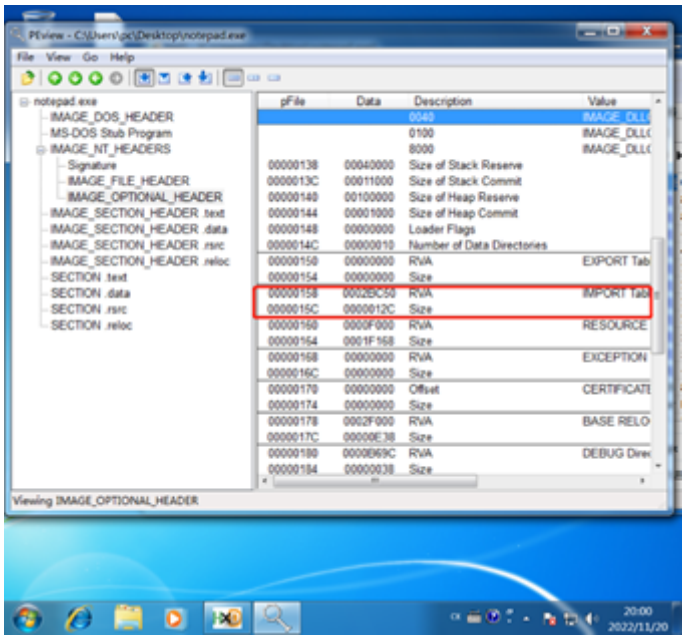
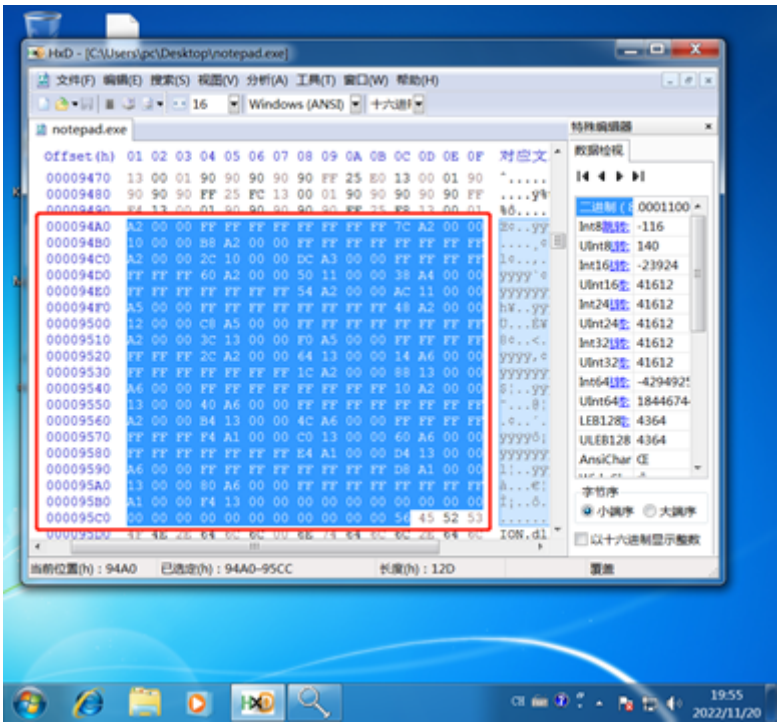
软件逆向上机作业2

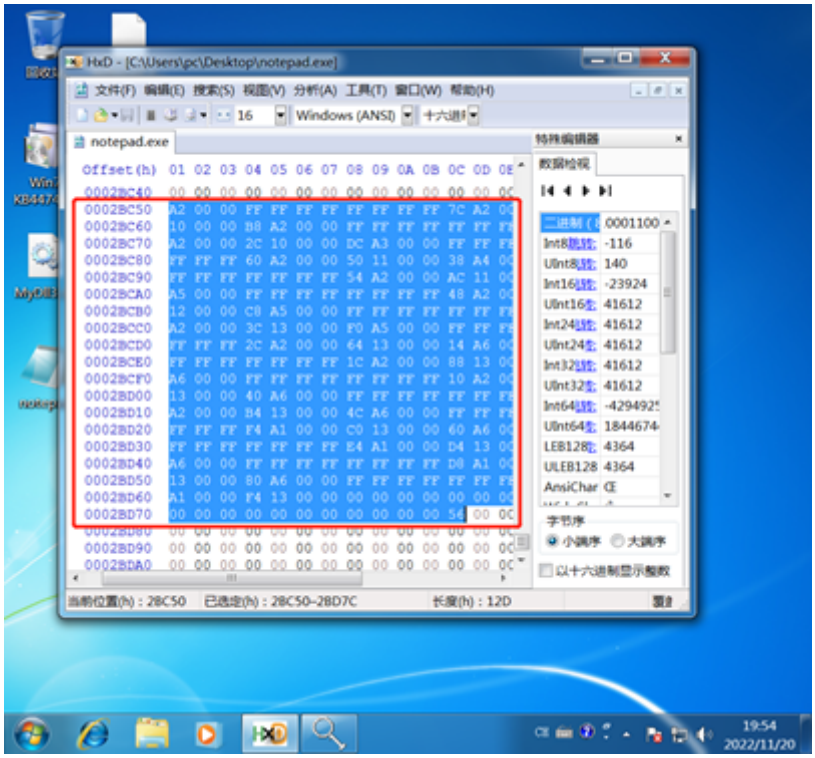
1. 因为装载了 mydll.dll 后导入表会比之前的更长，因此将移动导入表在文件末尾（原导入表长 12CH，新导入表需要加入新的长 20 字节 IMAGE_IMPORT_DESCRIPTOR 结构，所以长 140H）



根据 peview 显示的位置先去对应位置把原导入表的信息复制，再到 .reloc 节区末尾空位置覆盖写入新导入表，此时的大小是 140H。

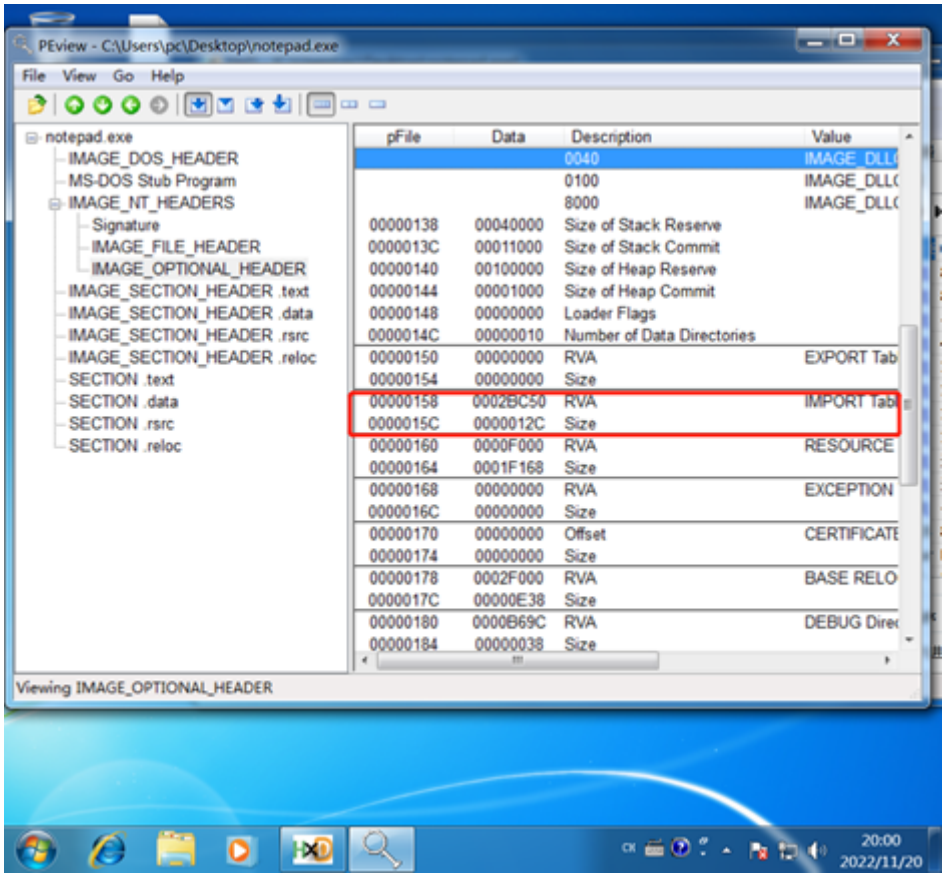
RAW 变化：原表是 94A0H-95CCH，现表是 2BC50H-2BD7CH。



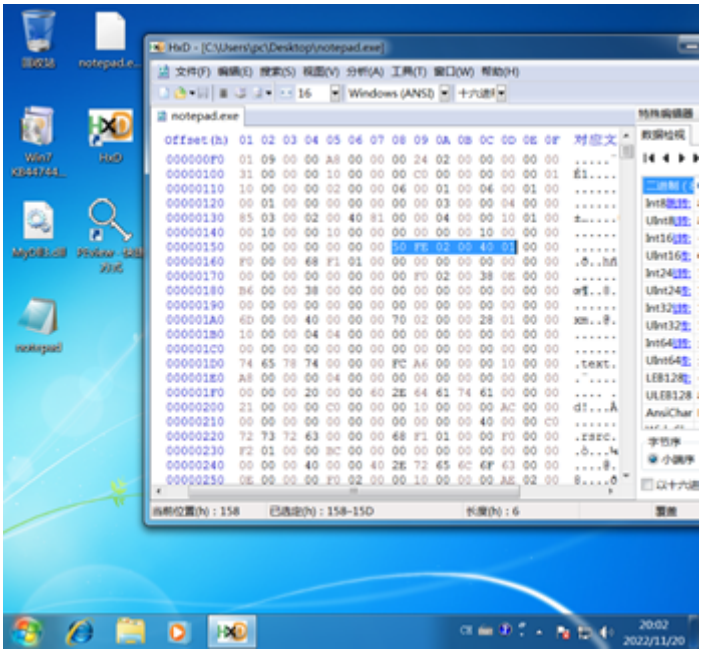


2. 需要修改此时的导入表对应的 DataDirectory[1]：RVA = RAW - RAW.reloc + RVA.reloc = 2BC50H - 2AE00H + 2F000H =2FE50H，size 从 12CH 改为 140H。

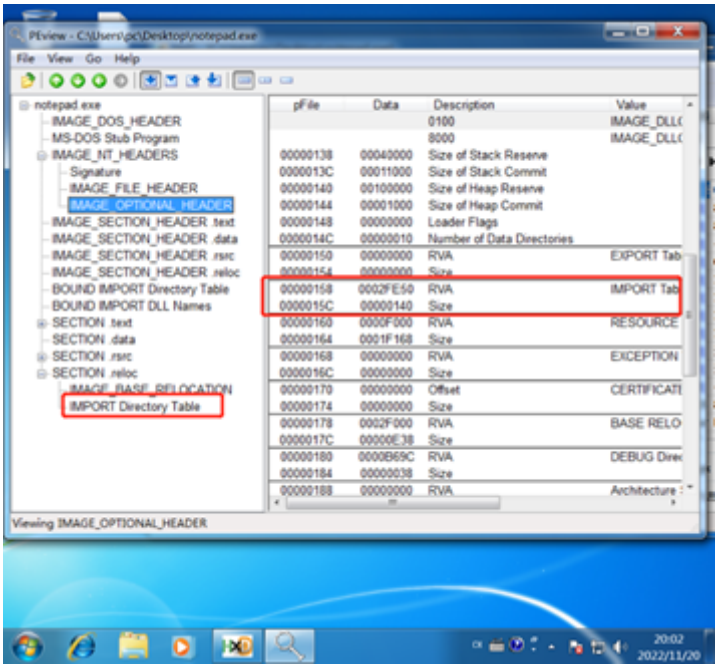
这是修改前的 DataDirectory[1]：



这是修改后的 DataDirectory[1]：



然后就可以在 peview 中看到导入表移到 .reloc 节区末尾了：



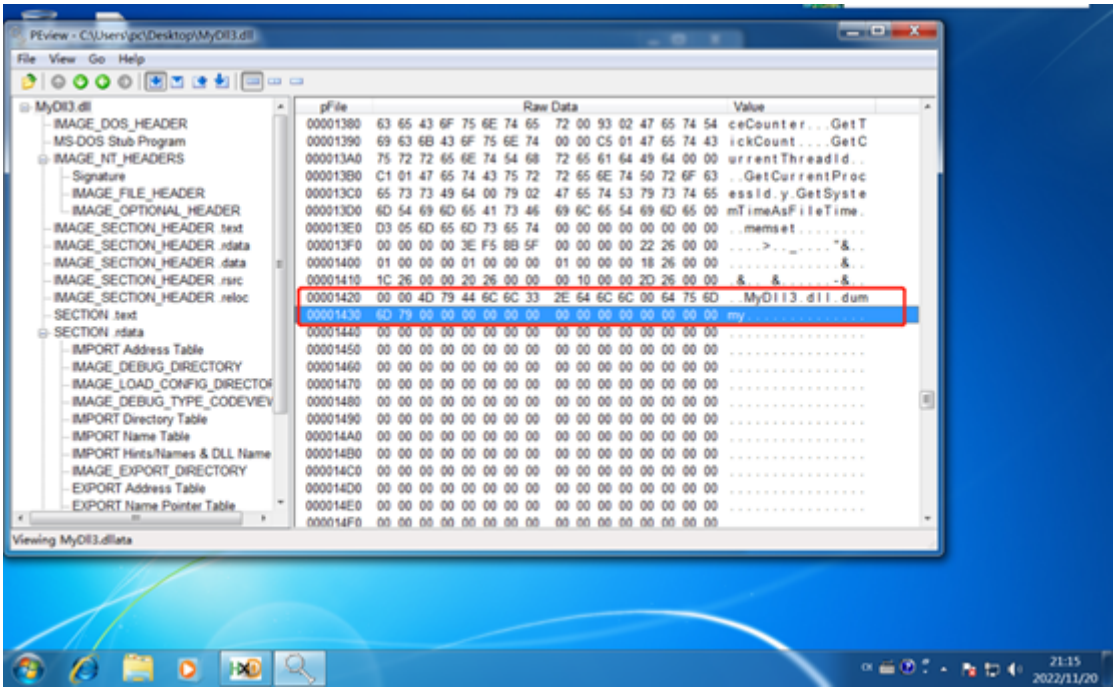
3. 接下来就是向新的 IMAGE_IMPORT_DESCRIPTOR 结构中加入 MyDll3.dll 对应的内容，写入的 RAW 为 2BD68H-2BD7CH。

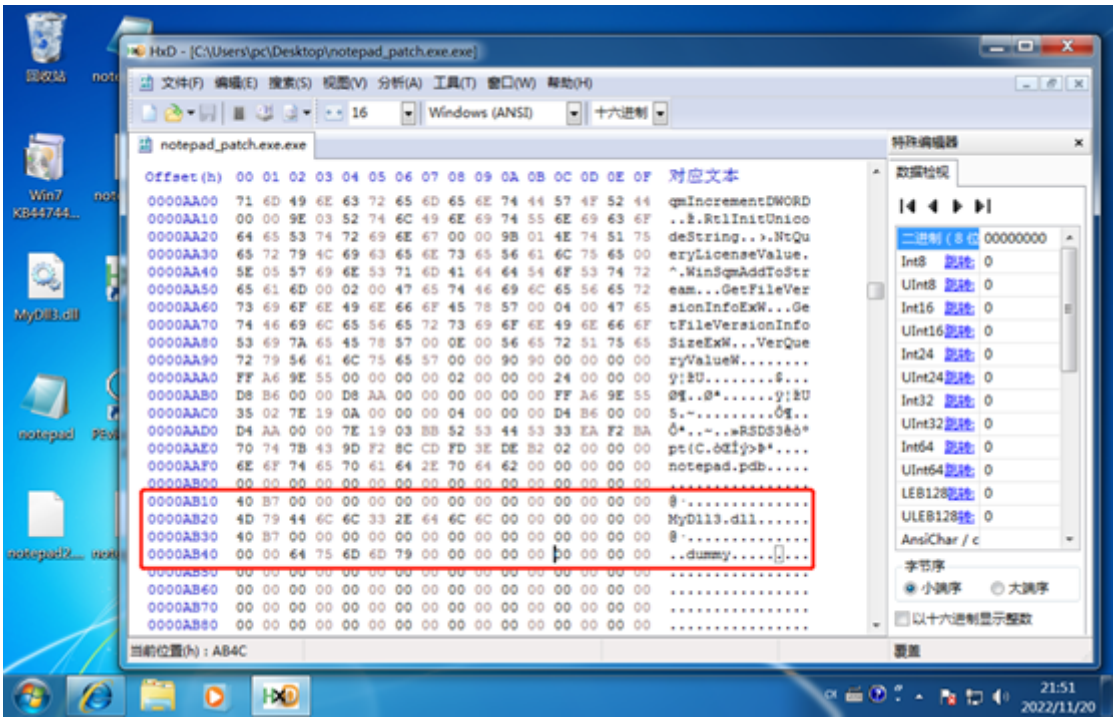
需要在 .text 节区末尾构造 INT，IAT，储存字符串 MyDll3.dll，还有 dummy() 也需要储存。此时 INT，IAT 只有一个结构表示指针，第二个结构为空结构。

RAW：

- INT:AB10H
- My.Dll3.dll：AB20H
- IAT:AB30H
- Dummy()：AB40H

对应内容可以用 peview 找到：





4．然后要计算RVA。

依次为:

INT：AB10H-400H+1000H=B710H

FFFFFFFFH

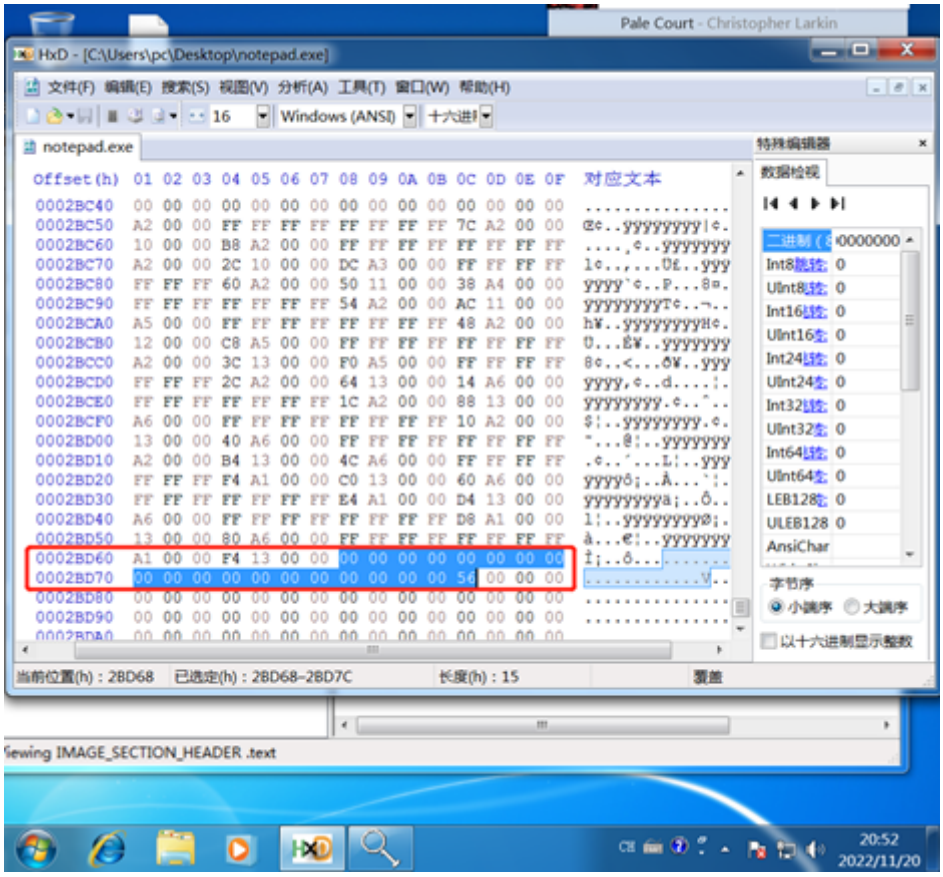
FFFFFFFFH

MyDll3.dll: AB20H-400H+1000H=B720H

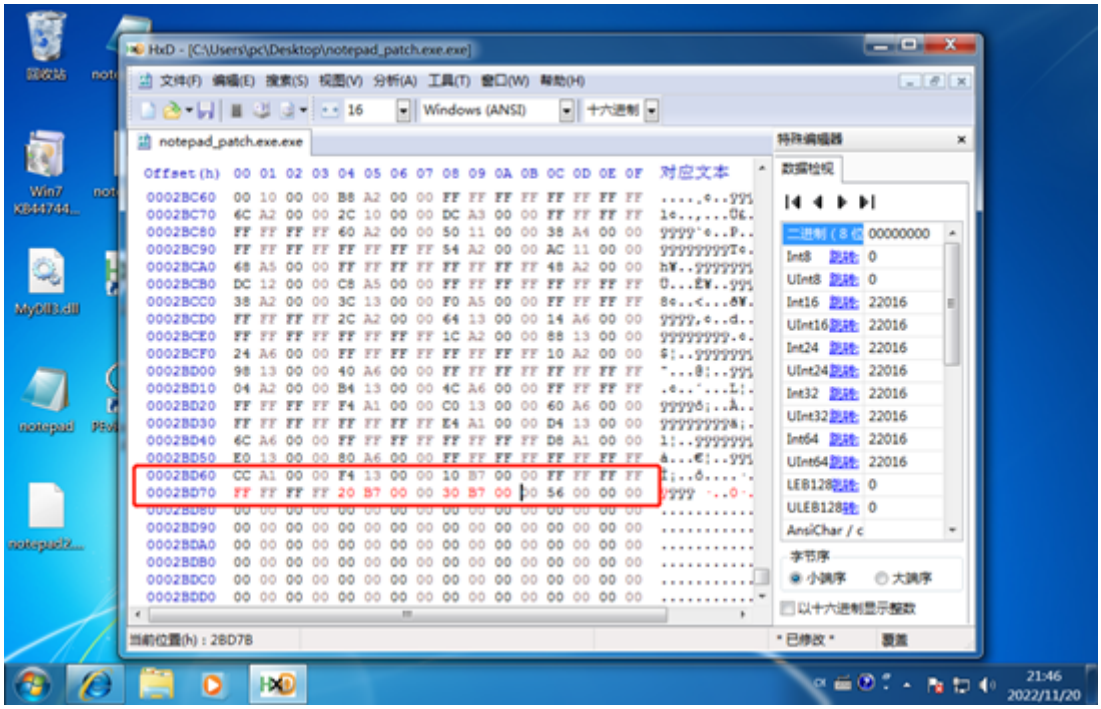
IAT:AB30H-400H+1000H=B730H

Dummy(): AB40H-400H+1000H=B740H

修改前:

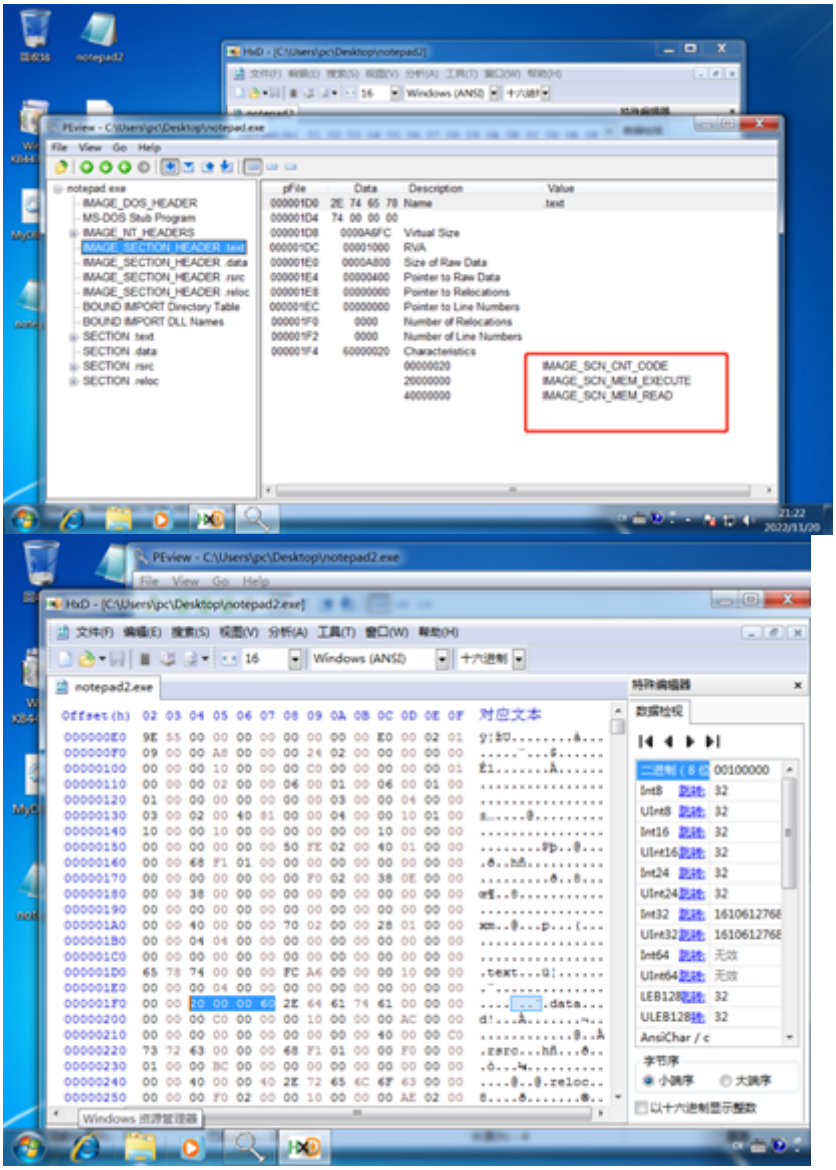


修改之后如下图：

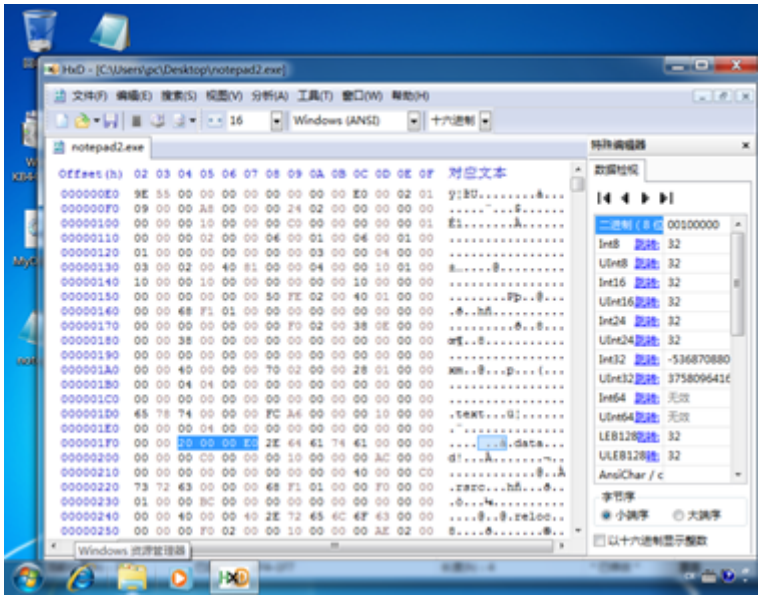


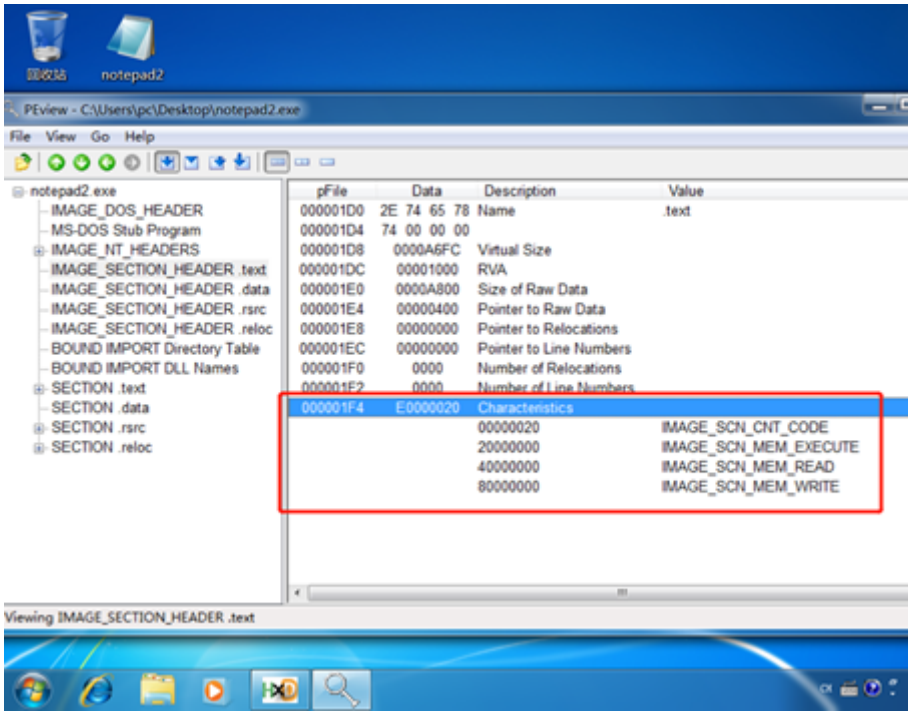
5. 可以看到原来 .text 节区没有 write 权限，但是 pe 文件装载到内存时，装载器修改 IAT 需要 write 权限，所以修改权限值，从 60000020H 改为 E0000020H。

修改前：



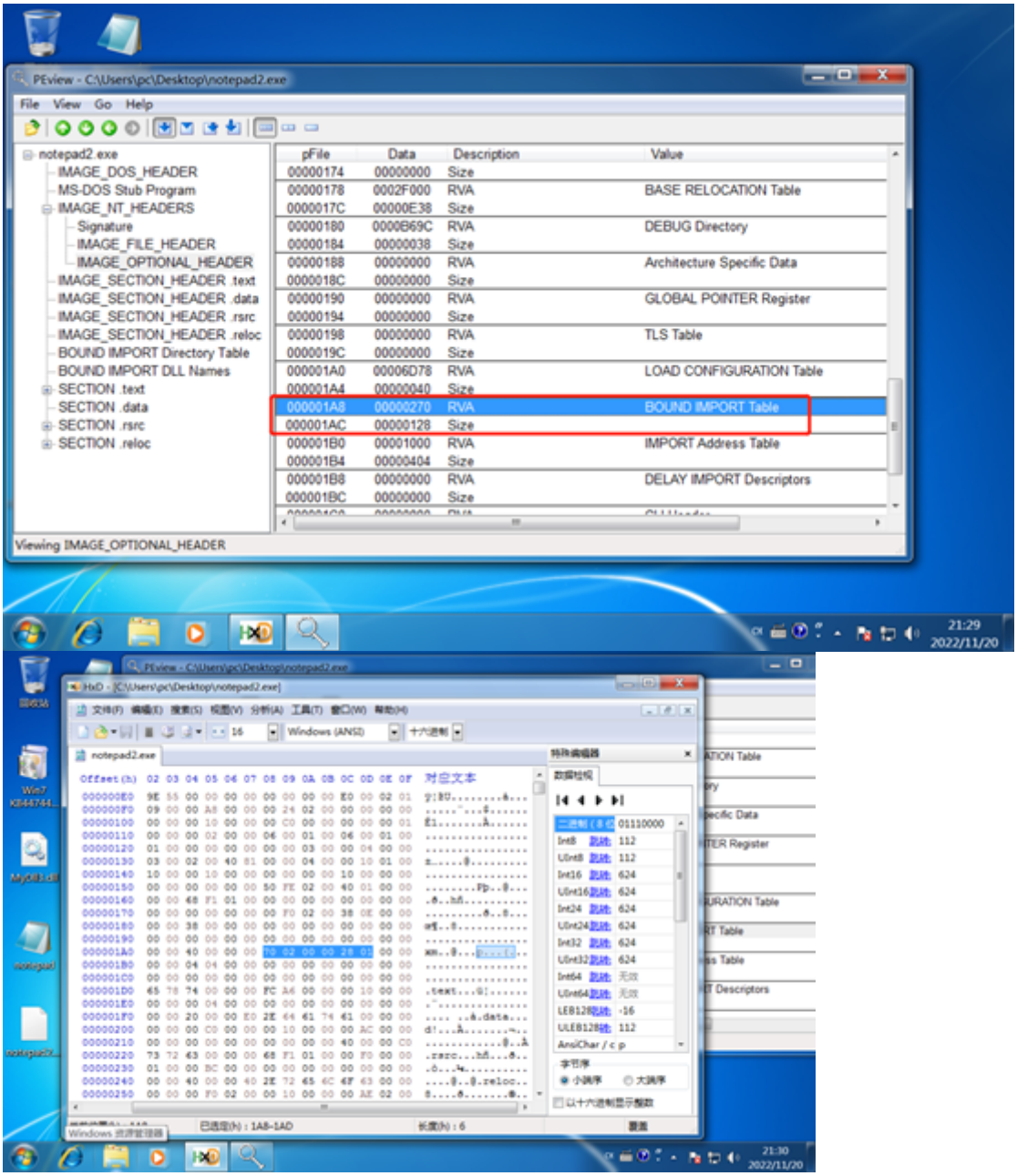
修改后：





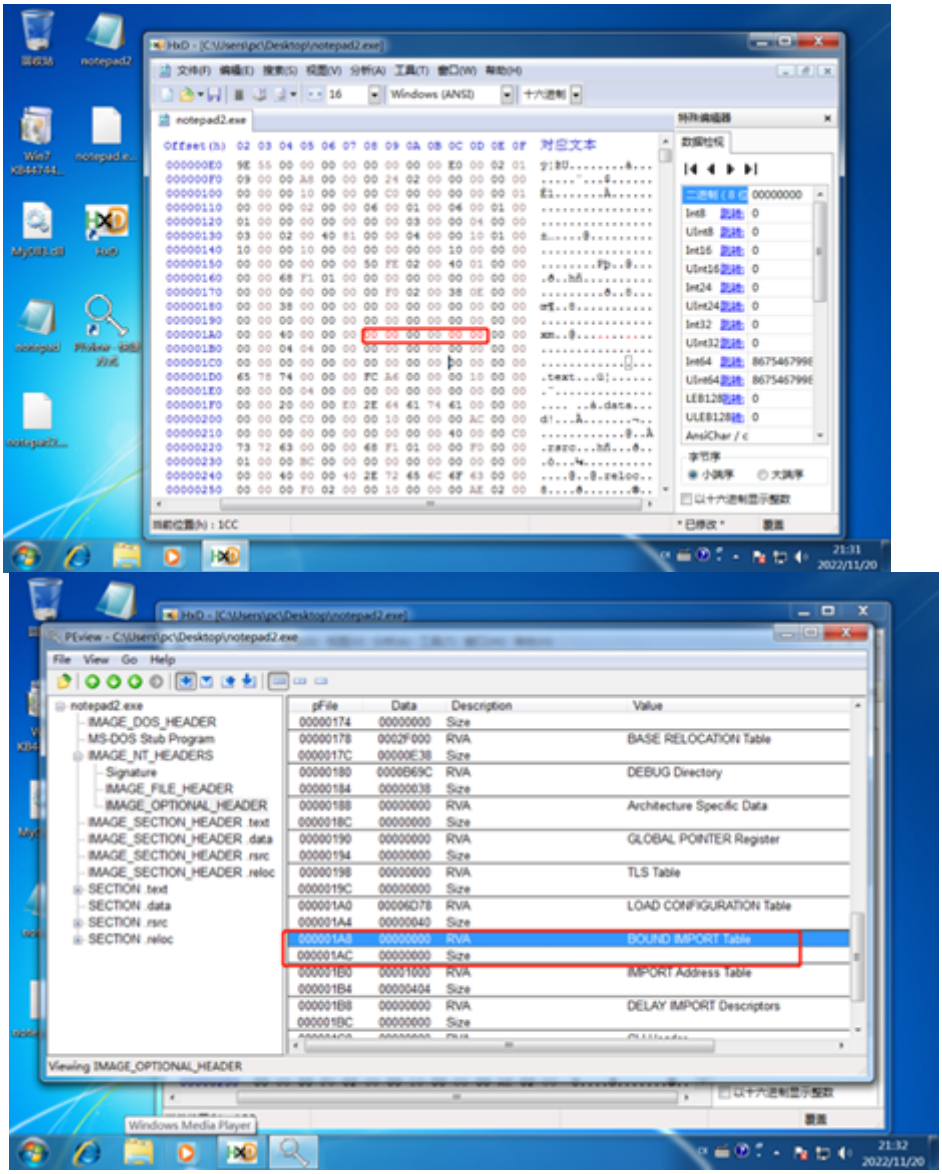
6. 为了不向绑定导入表中再添加信息，选择直接删除绑定导入表信息（内容和大小）。

删除信息前：

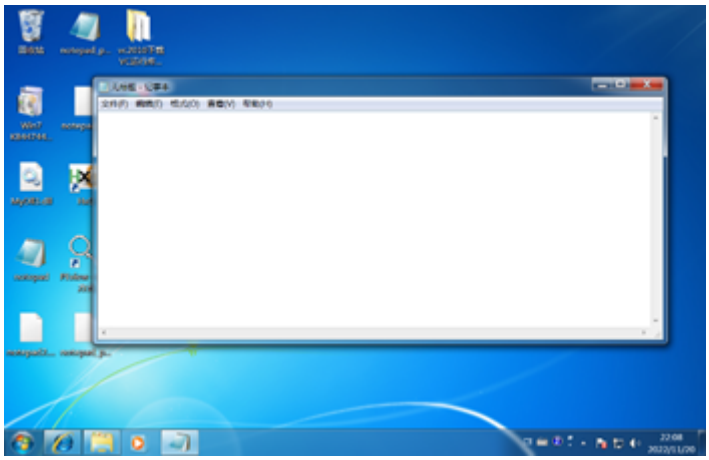

PEview - C:\Users\pc\Desktop\notepad2.exe
File View Go Help
notepad2.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .rsrc
IMAGE_SECTION_HEADER .reloc
BOUND IMPORT Directory Table
BOUND IMPORT DLL Names
SECTION .text
SECTION .data
SECTION .rsrc
SECTION .reloc
pFile Data Description Value
00000174 00000000 Size
00000178 0002F000 RVA BASE RELOCATION Table
0000017C 00000E38 Size
00000180 0000B69C RVA DEBUG Directory
00000184 00000038 Size
00000188 00000000 RVA Architecture Specific Data
0000018C 00000000 Size
00000190 00000000 RVA GLOBAL POINTER Register
00000194 00000000 Size
00000198 00000000 RVA TLS Table
0000019C 00000000 Size
000001A0 00006D78 RVA LOAD CONFIGURATION Table
000001A4 00000040 Size
000001A8 00000270 RVA BOUND IMPORT Table
000001AC 00000128 Size
000001B0 00001000 RVA IMPORT Address Table
000001B4 00000404 Size
000001B8 00000000 RVA DELAY IMPORT Descriptors
000001BC 00000000 Size
Viewing IMAGE_OPTIONAL_HEADER
21:29
2022/11/20

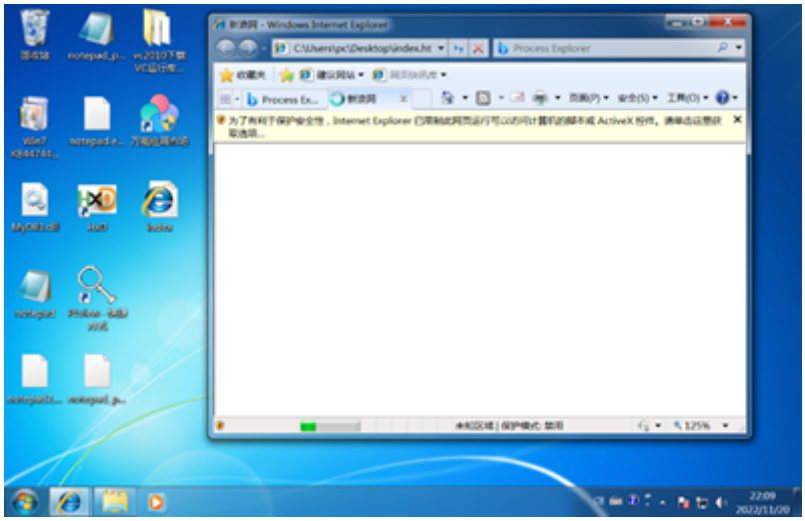
HxD - [C:\Users\pc\Desktop\notepad2.exe]
notepad2.exe
Windows (ANSI)
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
21:30
2022/11/20

删除后：



7. 结果：将修改后的 notepad_patch.exe 和 MyDll3.dll 都放到桌面上，运行 exe 文件，观察现象。成功。





8. 用 Process Explorer 观察运行中的 notepad_patch.exe，观察 MyDll3.dll 的装载。