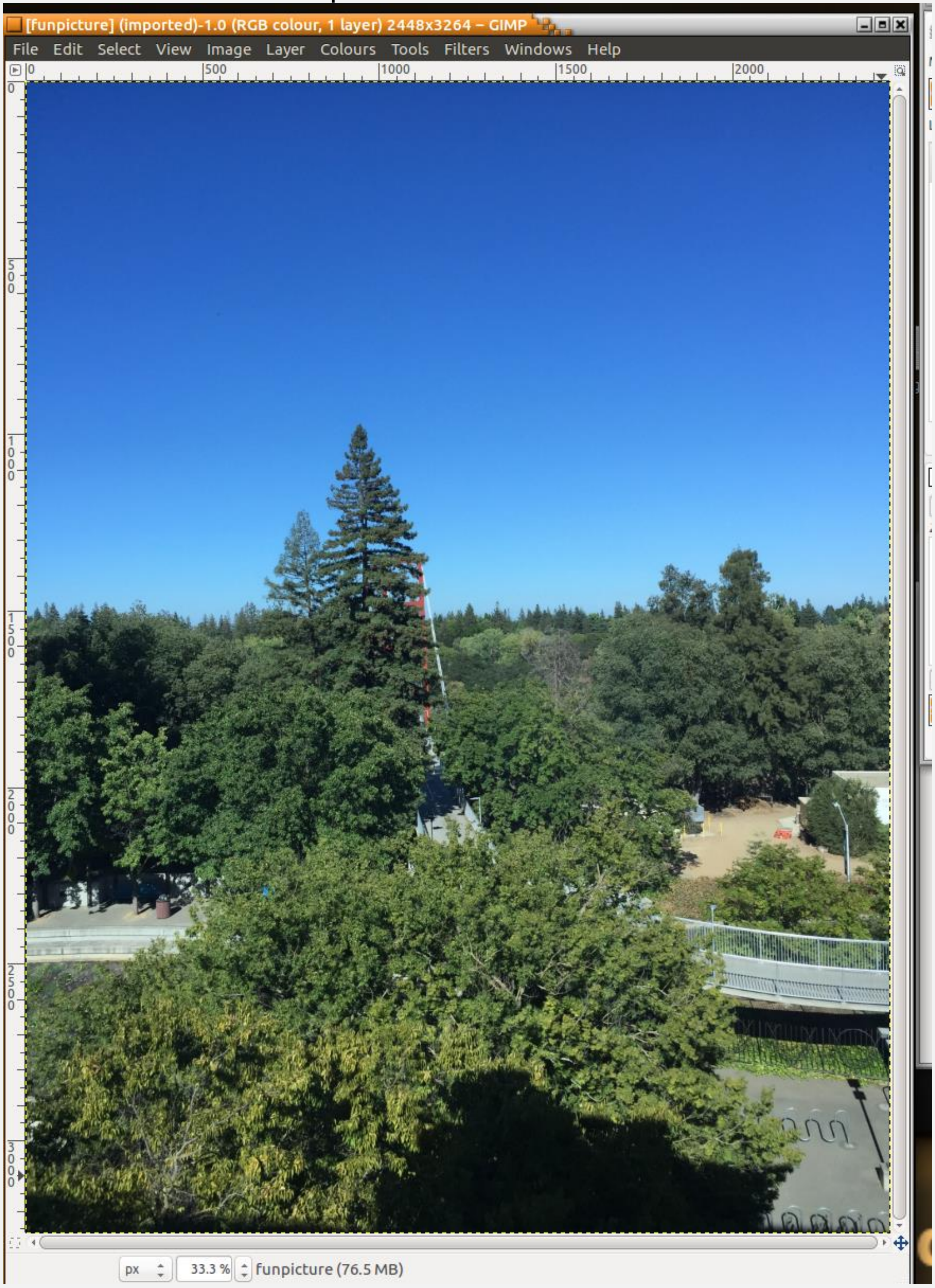
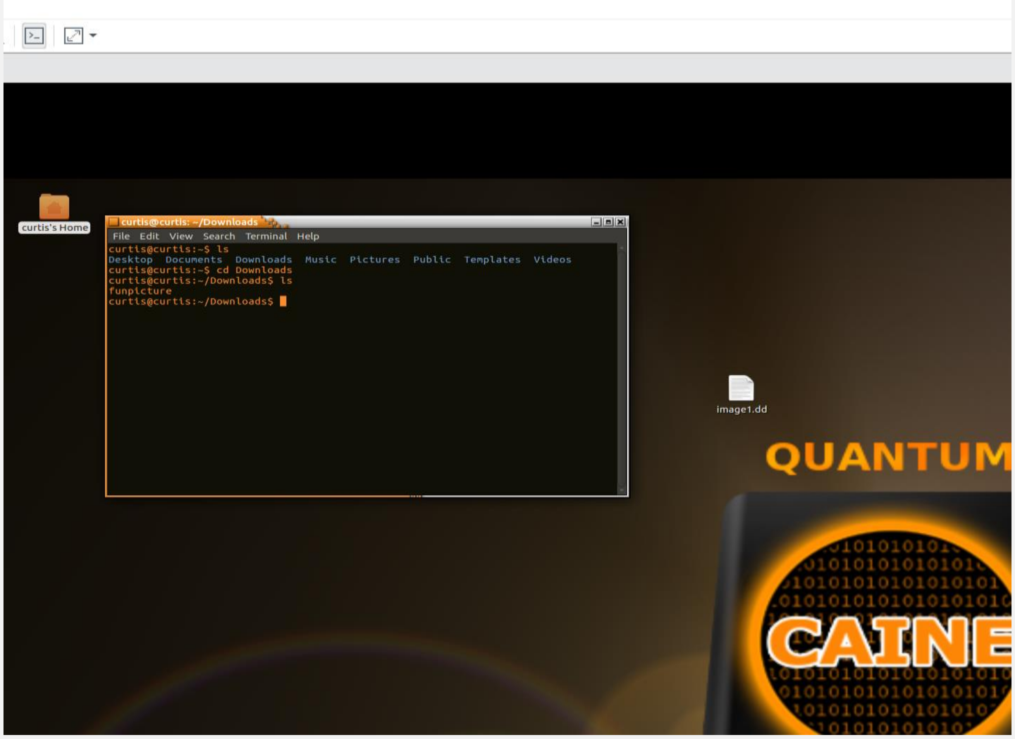
CSC 153 – Hands on Exercise 6

Part 1

1.Download the file “funpicture” from Canvas onto a Linux machine

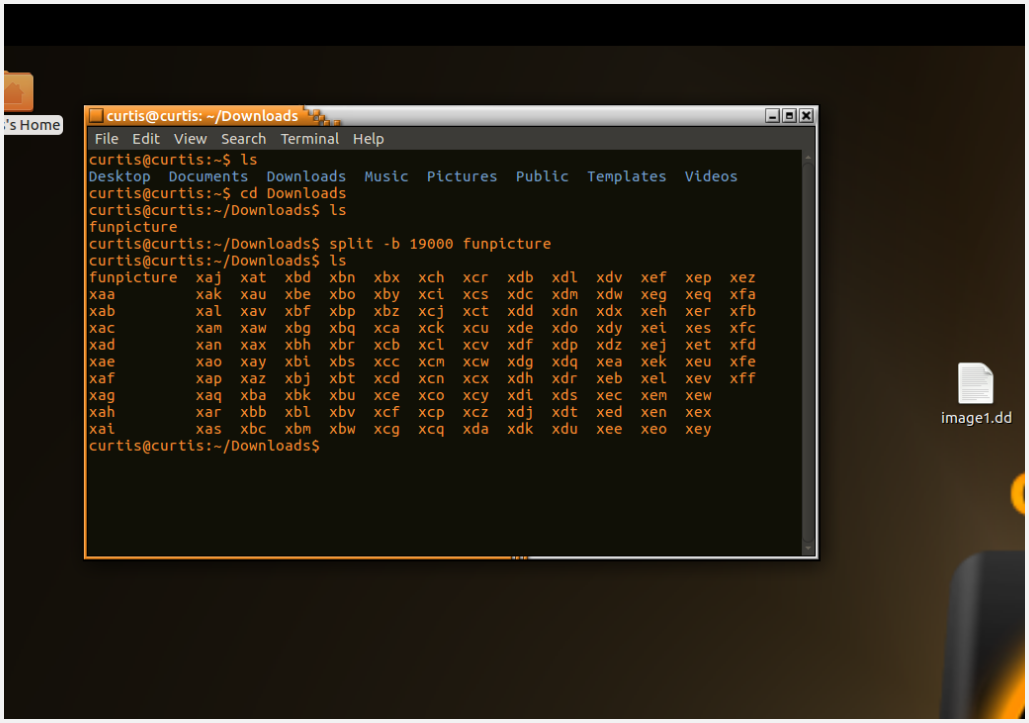

[funpicture] (imported)-1.0 (RGB colour, 1 layer) 2448x3264 – GIMP
File Edit Select View Image Layer Colours Tools Filters Windows Help
0
500
1000
1500
2000
500
1000
1500
2000
2500
3000
px
33.3 %
funpicture (76.5 MB)

2.Open terminal in Linux and change to the directory that contains funpicture.


curtis's Home
curtis@curtis: ~/Downloads
File Edit View Search Terminal Help
image1.dd
QUANTUM
CAINE

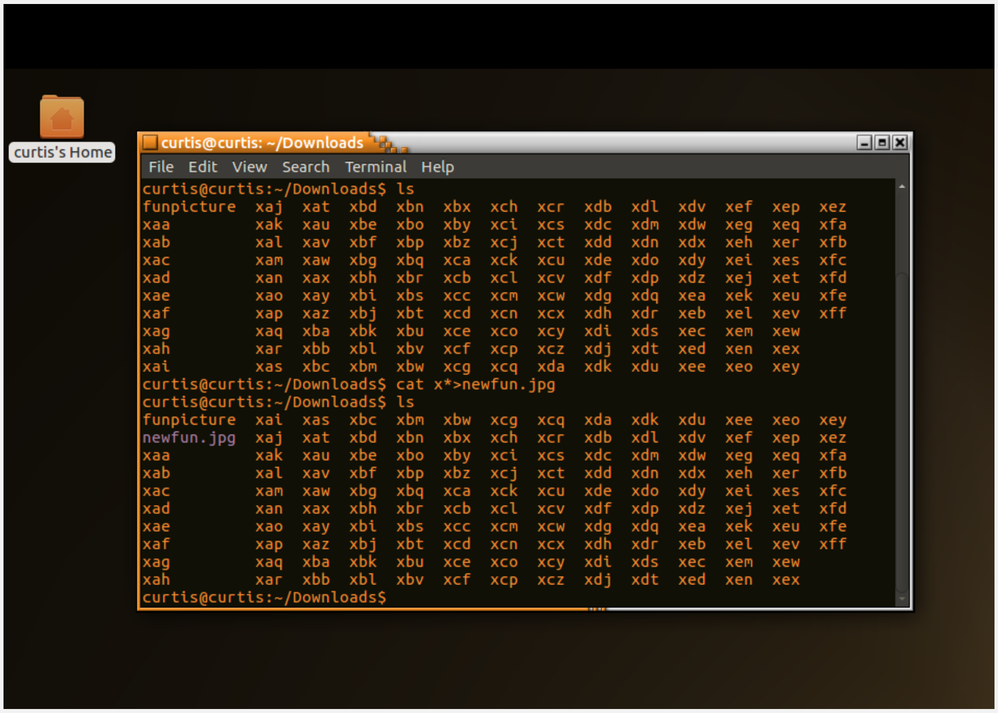
```
curtis@curtis:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
curtis@curtis:~$ cd Downloads
curtis@curtis:~/Downloads$ ls
funpicture
curtis@curtis:~/Downloads$ 
```

3.Split the file “funpicture” by typing command:split –b 19000 funpicture
4.Type command ls to see the file pieces.


's Home
curtis@curtis: ~/Downloads
File Edit View Search Terminal Help
image1.dd

```
curtis@curtis:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
curtis@curtis:~$ cd Downloads
curtis@curtis:~/Downloads$ ls
funpicture
curtis@curtis:~/Downloads$ split -b 19000 funpicture
curtis@curtis:~/Downloads$ ls
funpicture  xaj  xat  xbd  xbn  xbx  xch  xcr  xdb  xdl  xdv  xef  xep  xez
xaa         xak  xau  xbe  xbo  xby  xci  xcs  xdc  xdm  xdw  xeg  xeq  xfa
xab         xal  xav  xbf  xbp  xbz  xcj  xct  xdd  xdn  xdx  xeh  xer  xfb
xac         xam  xaw  xbg  xbq  xca  xck  xcu  xde  xdo  xdy  xei  xes  xfc
xad         xan  xax  xbh  xbr  xcb  xcl  xcv  xdf  xdp  xdz  xej  xet  xfd
xae         xao  xay  xbi  xbs  xcc  xcm  xcw  xdg  xdq  xea  xek  xeu  xfe
xaf         xap  xaz  xbj  xbt  xcd  xcn  xcx  xdh  xdr  xeb  xel  xev  xff
xag         xaq  xba  xbk  xbu  xce  xco  xcy  xdi  xds  xec  xem  xew
xah         xar  xbb  xbl  xbv  xcf  xcp  xcz  xdj  xdt  xed  xen  xex
xai         xas  xbc  xbm  xbw  xcg  xcq  xda  xdk  xdu  xee  xeo  xey
curtis@curtis:~/Downloads$
```

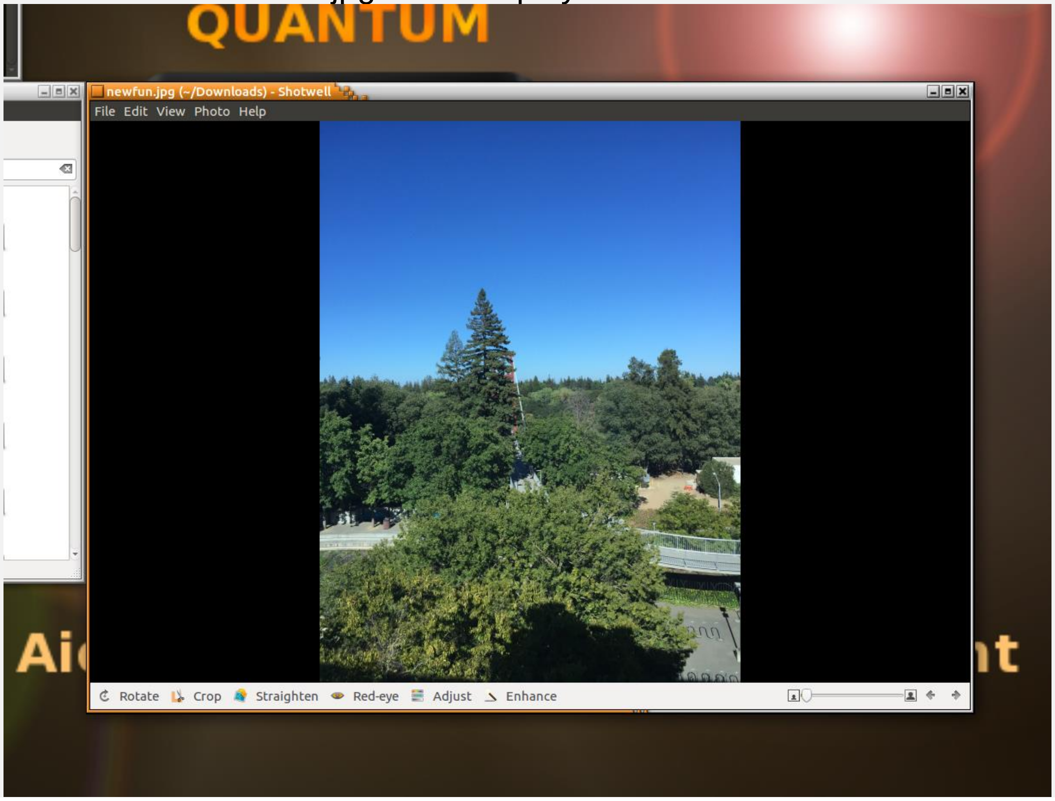
5/6. you can combine the steps 5-6 into one step by tying command:cat x*>newfun.jpg



curtis's Home
curtis@curtis: ~/Downloads
File Edit View Search Terminal Help

```
curtis@curtis:~/Downloads$ ls
funpicture  xaj  xat  xbd  xbn  xbx  xch  xcr  xdb  xdl  xdv  xef  xep  xez
xaa         xak  xau  xbe  xbo  xby  xci  xcs  xdc  xdm  xdw  xeg  xeq  xfa
xab         xal  xav  xbf  xbp  xbz  xcj  xct  xdd  xdn  xdx  xeh  xer  xfb
xac         xam  xaw  xbg  xbq  xca  xck  xcu  xde  xdo  xdy  xei  xes  xfc
xad         xan  xax  xbh  xbr  xcb  xcl  xcv  xdf  xdp  xdz  xej  xet  xfd
xae         xao  xay  xbi  xbs  xcc  xcm  xcw  xdg  xdq  xea  xek  xeu  xfe
xaf         xap  xaz  xbj  xbt  xcd  xcn  xcx  xdh  xdr  xeb  xel  xev  xff
xag         xaq  xba  xbk  xbu  xce  xco  xcy  xdi  xds  xec  xem  xew
xah         xar  xbb  xbl  xbv  xcf  xcp  xcz  xdj  xdt  xed  xen  xex
xai         xas  xbc  xbm  xbw  xcg  xcq  xda  xdk  xdu  xee  xeo  xey
curtis@curtis:~/Downloads$ cat x*>newfun.jpg
curtis@curtis:~/Downloads$ ls
funpicture  xai  xas  xbc  xbm  xbw  xcg  xcq  xda  xdk  xdu  xee  xeo  xey
newfun.jpg  xaj  xat  xbd  xbn  xbx  xch  xcr  xdb  xdl  xdv  xef  xep  xez
xaa         xak  xau  xbe  xbo  xby  xci  xcs  xdc  xdm  xdw  xeg  xeq  xfa
xab         xal  xav  xbf  xbp  xbz  xcj  xct  xdd  xdn  xdx  xeh  xer  xfb
xac         xam  xaw  xbg  xbq  xca  xck  xcu  xde  xdo  xdy  xei  xes  xfc
xad         xan  xax  xbh  xbr  xcb  xcl  xcv  xdf  xdp  xdz  xej  xet  xfd
xae         xao  xay  xbi  xbs  xcc  xcm  xcw  xdg  xdq  xea  xek  xeu  xfe
xaf         xap  xaz  xbj  xbt  xcd  xcn  xcx  xdh  xdr  xeb  xel  xev  xff
xag         xaq  xba  xbk  xbu  xce  xco  xcy  xdi  xds  xec  xem  xew
xah         xar  xbb  xbl  xbv  xcf  xcp  xcz  xdj  xdt  xed  xen  xex
curtis@curtis:~/Downloads$
```

7.Click on the newfun.jpg file to display it.

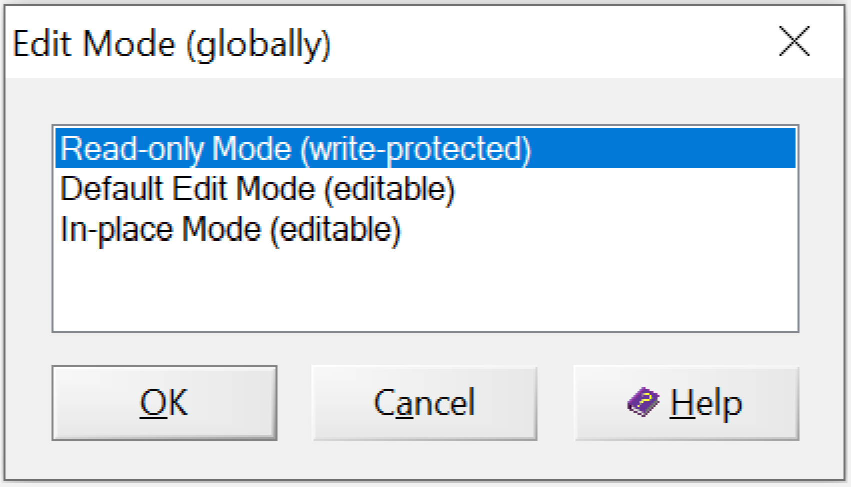


QUANTUM
newfun.jpg (~/Downloads) - Shotwell
File Edit View Photo Help
Rotate
Crop
Straighten
Red-eye
Adjust
Enhance

Part 2

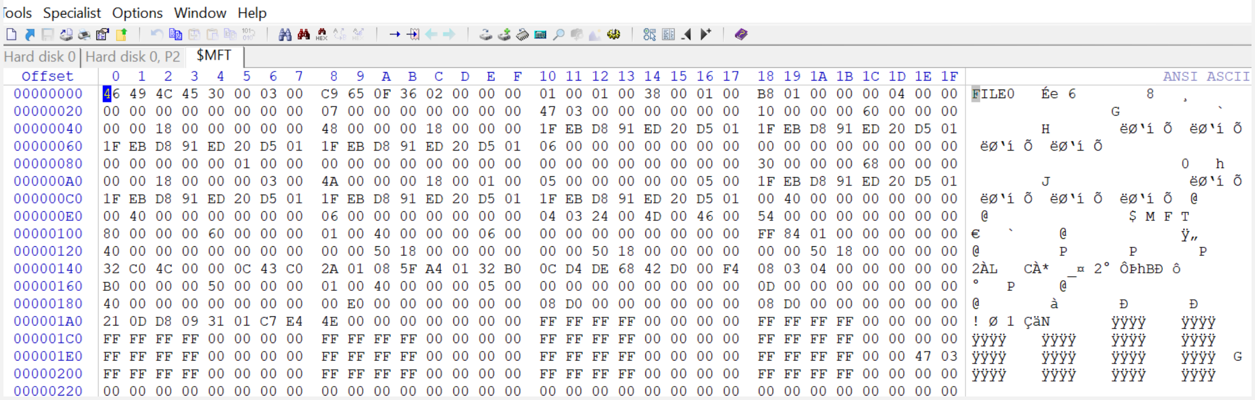
9.Downloadfile “smallsmallsmall” from Canvasand save it to a folder.This file is a PNG file, but the header has been modified by the suspect.

10.Start WinHex with the Run as administratoroption. If you see an evaluation warning message, click OK. As a safety precaution, click Options, Edit Mode from the menu. In the Select Mode dialog box, click Read-Only Mode(=write protected), as shown in Figure 2, and then click OK.


Edit Mode (globally)

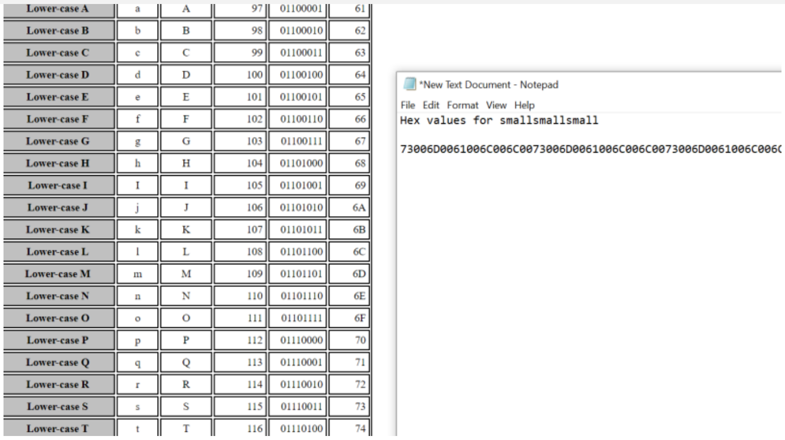
[✓ Read-only Mode (write-protected)]
Default Edit Mode (editable)
In-place Mode (editable)

12.Scroll down and find the $MFT file, right click and choose “open”. You’ll open the MFT file in a new window.



```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17  18 19 1A 1B 1C 1D 1E 1F            ANSI ASCII
00000000   46 49 4C 45 30 00 03 00  C9 65 0F 36 02 00 00 00  01 00 01 00 38 00 01 00  B8 01 00 00 00 04 00 00  FILE0   Ée 6       8   ¸
00000020   00 00 00 00 00 00 00 00  07 00 00 00 00 00 00 00  47 03 00 00 00 00 00 00  10 00 00 00 60 00 00 00                 G       `
00000040   00 00 18 00 00 00 00 00  48 00 00 00 18 00 00 00  1F EB D8 91 ED 20 D5 01  1F EB D8 91 ED 20 D5 01          H       ëØ'í Õ  ëØ'í Õ
00000060   1F EB D8 91 ED 20 D5 01  1F EB D8 91 ED 20 D5 01  06 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ëØ'í Õ  ëØ'í Õ
00000080   00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  30 00 00 00 68 00 00 00                          0   h
000000A0   00 00 18 00 00 00 03 00  4A 00 00 00 18 00 01 00  05 00 00 00 00 00 05 00  1F EB D8 91 ED 20 D5 01          J               ëØ'í Õ
000000C0   1F EB D8 91 ED 20 D5 01  1F EB D8 91 ED 20 D5 01  1F EB D8 91 ED 20 D5 01  00 40 00 00 00 00 00 00   ëØ'í Õ  ëØ'í Õ  ëØ'í Õ  @
000000E0   00 40 00 00 00 00 00 00  06 00 00 00 00 00 00 00  04 03 24 00 4D 00 46 00  54 00 00 00 00 00 00 00   @                  $ M F T
00000100   80 00 00 00 60 00 00 00  01 00 40 00 00 00 06 00  00 00 00 00 00 00 00 00  FF 84 01 00 00 00 00 00  €   `      @                ÿ„
00000120   40 00 00 00 00 00 00 00  00 00 50 18 00 00 00 00  00 00 50 18 00 00 00 00  00 00 50 18 00 00 00 00  @         P         P         P
00000140   32 C0 4C 00 00 0C 43 C0  2A 01 08 5F A4 01 32 B0  0C D4 DE 68 42 D0 00 F4  08 03 04 00 00 00 00 00  2ÀL   CÀ*  _¤ 2° ÔÞhBÐ ô
00000160   B0 00 00 00 50 00 00 00  01 00 40 00 00 00 05 00  00 00 00 00 00 00 00 00  0D 00 00 00 00 00 00 00  °   P      @
00000180   40 00 00 00 00 00 00 00  00 E0 00 00 00 00 00 00  08 D0 00 00 00 00 00 00  08 D0 00 00 00 00 00 00  @         à       Ð       Ð
000001A0   21 0D D8 09 31 01 C7 E4  4E 00 00 00 00 00 00 00  FF FF FF FF 00 00 00 00  FF FF FF FF 00 00 00 00  ! Ø 1 ÇäN       ÿÿÿÿ    ÿÿÿÿ
000001C0   FF FF FF FF 00 00 00 00  FF FF FF FF 00 00 00 00  FF FF FF FF 00 00 00 00  FF FF FF FF 00 00 00 00  ÿÿÿÿ    ÿÿÿÿ    ÿÿÿÿ    ÿÿÿÿ
000001E0   FF FF FF FF 00 00 00 00  FF FF FF FF 00 00 00 00  FF FF FF FF 00 00 00 00  FF FF FF FF 00 00 47 03  ÿÿÿÿ    ÿÿÿÿ    ÿÿÿÿ    ÿÿÿÿ  G
00000200   FF FF FF FF 00 00 00 00  FF FF FF FF 00 00 00 00  FF FF FF FF 00 00 00 00  FF FF FF FF 00 00 00 00  ÿÿÿÿ    ÿÿÿÿ    ÿÿÿÿ    ÿÿÿÿ
00000220   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

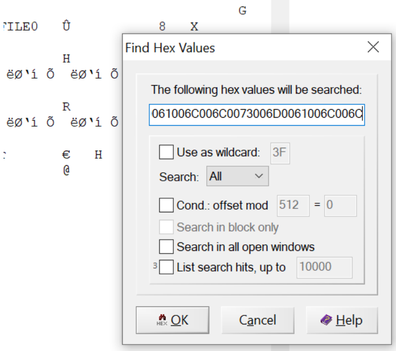
13.The next task is to find the “smallsmallsmall”file. In $MFT, the characters in a file name are usually separated by hexadecimal value “00”. For example, if the file name is “ab”, then it appearsin the $MFT as “61006200”. 61 is the hexadecimal value for letter “a”, and 62 is the hexadecimal for letter “b”. Please google search the hexadecimal values for “smallsmallsmall” and write them down. Prepare the hexadecimal values that should appear as the file name for “smallsmallsmall” file.



Lower-case A	a	A	97	01100001	61
Lower-case B	b	B	98	01100010	62
Lower-case C	c	C	99	01100011	63
Lower-case D	d	D	100	01100100	64
Lower-case E	e	E	101	01100101	65
Lower-case F	f	F	102	01100110	66
Lower-case G	g	G	103	01100111	67
Lower-case H	h	H	104	01101000	68
Lower-case I	I	I	105	01101001	69
Lower-case J	j	J	106	01101010	6A
Lower-case K	k	K	107	01101011	6B
Lower-case L	l	L	108	01101100	6C
Lower-case M	m	M	109	01101101	6D
Lower-case N	n	N	110	01101110	6E
Lower-case O	o	O	111	01101111	6F
Lower-case P	p	P	112	01110000	70
Lower-case Q	q	Q	113	01110001	71
Lower-case R	r	R	114	01110010	72
Lower-case S	s	S	115	01110011	73
Lower-case T	t	T	116	01110100	74

```
Hex values for smallsmallsmall

73006D0061006C006C0073006D0061006C006C0073006D0061006C006C
```

14.Click on Search, then Find Hex Values.



The following hex values will be searched:

061006C006C0073006D0061006C006C

☐ Use as wildcard: 3F

Search: All

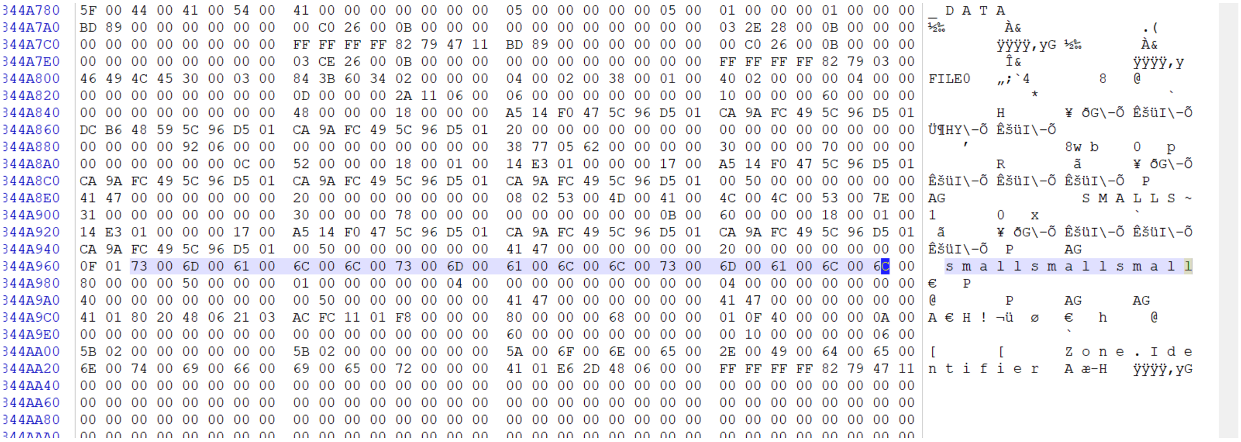
☐ Cond.: offset mod 512 = 0

☐ Search in block only

☐ Search in all open windows

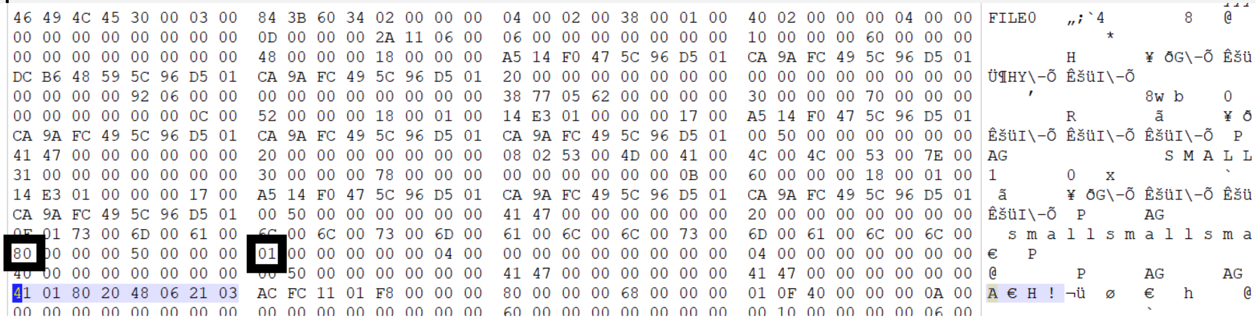
☐ List search hits, up to 10000

(file found)



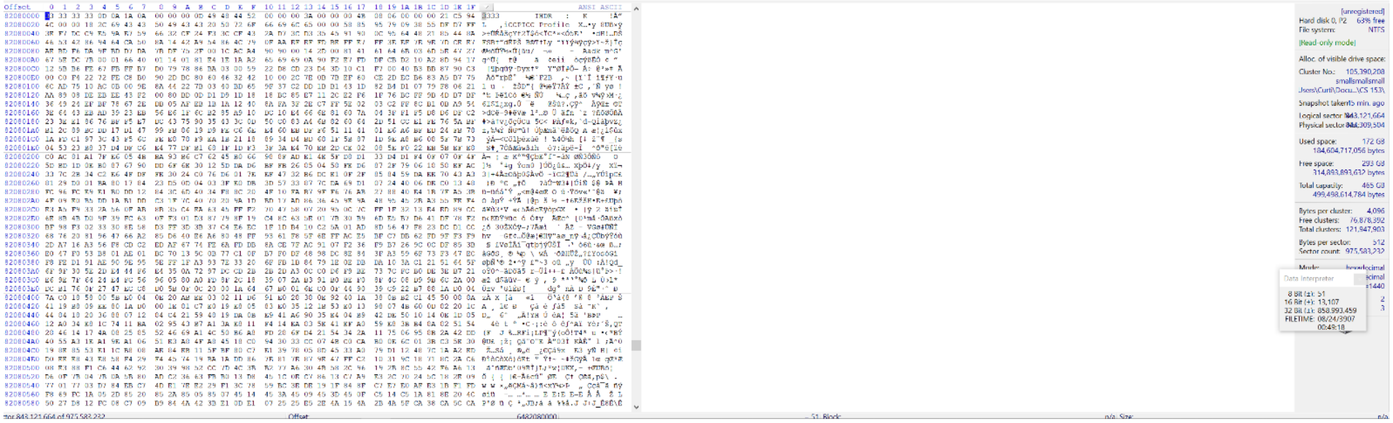
```
344A780  5F 00 44 00 41 00 54 00  41 00 00 00 00 00 00 00  05 00 00 00 00 00 05 00  01 00 00 00 01 00 00 00  _ D A T A
344A7A0  BD 89 00 00 00 00 00 00  00 C0 26 00 0B 00 00 00  00 00 00 00 00 00 00 00  03 2E 28 00 0B 00 00 00  ½‰      À&              .(
344A7C0  00 00 00 00 00 00 00 00  FF FF FF FF 82 79 47 11  BD 89 00 00 00 00 00 00  00 C0 26 00 0B 00 00 00          ÿÿÿÿ,yG ½‰      À&
344A7E0  00 00 00 00 00 00 00 00  03 CE 26 00 0B 00 00 00  00 00 00 00 00 00 00 00  FF FF FF FF 82 79 03 00           Î&             ÿÿÿÿ,y
344A800  46 49 4C 45 30 00 03 00  84 3B 60 34 02 00 00 00  04 00 02 00 38 00 01 00  40 02 00 00 00 04 00 00  FILE0   „;`4        8   @
344A820  00 00 00 00 00 00 00 00  0D 00 00 00 2A 11 06 00  06 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00              *               `
344A840  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00  A5 14 F0 47 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01          H       ¥ ðG\–Õ ÊšüI\–Õ
344A860  DC B6 48 59 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  Ü¶HY\–Õ ÊšüI\–Õ
344A880  00 00 00 00 92 06 00 00  00 00 00 00 00 00 00 00  38 77 05 62 00 00 00 00  30 00 00 00 70 00 00 00      ’           8w b    0   p
344A8A0  00 00 00 00 00 00 0C 00  52 00 00 00 18 00 01 00  14 E3 01 00 00 00 17 00  A5 14 F0 47 5C 96 D5 01          R        ã      ¥ ðG\–Õ
344A8C0  CA 9A FC 49 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  00 50 00 00 00 00 00 00  ÊšüI\–Õ ÊšüI\–Õ ÊšüI\–Õ  P
344A8E0  41 47 00 00 00 00 00 00  20 00 00 00 00 00 00 00  08 02 53 00 4D 00 41 00  4C 00 4C 00 53 00 7E 00  AG                 S M A L L S ~
344A900  31 00 00 00 00 00 00 00  30 00 00 00 78 00 00 00  00 00 00 00 00 00 0B 00  60 00 00 00 18 00 01 00  1       0   x           `
344A920  14 E3 01 00 00 00 17 00  A5 14 F0 47 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01   ã      ¥ ðG\–Õ ÊšüI\–Õ ÊšüI\–Õ
344A940  CA 9A FC 49 5C 96 D5 01  00 50 00 00 00 00 00 00  41 47 00 00 00 00 00 00  20 00 00 00 00 00 00 00  ÊšüI\–Õ  P      AG
344A960  0F 01 73 00 6D 00 61 00  6C 00 6C 00 73 00 6D 00  61 00 6C 00 6C 00 73 00  6D 00 61 00 6C 00 6C 00    s m a l l s m a l l s m a l l
344A980  80 00 00 00 50 00 00 00  01 00 00 00 00 00 04 00  00 00 00 00 00 00 00 00  04 00 00 00 00 00 00 00  €   P
344A9A0  40 00 00 00 00 00 00 00  00 50 00 00 00 00 00 00  41 47 00 00 00 00 00 00  41 47 00 00 00 00 00 00  @        P      AG      AG
344A9C0  41 01 80 20 48 06 21 03  AC FC 11 01 F8 00 00 00  80 00 00 00 68 00 00 00  01 0F 40 00 00 00 0A 00  A € H ! ¬ü  ø   €   h      @
344A9E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  60 00 00 00 00 00 00 00  00 10 00 00 00 00 06 00                  `
344AA00  5B 02 00 00 00 00 00 00  5B 02 00 00 00 00 00 00  5A 00 6F 00 6E 00 65 00  2E 00 49 00 64 00 65 00  [       [       Z o n e . I d e
344AA20  6E 00 74 00 69 00 66 00  69 00 65 00 72 00 00 00  41 01 E6 2D 48 06 00 00  FF FF FF FF 82 79 47 11  n t i f i e r   A æ-H  ÿÿÿÿ,yG
344AA40  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
344AA60  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
344AA80  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
344AAA0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

7.Please follow the same methodology as in hands-on activity 5 and lab 2 to examine this $MFT file record.You need to find out the dataruns for this file. In the demo, the first datarun information is “41 05 37 52 55 04”. This means the starting position of the first datarun is “0x 0455 52 37” and the size is “0x05”.

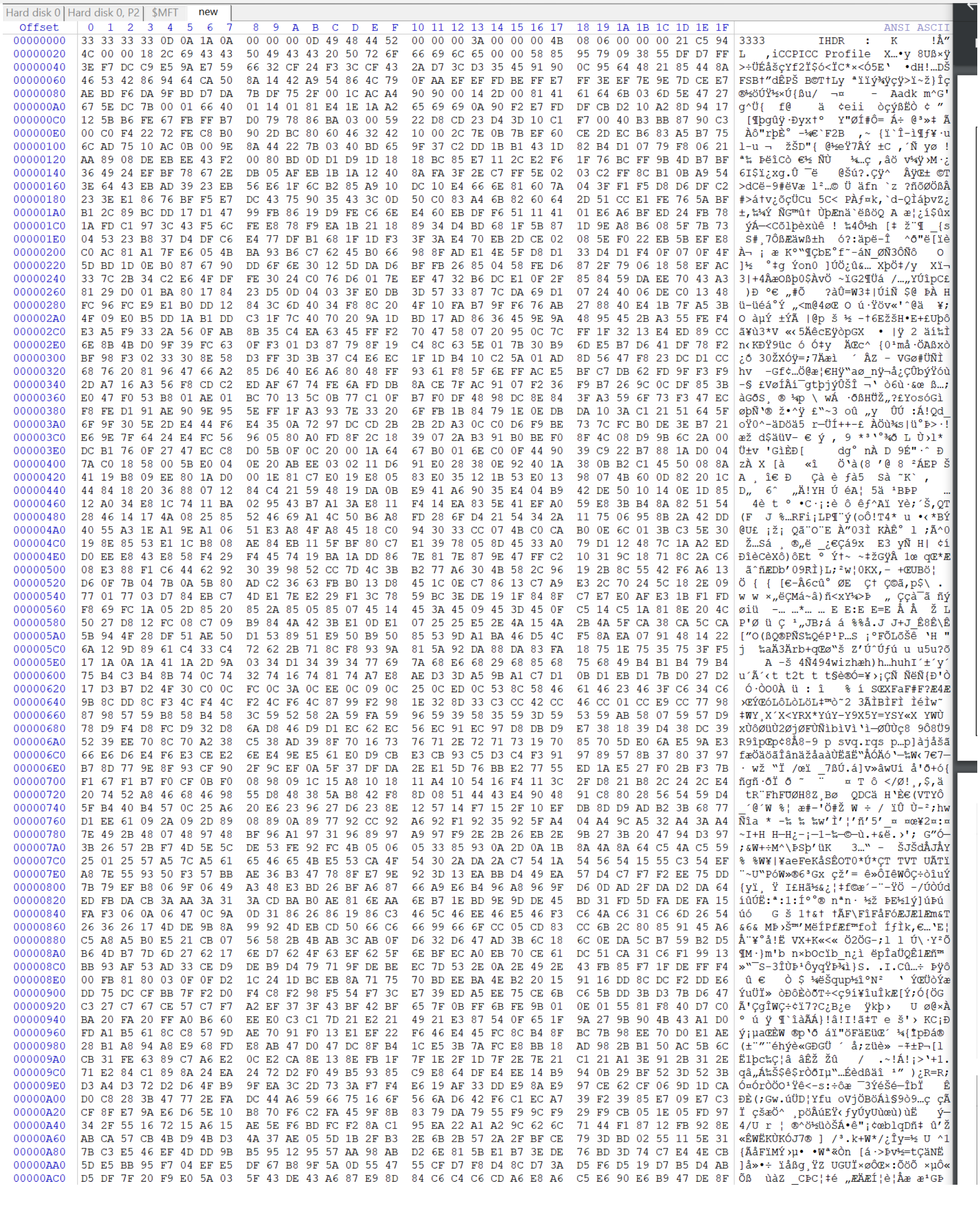


```
46 49 4C 45 30 00 03 00  84 3B 60 34 02 00 00 00  04 00 02 00 38 00 01 00  40 02 00 00 00 04 00 00  FILE0   „;`4        8   @
00 00 00 00 00 00 00 00  0D 00 00 00 2A 11 06 00  06 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00              *
00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00  A5 14 F0 47 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01          H       ¥ ðG\–Õ Êšü
DC B6 48 59 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  Ü¶HY\–Õ ÊšüI\–Õ
00 00 00 00 92 06 00 00  00 00 00 00 00 00 00 00  38 77 05 62 00 00 00 00  30 00 00 00 70 00 00 00      ’           8w b    0
00 00 00 00 00 00 0C 00  52 00 00 00 18 00 01 00  14 E3 01 00 00 00 17 00  A5 14 F0 47 5C 96 D5 01          R        ã      ¥ ð
CA 9A FC 49 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  00 50 00 00 00 00 00 00  ÊšüI\–Õ ÊšüI\–Õ ÊšüI\–Õ  P
41 47 00 00 00 00 00 00  20 00 00 00 00 00 00 00  08 02 53 00 4D 00 41 00  4C 00 4C 00 53 00 7E 00  AG                  S M A L L
31 00 00 00 00 00 00 00  30 00 00 00 78 00 00 00  00 00 00 00 00 00 0B 00  60 00 00 00 18 00 01 00  1       0   x           `
14 E3 01 00 00 00 17 00  A5 14 F0 47 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01   ã      ¥ ðG\–Õ ÊšüI\–Õ Êšü
CA 9A FC 49 5C 96 D5 01  00 50 00 00 00 00 00 00  41 47 00 00 00 00 00 00  20 00 00 00 00 00 00 00  ÊšüI\–Õ  P      AG
0E 01 73 00 6D 00 61 00  6C 00 6C 00 73 00 6D 00  61 00 6C 00 6C 00 73 00  6D 00 61 00 6C 00 6C 00    s m a l l s m a l l s m a
80 00 00 00 50 00 00 00  01 00 00 00 00 00 04 00  00 00 00 00 00 00 00 00  04 00 00 00 00 00 00 00  €   P
40 00 00 00 00 00 00 00  00 50 00 00 00 00 00 00  41 47 00 00 00 00 00 00  41 47 00 00 00 00 00 00  @        P      AG      AG
41 01 80 20 48 06 21 03  AC FC 11 01 F8 00 00 00  80 00 00 00 68 00 00 00  01 0F 40 00 00 00 0A 00  A € H ! ¬ü  ø   €   h      @
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  60 00 00 00 00 00 00 00  00 10 00 00 00 00 06 00                  `
```

The data run for this file begins at 6482080000

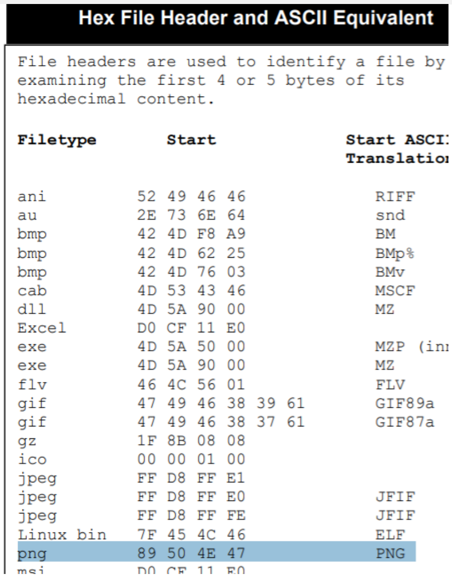


23.Go back to the beginning of the file again using go to offset. Click on the first byte of the file and drag it until the offset is “5000” (you need to replace the offset with your own number), which is the size of the first datarun. Right click and choose Edit, then choose Copy Block, then choose Into New File. Type in the file name as “ new” and click on Save.



```
Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17  18 19 1A 1B 1C 1D 1E 1F  ANSI ASCII
00000000  33 33 33 33 0D 0A 1A 0A  00 00 00 0D 49 48 44 52  00 00 00 3A 00 00 00 4B  08 06 00 00 00 21 C5 94  3333        IHDR   :   K     !Å”
00000020  4C 00 00 18 2C 69 43 43  50 49 43 43 20 50 72 6F  66 69 6C 65 00 00 58 85  95 79 09 38 55 DF D7 FF  L   ,iCCPICC Profile  X…•y 8UB×ÿ
00000040  3E F7 DC C9 E5 9A E7 59  66 32 CF 24 F3 3C CF 43  2A D7 3C D3 35 45 91 90  0C 95 64 48 21 85 44 8A  >÷ÜÉåšçYf2Ï$ó<ÏC*×<Ó5E‘  •dH!…DŠ
00000060  46 53 42 86 94 64 CA 50  8A 14 42 A9 54 86 4C 79  0F AA EF EF FD BE FF E7  FF 3E EF 7E 9E 7D CE E7  FSB†”dÊPŠ B©T†Ly ªïïý¾ÿçÿ>ï~ž}Îç
00000080  AE BD F6 DA 9F BD D7 DA  7B DF 75 2F 00 1C AC A4  90 90 00 14 2D 00 81 41  61 64 6B 03 6D 5E 47 27  ®½öÚŸ½×Ú{ßu/  ¬¤    -  Aadk m^G'
000000A0  67 5E DC 7B 00 01 66 40  01 14 01 81 E4 1E 1A A2  65 69 69 0A 90 F2 E7 FD  DF CB D2 10 A2 8D 94 17  g^Ü{  f@    ä  ¢eii  òçýßËÒ ¢ ”
000000C0  12 5B B6 FE 67 FB FF B7  D0 79 78 86 BA 03 00 59  22 D8 CD 23 D4 3D 10 C1  F7 00 40 B3 BB 87 90 C3   [¶þgûÿ·Ðyx†º  Y"ØÍ#Ô= Á÷ @³»‡ Ã
000000E0  00 C0 F4 22 72 FE C8 B0  90 2D BC 80 60 46 32 42  10 00 2C 7E 0B 7B EF 60  CE 2D EC B6 83 A5 B7 75   Àô"rþÈ° -¼€`F2B  ,~ {ï`Î-ì¶ƒ¥·u
00000100  6C AD 75 10 AC 0B 00 9E  8A 44 22 7B 03 40 BD 65  9F 37 C2 DD 1B B1 43 1D  82 B4 D1 07 79 F8 06 21  l-u ¬  žŠD"{ @½eŸ7ÂÝ ±C ‚´Ñ yø !
00000120  AA 89 08 DE EB EE 43 F2  00 80 BD 0D D1 D9 1D 18  18 BC 85 E7 11 2C E2 F6  1F 76 BC FF 9B 4D B7 BF  ª‰ ÞëîCò €½ ÑÙ   ¼…ç ,âö v¼ÿ›M·¿
00000140  36 49 24 EF BF 78 67 2E  DB 05 AF EB 1B 1A 12 40  8A FA 3F 2E C7 FF 5E 02  03 C2 FF 8C B1 0B A9 54  6I$ï¿xg.Û ¯ë   @Šú?.Çÿ^  ÂÿŒ± ©T
00000160  3E 64 43 EB AD 39 23 EB  56 E6 1F 6C B2 85 A9 10  DC 10 E4 66 6E 81 60 7A  04 3F F1 F5 D8 D6 DF C2  >dCë-9#ëVæ l²…© Ü äfn `z ?ñõØÖßÂ
00000180  23 3E E1 86 76 BF F5 E7  DC 43 75 90 35 43 3C 0D  50 C0 83 A4 6B 82 60 64  2D 51 CC E1 FE 76 5A BF  #>á†v¿õçÜCu 5C< PÀƒ¤k‚`d-QÌáþvZ¿
000001A0  B1 2C 89 BC DD 17 D1 47  99 FB 86 19 D9 FE C6 6E  E4 60 EB DF F6 51 11 41  01 E6 A6 BF ED 24 FB 78  ±,‰¼Ý ÑG™û† ÙþÆnä`ëßöQ A æ¦¿í$ûx
000001C0  1A FD C1 97 3C 43 F5 6C  FE E8 78 F9 EA 1B 21 18  89 34 D4 BD 68 1F 5B 87  1D 9E A8 B6 08 5F 7B 73   ýÁ—<Cõlþèxùê ! ‰4Ô½h [‡ ž¨¶ _{s
000001E0  04 53 23 B8 37 D4 DF C6  E4 77 DF B1 68 1F 1D F3  3F 3A E4 70 EB 2D CE 02  08 5E F0 22 EB 5B EF E8   S#¸7ÔßÆäwß±h  ó?:äpë-Î  ^ð"ë[ïè
00000200  C0 AC 81 A1 7F E6 05 4B  BA 93 B6 C7 62 45 B0 66  98 8F AD E1 4E 5F D8 D1  33 D4 D1 F4 0F 07 0F 4F  À¬ ¡ æ Kº“¶ÇbE°f˜ áN_ØÑ3ÔÑô   O
00000220  5D BD 1D 0E B0 87 67 90  DD 6F 6E 30 12 5D DA D6  BF FB 26 85 04 58 FE D6  87 2F 79 06 18 58 EF AC  ]½  °‡g Ýon0 ]ÚÖ¿û&… XþÖ‡/y  Xï¬
00000240  33 7C 2B 34 C2 E6 4F DF  FE 30 24 C0 76 D6 01 7E  EF 47 32 B6 DC E1 0F 2F  85 84 59 DA EE 70 43 A3  3|+4ÂæOßþ0$ÀvÖ ~ïG2¶Üá /…„YÚîpC£
00000260  81 29 D0 01 BA 80 17 84  23 D5 0D 04 03 3F E0 DB  3D 57 33 87 7C DA 69 D1  07 24 40 06 DE C0 13 48   )Ð º€ „#Õ   ?àÛ=W3‡|ÚiÑ $@ ÞÀ H
00000280  FC 96 FC E9 E1 B0 DD 12  84 3C 6D 40 34 F8 8C 20  4F 10 FA B7 9F F6 76 AB  27 88 40 E4 1B 7F A5 3B  ü–üéá°Ý „<m@4øŒ O ú·Ÿöv«'ˆ@ä  ¥;
000002A0  4F 09 E0 B5 DD 1A B1 DD  C3 1F 7C 40 70 20 9A 1D  BD 17 AD 86 36 45 9E 9A  48 95 45 2B A3 55 FE F4  O àµÝ ±ÝÃ |@p š ½ †6EžšH•E+£Uþô
000002C0  E3 A5 F9 33 2A 56 0F AB  8B 35 C4 EA 63 45 FF F2  70 47 58 07 20 95 0C 7C  FF 1F 32 13 E4 ED 89 CC  ã¥ù3*V «‹5ÄêcEÿòpGX  • |ÿ 2 äí‰Ì
000002E0  6E 8B 4B D0 9F 39 FC 63  0F F3 01 D3 87 79 8F 19  C4 8C 63 5E 01 7B 30 B9  6D E5 B7 D6 41 DF 78 F2  n‹KÐŸ9üc ó Ó‡y ÄŒc^ {0¹må·ÖAßxò
00000300  BF 98 F3 02 33 30 8E 58  D3 FF 3D 3B 37 C4 E6 EC  1F 1D B4 10 C2 5A 01 AD  8D 56 47 F8 23 DC D1 CC  ¿˜ó 30ŽXÓÿ=;7Äæì  ´ ÂZ  VGø#ÜÑÌ
00000320  68 76 20 81 96 47 66 A2  85 D6 40 E6 A6 80 48 FF  93 61 F8 5F 6E FF AC E5  BF C7 DB 62 FD 9F F3 F9  hv  –Gf¢…Ö@æ¦€Hÿ“aø_nÿ¬å¿ÇÛbýŸóù
00000340  2D A7 16 A3 56 F8 CD C2  ED AF 67 74 FE 6A FD DB  8A CE 7F AC 91 07 F2 36  F9 B7 26 9C 0C DF 85 3B  -§ £VøÍÂí¯gtþjýÛŠÎ ¬‘ ò6ù·&œ ß…;
00000360  E0 47 F0 53 B8 01 AE 01  BC 70 13 5C 0B 77 C1 0F  B7 F0 DF 48 98 DC 8E 84  3F A3 59 6F 73 F3 47 EC  àGðS¸ ® ¼p \ wÁ ·ðßH˜ÜŽ„?£YosóGì
00000380  F8 FE D1 91 AE 90 9E 95  5E FF 1F A3 93 7E 33 20  6F FB 1B 84 79 1E 0E DB  DA 10 3A C1 21 51 64 5F  øþÑ‘® ž•^ÿ £“~3 oû „y  ÛÚ :Á!Qd_
000003A0  6F 9F 30 5E 2D E4 44 F6  E4 35 0A 72 97 DC CD 2B  2B 2D A3 0C C0 D6 F9 BE  73 7C FC B0 DE 3E B7 21  oŸ0^-äDöä5 r—ÜÍ++-£ ÀÖù¾s|ü°Þ>·!
000003C0  E6 9E 7F 64 24 E4 FC 56  96 05 80 A0 FD 8F 2C 18  39 07 2A B3 91 B0 BE F0  8F 4C 08 D9 9B 6C 2A 00  æž d$äüV– € ý , 9 *³‘°¾ð L Ù›l* 
000003E0  DC B1 76 0F 27 47 EC C8  D0 5B 0F 0C 20 00 1A 64  67 B0 01 6E C0 0F 44 90  39 C9 22 B7 88 1A D0 04  Ü±v 'GìÈÐ[      dg° nÀ D 9É"·ˆ Ð 
00000400  7A C0 18 58 00 5B E0 04  0E 20 AB EE 03 02 11 D6  91 E0 28 38 0E 92 40 1A  38 0B B2 C1 45 50 08 8A  zÀ X [à   «î   Ö‘à(8 ’@ 8 ²ÁEP Š
00000420  41 19 B8 09 EE 80 1A D0  00 1E 81 C7 E0 19 E8 05  83 E0 35 12 1B 53 E0 13  98 07 4B 60 0D 82 20 1C  A ¸ î€ Ð   Çà è ƒà5  Sà ˜ K` ‚ 
00000440  44 84 18 20 36 88 07 12  84 C4 21 59 48 19 DA 0B  E9 41 A6 90 35 E4 04 B9  42 DE 50 10 14 0E 1D 85  D„  6ˆ  „Ä!YH Ú éA¦ 5ä ¹BÞP    …
00000460  12 A0 34 E8 1C 74 11 BA  02 95 43 B7 A1 3A E8 11  F4 14 EA 83 5E 41 EF A0  59 E8 3B B4 8A 82 51 54    4è t º •C·¡:è ô êƒ^Aï Yè;´Š‚QT
00000480  28 46 14 17 4A 08 25 85  52 46 69 A1 4C 50 B6 A8  FD 28 6F D4 21 54 34 2A  11 75 06 95 8B 2A 42 DD  (F  J %…RFi¡LP¶¨ý(oÔ!T4* u •‹*BÝ
000004A0  40 55 A3 1E A1 9E A1 06  51 E3 A8 4F A8 45 18 C0  94 30 33 CC 07 4B C0 CA  B0 0E 6C 01 3B C3 5E 30  @U£ ¡ž¡ Qã¨O¨E À”03Ì KÀÊ° l ;Ã^0
000004C0  19 8E 85 53 E1 1C B8 08  AE 84 EB 11 5F BF 80 C7  E1 39 78 05 8D 45 33 A0  79 D1 12 48 7C 1A A2 ED   Ž…Sá ¸ ®„ë _¿€Çá9x  E3 yÑ H| ¢í
000004E0  D0 EE E8 43 E8 58 F4 29  F4 45 74 19 BA 1A DD 86  7E 81 7E 87 9E 47 FF C2  10 31 9C 18 71 8C 2A C6  ÐîèCèXô)ôEt º Ý†~ ~‡žGÿÂ 1œ qŒ*Æ
00000500  08 E3 88 F1 C6 44 62 92  30 39 98 52 CC 7D 4C 3B  B2 77 A6 30 4B 58 2C 96  19 2B 8C 55 42 F6 A6 13   ãˆñÆDb’09˜RÌ}L;²w¦0KX,– +ŒUBö¦
00000520  D6 0F 7B 04 7B 0A 5B 80  AD C2 36 63 FB B0 13 D8  45 1C 0E C7 86 13 C7 A9  E3 2C 70 24 5C 18 2E 09  Ö { { [€Â6cû° ØE  Ç† Ç©ã,p$\ . 
00000540  77 01 77 03 D7 84 EB C7  4D E1 7E E2 29 F1 3C 78  59 BC 3E DE 19 1F 84 8F  C7 E7 E0 AF E3 1B F1 FD  w w ×„ëÇMá~â)ñ<xY¼>Þ  „ Ççà¯ã ñý
00000560  F8 69 FC 1A 05 2D 85 20  85 2A 85 05 85 07 45 14  45 3A 45 09 45 3D 45 0F  C5 14 C5 1A 81 8E 20 4C  øiü  -… …*… … E E:E E=E Å Å  Ž L
00000580  50 27 D8 12 FC 08 C7 09  B9 84 4A 42 3B E1 0D E1  07 25 25 E5 2E 4A 15 4A  2B 4A 5F CA 38 CA 5C CA  P'Ø ü Ç ¹„JB;á á %%å.J J+J_Ê8Ê\Ê
000005A0  5B 94 4F 28 DF 51 AE 50  D1 53 89 51 E9 50 B9 50  85 53 9D A1 BA 46 D5 4C  F5 8A EA 07 91 48 14 22  [”O(ßQ®PÑS‰QéP¹P…S ¡ºFÕLõŠê ‘H "
000005C0  6A 12 9D 89 61 C4 33 C4  72 62 2B 71 8C F8 93 9A  81 5A 92 DA 88 DA 83 FA  18 75 1E 75 35 75 3F F5  j  ‰aÄ3Ärb+qŒø“š Z’ÚˆÚƒú u u5u?õ
000005E0  17 1A 0A 1A 41 1A 2D 9A  03 34 D1 34 39 34 77 69  7A 68 E6 68 29 68 85 68  75 68 49 B4 B1 B4 79 B4      A -š 4Ñ494wizhæh)h…huhI´±´y´
00000600  75 B4 C3 B4 8B 74 0C 74  32 74 16 74 81 74 A7 E8  AE D3 3D A5 9B A1 C7 D1  0B D1 EB D1 7B D0 27 D2  u´Ã´‹t t2t t t§è®Ó=¥›¡ÇÑ ÑëÑ{Ð'Ò
00000620  17 D3 B7 D2 4F 30 C0 0C  FC 0C 3A 0C EE 0C 09 0C  25 0C ED 0C 53 8C 58 46  61 46 23 46 3F C6 34 C6   Ó·ÒO0À ü : î   % í SŒXFaF#F?Æ4Æ
00000640  9B 8C DD 8C F3 4C F4 4C  F2 4C F6 4C 87 99 F2 98  1E 32 8D 33 C3 CC 42 CC  46 CC 01 CC E9 CC 77 98  ›ŒÝŒóLôLòLöL‡™ò˜ 2 3ÃÌBÌFÌ ÌéÌw˜
00000660  87 98 57 59 B8 58 B4 58  3C 59 52 58 2A 59 FA 59  96 59 39 58 35 59 3D 59  53 59 AB 58 07 59 57 D9  ‡˜WY¸X´X<YRX*YúY–Y9X5Y=YSY«X YWÙ
00000680  78 D9 F4 D8 FC D9 32 D8  6A D8 46 D9 D1 EC 62 EC  56 EC 91 EC 97 D8 DB D9  E7 38 18 39 D4 38 DC 39  xÙôØüÙ2ØjØFÙÑìbìVì‘ì—ØÛÙç8 9Ô8Ü9
000006A0  52 39 EE 70 8C 70 A2 38  C5 38 AD 39 8F 70 16 73  76 71 2E 72 71 73 19 70  85 70 5D E0 6A E5 9A E3  R9îpŒp¢8Å8-9 p svq.rqs p…p]àjåšã
000006C0  66 E6 D6 E4 F6 E3 CE E2  6E E4 9E E5 61 E0 D9 CB  E3 CB 93 C5 D3 C4 F3 91  97 89 57 8B 37 80 37 97  fæÖäöãÎânäžåaàÙËãË“ÅÓÄó‘—‰W‹7€7—
000006E0  B7 8D 77 9E 8F 93 CF 90  2F 9C EF 0A 5F 37 DF DA  2E E1 5D 76 BB E2 77 55  ED 1A E5 27 F0 2B F3 7B  · wž “Ï /œï _7ßÚ.á]v»âwUí å'ð+ó{
00000700  F1 67 F1 B7 F0 CF 0B F0  08 98 09 1C 15 A8 10 18  11 A4 10 54 16 F4 11 3C  2F D8 21 B8 2C 24 2C E4  ñgñ·ðÏ ð ˜   ¨   ¤ T ô </Ø!¸,$,ä
00000720  20 74 52 A8 46 68 46 98  55 D8 48 38 5A B8 42 F8  8D 08 51 44 43 E4 90 48  91 C8 80 28 56 54 59 D4   tR¨FhF˜UØH8Z¸Bø  QDCä H‘È€(VTYÔ
00000740  5F B4 40 B4 57 0C 25 A6  20 E6 23 96 27 D6 23 8E  12 57 14 F7 15 2F 10 EF  DB 8D D9 AD B2 3B 68 77  _´@´W %¦ æ#–'Ö#Ž W ÷ / ïÛ Ù-²;hw
00000760  D1 EE 61 09 2A 09 2D 89  08 89 0A 89 77 92 CC 92  A6 92 F1 92 35 92 5F A4  04 A4 9C A5 32 A4 3A A4  Ñîa * -‰ ‰ ‰w’Ì’¦’ñ’5’_¤ ¤œ¥2¤:¤
00000780  7E 49 2B 48 07 48 97 48  BF 96 A1 97 31 96 89 97  A9 97 F9 2E 2B 26 EB 2E  9B 27 3B 20 47 94 D3 97  ~I+H H—H¿–¡—1–‰—©—ù.+&ë.›'; G”Ó—
000007A0  3B 26 57 2B F7 4D 5E 5C  DE 53 FE 92 FC 4B 05 06  05 33 85 93 0A 2D 0A 1B  8A 4A 8A 64 C5 4A C5 59  ;&W+÷M^\ÞSþ’üK   3…“ - ŠJŠdÅJÅY
000007C0  25 01 25 57 A5 7C A5 61  65 46 65 4B E5 53 CA 4F  54 30 2A DA 2A C7 54 1A  54 56 54 15 55 C3 54 EF  % %W¥|¥aeFeKåSÊOT0*Ú*ÇT TVT UÃTï
000007E0  A8 7E 55 93 50 F3 57 BB  AE 36 B3 47 78 8F E7 9E  92 3D 13 EA BB D4 49 EA  57 D4 C7 F7 F2 EE 75 DD  ¨~U“PóW»®6³Gx çž’= ê»ÔIêWÔÇ÷òîuÝ
00000800  7B 79 EF B8 06 9F 06 49  A3 48 E3 BD 26 BF A6 87  66 A9 E6 B4 96 A8 96 9F  D6 0D AD 2F DA D2 DA 64  {yï¸ Ÿ I£Hã½&¿¦‡f©æ´–¨–ŸÖ /ÚÒÚd
00000820  ED FB DA CB 3A AA 3A 31  3A CD BA B0 AE 81 6E AA  6E B7 1E BD 9E 9D DE 45  BD 31 FD 5D FA DE FA 15  íûÚË:ª:1:Íº°® nªn· ½ž ÞE½1ý]úÞú 
00000840  FA F3 06 0A 06 47 0C 9A  0D 31 86 26 86 19 86 C3  46 5C 46 EE 46 E5 46 F3  C6 4A C6 31 C6 6D 26 54  úó   G š 1†&† †ÃF\FîFåFóÆJÆ1Æm&T
00000860  26 36 26 17 4D DE 9B 8A  99 92 4D EB CD 50 66 C6  66 99 66 6F CC 05 CD 83  CC 6B 2C 80 85 91 45 A6  &6& MÞ›Š™’MëÍPfÆf™foÌ ÍƒÌk,€…‘E¦
00000880  C5 A8 A5 B0 E5 21 CB 07  56 58 2B 4B AB 3C AB 0F  D6 32 D6 47 AD 3B 6C 18  6C 0E DA 5C B7 59 B2 D5  Å¨¥°å!Ë VX+K«<« Ö2ÖG-;l l Ú\·Y²Õ
000008A0  B6 4D B7 7D 6D 27 62 17  6E D7 62 4F 63 EF 62 5F  6E BF EC A0 EB 70 CE 61  DC 51 CA 31 C6 F1 99 13  ¶M·}m'b n×bOcïb_n¿ì ëpÎaÜQÊ1Æñ™ 
000008C0  BB 93 AF 53 AD 33 CE D9  DE B9 D4 79 71 9F DE BE  EC 7D 53 2E 0A 2E 49 2E  43 FB 85 F7 1F DE FF F4  »“¯S-3ÎÙÞ¹ÔyqŸÞ¾ì}S. .I.Cû…÷ Þÿô
000008E0  00 FB 81 80 03 0F 0F D2  1C 24 1D BC EB 8A 71 75  70 BD EE BA 4E B2 20 15  91 16 DD 8C DC F2 DD E6   û €   Ò $ ¼ëŠqup½îºN²  ‘ ÝŒÜòÝæ
00000900  DD 75 DC CF BB 7F F2 D0  F4 C8 F2 98 F5 54 F7 3C  E7 39 ED A5 EE 75 CE 6B  C6 5B DD 3B D3 7B D6 47  ÝuÜÏ» òÐôÈò˜õT÷<ç9í¥îuÎkÆ[Ý;Ó{ÖG
00000920  C3 27 C7 67 CE 57 C7 F7  A2 EF 37 3F 43 BF 42 BF  65 7F 0B FF 6B FE 9B 01  0E 01 55 81 F8 40 D7 C0  Ã'ÇgÎWÇ÷¢ï7?C¿B¿e  ÿkþ›   U ø@×À
00000940  BA 20 FA 20 FF A0 B6 60  EE E0 C3 C1 7D 21 E2 21  49 21 E3 87 54 0F 65 1F  9A 27 9B 90 4B 43 A1 D0  º ú ÿ ¶`îàÃÁ}!â!I!ã‡T e š'› KC¡Ð
00000960  FD A1 B5 61 8C C8 57 9D  AE 70 91 F0 13 E1 EF 22  F6 46 E4 45 FC 8C B4 8F  BC 7B 98 EE 70 D0 E1 AE  ý¡µaŒÈW ®p‘ð áï"öFäEüŒ´ ¼{˜îpÐá®
00000980  28 B1 A8 94 A8 E9 68 FD  E8 AB 47 D0 47 DC 8F B4  1C E5 3B 7A FC E8 BB 18  AD 98 2B B1 50 AC 5B 6C  (±¨”¨éhýè«GÐGÜ ´ å;züè» ˜+±P¬[l
000009A0  CB 31 FE 63 89 C7 A6 E2  0C E2 CA 8E 13 8E FB 1F  7F 1E 2F 1D 7F 2E 7E 21  C1 21 A1 3E 91 2B 31 2E  Ë1þc‰Ç¦â âÊŽ Žû   /  .~!Á!¡>‘+1.
000009C0  71 E2 84 C1 89 8A 24 EA  24 72 D2 F0 49 B5 93 85  C9 E8 64 DF E4 EE 14 B9  94 0B 29 BF 52 3D 52 3B  qâ„Á‰Š$ê$rÒðIµ“…ÉèdßäÆ ¹” )¿R=R;
000009E0  D3 A4 D3 72 D2 D6 4F B9  9F EA 3C 2D 73 3A F7 F4  E6 19 AF 33 DD E9 8A E9  97 CE 62 CF 06 9D 1D CA  Ó¤ÓrÒÖO¹Ÿê<-s:÷ôæ ¯3ÝéŠé—ÎbÏ    Ê
00000A00  D0 C8 28 3B 47 77 2E FA  DC 44 A6 59 66 75 16 6F  56 6A D6 42 F6 C1 EC A7  39 F2 39 85 E7 09 E7 C3  ÐÈ(;Gw.úÜD¦Yfu oVjÖBöÁì§9ò9…ç çÃ
00000A20  CF 8F E7 9A E6 D6 5E 10  B8 70 F6 C2 FA 45 9F 8B  83 79 DA 79 55 F9 9C F9  29 F9 CB 05 1E 05 FD 97  Ï çšæÖ^ ¸pöÂúEŸ‹ƒyÚyUùœù)ùË   ý—
00000A40  34 2F 55 16 72 15 A6 15  AE 5E F6 BD FC F2 8A C1  95 EA 22 A1 A2 9C 62 6C  71 44 F1 87 12 FB 92 8E  4/U r ¦ ®^ö½üòŠÁ•ê"¡¢œblqDñ‡ û’Ž
00000A60  AB CA 57 CB 4B D9 4B D3  4A 37 AE 05 5D 1B 2F B3  2E 6B 2B 57 2A 2F BF CE  79 3D BD 02 55 11 5E 31  «ÊWËKÙKÓJ7® ] /³.k+W*/¿Îy=½ U ^1
00000A80  7B C3 E5 46 EF 4D DD 9B  B5 95 12 95 57 AA 98 AB  D2 6E 81 5B E1 B7 3E DE  76 BD 3D 74 C7 E4 4E CB  {ÃåFïMÝ›µ• •Wª˜«Òn [á·>Þv½=tÇäNË
00000AA0  5D E5 BB 95 F7 04 EF E5  DF 67 B8 9F 5A 0D 55 47  55 CF D7 F8 D4 8C D7 3A  D5 F6 D5 19 D7 B5 D4 AB  ]å»•÷ ïåßg¸ŸZ UGUÏ×øÔŒ×:ÕöÕ ×µÔ«
00000AC0  D5 DF 7F 20 F9 E0 5A 03  5F 43 DE 43 A6 87 E9 8D  84 C6 C4 C6 CD A6 E8 A6  C5 E6 90 E6 B9 47 DE 8F  Õß  ùàZ _CÞC¦‡é „ÆÄÆÍ¦è¦Åæ æ¹GÞ 
```

24.Google search the correct header for PNG fileformat,and change the header of the new file to the correct format.



Hex File Header and ASCII Equivalent

File headers are used to identify a file by examining the first 4 or 5 bytes of its hexadecimal content.

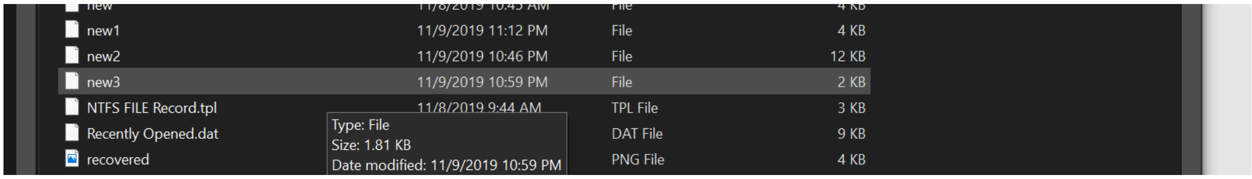
Filetype	Start	Start ASCI Translatio
ani	52 49 46 46	RIFF
au	2E 73 6E 64	snd
bmp	42 4D F8 A9	BM
bmp	42 4D 62 25	BMp%
bmp	42 4D 76 03	BMv
cab	4D 53 43 46	MSCF
dll	4D 5A 90 00	MZ
Excel	D0 CF 11 E0	
exe	4D 5A 50 00	MZP (in
exe	4D 5A 90 00	MZ
flv	46 4C 56 01	FLV
gif	47 49 46 38 39 61	GIF89a
gif	47 49 46 38 37 61	GIF87a
gz	1F 8B 08 08	
ico	00 00 01 00	
jpeg	FF D8 FF E1	
jpeg	FF D8 FF E0	JFIF
jpeg	FF D8 FF FE	JFIF
Linux bin	7F 45 4C 46	ELF
png	89 50 4E 47	PNG
msi	D0 CF 11 E0	

25.
(You may skip this step if you only have one data run.) If you have more than 1 data runs, you need to follow the same method as in Step 19-23 to copy the data in other dataruns and append that into “new” file. Pay attention to the following things:

a.The starting position for the second data run is a relative position from the starting position of the first datarun, so you should choose from “current position” when repeating step 19;

b.Instead of copying all data runs into the “new” file, a safer way is to first save the data runs in separate files, and then combine these files into one file.

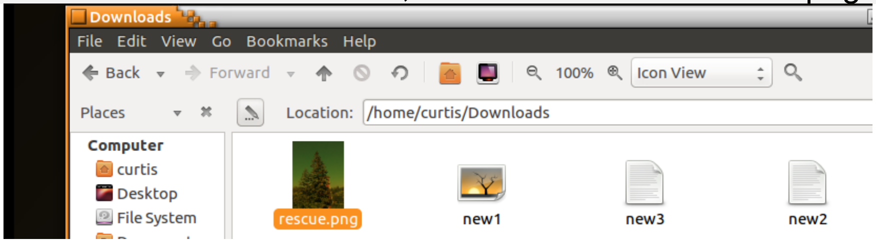
(3 files for the 3 data runs new1, new2, and new3)



new	11/8/2019 10:45 AM	File	4 KB
new1	11/9/2019 11:12 PM	File	4 KB
new2	11/9/2019 10:46 PM	File	12 KB
new3	11/9/2019 10:59 PM	File	2 KB
NTFS FILE Record.tpl	11/8/2019 9:44 AM	TPL File	3 KB
Recently Opened.dat		DAT File	9 KB
recovered		PNG File	4 KB

Type: File
Size: 1.81 KB
Date modified: 11/9/2019 10:59 PM

26.After the header is changed, click on File, and then Save As, type in “recovered” as the file name.
27.Find the “recovered” file, and add the extension of “png”.

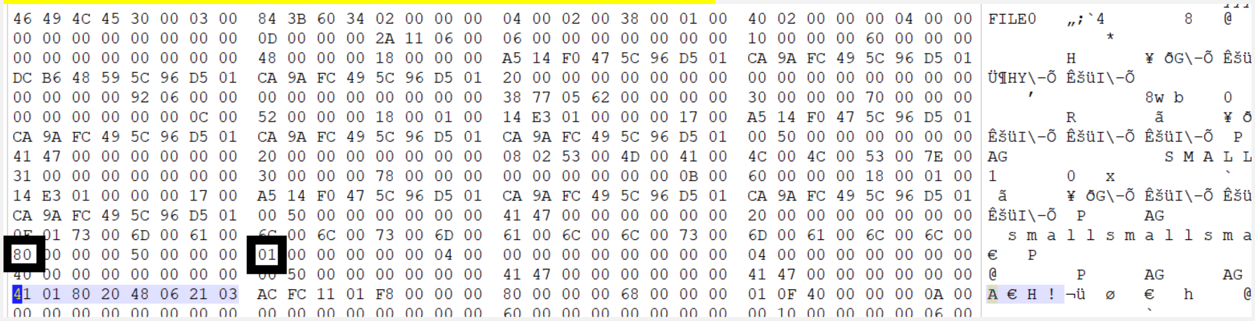


Location: /home/curtis/Downloads

Questions

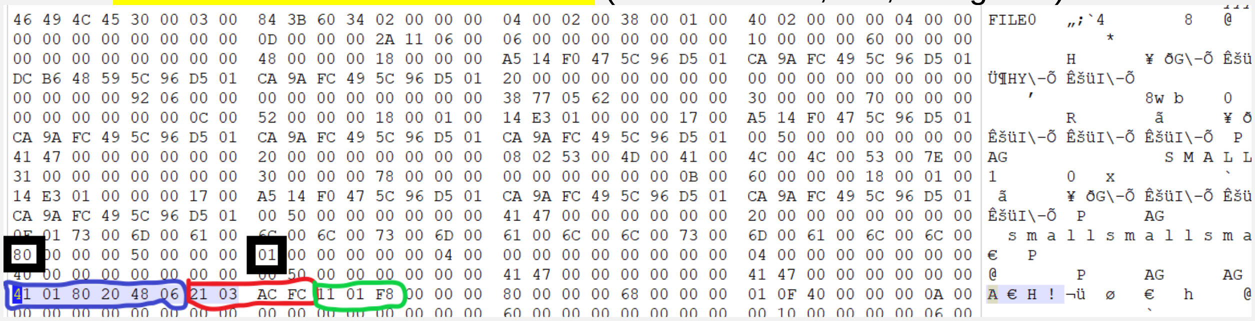
1.What the hexadecimal values did you use to search for the file “smallsmallsmall” in step 13 and 15? – 73006D0061006C006C0073006D0061006C006C0073006D0061006C006C00

2.Is the file a resident file or non-resident file? How do you know? Please take a screenshot to show the evidence. The non-resident market in attribute 80 was marked as 01 which indicates a non-resident file



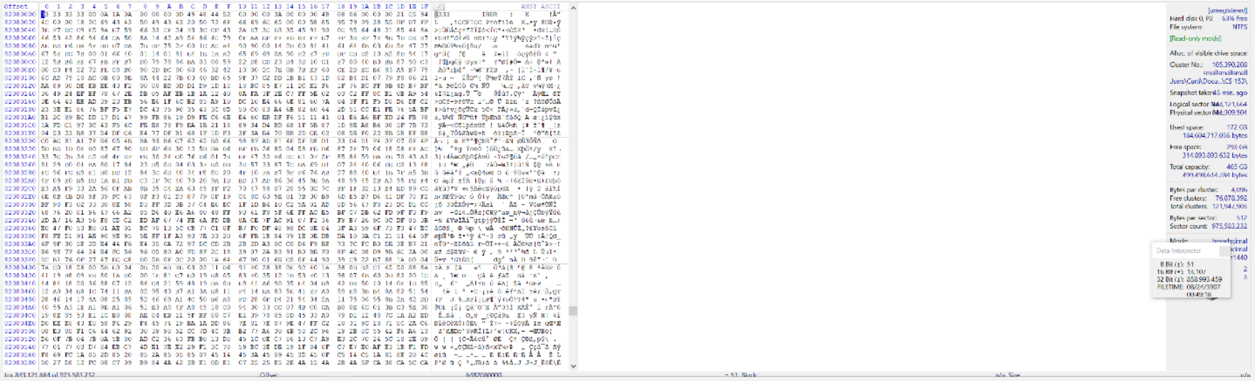
```
46 49 4C 45 30 00 03 00  84 3B 60 34 02 00 00 00  04 00 02 00 38 00 01 00  40 02 00 00 00 04 00 00  FILE0   „;`4        8  @
00 00 00 00 00 00 00 00  0D 00 00 00 2A 11 06 00  06 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00              *
00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00  A5 14 F0 47 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01          H       ¥ ðG\–Õ Êšü
DC B6 48 59 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  Ü¶HY\–Õ ÊšüI\–Õ
00 00 00 00 92 06 00 00  00 00 00 00 00 00 00 00  38 77 05 62 00 00 00 00  30 00 00 00 70 00 00 00      ’             8w b     0
00 00 00 00 00 00 0C 00  52 00 00 00 18 00 01 00  14 E3 01 00 00 00 17 00  A5 14 F0 47 5C 96 D5 01          R       ã       ¥ ð
CA 9A FC 49 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  00 50 00 00 00 00 00 00  ÊšüI\–Õ ÊšüI\–Õ ÊšüI\–Õ  P
41 47 00 00 00 00 00 00  20 00 00 00 00 00 00 00  08 02 53 00 4D 00 41 00  4C 00 4C 00 53 00 7E 00  AG              S M A L L
31 00 00 00 00 00 00 00  30 00 00 00 78 00 00 00  00 00 00 00 00 00 0B 00  60 00 00 00 18 00 01 00  1       0   x           `
14 E3 01 00 00 00 17 00  A5 14 F0 47 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01   ã      ¥ ðG\–Õ ÊšüI\–Õ Êšü
CA 9A FC 49 5C 96 D5 01  00 50 00 00 00 00 00 00  41 47 00 00 00 00 00 00  20 00 00 00 00 00 00 00  ÊšüI\–Õ  P      AG
0F 01 73 00 6D 00 61 00  6C 00 6C 00 73 00 6D 00  61 00 6C 00 6C 00 73 00  6D 00 61 00 6C 00 6C 00    s m a l l s m a l l s m a
80 00 00 00 50 00 00 00  01 00 00 00 00 00 04 00  00 00 00 00 00 00 00 00  04 00 00 00 00 00 00 00  €   P
40 00 00 00 00 00 00 00  00 50 00 00 00 00 00 00  41 47 00 00 00 00 00 00  41 47 00 00 00 00 00 00  @        P      AG      AG
41 01 80 20 48 06 21 03  AC FC 11 01 F8 00 00 00  80 00 00 00 68 00 00 00  01 0F 40 00 00 00 0A 00  A € H ! ¬ü  ø   €   h       @
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  60 00 00 00 00 00 00 00  00 10 00 00 00 00 06 00          `
```

3.How many data runs does this file has?Please take a screenshot to show the evidence. There are 3 data runs for this file (circled in blue, red, and green)



```
46 49 4C 45 30 00 03 00  84 3B 60 34 02 00 00 00  04 00 02 00 38 00 01 00  40 02 00 00 00 04 00 00  FILE0   „;`4        8  @
00 00 00 00 00 00 00 00  0D 00 00 00 2A 11 06 00  06 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00              *
00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00  A5 14 F0 47 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01          H       ¥ ðG\–Õ Êšü
DC B6 48 59 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  Ü¶HY\–Õ ÊšüI\–Õ
00 00 00 00 92 06 00 00  00 00 00 00 00 00 00 00  38 77 05 62 00 00 00 00  30 00 00 00 70 00 00 00      ’             8w b     0
00 00 00 00 00 00 0C 00  52 00 00 00 18 00 01 00  14 E3 01 00 00 00 17 00  A5 14 F0 47 5C 96 D5 01          R       ã       ¥ ð
CA 9A FC 49 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  00 50 00 00 00 00 00 00  ÊšüI\–Õ ÊšüI\–Õ ÊšüI\–Õ  P
41 47 00 00 00 00 00 00  20 00 00 00 00 00 00 00  08 02 53 00 4D 00 41 00  4C 00 4C 00 53 00 7E 00  AG              S M A L L
31 00 00 00 00 00 00 00  30 00 00 00 78 00 00 00  00 00 00 00 00 00 0B 00  60 00 00 00 18 00 01 00  1       0   x           `
14 E3 01 00 00 00 17 00  A5 14 F0 47 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01  CA 9A FC 49 5C 96 D5 01   ã      ¥ ðG\–Õ ÊšüI\–Õ Êšü
CA 9A FC 49 5C 96 D5 01  00 50 00 00 00 00 00 00  41 47 00 00 00 00 00 00  20 00 00 00 00 00 00 00  ÊšüI\–Õ  P      AG
0F 01 73 00 6D 00 61 00  6C 00 6C 00 73 00 6D 00  61 00 6C 00 6C 00 73 00  6D 00 61 00 6C 00 6C 00    s m a l l s m a l l s m a
80 00 00 00 50 00 00 00  01 00 00 00 00 00 04 00  00 00 00 00 00 00 00 00  04 00 00 00 00 00 00 00  €   P
40 00 00 00 00 00 00 00  00 50 00 00 00 00 00 00  41 47 00 00 00 00 00 00  41 47 00 00 00 00 00 00  @        P      AG      AG
41 01 80 20 48 06 21 03  AC FC 11 01 F8 00 00 00  80 00 00 00 68 00 00 00  01 0F 40 00 00 00 0A 00  A € H ! ¬ü  ø   €   h       @
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  60 00 00 00 00 00 00 00  00 10 00 00 00 00 06 00          `
```

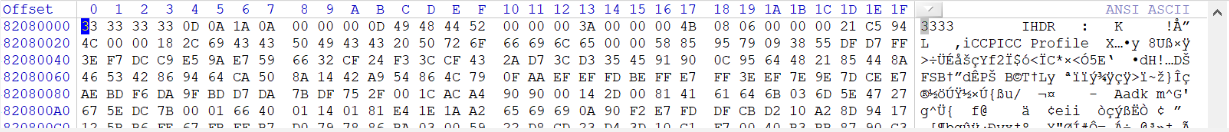
4.What is the starting position for the first data run? Please take a screenshot to show the evidence. The starting position for this data run is at offset 6482080000



```
[unregistered]
Hard disk 0, P2          63% free
File system:                 NTFS
[Read-only mode]

Alloc. of visible drive space:
Cluster No.:          105,390,208
                  smallsmallsmall
Jsers\Curti\Docu...\CS 153\
Snapshot taken      45 min. ago
Logical sector No.:   843,121,664
Physical sector No.:  843,309,504

Used space:                172 GB
           184,604,717,056 bytes
Free space:                293 GB
           314,893,893,632 bytes
Total capacity:            465 GB
           499,498,614,784 bytes

Bytes per cluster:          4,096
Free clusters:         76,878,392
Total clusters:       121,947,906
Bytes per sector:             512
Sector count:         975,583,232

Mode:                 hexadecimal

Data Interpreter
8 Bit (±):  51
16 Bit (±): 13,107
32 Bit (±): 858,993,459
FILETIME:   08/24/3907
            00:49:18

Sector 843,121,664 of 975,583,232     Offset:     6482080000
```

5.What is the size of the first data run? The size is 1 cluster, as indicated by the 01 in the second byte of the data run

6.In step 20, what is the headerof the file “smallsmallsmall” which you downloaded from Canvas?Please provide the first 4 bytes of the hexadecimal values.
Please take a screenshot to show the evidence. The header is 33 33 33 33



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17  18 19 1A 1B 1C 1D 1E 1F        ANSI ASCII
82080000  33 33 33 33 0D 0A 1A 0A  00 00 00 0D 49 48 44 52  00 00 00 3A 00 00 00 4B  08 06 00 00 00 21 C5 94  3333         IHDR   :   K      !Å”
82080020  4C 00 00 18 2C 69 43 43  50 49 43 43 20 50 72 6F  66 69 6C 65 00 00 58 85  95 79 09 38 55 DF D7 FF  L   ,iCCPICC Profile  X…•y 8Uß×ÿ
82080040  3E F7 DC C9 E5 9A E7 59  66 32 CF 24 F3 3C CF 43  2A D7 3C D3 35 45 91 90  0C 95 64 48 21 85 44 8A  >÷ÜÉåšçYf2Ï$ó<ÏC*×<Ó5E‘  •dH!…DŠ
82080060  46 53 42 86 94 64 CA 50  8A 14 42 A9 54 86 4C 79  0F AA EF EF FD BE FF E7  FF 3E EF 7E 9E 7D CE E7  FSB†”dÊPŠ B©T†Ly ªïïý¾ÿçÿ>ï~ž}Îç
82080080  AE BD F6 DA 9F BD D7 DA  7B DF 75 2F 00 1C AC A4  90 90 00 14 2D 00 81 41  61 64 6B 03 6D 5E 47 27  ®½öÚŸ½×Ú{ßu/  ¬¤     -  Aadk m^G'
820800A0  67 5E DC 7B 00 01 66 40  01 14 01 81 E4 1E 1A A2  65 69 69 0A 90 F2 E7 FD  DF CB D2 10 A2 8D 94 17  g^Ü{  f@    ä  ¢eii  òçýßËÒ ¢ ”
```

7.What should be the correct header of a PNG file? 89 50 4E 47

8.Take a screenshot to show the recovered file.