Examination Notes

Examination Number 1 Examiner Name: Akshay Chaurasia

Date & Time Activity

9/8/19
1:55 PM

The copy of the forensic image provided by the vice-president of the ForCorp Inc. was added to the Virtual Machine as a virtual floppy disk file. At the C:\ prompt in MS-DOS **diskedit a:** was typed to open the Norton Diskedit program. Then I went to the following directory: A:/

Here, I found the following three deleted objects:

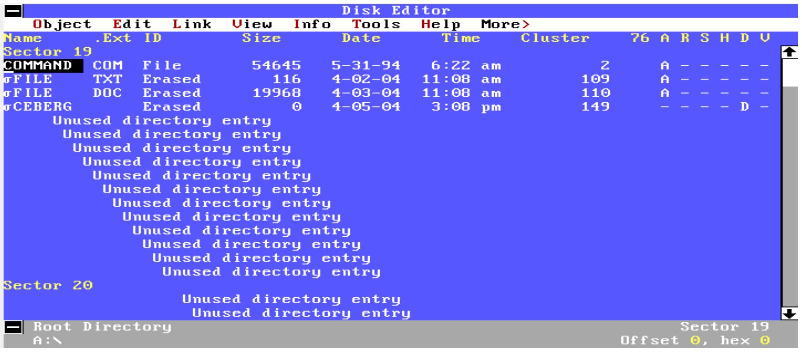
- **σFILE**: a TXT
- **σFILE**: a DOC
- **σCEBERG**: a folder

Within the “σCEBERG” folder, two more objects were found:

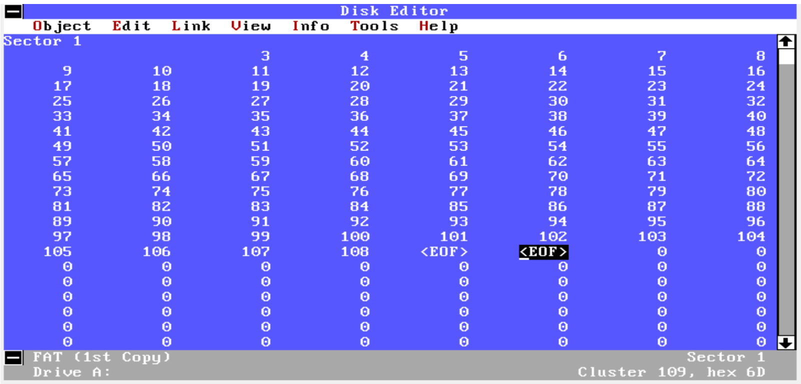
- **σFILE**: a TXT
- **σFILE**: a DOC

Recovering 1st Object: σFILE: a TXT

I recovered the first Object: σFILE: a TXT by replacing “σ” with an “!”. Then I went to the FAT 1 and scrolled to the cluster associated with it to change its value from 0 to <EOF>.

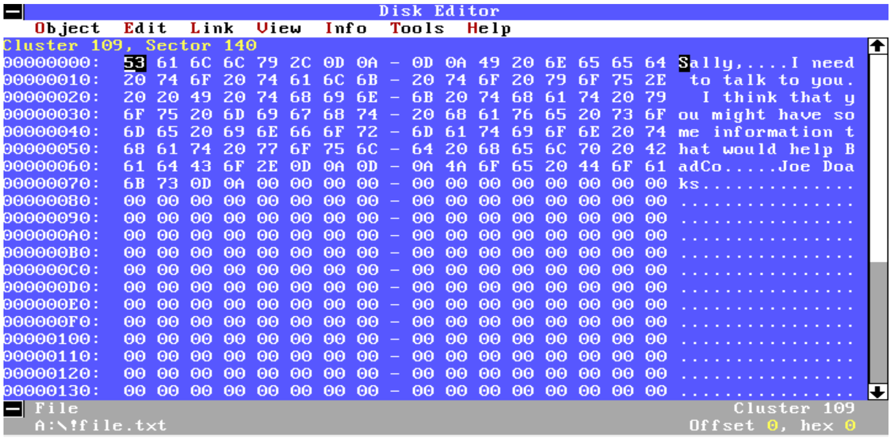


```
                              Disk Editor
   Object   Edit   Link   View   Info   Tools   Help   More>
Name      .Ext ID         Size       Date       Time     Cluster     76 A R S H D V
Sector 19
COMMAND   COM  File       54645    5-31-94    6:22 am          2     A - - - - -
σFILE     TXT  Erased       116    4-02-04   11:08 am        109     A - - - - -
σFILE     DOC  Erased     19968    4-03-04   11:08 am        110     A - - - - -
σCEBERG        Erased         0    4-05-04    3:08 pm        149     - - - - D -
     Unused directory entry
      Unused directory entry
       Unused directory entry
        Unused directory entry
         Unused directory entry
          Unused directory entry
           Unused directory entry
            Unused directory entry
             Unused directory entry
              Unused directory entry
               Unused directory entry
                Unused directory entry
Sector 20
                  Unused directory entry
                   Unused directory entry
   Root Directory                                                  Sector 19
   A:\                                                     Offset 0, hex 0
```



```
                              Disk Editor
   Object   Edit   Link   View   Info   Tools   Help
Sector 1
                           3          4          5          6          7          8
      9         10        11         12         13         14         15         16
     17         18        19         20         21         22         23         24
     25         26        27         28         29         30         31         32
     33         34        35         36         37         38         39         40
     41         42        43         44         45         46         47         48
     49         50        51         52         53         54         55         56
     57         58        59         60         61         62         63         64
     65         66        67         68         69         70         71         72
     73         74        75         76         77         78         79         80
     81         82        83         84         85         86         87         88
     89         90        91         92         93         94         95         96
     97         98        99        100        101        102        103        104
    105        106       107        108      <EOF>      <EOF>          0          0
      0          0         0          0          0          0          0          0
      0          0         0          0          0          0          0          0
      0          0         0          0          0          0          0          0
      0          0         0          0          0          0          0          0
      0          0         0          0          0          0          0          0
      0          0         0          0          0          0          0          0
   FAT (1st Copy)                                                   Sector 1
   Drive A:                                             Cluster 109, hex 6D
```

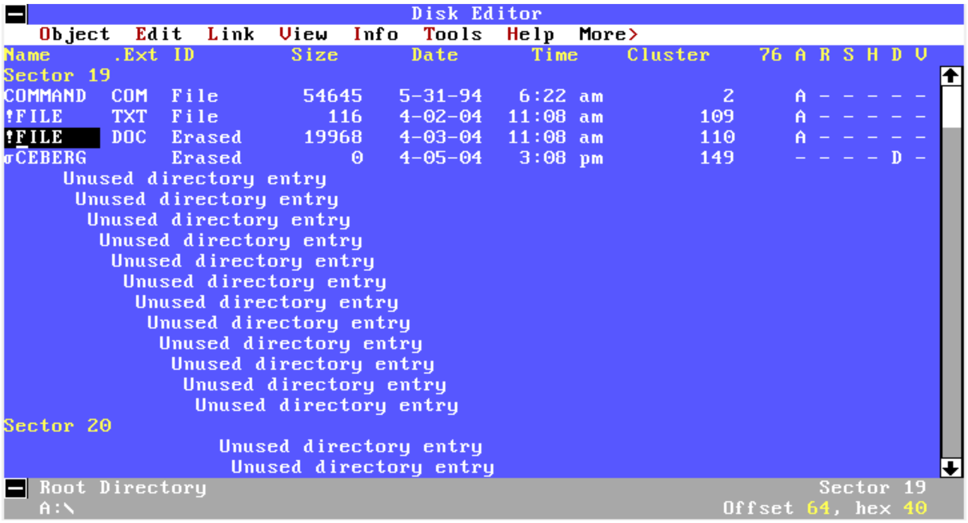
9/8/19
2:12 PM



```
Cluster 109, Sector 140
00000000:  53 61 6C 6C 79 2C 0D 0A - 0D 0A 49 20 6E 65 65 64 Sally,....I need
00000010:  20 74 6F 20 74 61 6C 6B - 20 74 6F 20 79 6F 75 2E  to talk to you.
00000020:  20 20 49 20 74 68 69 6E - 6B 20 74 68 61 74 20 79   I think that y
00000030:  6F 75 20 6D 69 67 68 74 - 20 68 61 76 65 20 73 6F ou might have so
00000040:  6D 65 20 69 6E 66 6F 72 - 6D 61 74 69 6F 6E 20 74 me information t
00000050:  68 61 74 20 77 6F 75 6C - 64 20 68 65 6C 70 20 42 hat would help B
00000060:  61 64 43 6F 2E 0D 0A 0D - 0A 4A 6F 65 20 44 6F 61 adCo.....Joe Doa
00000070:  6B 73 0D 0A 00 00 00 00 - 00 00 00 00 00 00 00 00 ks..............
00000080:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
00000090:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000000A0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000000B0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000000C0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000000D0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000000E0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000000F0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
00000100:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
00000110:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
00000120:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
00000130:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
 File                                                         Cluster 109
 A:\!file.txt                                             Offset 0, hex 0
```

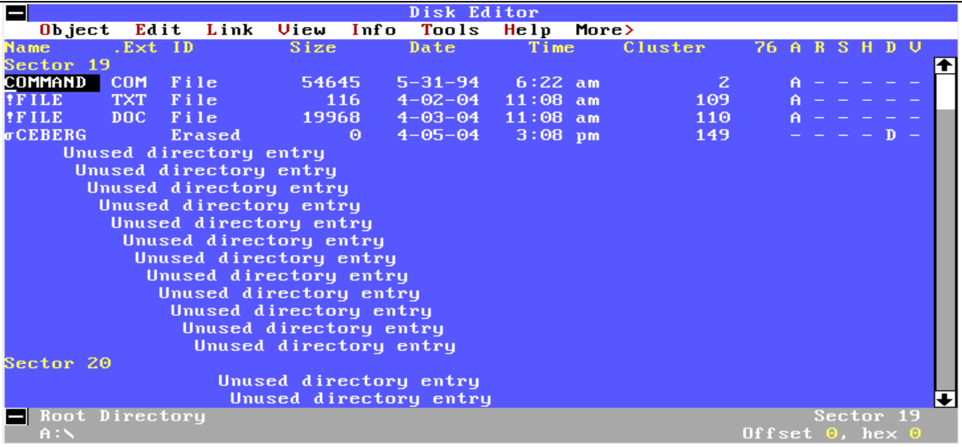
Recovering 2nd Object: σFILE: a DOC

I recovered the second Object: σFILE: a DOC by replacing "σ" with an "!". Then I went to the FAT 1 and scrolled to the clusters associated with it (110-147) to change their value from 0 to their immediate next cluster. And changed cluster number 148 to <EOF>.

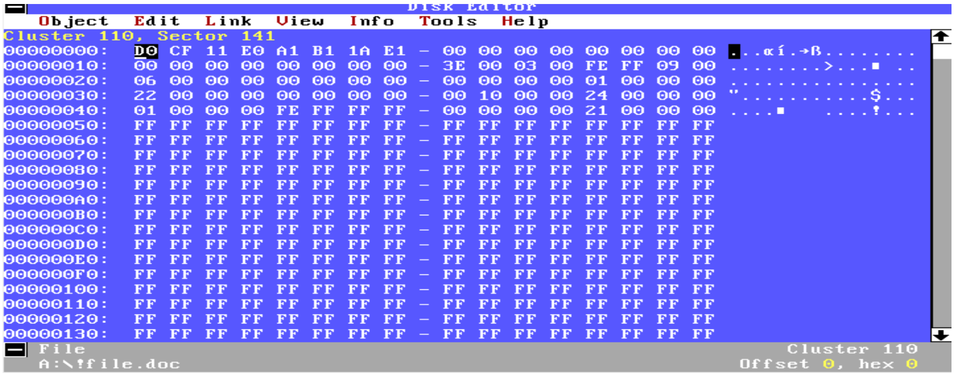


```
Name      .Ext ID        Size     Date       Time     Cluster    76 A R S H D V
Sector 19
COMMAND   COM  File      54645   5-31-94    6:22 am         2       A - - - - -
!FILE     TXT  File        116   4-02-04   11:08 am       109       A - - - - -
!FILE     DOC  Erased    19968   4-03-04   11:08 am       110       A - - - - -
σCEBERG        Erased        0   4-05-04    3:08 pm       149       - - - - D -
     Unused directory entry
      Unused directory entry
       Unused directory entry
        Unused directory entry
         Unused directory entry
          Unused directory entry
           Unused directory entry
            Unused directory entry
             Unused directory entry
              Unused directory entry
               Unused directory entry
                Unused directory entry
Sector 20
                  Unused directory entry
                   Unused directory entry
 Root Directory                                               Sector 19
 A:\                                                  Offset 64, hex 40
```

9/8/19
2:22 PM



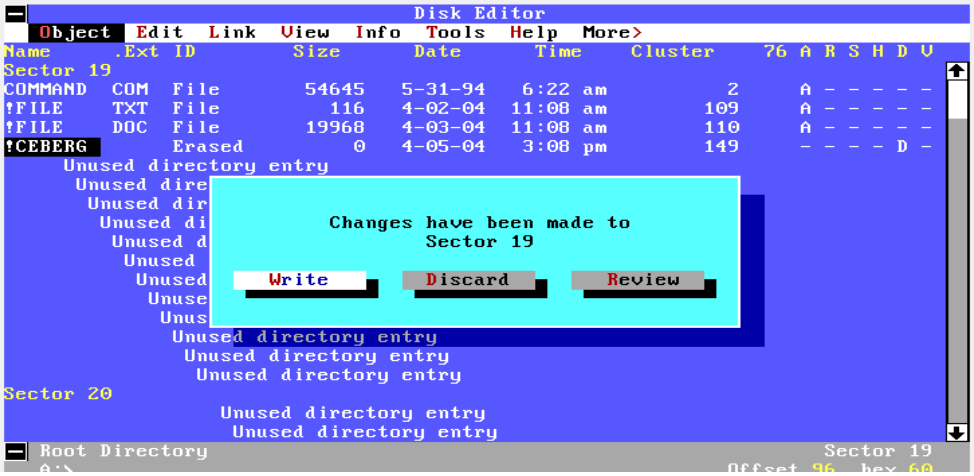
```
Name      .Ext ID        Size      Date       Time     Cluster     76 A R S H D V
Sector 19
COMMAND    COM  File     54645   5-31-94    6:22 am         2      A - - - - -
!FILE      TXT  File       116   4-02-04   11:08 am       109      A - - - - -
!FILE      DOC  File     19968   4-03-04   11:08 am       110      A - - - - -
σCEBERG         Erased       0   4-05-04    3:08 pm       149      - - - - D -
     Unused directory entry
      Unused directory entry
       Unused directory entry
        Unused directory entry
         Unused directory entry
          Unused directory entry
           Unused directory entry
            Unused directory entry
             Unused directory entry
              Unused directory entry
               Unused directory entry
                Unused directory entry
Sector 20
                  Unused directory entry
                   Unused directory entry
Root Directory                                               Sector 19
A:\                                                  Offset 0, hex 0
```



```
Cluster 110, Sector 141
00000000:  D0 CF 11 E0 A1 B1 1A E1 - 00 00 00 00 00 00 00 00  ...αí.→ß........
00000010:  00 00 00 00 00 00 00 00 - 3E 00 03 00 FE FF 09 00  ........>...■ ..
00000020:  06 00 00 00 00 00 00 00 - 00 00 00 00 01 00 00 00  ................
00000030:  22 00 00 00 00 00 00 00 - 00 10 00 00 24 00 00 00  "...........$...
00000040:  01 00 00 00 FE FF FF FF - 00 00 00 00 21 00 00 00  ....■    ....!...
00000050:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000060:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000070:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000080:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000090:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
000000A0:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
000000B0:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
000000C0:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
000000D0:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
000000E0:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
000000F0:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000100:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000110:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000120:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000130:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
File                                                    Cluster 110
A:\!file.doc                                        Offset 0, hex 0
```

Recovering the Object: σCEBERG: a Folder

I recovered the first Object: σCEBERG: a Folder by replacing "σ" with an "!". Then I went to the FAT 1 and scrolled to the cluster associated with it (149) to change its value from 0 to <EOF>.

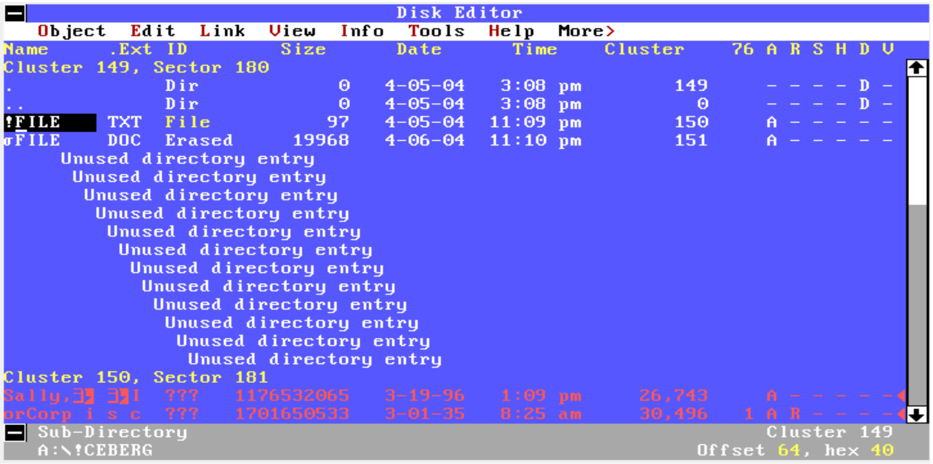


```
Name      .Ext ID        Size      Date       Time     Cluster     76 A R S H D V
Sector 19
COMMAND    COM  File     54645   5-31-94    6:22 am         2      A - - - - -
!FILE      TXT  File       116   4-02-04   11:08 am       109      A - - - - -
!FILE      DOC  File     19968   4-03-04   11:08 am       110      A - - - - -
!CEBERG         Erased       0   4-05-04    3:08 pm       149      - - - - D -
     Unused directory entry

          Changes have been made to
                  Sector 19

Sector 20
                  Unused directory entry
                   Unused directory entry
Root Directory                                               Sector 19
A:\                                                 Offset 96, hex 60
```

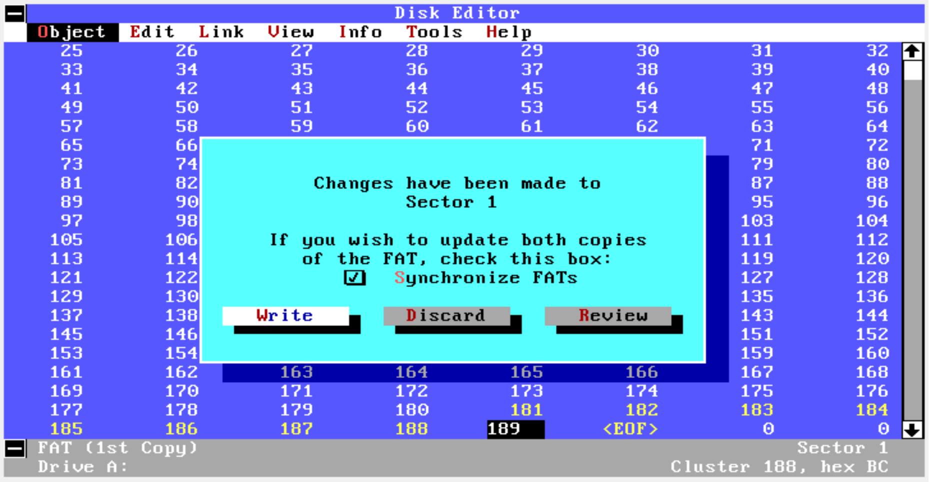
9/8/19
2:28 PM

Recovering 3rd and 4th Object

I recovered the third and fourth objects in the same way as I recovered the 1st and 2nd objects.

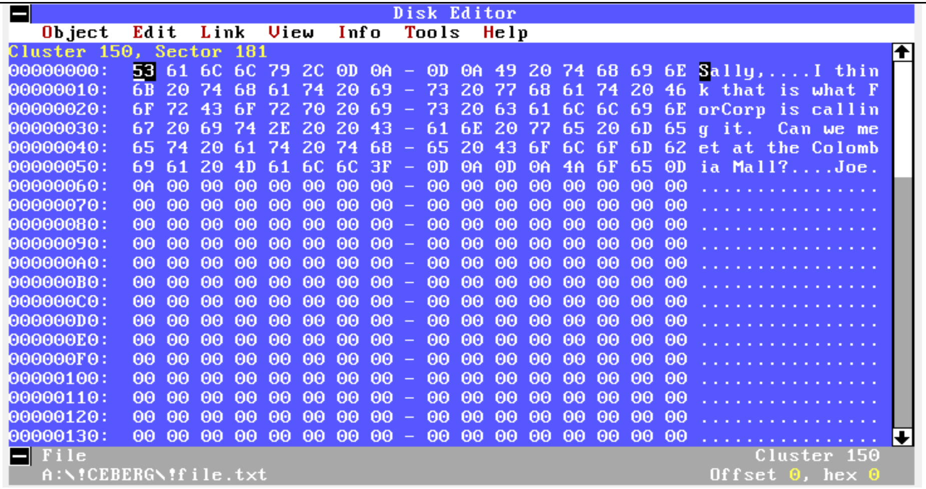


```
                              Disk Editor
   Object  Edit  Link  View  Info  Tools  Help  More>
Name      .Ext ID        Size       Date       Time    Cluster    76 A R S H D V
Cluster 149, Sector 180
.             Dir           0    4-05-04   3:08 pm        149       - - - - D -
..            Dir           0    4-05-04   3:08 pm          0       - - - - D -
!FILE    TXT  File         97    4-05-04  11:09 pm        150       A - - - - -
σFILE    DOC  Erased    19968    4-06-04  11:10 pm        151       A - - - - -
     Unused directory entry
      Unused directory entry
       Unused directory entry
        Unused directory entry
         Unused directory entry
          Unused directory entry
           Unused directory entry
            Unused directory entry
             Unused directory entry
              Unused directory entry
               Unused directory entry
                Unused directory entry
Cluster 150, Sector 181
Sally,3▌ 3▌I  ???  1176532065  3-19-96   1:09 pm     26,743       A - - - - -
orCorp i s c  ???  1701650533  3-01-35   8:25 am     30,496     1 A R - - - -
   Sub-Directory                                               Cluster 149
   A:\!CEBERG                                            Offset 64, hex 40
```

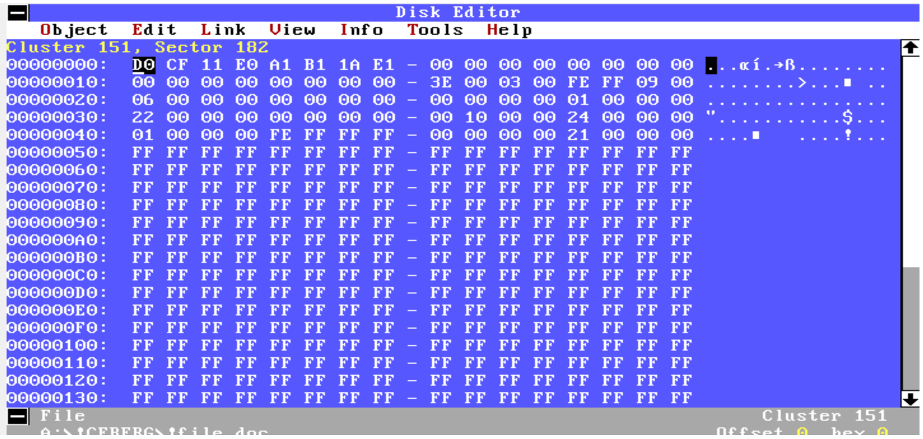


```
                              Disk Editor
   Object  Edit  Link  View  Info  Tools  Help
    25       26       27       28       29       30       31       32
    33       34       35       36       37       38       39       40
    41       42       43       44       45       46       47       48
    49       50       51       52       53       54       55       56
    57       58       59       60       61       62       63       64
    65       66                                           71       72
    73       74                                           79       80
    81       82     Changes have been made to             87       88
    89       90             Sector 1                      95       96
    97       98                                          103      104
   105      106   If you wish to update both copies      111      112
   113      114     of the FAT, check this box:          119      120
   121      122        ☑  Synchronize FATs               127      128
   129      130                                          135      136
   137      138    Write      Discard      Review        143      144
   145      146                                          151      152
   153      154                                          159      160
   161      162      163      164      165      166      167      168
   169      170      171      172      173      174      175      176
   177      178      179      180      181      182      183      184
   185      186      187      188      189     <EOF>       0        0
   FAT (1st Copy)                                              Sector 1
   Drive A:                                         Cluster 188, hex BC
```

9/8/19
2:43 PM

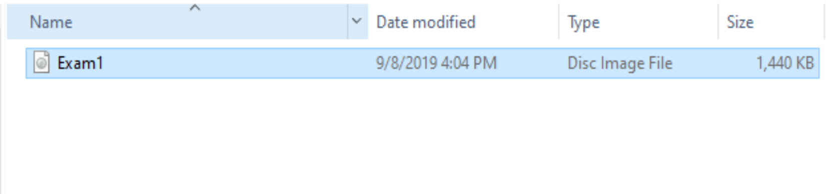


```
Cluster 150, Sector 181
00000000:  53 61 6C 6C 79 2C 0D 0A - 0D 0A 49 20 74 68 69 6E Sally,....I thin
00000010:  6B 20 74 68 61 74 20 69 - 73 20 77 68 61 74 20 46 k that is what F
00000020:  6F 72 43 6F 72 70 20 69 - 73 20 63 61 6C 6C 69 6E orCorp is callin
00000030:  67 20 69 74 2E 20 20 43 - 61 6E 20 77 65 20 6D 65 g it.  Can we me
00000040:  65 74 20 61 74 20 74 68 - 65 20 43 6F 6C 6F 6D 62 et at the Colomb
00000050:  69 61 20 4D 61 6C 6C 3F - 0D 0A 0D 0A 4A 6F 65 0D ia Mall?....Joe.
00000060:  0A 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
00000070:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
00000080:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
00000090:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000000A0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000000B0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000000C0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000000D0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000000E0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
000000F0:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
00000100:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
00000110:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
00000120:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
00000130:  00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ................
 File                                                          Cluster 150
 A:\!CEBERG\!file.txt                                     Offset 0, hex 0
```



```
Cluster 151, Sector 182
00000000:  D0 CF 11 E0 A1 B1 1A E1 - 00 00 00 00 00 00 00 00 ...αí.→ß........
00000010:  00 00 00 00 00 00 00 00 - 3E 00 03 00 FE FF 09 00 ........>...■ ..
00000020:  06 00 00 00 00 00 00 00 - 00 00 00 00 01 00 00 00 ................
00000030:  22 00 00 00 00 00 00 00 - 00 10 00 00 24 00 00 00 "...........$...
00000040:  01 00 00 00 FE FF FF FF - 00 00 00 00 21 00 00 00 ....■    ....!...
00000050:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000060:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000070:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000080:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000090:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
000000A0:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
000000B0:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
000000C0:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
000000D0:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
000000E0:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
000000F0:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000100:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000110:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000120:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
00000130:  FF FF FF FF FF FF FF FF - FF FF FF FF FF FF FF FF
 File                                                          Cluster 151
 A:\!CEBERG\!file.doc                                     Offset 0, hex 0
```

After recovering all the objects, I unmounted the vrtual disk image from the MS DOS and copied it to desktop.



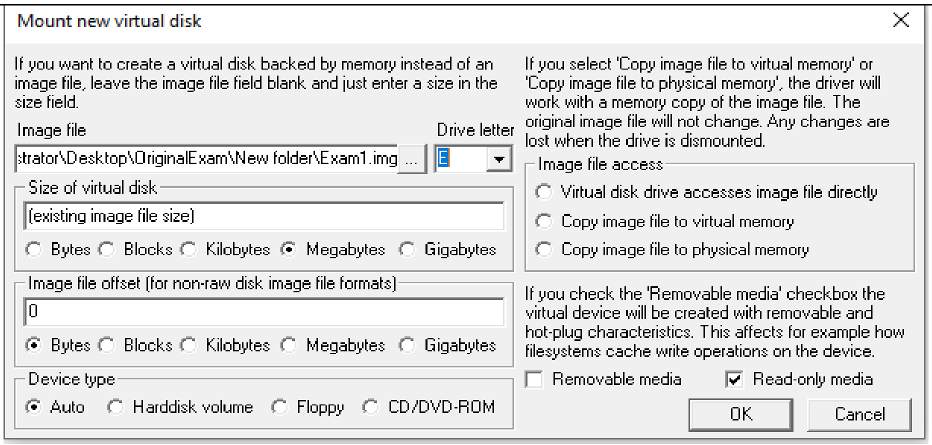
Name	Date modified	Type	Size
Exam1	9/8/2019 4:04 PM	Disc Image File	1,440 KB

Then, I mounted it on the E:/ for the futher review

Examination Notes

Examination Number 1 Examiner Name: Akshay Chaurasia

9/8/19
2:53 PM



Mount new virtual disk

If you want to create a virtual disk backed by memory instead of an image file, leave the image file field blank and just enter a size in the size field.

Image file: strator\Desktop\OriginalExam\New folder\Exam1.img

Drive letter: E

Size of virtual disk: (existing image file size)

○ Bytes ○ Blocks ○ Kilobytes ● Megabytes ○ Gigabytes

Image file offset (for non-raw disk image file formats): 0

● Bytes ○ Blocks ○ Kilobytes ○ Megabytes ○ Gigabytes

Device type

● Auto ○ Harddisk volume ○ Floppy ○ CD/DVD-ROM

If you select 'Copy image file to virtual memory' or 'Copy image file to physical memory', the driver will work with a memory copy of the image file. The original image file will not change. Any changes are lost when the drive is dismounted.

Image file access

○ Virtual disk drive accesses image file directly

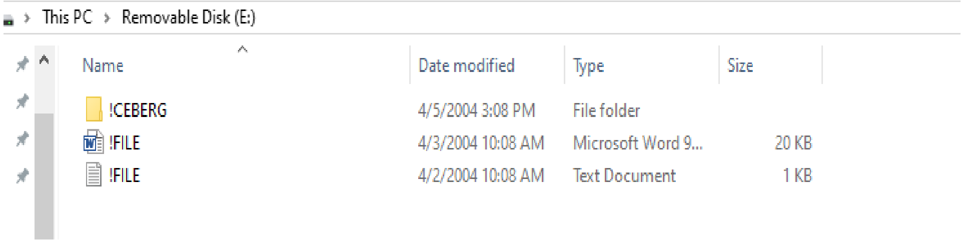
○ Copy image file to virtual memory

○ Copy image file to physical memory

If you check the 'Removable media' checkbox the virtual device will be created with removable and hot-plug characteristics. This affects for example how filesystems cache write operations on the device.

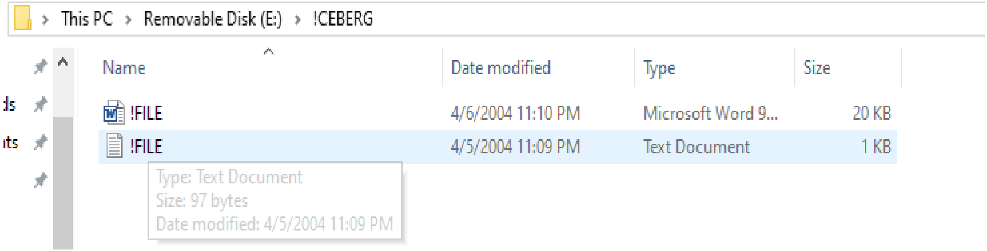
☐ Removable media ☑ Read-only media

After mounting it on E:/, the file was ready for review for the examination.



This PC › Removable Disk (E:)

Name	Date modified	Type	Size
!CEBERG	4/5/2004 3:08 PM	File folder	
!FILE	4/3/2004 10:08 AM	Microsoft Word 9...	20 KB
!FILE	4/2/2004 10:08 AM	Text Document	1 KB



This PC › Removable Disk (E:) › !CEBERG

Name	Date modified	Type	Size
!FILE	4/6/2004 11:10 PM	Microsoft Word 9...	20 KB
!FILE	4/5/2004 11:09 PM	Text Document	1 KB

Type: Text Document
Size: 97 bytes
Date modified: 4/5/2004 11:09 PM