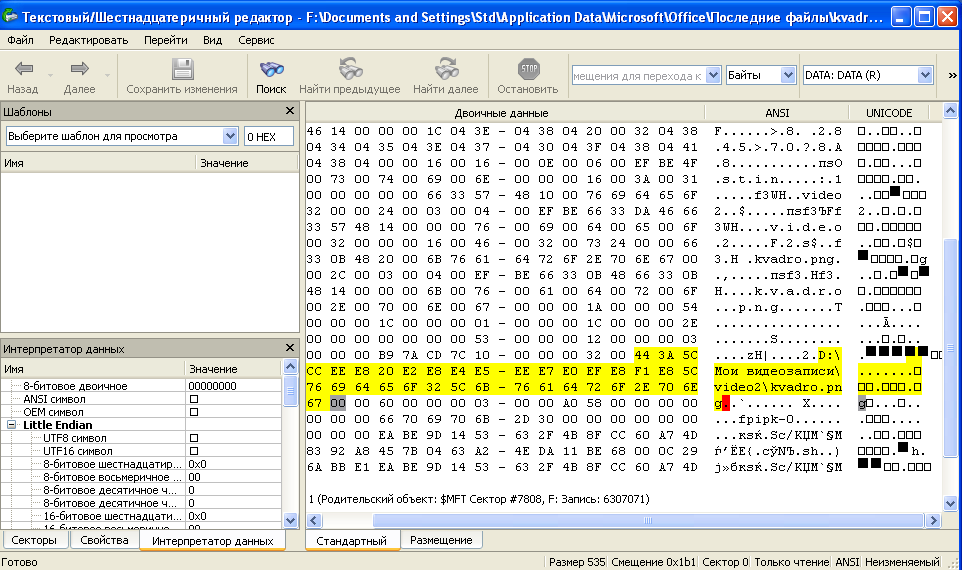
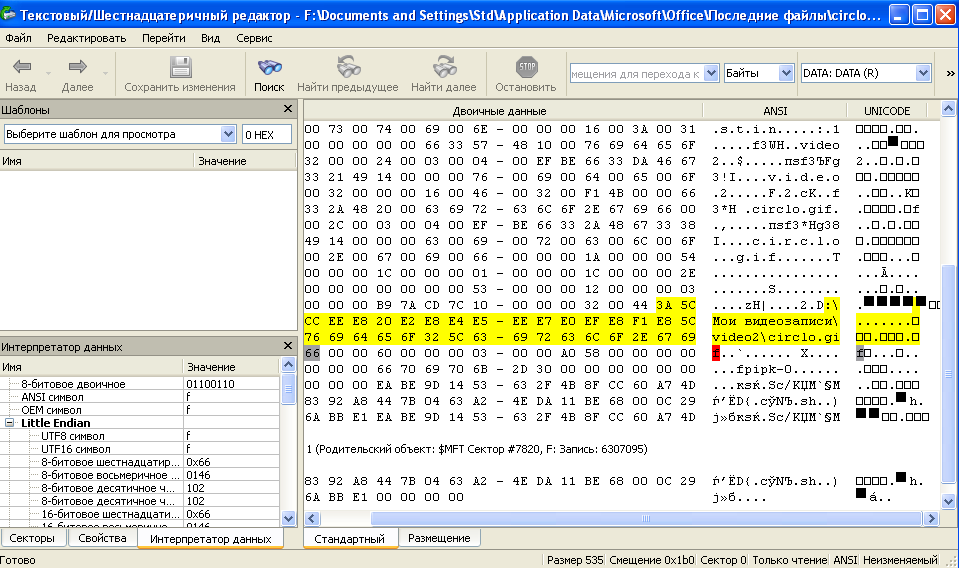
Факт открытия файлов (фотографий) с помощью программ MS Office пользователем Std:

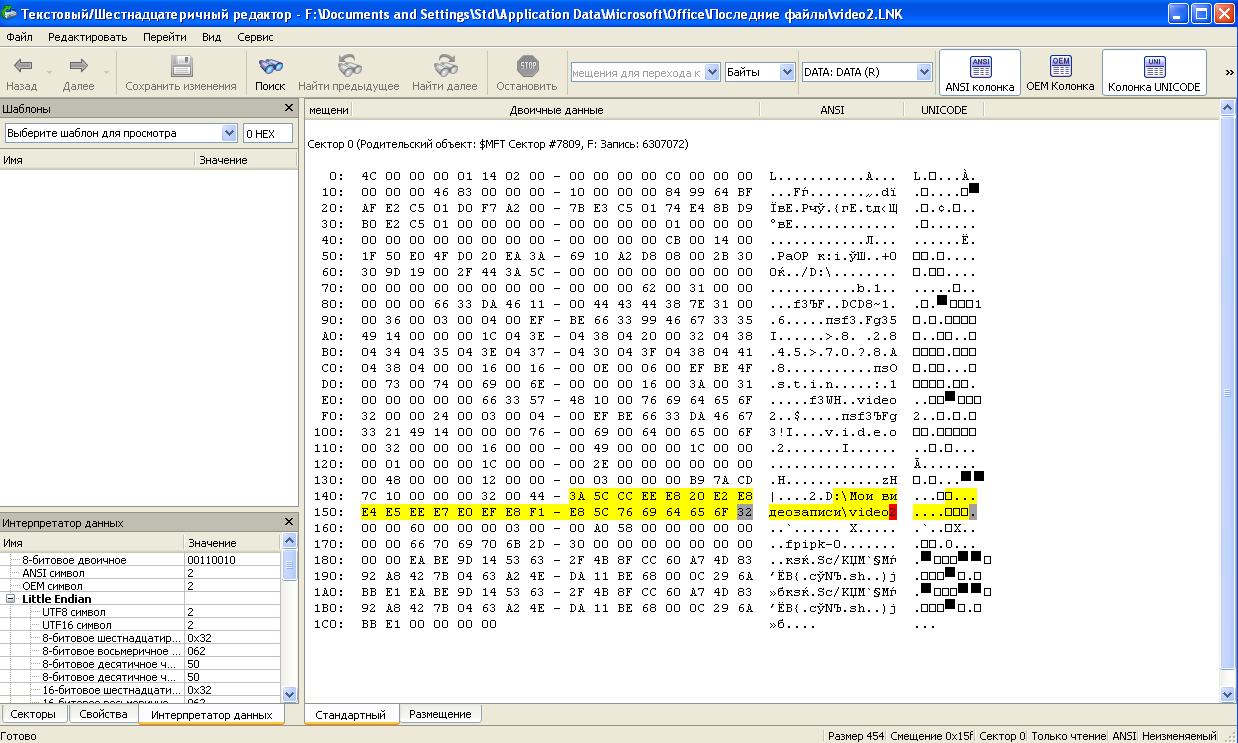


На системном диске в папке пользователя Std по адресу ApplicationData/Microsoft/Office/recent был найден список недавно использованных файлов в программах MS Office, среди которых присутствуют файлы kvadro, video2(папка), также на данном скриншоте присутстует факт использования самого офиса для редактирования .doc документов:



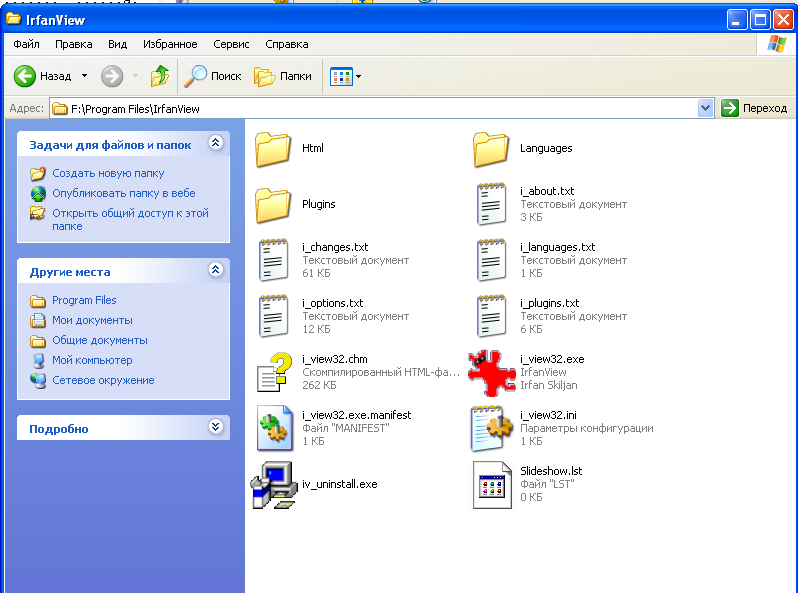
Пути к найденным использованным файлам:



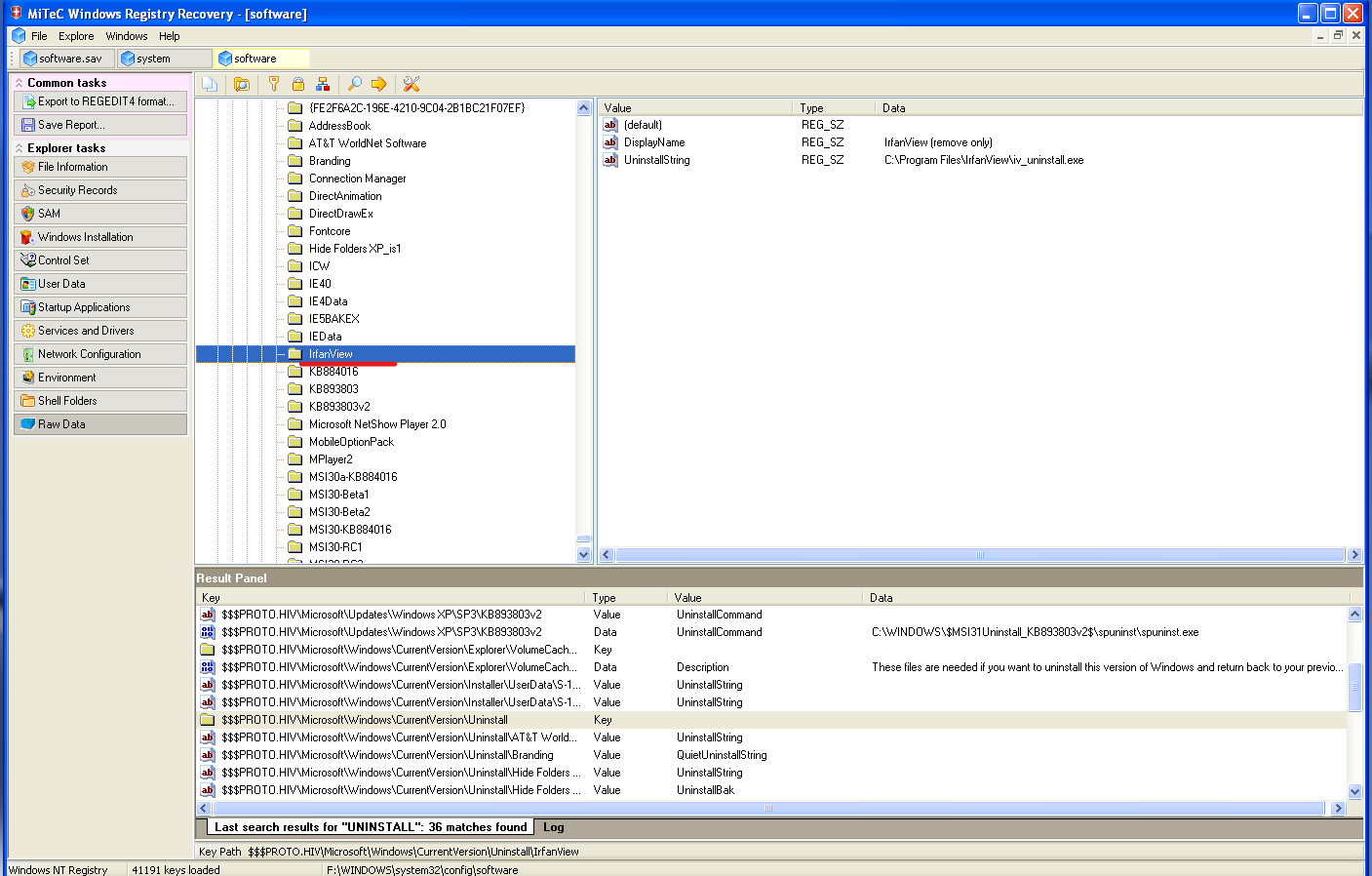


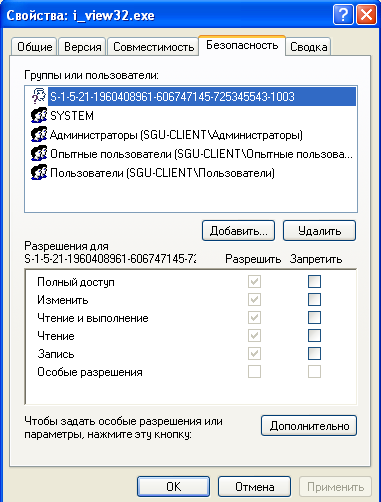
**Программы для редактирования растровой графики:**

Ранее был найден след использования программы IrfanView (в очереди печати принтера производителя Samsung). В следе был указан адрес расположения программы, перешел по нему и программа оказалась действительно установленной:

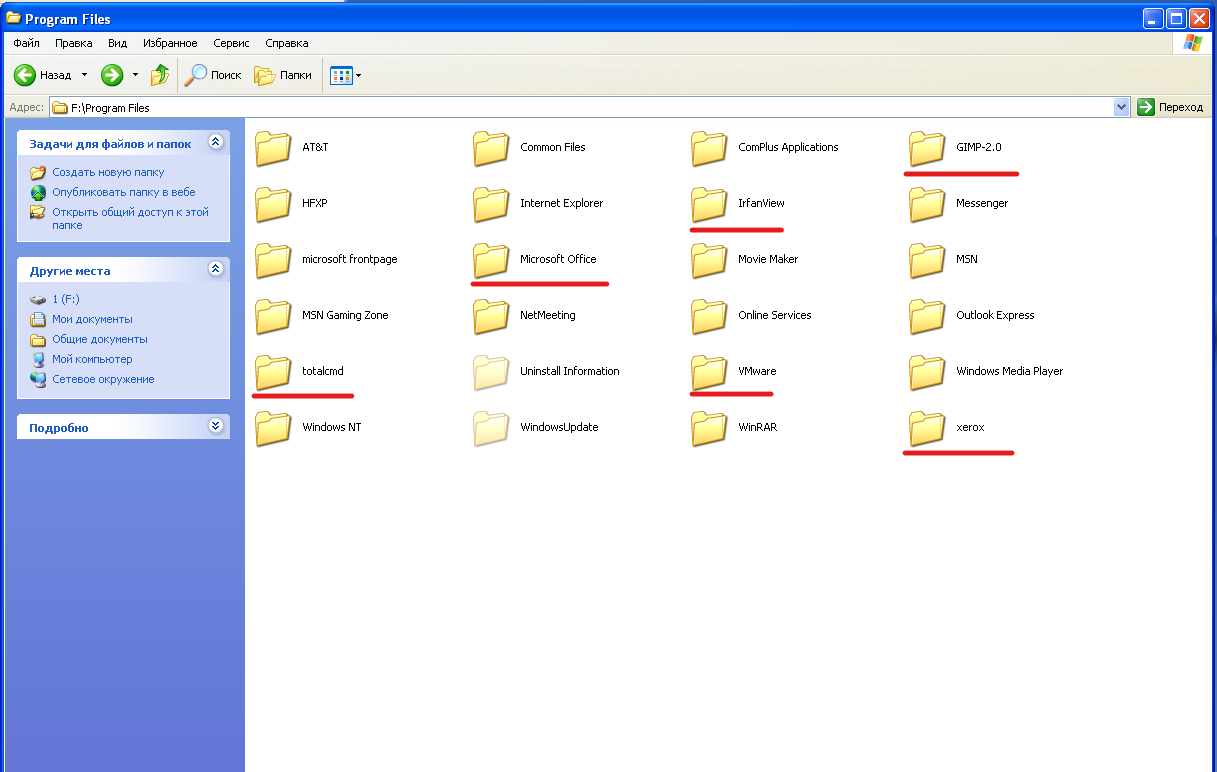


Та же программа, след в пассивном реестре:

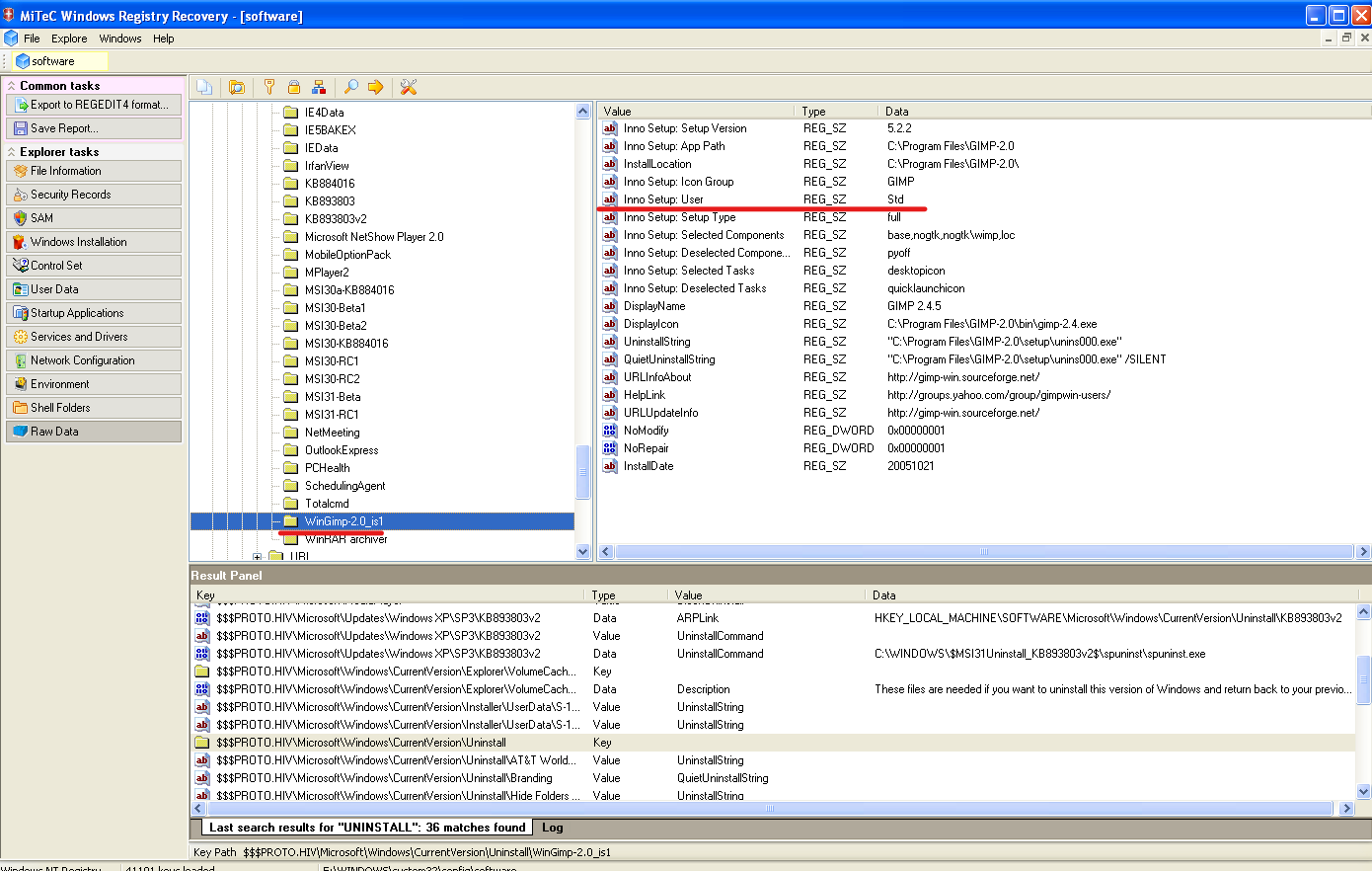


 Более того, к факту установки был причастен непосредственно пользователь Std, так к .exe-файлу программы имел доступ:

Также, в директории ProgramFiles располагались интересные для поиска следов программы, среди которых присутствовал ранее изученные Xerox и MS Office, папка TotalCommander(файловый менеджер), а также папка GIMP 2.0 (редактор растровой графики):



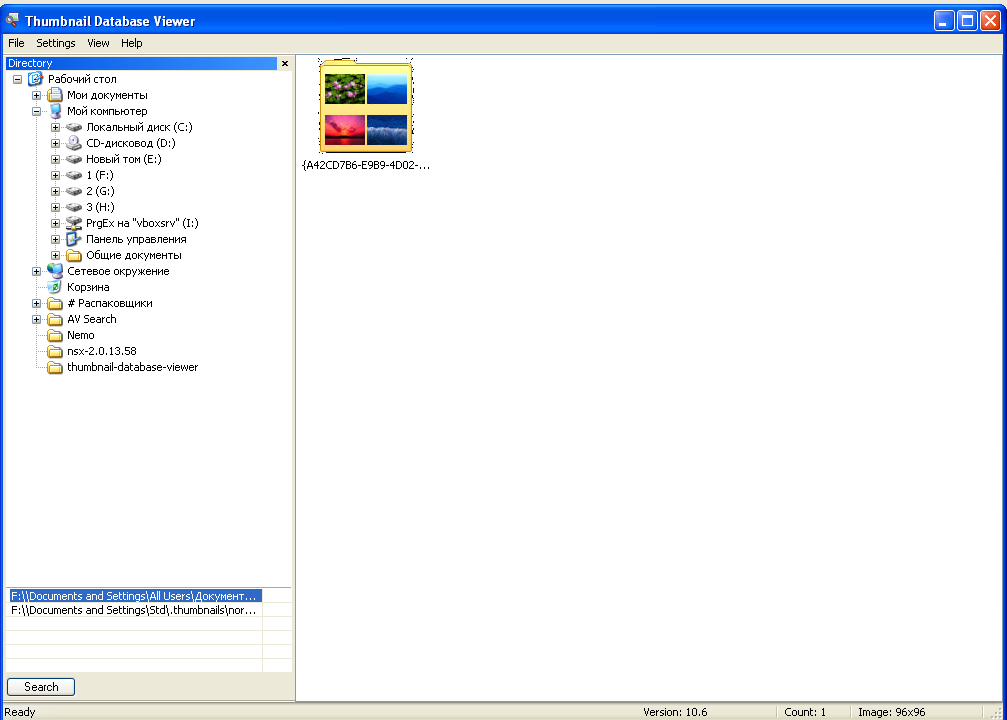
В пассивном реестре информация о GIMP также располагалась и была установлена пользователем Std:



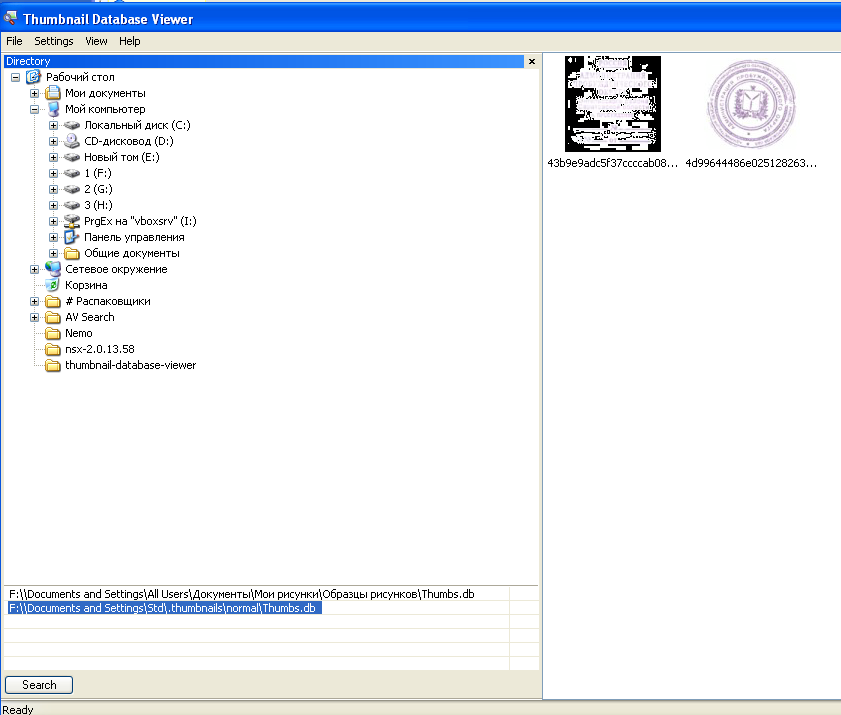
В данной части работы рассмотрены редакторы растровой графики, так что стоит отметить, что при работе, например с приложением GIMP, остаются следы ввиде .thumbnails.db-файлов (базами данных использованных миниатюр). Для работы с такими базами данных будет использовано приложение Thumbnail Database Viewer (ThumbViewer.exe).

Выполним поиск всех баз данных с такими миниатюрами на представленном носителе:

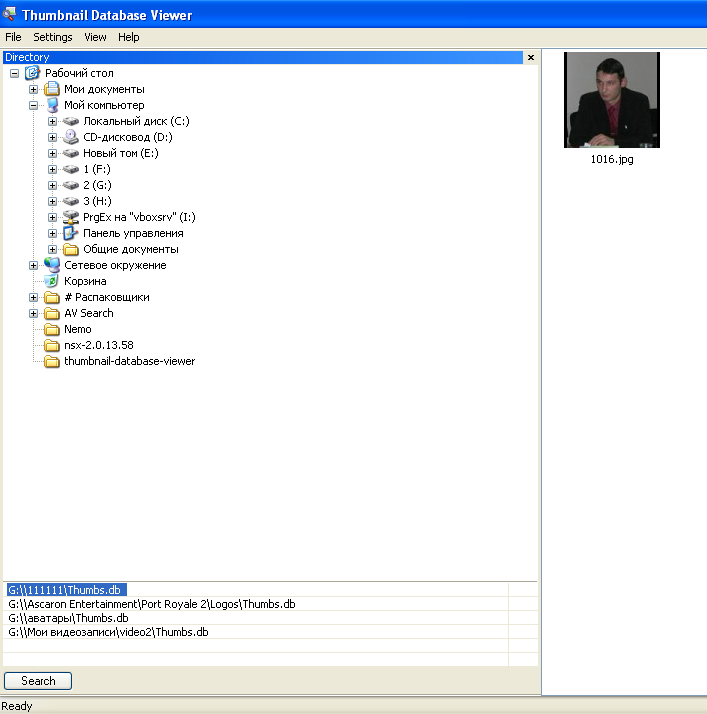
Стандартные миниатюры Windows:



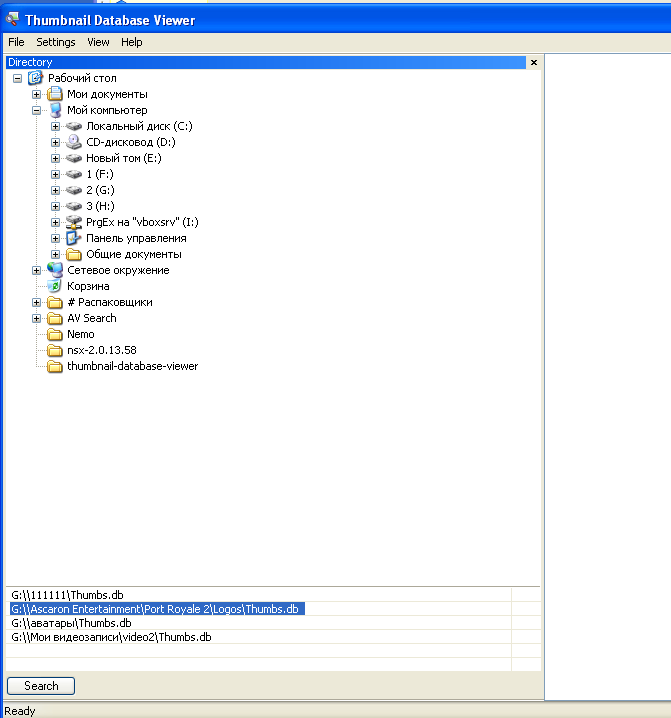
Миниатюры, расположенные по пути \\Documents and Settings\Std\.thumbnails\normal\Thumbs.db:



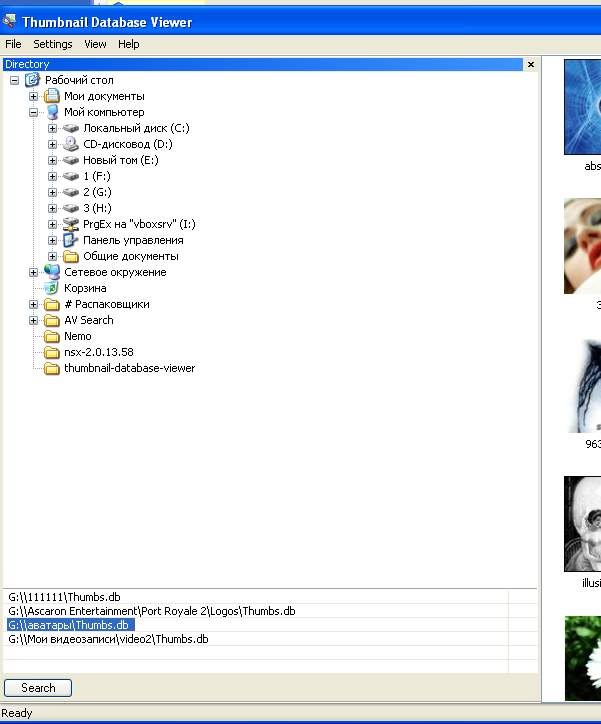
Миниатюры, расположенные по пути \\111111\Thumbs.db:



База данных, расположенная по пути Ascaron Entertainment\Port Royale 2\Logos\Thumbs.db оказалась пустой, но на самом деле она была защищена от редактирования и в последствии просмотрена, содержимое базы данных не уточняется:

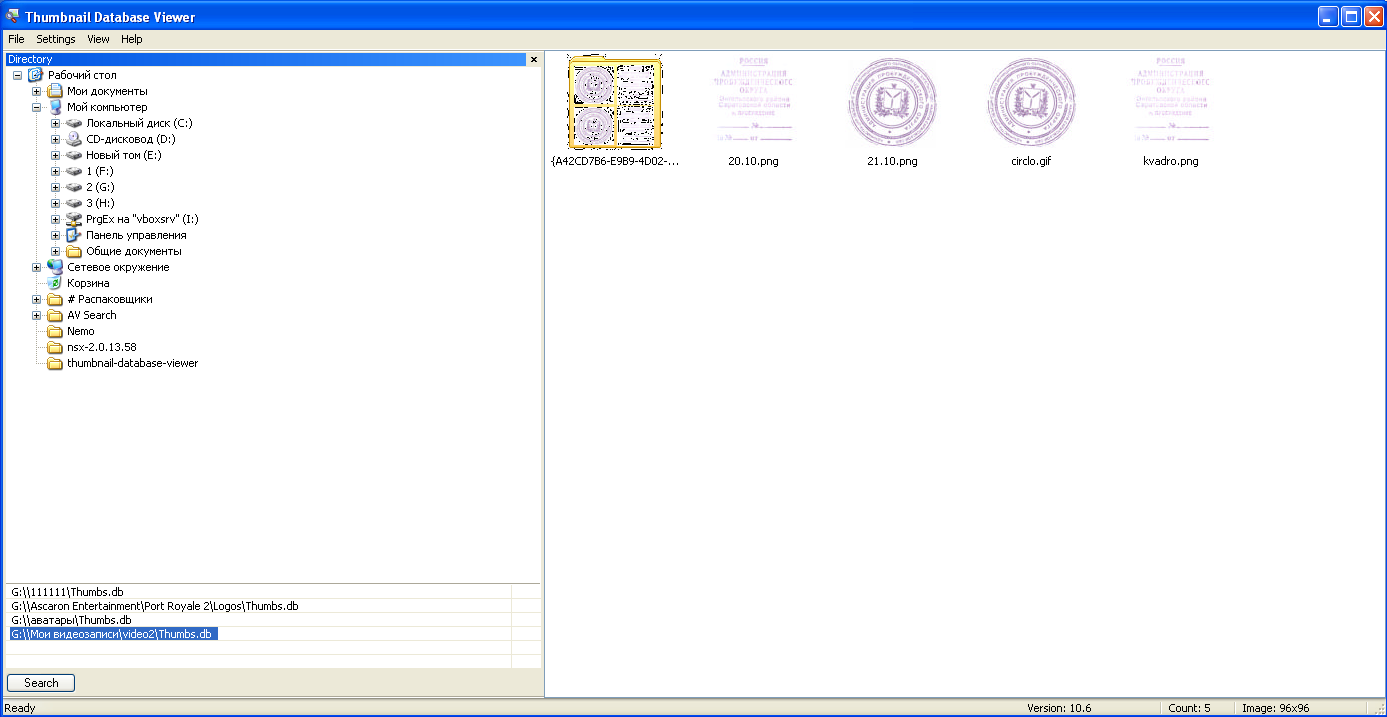


Содержимое базы данных, расположенной по пути \\аватары\Thumbs.db также не уточняется:

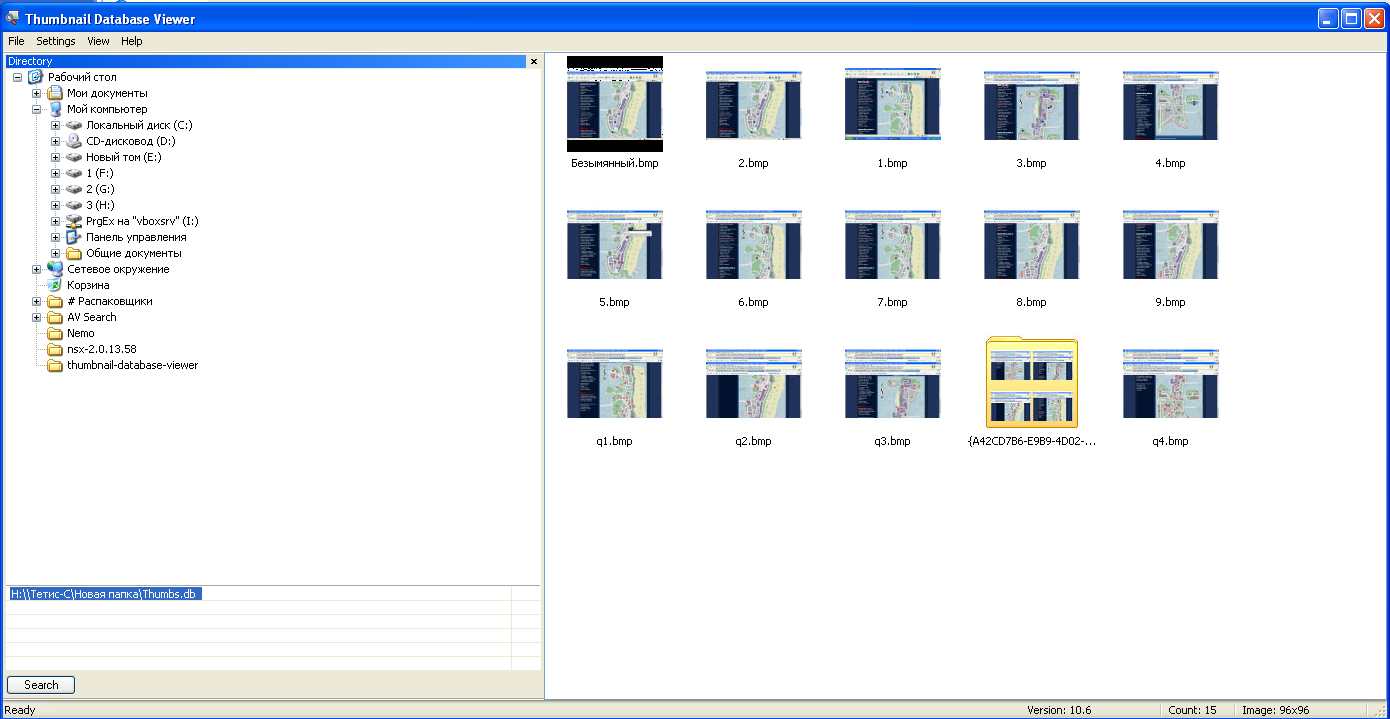


В

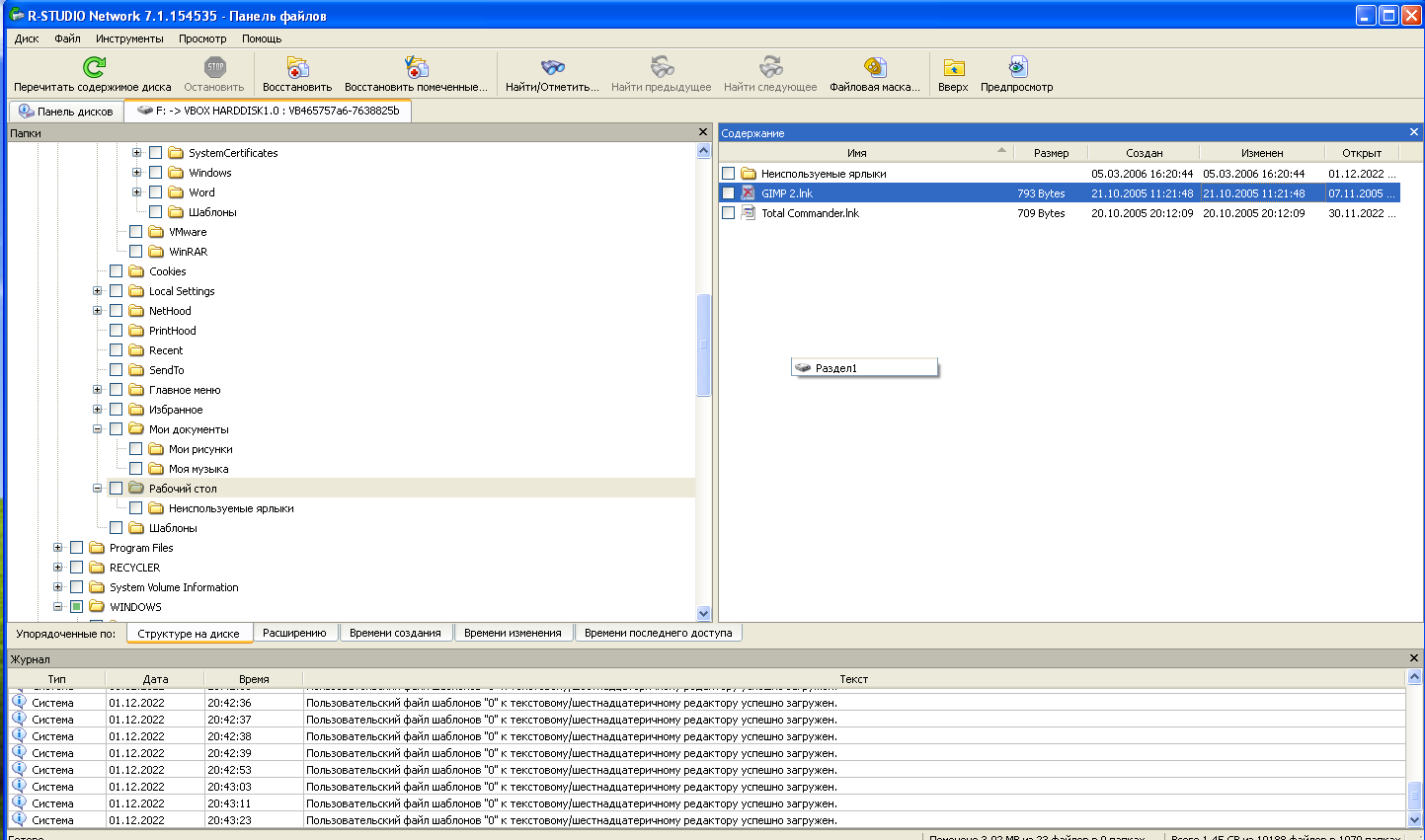
Содержимое базы данных, расположенной по пути \\Мои видеозаписи\video2\Thumbs.db:

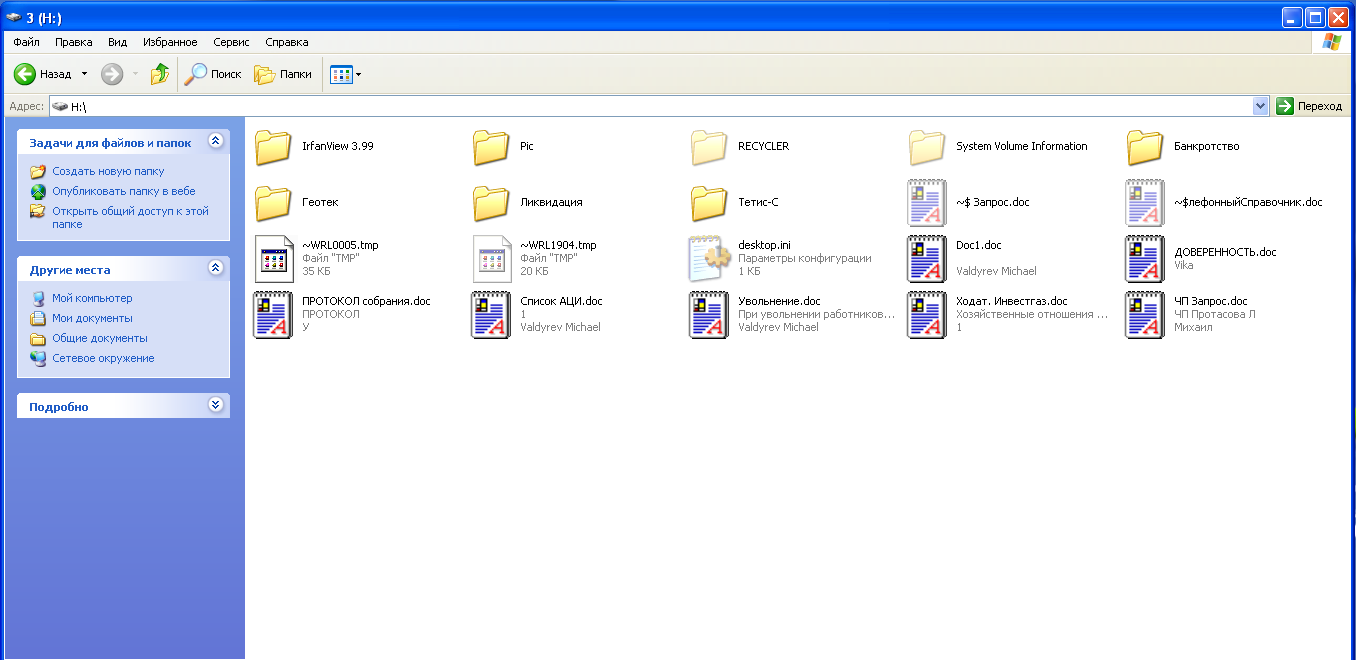


Содержимое базы данных, расположенной по пути \\Тетис-С\Новая папка\\Thumbs.db:

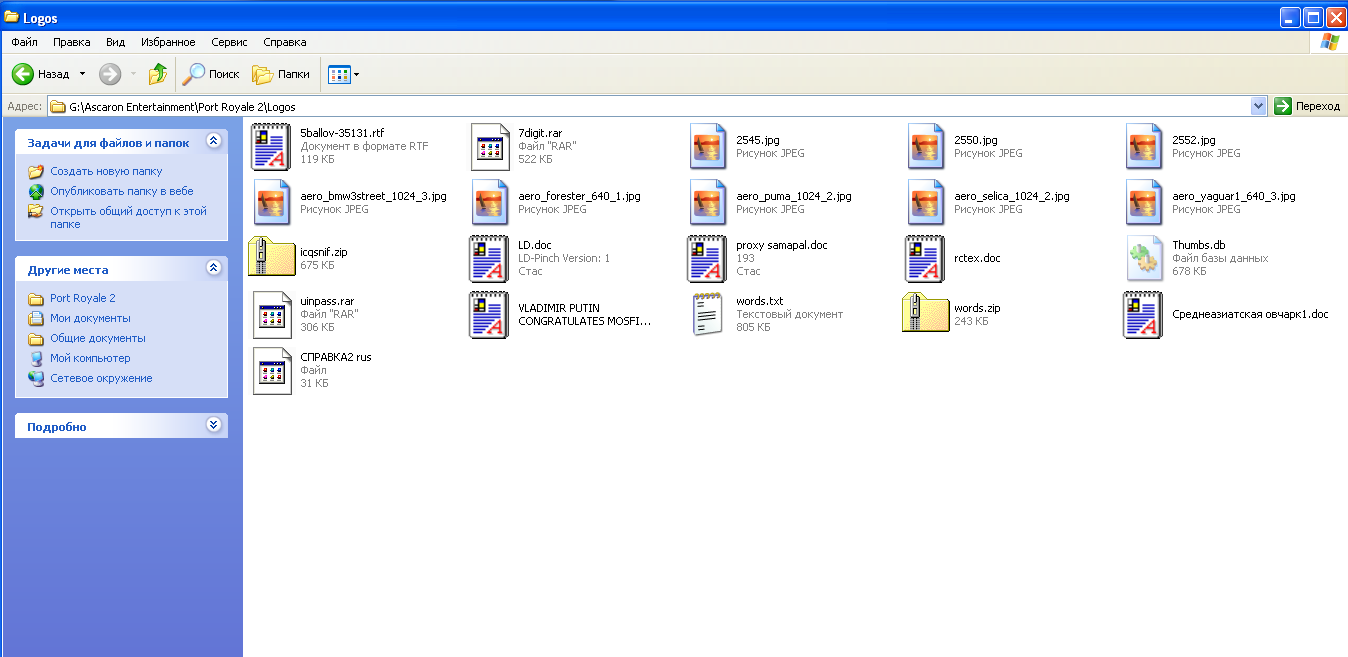


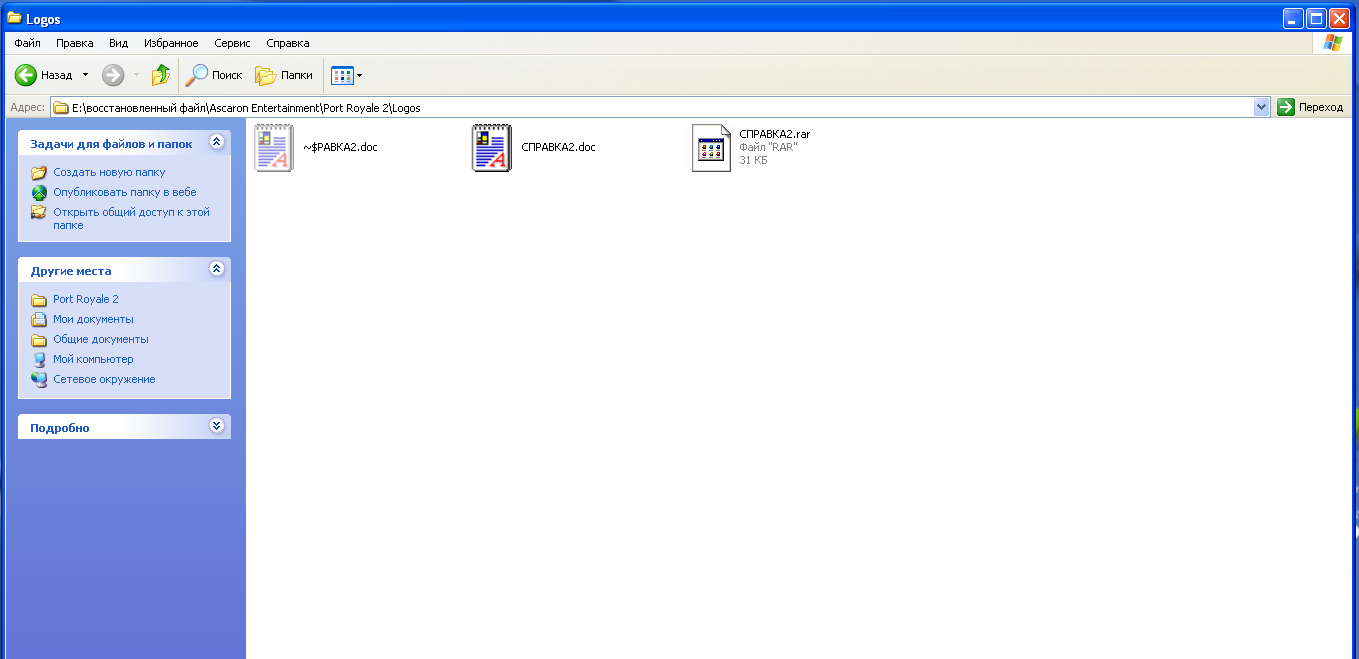
В программе R-Studio нашел, что с рабочего стола была удалена иконка GIMP:

Далее в исследовательских целях были просмотрены все разделы диска и найдено множество файлов формата .docx, к примеру:

В скриншоте выше также виды создаваемые в процессе редактирования временные файлы Word-a ~$

Интерес вызвала папка СПРАВКА2.doc, поэтому был выполнен контекстный поиск по все директориям файловой системы по запросу «\*СПРАВКА2\*» и был найден файл „СПРАВКА2 rus”:

Содержимое было восстановлено:



Далее в программе AV Search контекстным поиском были найдены все вхождения СПРАВКА2:

