Recovery of deleted files on a TrueCrypt volume

March 23, 2010
rationallyparanoid.com

TrueCrypt is a well-known and widely used open source application used for encryption. However at the bottom of their lengthy FAQ is a very important note that some people may have missed:

> ***Do I have to "wipe" free space and/or files on a TrueCrypt volume?***
>
> *If you believe that an adversary will be able to decrypt the volume (for example that he will make you reveal the password), then the answer is yes. Otherwise, it is not necessary, because the volume is entirely encrypted.*
>
> *http://www.truecrypt.org/faq*

Does this mean that deleted files on an encrypted TrueCrypt volume can be recovered? The answer is yes with the condition that the TrueCrypt volume must be decrypted first.

To demonstrate this we will be taking three images of decrypted TrueCrypt volumes: the first will be of an unused TrueCrypt volume, the second will be a TrueCrypt volume after files were copied to it, and the third will be a TrueCrypt volume in which files were deleted. We will then use The Sleuth Kit to see whether we can detect and recover any deleted files.

Step I: Creation of TrueCrypt volume & imaging

We begin by downloading & installing the latest version of TrueCrypt (currently 6.3a) onto a Windows XP computer. DD for Windows (http://www.chrysocome.net/dd) will be installed as well for acquiring the images.

We start the TrueCrypt volume creation wizard and create an encrypted file container. This will be a 10 MB standard TrueCrypt volume using AES with SHA-512, and based on a FAT file system with a cluster size of 512 bytes.

With the volume created we mount it to the X: drive by entering the TrueCrypt password for our encrypted volume, and once it is mounted we use dd for Windows to create an image of the entire X: drive called tc_x_unused.dd as shown below:

```
C:\Documents and Settings\User\Desktop>dd.exe if=\\.\x: of=c:\tc_x_unused.dd
rawwrite dd for windows version 0.5.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by the GPL.  See copying.txt for details
19968+0 records in
19968+0 records out
```

We now have acquired an image of a decrypted, unused TrueCrypt volume (i.e. no files have been copied to it yet). We are doing this simply as a reference to compare against the other two images that we will be taking.

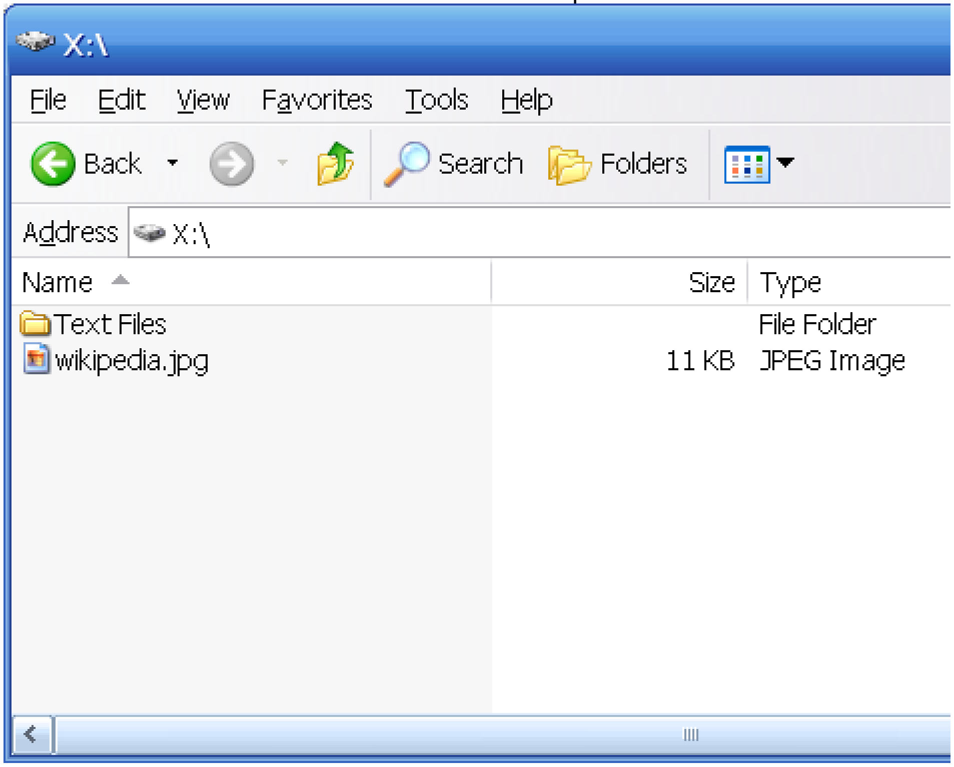
The next step will be to copy some test files to the TrueCrypt volume and take an image of it. One will be a folder called “Text Files” featuring two simple files containing the following data:

text1.txt
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ

text2.txt
0123456789

The other will be a JPEG image taken from Wikipedia's main page (http://www.wikipedia.org/) which we will rename to wikipedia.jpg before copying it over to the X: drive.

Below is the final view of the X: drive after the files have been copied:



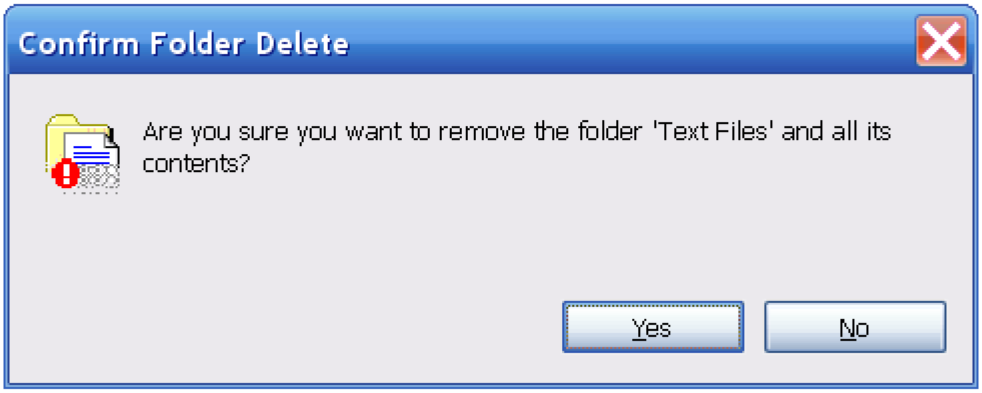
Name	Size	Type
Text Files		File Folder
wikipedia.jpg	11 KB	JPEG Image

Once the copying is completed we will unmount the volume and close TrueCrypt to confirm that everything was written to the volume and encrypted.

We will now take our second image. We mount the volume again but this time to the Y: drive (this is done simply to distinguish each of our steps) and take another image using dd:

```
C:\Documents and Settings\User\Desktop>dd if=\\.\y: of=c:\tc_y_used.dd
rawwrite dd for windows version 0.5.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by the GPL.  See copying.txt for details
19968+0 records in
19968+0 records out
```

Once this is done, we proceed to delete the Text Files folder by holding the shift key while pressing the delete key on the keyboard:



Are you sure you want to remove the folder 'Text Files' and all its contents?

Note: In the process above, the file Thumbs.db was auto-created by Windows due to viewing the folder with the presence of the image file wikipedia.jpg. This will be shown shortly.

We unmount the volume again confirming that the files were deleted and the volume encrypted. Then we mount it one last time to the Z: drive and take the last dd image:

```
C:\Documents and Settings\User\Desktop>dd.exe if=\\.\z: of=c:\tc_z_deleted.dd
rawwrite dd for windows version 0.5.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by the GPL.  See copying.txt for details
19968+0 records in
19968+0 records out
```

We can now proceed to analyzing the results.

Step II: Analysis

We have three files to work with:

tc_x_unused.dd: Image of TrueCrypt volume before it was used
tc_y_used.dd: Image of TrueCrypt volume with Text Files folder and wikipedia.jpg copied to it
tc_z_deleted.dd: Image of TrueCrypt volume with Text Files folder deleted

Let's begin by using fsstat on tc_x_unused.dd to take a look at the file system information:

```
user@Linux:~$ fsstat tc_x_unused.dd
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT16

OEM Name: MSDOS5.0
Volume ID: 0xaf66229e
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT16

Sectors before file system: 0

File System Layout (in sectors)
Total Range: 0 - 19967
```

```
* Reserved: 0 - 1
** Boot Sector: 0
* FAT 0: 2 - 79
* FAT 1: 80 - 157
* Data Area: 158 - 19967
** Root Directory: 158 - 189
** Cluster Area: 190 - 19967

METADATA INFORMATION
--------------------------------------------
Range: 2 - 316962
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 19779

FAT CONTENTS (in sectors)
--------------------------------------------
```

This is a FAT16 file system, with the sector and cluster sizes both 512 bytes. The FAT contents show nothing present, and we can confirm that no files exist by using fls:

```
user@Linux:~$ fls -r tc_x_unused.dd
user@Linux:~$
```

There are no results as should be the case because this is the image of the unused volume. Now let us examine the second image:

```
user@Linux:~$ fsstat tc_y_used.dd
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT16

OEM Name: MSDOS5.0
Volume ID: 0xaf66229e
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT16

Sectors before file system: 0

File System Layout (in sectors)
Total Range: 0 - 19967
* Reserved: 0 - 1
** Boot Sector: 0
* FAT 0: 2 - 79
* FAT 1: 80 - 157
* Data Area: 158 - 19967
** Root Directory: 158 - 189
** Cluster Area: 190 - 19967

METADATA INFORMATION
--------------------------------------------
Range: 2 - 316962
```

```
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 19779

FAT CONTENTS (in sectors)
--------------------------------------------
190-190 (1) -> EOF
191-191 (1) -> EOF
192-192 (1) -> EOF
193-214 (22) -> EOF
```

The difference is that here we can see in the FAT contents that sectors 190 to 214 are allocated. We'll use fls to see what files and directories exist:

```
user@Linux:~$ fls -r tc_y_used.dd
d/d 4:      Text Files
+ r/r 517:  text1.txt
+ r/r 518:  text2.txt
r/r 6:      wikipedia.jpg
```

This shows the files and folder that we copied over. Nothing is deleted (nor should anything be deleted). Contrast this with the last volume:

```
user@Linux:~$ fls -r tc_z_deleted.dd
d/d * 4:    Text Files
+ r/r * 517:      text1.txt
+ r/r * 518:      text2.txt
r/r 6:      wikipedia.jpg
r/r 8:      Thumbs.db
```

The asterisks above show that the directory “Text Files” along with the files text1.txt, text2.txt are deleted. Also notice the creation of Thumbs.db which was created as a result of us browsing the drive with Windows explorer.

The table below summarizes the results of fls:

tc_x_unused.dd	**tc_y_used.dd**	**tc_z_deleted.dd**
<no data>	d/d 4: Text Files + r/r 517: text1.txt + r/r 518: text2.txt r/r 6: wikipedia.jpg	d/d * 4: Text Files + r/r * 517: text1.txt + r/r * 518: text2.txt r/r 6: wikipedia.jpg r/r 8: Thumbs.db

So the question is, can we recover the deleted files from tc_z_deleted.dd? The answer is yes, very easily, because the sectors for these deleted files have not been reused yet. We'll use icat to recover the deleted files:

```
user@Linux:~$ icat -r tc_z_deleted.dd 517 > text1.txt
user@Linux:~$ icat -r tc_z_deleted.dd 518 > text2.txt
```

Below we demonstrate that the contents of the files have been recovered:

```
user@Linux:~$ cat text1.txt
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ

user@Linux:~$ cat text2.txt
0123456789
```

So we can see how deleted files can easily be recovered from a decrypted TrueCrypt volume. Also notice that given the peculiarities of an operating system or application, it is possible for certain artifacts to be created (i.e. the Thumbs.db file) without your knowledge when viewing, creating, or modifying your data.

To see a list of various Sleuth Kit commands along with examples of how they are used, see the guide at http://rationallyparanoid.com/articles/sleuth-kit.html