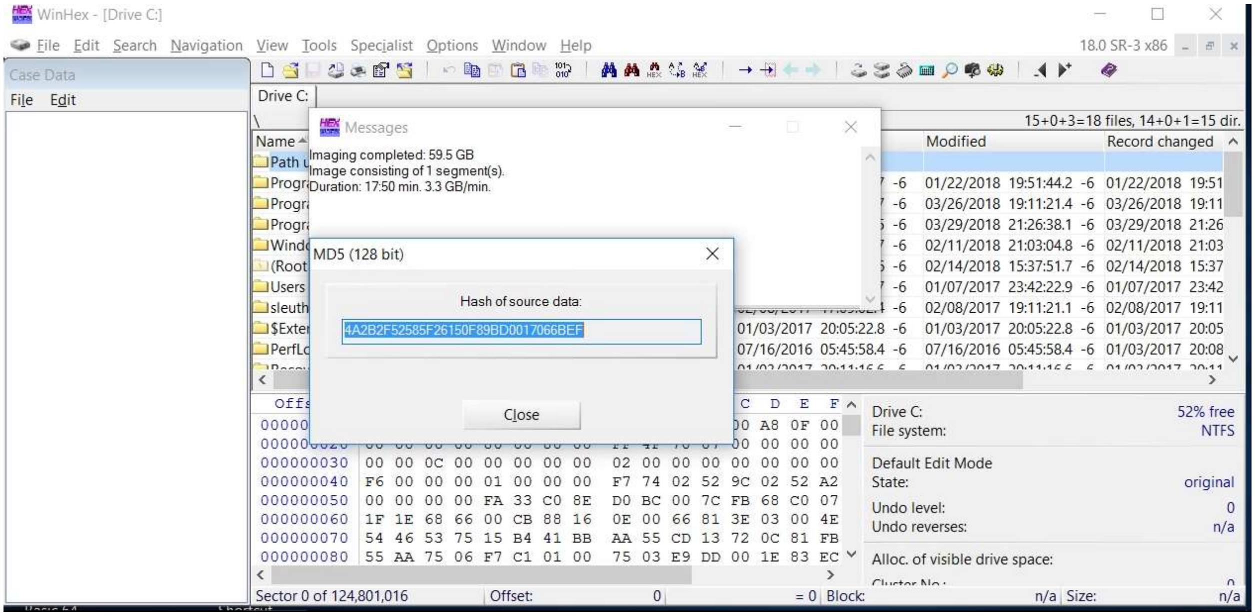
Timothy Kang
ITMS 538
Assign09

Special Problem 08a:

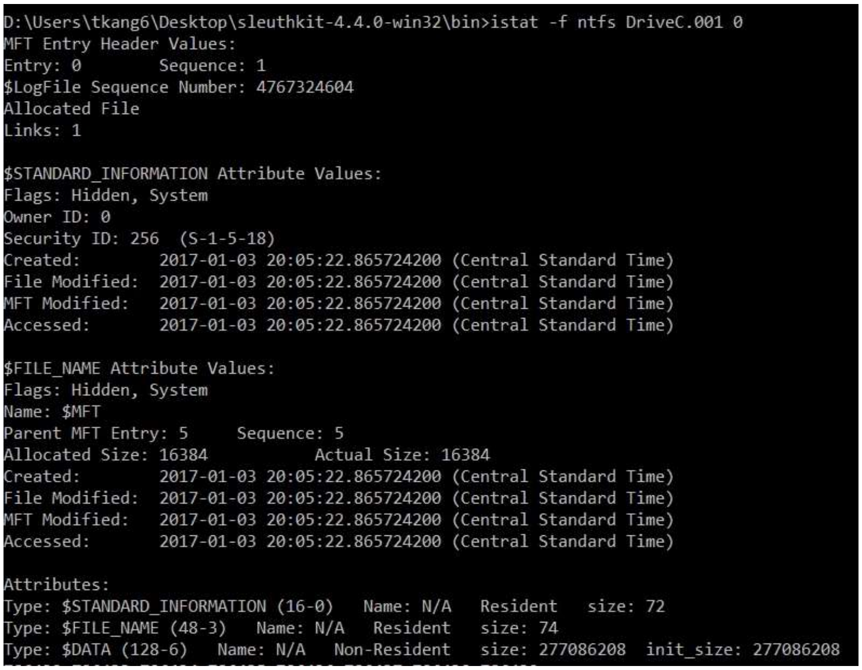
For this case, a Win 10 C: partition was examined within RADISH. Just like with any other case, the first step was to create a disk image file of the drive so that it can be examined. It is possible to do so using WinHex as seen in Figure 1. Now that the C drive image has been created, TSK and other hex viewer tools can be used to further understand this drive. One thing to note is that we know that the file system of the drive is NTFS. First TSK tool that I used was istat which shows metadata details depending on what inode/MFT entry number you input. For this case, I used Inode 0, 1, 2, 6, 7 which correspond to $MFT, $MFTMirr, $LogFile, $Bitmap, $Boot. Fsstat was used to find a more detailed display of the file system and meta data information. Other tools that were used include img_stat, fls, and blkcat. In addition to this, I was able to add the disk image file to WinHex for further inspection of hexadecimal and ASCII values of each section. This made it possible to not only see the Partition Boot Sector but to also see the format and pinpoint each field name as seen in Figure 20. In order to find out more about the partition table such as starting sector numbers and sizes, the diskpart and mmls tools were used. Diskpart allowed me to list all disks on RADISH which can be used in conjunction with mmls to list partition table contents.



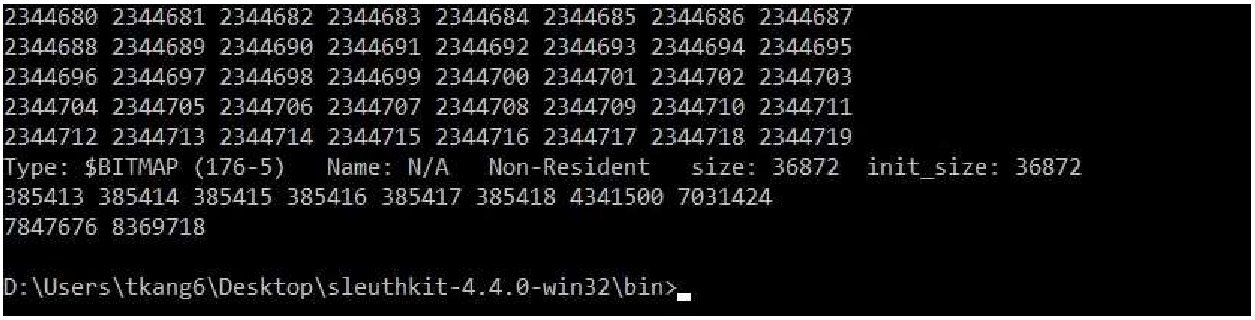
```
Imaging completed: 59.5 GB
Image consisting of 1 segment(s).
Duration: 17:50 min. 3.3 GB/min.
```

```
Hash of source data:
4A2B2F52585F26150F89BD0017066BEF
```

Fig 1: After successfully creating a disk image file of the C drive on WinHex. (File→ Create Disk Image)

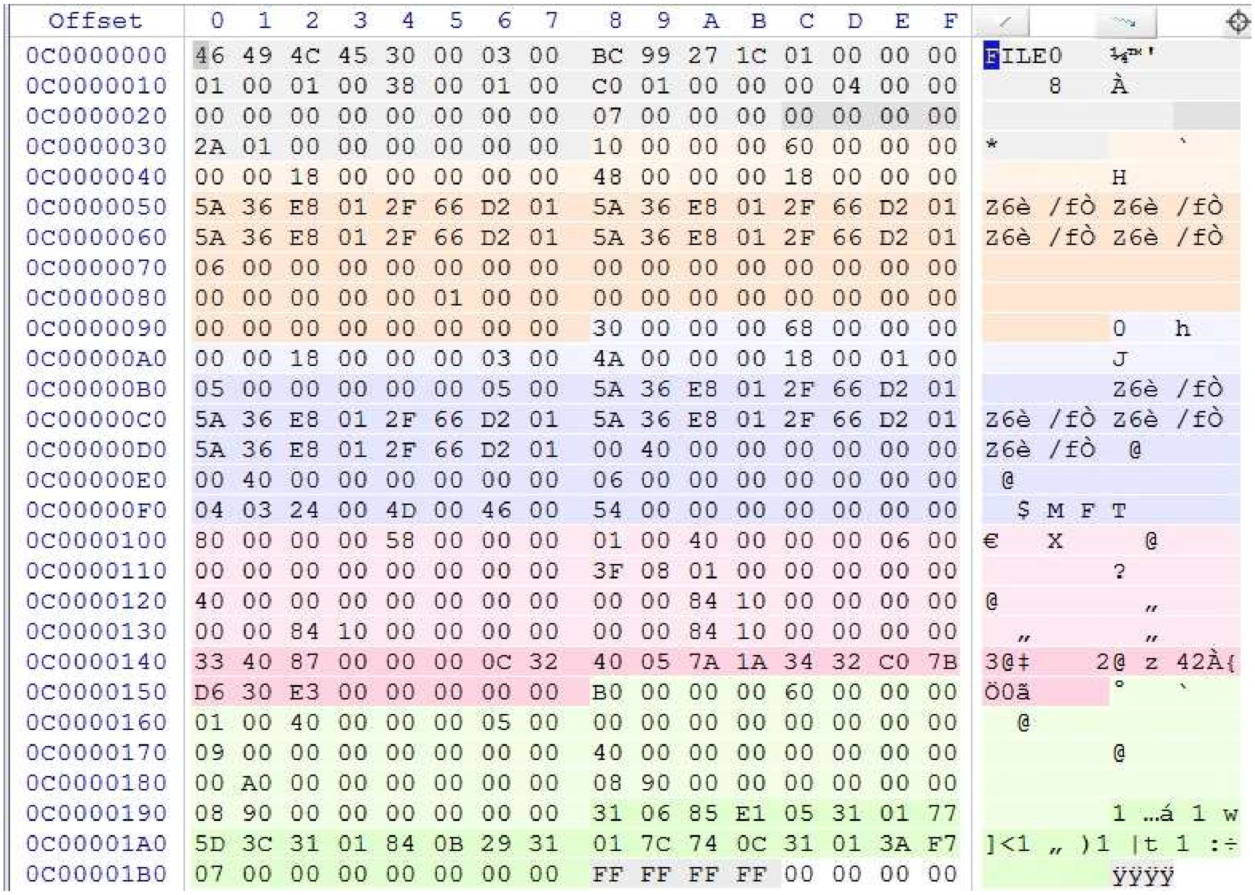


```
D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>istat -f ntfs DriveC.001 0
MFT Entry Header Values:
Entry: 0        Sequence: 1
$LogFile Sequence Number: 4767324604
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256  (S-1-5-18)
Created:        2017-01-03 20:05:22.865724200 (Central Standard Time)
File Modified:  2017-01-03 20:05:22.865724200 (Central Standard Time)
MFT Modified:   2017-01-03 20:05:22.865724200 (Central Standard Time)
Accessed:       2017-01-03 20:05:22.865724200 (Central Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $MFT
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 16384          Actual Size: 16384
Created:        2017-01-03 20:05:22.865724200 (Central Standard Time)
File Modified:  2017-01-03 20:05:22.865724200 (Central Standard Time)
MFT Modified:   2017-01-03 20:05:22.865724200 (Central Standard Time)
Accessed:       2017-01-03 20:05:22.865724200 (Central Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-3)   Name: N/A   Resident   size: 74
Type: $DATA (128-6)   Name: N/A   Non-Resident   size: 277086208  init_size: 277086208
```

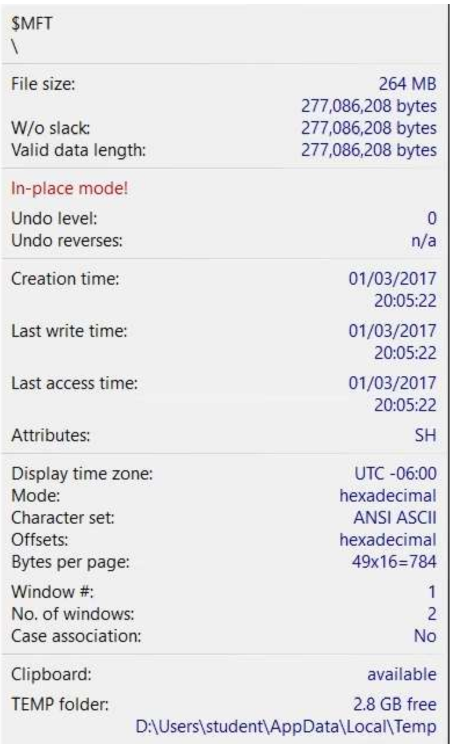


```
2344680 2344681 2344682 2344683 2344684 2344685 2344686 2344687
2344688 2344689 2344690 2344691 2344692 2344693 2344694 2344695
2344696 2344697 2344698 2344699 2344700 2344701 2344702 2344703
2344704 2344705 2344706 2344707 2344708 2344709 2344710 2344711
2344712 2344713 2344714 2344715 2344716 2344717 2344718 2344719
Type: $BITMAP (176-5)   Name: N/A   Non-Resident   size: 36872  init_size: 36872
385413 385414 385415 385416 385417 385418 4341500 7031424
7847676 8369718

D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>_
```

Fig 2: After running “istat -f ntfs DriveC.001 0” → $MFT (Inode 0) Details Using istat (output is too long to screenshot so there are only 2 partial screenshots: one of beginning, one of end)

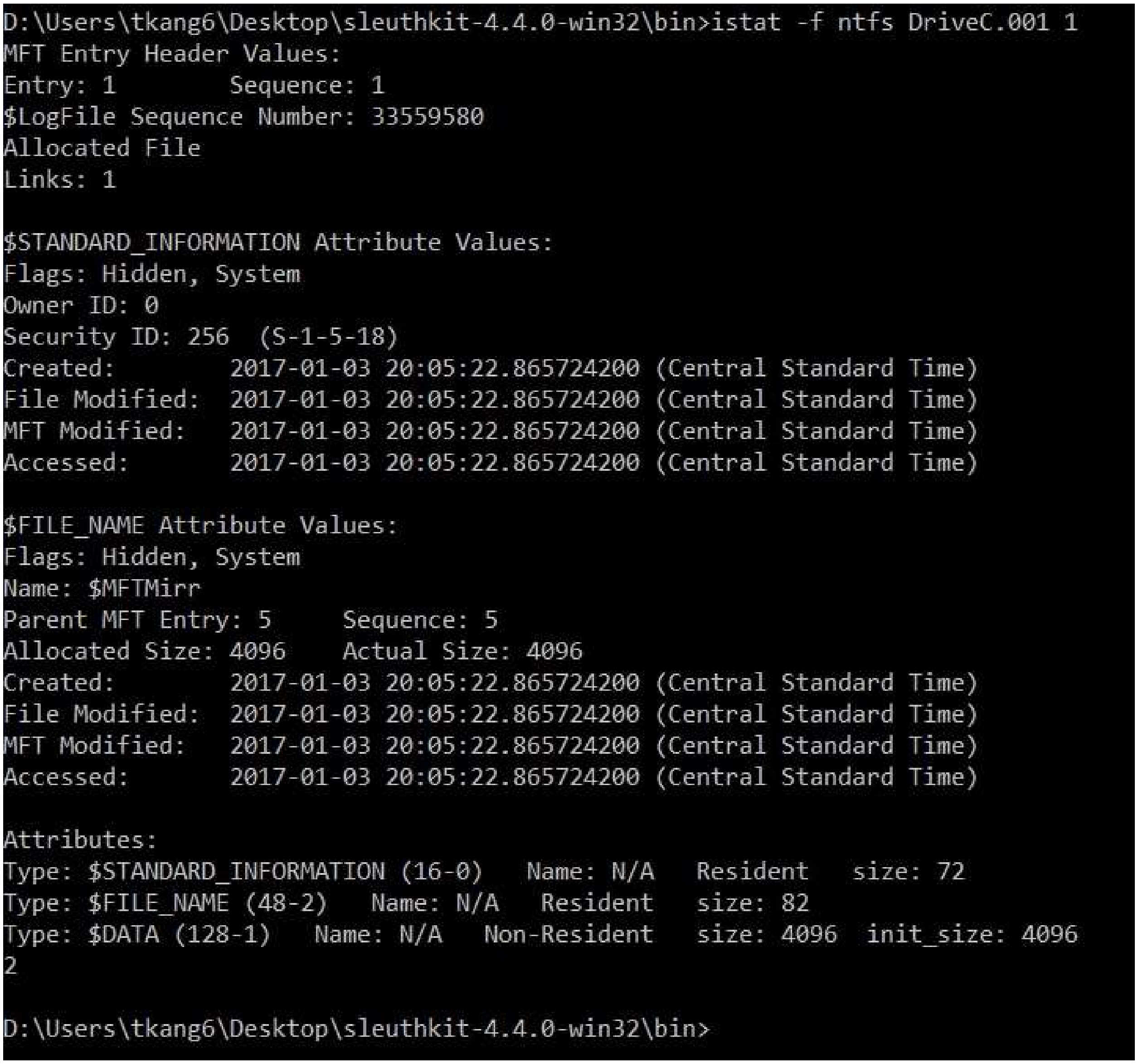


```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0C0000000  46 49 4C 45 30 00 03 00  BC 99 27 1C 01 00 00 00  FILE0   ¼™'
0C0000010  01 00 01 00 38 00 01 00  C0 01 00 00 00 04 00 00      8   À
0C0000020  00 00 00 00 00 00 00 00  07 00 00 00 00 00 00 00
0C0000030  2A 01 00 00 00 00 00 00  10 00 00 00 60 00 00 00  *           `
0C0000040  00 00 18 00 00 00 00 00  48 00 00 00 18 00 00 00          H
0C0000050  5A 36 E8 01 2F 66 D2 01  5A 36 E8 01 2F 66 D2 01  Z6è /fò Z6è /fò
0C0000060  5A 36 E8 01 2F 66 D2 01  5A 36 E8 01 2F 66 D2 01  Z6è /fò Z6è /fò
0C0000070  06 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C0000080  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00
0C0000090  00 00 00 00 00 00 00 00  30 00 00 00 68 00 00 00          0   h
0C00000A0  00 00 18 00 00 00 03 00  4A 00 00 00 18 00 01 00          J
0C00000B0  05 00 00 00 00 00 05 00  5A 36 E8 01 2F 66 D2 01          Z6è /fò
0C00000C0  5A 36 E8 01 2F 66 D2 01  5A 36 E8 01 2F 66 D2 01  Z6è /fò Z6è /fò
0C00000D0  5A 36 E8 01 2F 66 D2 01  00 40 00 00 00 00 00 00  Z6è /fò  @
0C00000E0  00 40 00 00 00 00 00 00  06 00 00 00 00 00 00 00   @
0C00000F0  04 03 24 00 4D 00 46 00  54 00 00 00 00 00 00 00    $ M F T
0C0000100  80 00 00 00 58 00 00 00  01 00 40 00 00 00 06 00  €   X     @
0C0000110  00 00 00 00 00 00 00 00  3F 08 01 00 00 00 00 00          ?
0C0000120  40 00 00 00 00 00 00 00  00 00 84 10 00 00 00 00  @         „
0C0000130  00 00 84 10 00 00 00 00  00 00 84 10 00 00 00 00    „       „
0C0000140  33 40 87 00 00 00 0C 32  40 05 7A 1A 34 32 C0 7B  3@‡    2@ z 42À{
0C0000150  D6 30 E3 00 00 00 00 00  B0 00 00 00 60 00 00 00  Ö0ã     °   `
0C0000160  01 00 40 00 00 00 05 00  00 00 00 00 00 00 00 00    @
0C0000170  09 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00          @
0C0000180  00 A0 00 00 00 00 00 00  08 90 00 00 00 00 00 00
0C0000190  08 90 00 00 00 00 00 00  31 06 85 E1 05 31 01 77          1 …á 1 w
0C00001A0  5D 3C 31 01 84 0B 29 31  01 7C 74 0C 31 01 3A F7  ]<1 „ )1 |t 1 :÷
0C00001B0  07 00 00 00 00 00 00 00  FF FF FF FF 00 00 00 00          ÿÿÿÿ
```



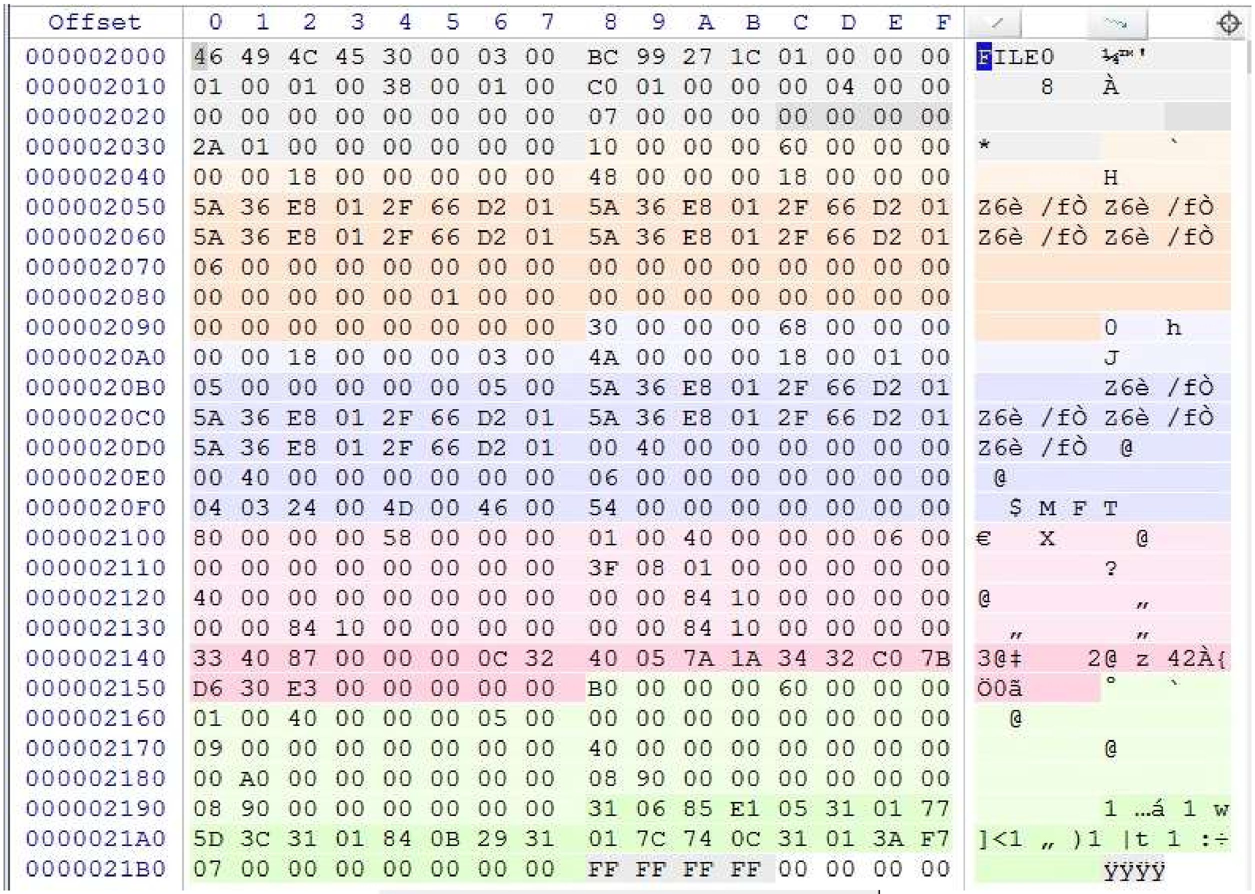
```
$MFT
\

File size:                         264 MB
                        277,086,208 bytes
W/o slack:              277,086,208 bytes
Valid data length:      277,086,208 bytes

In-place mode!
Undo level:                             0
Undo reverses:                        n/a

Creation time:                 01/03/2017
                                 20:05:22
Last write time:               01/03/2017
                                 20:05:22
Last access time:              01/03/2017
                                 20:05:22
Attributes:                            SH

Display time zone:             UTC -06:00
Mode:                         hexadecimal
Character set:                 ANSI ASCII
Offsets:                      hexadecimal
Bytes per page:              49x16=784
Window #:                               1
No. of windows:                         2
Case association:                      No

Clipboard:                      available
TEMP folder:                  2.8 GB free
      D:\Users\student\AppData\Local\Temp
```

Fig 3: $MFT details in WinHex

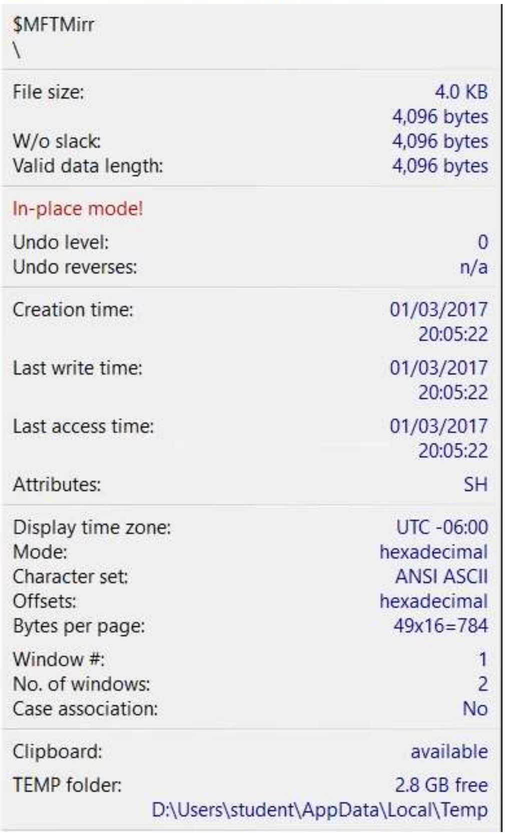


```
D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>istat -f ntfs DriveC.001 1
MFT Entry Header Values:
Entry: 1        Sequence: 1
$LogFile Sequence Number: 33559580
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256  (S-1-5-18)
Created:        2017-01-03 20:05:22.865724200 (Central Standard Time)
File Modified:  2017-01-03 20:05:22.865724200 (Central Standard Time)
MFT Modified:   2017-01-03 20:05:22.865724200 (Central Standard Time)
Accessed:       2017-01-03 20:05:22.865724200 (Central Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $MFTMirr
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 4096    Actual Size: 4096
Created:        2017-01-03 20:05:22.865724200 (Central Standard Time)
File Modified:  2017-01-03 20:05:22.865724200 (Central Standard Time)
MFT Modified:   2017-01-03 20:05:22.865724200 (Central Standard Time)
Accessed:       2017-01-03 20:05:22.865724200 (Central Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 82
Type: $DATA (128-1)   Name: N/A   Non-Resident   size: 4096  init_size: 4096
2

D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>
```

Fig 4: After running “istat -f ntfs DriveC.001 1” → $MFTMirr Details Using istat



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000002000 46 49 4C 45 30 00 03 00  BC 99 27 1C 01 00 00 00  FILE0   ¼™'
000002010 01 00 01 00 38 00 01 00  C0 01 00 00 00 04 00 00      8   À
000002020 00 00 00 00 00 00 00 00  07 00 00 00 00 00 00 00
000002030 2A 01 00 00 00 00 00 00  10 00 00 00 60 00 00 00  *           `
000002040 00 00 18 00 00 00 00 00  48 00 00 00 18 00 00 00          H
000002050 5A 36 E8 01 2F 66 D2 01  5A 36 E8 01 2F 66 D2 01  Z6è /fÒ Z6è /fÒ
000002060 5A 36 E8 01 2F 66 D2 01  5A 36 E8 01 2F 66 D2 01  Z6è /fÒ Z6è /fÒ
000002070 06 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000002080 00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00
000002090 00 00 00 00 00 00 00 00  30 00 00 00 68 00 00 00          0   h
0000020A0 00 00 18 00 00 00 03 00  4A 00 00 00 18 00 01 00          J
0000020B0 05 00 00 00 00 00 05 00  5A 36 E8 01 2F 66 D2 01          Z6è /fÒ
0000020C0 5A 36 E8 01 2F 66 D2 01  5A 36 E8 01 2F 66 D2 01  Z6è /fÒ Z6è /fÒ
0000020D0 5A 36 E8 01 2F 66 D2 01  00 40 00 00 00 00 00 00  Z6è /fÒ  @
0000020E0 00 40 00 00 00 00 00 00  06 00 00 00 00 00 00 00   @
0000020F0 04 03 24 00 4D 00 46 00  54 00 00 00 00 00 00 00    $ M F T
000002100 80 00 00 00 58 00 00 00  01 00 40 00 00 00 06 00  €   X     @
000002110 00 00 00 00 00 00 00 00  3F 08 01 00 00 00 00 00          ?
000002120 40 00 00 00 00 00 00 00  00 00 84 10 00 00 00 00  @         „
000002130 00 00 84 10 00 00 00 00  00 00 84 10 00 00 00 00    „       „
000002140 33 40 87 00 00 00 0C 32  40 05 7A 1A 34 32 C0 7B  3@‡    2@ z 42À{
000002150 D6 30 E3 00 00 00 00 00  B0 00 00 00 60 00 00 00  Ö0ã     °   `
000002160 01 00 40 00 00 00 05 00  00 00 00 00 00 00 00 00    @
000002170 09 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00          @
000002180 00 A0 00 00 00 00 00 00  08 90 00 00 00 00 00 00
000002190 08 90 00 00 00 00 00 00  31 06 85 E1 05 31 01 77          1 …á 1 w
0000021A0 5D 3C 31 01 84 0B 29 31  01 7C 74 0C 31 01 3A F7  ]<1 „ )1 |t 1 :÷
0000021B0 07 00 00 00 00 00 00 00  FF FF FF FF 00 00 00 00          ÿÿÿÿ
```



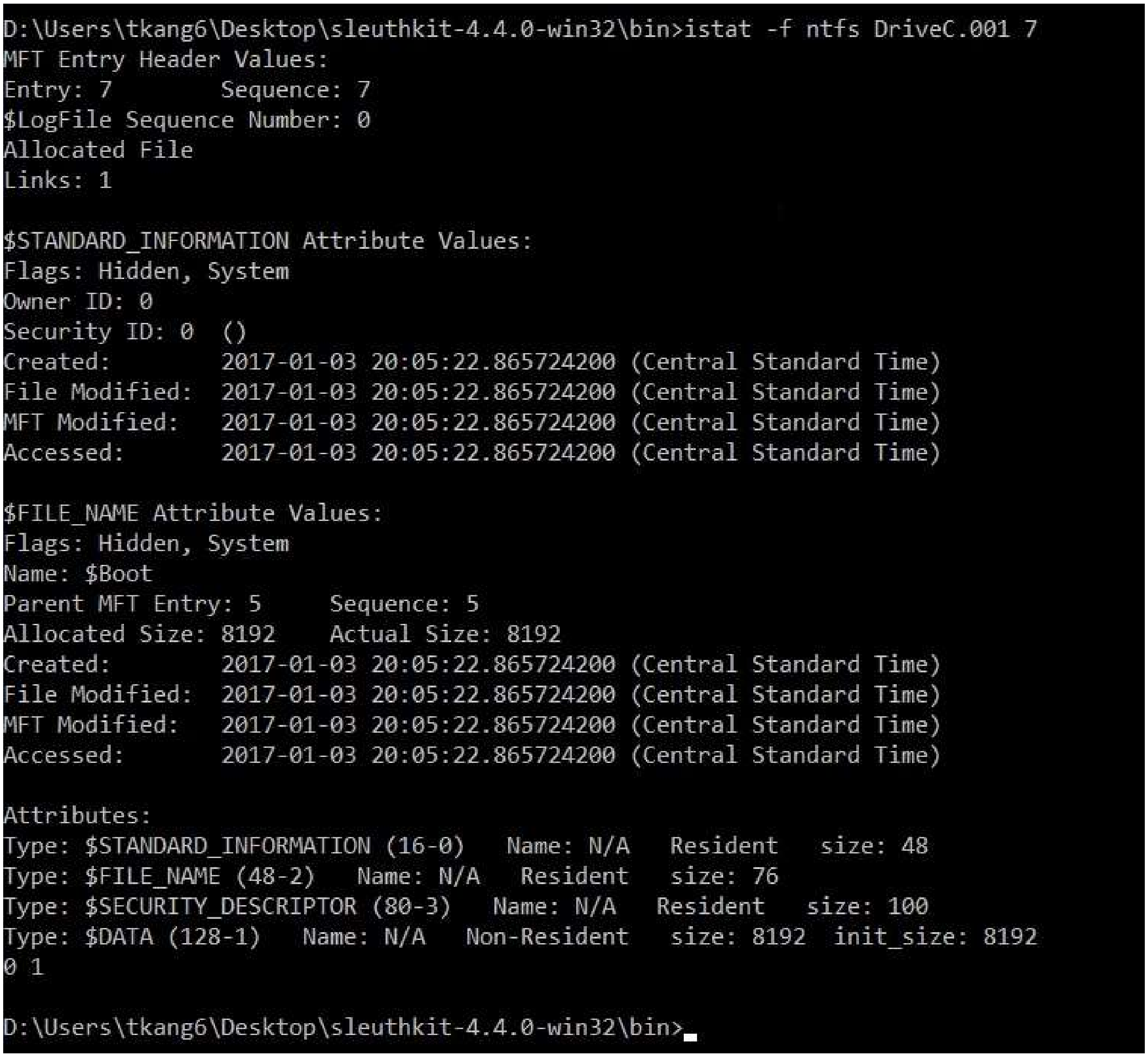
$MFTMirr
\

File size:	4.0 KB 4,096 bytes
W/o slack:	4,096 bytes
Valid data length:	4,096 bytes

In-place mode!

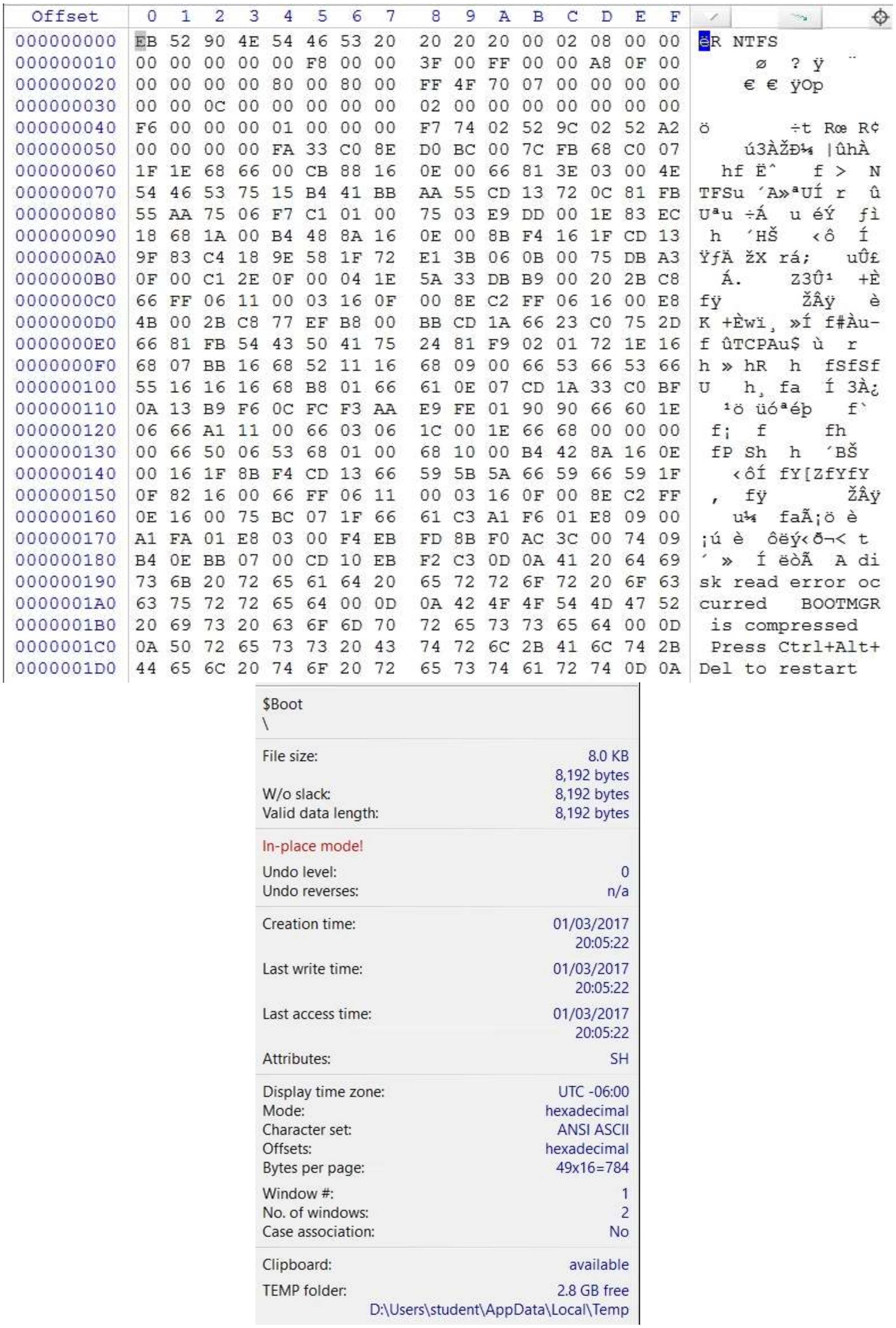
Undo level:	0
Undo reverses:	n/a
Creation time:	01/03/2017 20:05:22
Last write time:	01/03/2017 20:05:22
Last access time:	01/03/2017 20:05:22
Attributes:	SH
Display time zone:	UTC -06:00
Mode:	hexadecimal
Character set:	ANSI ASCII
Offsets:	hexadecimal
Bytes per page:	49x16=784
Window #:	1
No. of windows:	2
Case association:	No
Clipboard:	available
TEMP folder:	2.8 GB free D:\Users\student\AppData\Local\Temp

Fig 5: $MFTMirr details in WinHex



```
D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>istat -f ntfs DriveC.001 7
MFT Entry Header Values:
Entry: 7        Sequence: 7
$LogFile Sequence Number: 0
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 0  ()
Created:        2017-01-03 20:05:22.865724200 (Central Standard Time)
File Modified:  2017-01-03 20:05:22.865724200 (Central Standard Time)
MFT Modified:   2017-01-03 20:05:22.865724200 (Central Standard Time)
Accessed:       2017-01-03 20:05:22.865724200 (Central Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $Boot
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 8192    Actual Size: 8192
Created:        2017-01-03 20:05:22.865724200 (Central Standard Time)
File Modified:  2017-01-03 20:05:22.865724200 (Central Standard Time)
MFT Modified:   2017-01-03 20:05:22.865724200 (Central Standard Time)
Accessed:       2017-01-03 20:05:22.865724200 (Central Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 48
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 76
Type: $SECURITY_DESCRIPTOR (80-3)   Name: N/A   Resident   size: 100
Type: $DATA (128-1)   Name: N/A   Non-Resident   size: 8192  init_size: 8192
0 1

D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>
```

Fig 6: After running “istat -f ntfs DriveC.001 7” → $Boot Details Using istat



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000000000 EB 52 90 4E 54 46 53 20  20 20 20 00 02 08 00 00  ëR NTFS
000000010 00 00 00 00 00 F8 00 00  3F 00 FF 00 00 A8 0F 00       ø  ? ÿ  ¨
000000020 00 00 00 00 80 00 80 00  FF 4F 70 07 00 00 00 00      € € ÿOp
000000030 00 00 0C 00 00 00 00 00  02 00 00 00 00 00 00 00
000000040 F6 00 00 00 01 00 00 00  F7 74 02 52 9C 02 52 A2  ö       ÷t Rœ R¢
000000050 00 00 00 00 FA 33 C0 8E  D0 BC 00 7C FB 68 C0 07      ú3ÀŽÐ¼ |ûhÀ
000000060 1F 1E 68 66 00 CB 88 16  0E 00 66 81 3E 03 00 4E    hf Ëˆ   f >  N
000000070 54 46 53 75 15 B4 41 BB  AA 55 CD 13 72 0C 81 FB  TFSu ´A»ªUÍ r  û
000000080 55 AA 75 06 F7 C1 01 00  75 03 E9 DD 00 1E 83 EC  Uªu ÷Á  u éÝ  ƒì
000000090 18 68 1A 00 B4 48 8A 16  0E 00 8B F4 16 1F CD 13   h  ´HŠ   ‹ô  Í
0000000A0 9F 83 C4 18 9E 58 1F 72  E1 3B 06 0B 00 75 DB A3  ŸƒÄ žX rá;   uÛ£
0000000B0 0F 00 C1 2E 0F 00 04 1E  5A 33 DB B9 00 20 2B C8    Á.    Z3Û¹  +È
0000000C0 66 FF 06 11 00 03 16 0F  00 8E C2 FF 06 16 00 E8  fÿ       ŽÂÿ   è
0000000D0 4B 00 2B C8 77 EF B8 00  BB CD 1A 66 23 C0 75 2D  K +Èwï¸ »Í f#Àu-
0000000E0 66 81 FB 54 43 50 41 75  24 81 F9 02 01 72 1E 16  f ûTCPAu$ ù  r
0000000F0 68 07 BB 16 68 52 11 16  68 09 00 66 53 66 53 66  h » hR  h  fSfSf
000000100 55 16 16 16 68 B8 01 66  61 0E 07 CD 1A 33 C0 BF  U   h¸ fa  Í 3À¿
000000110 0A 13 B9 F6 0C FC F3 AA  E9 FE 01 90 90 66 60 1E    ¹ö üóªéþ   f`
000000120 06 66 A1 11 00 66 03 06  1C 00 1E 66 68 00 00 00   f¡  f     fh
000000130 00 66 50 06 53 68 01 00  68 10 00 B4 42 8A 16 0E   fP Sh  h  ´BŠ
000000140 00 16 1F 8B F4 CD 13 66  59 5B 5A 66 59 66 59 1F     ‹ôÍ fY[ZfYfY
000000150 0F 82 16 00 66 FF 06 11  00 03 16 0F 00 8E C2 FF   ‚  fÿ       ŽÂÿ
000000160 0E 16 00 75 BC 07 1F 66  61 C3 A1 F6 01 E8 09 00     u¼  faÃ¡ö è
000000170 A1 FA 01 E8 03 00 F4 EB  FD 8B F0 AC 3C 00 74 09  ¡ú è  ôëý‹ð¬< t
000000180 B4 0E BB 07 00 CD 10 EB  F2 C3 0D 0A 41 20 64 69  ´ »  Í ëòÃ  A di
000000190 73 6B 20 72 65 61 64 20  65 72 72 6F 72 20 6F 63  sk read error oc
0000001A0 63 75 72 72 65 64 00 0D  0A 42 4F 4F 54 4D 47 52  curred   BOOTMGR
0000001B0 20 69 73 20 63 6F 6D 70  72 65 73 73 65 64 00 0D   is compressed
0000001C0 0A 50 72 65 73 73 20 43  74 72 6C 2B 41 6C 74 2B   Press Ctrl+Alt+
0000001D0 44 65 6C 20 74 6F 20 72  65 73 74 61 72 74 0D 0A  Del to restart
```

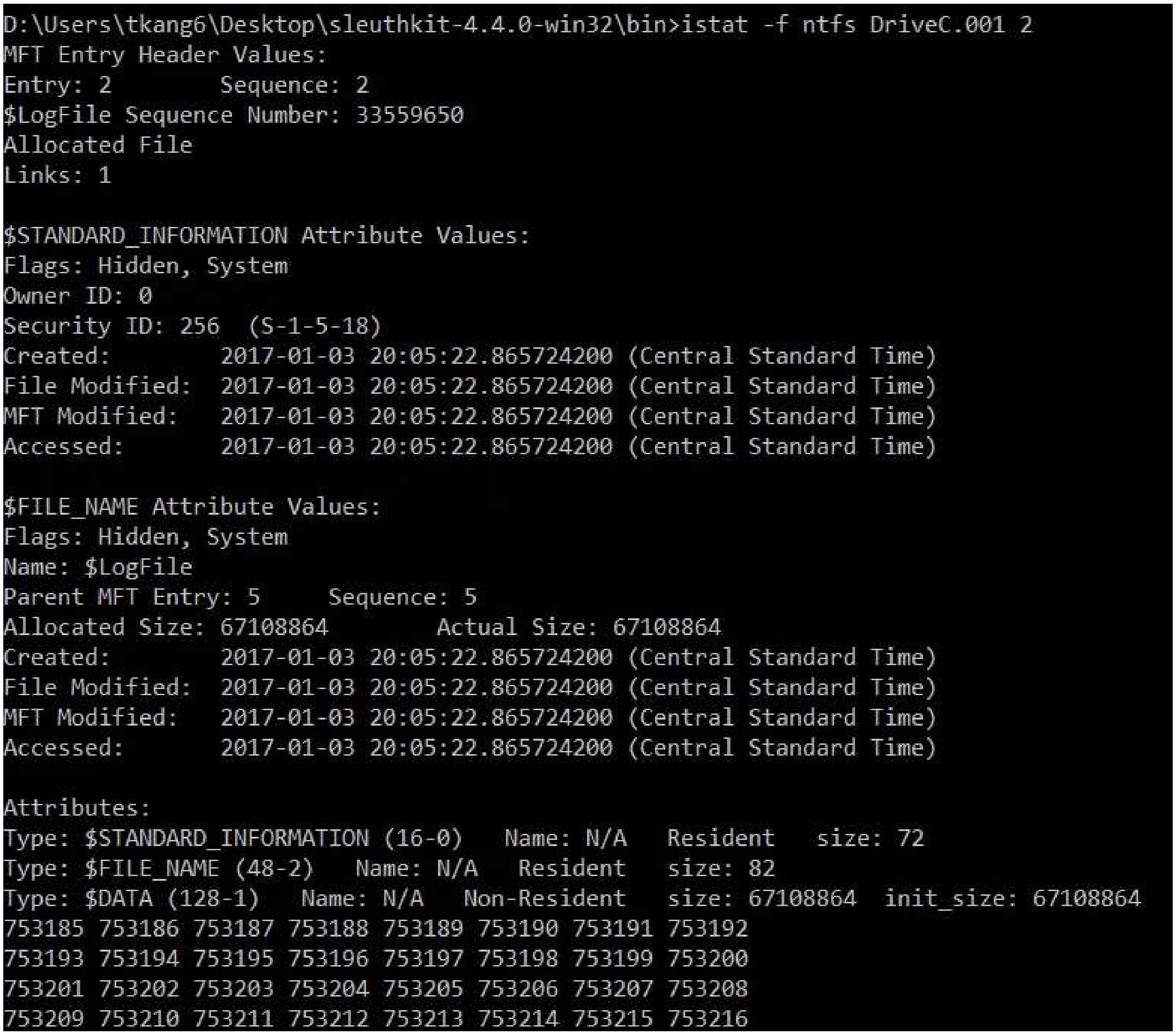
$Boot
\

File size:	8.0 KB 8,192 bytes
W/o slack:	8,192 bytes
Valid data length:	8,192 bytes

In-place mode!

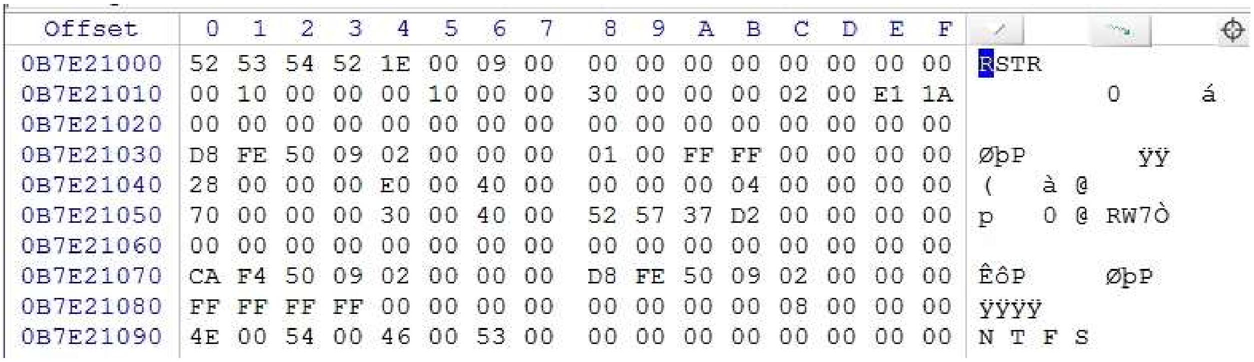
Undo level:	0
Undo reverses:	n/a
Creation time:	01/03/2017 20:05:22
Last write time:	01/03/2017 20:05:22
Last access time:	01/03/2017 20:05:22
Attributes:	SH
Display time zone:	UTC -06:00
Mode:	hexadecimal
Character set:	ANSI ASCII
Offsets:	hexadecimal
Bytes per page:	49x16=784
Window #:	1
No. of windows:	2
Case association:	No
Clipboard:	available
TEMP folder:	2.8 GB free D:\Users\student\AppData\Local\Temp

Fig 7: $Boot details in WinHex

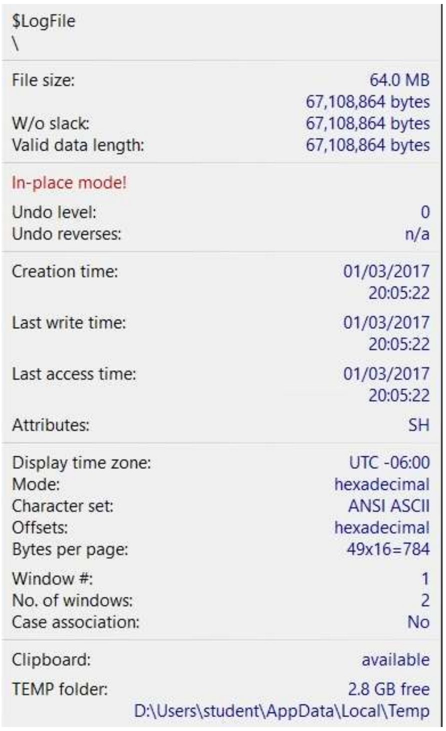


```
D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>istat -f ntfs DriveC.001 2
MFT Entry Header Values:
Entry: 2        Sequence: 2
$LogFile Sequence Number: 33559650
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256  (S-1-5-18)
Created:        2017-01-03 20:05:22.865724200 (Central Standard Time)
File Modified:  2017-01-03 20:05:22.865724200 (Central Standard Time)
MFT Modified:   2017-01-03 20:05:22.865724200 (Central Standard Time)
Accessed:       2017-01-03 20:05:22.865724200 (Central Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $LogFile
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 67108864        Actual Size: 67108864
Created:        2017-01-03 20:05:22.865724200 (Central Standard Time)
File Modified:  2017-01-03 20:05:22.865724200 (Central Standard Time)
MFT Modified:   2017-01-03 20:05:22.865724200 (Central Standard Time)
Accessed:       2017-01-03 20:05:22.865724200 (Central Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 82
Type: $DATA (128-1)   Name: N/A   Non-Resident   size: 67108864  init_size: 67108864
753185 753186 753187 753188 753189 753190 753191 753192
753193 753194 753195 753196 753197 753198 753199 753200
753201 753202 753203 753204 753205 753206 753207 753208
753209 753210 753211 753212 753213 753214 753215 753216
```

Fig 8: After running “istat -f ntfs DriveC.001 2” → $LogFile Details Using istat

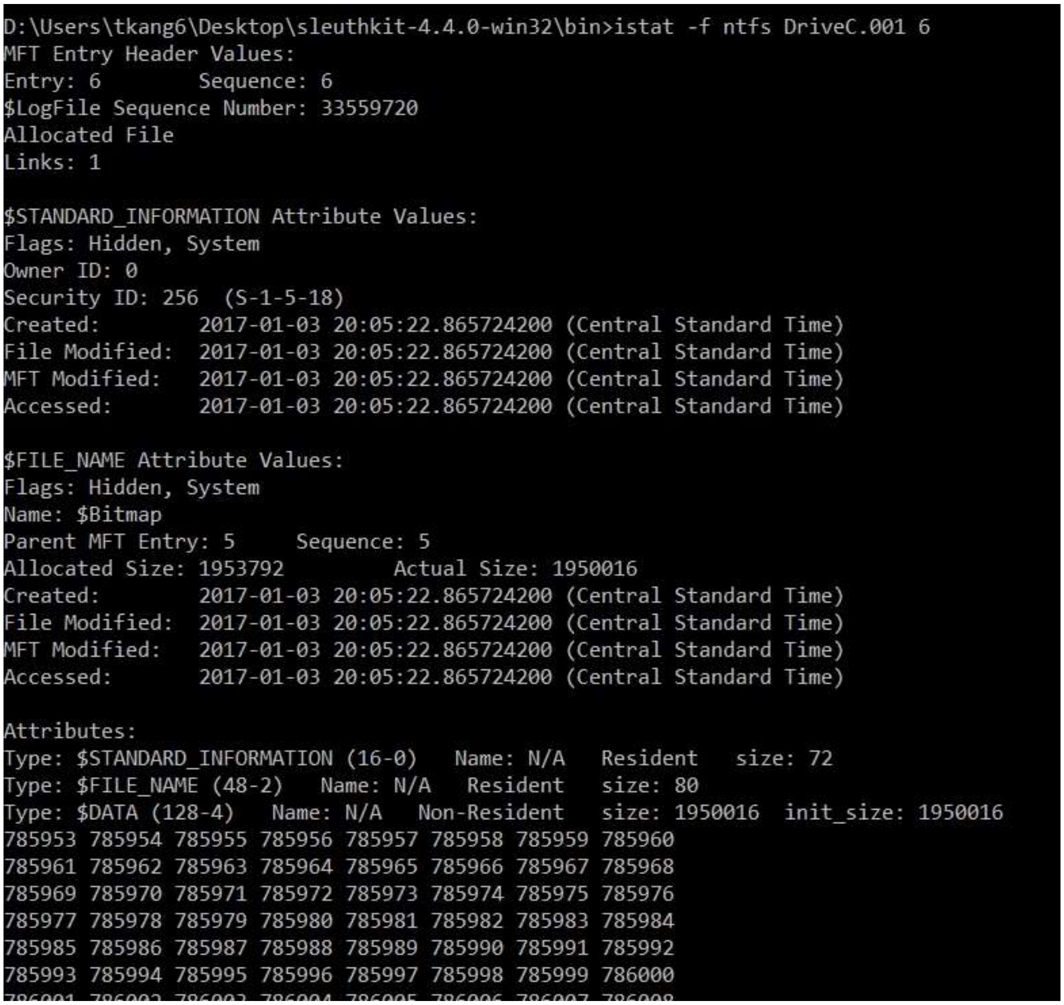


```
 Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0B7E21000  52 53 54 52 1E 00 09 00  00 00 00 00 00 00 00 00  RSTR
0B7E21010  00 10 00 00 00 10 00 00  30 00 00 00 02 00 E1 1A          0      á
0B7E21020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0B7E21030  D8 FE 50 09 02 00 00 00  01 00 FF FF 00 00 00 00  ØþP       ÿÿ
0B7E21040  28 00 00 00 E0 00 40 00  00 00 00 04 00 00 00 00  (   à @
0B7E21050  70 00 00 00 30 00 40 00  52 57 37 D2 00 00 00 00  p   0 @ RW7Ò
0B7E21060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0B7E21070  CA F4 50 09 02 00 00 00  D8 FE 50 09 02 00 00 00  ÊôP     ØþP
0B7E21080  FF FF FF FF 00 00 00 00  00 00 00 00 08 00 00 00  ÿÿÿÿ
0B7E21090  4E 00 54 00 46 00 53 00  00 00 00 00 00 00 00 00  N T F S
```



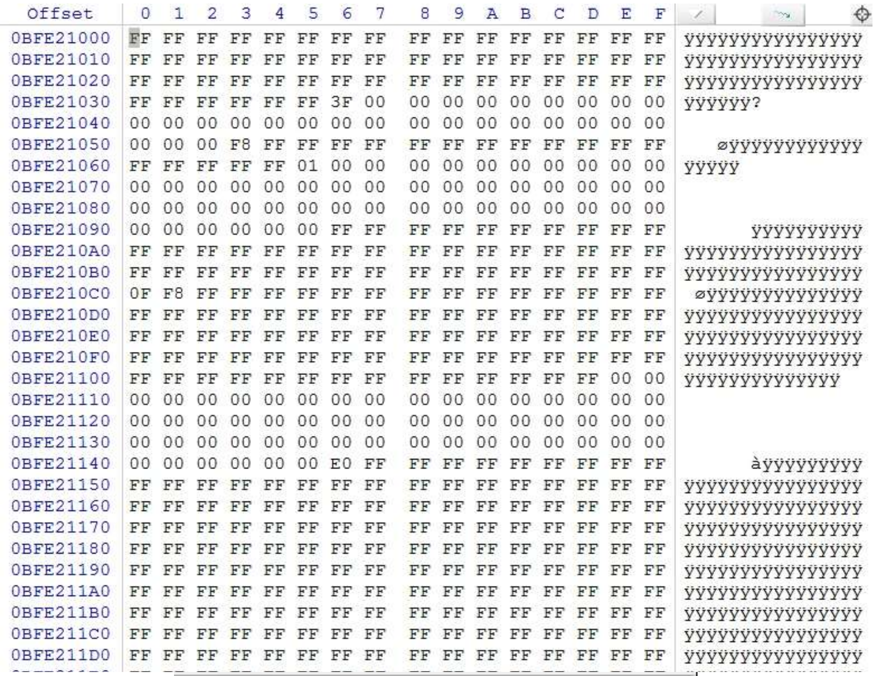
```
$LogFile
\

File size:                          64.0 MB
                          67,108,864 bytes
W/o slack:                67,108,864 bytes
Valid data length:        67,108,864 bytes

In-place mode!
Undo level:                              0
Undo reverses:                         n/a

Creation time:                  01/03/2017
                                  20:05:22
Last write time:                01/03/2017
                                  20:05:22
Last access time:               01/03/2017
                                  20:05:22
Attributes:                             SH

Display time zone:              UTC -06:00
Mode:                          hexadecimal
Character set:                  ANSI ASCII
Offsets:                       hexadecimal
Bytes per page:                49x16=784
Window #:                                1
No. of windows:                          2
Case association:                       No

Clipboard:                       available
TEMP folder:                   2.8 GB free
      D:\Users\student\AppData\Local\Temp
```

Fig 9: $LogFile details in WinHex

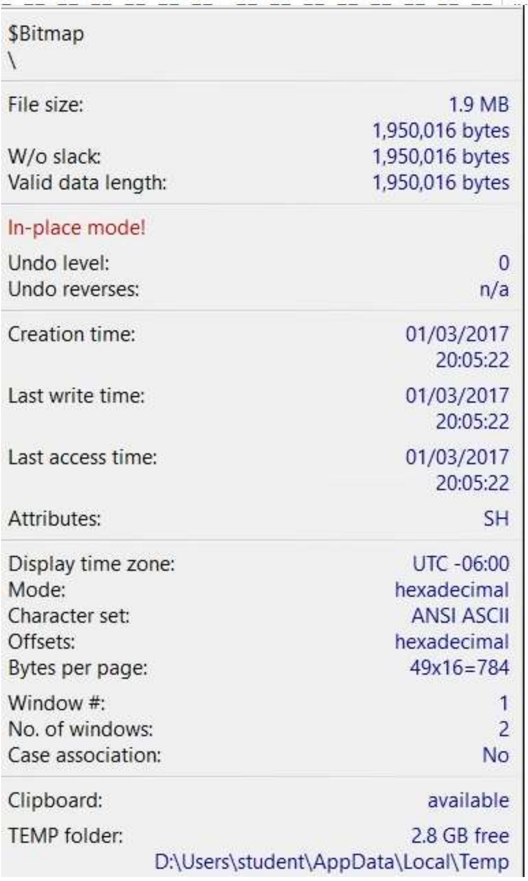


```
D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>istat -f ntfs DriveC.001 6
MFT Entry Header Values:
Entry: 6        Sequence: 6
$LogFile Sequence Number: 33559720
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256  (S-1-5-18)
Created:        2017-01-03 20:05:22.865724200 (Central Standard Time)
File Modified:  2017-01-03 20:05:22.865724200 (Central Standard Time)
MFT Modified:   2017-01-03 20:05:22.865724200 (Central Standard Time)
Accessed:       2017-01-03 20:05:22.865724200 (Central Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $Bitmap
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 1953792         Actual Size: 1950016
Created:        2017-01-03 20:05:22.865724200 (Central Standard Time)
File Modified:  2017-01-03 20:05:22.865724200 (Central Standard Time)
MFT Modified:   2017-01-03 20:05:22.865724200 (Central Standard Time)
Accessed:       2017-01-03 20:05:22.865724200 (Central Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-2)   Name: N/A   Resident   size: 80
Type: $DATA (128-4)   Name: N/A   Non-Resident   size: 1950016  init_size: 1950016
785953 785954 785955 785956 785957 785958 785959 785960
785961 785962 785963 785964 785965 785966 785967 785968
785969 785970 785971 785972 785973 785974 785975 785976
785977 785978 785979 785980 785981 785982 785983 785984
785985 785986 785987 785988 785989 785990 785991 785992
785993 785994 785995 785996 785997 785998 785999 786000
786001 786002 786003 786004 786005 786006 786007 786008
```

Fig 10: After running “istat -f ntfs DriveC.001 6” → $Bitmap Details Using istat



```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
0BFE21000  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE21010  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE21020  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE21030  FF FF FF FF FF FF 3F 00  00 00 00 00 00 00 00 00  ÿÿÿÿÿÿ?
0BFE21040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0BFE21050  00 00 00 F8 FF FF FF FF  FF FF FF FF FF FF FF FF     øÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE21060  FF FF FF FF FF 01 00 00  00 00 00 00 00 00 00 00  ÿÿÿÿÿ
0BFE21070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0BFE21080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0BFE21090  00 00 00 00 00 00 FF FF  FF FF FF FF FF FF FF FF        ÿÿÿÿÿÿÿÿÿÿ
0BFE210A0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE210B0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE210C0  0F F8 FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   øÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE210D0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE210E0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE210F0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE21100  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF 00 00  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE21110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0BFE21120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0BFE21130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0BFE21140  00 00 00 00 00 00 E0 FF  FF FF FF FF FF FF FF FF        àÿÿÿÿÿÿÿÿÿ
0BFE21150  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE21160  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE21170  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE21180  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE21190  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE211A0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE211B0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE211C0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0BFE211D0  FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

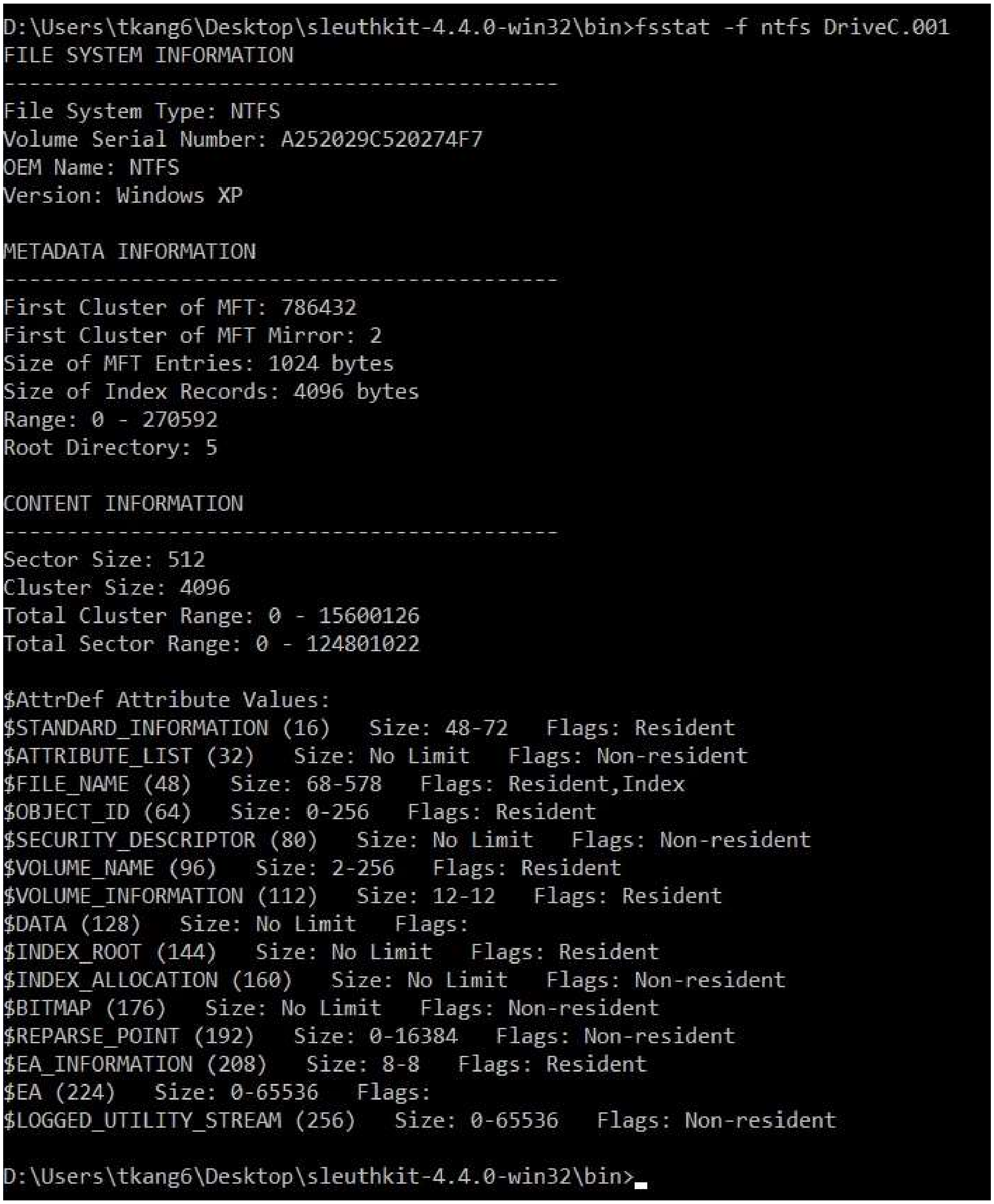


```
$Bitmap
\

File size:                         1.9 MB
                          1,950,016 bytes
W/o slack:                1,950,016 bytes
Valid data length:        1,950,016 bytes

In-place mode!
Undo level:                             0
Undo reverses:                        n/a

Creation time:                 01/03/2017
                                 20:05:22
Last write time:               01/03/2017
                                 20:05:22
Last access time:              01/03/2017
                                 20:05:22
Attributes:                            SH

Display time zone:             UTC -06:00
Mode:                         hexadecimal
Character set:                 ANSI ASCII
Offsets:                      hexadecimal
Bytes per page:              49x16=784
Window #:                               1
No. of windows:                         2
Case association:                      No

Clipboard:                      available
TEMP folder:                  2.8 GB free
        D:\Users\student\AppData\Local\Temp
```

Fig 11: $Bitmap details in WinHex

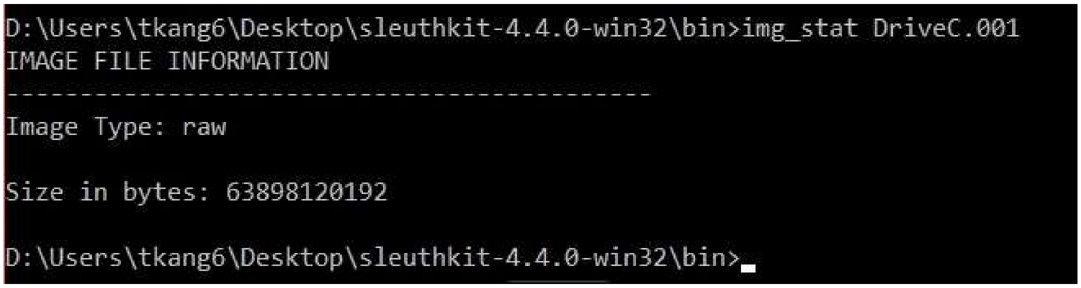
MFT Entry	The sector location	Sector size	Attributes
$MFT	6291456	1024 bytes	0x10, 0x30, 0x80, 0xB0
$MTFMirr	16	1024 bytes	0x10, 0x30, 0x80, 0xB0
$Boot	0	1024 bytes	
$LogFile	6025480	1024 bytes	
$Bitmap	6287624	1024 bytes	

Fig 12: table with information of each MFT entry



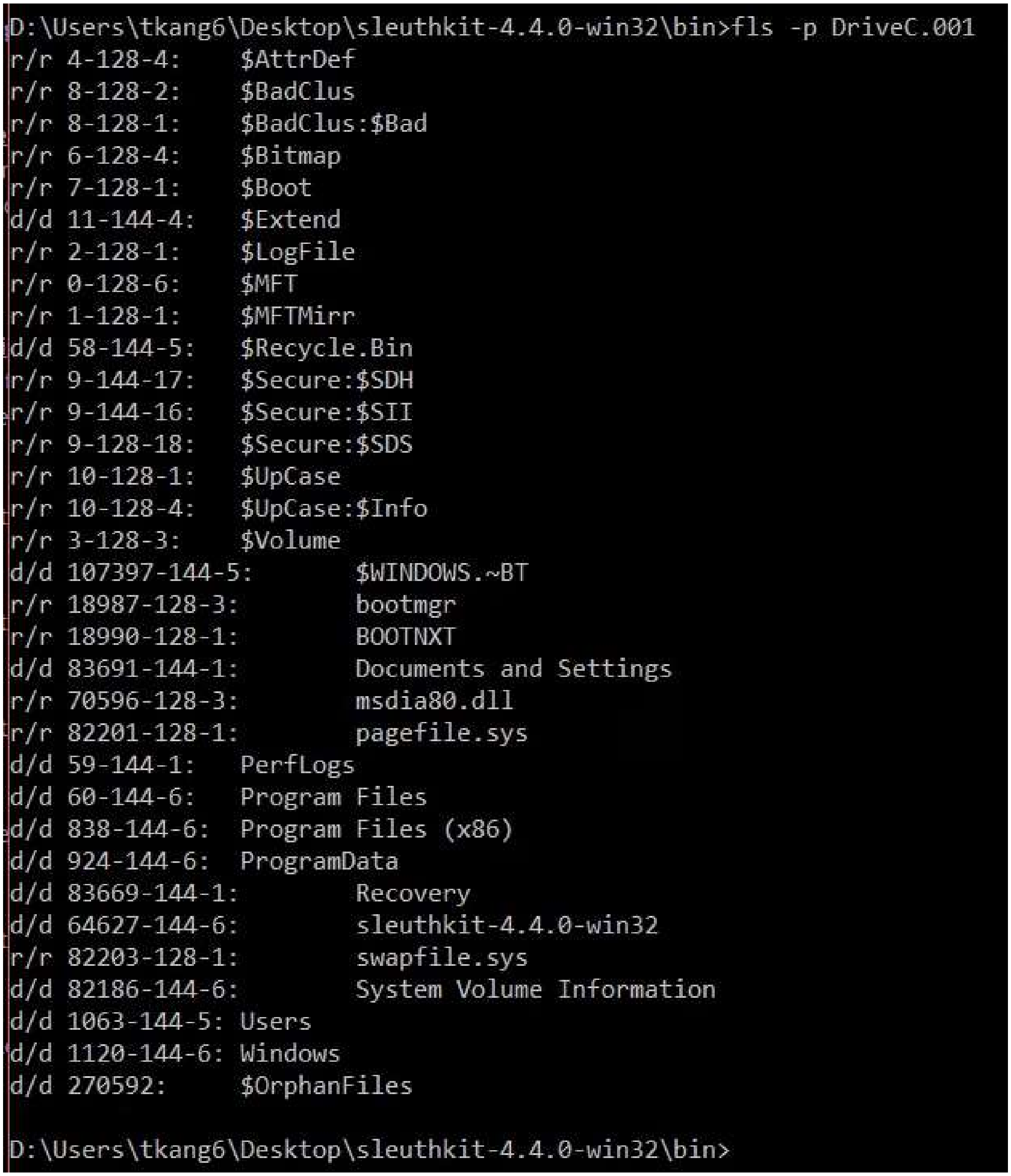
```
D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>fsstat -f ntfs DriveC.001
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: A252029C520274F7
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 786432
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 270592
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 15600126
Total Sector Range: 0 - 124801022

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit   Flags: Non-resident
$VOLUME_NAME (96)   Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)   Size: No Limit   Flags:
$INDEX_ROOT (144)   Size: No Limit   Flags: Resident
$INDEX_ALLOCATION (160)   Size: No Limit   Flags: Non-resident
$BITMAP (176)   Size: No Limit   Flags: Non-resident
$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident

D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>_
```

Fig 13: After running “fsstat -f ntfs DriveC.001”→ Disk details using fsstat



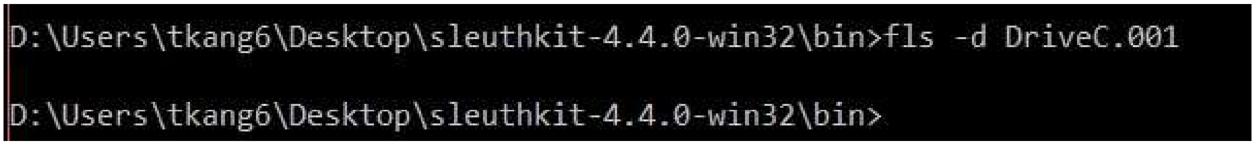
```
D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>img_stat DriveC.001
IMAGE FILE INFORMATION
--------------------------------------------
Image Type: raw

Size in bytes: 63898120192

D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>_
```

Fig 14: After running “img_stat DriveC.001”→ displaying basic details about the image file



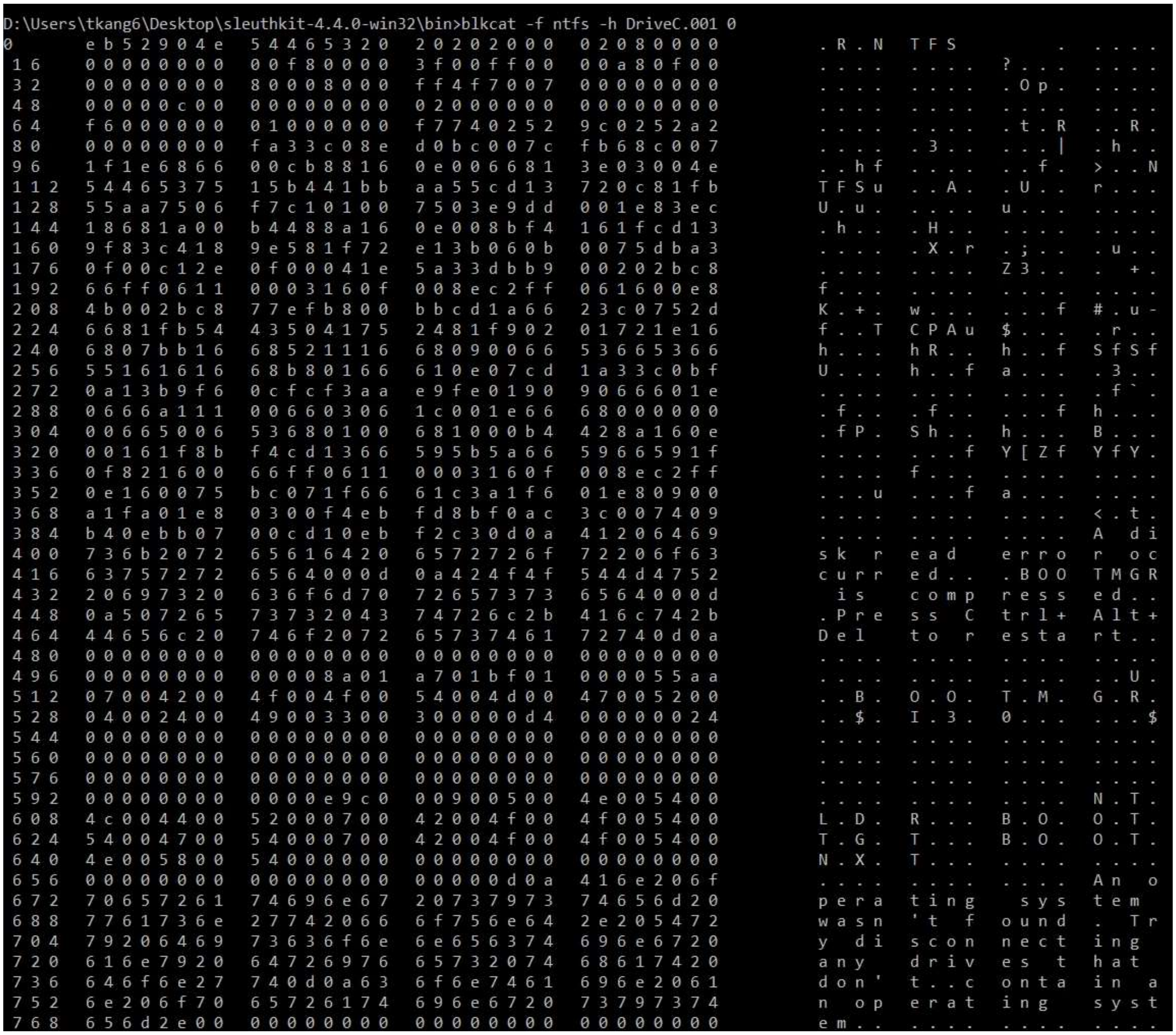
```
D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>fls -p DriveC.001
r/r 4-128-4:    $AttrDef
r/r 8-128-2:    $BadClus
r/r 8-128-1:    $BadClus:$Bad
r/r 6-128-4:    $Bitmap
r/r 7-128-1:    $Boot
d/d 11-144-4:   $Extend
r/r 2-128-1:    $LogFile
r/r 0-128-6:    $MFT
r/r 1-128-1:    $MFTMirr
d/d 58-144-5:   $Recycle.Bin
r/r 9-144-17:   $Secure:$SDH
r/r 9-144-16:   $Secure:$SII
r/r 9-128-18:   $Secure:$SDS
r/r 10-128-1:   $UpCase
r/r 10-128-4:   $UpCase:$Info
r/r 3-128-3:    $Volume
d/d 107397-144-5:       $WINDOWS.~BT
r/r 18987-128-3:        bootmgr
r/r 18990-128-1:        BOOTNXT
d/d 83691-144-1:        Documents and Settings
r/r 70596-128-3:        msdia80.dll
r/r 82201-128-1:        pagefile.sys
d/d 59-144-1:   PerfLogs
d/d 60-144-6:   Program Files
d/d 838-144-6:  Program Files (x86)
d/d 924-144-6:  ProgramData
d/d 83669-144-1:        Recovery
d/d 64627-144-6:        sleuthkit-4.4.0-win32
r/r 82203-128-1:        swapfile.sys
d/d 82186-144-6:        System Volume Information
d/d 1063-144-5: Users
d/d 1120-144-6: Windows
d/d 270592:     $OrphanFiles

D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>
```

Fig 15: After running “fls -p DriveC.001”→ listing file/directory names and full path of files



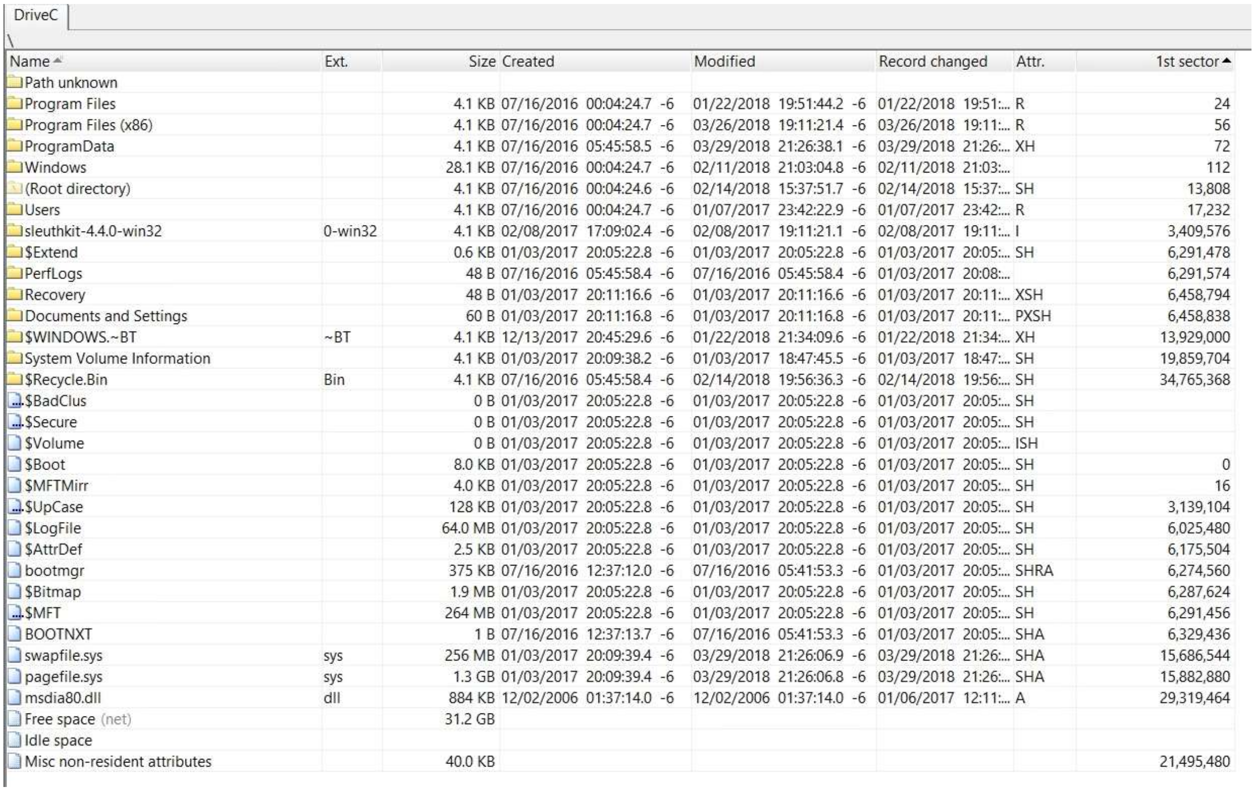
```
D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>fls -d DriveC.001

D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>
```

Fig 16: After running “fls -d DriveC.001”→ listing deleted entries of C Drive



```
D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>blkcat -f ntfs -h DriveC.001 0
0       eb52904e 54465320 20202000 02080000     .R.N TFS     . ....
16      00000000 00f80000 3f00ff00 00a80f00     .... .... ?... ....
32      00000000 80008000 ff4f7007 00000000     .... .... .Op. ....
48      00000c00 00000000 02000000 00000000     .... .... .... ....
64      f6000000 01000000 f7740252 9c0252a2     .... .... .t.R ..R.
80      00000000 fa33c08e d0bc007c fb68c007     .... .3.. ...| .h..
96      1f1e6866 00cb8816 0e006681 3e03004e     ..hf .... ..f. >..N
112     54465375 15b441bb aa55cd13 720c81fb     TFSu ..A. .U.. r...
128     55aa7506 f7c10100 7503e9dd 001e83ec     U.u. .... u... ....
144     18681a00 b4488a16 0e008bf4 161fcd13     .h.. .H.. .... ....
160     9f83c418 9e581f72 e13b060b 0075dba3     .... .X.r .;.. .u..
176     0f00c12e 0f00041e 5a33dbb9 00202bc8     .... .... Z3.. . +.
192     66ff0611 0003160f 008ec2ff 061600e8     f... .... .... ....
208     4b002bc8 77efb800 bbcd1a66 23c0752d     K.+. w... ...f #.u-
224     6681fb54 43504175 2481f902 01721e16     f..T CPAu $... .r..
240     6807bb16 68521116 68090066 53665366     h... hR.. h..f SfSf
256     55161616 68b80166 610e07cd 1a33c0bf     U... h..f a... .3..
272     0a13b9f6 0cfcf3aa e9fe0190 9066601e     .... .... .... .f`.
288     0666a111 00660306 1c001e66 68000000     .f.. .f.. ...f h...
304     00665006 53680100 681000b4 428a160e     .fP. Sh.. h... B...
320     00161f8b f4cd1366 595b5a66 5966591f     .... ...f Y[Zf YfY.
336     0f821600 66ff0611 0003160f 008ec2ff     .... f... .... ....
352     0e160075 bc071f66 61c3a1f6 01e80900     ...u ...f a... ....
368     a1fa01e8 0300f4eb fd8bf0ac 3c007409     .... .... .... <.t.
384     b40ebb07 00cd10eb f2c30d0a 41206469     .... .... .... A di
400     736b2072 65616420 6572726f 72206f63     sk r ead  erro r oc
416     63757272 6564000d 0a424f4f 544d4752     curr ed.. .BOO TMGR
432     20697320 636f6d70 72657373 6564000d      is  comp ress ed..
448     0a507265 73732043 74726c2b 416c742b     .Pre ss C trl+ Alt+
464     44656c20 746f2072 65737461 72740d0a     Del  to r esta rt..
480     00000000 00000000 00000000 00000000     .... .... .... ....
496     00000000 00008a01 a701bf01 000055aa     .... .... .... ..U.
512     07004200 4f004f00 54004d00 47005200     ..B. O.O. T.M. G.R.
528     04002400 49003300 300000d4 00000024     ..$. I.3. 0... ...$
544     00000000 00000000 00000000 00000000     .... .... .... ....
560     00000000 00000000 00000000 00000000     .... .... .... ....
576     00000000 00000000 00000000 00000000     .... .... .... ....
592     00000000 0000e9c0 00900500 4e005400     .... .... .... N.T.
608     4c004400 52000700 42004f00 4f005400     L.D. R... B.O. O.T.
624     54004700 54000700 42004f00 4f005400     T.G. T... B.O. O.T.
640     4e005800 54000000 00000000 00000000     N.X. T... .... ....
656     00000000 00000000 00000d0a 416e206f     .... .... .... An o
672     70657261 74696e67 20737973 74656d20     pera ting  sys tem 
688     7761736e 27742066 6f756e64 2e205472     wasn 't f ound . Tr
704     79206469 73636f6e 6e656374 696e6720     y di scon nect ing 
720     616e7920 64726976 65732074 68617420     any  driv es t hat 
736     646f6e27 740d0a63 6f6e7461 696e2061     don' t..c onta in a
752     6e206f70 65726174 696e6720 73797374     n op erat ing  syst
768     656d2e00 00000000 00000000 00000000     em.. .... .... ....
```

Fig 17: After running "blkcat -f ntfs -h DriveC.001 0"→Displaying hex and ASCII contents of file system in disk image within terminal

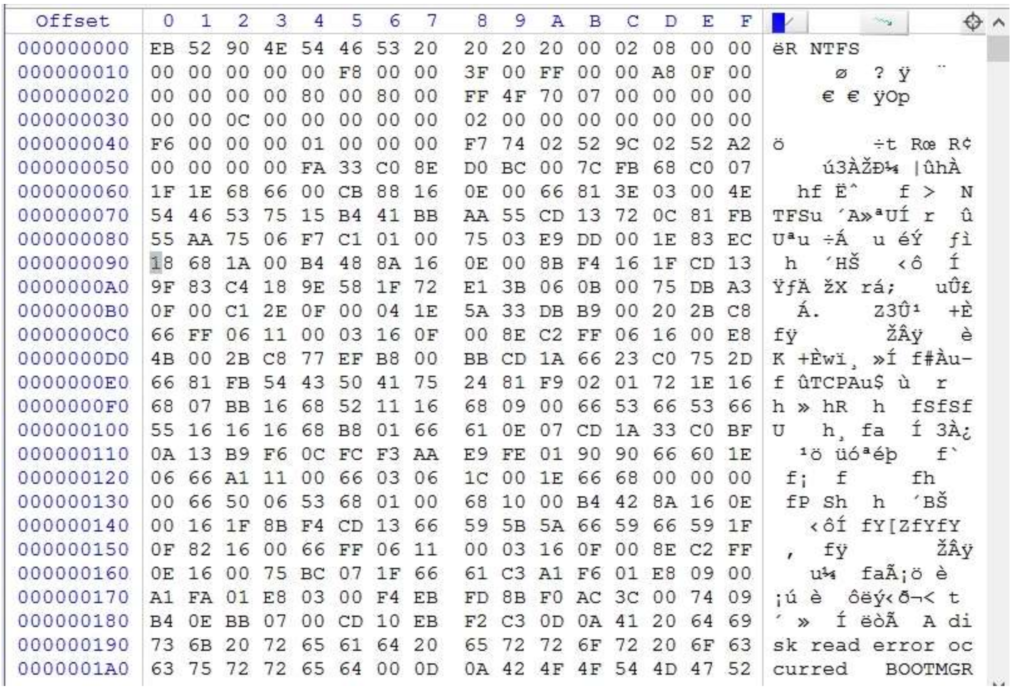


DriveC

\

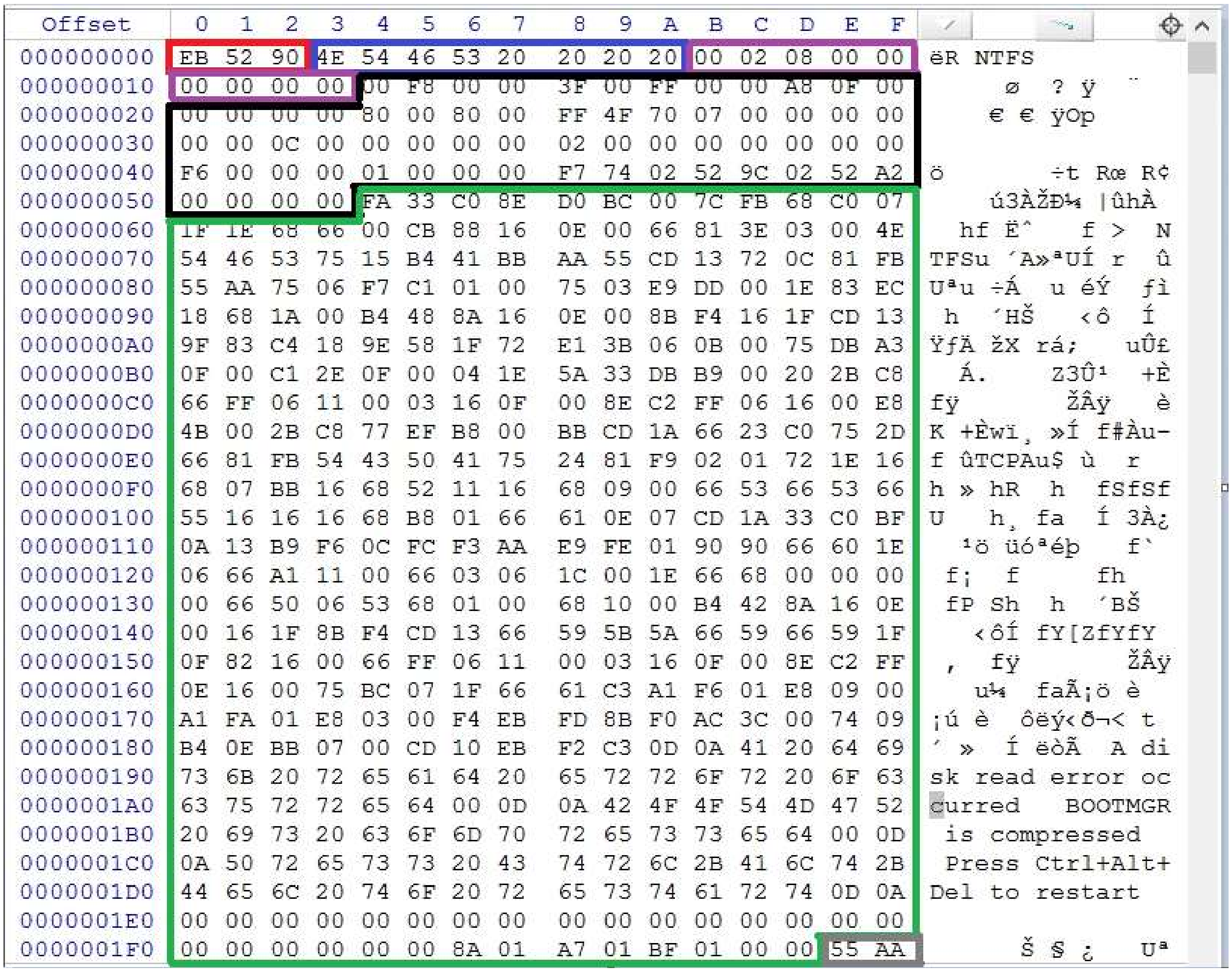
Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
Path unknown							
Program Files		4.1 KB	07/16/2016 00:04:24.7 -6	01/22/2018 19:51:44.2 -6	01/22/2018 19:51:...	R	24
Program Files (x86)		4.1 KB	07/16/2016 00:04:24.7 -6	03/26/2018 19:11:21.4 -6	03/26/2018 19:11:...	R	56
ProgramData		4.1 KB	07/16/2016 05:45:58.5 -6	03/29/2018 21:26:38.1 -6	03/29/2018 21:26:...	XH	72
Windows		28.1 KB	07/16/2016 00:04:24.7 -6	02/11/2018 21:03:04.8 -6	02/11/2018 21:03:...		112
(Root directory)		4.1 KB	07/16/2016 00:04:24.6 -6	02/14/2018 15:37:51.7 -6	02/14/2018 15:37:...	SH	13,808
Users		4.1 KB	07/16/2016 00:04:24.7 -6	01/07/2017 23:42:22.9 -6	01/07/2017 23:42:...	R	17,232
sleuthkit-4.4.0-win32	0-win32	4.1 KB	02/08/2017 17:09:02.4 -6	02/08/2017 19:11:21.1 -6	02/08/2017 19:11:...	I	3,409,576
$Extend		0.6 KB	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:...	SH	6,291,478
PerfLogs		48 B	07/16/2016 05:45:58.4 -6	07/16/2016 05:45:58.4 -6	01/03/2017 20:08:...		6,291,574
Recovery		48 B	01/03/2017 20:11:16.6 -6	01/03/2017 20:11:16.6 -6	01/03/2017 20:11:...	XSH	6,458,794
Documents and Settings		60 B	01/03/2017 20:11:16.8 -6	01/03/2017 20:11:16.8 -6	01/03/2017 20:11:...	PXSH	6,458,838
$WINDOWS.~BT	~BT	4.1 KB	12/13/2017 20:45:29.6 -6	01/22/2018 21:34:09.6 -6	01/22/2018 21:34:...	XH	13,929,000
System Volume Information		4.1 KB	01/03/2017 20:09:38.2 -6	01/03/2017 18:47:45.5 -6	01/03/2017 18:47:...	SH	19,859,704
$Recycle.Bin	Bin	4.1 KB	07/16/2016 05:45:58.4 -6	02/14/2018 19:56:36.3 -6	02/14/2018 19:56:...	SH	34,765,368
$BadClus		0 B	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:...	SH	
$Secure		0 B	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:...	SH	
$Volume		0 B	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:...	ISH	
$Boot		8.0 KB	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:...	SH	0
$MFTMirr		4.0 KB	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:...	SH	16
$UpCase		128 KB	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:...	SH	3,139,104
$LogFile		64.0 MB	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:...	SH	6,025,480
$AttrDef		2.5 KB	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:...	SH	6,175,504
bootmgr		375 KB	07/16/2016 12:37:12.0 -6	07/16/2016 05:41:53.3 -6	01/03/2017 20:05:...	SHRA	6,274,560
$Bitmap		1.9 MB	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:...	SH	6,287,624
$MFT		264 MB	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:22.8 -6	01/03/2017 20:05:...	SH	6,291,456
BOOTNXT		1 B	07/16/2016 12:37:13.7 -6	07/16/2016 05:41:53.3 -6	01/03/2017 20:05:...	SHA	6,329,436
swapfile.sys	sys	256 MB	01/03/2017 20:09:39.4 -6	03/29/2018 21:26:06.9 -6	03/29/2018 21:26:...	SHA	15,686,544
pagefile.sys	sys	1.3 GB	01/03/2017 20:09:39.4 -6	03/29/2018 21:26:06.8 -6	03/29/2018 21:26:...	SHA	15,882,880
msdia80.dll	dll	884 KB	12/02/2006 01:37:14.0 -6	12/02/2006 01:37:14.0 -6	01/06/2017 12:11:...	A	29,319,464
Free space (net)		31.2 GB					
Idle space							
Misc non-resident attributes		40.0 KB					21,495,480

Fig 18: Opening image file in WinHex (Shows all folders, system files, and other things such as free/idle space)



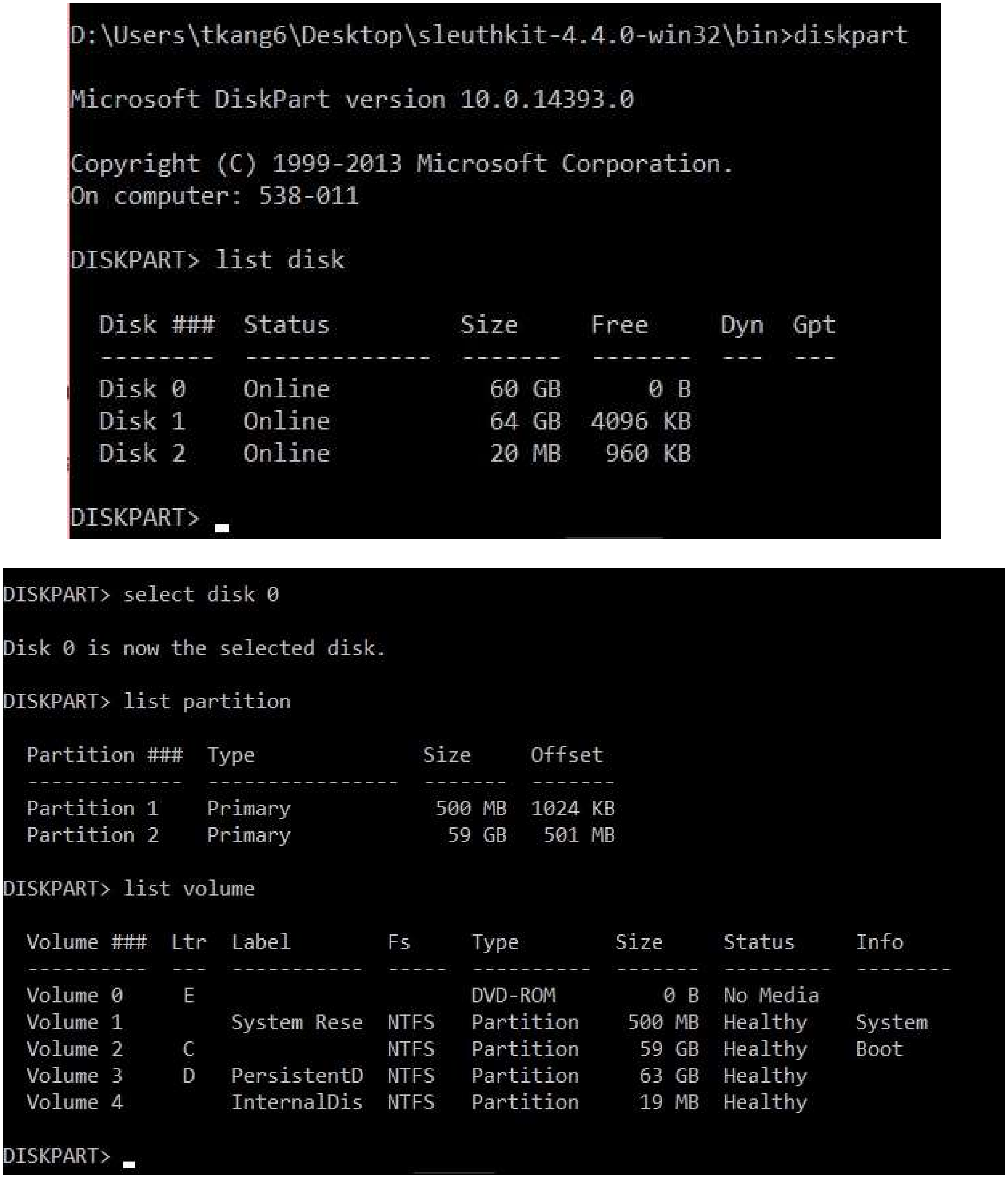
```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000000000  EB 52 90 4E 54 46 53 20  20 20 20 00 02 08 00 00  ëR NTFS
000000010  00 00 00 00 00 F8 00 00  3F 00 FF 00 00 A8 0F 00       ø  ? ÿ  ¨
000000020  00 00 00 00 80 00 80 00  FF 4F 70 07 00 00 00 00      € € ÿOp
000000030  00 00 0C 00 00 00 00 00  02 00 00 00 00 00 00 00
000000040  F6 00 00 00 01 00 00 00  F7 74 02 52 9C 02 52 A2  ö       ÷t Rœ R¢
000000050  00 00 00 00 FA 33 C0 8E  D0 BC 00 7C FB 68 C0 07      ú3ÀŽÐ¼ |ûhÀ
000000060  1F 1E 68 66 00 CB 88 16  0E 00 66 81 3E 03 00 4E    hf Ëˆ   f >  N
000000070  54 46 53 75 15 B4 41 BB  AA 55 CD 13 72 0C 81 FB  TFSu ´A»ªUÍ r  û
000000080  55 AA 75 06 F7 C1 01 00  75 03 E9 DD 00 1E 83 EC  Uªu ÷Á  u éÝ  ƒì
000000090  18 68 1A 00 B4 48 8A 16  0E 00 8B F4 16 1F CD 13   h  ´HŠ   ‹ô  Í
0000000A0  9F 83 C4 18 9E 58 1F 72  E1 3B 06 0B 00 75 DB A3  ŸƒÄ žX rá;   uÛ£
0000000B0  0F 00 C1 2E 0F 00 04 1E  5A 33 DB B9 00 20 2B C8    Á.    Z3Û¹  +È
0000000C0  66 FF 06 11 00 03 16 0F  00 8E C2 FF 06 16 00 E8  fÿ       ŽÂÿ   è
0000000D0  4B 00 2B C8 77 EF B8 00  BB CD 1A 66 23 C0 75 2D  K +Èwï¸ »Í f#Àu-
0000000E0  66 81 FB 54 43 50 41 75  24 81 F9 02 01 72 1E 16  f ûTCPAu$ ù  r
0000000F0  68 07 BB 16 68 52 11 16  68 09 00 66 53 66 53 66  h » hR  h  fSfSf
000000100  55 16 16 16 68 B8 01 66  61 0E 07 CD 1A 33 C0 BF  U   h¸ fa  Í 3À¿
000000110  0A 13 B9 F6 0C FC F3 AA  E9 FE 01 90 90 66 60 1E    ¹ö üóªéþ    f`
000000120  06 66 A1 11 00 66 03 06  1C 00 1E 66 68 00 00 00   f¡  f      fh
000000130  00 66 50 06 53 68 01 00  68 10 00 B4 42 8A 16 0E   fP Sh  h  ´BŠ
000000140  00 16 1F 8B F4 CD 13 66  59 5B 5A 66 59 66 59 1F     ‹ôÍ fY[ZfYfY
000000150  0F 82 16 00 66 FF 06 11  00 03 16 0F 00 8E C2 FF   ‚  fÿ        ŽÂÿ
000000160  0E 16 00 75 BC 07 1F 66  61 C3 A1 F6 01 E8 09 00     u¼  faÃ¡ö è
000000170  A1 FA 01 E8 03 00 F4 EB  FD 8B F0 AC 3C 00 74 09  ¡ú è  ôëý‹ð¬< t
000000180  B4 0E BB 07 00 CD 10 EB  F2 C3 0D 0A 41 20 64 69  ´ »  Í ëòÃ  A di
000000190  73 6B 20 72 65 61 64 20  65 72 72 6F 72 20 6F 63  sk read error oc
0000001A0  63 75 72 72 65 64 00 0D  0A 42 4F 4F 54 4D 47 52  curred   BOOTMGR
```

Fig 19: Hex and ASCII values in WinHex



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000000000 EB 52 90 4E 54 46 53 20  20 20 20 00 02 08 00 00 ëR NTFS
000000010 00 00 00 00 00 F8 00 00  3F 00 FF 00 00 A8 0F 00      ø  ? ÿ   ¨
000000020 00 00 00 00 80 00 80 00  FF 4F 70 07 00 00 00 00     € € ÿOp
000000030 00 00 0C 00 00 00 00 00  02 00 00 00 00 00 00 00
000000040 F6 00 00 00 01 00 00 00  F7 74 02 52 9C 02 52 A2 ö       ÷t Rœ R¢
000000050 00 00 00 00 FA 33 C0 8E  D0 BC 00 7C FB 68 C0 07     ú3ÀŽÐ¼ |ûhÀ
000000060 1F 1E 68 66 00 CB 88 16  0E 00 66 81 3E 03 00 4E   hf Ëˆ   f >  N
000000070 54 46 53 75 15 B4 41 BB  AA 55 CD 13 72 0C 81 FB TFSu ´A»ªUÍ r  û
000000080 55 AA 75 06 F7 C1 01 00  75 03 E9 DD 00 1E 83 EC Uªu ÷Á  u éÝ  ƒì
000000090 18 68 1A 00 B4 48 8A 16  0E 00 8B F4 16 1F CD 13  h  ´HŠ   ‹ô  Í
0000000A0 9F 83 C4 18 9E 58 1F 72  E1 3B 06 0B 00 75 DB A3 ŸƒÄ žX rá;   uÛ£
0000000B0 0F 00 C1 2E 0F 00 04 1E  5A 33 DB B9 00 20 2B C8   Á.    Z3Û¹  +È
0000000C0 66 FF 06 11 00 03 16 0F  00 8E C2 FF 06 16 00 E8 fÿ       ŽÂÿ   è
0000000D0 4B 00 2B C8 77 EF B8 00  BB CD 1A 66 23 C0 75 2D K +Èwï¸ »Í f#Àu-
0000000E0 66 81 FB 54 43 50 41 75  24 81 F9 02 01 72 1E 16 f ûTCPAu$ ù  r
0000000F0 68 07 BB 16 68 52 11 16  68 09 00 66 53 66 53 66 h » hR  h  fSfSf
000000100 55 16 16 16 68 B8 01 66  61 0E 07 CD 1A 33 C0 BF U   h¸ fa  Í 3À¿
000000110 0A 13 B9 F6 0C FC F3 AA  E9 FE 01 90 90 66 60 1E   ¹ö üóªéþ   f`
000000120 06 66 A1 11 00 66 03 06  1C 00 1E 66 68 00 00 00  f¡  f     fh
000000130 00 66 50 06 53 68 01 00  68 10 00 B4 42 8A 16 0E  fP Sh  h  ´BŠ
000000140 00 16 1F 8B F4 CD 13 66  59 5B 5A 66 59 66 59 1F    ‹ôÍ fY[ZfYfY
000000150 0F 82 16 00 66 FF 06 11  00 03 16 0F 00 8E C2 FF  ‚  fÿ       ŽÂÿ
000000160 0E 16 00 75 BC 07 1F 66  61 C3 A1 F6 01 E8 09 00    u¼  faÃ¡ö è
000000170 A1 FA 01 E8 03 00 F4 EB  FD 8B F0 AC 3C 00 74 09 ¡ú è  ôëý‹ð¬< t
000000180 B4 0E BB 07 00 CD 10 EB  F2 C3 0D 0A 41 20 64 69 ´ »  Í ëòÃ  A di
000000190 73 6B 20 72 65 61 64 20  65 72 72 6F 72 20 6F 63 sk read error oc
0000001A0 63 75 72 72 65 64 00 0D  0A 42 4F 4F 54 4D 47 52 curred   BOOTMGR
0000001B0 20 69 73 20 63 6F 6D 70  72 65 73 73 65 64 00 0D  is compressed
0000001C0 0A 50 72 65 73 73 20 43  74 72 6C 2B 41 6C 74 2B  Press Ctrl+Alt+
0000001D0 44 65 6C 20 74 6F 20 72  65 73 74 61 72 74 0D 0A Del to restart
0000001E0 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001F0 00 00 00 00 00 00 8A 01  A7 01 BF 01 00 00 55 AA       Š § ¿  Uª
```

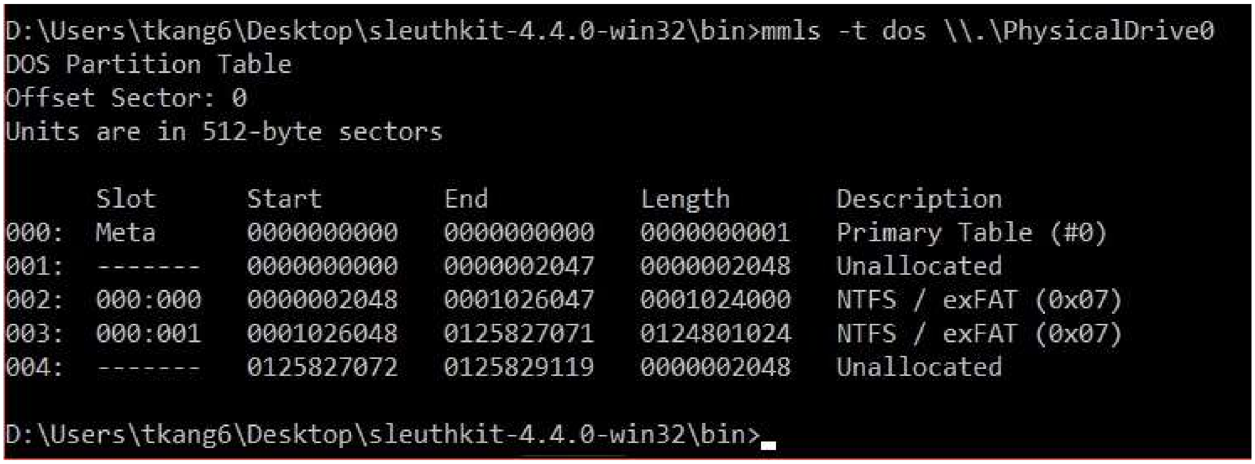
Fig 20: PBS Format
Jump instruction is highlighted in red, OEM ID is highlighted in blue, BIOS parameter block (BPB) is highlighted in purple, extended PBP is highlighted in black, bootstrap code is highlighted in green, end of sector marker (55AA) is highlighted in gray. Partition table starts from 1BE and ends at 1FE which is right before the sector marker.



```
D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>diskpart

Microsoft DiskPart version 10.0.14393.0

Copyright (C) 1999-2013 Microsoft Corporation.
On computer: 538-011

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           60 GB      0 B
  Disk 1    Online           64 GB  4096 KB
  Disk 2    Online           20 MB   960 KB

DISKPART>
```

```
DISKPART> select disk 0

Disk 0 is now the selected disk.

DISKPART> list partition

  Partition ###  Type              Size     Offset
  -------------  ----------------  -------  -------
  Partition 1    Primary            500 MB  1024 KB
  Partition 2    Primary             59 GB   501 MB

DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     E                       DVD-ROM         0 B  No Media
  Volume 1         System Rese  NTFS   Partition    500 MB  Healthy    System
  Volume 2     C                NTFS   Partition     59 GB  Healthy    Boot
  Volume 3     D   PersistentD  NTFS   Partition     63 GB  Healthy
  Volume 4         InternalDis  NTFS   Partition     19 MB  Healthy

DISKPART>
```

Fig 21: Using diskpart to find out about C: Drive



```
D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>mmls -t dos \\.\PhysicalDrive0
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0001026047   0001024000   NTFS / exFAT (0x07)
003:  000:001   0001026048   0125827071   0124801024   NTFS / exFAT (0x07)
004:  -------   0125827072   0125829119   0000002048   Unallocated

D:\Users\tkang6\Desktop\sleuthkit-4.4.0-win32\bin>
```

Fig 22: After running “mmls -t dos \\.\PhysicalDrive0” → listing partition table content

	Starting sector numbers	Size in hex	Size in decimal
The entire partition	0	F00000200	64,424,509,952
The PBS	0	200	512
The partition table	2048	EFFF00000	64,423,460,864

Fig 23: Table displaying information for NTFS partition