Эффективность экспертного исследования Windows XP.

Декабрь 2001

Авторы:Kimberly Stone и Richard Keightley

Перевод: Фомичев Александр Николаевич
Корректоры: Михайлов Игорь Юрьевич
Капинус Ольга Валерьевна

Аннотация

Windows XP- последняя разработка компании Microsoft, которая все чаще и чаще является объектом судебной экспертизы. Эксперты тщательно изучают возможности Windows XP для использования результатов ее исследования в качестве доказательств.

Есть разные мнения относительно того, как проводить судебную экспертизу XP систем. Существует масса спекуляций на тему, что Windows XP существенно препятствует проведению судебной экспертизы. Ниже будет проверена эта версия а так же возможность использования Windows XP в качестве ОС стенда для проведения КТЭ.

Данное тестирование проводилось с использованием EnCase®. EnCase - это windows- приложение, ориентированное на поиск улик судебными экспертами на жестких дисках (НЖМД). Кроме этого, в данной работе проведено исследование файловой системы Windows XP.

Введение

Windows XP позиционируется, как операционная система, отличительной чертой которой является: стабильность, дружелюбие по отношению к пользователю и т.п., и что особенно важно для экспертов, повышенная безопасность. Она заключается в «гарантированном» удалении файлов («scrubbing») и встроенной возможности шифрования файлов.

Данная работа показывает, что экспертам необходимо четкое понимание работы NTFS (файловая система Windows XP). В противном случае, в сфере компьютерной безопасности появится много мифов, связанных с Windows XP.

Windows XP поставляется в двух вариантах: Home Edition Windows XP и Professional Windows XP. Данное исследование проводилось на Professional Windows XP, так как Home Edition Windows XP - это урезанная версия Professional Windows XP (далее под Windows XP мы понимаем Professional Windows XP).

Используемые термины приведены в конце.

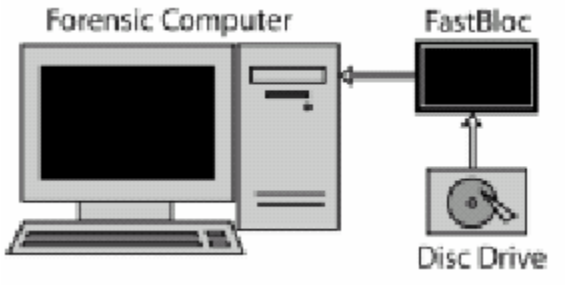
Часть 1 Тестирование: Windows XP как платформа для работы эксперта

Подобно любой новой операционной системе от Microsoft, Windows XP,в отличие от старых версий, нуждается как в большем объеме жесткого диска(1,5 Гб при полной установке), так и оперативной памяти. Microsoft рекомендует чтобы пользователям устанавливали 128 Мб оперативной памяти. Для комфортной работы нужно 256 Мб, особенно если использовать все особенности XP. Придерживаясь рекомендаций Microsoft, все испытания проводились на типичном персональном компьютере (процессор P-III 600 МГц, 128 Мб оперативной памяти), с использованием EnCase® v3.16.

[Обратите внимание: судебные эксперты используют высокопроизводительные системы с большим объемом оперативной памяти и жесткими дисками большей емкости].

Экспертные методы

При подготовке к тестированию диск объемом 8.4 Гб был стерт, разбит на разделы и отформатирован в NTFS (это необходимо, чтобы использовать возможность Windows XP – шифрования файлов). Значительное количество файлов было скопировано, некоторые из них были зашифрованы, а другие - удалены, чтобы сымитировать типичный жесткий диск.



Накопитель на жестком диске был подключен через интерфейс IDE с использованием FastBloc™ (специальное аппаратное средство, поставляемое Guidance). Установка FastBloc в Windows XP проста. Для Windows ’98 и Windows 2000 требуется установочный диск, а Windows XP самостоятельно обнаруживает и устанавливает драйвера для FastBloc без каких-либо запросов к пользователю.

Следующий шаг - это создание образа диска Windows XP Professional и в Windows 2000 (SP2) как с компрессией, так и без нее.

Результаты теста: создание образа диска:

Без сжатия

• Windows 2000: 15 минут, 6 секунд
• Windows XP: 14 минут, 45 секунд

С максимальным сжатием

• Windows 2000: 30 минут, 16 секунд
• Windows XP: 30 минут, 2 секунды

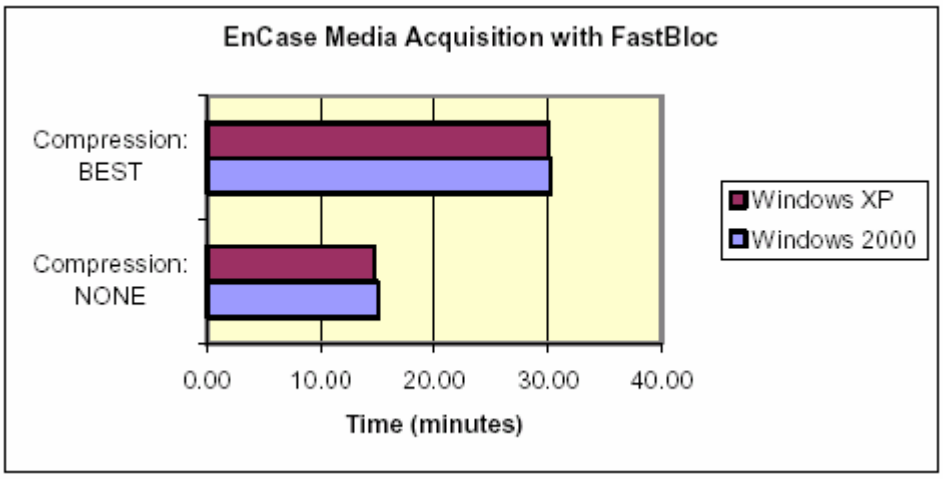


Рис.2. В Windows XP образ диска был создан быстрее, чем в Windows 2000.

Как показал данный тест, образ диска в ОС Windows XP был создан быстрее, чем в Windows 2000.

Зная потребности XP в оперативной памяти, было бы логично сделать предположение, что Windows 2000 будет побеждать Windows XP в каждом

тестировании, однако оказалось, что это не так. Далее, EnCase 3.16 работала в ОС Windows 2000 Professional (sp2) и в Windows XP.
Было проведено еще пять тестов:
Тест 1: Распознавание форматов файлов

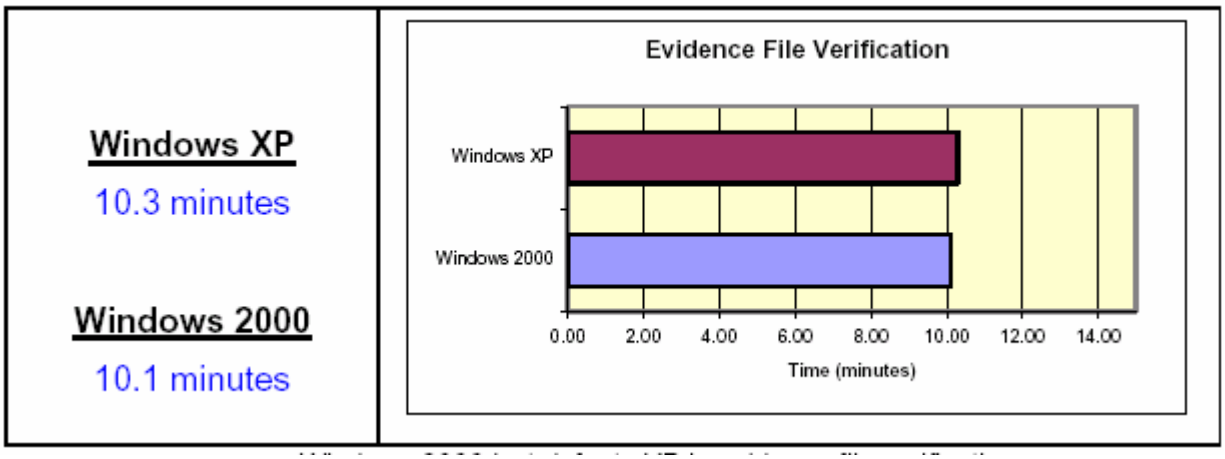


Рис.3. Windows 2000 произвела анализ файлов быстрее, чем Windows XP.

Тест 2: Хеширование диска

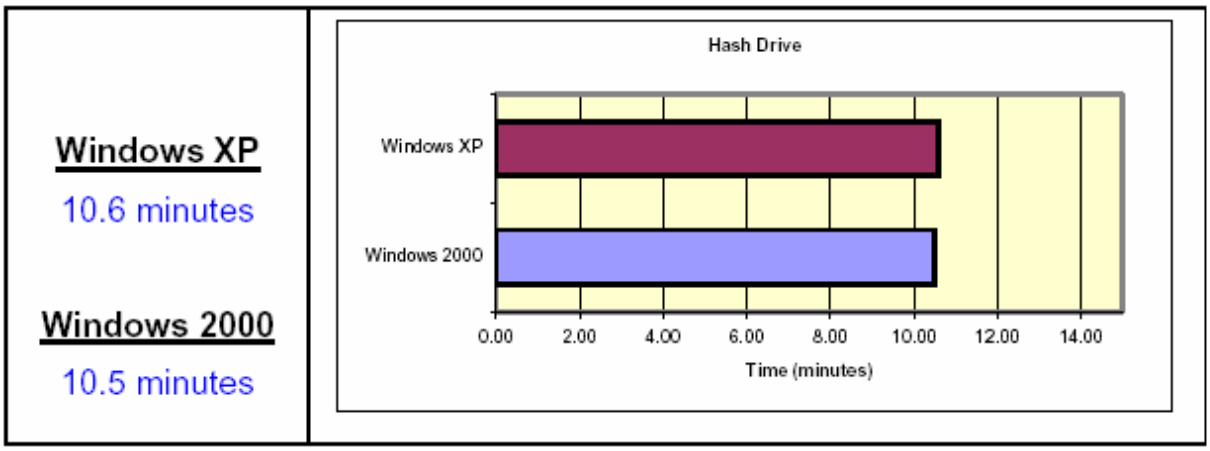


Рис.4. Windows 2000 быстрее произвела хеширование диска, чем Windows XP.

Тест 3: Поиск по 1 ключевому слову

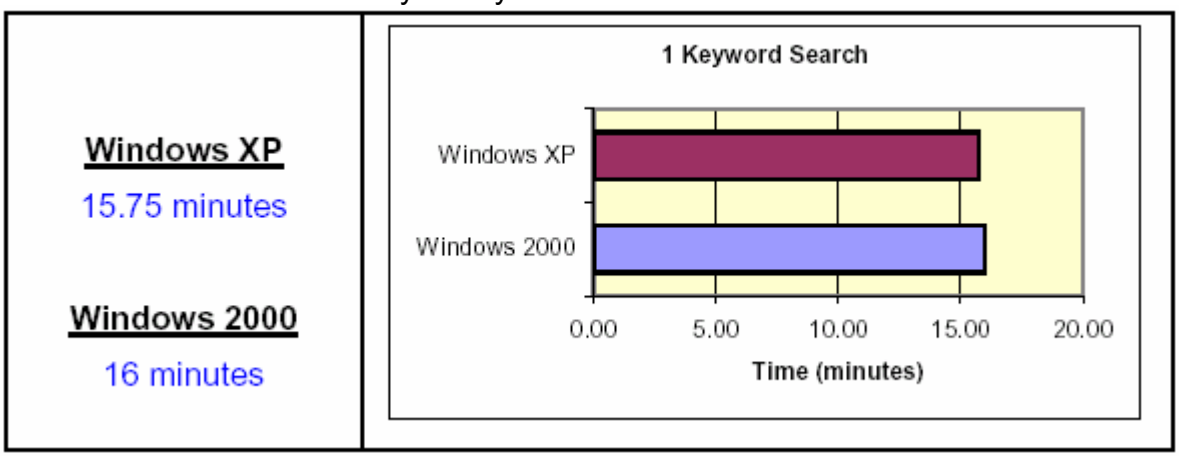


Рис.5. Windows 2000 только в этом тесте уступает Windows XP.

Тест 4: Поиск по 10 ключевым словам

Windows XP

102.5 minutes

Windows 2000

60.75 minutes

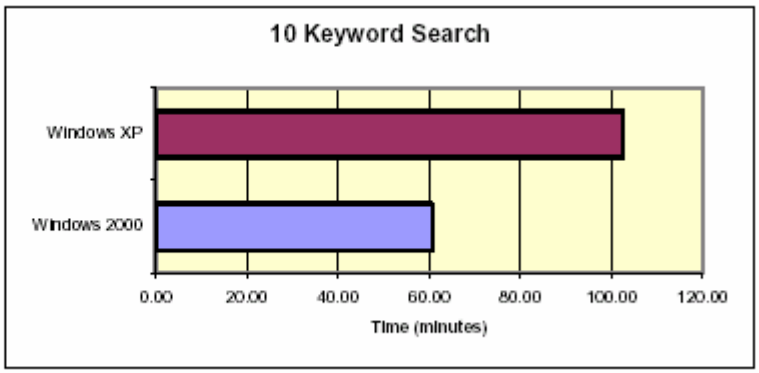


Рис.6. Windows 2000 вне конкуренции в поиске по 10 ключевым словам.

Тест 5: Предпросмотр в галерее объектов

Windows XP

8 seconds

Windows 2000

6 seconds

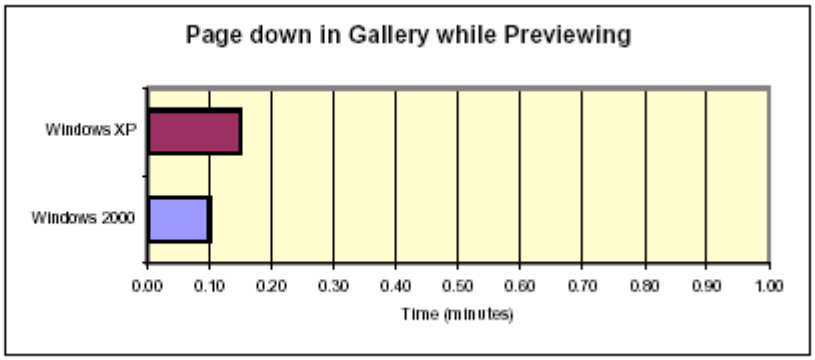


Рис.7. Снова 2-х секундная задержка.

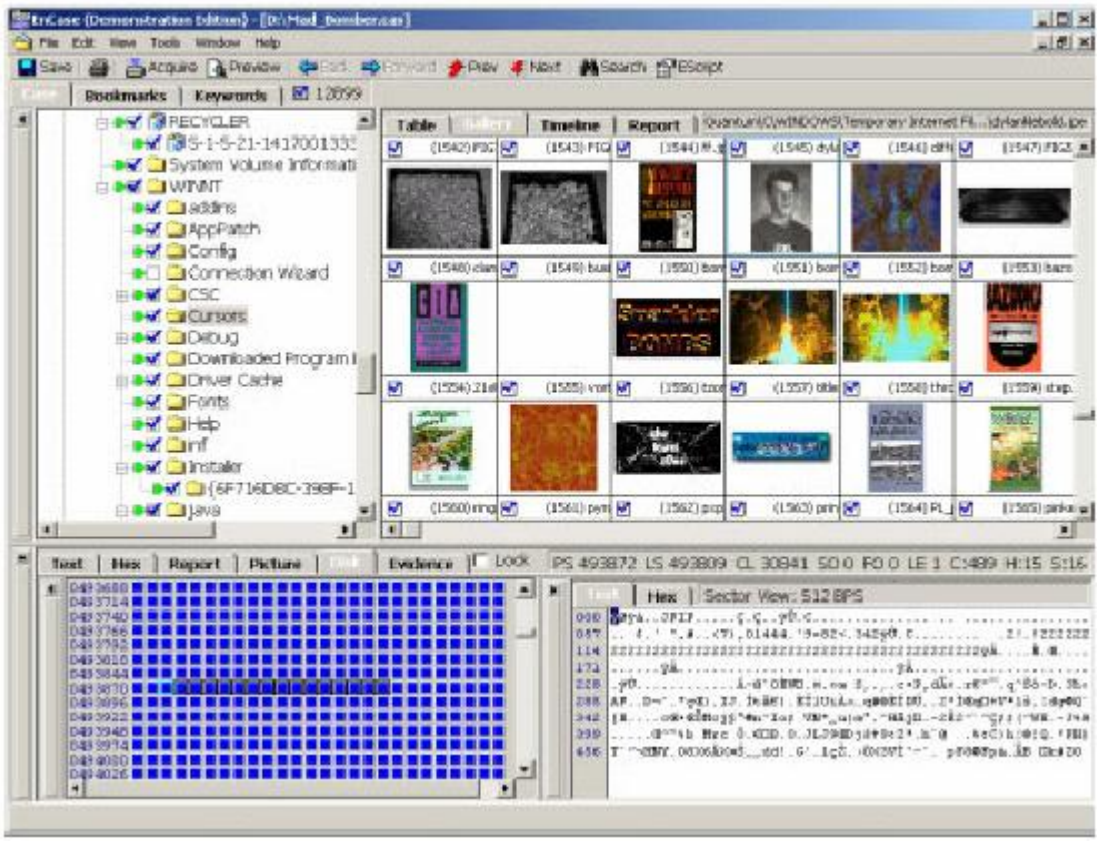


Рис.8. Предпросмотр в EnCase.

Результаты пяти тестов:
Как показано выше, Windows 2000 выигрывает у Windows XP в большинстве тестов, отставая только в поиске по одному ключевому слову, но вне конкуренции в поиске по 10 ключевым словам.

Один из самых интересных результатов показал тест при предпросмотре графических объектов в галерее объектов. Windows 2000 выигрывает у Windows XP две секунды. При просмотре одной страницы это не критично, однако, при просмотре большого количества страниц, разница ощутима.

Приведенные тесты показывают, что с EnCase можно комфортно работать в Windows XP и даже в некоторых случаях быстрее, чем в Windows 2000.

Часть 2 Экспертный анализ Windows XP
Введение
В настоящее время, большинство компьютеров поставляется с Home Edition или Professional версиями Windows XP. Поэтому, судебным экспертам необходимо знать файловую систему Windows XP для эффективного выполнения своих обязанностей. В данной статье сосредоточено внимание на следующих аспектах: 1) особенности файловой системы Windows XP; 2) особенности хранения и удаления файлов; и 3) «гарантированное» удаление файлов.
Создание, хранение и удаление данных - основная функции любой файловой системы. Как данные создаются, где они хранятся и что происходит при удалении - вопросы, которые постоянно задаются экспертам. Восстановление данных в каждой из этих стадий тоже один из главных вопросов. При появлении новой операционной системы появляется много вопросов. Эксперты должны решить как

проводить исследования, где искать данные и какой ожидать результат. Это руководство затронет эти вопросы и расскажет про «гарантированное» удаление данных.
Многие особенности файловой системы NTFS не описаны в этом документе, так как это не новые возможности NTFS в Windows XP.

Начало тестирования
EnCase 3.16 использовалась во всех тестах, в которых были проверены основные возможности файловой системы Windows XP.

ШАГ 1 – ФАЙЛОВАЯ СИСТЕМА
Windows XP Professional (версия 5.1, сборка 2600), была установлена на диск емкостью 4 Гб, который был предварительно очищен. В процессе установки была создана учетная запись администратора. Затем компьютер был выключен, с жесткого диска снят образ. По умолчанию, Windows XP устанавливает NTFS (однако при установке можно выбрать и FAT32). В нашем случае была установлена NTFS.
В первую очередь была исследована NTFS. В процессе установки на логическом диске NTFS были созданы файлы, примерно такие же, как и при установке Windows 2000.

System File	Windows NT	Windows 2000	Windows XP
MFT	X	X	X
MFT Mirror	X	X	X
Log File	X	X	X
Volume	X	X	X
Attribute Def. Table	X	X	X
Root Filename Index	X	X	X
Cluster Bitmap	X	X	X
Partition Boot Sector	X	X	X
Bad Cluster File	X	X	X
Secure File	-	X	X
UpCase Table	X	X	X
Quota Table	X	-	-

Были созданы следующие папки: $Extend, Documents and Settings, Program Files, Recycler, System Volume Information, and Windows. Это по существу то же самое, что и в Windows 2000, только вместо WINNT - WINDOWS.
Структура Master File Table (MFT) была проанализирована, и было выявлено, что она практически такая же, как и в предыдущих версиях. Записи MFT и атрибуты файлов остались без изменений.
Резидентные и нерезидентные данные хранятся так же, как и в предыдущих версиях NTFS.

ШАГ 2 – ХРАНЕНИЕ ФАЙЛОВ
Было проведено несколько тестов, чтобы определить: как файлы хранятся в Windows XP. Был запущен Windows XP и созданы три небольших текстовых файла, которые были сохранены на диске. Затем с диска был снят образ и файлы были исследованы. Все три файла сохранены в MTF, как резидентные.

Была запущена Windows XP и созданы пять больших файлов. Затем с диска был снят образ. Файлы были все сохранены как нерезидентные данные. В MFT были прописаны указатели на места хранения данных.

В целом, процесс хранения происходит таким же образом, что и в предшествующих NTFS-системах. Это обеспечивает хорошую основу для тестирования процесса удаления.

ШАГ 3 – УДАЛЕНИЕ ФАЙЛОВ

Первый шаг в исследовании жесткого диска Windows XP - удаление резидентного файла. Серия испытаний проводилась, когда были созданы резидентные файлы, удалены в корзину и удалены из корзины. Для получения результатов использовалась EnCase. Первичное удаление осталось тем же самым, как и в предыдущих версиях Windows: запись файла в MFT обновляется при удаление из «мусорной» корзины. Процесс удаления остался таким же; записи MFT, содержащие резидентные данные, остаются в MFT как удаленные, пока не переписываются новыми записями MFT. Как заключительное испытание, было создано 150 резидентных файлов. Все они были затем удалены. С жесткого диска был снят образ, который затем был проанализирован программой EnCase. EnCase показала все удаленные файлы.

Тот же ряд испытаний проводился с нерезидентными файлами, которые были созданы, удалены в корзину и удалены из корзины. EnCase использовалась чтобы отследить записи MFT и перемещение данных в процессе тестирования. Когда файлы были удалены в корзину, а затем и из нее, записи MFT оставались помеченными как удаленные, пока не переписывались новыми записями MFT. Данные оставались нетронутыми в группах, пока не переписывались другими файлами. Процесс предварительного удаления остался таким же, как и в предыдущих версиях Windows. Как заключительное тестирование нерезидентных файлов, было создано 150 файлов с нерезидентными данными. Все они были затем удалены. С жесткого диска был снят образ, который затем был использован для анализа EnCase. EnCase показала все удаленные файлы.

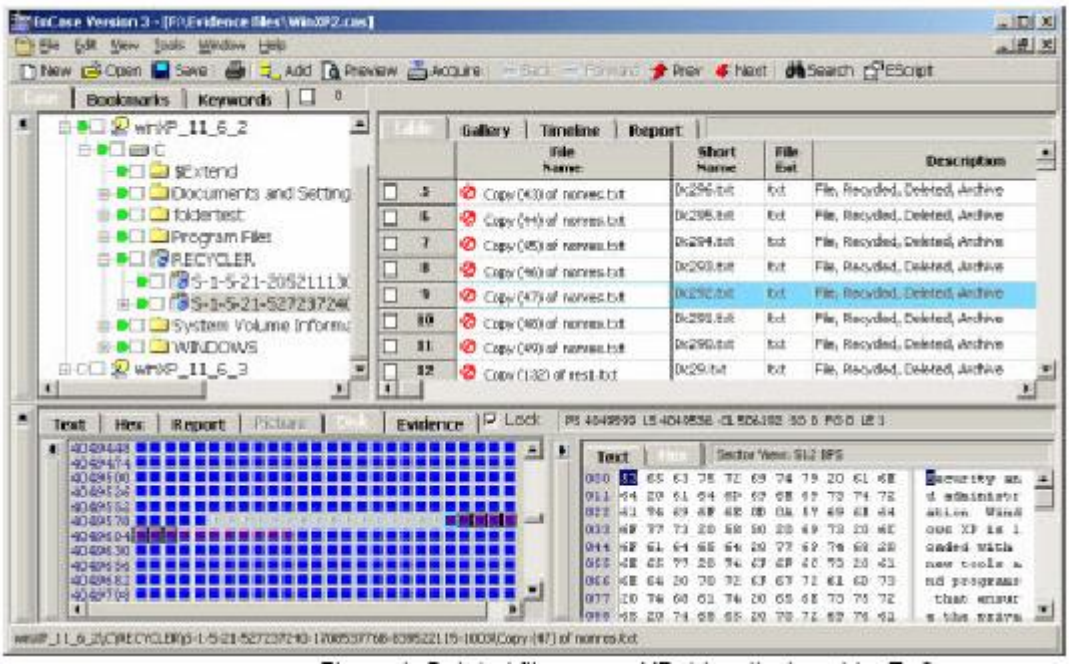
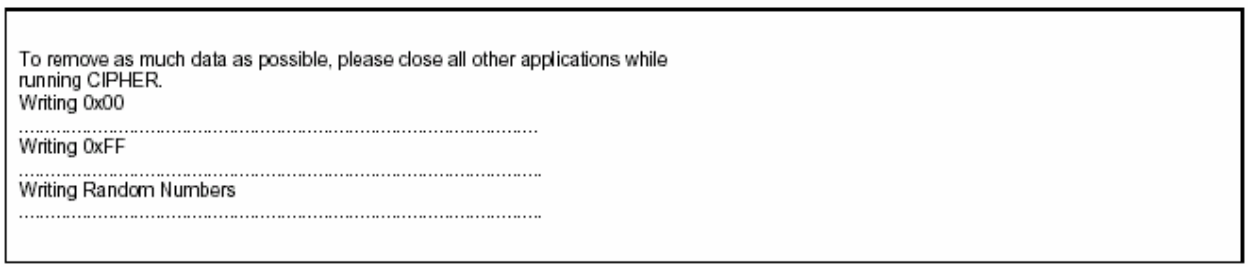


Рис.9.Удаленные файлы видны в EnCase.

ШАГ 4 – «ГАРАНТИРОВАННОЕ» УДАЛЕНИЕ

Windows 2000 и Windows XP поддерживают так называемое «гарантированное» удаление. Наличие этой возможности породило множество вопросов и домыслов. Эта функция обеспечивается запуском из командной строки специальной программы (CIPHER), включенную в Windows 2000 и Windows XP, которая обеспечивает дополнительную возможность для управления EFS. Версия программы, включенная в Windows XP, предназначена для переписывания или «гарантированного» удаления данных. Программа делает три прохода и делает записи по незанятым местам логического диска. Первый проход – шестнадцатеричный 00, второй - шестнадцатеричный FF и последний проход - случайные значения, делая, таким образом, невозможным восстановление данных. Данная программа, казалось бы, выполняет чистку диска в соответствии со стандартом 5220. 22-M Министерства обороны США, который гласит:
«Накопители на жестких дисках должны быть обработаны для повторного использования, «переписывая все адресуемое пространство случайными значениями»».
Испытания проводились таким образом, чтобы «гарантированно» удалить все неразмеченные данные в корневой папке. После того, как программа закончила работу, с диска был снят образ.

Пример работы программы:



Результат: Все неразмеченное пространство было заполнено случайными значениями (что очень важно при восстановлении файлов); однако, программа отработала только неразмеченное пространство и очень маленькую часть MFT; 10-15 записей были переписаны в MFT, и большинство записей, помеченные как удаленные, остались нетронутыми. Утилита не затрагивает и другие места, представляющие интерес в NTFS, например, резервные (временные) файлы, системный реестр, ярлыки и pagefile (файл подкачки).

В понимании конечного пользователя данная программа – терминальная программа, с которой сложно работать. Следует обратить внимание, что данная возможность доступна только Professional Windows XP, но не в Home Edition Windows XP , Windows 2000. Несмотря на некоторые слухи, данная функция не установлена по умолчанию. Программа должна выполняться каждый раз из командной строки. Кроме того, она имеет очень скудное описание, ориентированное на программистов и системных администраторов.

ЗАКЛЮЧЕНИЕ И РЕКОМЕНДАЦИИ

Windows XP – операционная система, пригодная для работы судебных экспертов, с характеристиками приблизительно такими же, как при работе в Windows 2000.

Полученные результаты говорят о том, что Windows XP создает новые сложности для экспертного исследования. С появлением Windows XP все чаще на домашних компьютерах устанавливается NTFS, однако, несмотря на это, в большинстве случаев на компьютерах все еще стоит FAT 32. Весьма вероятно, что в руки

экспертов все чаще будет попадать NTFS. С использованием специальных инструментов и методов эксперты будут находить необходимые доказательства.
«Гарантированное» удаление - это функция Windows XP, но это неполноценный механизм. Это - инструмент командной строки, который труден для использования и, не что иное, как хорошая утилита удаления. Обычный пользователь наверняка не знает, как ее использовать, а даже если знает и пользуется, то часть улик все равно сохранится.
Из-за свойственной сложности файловых систем и их взаимодействия с операционной системой, все эксперты, которые хотят качественно работать, должны пройти базовый курс по NTFS. Guidance Software предлагает такое обучение для судебных экспертов в рамках специального учебного курса.

ОПРЕДЕЛЕНИЕ ТЕРМИНОВ

EFS - шифрованная файловая система.
MFT - Master File Table.
Выключение компьютера - выключение компьютера с помощью команды «Shut Down».
«Гарантированное» удаление – способ, при котором на место файла на жесткий диск записывается символ в шестнадцатеричном формате обычно 00, но может быть и случайный символ.
КТЭ – компьютерно-техническая экспертиза.
Нерезидентный файл - большой файл, расположенный в нескольких местах логического диска, указатели на местоположение которых хранятся в MFT.
НЖМД – накопители на жестких магнитных дисках.
ОС – операционная система.
Первичное удаление файла - помещение файла в «мусорную» корзину.
Резидентный файл – файл, хранящийся целиком в виде одной записи в MFT.
Удаление - файл, удаленный вручную из «корзины».