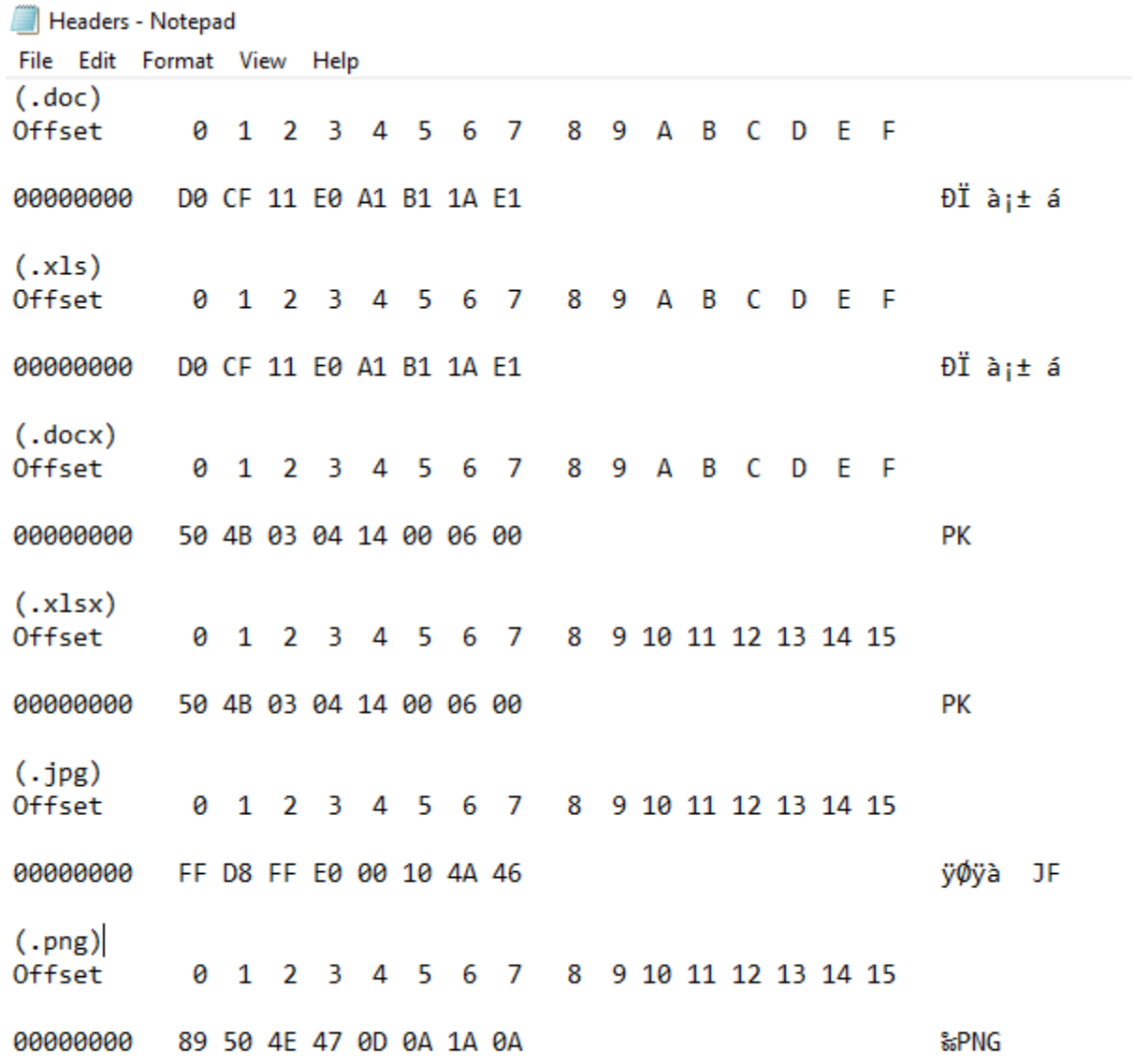
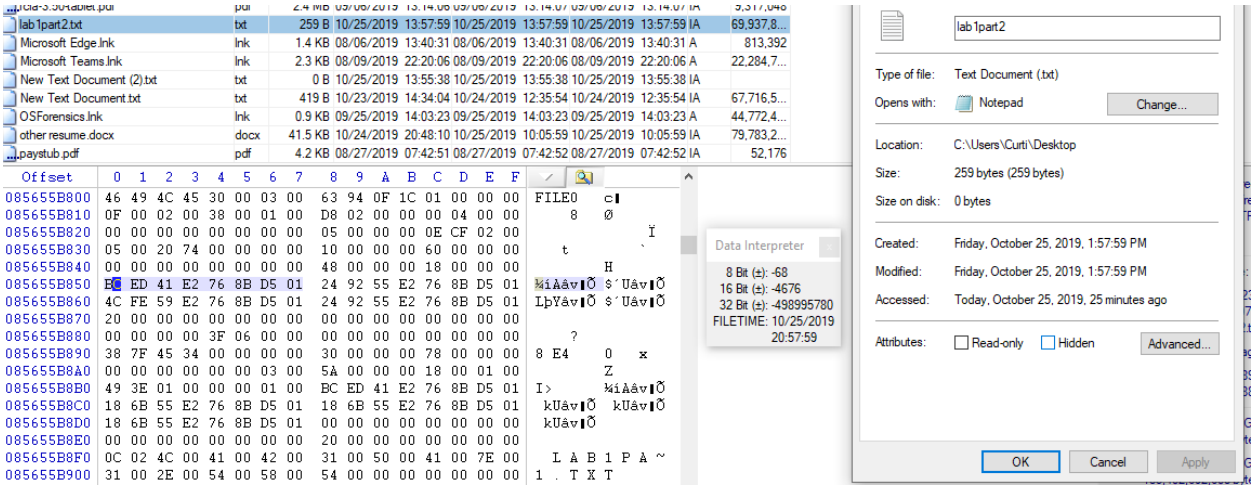
Part 1

Observation – The headers for a certain program are the same. In this case the older format of Microsoft Office programs (doc, xls) have the same header, as do docx and xlsx. The .jpg and .png have different hearers. This would be useful in a forensic investigation because it can narrow down the type of software you might need to interpret some data.

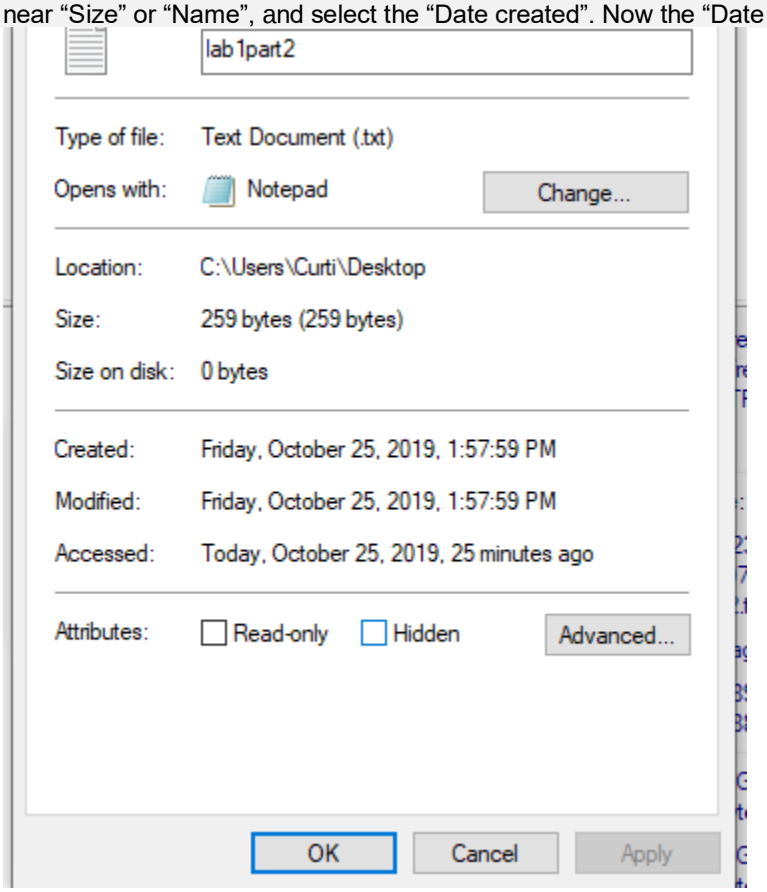


Part 2

1.According to the data interpreter, what is the file create date and time for the file lab1par2t.txt?
According to the data interpreter the file was created at 20:57:59 on 10/25/2019



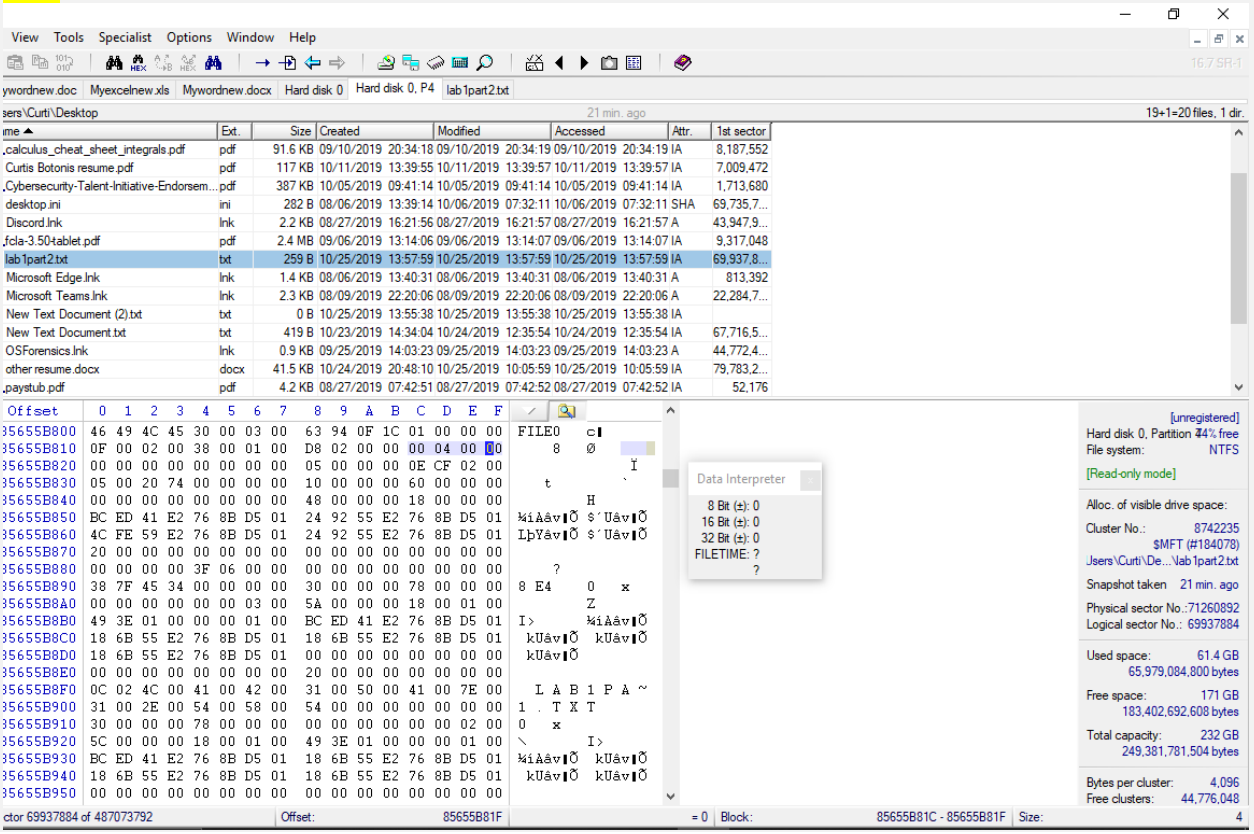
Using File Explorer and go to the folder where the lab1part2.txt located, right click on the arrow near “Size” or “Name”, and select the “Date created”. Now the “Date created” time is also displayed.



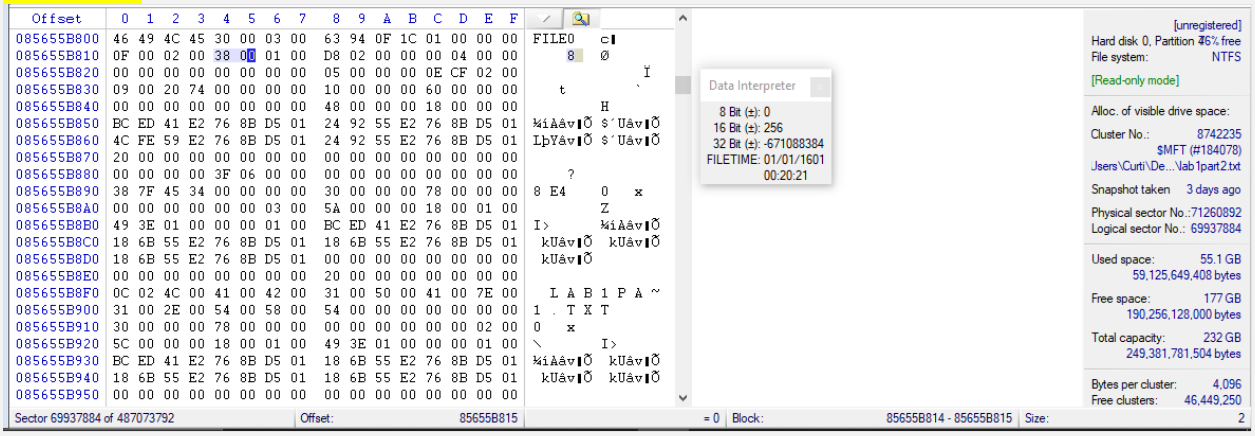
3.Compare this time and the time you got from data interpreter. Are they the same? If not, why (You may google online to get the answer)? The date and time created are different than the actual time created because (see picture below)

X-Ways Forensics employs its own, not Windows' logic to convert UTC timestamps to a freely chosen time zone for display in the directory browser, in report tables and exported lists. It displays timestamps independently of the time zone selected in the examiner's system's Control Panel. The display of timestamps in X-Ways Forensics may differ from Windows because in Windows a timestamp in daylight saving time is not displayed based on daylight saving time if daylight saving time is not active when looking at that timestamp.

4. What is the size of the MFT record? The size of the MFT record is 400 bytes and is located at offset 0x1C to 0x1F

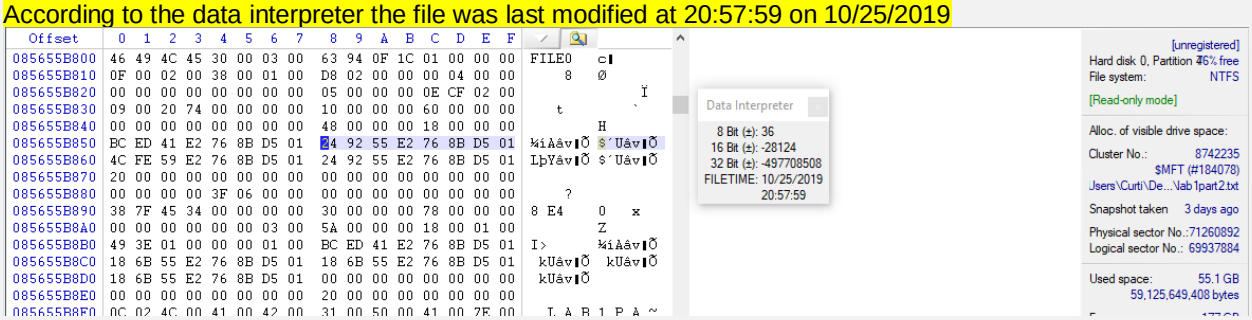


5. What is the length of the header for the MFT record? The length of the header is 38 and is located at offset 0x14 – 0x15

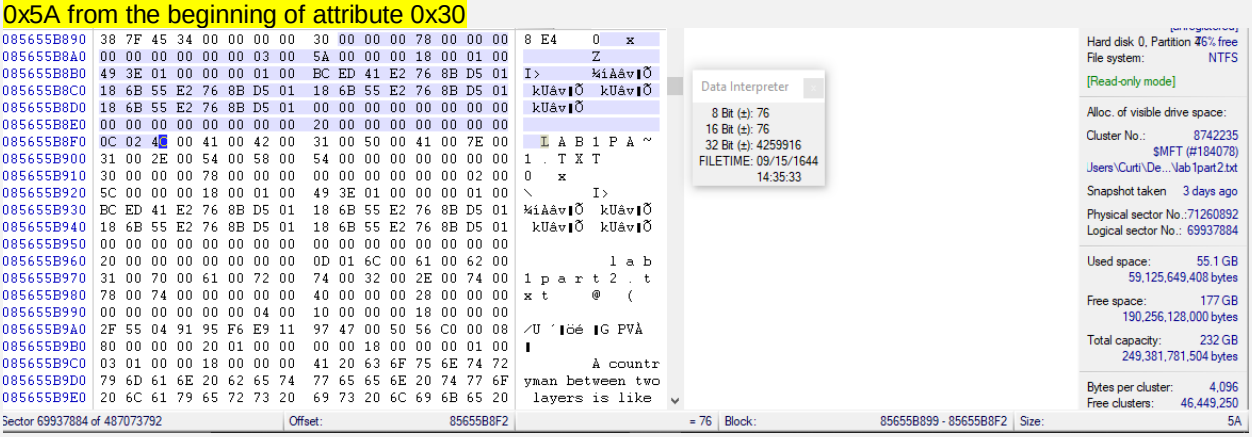


6.What is the file's last modified date and time? Take a screenshot with data interpreter to prove your answer.

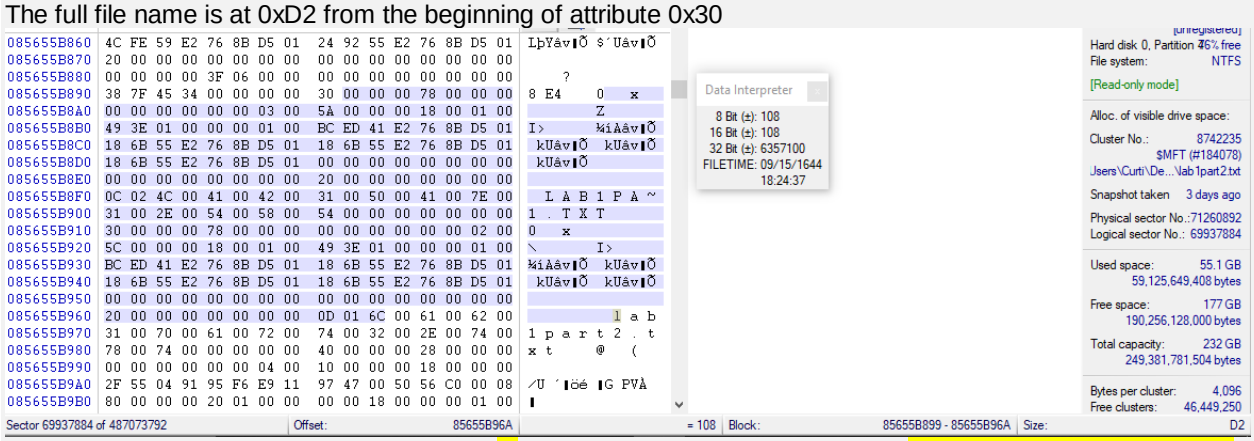
According to the data interpreter the file was last modified at 20:57:59 on 10/25/2019



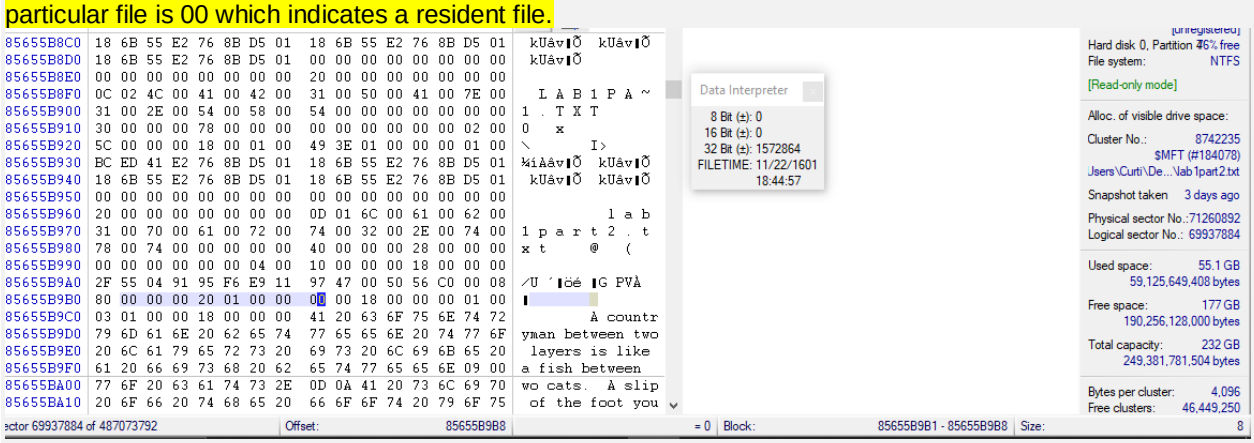
7.What is the file name? In which attribute and at what position can you find it? The short file name is at offset 0x5A from the beginning of attribute 0x30



The full file name is at 0xD2 from the beginning of attribute 0x30



8.Is this file a resident file or nonresident file? Where can you find the evidence? The file is a resident file. You can find the resident/nonresident flag at offset 0x08 from the beginning of the attribute 0x80. The flag for this particular file is 00 which indicates a resident file.



9.In which attribute can you find the data run? Where is the start of the data run? The data run is in attribute 0x80. The start of the data run for the file is located at offset 0x18 from the beginning of attribute 0x80