Paige Fenwick

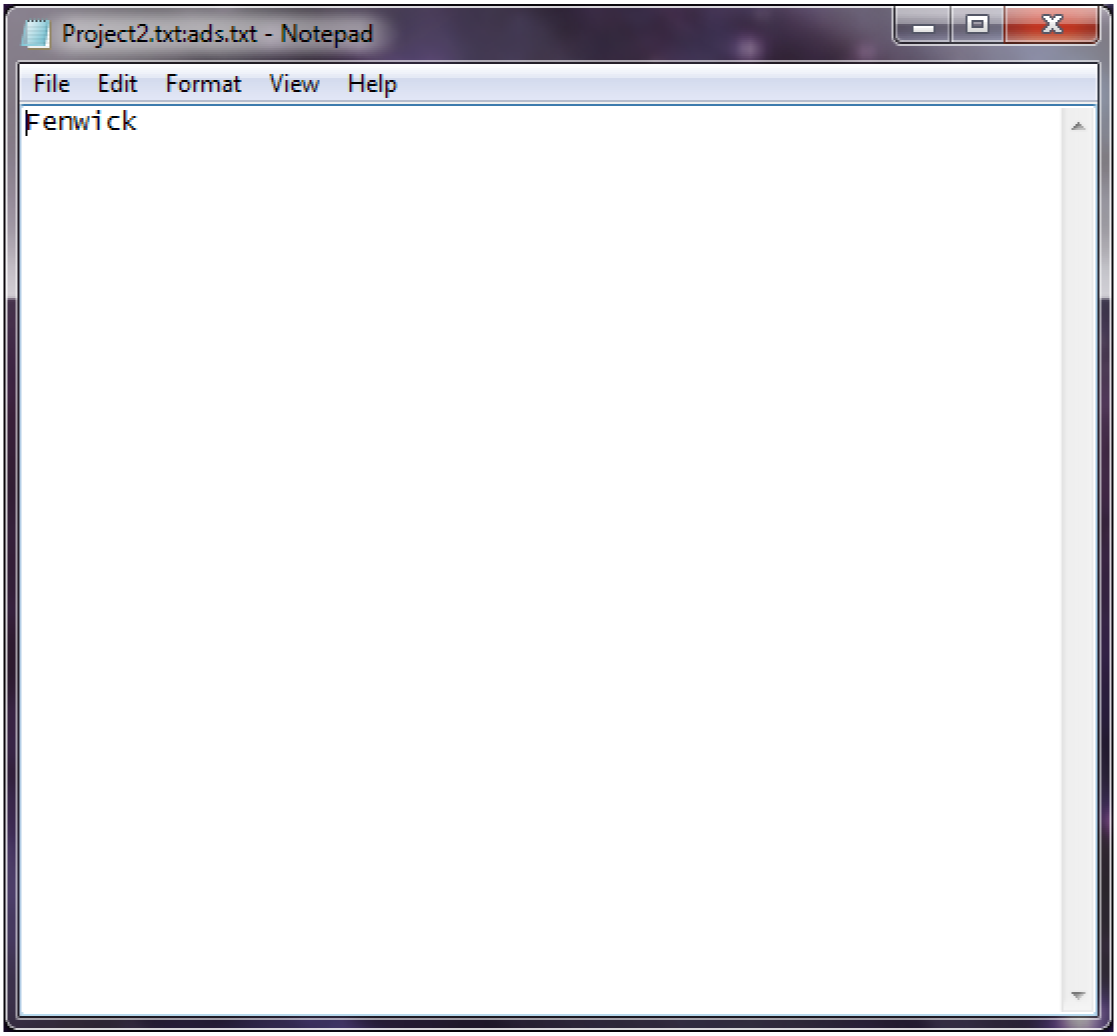
1A

i. The file size for this particular file is 78 bytes and the offset is 100003C.
ii. The creation date and time is 02/24/2016 at 13:24:16 and the offset is 100002E.
iii. The last modified date and time is 02/24/2016 at 13:24:18 and the offset is 1000036.
iv. The last access and time is 02/24/2016 and the offset is 1000030.
v. The starting cluster is 3 and the offset is 100003A.
vi. You cannot determine the last accessed time of the file because

1B

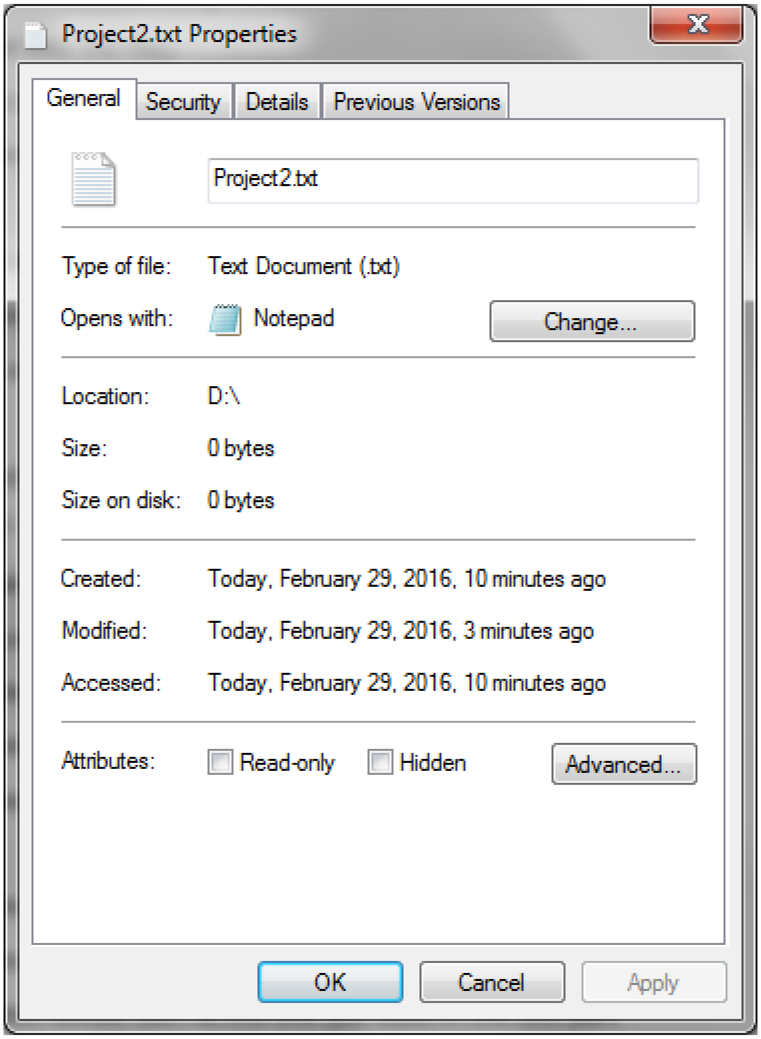
i. The only change within the directory entry was in the 100020 offset, the value was changed to E5 indicating that the file was erased. Everything else was the same.
ii. This would affect a forensic examination because the examiner could see that the file was deleted and could make inferences based on that information.

2A

i. 

Fenwick

ii. The properties window shows that the file is 0 bytes. From this, we can conclude that the data stream is working correctly because the actual data is stored through the data stream and no within the actual file.



Project2.txt

Type of file: Text Document (.txt)

Opens with: Notepad

Location: D:\

Size: 0 bytes

Size on disk: 0 bytes

Created: Today, February 29, 2016, 10 minutes ago

Modified: Today, February 29, 2016, 3 minutes ago

Accessed: Today, February 29, 2016, 10 minutes ago

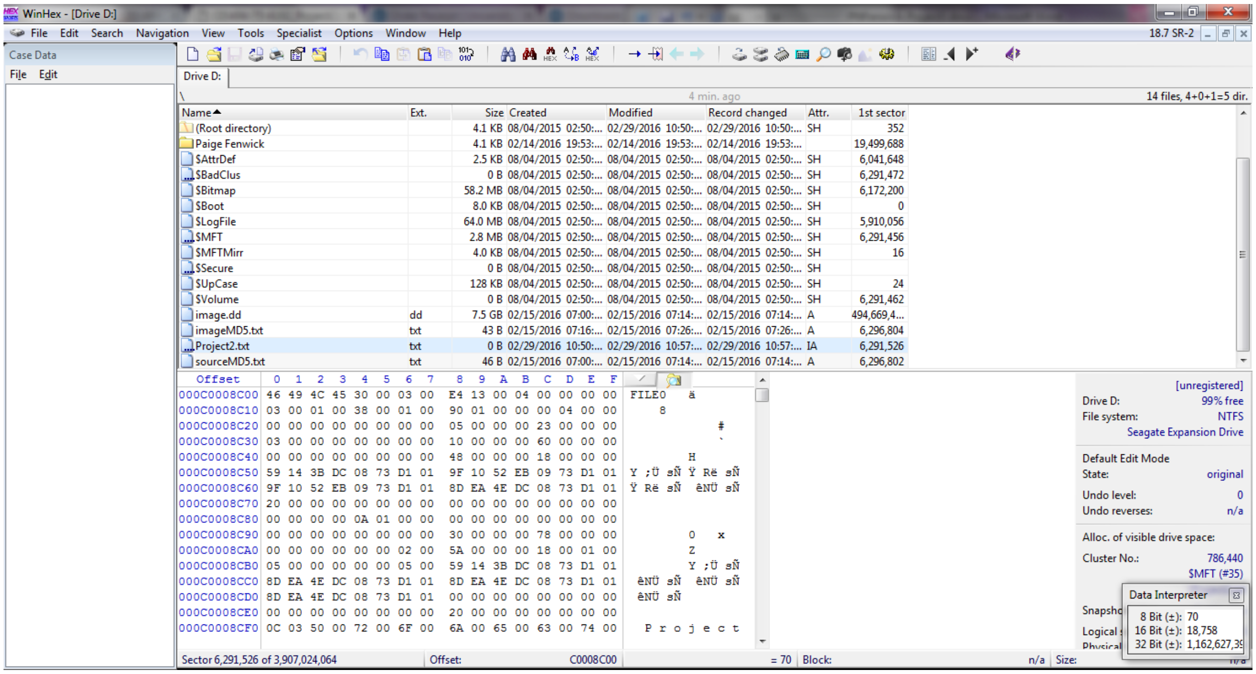
Attributes: ☐ Read-only ☐ Hidden

2B

i. Before the data stream was created, the file didn't indicate that it was FILE0 within WinHex. Now that the data stream has been created, it is indicated as FILE0 which means it is created as a data stream file.

ii. This is important to a forensic investigation because understanding how data streams are creating and how to locate them within a forensic tool such as WinHex will indicate to the examiner that the information is stored in a separate location and more investigation is required to find the information.

iii.


WinHex - [Drive D:]
File Edit Search Navigation View Tools Specialist Options Window Help
18.7 SR-2
Case Data
File Edit
Drive D:

\ 4 min. ago 14 files, 4+0+1=5 dir.

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
(Root directory)		4.1 KB	08/04/2015 02:50:...	02/29/2016 10:50:...	02/29/2016 10:50:...	SH	352
Paige Fenwick		4.1 KB	02/14/2016 19:53:...	02/14/2016 19:53:...	02/14/2016 19:53:...		19,499,688
$AttrDef		2.5 KB	08/04/2015 02:50:...	08/04/2015 02:50:...	08/04/2015 02:50:...	SH	6,041,648
$BadClus		0 B	08/04/2015 02:50:...	08/04/2015 02:50:...	08/04/2015 02:50:...	SH	6,291,472
$Bitmap		58.2 MB	08/04/2015 02:50:...	08/04/2015 02:50:...	08/04/2015 02:50:...	SH	6,172,200
$Boot		8.0 KB	08/04/2015 02:50:...	08/04/2015 02:50:...	08/04/2015 02:50:...	SH	0
$LogFile		64.0 MB	08/04/2015 02:50:...	08/04/2015 02:50:...	08/04/2015 02:50:...	SH	5,910,056
$MFT		2.8 MB	08/04/2015 02:50:...	08/04/2015 02:50:...	08/04/2015 02:50:...	SH	6,291,456
$MFTMirr		4.0 KB	08/04/2015 02:50:...	08/04/2015 02:50:...	08/04/2015 02:50:...	SH	16
$Secure		0 B	08/04/2015 02:50:...	08/04/2015 02:50:...	08/04/2015 02:50:...	SH	
$UpCase		128 KB	08/04/2015 02:50:...	08/04/2015 02:50:...	08/04/2015 02:50:...	SH	24
$Volume		0 B	08/04/2015 02:50:...	08/04/2015 02:50:...	08/04/2015 02:50:...	SH	6,291,462
image.dd	dd	7.5 GB	02/15/2016 07:00:...	02/15/2016 07:14:...	02/15/2016 07:14:...	A	494,669,4...
imageMD5.txt	txt	43 B	02/15/2016 07:16:...	02/15/2016 07:26:...	02/15/2016 07:26:...	A	6,296,804
Project2.txt	txt	0 B	02/29/2016 10:50:...	02/29/2016 10:57:...	02/29/2016 10:57:...	IA	6,291,526
sourceMD5.txt	txt	46 B	02/15/2016 07:00:...	02/15/2016 07:14:...	02/15/2016 07:14:...	A	6,296,802

```
  Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
000C0008C00  46 49 4C 45 30 00 03 00  E4 13 00 04 00 00 00 00  FILE0   ä
000C0008C10  03 00 01 00 38 00 01 00  90 01 00 00 00 04 00 00      8
000C0008C20  00 00 00 00 00 00 00 00  05 00 00 00 23 00 00 00              #
000C0008C30  03 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00              `
000C0008C40  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00          H
000C0008C50  59 14 3B DC 08 73 D1 01  9F 10 52 EB 09 73 D1 01  Y ;Ü sÑ Ÿ Rë sÑ
000C0008C60  9F 10 52 EB 09 73 D1 01  8D EA 4E DC 08 73 D1 01  Ÿ Rë sÑ  êNÜ sÑ
000C0008C70  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000C0008C80  00 00 00 00 0A 01 00 00  00 00 00 00 00 00 00 00
000C0008C90  00 00 00 00 00 00 00 00  30 00 00 00 78 00 00 00          0   x
000C0008CA0  00 00 00 00 00 00 02 00  5A 00 00 00 18 00 01 00          Z
000C0008CB0  05 00 00 00 00 00 05 00  59 14 3B DC 08 73 D1 01          Y ;Ü sÑ
000C0008CC0  8D EA 4E DC 08 73 D1 01  8D EA 4E DC 08 73 D1 01   êNÜ sÑ  êNÜ sÑ
000C0008CD0  8D EA 4E DC 08 73 D1 01  00 00 00 00 00 00 00 00   êNÜ sÑ
000C0008CE0  00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
000C0008CF0  0C 03 50 00 72 00 6F 00  6A 00 65 00 63 00 74 00    P r o j e c t
```

[unregistered]
Drive D: 99% free
File system: NTFS
Seagate Expansion Drive

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

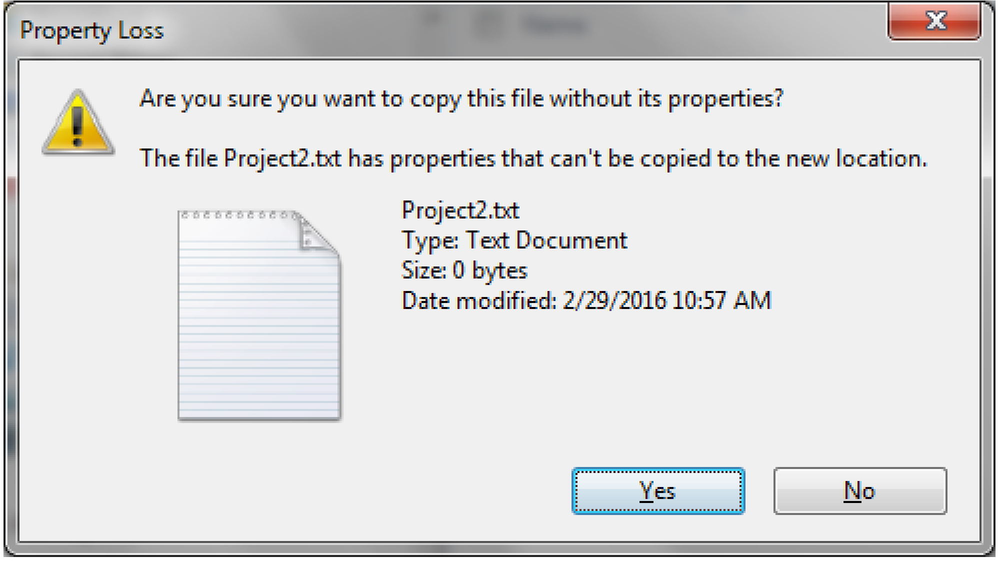
Alloc. of visible drive space:
Cluster No.: 786,440
$MFT (#35)

Data Interpreter
8 Bit (±): 70
16 Bit (±): 18,758
32 Bit (±): 1,162,627,39

Sector 6,291,526 of 3,907,024,064 Offset: C0008C00 = 70 Block: n/a Size: n/a

2C

i. An error message occurred when trying to copy the file over indicating that not all the file properties can be included in the copy and paste.



Property Loss

Are you sure you want to copy this file without its properties?

The file Project2.txt has properties that can't be copied to the new location.

Project2.txt
Type: Text Document
Size: 0 bytes
Date modified: 2/29/2016 10:57 AM

ii. Alternate data streams are only available within NTFS file formats and by copying it into a FAT32 file, not all the properties are available, 3

a. The file is unallocated and the byte offset is 21-22.
b. The record number is 35 and the byte offset is 44-47.
c. The creation date and time is Fri, 21 August 2015 16:57:34 UTC and the byte offset is 80 to 87.
d. The last modified date and time is Sun, 28 December 2014 14:27:24 UTC and the byte offset is 88-95.
e. The record update date and time is Thu, 15 January 2015 00:53:13 UTC and the byte offset is 96-103.
f. The accessed date and time is Sun, 15 February 2015 15:38:41 UTC and the byte offset is 104-111
g. The file name is louisvilleshot.doc and the byte offset is 242-276.
h. Within the MFT record, there are 4 time stamps in the $STANDARD_INFORMATION attribute, which are creation, modified, record update and last accessed. Additionally, within the $FILE_NAME attribute there are creation, modified, record update and last accessed date and time stamps. Altogether, there are 8 time stamps.
i. The starting cluster is 261,337 and the byte offset is 347-349.
j. The file is non-resident and the byte offset is 288.
k. This file has one data attribute beginning at offset 344.
l. The file is fragmented because the file is non-resident. Non-resident indicates that the file is not all stored within this MFT record but within clusters located outside of the record. This is another way of saying that the file is fragmented.
m. This is this the first time the MFT record has been used. The value at byte offset 16-17 starts with 1 indicating this is the first time it's been opened.

4.

Hardware:

- 8GB Ativa Flash Drive
- 2TB Segate Expansion Portable Drive (NTFS drive substitute instead of my C drive)
- Lenovo ThinkPad

Software:

- WinHex
- DCode
- Windows 8
- Notepad