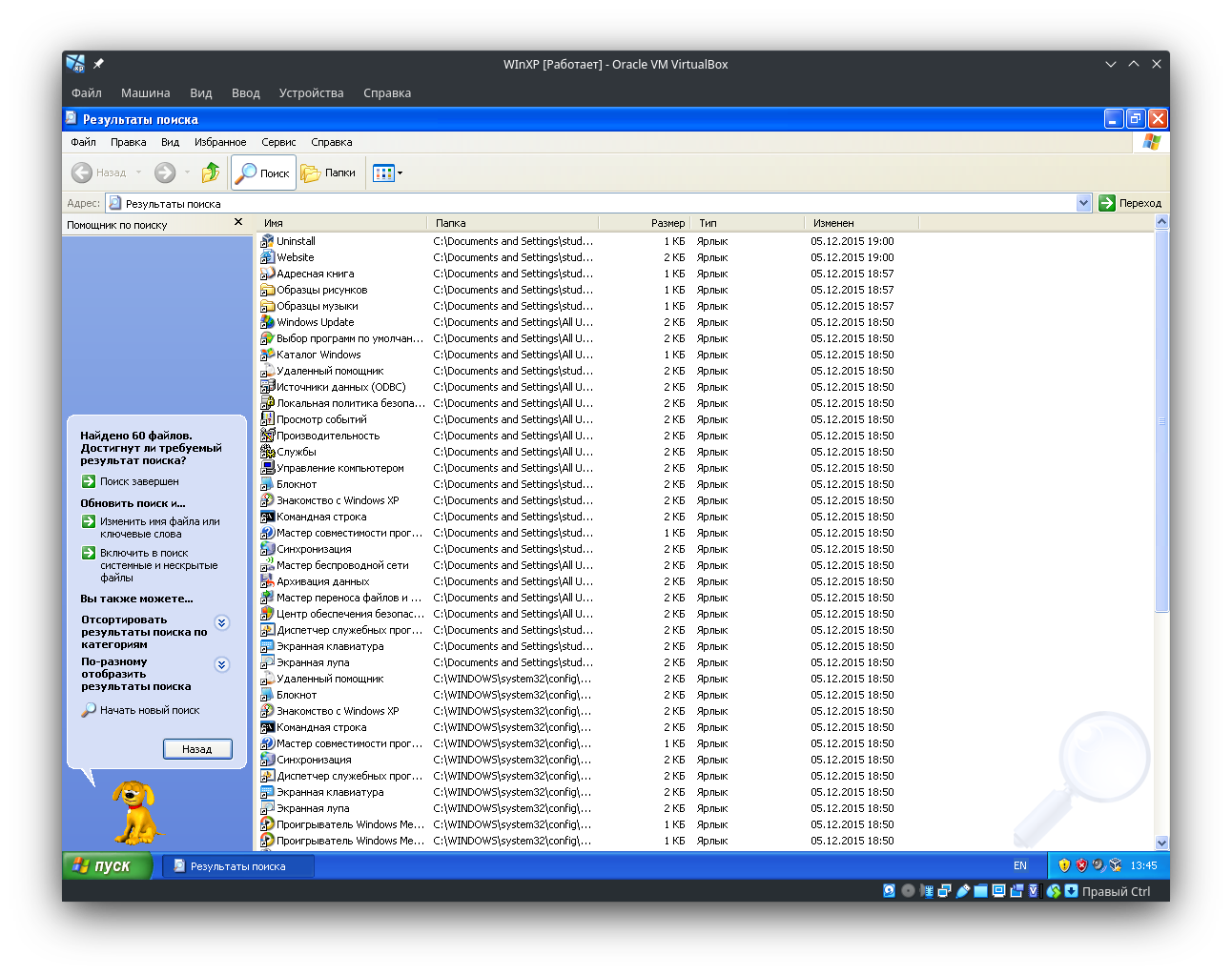
## Следы использования программного обеспечения в Windows

Ответы на вопросы предваряются опытами по обнаружению и оценке следов, возникающих вследствие действий, указанных в вопросе.

Для диагностического исследования использовать виртуальный диск резервной ОС Windows.

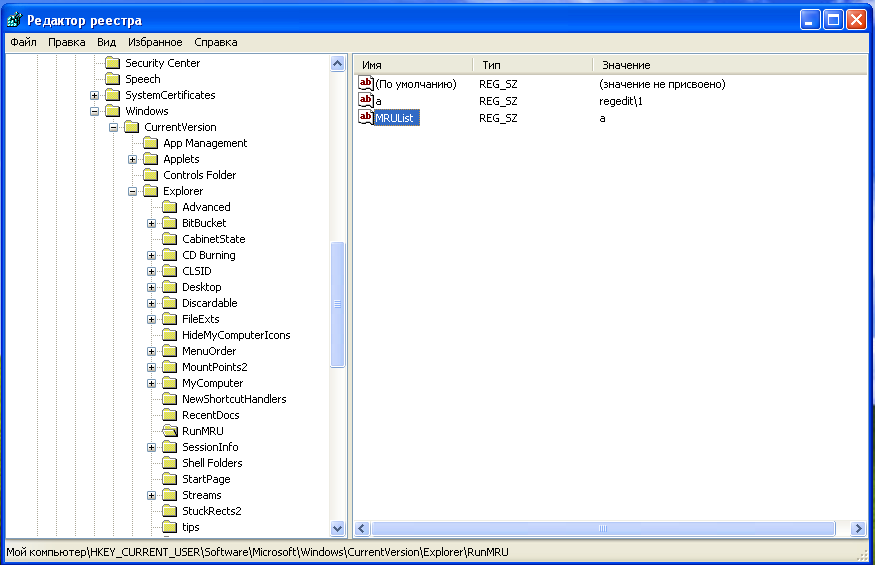
1. Собственно ОС (lnk, MRU в реестре, DR.Watson, \*.evt с помощью EventLog Explorer, Проводник)
   1. Обнаружить хранилища всех файлов LNK на системном диске. Ответить на вопросы для LNK какие файлы-документы открывались последними?



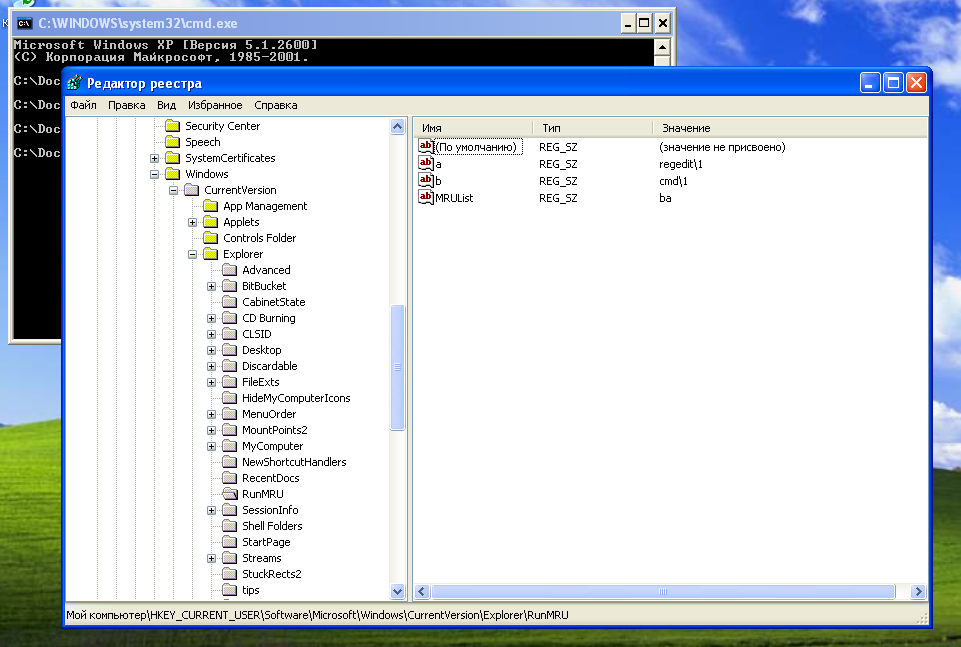
* 1. На основе анализа параметров MRU реестра и содержимого каталога Prefetch ответить на вопрос: какие программы запускались последними?

Откроем редактор реестра

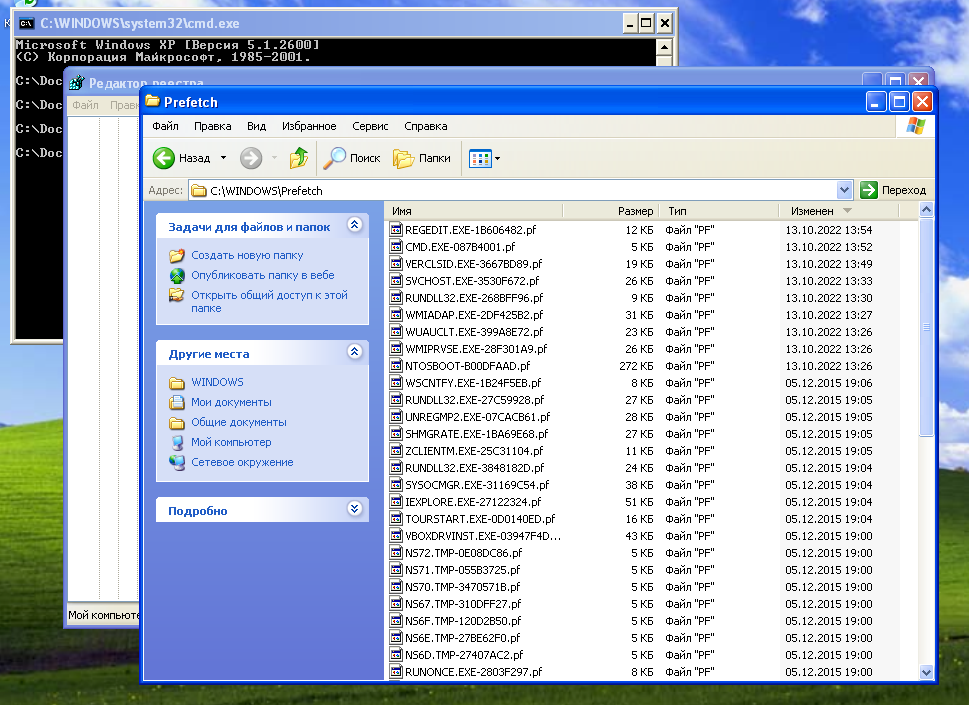
HKEY\_CURRENT\_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/RunMRU



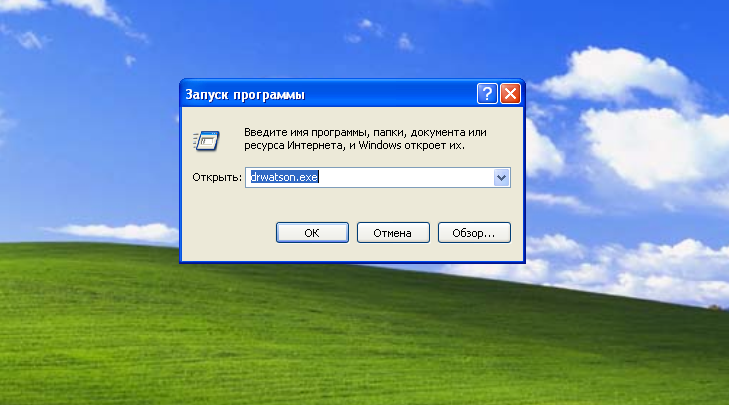
Откроем командную строку через «выполнить» и обновим редактор реестра. Список выполненных последних команд обновился.



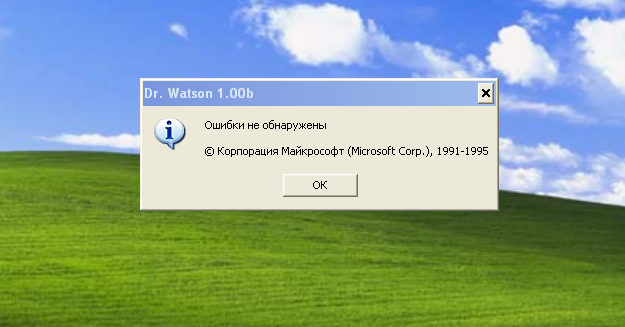
Откроем каталог С:\Windows\Prefetch, и отсортирует по дате изменения



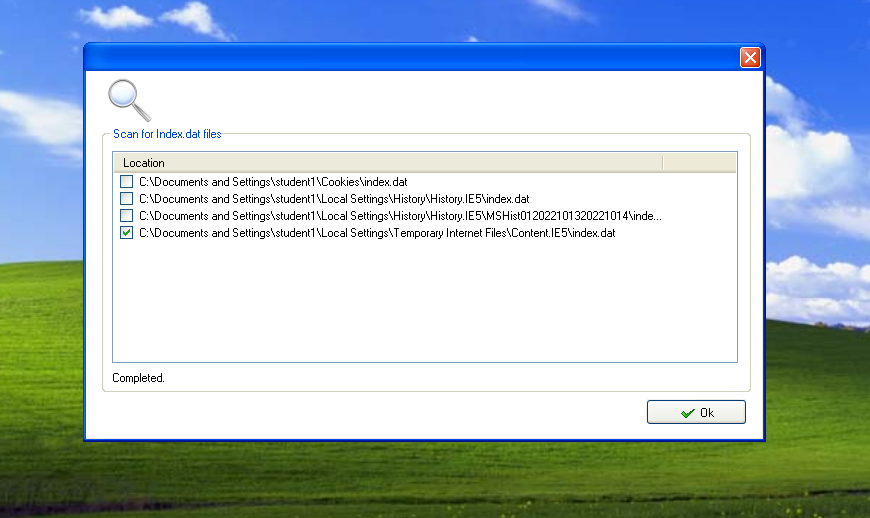
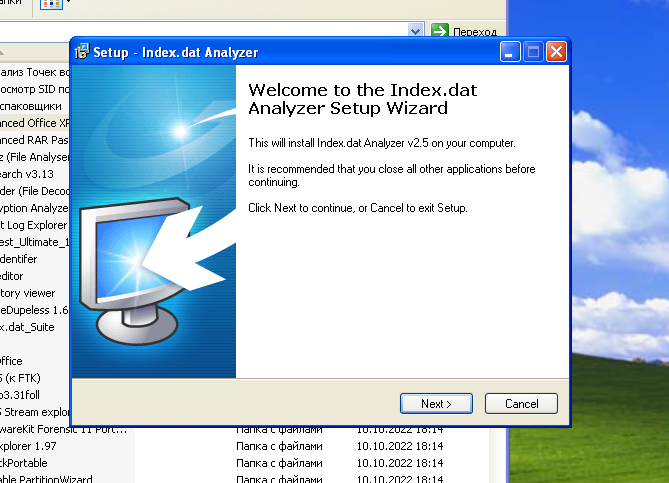
* 1. Ответить на вопросы для DR.Watson:



* + 1. Какие программы вызвали ошибку, дата и время возникновения ошибок?



* + 1. – Каковы имя компьютера, имя пользователя, количество процессоров, тип процессора, версия Windows? – ошибки не обнаружены
    2. – Какие задачи выполнялись в системе во время возникновения ошибок? – ошибки не обнаружены
    3. – Какие модули загружала каждая программа? – ошибки не обнаружены
  1. Ответить на вопросы для Проводник (С:\Documents and Settings\[профиль]\Local Settings\Temporary Internet Files\Content.IE5\ index.dat):

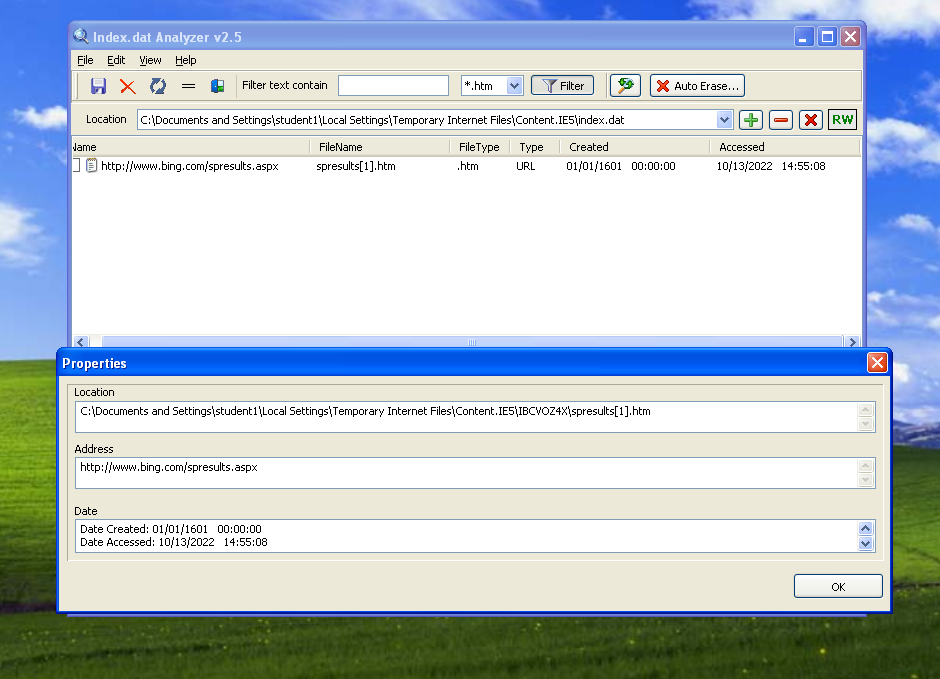


* + 1. – адреса сетевых ресурсов, посещенных пользователем,

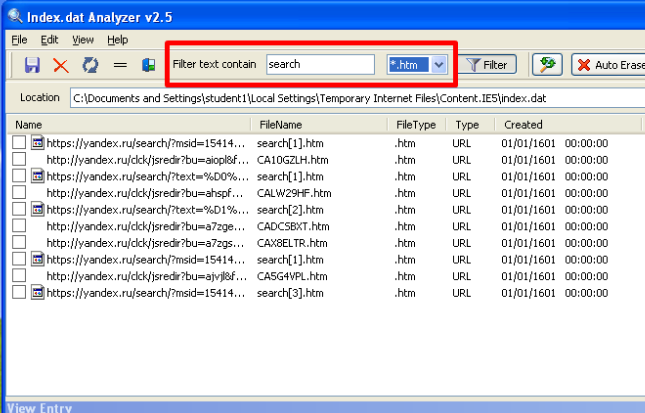
Отфильтруем все найденные программой index.dat Analyzer ссылки по маске \*.htm и

отсортируем найденные ссылки по возрастанию времени последнего доступа.

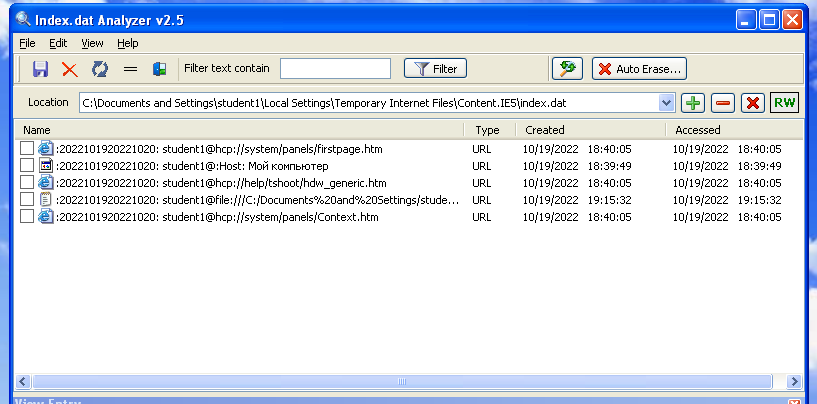
* + 1. – дату и время посещения каждого ресурса (время изменения, время доступа),



* + 1. – поисковые запросы,



* + 1. – локальную работу с файлами.



1. Офисов
   1. Методом мониторинга файловой системы и реестра Windows (ProcMon) определите области следообразования при выполнении следующих операций:
      1. Установка MSOffice2003 – только word (отследите по «Image Path» процесс SETUP, когда запустите установку; отфильтруйте список событий так же и по операции (Operation: CreateFile, RegCreateKey – см рис 1.), обратите внимание на создание файлов с расширениями \*.ini, \*.txt, \*.xml. Действительно ли изменяются dll файлы в системных каталогах windows, указанные ProcMon как создаваемые в процессе инсталляции? Установите это методом сравнения дат создания файлов до и после операции инсталляции. Для этого используйте не измененную версию ОС)

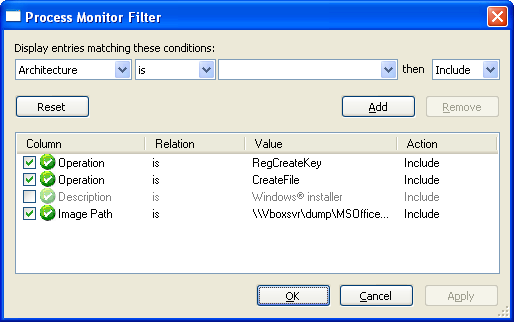
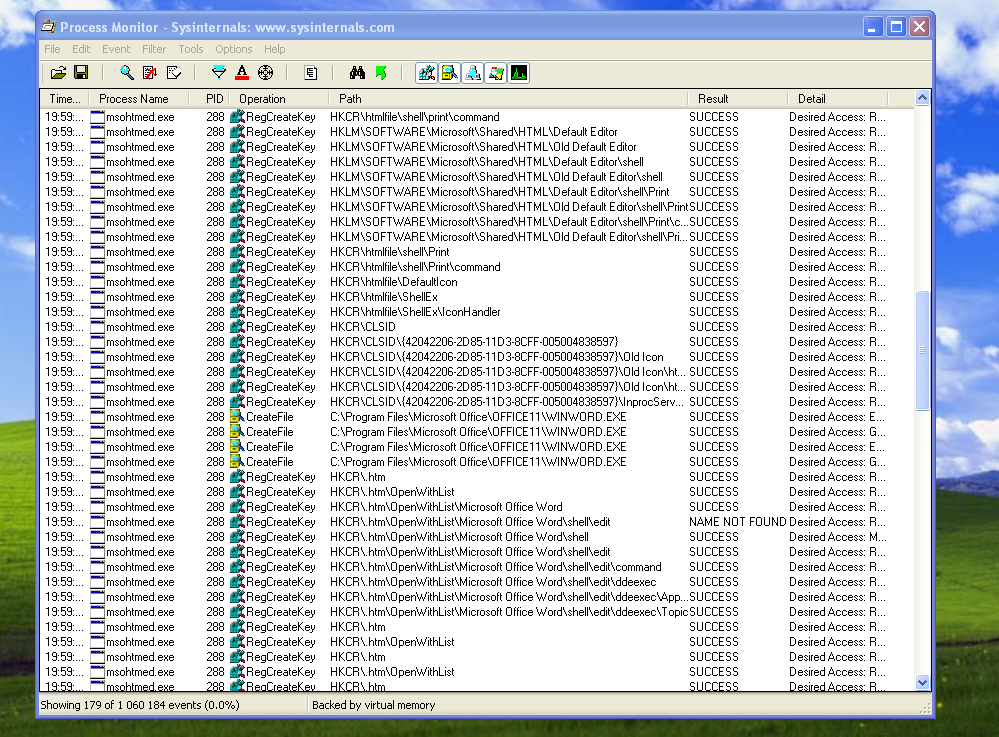
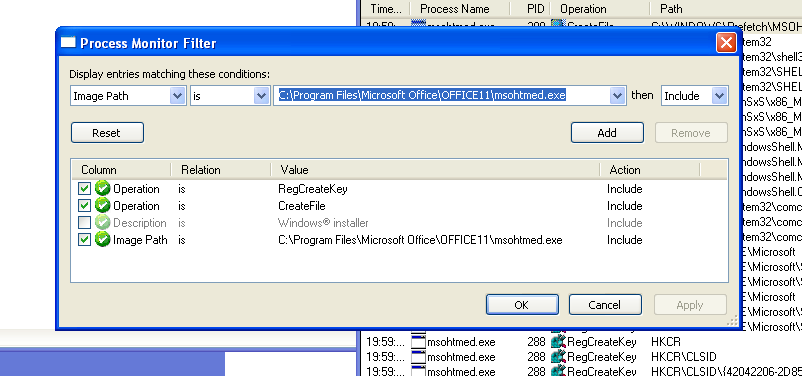
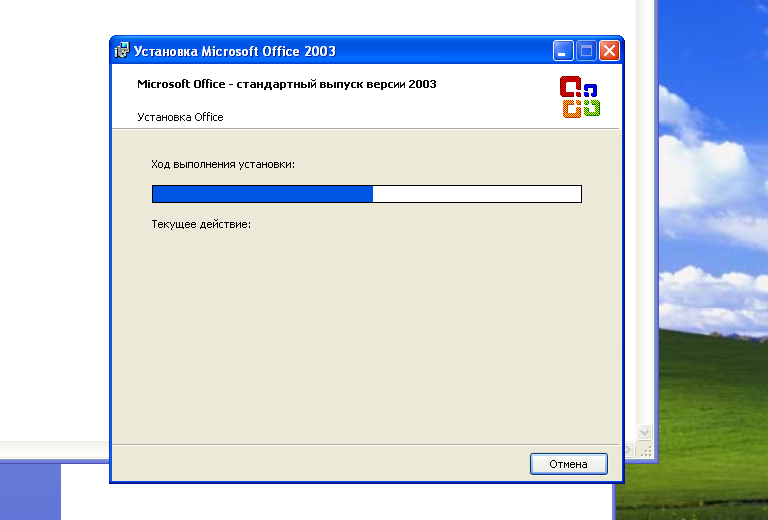
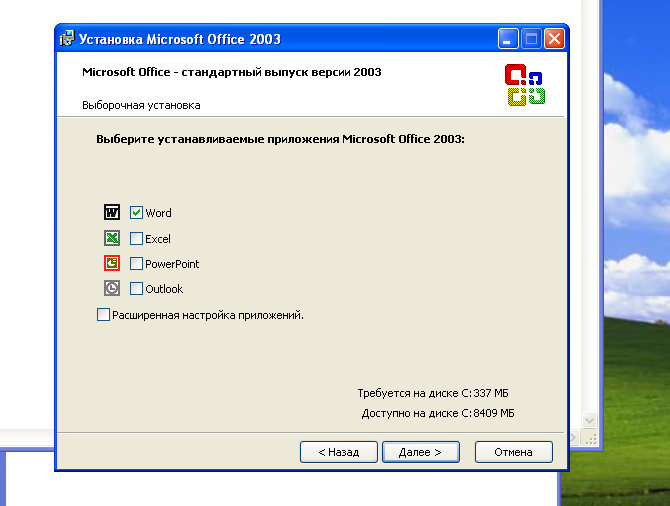
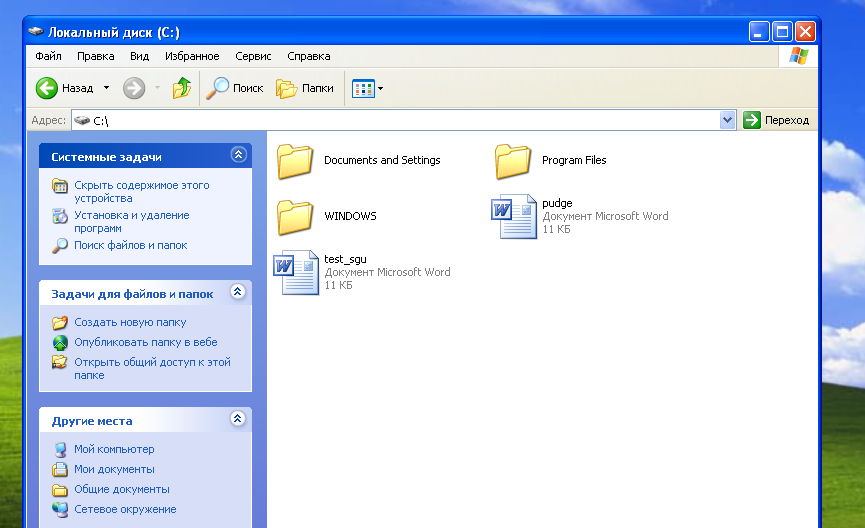


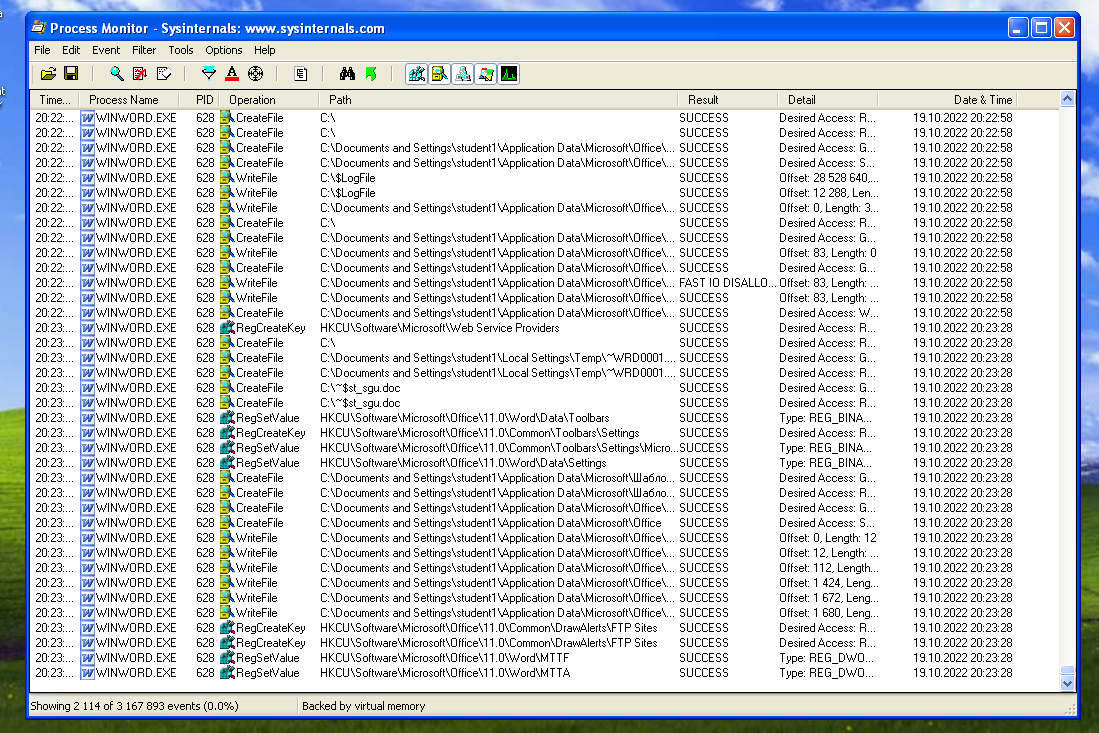
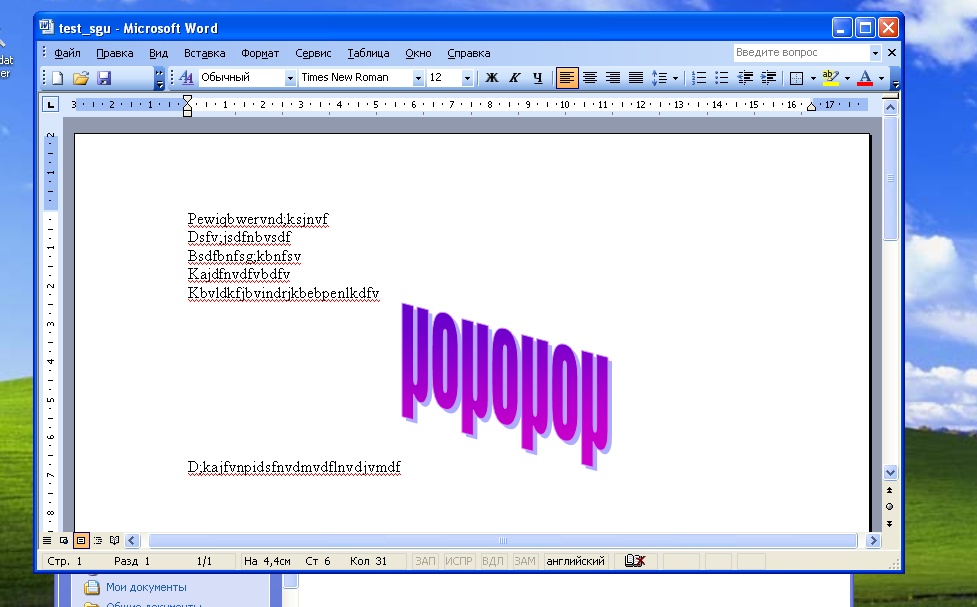
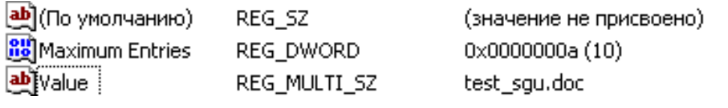
Рис. Предпочитаемые фильтры имеют установленную галочку.



* + 1. Создание и редактирование файла (Обратите внимание на создание в реестре в ветвях с именем MRU новых параметров и файлов \*.lnk, \*.doc, \*.tmp в файловой системе). С этой целью установите в ProcMon фильтры событий Image Path:WinWord, Operation: WriteFile, Write, RegSetValue.



Если создать файл test\_sgu.doc, то имя файла помещается в ветвь реестра HKEY\_CURRENT\_USER\Software\Microsoft\Office\11.0\Common\Open Find\Microsoft Office Word\Settings\Сохранение документа\File Name MRU



При создании и редактировании файла появляется файл: wrdxxxx.tmp

1. Браузера FireFox
   1. Установите этот браузер
   2. Установите в Virtual Box эмуляцию сети NAT, адаптер установите PCNet-Fast III .
   3. Методом мониторинга файловой системы и реестра Windows (ProcMon) определите области следообразования при выполнении следующих операций:
      1. Осуществите заход из виртуальной машины на сайты по протоколам http и https. Найдите области следообразования, указывающие на факт посещения сайтов.

Посещенные пользователем сайты хранятся в файле places.sqllite в папке C:\Documents and Settings\Администратор\Application Data\Mozilla\Firefox\Profiles\f86qcclg.default

