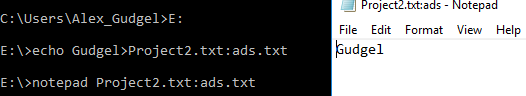
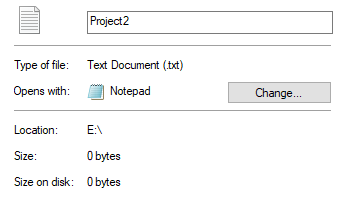
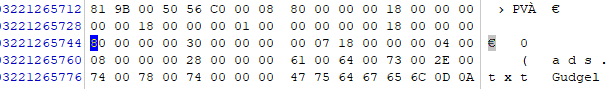
* + 1. The size of the file is 231 bytes. The bytes offset is 28-31.
    2. 02/19/2018, 17:55:34. The bytes offset is 13-17.
    3. 02/19/2018, 18:27:08. The bytes offset is 22-25.
    4. 02/19/2018. The bytes offset is 18-19.
    5. Starting cluster is 6. The bytes offset is 20-21 and 26-27
    6. This is because Windows environments tend to access a newly attached drive without asking, thereby altering the last access dates of some files.
    7. The only part of the directory entry that changed was the first Hex value in the file name changed to E5.
    8. We can use the directory entry of the deleted file to identify the starting cluster and size of the deleted file but since FAT entries are zeroed when a file is deleted, we have no cluster information past the starting cluster. We can read only unallocated clusters after the starting cluster, using the file size as a stopping point.



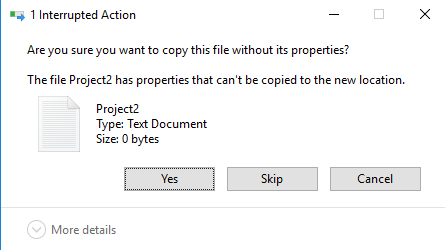
* + 1. The file shows that there are zero bytes in the file or no data but there actually is data in the file. This draws the conclusion that the data is hidden within the file.



* + 1. I can tell the file has an alternative data stream because there are two attribute 0x80 fields.
    2. They might affect a forensic examination because the examiner might not realize that the person being examined is hiding files on their drive.



* + 1. The file was going to be copied with certain properties being left behind.



* + 1. The reason this happens is because FAT file systems do not support ADS.
  1. Unallocated because hex value of 00. Bytes offset 22-23.
  2. Record number 23. Byte offset of 44.
  3. Fri, 21 Aug 2015 16:57:34. Bytes offset 80-87
  4. Sun, 28 Dec 2014 14:27:24. Bytes offset 88-95
  5. Thu, 15 Jan 2015 00:53:13. Bytes offset 96-103
  6. Sun, 15 Feb 2015 15:38:41. Bytes offset 104-111
  7. Louisvilleshot.doc. Bytes offset 241-276
  8. There are 8 timestamps in this file and are in $FILE\_NAME and $STANDARD\_INFORMATION.
  9. The starting cluster is within the data run 32 2D 01 D9 FC 03. Bytes offset 344-349
  10. The content of this file is non-resident because the no-resident flag of 01. Bytes offset 280-288.
  11. Has two data attributes. Bytes offset 280-447.
  12. Yes it is fragmented because there is a data run. Bytes offset 344-349.
  13. Yes it is the first time being used within the file system because the sequence number is 01. Byte offset 16.

Windows10, USB Sandisk, WinHex, Notepad, MFT stampede, HP notebook, command prompt.