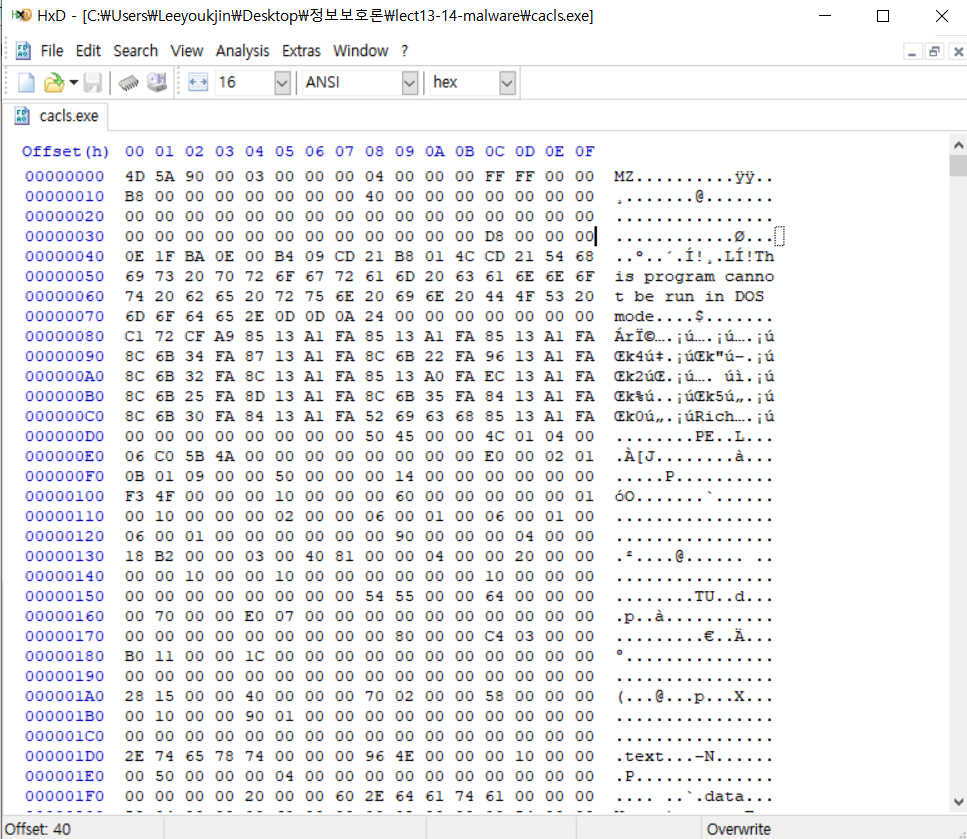
Lect13\_malware\_first

**12141163 이욱진**

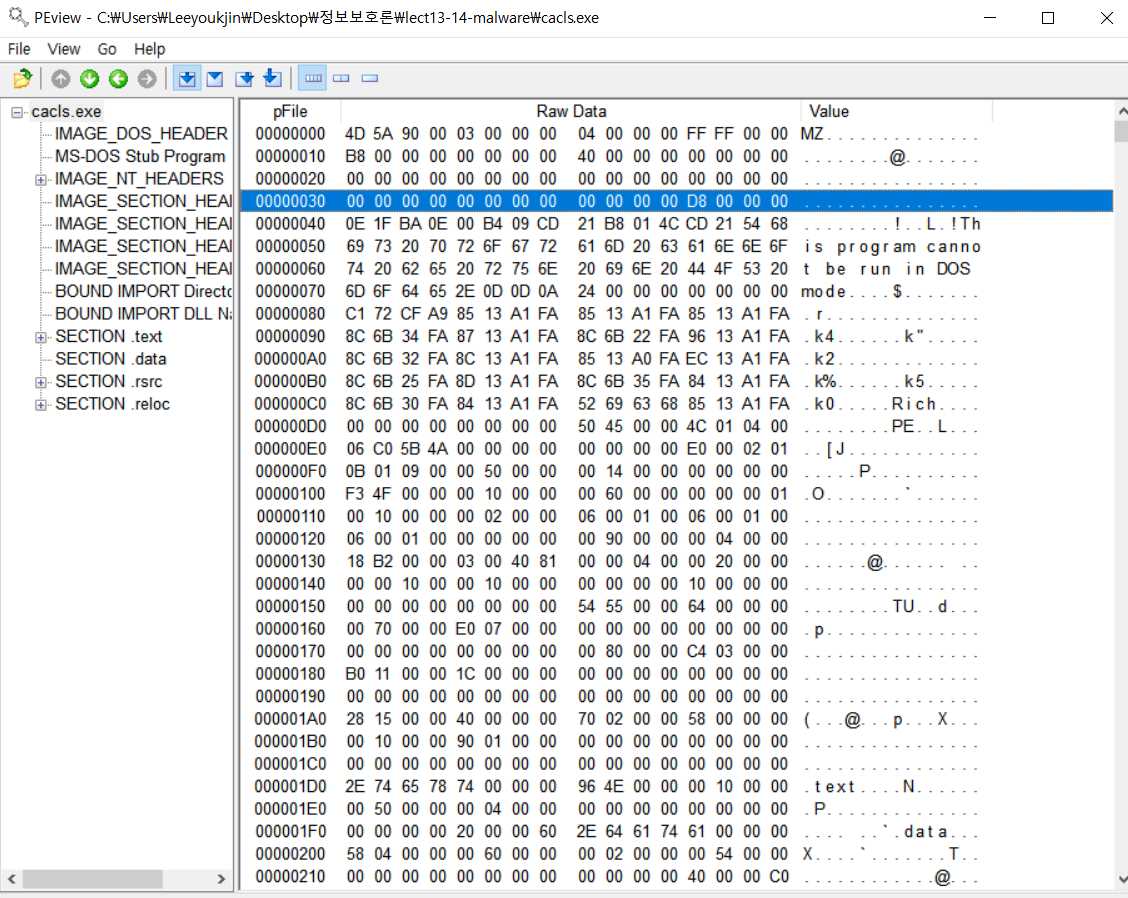
Homework

1) Open cacls.exe with HxD and extract following informtion: e\_lfanew, NumberOfSections, AddressOfEntryPoint, BaseOfCode, BaseOfData, and ImageBase. Check your answer with PEview. (If you are using MacOS, use xxd instead of HxD and skip PEview part.)

HxD를 통하여 cacls.exe 를 열어보았습니다.



이어서 PEview를 통해서도 열어보았고 PEview는 PE format에 맞게 정리되어 나타내고있었습니다.

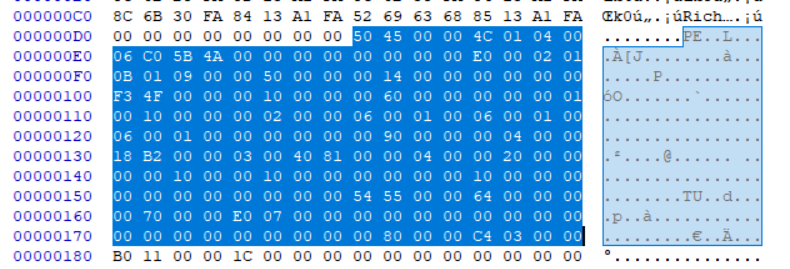


e\_lfanew : 0000003c~3f 까지 존재하였고 000000D8에 nt header가 존재하는 것을 알 수 있었습니다.

<PEview e\_lfanew>

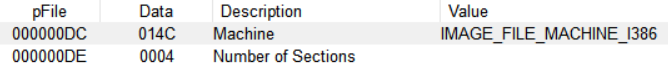


NumberofSections : 아래 사진의 드래그한 부분은 image nt header에대한 부분이고 그 중에서 첫 4바이트는 pe signature(00 00 45 50), machine(01 4C), NumberOfSections(00 04)로 시작했습니다.

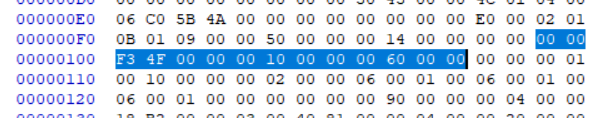


<PEview NumberofSections>





Optional header의 standard fields에서 magic(2 byte), AddressOfEntryPoint(4 byte), BaseOfCode(4 byte), BaseOfData(4 byte)는 아래사진과 같이 찾을 수 있었습니다.



Magic : 00 00

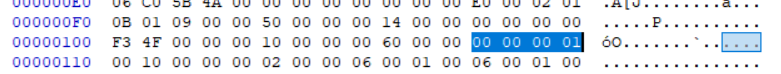
AddressOfEntryPoint: 00 00 4f f3

BaseOfCode : 00 00 10 00

BaseOfData : 00 00 60 00

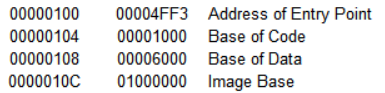
이어서 Optional header의 NT additional fields에서 ImageBase(4 byte)를 찾을 수 있었습니다.

ImageBase : 01 00 00 00



<PEview Optional header>





2) How many sections are there in cacls.exe? Show the name, rva, and file offset of all section.

3) What is the file offset for IMAGE\_DATA\_DIRECTORY array? What is the file offset of the import directory? How many DLLs do you see in the import directory?

4) Show the file offset of OriginalFirstThunk, Name, and FirstThunk for all DLLs in cacls.exe.

5) Go to the file offset you found in 4) and show names, first 5 API names, and first 5 API function addresses (which are yet garbage addresses) for all DLLs in cacls.exe. Do not use PEview for this problem.

6) Repeat 1)-5) for the programs in Sect 10 and 11. Also run the programs and compare the results with your analysis.