Examine Evidence Partitions

You are provided four NTFS partitions from a hard drive, each about 100MB in size. One of the partitions has been defragmented, one used file encryption, and one used secure file deletion; no action has been taken on the other. Your task is to determine which action (if any) has been applied to each partition.

You will examine each partition using FTK (Imager is sufficient) and the Windows operating system. Your guidance for determining which actions have been taken on a specific partition are as follows:

Normal (no action):

- files are scattered throughout the partition
- you will see deleted files with content
- you will see data in file slack space

Defragmentation:

- files are stored in contiguous locations
- file slack space is zeroed out
- measurable with native OS tools

Encryption:

- file contents are “jibberish” (very little readable plain text)
- FTK may show a "key" icon
- OS may indicate encryption (e.g., "lock" icon)

Secure Wipe:

- deleted files in unallocated space will not contain any readable content
- there will not be any data in file slack space

To examine each of the partitions, perform the following steps until you are confident about which action was applied to each partition. The partitions for this exercise are raw dumps and are named partition_blue.dd, partition_green.dd, partition_red.dd, and partition_yellow.dd.

1. Mount partitions (images) in Windows OS:

Run FTK or FTK Imager; select File: Image Mounting with the settings below (your file paths will differ).

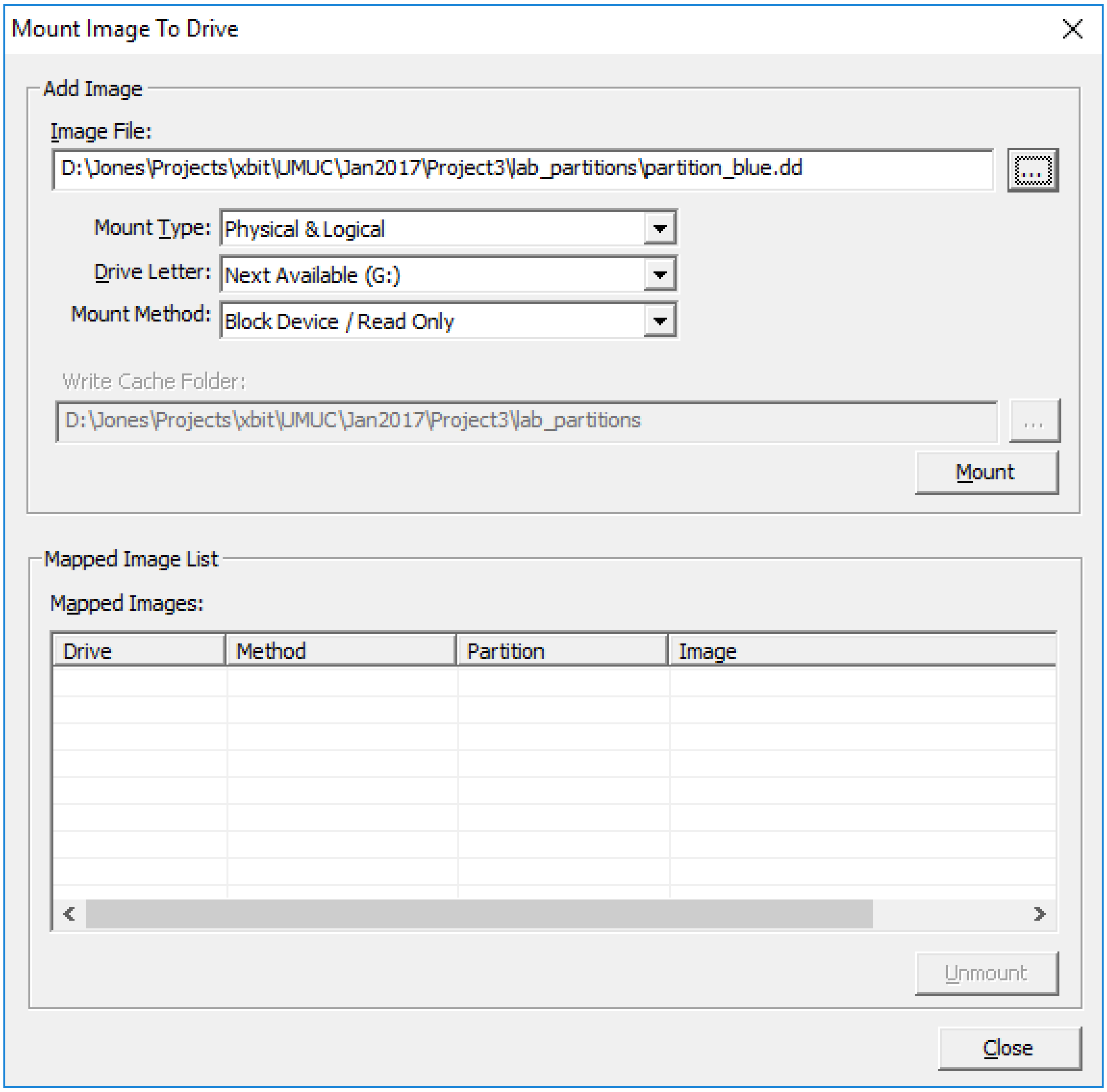


Image File: D:\Jones\Projects\xbit\UMUC\Jan2017\Project3\lab_partitions\partition_blue.dd

Mount Type: Physical & Logical

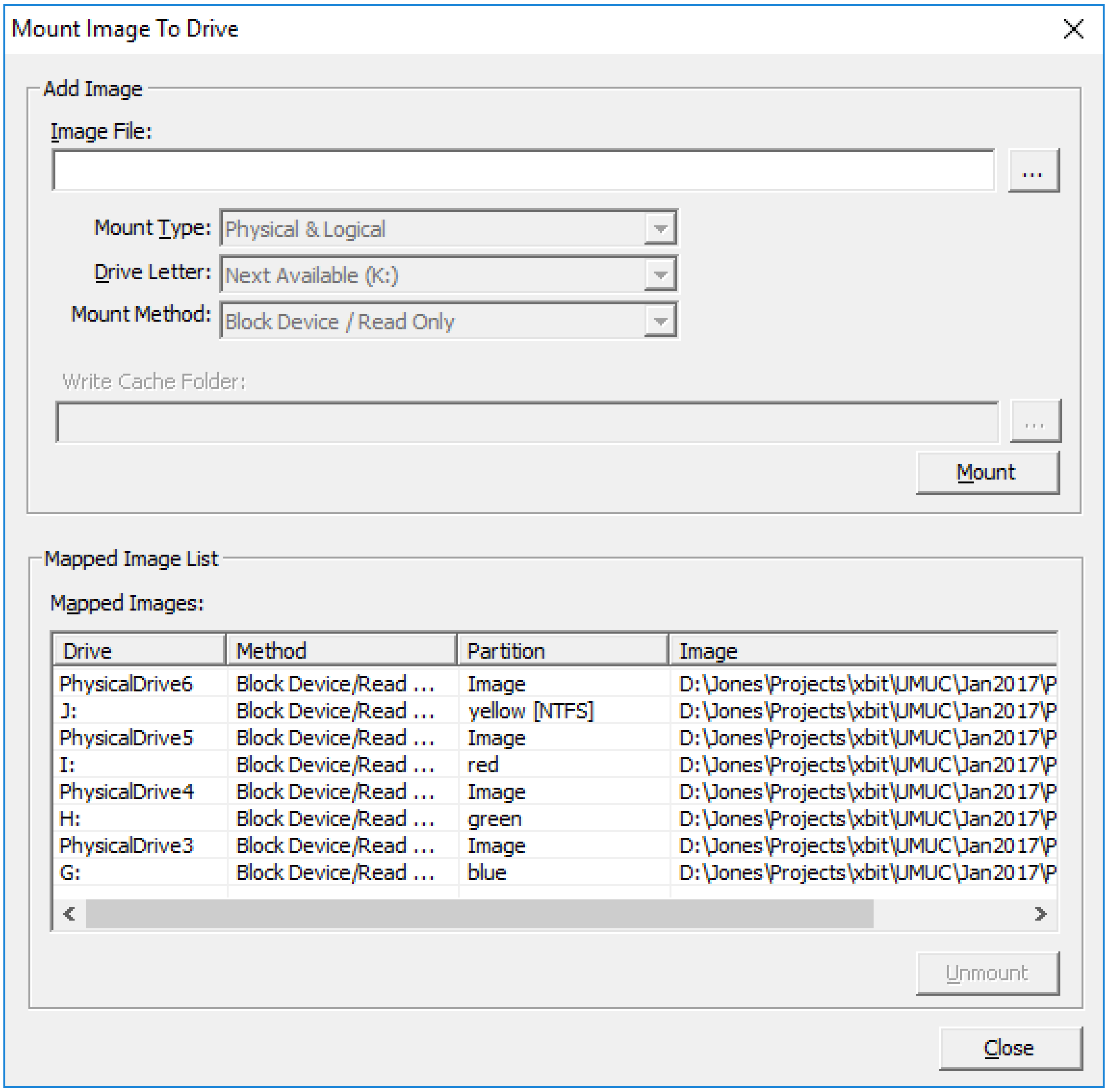
Drive Letter: Next Available (G:)

Mount Method: Block Device / Read Only

Write Cache Folder: D:\Jones\Projects\xbit\UMUC\Jan2017\Project3\lab_partitions

Drive	Method	Partition	Image

Repeat for all four partitions and you should see each partition show up in the "Mapped Images" portion of the window (eight entries, one physical and one logical for each partition). When all four images are mounted, click Close.



Mount Image To Drive

Add Image

Image File:

Mount Type: Physical & Logical

Drive Letter: Next Available (K:)

Mount Method: Block Device / Read Only

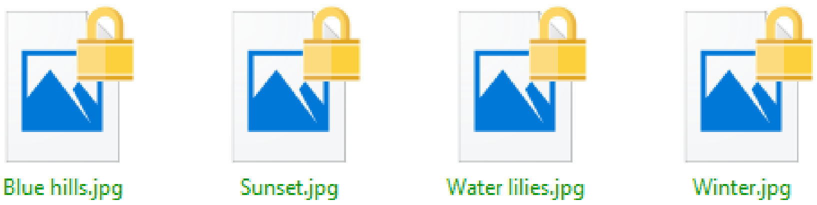
Write Cache Folder:

Mapped Image List

Mapped Images:

Drive	Method	Partition	Image
PhysicalDrive6	Block Device/Read ...	Image	D:\Jones\Projects\xbit\UMUC\Jan2017\P
J:	Block Device/Read ...	yellow [NTFS]	D:\Jones\Projects\xbit\UMUC\Jan2017\P
PhysicalDrive5	Block Device/Read ...	Image	D:\Jones\Projects\xbit\UMUC\Jan2017\P
I:	Block Device/Read ...	red	D:\Jones\Projects\xbit\UMUC\Jan2017\P
PhysicalDrive4	Block Device/Read ...	Image	D:\Jones\Projects\xbit\UMUC\Jan2017\P
H:	Block Device/Read ...	green	D:\Jones\Projects\xbit\UMUC\Jan2017\P
PhysicalDrive3	Block Device/Read ...	Image	D:\Jones\Projects\xbit\UMUC\Jan2017\P
G:	Block Device/Read ...	blue	D:\Jones\Projects\xbit\UMUC\Jan2017\P

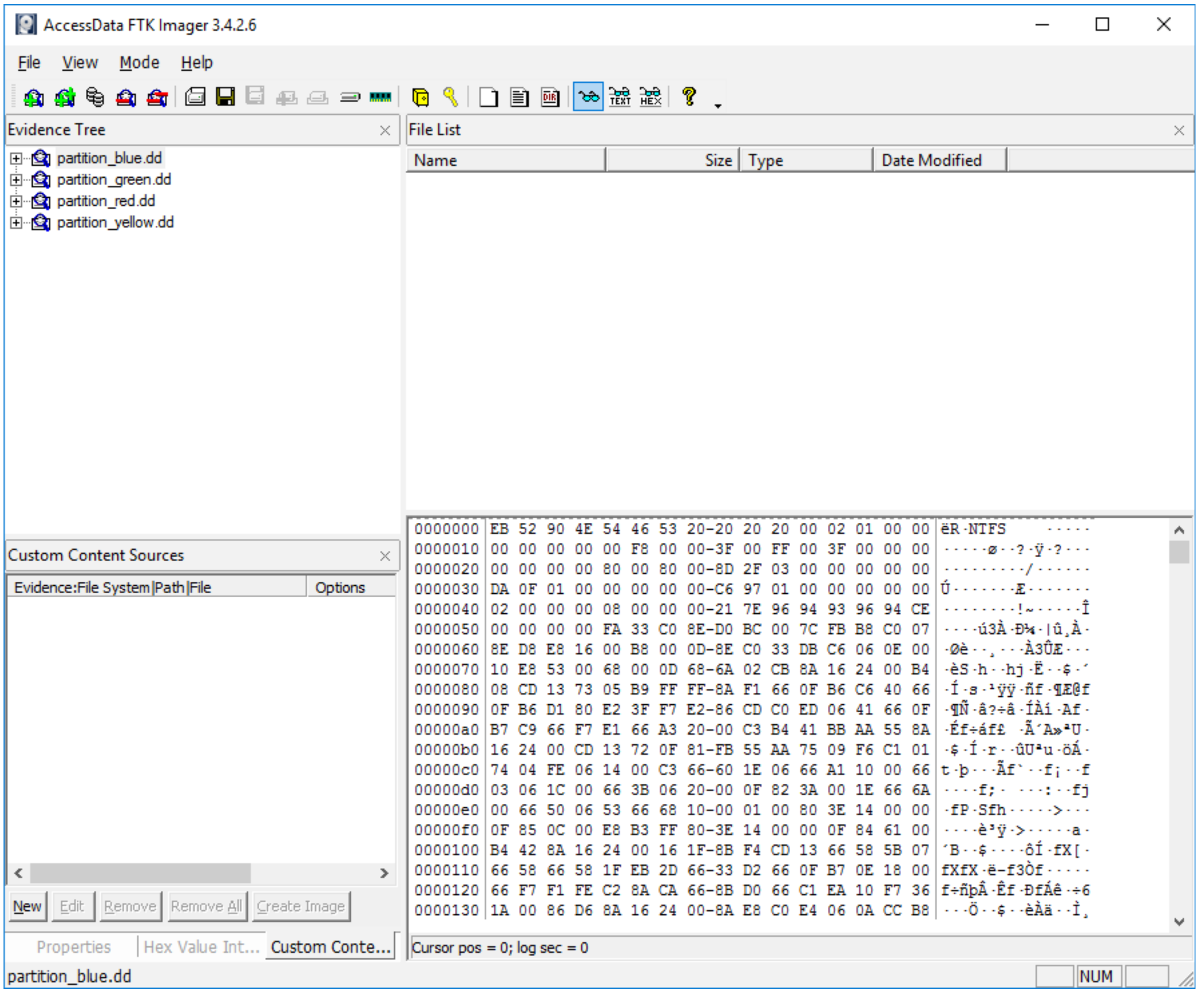
Examine the mounted partitions and files in Windows Explorer. If files appear to be present but you can't open them or see the file contents, then encryption is a possibility (confirmed if you see a "lock" icon over some files, such as image files that can't render the thumbnail):



2. Examine the partitions in FTK

Using FTK or FTK Imager, examine each of the four partitions.

Choose File: Add Evidence Items, then Image File, then Next, browse to the partition image folder, select the image (dd) file, then select Finish. Repeat for all four partitions and FTK (Imager) should look like this:



partition_blue.dd
partition_green.dd
partition_red.dd
partition_yellow.dd

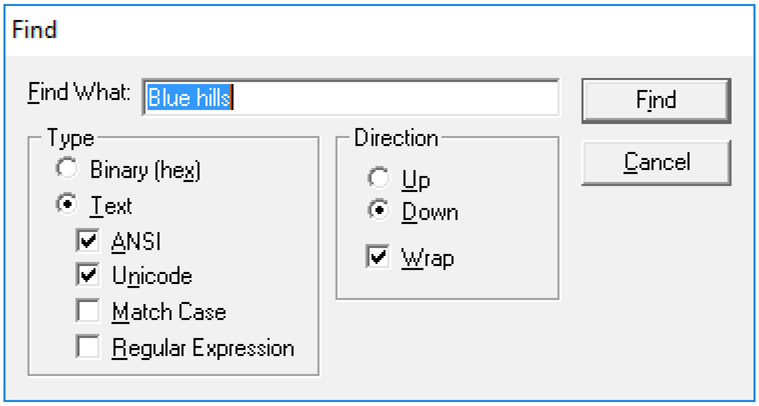
```
0000000 EB 52 90 4E 54 46 53 20-20 20 20 00 02 01 00 00 ëR·NTFS    ·····
0000010 00 00 00 00 00 F8 00 00-3F 00 FF 00 3F 00 00 00 ·····ø··?·ÿ·?···
0000020 00 00 00 00 80 00 80 00-8D 2F 03 00 00 00 00 00 ·········/······
0000030 DA 0F 01 00 00 00 00 00-C6 97 01 00 00 00 00 00 Ú·······Æ·······
0000040 02 00 00 00 08 00 00 00-21 7E 96 94 93 96 94 CE ········!~·····Î
0000050 00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB B8 C0 07 ····ú3À·Ð¼·|û¸À·
0000060 8E D8 E8 16 00 B8 00 0D-8E C0 33 DB C6 06 0E 00 ·Øè··¸···À3ÛÆ···
0000070 10 E8 53 00 68 00 0D 68-6A 02 CB 8A 16 24 00 B4 ·èS·h··hj·Ë··$·´
0000080 08 CD 13 73 05 B9 FF FF-8A F1 66 0F B6 C6 40 66 ·Í·s·¹ÿÿ·ñf·¶Æ@f
0000090 0F B6 D1 80 E2 3F F7 E2-86 CD C0 ED 06 41 66 0F ·¶Ñ·â?÷â·ÍÀí·Af·
00000a0 B7 C9 66 F7 E1 66 A3 20-00 C3 B4 41 BB AA 55 8A ·Éf÷áf£ ·Ã´A»ªU·
00000b0 16 24 00 CD 13 72 0F 81-FB 55 AA 75 09 F6 C1 01 ·$·Í·r··ûUªu·öÁ·
00000c0 74 04 FE 06 14 00 C3 66-60 1E 06 66 A1 10 00 66 t·þ···Ãf`··f¡··f
00000d0 03 06 1C 00 66 3B 06 20-00 0F 82 3A 00 1E 66 6A ····f;· ···:··fj
00000e0 00 66 50 06 53 66 68 10-00 01 00 80 3E 14 00 00 ·fP·Sfh·····>···
00000f0 0F 85 0C 00 E8 B3 FF 80-3E 14 00 00 0F 84 61 00 ····è³ÿ·>·····a·
0000100 B4 42 8A 16 24 00 16 1F-8B F4 CD 13 66 58 5B 07 ´B··$····ôÍ·fX[·
0000110 66 58 66 58 1F EB 2D 66-33 D2 66 0F B7 0E 18 00 fXfX·ë-f3Òf·····
0000120 66 F7 F1 FE C2 8A CA 66-8B D0 66 C1 EA 10 F7 36 f÷ñþÂ·Êf·ÐfÁê·÷6
0000130 1A 00 86 D6 8A 16 24 00-8A E8 C0 E4 06 0A CC B8 ···Ö··$··èÀä··Ì¸
```

Cursor pos = 0; log sec = 0

partition_blue.dd

Look for the following features and characteristics to help determine actions performed on the partition:

- While at the base of each image (i.e., don't start browsing the filesystems yet), search for a file name on each of the partitions (e.g., "Blue hills", but any file name you saw in Windows Explorer with a lock icon will work). Be sure to check the Unicode box (see the first screenshot below). You should find references to the file on all four partitions, but some of the references will have the characters "$.E.F.S.1" (EFS1 in unicode) about 150 bytes after the filename. This indicates use of the Microsoft NTFS Encrypted File System, and this partition should be the same one you found above that suggested encryption.

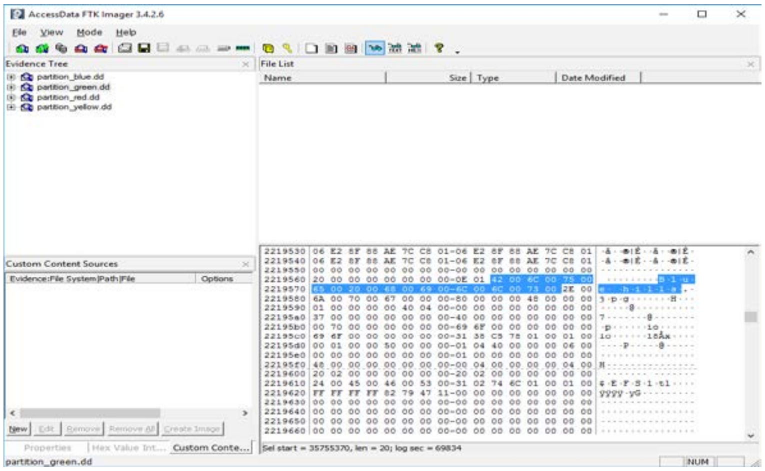


Find

Find What: Blue hills

Type
- ○ Binary (hex)
- ● Text
  - ☑ ANSI
  - ☑ Unicode
  - □ Match Case
  - □ Regular Expression

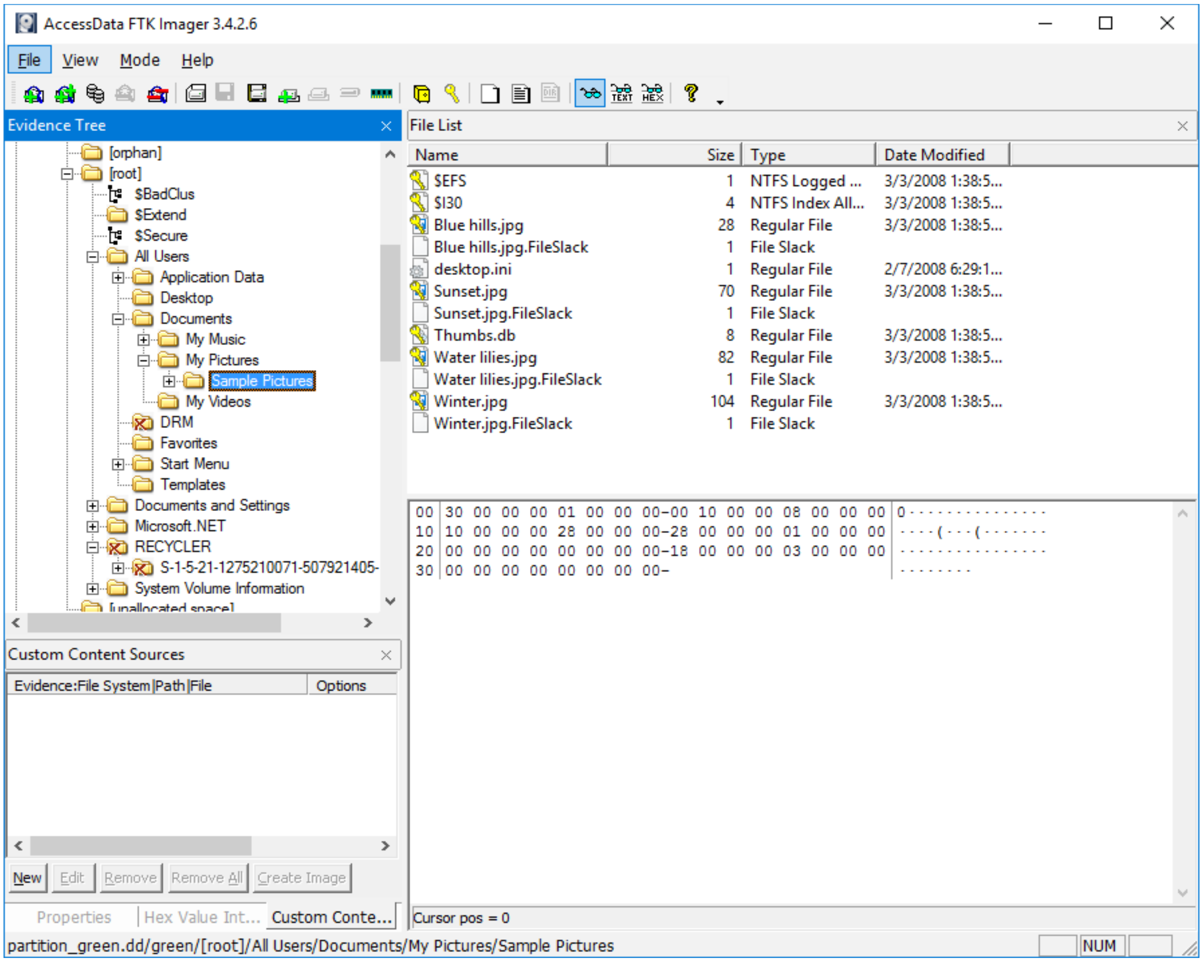
Direction
- ○ Up
- ● Down
- ☑ Wrap



```
2219530 06 E2 8F 88 AE 7C C8 01-06 E2 8F 88 AE 7C C8 01  ·â··®|È··â··®|È·
2219540 06 E2 8F 88 AE 7C C8 01-06 E2 8F 88 AE 7C C8 01  ·â··®|È··â··®|È·
2219550 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
2219560 20 00 00 00 00 00 00 00-0E 01 42 00 6C 00 75 00   ·········B·l·u·
2219570 65 00 20 00 68 00 69 00-6C 00 6C 00 73 00 2E 00  e· ·h·i·l·l·s·.·
2219580 6A 00 70 00 67 00 00 00-80 00 00 00 48 00 00 00  j·p·g·······H···
2219590 01 00 00 00 00 40 04 00-00 00 00 00 00 00 00 00  ·····@··········
22195a0 37 00 00 00 00 00 00 00-40 00 00 00 00 00 00 00  7·······@·······
22195b0 00 70 00 00 00 00 00 00-69 6F 00 00 00 00 00 00  ·p······io······
22195c0 69 6F 00 00 00 00 00 00-31 38 C5 78 01 00 01 00  io······18Åx····
22195d0 00 01 00 00 50 00 00 00-01 04 40 00 00 00 06 00  ····P·····@·····
22195e0 00 00 00 00 00 00 00 00-01 00 00 00 00 00 00 00  ················
22195f0 48 00 00 00 00 00 00 00-00 04 00 00 00 00 04 00  H···············
2219600 20 02 00 00 00 00 00 00-20 02 00 00 00 00 00 00   ······· ·······
2219610 24 00 45 00 46 00 53 00-31 02 74 6C 01 00 01 00  $·E·F·S·1·tl····
2219620 FF FF FF FF 82 79 47 11-00 00 00 00 00 00 00 00  ÿÿÿÿ·yG·········
2219630 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
2219640 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
2219650 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
2219660 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

Sel start = 35755370, len = 20; log sec = 69834

Confirm that you have identified the encrypted partition by looking through the filesystem of that partition and noticing all the key icons (see screenshot below). If so, you've identified which partition was encrypted, and the encryption implementation used (EFS). Note that other encryption implementations have different "signatures", some less obvious than others.



Name	Size	Type	Date Modified
$EFS	1	NTFS Logged ...	3/3/2008 1:38:5...
$I30	4	NTFS Index All...	3/3/2008 1:38:5...
Blue hills.jpg	28	Regular File	3/3/2008 1:38:5...
Blue hills.jpg.FileSlack	1	File Slack	
desktop.ini	1	Regular File	2/7/2008 6:29:1...
Sunset.jpg	70	Regular File	3/3/2008 1:38:5...
Sunset.jpg.FileSlack	1	File Slack	
Thumbs.db	8	Regular File	3/3/2008 1:38:5...
Water lilies.jpg	82	Regular File	3/3/2008 1:38:5...
Water lilies.jpg.FileSlack	1	File Slack	
Winter.jpg	104	Regular File	3/3/2008 1:38:5...
Winter.jpg.FileSlack	1	File Slack	

```
00  30 00 00 00 01 00 00 00-00 10 00 00 08 00 00 00  0...............
10  10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00  ....(...(.......
20  00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00  ................
30  00 00 00 00 00 00 00 00-                          ........
```

Cursor pos = 0

partition_green.dd/green/[root]/All Users/Documents/My Pictures/Sample Pictures

3. Find the defragmented partition

Using the Windows command line, check the fragmentation level of the three remaining partitions (the fourth is the encrypted partition).

```
C:\> defrag X: /a
```

where X is the drive letter of the partition you're checking (see the drive letters in Windows Explorer) and /a means just analyze the partitions (don't actually defragment them).

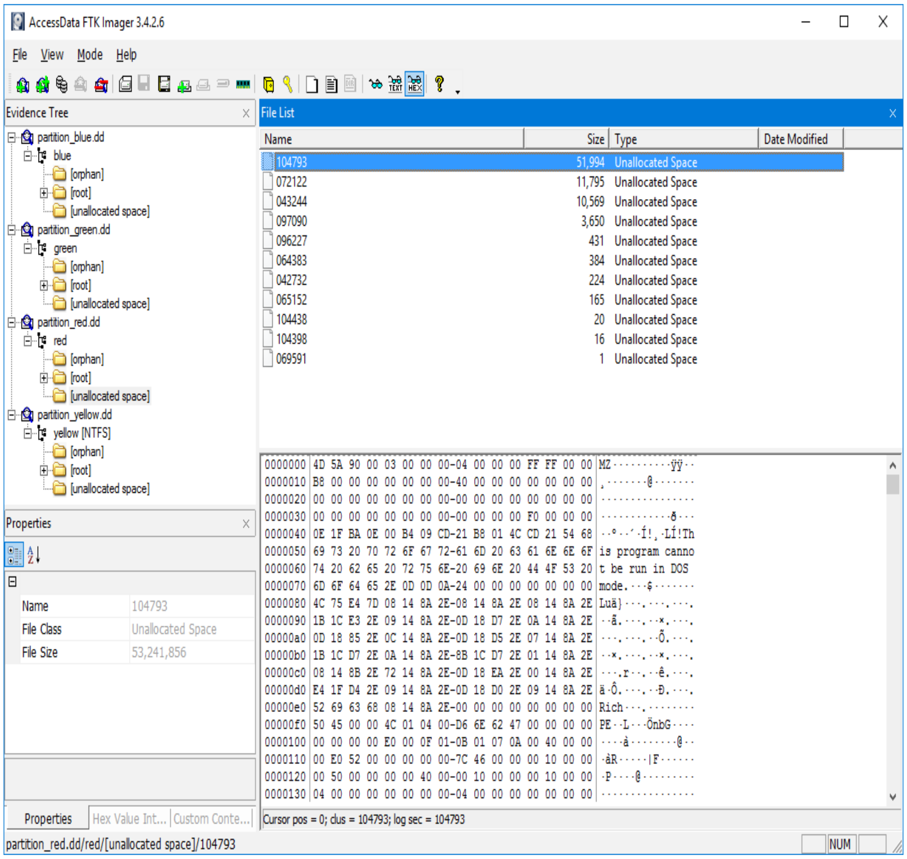
You should find one partition with 0% fragmentation and two partitions with 2% fragmentation. The partition with 0% fragmentation is the one that has been defragmented.

4. Find the secure delete partition

Secure delete tools overwrite deleted content so that it cannot be recovered (normally we find useful data from deleted files in the unallocated portions of media).

Using FTK (Imager), examine the entries in the [unallocated space] of the two remaining partitions. If a secure delete tool has been used, the entries in unallocated space will contain only random data and INDX records (from the filesystem; readable but not containing actual deleted file content). If the entries in unallocated space contain readable data from deleted files, then those files were not securely deleted.

For example, this executable file (note the MZ at the start of the file and readable text) was not securely deleted:



Name	Size	Type	Date Modified
104793	51,994	Unallocated Space	
072122	11,795	Unallocated Space	
043244	10,569	Unallocated Space	
097090	3,650	Unallocated Space	
096227	431	Unallocated Space	
064383	384	Unallocated Space	
042732	224	Unallocated Space	
065152	165	Unallocated Space	
104438	20	Unallocated Space	
104398	16	Unallocated Space	
069591	1	Unallocated Space	

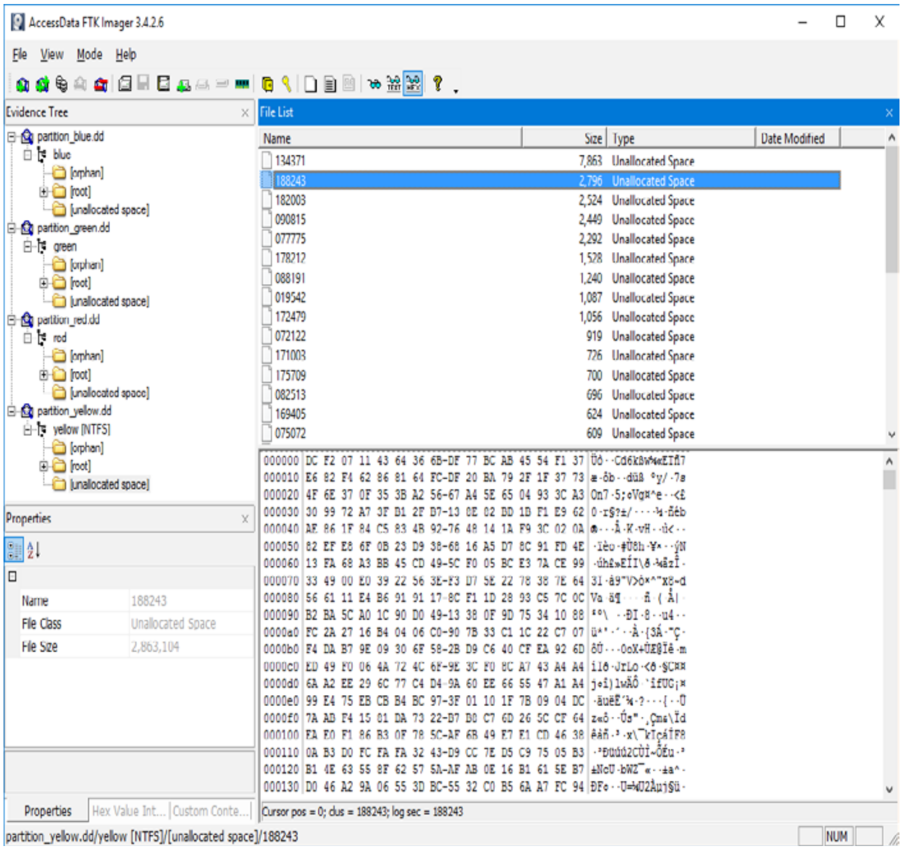
Name	104793
File Class	Unallocated Space
File Size	53,241,856

```
0000000 4D 5A 90 00 03 00 00 00-04 00 00 00 FF FF 00 00 MZ··········ÿÿ··
0000010 B8 00 00 00 00 00 00 00-40 00 00 00 00 00 00 00 ¸·······@·······
0000020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000030 00 00 00 00 00 00 00 00-00 00 00 00 F0 00 00 00 ············ð···
0000040 0E 1F BA 0E 00 B4 09 CD-21 B8 01 4C CD 21 54 68 ··º··´·Í!¸·LÍ!Th
0000050 69 73 20 70 72 6F 67 72-61 6D 20 63 61 6E 6E 6F is program canno
0000060 74 20 62 65 20 72 75 6E-20 69 6E 20 44 4F 53 20 t be run in DOS 
0000070 6D 6F 64 65 2E 0D 0D 0A-24 00 00 00 00 00 00 00 mode.···$·······
0000080 4C 75 E4 7D 08 14 8A 2E-08 14 8A 2E 08 14 8A 2E Luä}···.···.···.
0000090 1B 1C E3 2E 09 14 8A 2E-0D 18 D7 2E 0A 14 8A 2E ··ã.···.··×.···.
00000a0 0D 18 85 2E 0C 14 8A 2E-0D 18 D5 2E 07 14 8A 2E ···.···.··Õ.···.
00000b0 1B 1C D7 2E 0A 14 8A 2E-8B 1C D7 2E 01 14 8A 2E ··×.···.··×.···.
00000c0 08 14 8B 2E 72 14 8A 2E-0D 18 EA 2E 00 14 8A 2E ···.r··.··ê.···.
00000d0 E4 1F D4 2E 09 14 8A 2E-0D 18 D0 2E 09 14 8A 2E ä·Ô.···.··Ð.···.
00000e0 52 69 63 68 08 14 8A 2E-00 00 00 00 00 00 00 00 Rich···.········
00000f0 50 45 00 00 4C 01 04 00-D6 6E 62 47 00 00 00 00 PE··L···ÖnbG····
0000100 00 00 00 00 E0 00 0F 01-0B 01 07 0A 00 40 00 00 ····à········@··
0000110 00 E0 52 00 00 00 00 00-7C 46 00 00 00 10 00 00 ·àR·····|F······
0000120 00 50 00 00 00 00 40 00-00 10 00 00 00 10 00 00 ·P····@·········
0000130 04 00 00 00 00 00 00 00-04 00 00 00 00 00 00 00 ················
```

Cursor pos = 0; clus = 104793; log sec = 104793

partition_red.dd/red/[unallocated space]/104793

and this file was securely deleted:



Name	Size	Type	Date Modified
134371	7,863	Unallocated Space	
188243	2,796	Unallocated Space	
182003	2,524	Unallocated Space	
090815	2,449	Unallocated Space	
077775	2,292	Unallocated Space	
178212	1,528	Unallocated Space	
088191	1,240	Unallocated Space	
019542	1,087	Unallocated Space	
172479	1,056	Unallocated Space	
072122	919	Unallocated Space	
171003	726	Unallocated Space	
175709	700	Unallocated Space	
082513	696	Unallocated Space	
169405	624	Unallocated Space	
075072	609	Unallocated Space	

```
000000 DC F2 07 11 43 64 36 6B-DF 77 BC AB 45 54 F1 37 Üò··Cd6kßw¼«ETñ7
000010 E6 82 F4 62 86 81 64 FC-DF 20 BA 79 2F 1F 37 73 æ·ôb··düß °y/·7s
000020 4F 6E 37 0F 35 3B A2 56-67 A4 5E 65 04 93 3C A3 On7·5;¢Vg¤^e··<£
000030 30 99 72 A7 3F B1 2F D7-13 0E 02 BD 1D F1 E9 62 0·r§?±/×···½·ñéb
000040 AE 86 1F 84 C5 83 4B 92-76 48 14 1A F9 3C 02 0A ®···Å·K·vH··ù<··
000050 82 EF E8 6F 0B 23 D9 38-68 16 A5 D7 8C 91 FD 4E ·ïèo·#Ù8h·¥×··ýN
000060 13 FA 68 A3 BB 45 CD 49-5C F0 05 BC E3 7A CE 99 ·úh£»EÍI\ð·¼ãzÎ·
000070 33 49 00 E0 39 22 56 3E-F3 D7 5E 22 78 38 7E 64 3I·à9"V>ó×^"x8~d
000080 56 61 11 E4 B6 91 91 17-8C F1 1D 28 93 C5 7C 0C Va·ä¶····ñ·(·Å|·
000090 B2 BA 5C A0 1C 90 D0 49-13 38 0F 9D 75 34 10 88 ²º\ ··ÐI·8··u4··
0000a0 FC 2A 27 16 B4 04 06 C0-90 7B 33 C1 1C 22 C7 07 ü*'·´··À·{3Á·"Ç·
0000b0 F4 DA B7 9E 09 30 6F 58-2B D9 C6 40 CF EA 92 6D ôÚ···0oX+ÙÆ@Ïê·m
0000c0 ED 49 F0 06 4A 72 4C 6F-9E 3C F0 8C A7 43 A4 A4 íIð·JrLo·<ð·§C¤¤
0000d0 6A A2 EE 29 6C 77 C4 D4-9A 60 EE 66 55 47 A1 A4 j¢î)lwÄÔ·`îfUG¡¤
0000e0 99 E4 75 EB CB B4 BC 97-3F 01 10 1F 7B 09 04 DC ·äuëË´¼·?···{··Ü
0000f0 7A AD F4 15 01 DA 73 22-B7 D0 C7 6D 26 5C CF 64 zô··Ús"·ÐÇm&\Ïd
000100 EA E0 F1 86 B3 0F 78 5C-AF 6B 49 E7 E1 CD 46 38 êàñ·³·x\¯kIçáÍF8
000110 0A B3 D0 FC FA FA 32 43-D9 CC 7E D5 C9 75 05 B3 ·³Ðüúú2CÙÌ~ÕÉu·³
000120 B1 4E 63 55 8F 62 57 5A-AF AB 0E 16 B1 61 5E B7 ±NcU·bWZ¯«··±a^·
000130 D0 46 A2 9A 06 55 3D BC-55 32 C0 B5 6A A7 FC 94 ÐF¢··U=¼U2Àµj§ü·
```

Cursor pos = 0; clus = 188243; log sec = 188243

Name	188243
File Class	Unallocated Space
File Size	2,863,104

partition_yellow.dd/yellow [NTFS]/[unallocated space]/188243

5. The remaining partition is the one on which no actions were taken.

Based on your analysis above, identify which action (defragmented, encrypted, secure delete, no action) was applied to each partition. Include your process and results in your writeup.

partition_blue.dd: ____________________

partition_green.dd: ____________________

partition_red.dd: ____________________

partition_yellow.dd: ____________________