1. Number 1
   1. Done
      1. File is 20 bytes, 20 offsets
      2. Creation date/time is 2/3/2020 at 22:03:21, 13 offsets
      3. Last modified date is 2/3/2020 at 22:04:54, 22 offsets
      4. Last accessed day is 2/4/2020, 18 offsets
      5. Start cluster is 0x000008FE, 20 offsets
      6. FAT32 date accessed does not include timestamp
   2. Done
      1. The starting byte is now 0xE5 which in FAT means the file is deleted
      2. E5 tells an examination team that the file was intentionally deleted and does not affect forensic examination past flagging the file as “tampered with”. Clusters past the starting cluster are unallocated but an examination program can still be used to manually look at the bytes, which remain on the disk.
2. Number 2
   1. Done
      1. Screenshot
      2. (Screenshot) Project2.txt has a size of 0 bytes. The ADS isn’t included in the Windows properties of the file.
   2. Dnoe
      1. The MFT starts with 0x80 which means that a second instance of the same file has a data stream.
      2. (Screenshot) ADSs can be used to hide files inside other inconspicuous files (eg, hiding pictures or videos in a word document, hiding encryption keys in photos, hiding emails in text files, etc.) . While easy to find if you’re looking for them, they’re also easy to miss.
   3. Done
      1. I was given a warning with the message “The file Project2.txt has properties that can’t be copied to the new location”
      2. This occurs because FAT does not have ADS capabilities as does NTFS, and Windows is smart enough to know that the ADS files would not be copied over. It still gives me the option to copy the file over though.
3. Number 3
   1. Unallocated
   2. MFT Record Number in Decimal is 11341, offset 44-47
   3. Tue, 14 Aug 2018 04:16:39 range 80-87
   4. Tue, 14 Aug 2018 04:16:40, range 88-95
   5. Tue, 28 Aug 2018 21:43:00 range 96-103
   6. Tue, 14 Aug 2018 04:16:13, range 104-111
   7. 19710002211.pdf, range 362-390
   8. There are 8 timestamps, 4 each for $STANDARD\_INFORMATION and $FILE\_NAME
   9. Starting cluster is 0x00000A00 , range 404-407
   10. Non-resident due to the presence of 0x80
   11. Two
   12. Not fragmented due to the presence of 1 data run
4. Hardware: Surface Laptop 3, Sandisk Cruzer 8GB

Software: Windows 10, WinHex, MFT Stampede, MS Word