

Richard Patrick

Project 2

Due 2/26/2018

1-A)

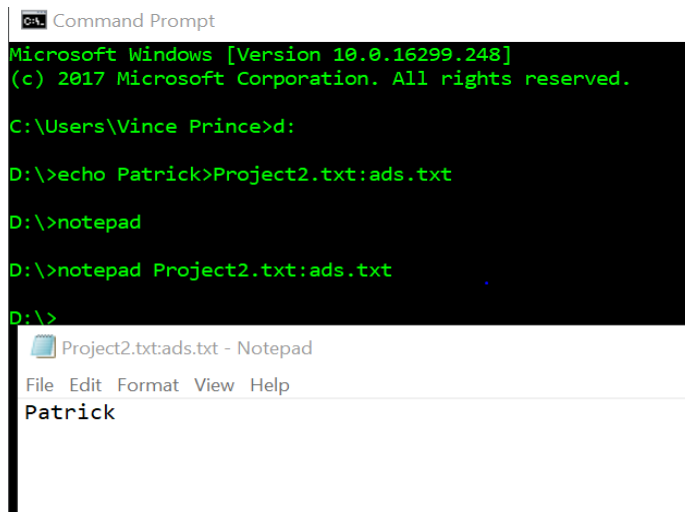
- i. The file size is 82 bytes and is found at the byte offset of 28 relative to the start of the directory entry.
- ii. The creation date and time is 2/20/2018 20:45:46 found at byte offset 13-17
- iii. The last modified date is 2/20/2018 20:44:24 found at byte offset 22-25.
- iv. The last accessed date is 2/20/2018 found at byte offset 18-19.
- v. 0x00 06 00 00 or 393,216 is the starting cluster found at byte offset 20-21 and 26- 27.
- vi. FAT file systems do not have times associated with the last access, only the day. Knowing this can help you distinguish from a NTFS system which does keep tracks of last accessed times.

1-B)

- i. The first hexadecimal or byte offset 0 changed from 46 to E5 while the rest remained the same meaning the file has been deleted.
- ii. E5 will tell the investigator that the file has been deleted. They can use the directory entry of the deleted file to identify the starting cluster and size. You can use the starting cluster number so you know where to start looking for the file on the disk while the file size will tell us how many clusters we need to read beyond the starting cluster. But if the file is not contiguous, it will be difficult to recover because there is no other data structure to tell you where to look for each cluster associated with the file.

2-A)

i.



The screenshot shows a Windows Command Prompt window with the following text:

```
Microsoft Windows [Version 10.0.16299.248]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Vince Prince>d:

D:\>echo Patrick>Project2.txt:ads.txt

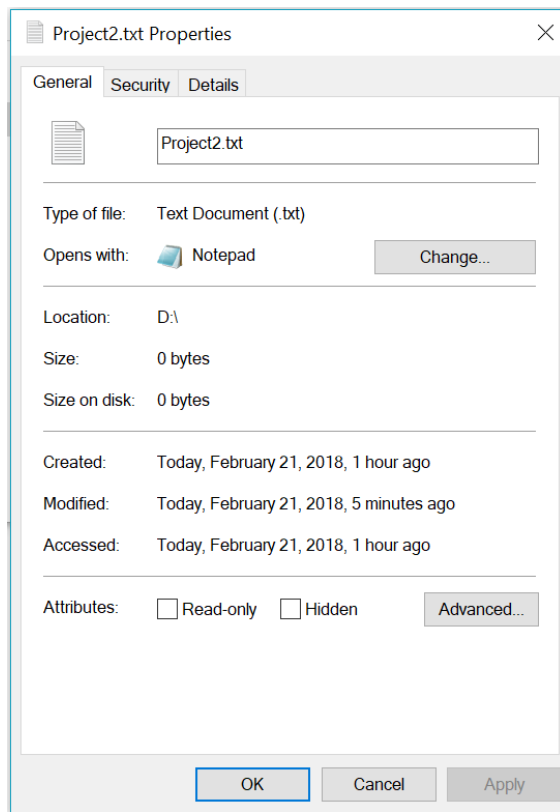
D:\>notepad

D:\>notepad Project2.txt:ads.txt

D:\>
```

Below the Command Prompt, a Notepad window titled "Project2.txt:ads.txt - Notepad" is open, displaying the word "Patrick".

ii.



It shows that the size of the file is 0 bytes and from this I can conclude that the alternate data stream does not affect a file's properties itself, but just appends data that becomes a file attribute which can be identified when analyzing the MFT record.

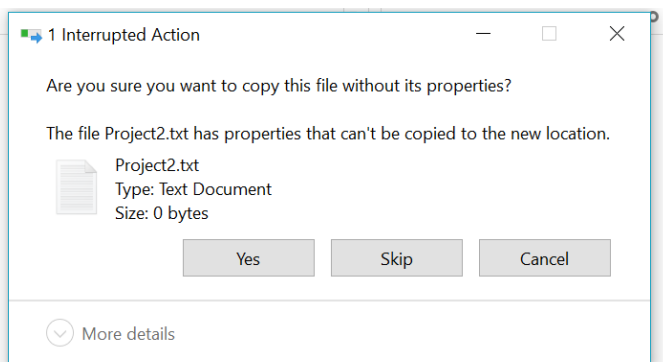
2-B)

- i. There are two 0x80 attributes which shows there is a hidden alternate data stream
- ii. Alternate data streams could provide a forensic investigation additional hidden information about the file but they are difficult to detect and they could be harmful or contain malicious code that hinder the investigation of the file.
- iii.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0C0009CE0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	
0C0009CF0	0C	00	50	00	72	00	6F	00	6A	00	65	00	63	00	74	00	P r o j e c t
0C0009D00	32	00	2E	00	74	00	78	00	74	00	00	00	00	00	00	00	2 . t x t
0C0009D10	40	00	00	00	28	00	00	00	00	00	00	00	00	00	04	00	@ (
0C0009D20	10	00	00	00	18	00	00	00	0B	97	CF	0B	9A	15	E8	11	- ĭ š è
0C0009D30	8E	0C	00	50	56	C0	00	08	80	00	00	00	18	00	00	00	ž PVÀ €
0C0009D40	00	00	18	00	00	00	01	00	00	00	00	00	18	00	00	00	
0C0009D50	80	00	00	00	38	00	00	00	00	07	18	00	00	00	05	00	€ 8
0C0009D60	09	00	00	00	28	00	00	00	61	00	64	00	73	00	2E	00	( a d s .
0C0009D70	74	00	78	00	74	00	00	00	50	61	74	72	69	63	6B	0D	t x t Patrick
0C0009D80	0A	00	00	00	00	00	00	00	FF	FF	FF	FF	82	79	47	11	ÿÿÿÿ,yG
0C0009D90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0C0009DA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0C0009DB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

2-C)

i. I received a message explaining that some of the properties of the file can't be copied to the FAT32 drive.



ii. This message appeared due to the alternate data stream that I made on this text file earlier. It became an attribute of the text file in NTFS but FAT32 does not support alternate data streams, therefore, it could not be carried over.

3-A) The file has been deleted and now unallocated due to the bytes being 00 00 in offset 22- 23.

3-B) The MFT record number is 35 in decimal due to the byte offset in 44-47.

3-C) The date and time created is Fri, 21 Aug 2015 16:57:34. This is found in offset 80-87 relative to the beginning of the MFT record.

3-D) The last modified date and time is Sun, 28 Dec 2014 14:27:24 found in byte offset 88-95.

3-E) The last record update is Thu, 15 Jan 2015 00:53:13 found in byte offset 96-103.

3-F) The last accessed date and time is Sun, 15 Feb 2015 15:38:41 found in byte offset 104-111.

3-G) Louisvilleshot.doc is the name of file found in byte offset 242-276.

3-H) There are 8 timestamps in the MFT record 4 in the \$STANDARD\_INFORMATION section and 4 in the \$FILE\_NAME attribute that are found in byte offset 80-111 and 184-215 respectively.

3-I) 261,337 is the starting cluster due to the data offset 0x03 FC D9. This can be found in byte offset 347-349.

3-J) The content is non-resident found at byte offset 288.

3-K) There are two instances of 0x80, therefore, two data attributes. These are found at byte offset 280 and 352.

3-L) The file is unfragmented because there is only one data run at byte offset 344-349.

3-M) This is the first time the MFT record has been used in the file system due to the sequence number being 1 at byte offset 16. I know this because the sequence number is the number of times the MFT record has been reused. The increment skips 0 and starts at 1 and it is incremented each time the file has been deleted and reallocated. Therefore, since this sequence number is 1, it is the first time the MFT record has been used in the file system.

4) I used an ASUS Zenbook with Windows 10.0.16299 Home along with an 8GB Toshiba flash drive and a 16GB Kingston flash drive. The software I used was WinHex and MFT Stampede.