Worcester Polytechnic Institute
Department of Computer Science

Module 3: Alternate data streams

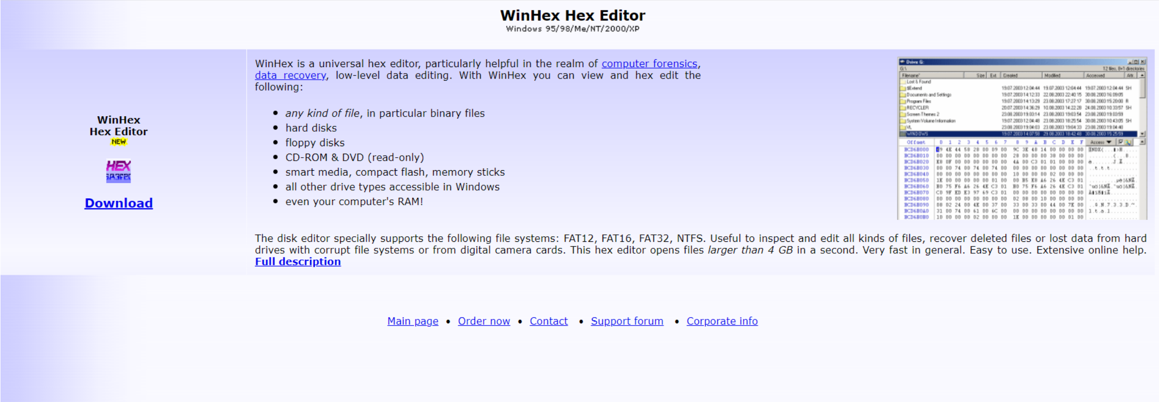
Objectives

- Append hidden data to a file using alternate data streams
- Reveal the hidden data by analyzing the file MFT

Task

Task 1. Software Preparation

1. Download the WinHex. The download link is: http://www.winhex.com/winhex/hex-editor.html



WinHex Hex Editor
Windows 95/98/Me/NT/2000/XP

WinHex is a universal hex editor, particularly helpful in the realm of computer forensics, data recovery, low-level data editing. With WinHex you can view and hex edit the following:

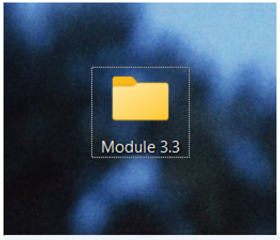
- *any kind of file*, in particular binary files
- hard disks
- floppy disks
- CD-ROM & DVD (read-only)
- smart media, compact flash, memory sticks
- all other drive types accessible in Windows
- even your computer's RAM!

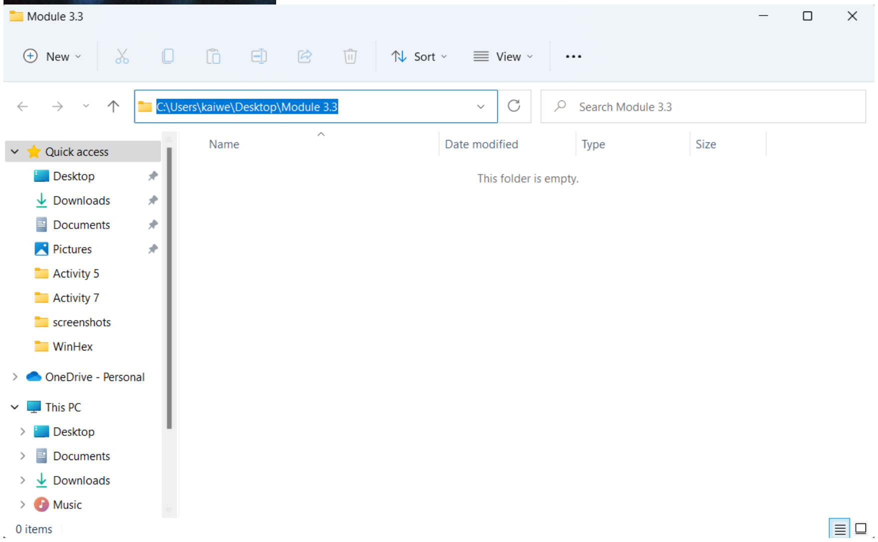
The disk editor specially supports the following file systems: FAT12, FAT16, FAT32, NTFS. Useful to inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems or from digital camera cards. This hex editor opens files *larger than 4 GB* in a second. Very fast in general. Easy to use. Extensive online help.
Full description

WinHex
Hex Editor
NEW
HEX
Download
Main page • Order now • Contact • Support forum • Corporate info

Task 2. Append hidden data to a file using alternate data stream

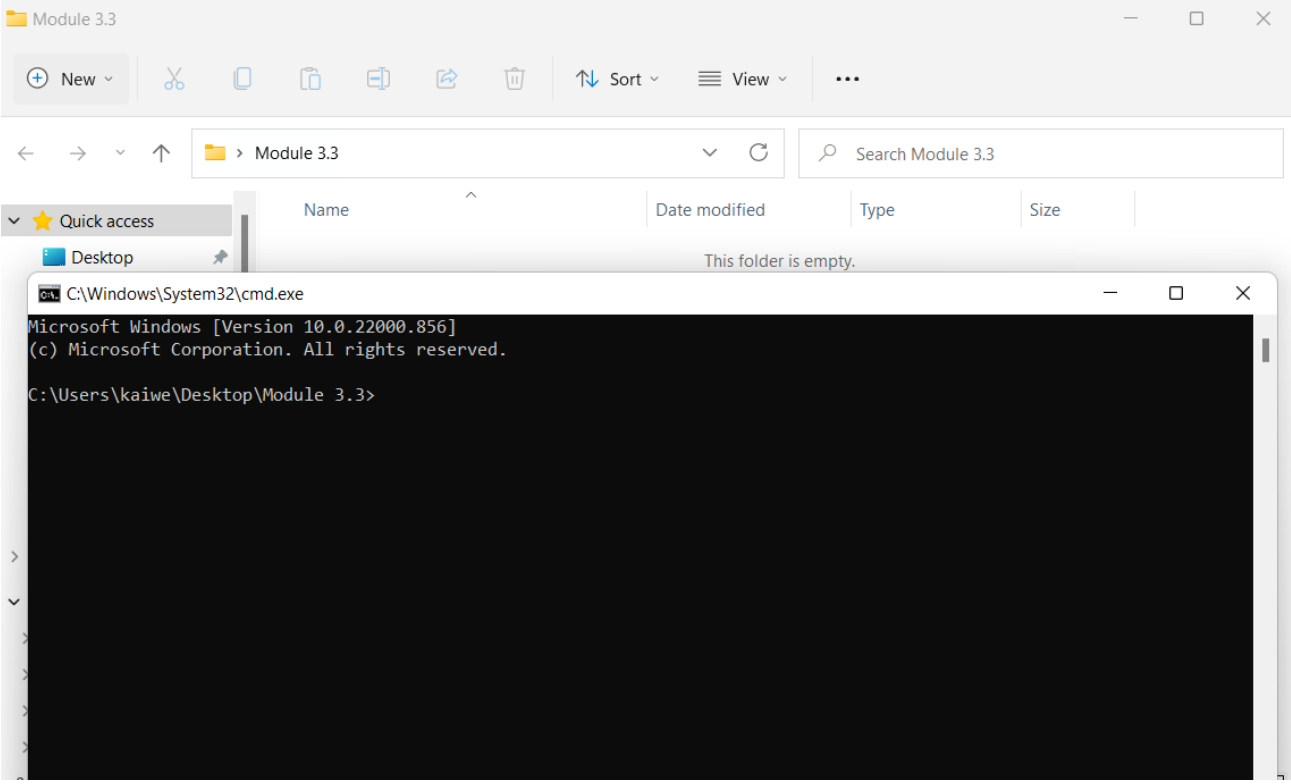
2. Create a folder. Open the folder and then type "cmd" to open cmd command prompt in Windows.





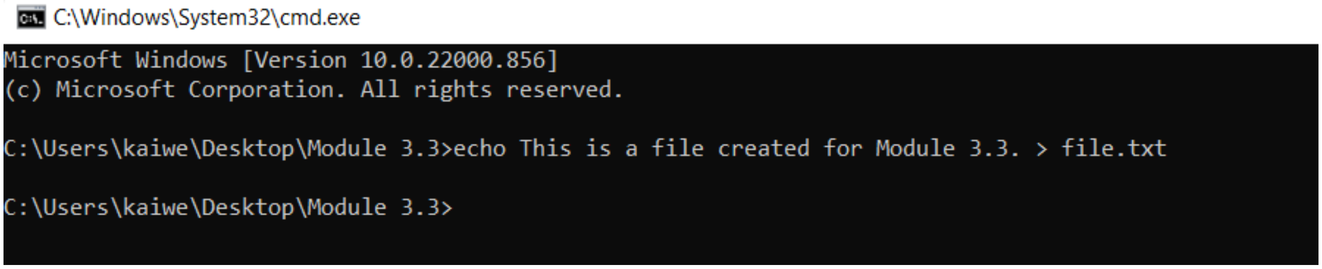
C:\Users\kaiwe\Desktop\Module 3.3

This folder is empty.



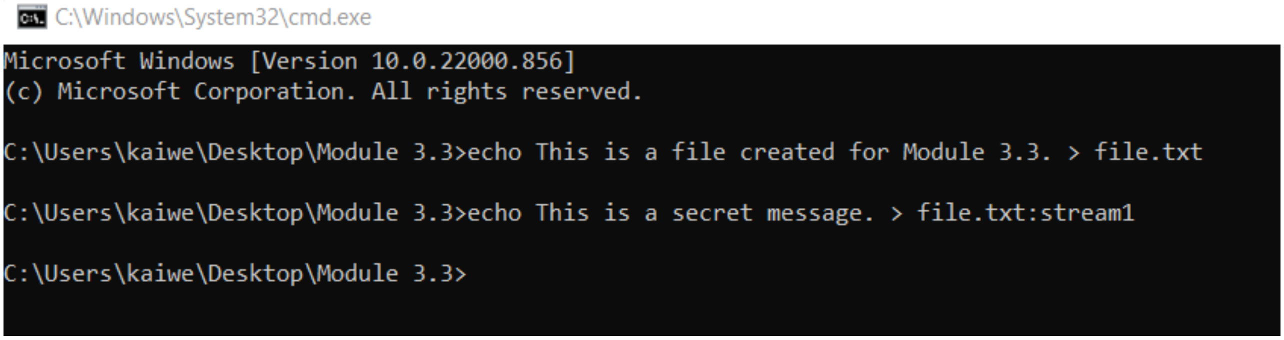
```
Microsoft Windows [Version 10.0.22000.856]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kaiwe\Desktop\Module 3.3>
```

3. Create a file called file.txt in Module 3.3 folder and store the message “This is a file created for Module 3.3.”.
The command for creating a file and storing the message is: ***echo This is a file created for Module 3.3. > file.txt***



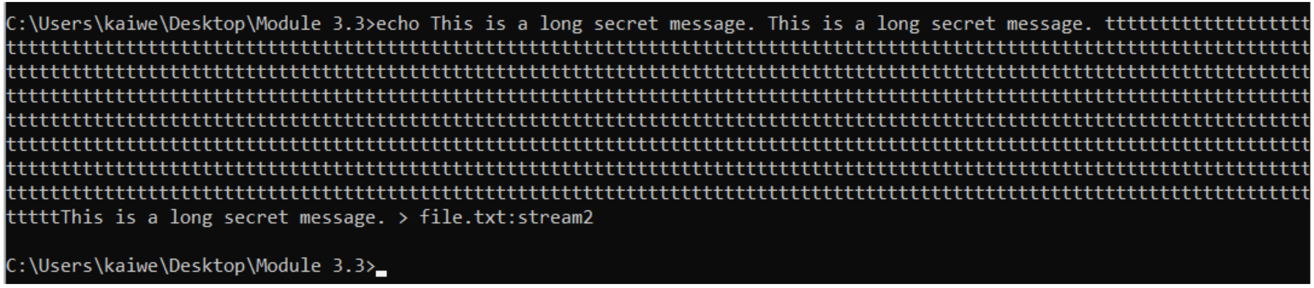
```
Microsoft Windows [Version 10.0.22000.856]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kaiwe\Desktop\Module 3.3>echo This is a file created for Module 3.3. > file.txt

C:\Users\kaiwe\Desktop\Module 3.3>
```

4. Append a short-hidden message to the file.txt using alternate data stream.
Command: ***echo This is a secret message. > file.txt:stream1***



```
Microsoft Windows [Version 10.0.22000.856]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kaiwe\Desktop\Module 3.3>echo This is a file created for Module 3.3. > file.txt

C:\Users\kaiwe\Desktop\Module 3.3>echo This is a secret message. > file.txt:stream1

C:\Users\kaiwe\Desktop\Module 3.3>
```

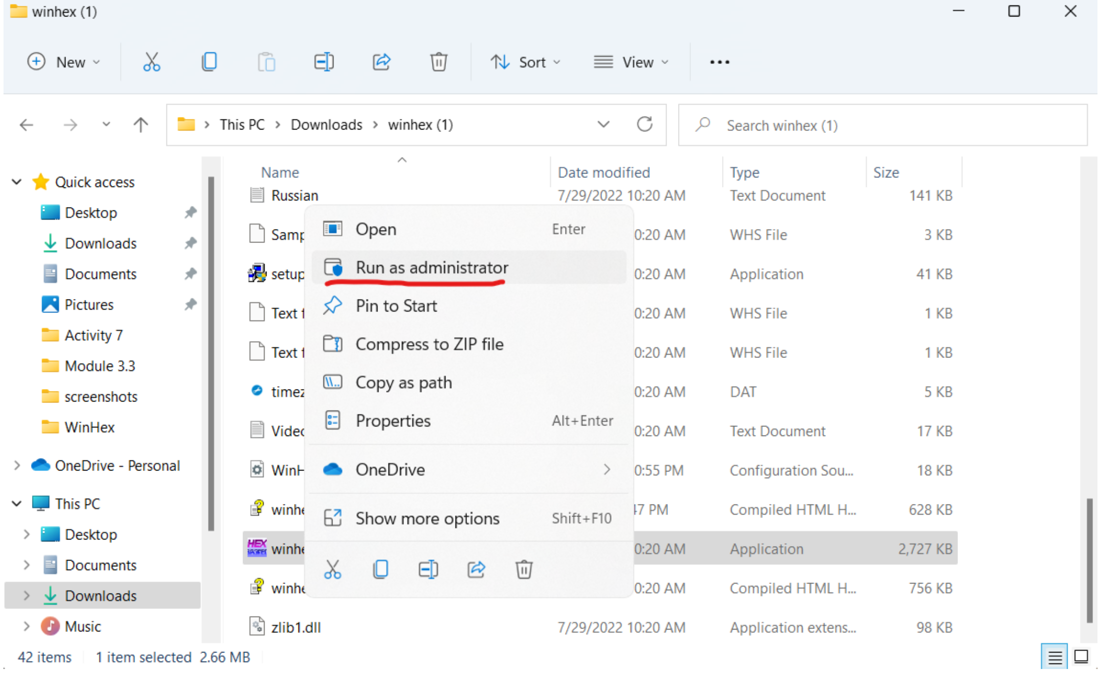
5. Append a long-hidden message to the file.txt using alternate data stream.
(Please note: The content of the message can be changed but please make sure the size of the message is larger than 512 bytes).
Command: ***echo This is a long secret message. This is a long secret message. ttttttttttttt…ttttttttttttt This is a long secret message. > file.txt:stream2***



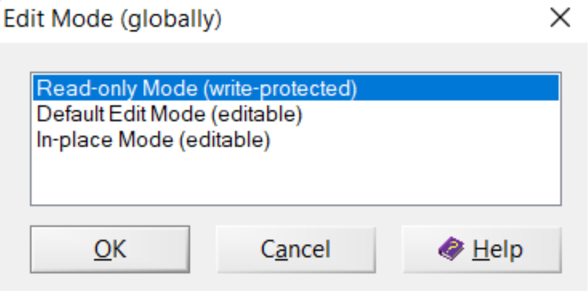
```
C:\Users\kaiwe\Desktop\Module 3.3>echo This is a long secret message. This is a long secret message. ttttttttttttttttttt
tttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttt
tttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttt
tttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttt
tttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttt
tttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttt
tttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttt
tttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttttt
tttttThis is a long secret message. > file.txt:stream2

C:\Users\kaiwe\Desktop\Module 3.3>_
```

Task 3. Reveal the hidden data by analyzing the file MFT

6. Right click on WinHex and choose "**Run as an Administrator**" to start WinHex. If you see an evaluation warning message, click on **OK**.



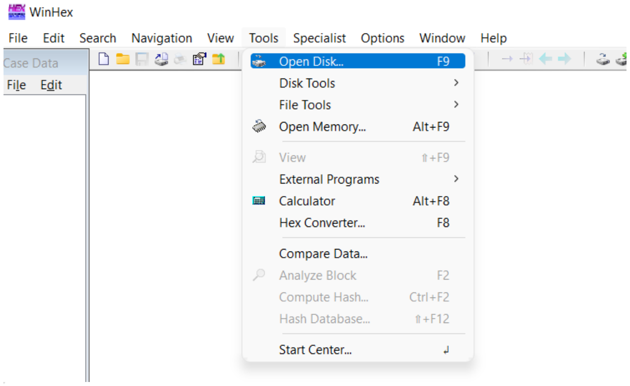
7. After opening WinHex, as a safety precaution, click **Options**, **Edit Mode** from the menu. In the Select Mode dialog box, click **Read-Only Mode (=write-protected)**, as shown in the screenshot below, and click **OK**.

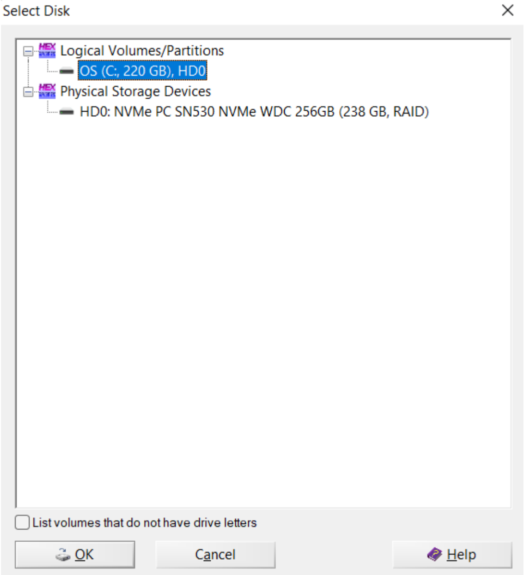


Edit Mode (globally)

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

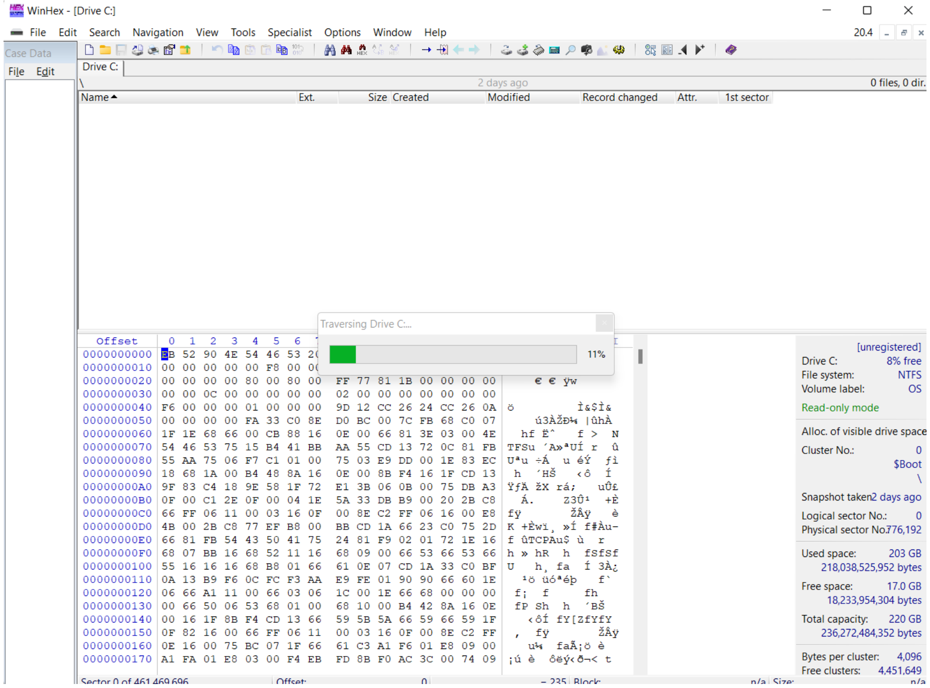
8. Click **Tools**, **Open Disk** from the menu. In the View Disk dialog box, click the drive where the file.txt is stored, and then click **OK**. If you're prompted to take a new snapshot, click **Take a new one**.




Select Disk

- Logical Volumes/Partitions
  - OS (C:, 220 GB), HD0
- Physical Storage Devices
  - HD0: NVMe PC SN530 NVMe WDC 256GB (238 GB, RAID)

☐ List volumes that do not have drive letters



Traversing Drive C:...

11%

```
    Offset   0  1  2  3  4  5  6  7
0000000000  EB 52 90 4E 54 46 53 20
0000000010  00 00 00 00 00 F8 00 00
0000000020  00 00 00 00 80 00 80 00  FF 77 81 1B 00 00 00 00      € € ÿw
0000000030  00 00 0C 00 00 00 00 00  02 00 00 00 00 00 00 00
0000000040  F6 00 00 00 01 00 00 00  9D 12 CC 26 24 CC 26 0A  ö         Ì&$Ì&
0000000050  00 00 00 00 FA 33 C0 8E  D0 BC 00 7C FB 68 C0 07      ú3ÀŽÐ¼ |ûhÀ
0000000060  1F 1E 68 66 00 CB 88 16  0E 00 66 81 3E 03 00 4E    hf Ëˆ   f >  N
0000000070  54 46 53 75 15 B4 41 BB  AA 55 CD 13 72 0C 81 FB  TFSu ´A»ªUÍ r  û
0000000080  55 AA 75 06 F7 C1 01 00  75 03 E9 DD 00 1E 83 EC  Uªu ÷Á  u éÝ  ƒì
0000000090  18 68 1A 00 B4 48 8A 16  0E 00 8B F4 16 1F CD 13   h  ´HŠ   ‹ô  Í
00000000A0  9F 83 C4 18 9E 58 1F 72  E1 3B 06 0B 00 75 DB A3  ŸƒÄ žX rá;   uÛ£
00000000B0  0F 00 C1 2E 0F 00 04 1E  5A 33 DB B9 00 20 2B C8    Á.     Z3Û¹  +È
00000000C0  66 FF 06 11 00 03 16 0F  00 8E C2 FF 06 16 00 E8  fÿ         ŽÂÿ   è
00000000D0  4B 00 2B C8 77 EF B8 00  BB CD 1A 66 23 C0 75 2D  K +Èwï¸ »Í f#Àu-
00000000E0  66 81 FB 54 43 50 41 75  24 81 F9 02 01 72 1E 16  f ûTCPAu$ ù  r
00000000F0  68 07 BB 16 68 52 11 16  68 09 00 66 53 66 53 66  h » hR  h  fSfSf
0000000100  55 16 16 16 68 B8 01 66  61 0E 07 CD 1A 33 C0 BF  U   h¸ fa  Í 3À¿
0000000110  0A 13 B9 F6 0C FC F3 AA  E9 FE 01 90 90 66 60 1E    ¹ö üóªéþ   f`
0000000120  06 66 A1 11 00 66 03 06  1C 00 1E 66 68 00 00 00   f¡  f     fh
0000000130  00 66 50 06 53 68 01 00  68 10 00 B4 42 8A 16 0E   fP Sh  h  ´BŠ
0000000140  00 16 1F 8B F4 CD 13 66  59 5B 5A 66 59 66 59 1F     ‹ôÍ fY[ZfYfY
0000000150  0F 82 16 00 66 FF 06 11  00 03 16 0F 00 8E C2 FF   ‚  fÿ        ŽÂÿ
0000000160  0E 16 00 75 BC 07 1F 66  61 C3 A1 F6 01 E8 09 00     u¼  faÃ¡ö è
0000000170  A1 FA 01 E8 03 00 F4 EB  FD 8B F0 AC 3C 00 74 09  ¡ú è  ôëý‹ð¬< t
Sector 0 of 461,469,696        Offset:        0        = 235  Block:        n/a  Size:        n/a
```

[unregistered]
Drive C: 8% free
File system: NTFS
Volume label: OS
Read-only mode

Alloc. of visible drive space
Cluster No.: 0
$Boot
\

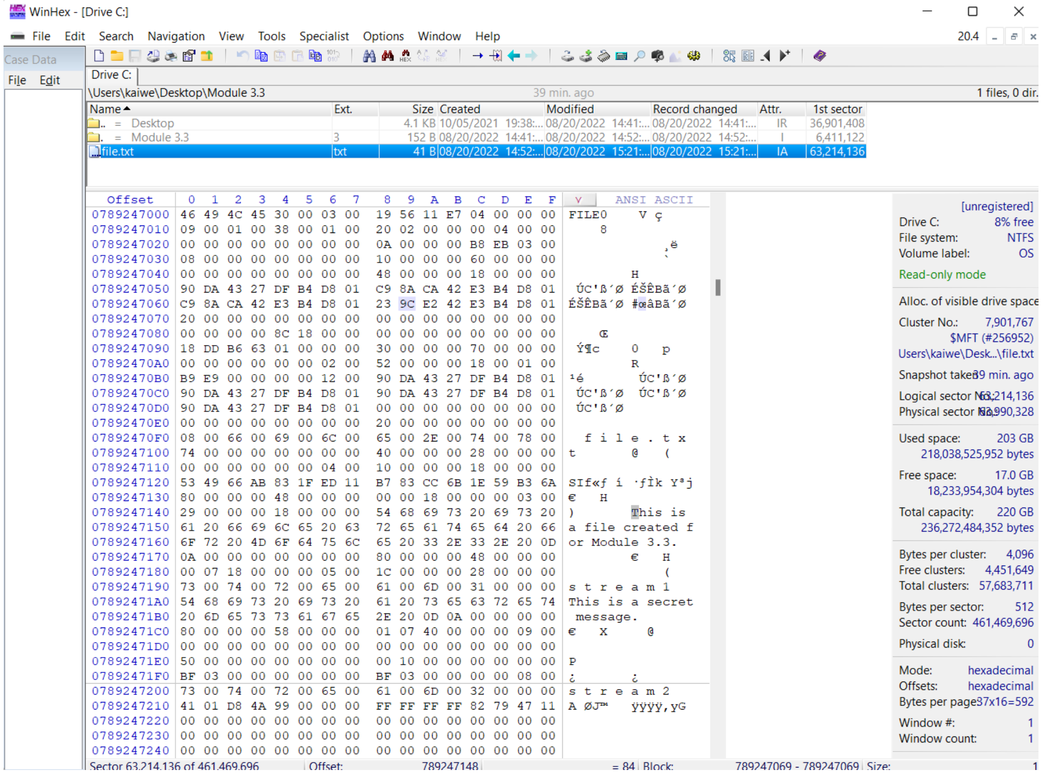
Snapshot taken2 days ago
Logical sector No.: 0
Physical sector No.776,192

Used space: 203 GB
218,038,525,952 bytes
Free space: 17.0 GB
18,233,954,304 bytes
Total capacity: 220 GB
236,272,484,352 bytes

Bytes per cluster: 4,096
Free clusters: 4,451,649

9. Open the file.txt.

(Note: You need to analyze the MFT within the Drive. If you double click on the file and open another tab for this file in WinHex, it only shows the content of the file, but doesn't show the MFT information.


WinHex - [Drive C:]
File Edit Search Navigation View Tools Specialist Options Window Help
20.4
Case Data
File Edit
Drive C:

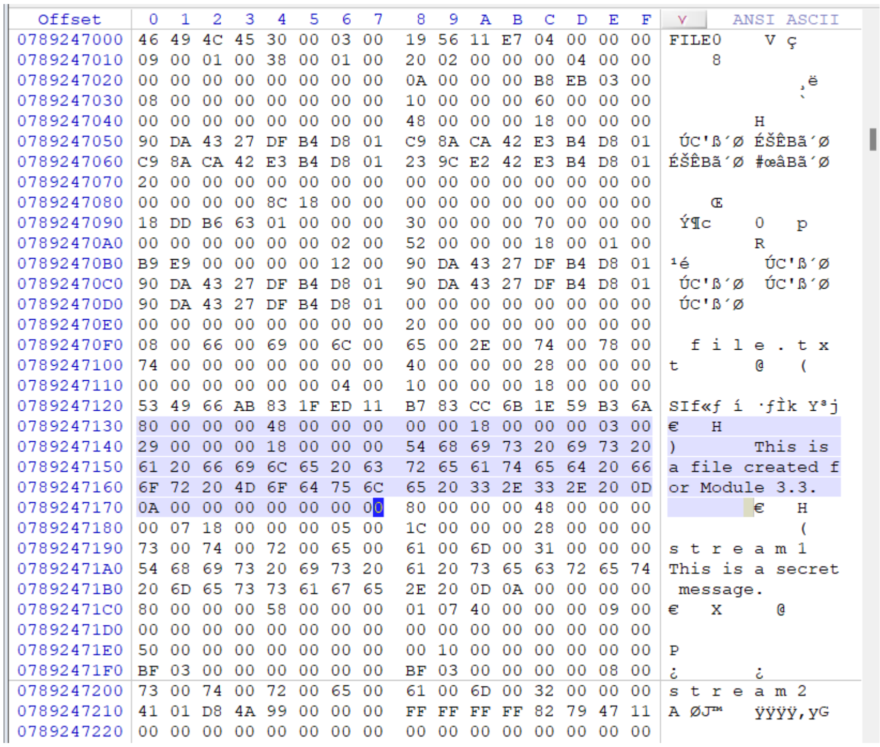
```
\Users\kaiwe\Desktop\Module 3.3                39 min. ago                                  1 files, 0 dir.
Name ▲            Ext.   Size Created             Modified            Record changed      Attr.  1st sector
.. = Desktop             4.1 KB 10/05/2021 19:38:... 08/20/2022 14:41:... 08/20/2022 14:41:...  IR   36,901,408
.  = Module 3.3   3      152 B 08/20/2022 14:41:... 08/20/2022 14:52:... 08/20/2022 14:52:...  I     6,411,122
file.txt          txt     41 B 08/20/2022 14:52:... 08/20/2022 15:21:... 08/20/2022 15:21:...  IA   63,214,136
```

```
Offset       0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
0789247000  46 49 4C 45 30 00 03 00  19 56 11 E7 04 00 00 00  FILE0    V ç
0789247010  09 00 01 00 38 00 01 00  20 02 00 00 00 04 00 00      8
0789247020  00 00 00 00 00 00 00 00  0A 00 00 00 B8 EB 03 00              ¸ë
0789247030  08 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00
0789247040  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
0789247050  90 DA 43 27 DF B4 D8 01  C9 8A CA 42 E3 B4 D8 01   ÚC'ß´Ø ÉŠÊBã´Ø
0789247060  C9 8A CA 42 E3 B4 D8 01  23 9C E2 42 E3 B4 D8 01  ÉŠÊBã´Ø #œâBã´Ø
0789247070  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0789247080  00 00 00 00 8C 18 00 00  00 00 00 00 00 00 00 00      Œ
0789247090  18 DD B6 63 01 00 00 00  30 00 00 00 70 00 00 00   Ý¶c    0   p
07892470A0  00 00 00 00 00 00 02 00  52 00 00 00 18 00 01 00          R
07892470B0  B9 E9 00 00 00 00 12 00  90 DA 43 27 DF B4 D8 01  ¹é       ÚC'ß´Ø
07892470C0  90 DA 43 27 DF B4 D8 01  90 DA 43 27 DF B4 D8 01   ÚC'ß´Ø  ÚC'ß´Ø
07892470D0  90 DA 43 27 DF B4 D8 01  00 00 00 00 00 00 00 00   ÚC'ß´Ø
07892470E0  00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
07892470F0  08 00 66 00 69 00 6C 00  65 00 2E 00 74 00 78 00    f i l e . t x
0789247100  74 00 00 00 00 00 00 00  40 00 00 00 28 00 00 00  t       @   (
0789247110  00 00 00 00 00 00 04 00  10 00 00 00 18 00 00 00
0789247120  53 49 66 AB 83 1F ED 11  B7 83 CC 6B 1E 59 B3 6A  SIf«ƒ í ·ƒÌk Y³j
0789247130  80 00 00 00 48 00 00 00  00 00 18 00 00 00 03 00  €   H
0789247140  29 00 00 00 18 00 00 00  54 68 69 73 20 69 73 20  )       This is
0789247150  61 20 66 69 6C 65 20 63  72 65 61 74 65 64 20 66  a file created f
0789247160  6F 72 20 4D 6F 64 75 6C  65 20 33 2E 33 2E 20 0D  or Module 3.3.
0789247170  0A 00 00 00 00 00 00 00  80 00 00 00 48 00 00 00          €   H
0789247180  00 07 18 00 00 00 05 00  1C 00 00 00 28 00 00 00              (
0789247190  73 00 74 00 72 00 65 00  61 00 6D 00 31 00 00 00  s t r e a m 1
07892471A0  54 68 69 73 20 69 73 20  61 20 73 65 63 72 65 74  This is a secret
07892471B0  20 6D 65 73 73 61 67 65  2E 20 0D 0A 00 00 00 00   message.
07892471C0  80 00 00 00 58 00 00 00  01 07 40 00 00 00 09 00  €   X     @
07892471D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
07892471E0  50 00 00 00 00 00 00 00  00 10 00 00 00 00 00 00  P
07892471F0  BF 03 00 00 00 00 00 00  BF 03 00 00 00 00 08 00  ¿       ¿
0789247200  73 00 74 00 72 00 65 00  61 00 6D 00 32 00 00 00  s t r e a m 2
0789247210  41 01 D8 4A 99 00 00 00  FF FF FF FF 82 79 47 11  A ØJ™    ÿÿÿÿ‚yG
0789247220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0789247230  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0789247240  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
Sector 63,214,136 of 461,469,696   Offset:   789247148   = 84  Block:   789247069 - 789247069  Size:   1
```

```
[unregistered]
Drive C:                 8% free
File system:                NTFS
Volume label:                 OS
Read-only mode

Alloc. of visible drive space
Cluster No.:           7,901,767
                 $MFT (#256952)
Users\kaiwe\Desk...\file.txt
Snapshot taken     39 min. ago
Logical sector No.:   63,214,136
Physical sector No.:  63,990,328

Used space:               203 GB
         218,038,525,952 bytes
Free space:              17.0 GB
          18,233,954,304 bytes
Total capacity:           220 GB
         236,272,484,352 bytes

Bytes per cluster:         4,096
Free clusters:         4,451,649
Total clusters:       57,683,711
Bytes per sector:            512
Sector count:        461,469,696
Physical disk:                 0

Mode:                hexadecimal
Offsets:             hexadecimal
Bytes per page      37x16=592
Window #:                      1
Window count:                  1
```

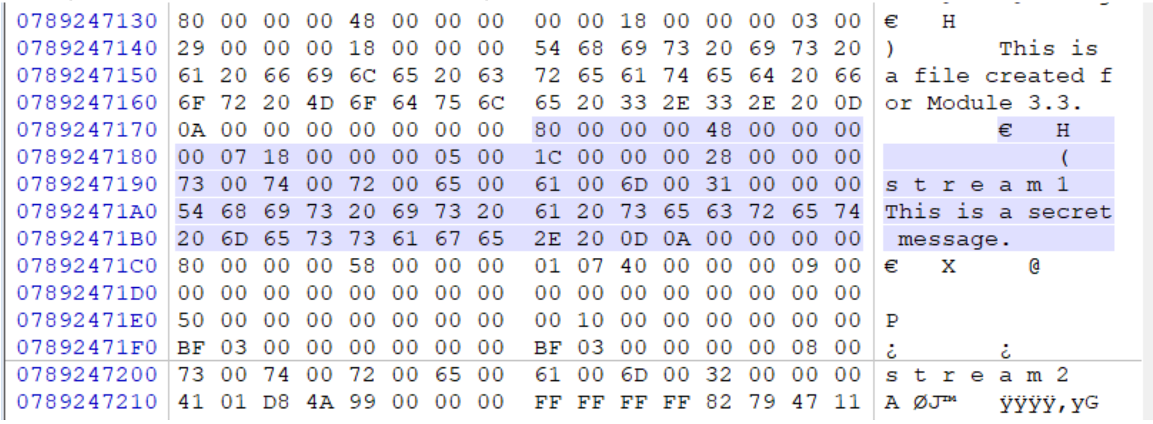
10. Find the attribute 0x80.

After the attribute 0x40, there is the first attribute 0x80. The first one contains the message that stored when created the file.txt.



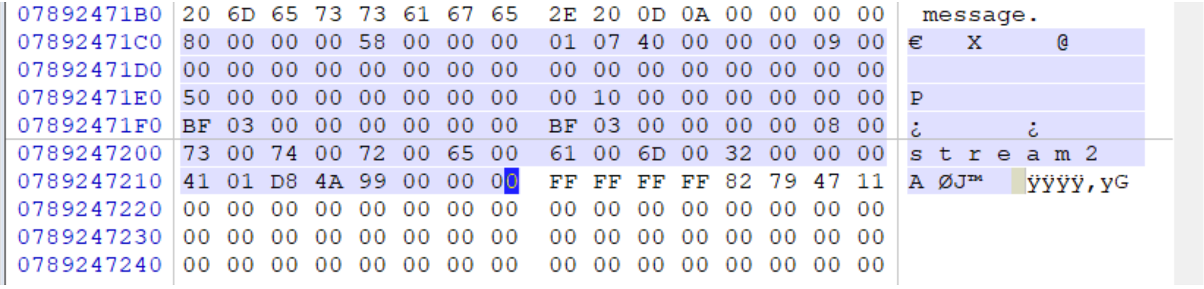
```
Offset       0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
0789247000  46 49 4C 45 30 00 03 00  19 56 11 E7 04 00 00 00  FILE0    V ç
0789247010  09 00 01 00 38 00 01 00  20 02 00 00 00 04 00 00      8
0789247020  00 00 00 00 00 00 00 00  0A 00 00 00 B8 EB 03 00              ¸ë
0789247030  08 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00
0789247040  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
0789247050  90 DA 43 27 DF B4 D8 01  C9 8A CA 42 E3 B4 D8 01   ÚC'ß´Ø ÉŠÊBã´Ø
0789247060  C9 8A CA 42 E3 B4 D8 01  23 9C E2 42 E3 B4 D8 01  ÉŠÊBã´Ø #œâBã´Ø
0789247070  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0789247080  00 00 00 00 8C 18 00 00  00 00 00 00 00 00 00 00      Œ
0789247090  18 DD B6 63 01 00 00 00  30 00 00 00 70 00 00 00   Ý¶c    0   p
07892470A0  00 00 00 00 00 00 02 00  52 00 00 00 18 00 01 00          R
07892470B0  B9 E9 00 00 00 00 12 00  90 DA 43 27 DF B4 D8 01  ¹é       ÚC'ß´Ø
07892470C0  90 DA 43 27 DF B4 D8 01  90 DA 43 27 DF B4 D8 01   ÚC'ß´Ø  ÚC'ß´Ø
07892470D0  90 DA 43 27 DF B4 D8 01  00 00 00 00 00 00 00 00   ÚC'ß´Ø
07892470E0  00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
07892470F0  08 00 66 00 69 00 6C 00  65 00 2E 00 74 00 78 00    f i l e . t x
0789247100  74 00 00 00 00 00 00 00  40 00 00 00 28 00 00 00  t       @   (
0789247110  00 00 00 00 00 00 04 00  10 00 00 00 18 00 00 00
0789247120  53 49 66 AB 83 1F ED 11  B7 83 CC 6B 1E 59 B3 6A  SIf«ƒ í ·ƒÌk Y³j
0789247130  80 00 00 00 48 00 00 00  00 00 18 00 00 00 03 00  €   H
0789247140  29 00 00 00 18 00 00 00  54 68 69 73 20 69 73 20  )       This is
0789247150  61 20 66 69 6C 65 20 63  72 65 61 74 65 64 20 66  a file created f
0789247160  6F 72 20 4D 6F 64 75 6C  65 20 33 2E 33 2E 20 0D  or Module 3.3.
0789247170  0A 00 00 00 00 00 00 00  80 00 00 00 48 00 00 00          €   H
0789247180  00 07 18 00 00 00 05 00  1C 00 00 00 28 00 00 00              (
0789247190  73 00 74 00 72 00 65 00  61 00 6D 00 31 00 00 00  s t r e a m 1
07892471A0  54 68 69 73 20 69 73 20  61 20 73 65 63 72 65 74  This is a secret
07892471B0  20 6D 65 73 73 61 67 65  2E 20 0D 0A 00 00 00 00   message.
07892471C0  80 00 00 00 58 00 00 00  01 07 40 00 00 00 09 00  €   X     @
07892471D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
07892471E0  50 00 00 00 00 00 00 00  00 10 00 00 00 00 00 00  P
07892471F0  BF 03 00 00 00 00 00 00  BF 03 00 00 00 00 08 00  ¿       ¿
0789247200  73 00 74 00 72 00 65 00  61 00 6D 00 32 00 00 00  s t r e a m 2
0789247210  41 01 D8 4A 99 00 00 00  FF FF FF FF 82 79 47 11  A ØJ™    ÿÿÿÿ‚yG
0789247220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

After the first attribute 0x80, there is another attribute 0x80. Since in NTFS, an alternate data stream becomes an additional file attribute, the second attribute 0x80 contains the information of the hidden data stream1. And as shown in the screenshot below, there is another attribute 0x80 and this attribute 0x80 stores stream1, which is the first secret message that we stored in previous steps.
And at offset 0x08, the resident flag is 0x00, therefore, the content of hidden data stream is shown on the right column. “This is a secret message.”



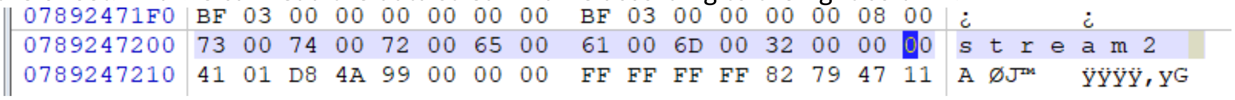
```
0789247130  80 00 00 00 48 00 00 00  00 00 18 00 00 00 03 00  €   H
0789247140  29 00 00 00 18 00 00 00  54 68 69 73 20 69 73 20  )       This is
0789247150  61 20 66 69 6C 65 20 63  72 65 61 74 65 64 20 66  a file created f
0789247160  6F 72 20 4D 6F 64 75 6C  65 20 33 2E 33 2E 20 0D  or Module 3.3.
0789247170  0A 00 00 00 00 00 00 00  80 00 00 00 48 00 00 00          €   H
0789247180  00 07 18 00 00 00 05 00  1C 00 00 00 28 00 00 00              (
0789247190  73 00 74 00 72 00 65 00  61 00 6D 00 31 00 00 00  s t r e a m 1
07892471A0  54 68 69 73 20 69 73 20  61 20 73 65 63 72 65 74  This is a secret
07892471B0  20 6D 65 73 73 61 67 65  2E 20 0D 0A 00 00 00 00   message.
07892471C0  80 00 00 00 58 00 00 00  01 07 40 00 00 00 09 00  €   X     @
07892471D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
07892471E0  50 00 00 00 00 00 00 00  00 10 00 00 00 00 00 00  P
07892471F0  BF 03 00 00 00 00 00 00  BF 03 00 00 00 00 08 00  ¿       ¿
0789247200  73 00 74 00 72 00 65 00  61 00 6D 00 32 00 00 00  s t r e a m 2
0789247210  41 01 D8 4A 99 00 00 00  FF FF FF FF 82 79 47 11  A ØJ™    ÿÿÿÿ‚yG
```

After the second attribute 0x80, there is another attribute 0x80. The third attribute 0x80 stored the second hidden data stream that we stored. And as shown below, since the size of the second secret message is too large, and at the offset 0x08, the resident flag is 0x01, which means the content of the message cannot be viewed directly. Therefore, we need to find the data run and find the place that stored the message.



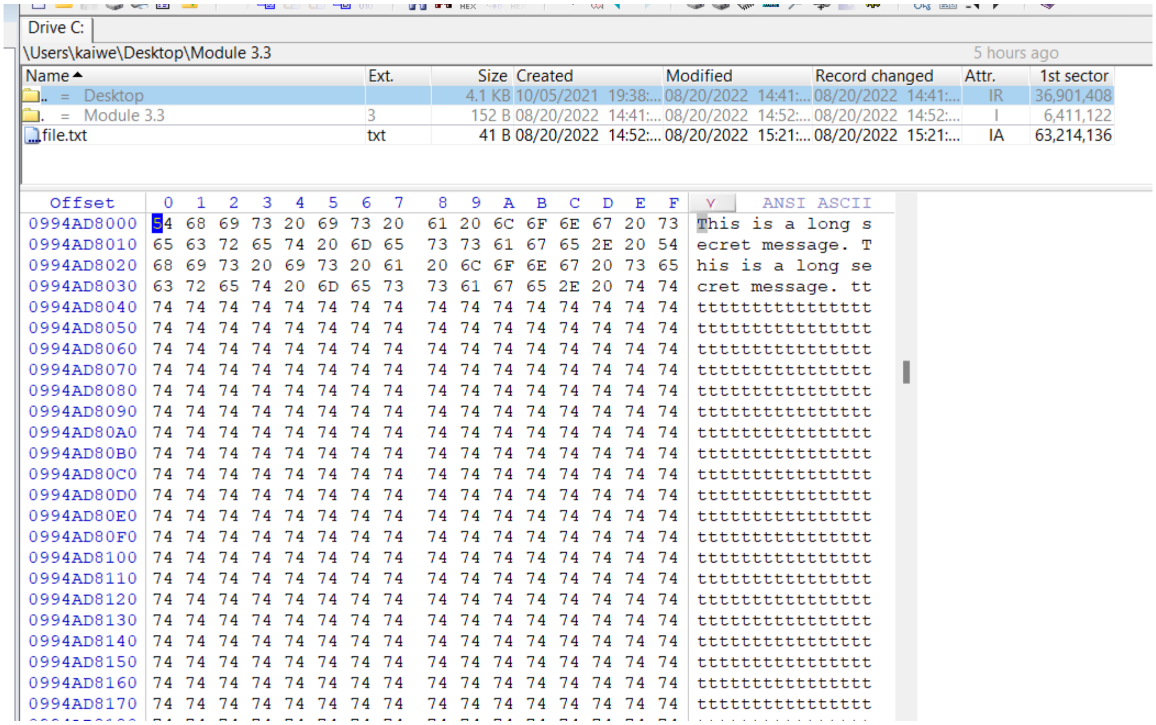
```
07892471B0  20 6D 65 73 73 61 67 65  2E 20 0D 0A 00 00 00 00   message.
07892471C0  80 00 00 00 58 00 00 00  01 07 40 00 00 00 09 00  €   X     @
07892471D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
07892471E0  50 00 00 00 00 00 00 00  00 10 00 00 00 00 00 00  P
07892471F0  BF 03 00 00 00 00 00 00  BF 03 00 00 00 00 08 00  ¿       ¿
0789247200  73 00 74 00 72 00 65 00  61 00 6D 00 32 00 00 00  s t r e a m 2
0789247210  41 01 D8 4A 99 00 00 00  FF FF FF FF 82 79 47 11  A ØJ™    ÿÿÿÿ‚yG
0789247220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0789247230  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0789247240  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

11. Find the second hidden message.
As shown in the previous screenshot, the start offset for the third attribute 0x80 is 0x07892471C0. At the offset 0x40, is the start of the data run. From offset 0x0789247200 to 0x078924720F, is the name of the offset. And we can read the data stream name according to the right column.



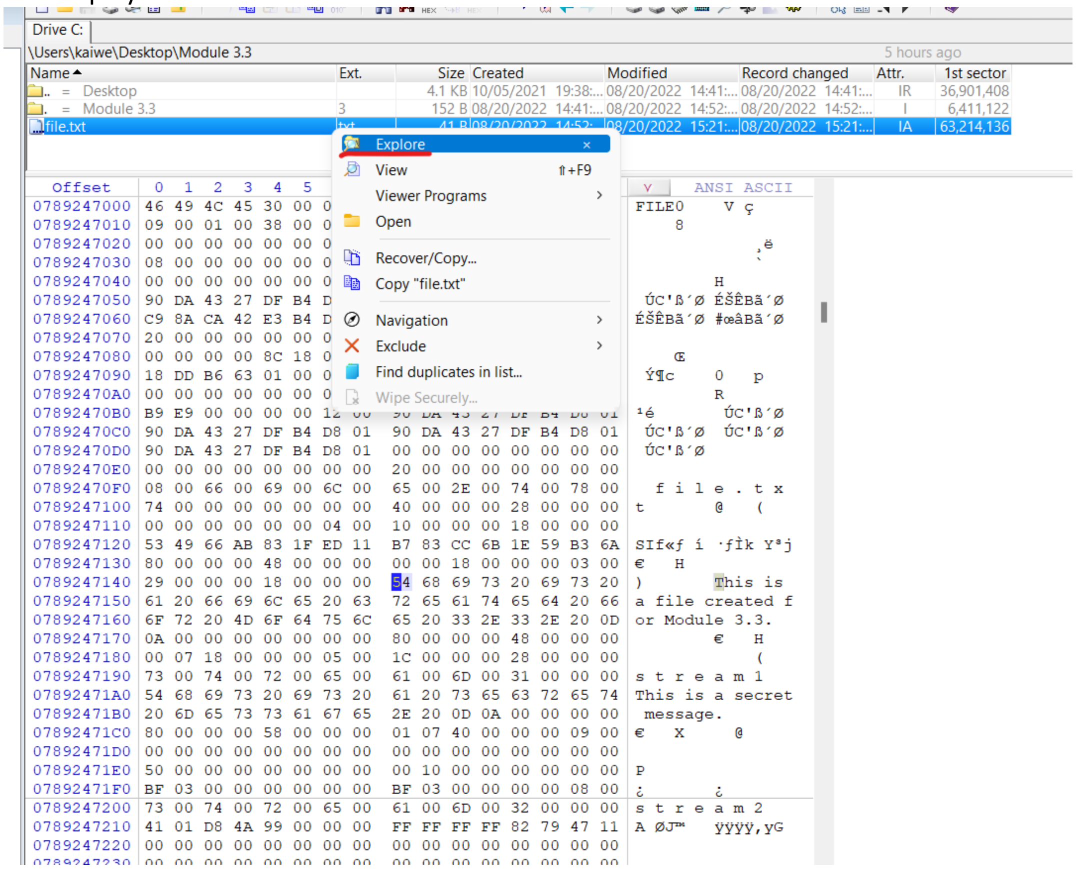
```
07892471F0  BF 03 00 00 00 00 00 00  BF 03 00 00 00 00 08 00  ¿       ¿
0789247200  73 00 74 00 72 00 65 00  61 00 6D 00 32 00 00 00  s t r e a m 2
0789247210  41 01 D8 4A 99 00 00 00  FF FF FF FF 82 79 47 11  A ØJ™    ÿÿÿÿ‚yG
```

Offset 0x0789247210 to 0x0789247217 contains the information of the offset. Offset 0x0789247210 is 41, and ‘1’ is the bytes needed to store the number of clusters assigned to this data run. And ‘4’ is the bytes needed to store the LCN address value. Therefore, the offset 0x078924711 is the number of clusters assigned to this data run which is ‘01’. And the starting LCN address is ‘D8 4A 99 00’. Since we are using a hexadecimal editor viewing the MFT record, the data is displayed in little-endian format, after changing ‘D8 4A 99 00’ to big-endian, the LCN address for this data run is ’00 99 4A D8’. And if you go to offset 0x00994AD8, the second secret message is stored there. As shown in the screenshot below.

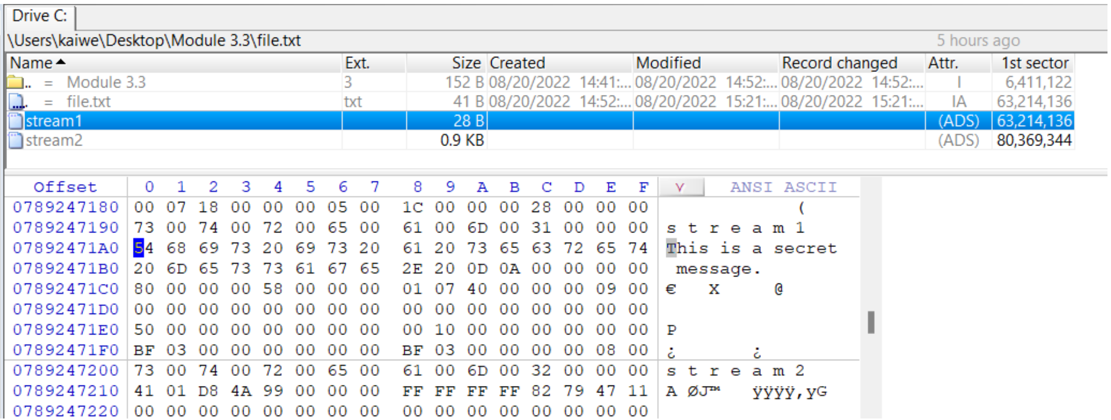


```
Drive C:
\Users\kaiwe\Desktop\Module 3.3                                                   5 hours ago
Name ▲            Ext.   Size   Created             Modified            Record changed      Attr.  1st sector
.. = Desktop             4.1 KB 10/05/2021 19:38:... 08/20/2022 14:41:... 08/20/2022 14:41:... IR     36,901,408
.  = Module 3.3   3      152 B  08/20/2022 14:41:... 08/20/2022 14:52:... 08/20/2022 14:52:... I      6,411,122
file.txt          txt    41 B   08/20/2022 14:52:... 08/20/2022 15:21:... 08/20/2022 15:21:... IA     63,214,136

Offset       0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
0994AD8000  54 68 69 73 20 69 73 20  61 20 6C 6F 6E 67 20 73  This is a long s
0994AD8010  65 63 72 65 74 20 6D 65  73 73 61 67 65 2E 20 54  ecret message. T
0994AD8020  68 69 73 20 69 73 20 61  20 6C 6F 6E 67 20 73 65  his is a long se
0994AD8030  63 72 65 74 20 6D 65 73  73 61 67 65 2E 20 74 74  cret message. tt
0994AD8040  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8050  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8060  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8070  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8080  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8090  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD80A0  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD80B0  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD80C0  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD80D0  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD80E0  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD80F0  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8100  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8110  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8120  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8130  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8140  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8150  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8160  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8170  74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
```

12. Easier way to find the hidden data stream.
Right click **file.txt**, and click **Explore**, then click **stream1** or **stream2**, WinHex will automatically locate and display the stream1 and stream2.



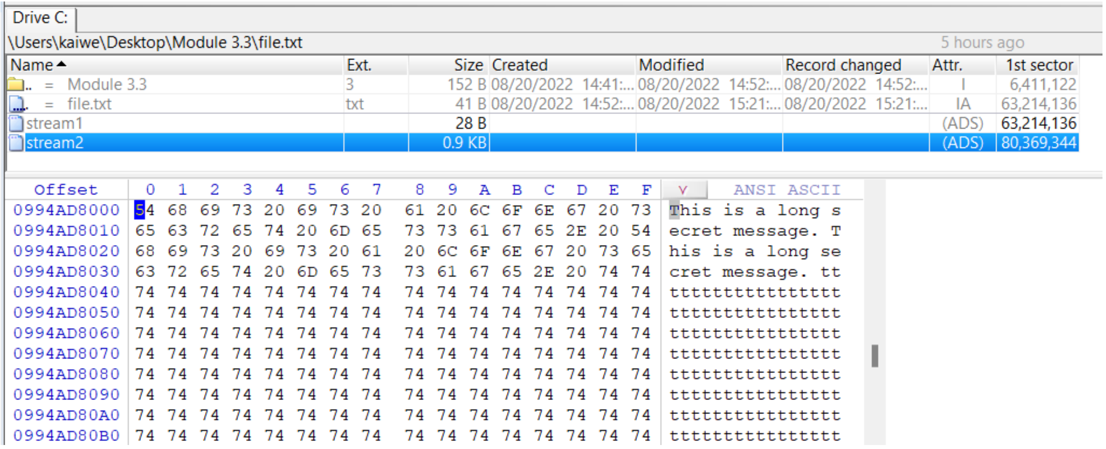
```
Drive C:
\Users\kaiwe\Desktop\Module 3.3                                                   5 hours ago
Name ▲            Ext.   Size   Created             Modified            Record changed      Attr.  1st sector
.. = Desktop             4.1 KB 10/05/2021 19:38:... 08/20/2022 14:41:... 08/20/2022 14:41:... IR     36,901,408
.  = Module 3.3   3      152 B  08/20/2022 14:41:... 08/20/2022 14:52:... 08/20/2022 14:52:... I      6,411,122
file.txt          txt    41 B   08/20/2022 14:52:... 08/20/2022 15:21:... 08/20/2022 15:21:... IA     63,214,136

Offset       0  1  2  3  4  5                                 ANSI ASCII
0789247000  46 49 4C 45 30 00 0                                FILE0    V ç
0789247010  09 00 01 00 38 00 0                                    8
0789247020  00 00 00 00 00 00 0                                          ¸ë
0789247030  08 00 00 00 00 00 0                                          `
0789247040  00 00 00 00 00 00 0                                       H
0789247050  90 DA 43 27 DF B4 D                                 ÚC'ß´Ø ÉŠÊBã´Ø
0789247060  C9 8A CA 42 E3 B4 D                                ÉŠÊBã´Ø #œâBã´Ø
0789247070  20 00 00 00 00 00 0
0789247080  00 00 00 00 8C 18 0                                    Œ
0789247090  18 DD B6 63 01 00 0                                 Ý¶c     0   p
07892470A0  00 00 00 00 00 00 0                                       R
07892470B0  B9 E9 00 00 00 00 12 00  90 DA 43 27 DF B4 D8 01  ¹é        ÚC'ß´Ø
07892470C0  90 DA 43 27 DF B4 D8 01  90 DA 43 27 DF B4 D8 01   ÚC'ß´Ø  ÚC'ß´Ø
07892470D0  90 DA 43 27 DF B4 D8 01  00 00 00 00 00 00 00 00   ÚC'ß´Ø
07892470E0  00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
07892470F0  08 00 66 00 69 00 6C 00  65 00 2E 00 74 00 78 00    f i l e . t x
0789247100  74 00 00 00 00 00 00 00  40 00 00 00 28 00 00 00  t       @   (
0789247110  00 00 00 00 00 00 04 00  10 00 00 00 18 00 00 00
0789247120  53 49 66 AB 83 1F ED 11  B7 83 CC 6B 1E 59 B3 6A  SIf«ƒ í ·ƒÌk Y³j
0789247130  80 00 00 00 48 00 00 00  00 00 18 00 00 00 03 00  €   H
0789247140  29 00 00 00 18 00 00 00  54 68 69 73 20 69 73 20  )       This is
0789247150  61 20 66 69 6C 65 20 63  72 65 61 74 65 64 20 66  a file created f
0789247160  6F 72 20 4D 6F 64 75 6C  65 20 33 2E 33 2E 20 0D  or Module 3.3.
0789247170  0A 00 00 00 00 00 00 00  80 00 00 00 48 00 00 00          €   H
0789247180  00 07 18 00 00 00 05 00  1C 00 00 00 28 00 00 00              (
0789247190  73 00 74 00 72 00 65 00  61 00 6D 00 31 00 00 00  s t r e a m 1
07892471A0  54 68 69 73 20 69 73 20  61 20 73 65 63 72 65 74  This is a secret
07892471B0  20 6D 65 73 73 61 67 65  2E 20 0D 0A 00 00 00 00   message.
07892471C0  80 00 00 00 58 00 00 00  01 07 40 00 00 00 09 00  €   X     @
07892471D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
07892471E0  50 00 00 00 00 00 00 00  00 10 00 00 00 00 00 00  P
07892471F0  BF 03 00 00 00 00 00 00  BF 03 00 00 00 00 08 00  ¿       ¿
0789247200  73 00 74 00 72 00 65 00  61 00 6D 00 32 00 00 00  s t r e a m 2
0789247210  41 01 D8 4A 99 00 00 00  FF FF FF FF 82 79 47 11  A ØJ™    ÿÿÿÿ‚yG
0789247220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```



\Users\kaiwe\Desktop\Module 3.3\file.txt — 5 hours ago

Name ▲	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
.. = Module 3.3	3	152 B	08/20/2022 14:41:...	08/20/2022 14:52:...	08/20/2022 14:52:...	I	6,411,122
. = file.txt	txt	41 B	08/20/2022 14:52:...	08/20/2022 15:21:...	08/20/2022 15:21:...	IA	63,214,136
stream1		28 B				(ADS)	63,214,136
stream2		0.9 KB				(ADS)	80,369,344

```
   Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
0789247180   00 07 18 00 00 00 05 00  1C 00 00 00 28 00 00 00              (
0789247190   73 00 74 00 72 00 65 00  61 00 6D 00 31 00 00 00  s t r e a m 1
07892471A0   54 68 69 73 20 69 73 20  61 20 73 65 63 72 65 74  This is a secret
07892471B0   20 6D 65 73 73 61 67 65  2E 20 0D 0A 00 00 00 00   message.
07892471C0   80 00 00 00 58 00 00 00  01 07 40 00 00 00 09 00  €   X     @
07892471D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
07892471E0   50 00 00 00 00 00 00 00  00 10 00 00 00 00 00 00  P
07892471F0   BF 03 00 00 00 00 00 00  BF 03 00 00 00 00 08 00  ¿       ¿
0789247200   73 00 74 00 72 00 65 00  61 00 6D 00 32 00 00 00  s t r e a m 2
0789247210   41 01 D8 4A 99 00 00 00  FF FF FF FF 82 79 47 11  A ØJ™    ÿÿÿÿ‚yG
0789247220   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```



\Users\kaiwe\Desktop\Module 3.3\file.txt — 5 hours ago

Name ▲	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
.. = Module 3.3	3	152 B	08/20/2022 14:41:...	08/20/2022 14:52:...	08/20/2022 14:52:...	I	6,411,122
. = file.txt	txt	41 B	08/20/2022 14:52:...	08/20/2022 15:21:...	08/20/2022 15:21:...	IA	63,214,136
stream1		28 B				(ADS)	63,214,136
stream2		0.9 KB				(ADS)	80,369,344

```
   Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
0994AD8000   54 68 69 73 20 69 73 20  61 20 6C 6F 6E 67 20 73  This is a long s
0994AD8010   65 63 72 65 74 20 6D 65  73 73 61 67 65 2E 20 54  ecret message. T
0994AD8020   68 69 73 20 69 73 20 61  20 6C 6F 6E 67 20 73 65  his is a long se
0994AD8030   63 72 65 74 20 6D 65 73  73 61 67 65 2E 20 74 74  cret message. tt
0994AD8040   74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8050   74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8060   74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8070   74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8080   74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD8090   74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD80A0   74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
0994AD80B0   74 74 74 74 74 74 74 74  74 74 74 74 74 74 74 74  tttttttttttttttt
```

Questions:

1. How many hidden messages do we append to the file.txt using alternate data stream?

2. How many attribute 0x80 do you find using WinHex?

3. How do you know the first short hidden message is not in the third attribute 0x80?

4. What is the LCN address of the second data run? Please use a screenshot to prove your answer.

5. What is a faster way to help you find the hidden data runs?