Перевод: Храмов С.А.

Оценка данных, находящихся в удалённых файлах и перезаписанных «поверх» другими файлами.

Данное описание показывает: как легко могут быть ошибочно истолкованы сведения о файлах, которые были удалены, либо удалены и перезаписаны «поверх» другими файлами. Это относится только к FAT-дискам, где сведения о файлах сохраняются как элементы каталога. Обычно, при удалении файла, остается элемент каталога, откуда EnCase и получает соответствующие сведения.

В какой-то момент информация, содержащаяся в элементе каталога удаленного файла, будет соответствующим образом изменена, и область дискового пространства, содержавшая файл, будет считаться свободной. Что произойдет, если существует другой, ранее созданный, элемент каталога, указывающий на тот же самый начальный кластер? В этом случае указанная область данных не будет отображаться как свободная, а будет считаться принадлежащей другому файлу, не имеющему к ней никакого отношения!

Несмотря на то, что таковые случаи достаточно редки, они всё же могут иметь место и должны быть учтены.

Примечание: В действительности, случай, используемый для примера, маловероятен, однако, для более простого объяснения, описывается именно такая ситуация.

Элементы каталога для директории My Pictures (C:/My Documents/My Pictures)

Name (Имя)	Created (Дата создания)	Written (Дата последней записи в файл)	Accessed (Дата последнего доступа к файлу)	Size (Размер)	Cluster (Номер начального кластера)
.	04/01/01 15:06:54	04/01/01 15:06:56	04/01/01	0	42958
..	04/01/01 15:06:54	04/01/01 15:06:56	04/01/01	0	0
_ROJEC~2.JPG	11/03/01 06:01:18	11/03/01 06:01:12	20/07/01	XXXXXX	100

Представленная в табличном виде структура условно выбранного каталога показывает, что файл «_rojec~2.jpg» начинается с кластера 100. Этот файл удалён (первый символ в имени файла заменен знаком «_»). Данные этого файла всё еще присутствуют в полном объёме на диске и данные из соответствующего элемента каталога всё еще читаемы.

Предположим теперь, что другой файл с именем «hc32.jpg» сохраняется на диск. Операционная система определяет, что данные кластера 100 можно перезаписать новыми, так как файл, ранее занимавший его, считается удаленным. Поэтому, новый файл сохраняется в этом месте (при этом создается новый элемент каталога).

Элементы каталога для директории My Pictures (C:/My Documents/My Pictures)					
Name (Имя)	**Created (Дата создания)**	**Written (Дата последней записи в файл)**	**Accessed (Дата последнего доступа к файлу)**	**Size (Размер)**	**Cluster (Номер начального кластера)**
.	04/01/01 15:06:54	04/01/01 15:06:56	04/01/01	0	42958
..	04/01/01 15:06:54	04/01/01 15:06:56	04/01/01	0	0
_ROJEC~2.JPG	11/03/01 06:01:18	11/03/01 06:01:12	20/07/01	XXXXXX	100
HC32.JPG	11/03/01 06:01:18	11/03/01 06:01:12	11/01/02	XXXXXX	100

Как видим из таблицы, теперь и файл «hc32.jpg» также начинается с кластера 100, поэтому EnCase отобразит файл «_ROJEC~2.jpg» со значком **X** (удален и перезаписан), а в нижнем основании окна EnCase покажет рядом со значком └▶ имя «перекрывающего» файла – «hc32.jpg». Таким образом, при выборе любого файла будет отображаться содержимое файла «hc32.jpg».

Предположим теперь, что файл «hc32.jpg» удаляется. EnCase пометит его значком **Ø** (удаленный), а сведения о файле и его содержание будут доступны, так как файл не был перезаписан «поверх».

Теперь переходим к сути проблемы:

Предположим, что пользователь в течение некоторого времени «бродил» в Интернете, где «натолкнулся» на изображение непристойного характера, которое было автоматически кэшировано в папку Temporary Internet Files и было записано в область диска (начинающуюся с кластера 100), ранее занимаемую файлом «hc32.jpg». Каталог будет выглядеть так:

Элементы каталога для директории My Pictures (C:/My Documents/My Pictures)					
Name (Имя)	**Created (Дата создания)**	**Written (Дата последней записи в файл)**	**Accessed (Дата последнего доступа к файлу)**	**Size (Размер)**	**Cluster (Номер начального кластера)**
.	04/01/01 15:06:54	04/01/01 15:06:56	04/01/01	0	42958
..	04/01/01 15:06:54	04/01/01 15:06:56	04/01/01	0	0
indecent.JPG	xxxxxxxx xxxxxxxx	xxxxxxxx xxxxxxxx	xxxxxxxx	XXXXXX	100

Если бы состояние данных на диске оставалось бы таким к началу исследования, то проблема бы не возникла, так как EnCase бы отразила следующее:

X **ROJEC~2.jpg**	**(**перекрыт файлом **«indecent.jpg» –** поэтому**,** указывает на кластер **100 ,** т.е. содержание непристойного изображения**)**
X **hc32.jpg**	**(**перекрыт файлом **«indecent.jpg» –** поэтому**,** указывает на кластер **100 ,** т.е. содержание непристойного изображения**)**
Indecent.jpg	**(**указывает на кластер **100 ,** т.е. содержит непристойное изображение**)**

Папка Temporary Internet Files предназначена для автоматического сохранения множества временных файлов, полученных из Интернета. Предположим, что в дальнейшем содержимое указанной папки будет удалено. В этом случае EnCase всё равно бы установила данные, находящиеся в файле «Indecent.jpg».

Но если фактически элемент каталога в папке Temporary Internet Files был также удален, то не остается более указателей на кластер 100 или ссылок на файл «indecent.jpg». Поэтому, теперь только элементы каталога файлов «ROJEC~2.jpg» и «hc32.jpg» будут ссылаться на кластер 100 и соответственно на изображение непристойного характера, хотя содержание этих файлов и не имело ничего общего с указанным изображением.

Таким образом, в случае, если «источником» изображения непристойного характера являлась папка Temporary Internet Files, и нигде, в другом месте диска, не сохранялось пользователем, то пользователь мог вообще не знать о том, что таковое изображение содержится на его компьютере.

Примечание: оригинал статьи находится по адресу -
http://guidancesoftware.com/support/articles/ExplainDeleted.asp