실행 압축

SCP 부원 신재형

실행 압축

실행파일(PE File)

0 or 1

암호화
or
압축

차이점

항목	일반 압축	실행 압축
대상파일	모든 파일	PE 파일(exe, dll, sys)
압축 결과물	압축(zip, rar)파일	PE 파일(exe, dll, sys)
압축해제 방식	전용 압축해제 프로그램 사용	자체 실행 가능
파일 실행 여부	자체 실행 불가	자체 실행 가능
장점	모든 파일에 대해 높은 압축율로 압축 가능	별도의 해제 프로그램 없이 바로 실행 가능
단점	전용 압축해제 프로그램이 없으면 해당 압축 파일을 사용할 수 없다.	실행할 때마다 decoding 루틴이 호출되기 때문에 실행시간이 아주 미세하게 느려진다

패커

1. PE 파일의 크기를 줄이고자 하는 목적

2. PE 파일의 내부 코드와 리소스를 감추기 위한 목적

순수한 의도의 패커 : UPX, ASPack

불순한 의도의 패커 : Upack, PESpin, NSAnti

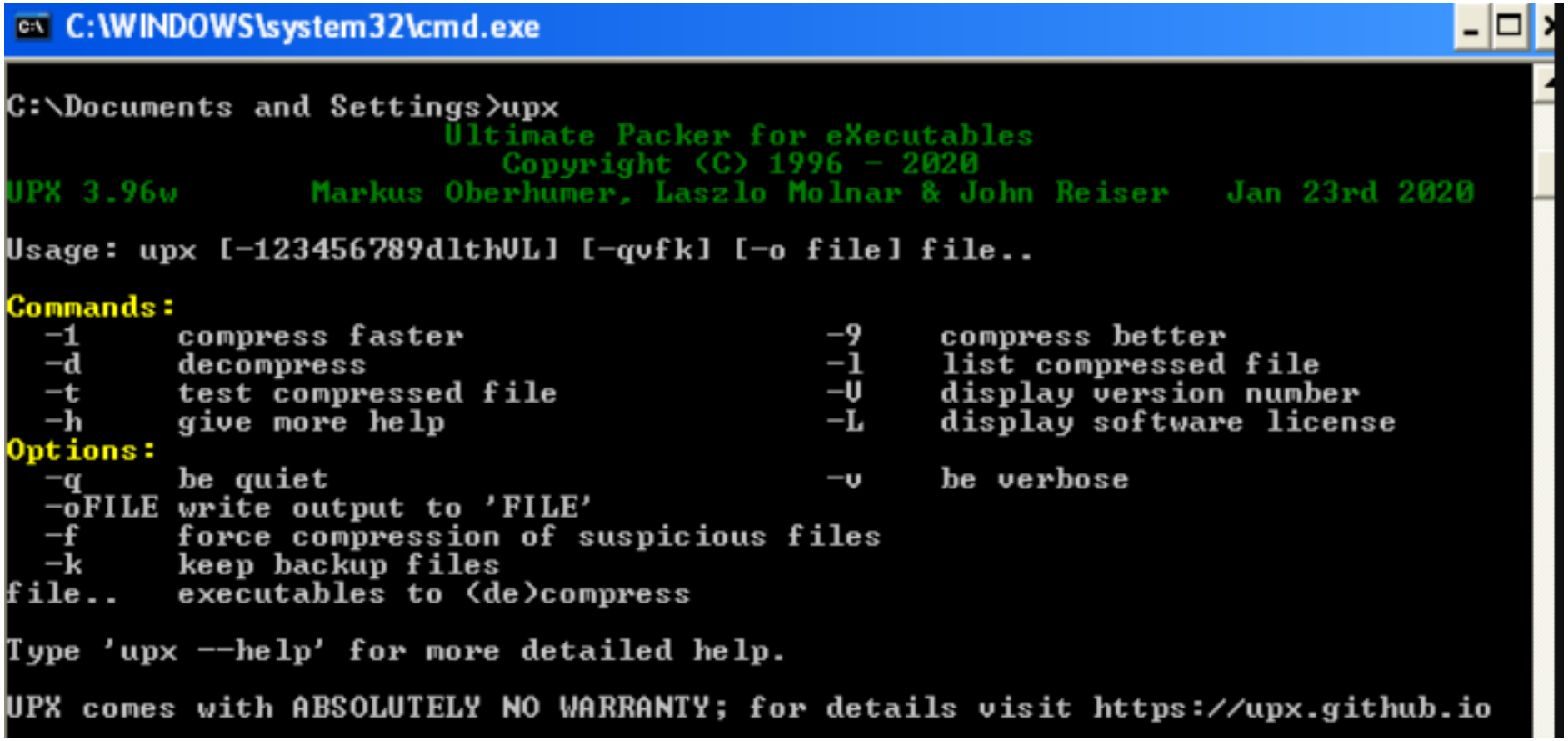
PE 프로텍터

PE 프로텍터 : PE 파일을 리버싱으로부터 보호하기 위한 유틸리티

Anti-Debugging, Anti-Emulating, Code Obfuscating,
Polymorphic Code, Garbage Code, Debugger Detection

1. 크래킹 방지
2. 코드 및 리소스 보호

실습


C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings>upx
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2020
UPX 3.96w Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020
Usage: upx [-123456789dlthVL] [-qvfk] [-o file] file..
Commands:
-1 compress faster
-9 compress better
-d decompress
-l list compressed file
-t test compressed file
-V display version number
-h give more help
-L display software license
Options:
-q be quiet
-v be verbose
-oFILE write output to 'FILE'
-f force compression of suspicious files
-k keep backup files
file.. executables to (de)compress
Type 'upx --help' for more detailed help.
UPX comes with ABSOLUTELY NO WARRANTY; for details visit https://upx.github.io

실습

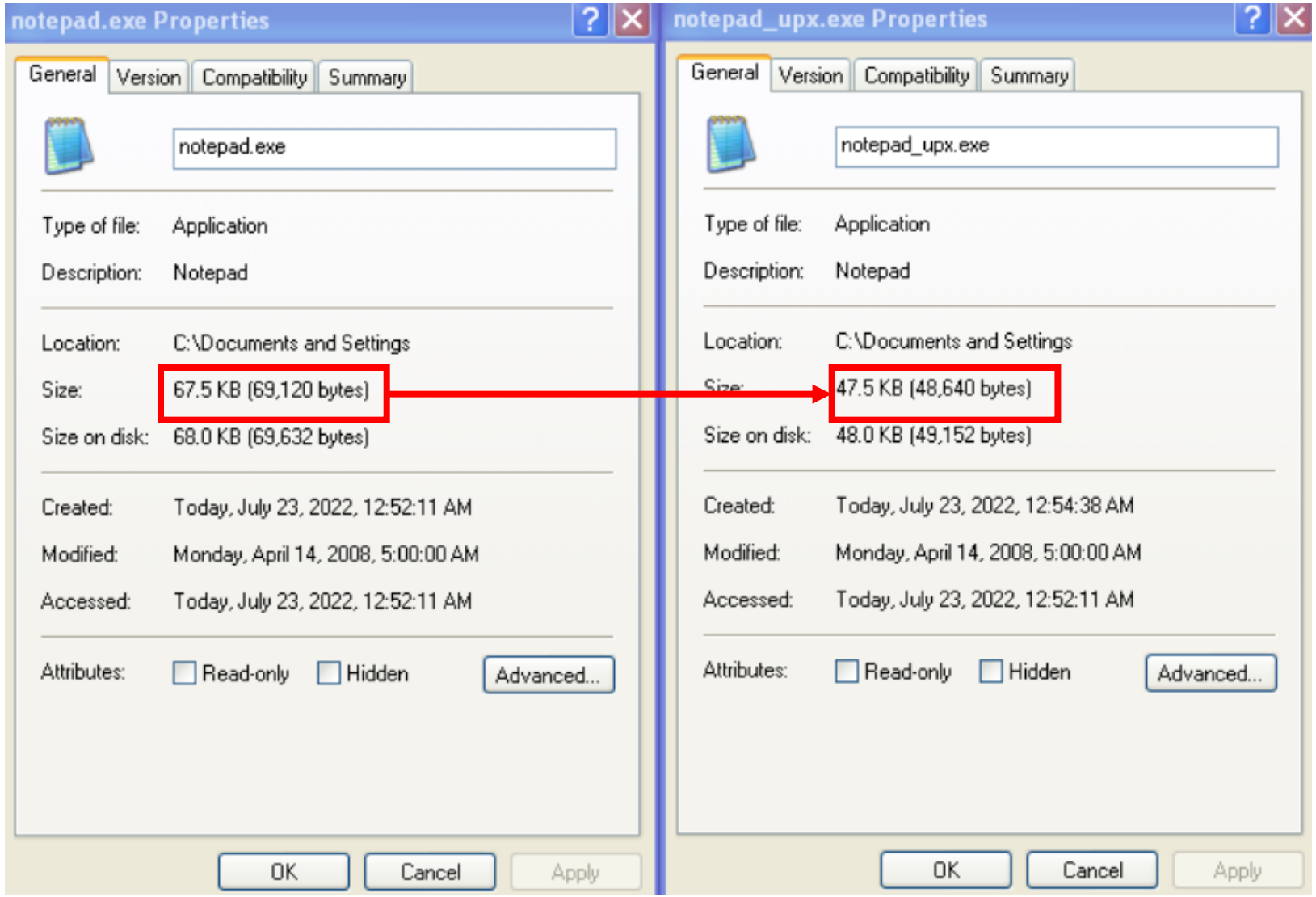
upx -o notepad_upx.exe notepad.exe

```
C:\Documents and Settings>upx -o notepad_upx.exe notepad.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     69120 ->     48640   70.37%    win32/pe     notepad_upx.exe

Packed 1 file.
```

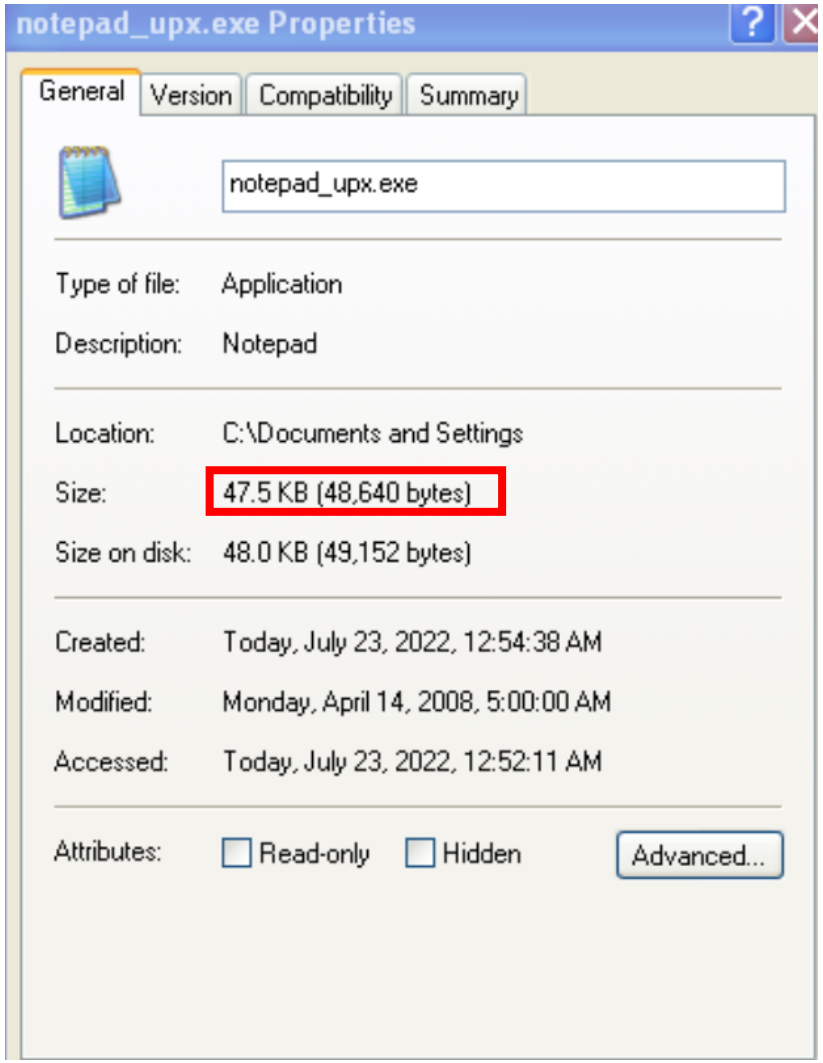
notepad.exe
Notepad
Microsoft Corporation

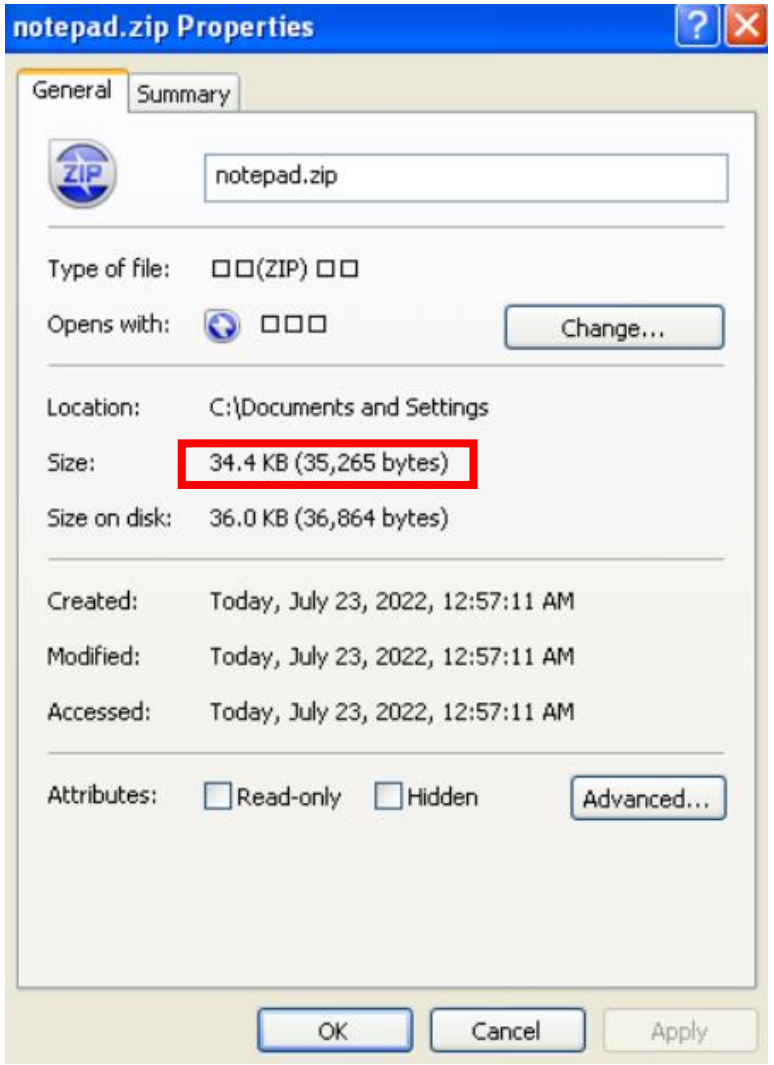
notepad_upx.exe
Notepad
Microsoft Corporation

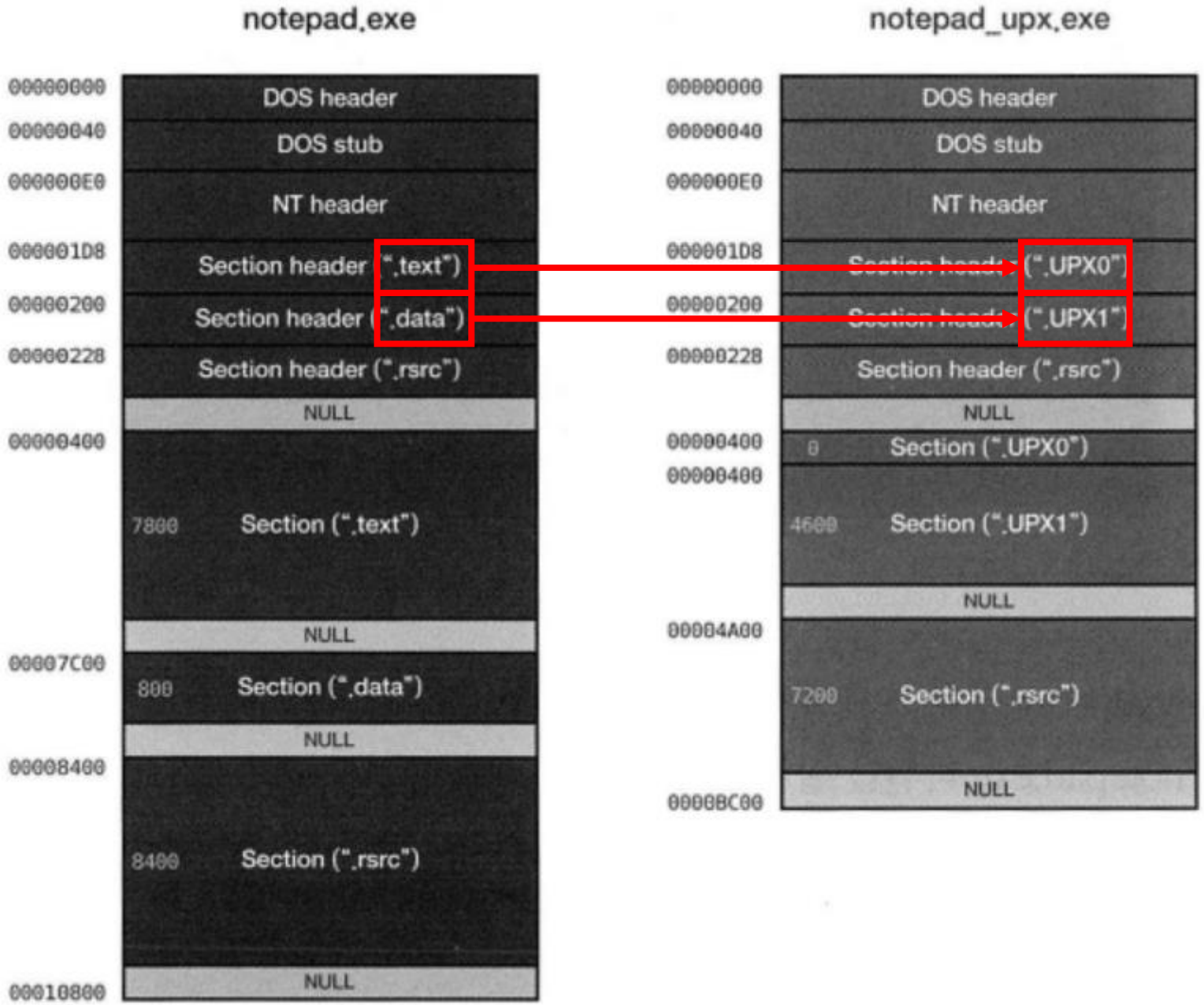
실습


notepad.exe Properties
General
Version
Compatibility
Summary
notepad.exe
Type of file: Application
Description: Notepad
Location: C:\Documents and Settings
Size: 67.5 KB (69,120 bytes)
Size on disk: 68.0 KB (69,632 bytes)
Created: Today, July 23, 2022, 12:52:11 AM
Modified: Monday, April 14, 2008, 5:00:00 AM
Accessed: Today, July 23, 2022, 12:52:11 AM
Attributes: Read-only Hidden Advanced...
OK
Cancel
Apply
notepad_upx.exe Properties
General
Version
Compatibility
Summary
notepad_upx.exe
Type of file: Application
Description: Notepad
Location: C:\Documents and Settings
Size: 47.5 KB (48,640 bytes)
Size on disk: 48.0 KB (49,152 bytes)
Created: Today, July 23, 2022, 12:54:38 AM
Modified: Monday, April 14, 2008, 5:00:00 AM
Accessed: Today, July 23, 2022, 12:52:11 AM
Attributes: Read-only Hidden Advanced...
OK
Cancel
Apply

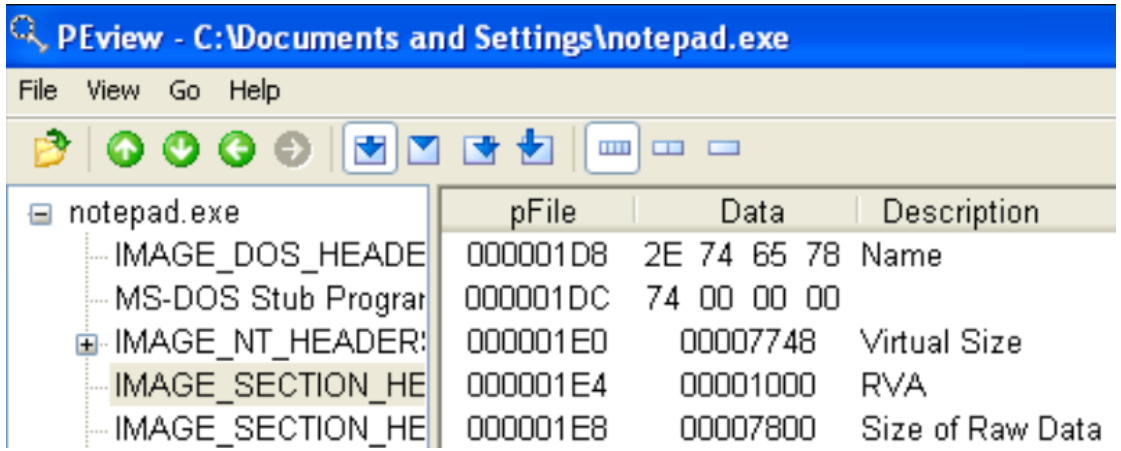
실습

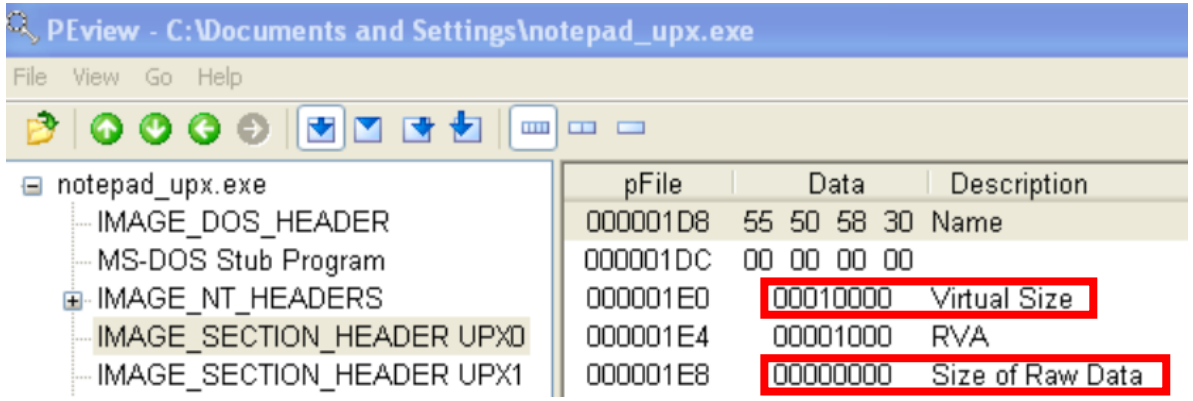

notepad_upx.exe Properties
General
Version
Compatibility
Summary
notepad_upx.exe
Type of file: Application
Description: Notepad
Location: C:\Documents and Settings
Size: 47.5 KB (48,640 bytes)
Size on disk: 48.0 KB (49,152 bytes)
Created: Today, July 23, 2022, 12:54:38 AM
Modified: Monday, April 14, 2008, 5:00:00 AM
Accessed: Today, July 23, 2022, 12:52:11 AM
Attributes: Read-only Hidden Advanced...


notepad.zip Properties
General
Summary
notepad.zip
Type of file: □□(ZIP) □□
Opens with: □□□
Change...
Location: C:\Documents and Settings
Size: 34.4 KB (35,265 bytes)
Size on disk: 36.0 KB (36,864 bytes)
Created: Today, July 23, 2022, 12:57:11 AM
Modified: Today, July 23, 2022, 12:57:11 AM
Accessed: Today, July 23, 2022, 12:57:11 AM
Attributes: Read-only Hidden Advanced...
OK
Cancel
Apply

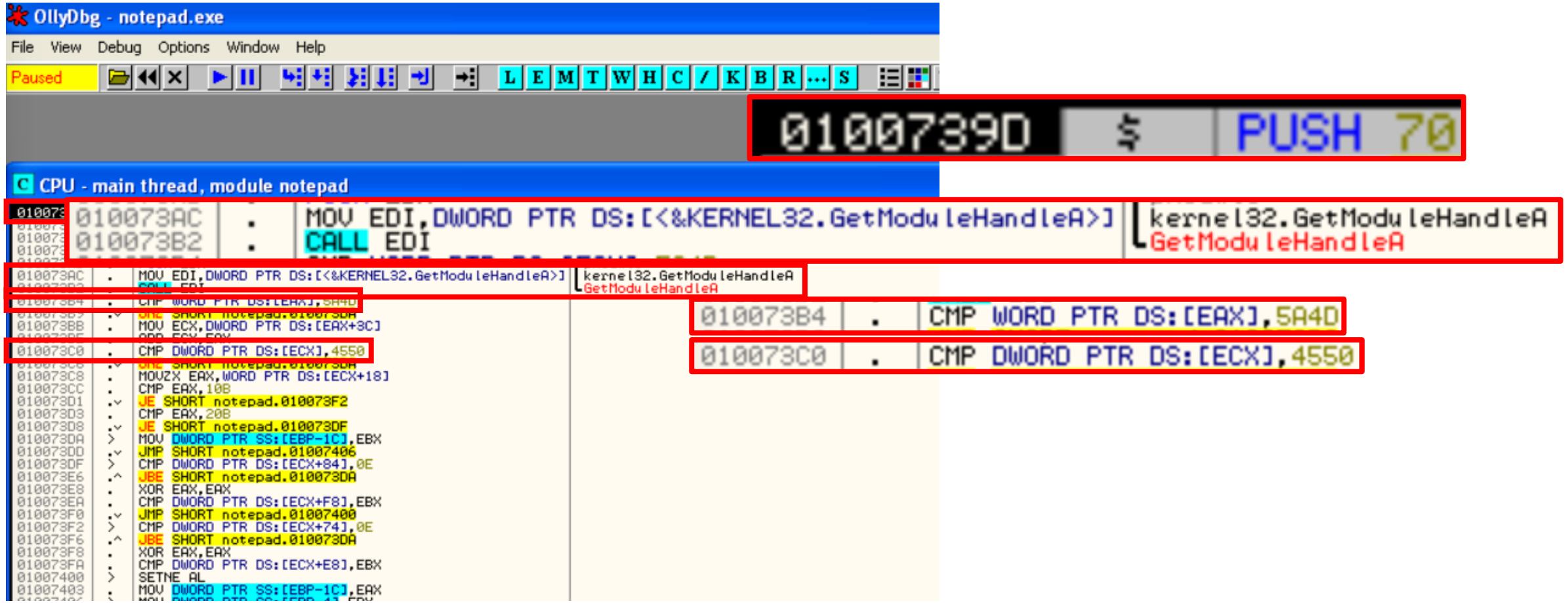

notepad.exe
00000000
DOS header
00000040
DOS stub
000000E0
NT header
000001D8
Section header (".text")
00000200
Section header (".data")
00000228
Section header (".rsrc")
NULL
00000400
7800
Section (".text")
NULL
00007C00
800
Section (".data")
NULL
00008400
8400
Section (".rsrc")
NULL
00010800
notepad_upx.exe
00000000
DOS header
00000040
DOS stub
000000E0
NT header
000001D8
(".UPX0")
00000200
(".UPX1")
00000228
Section header (".rsrc")
NULL
00000400
0
Section (".UPX0")
00000400
4600
Section (".UPX1")
NULL
00004A00
7200
Section (".rsrc")
NULL
0000BC00

실습

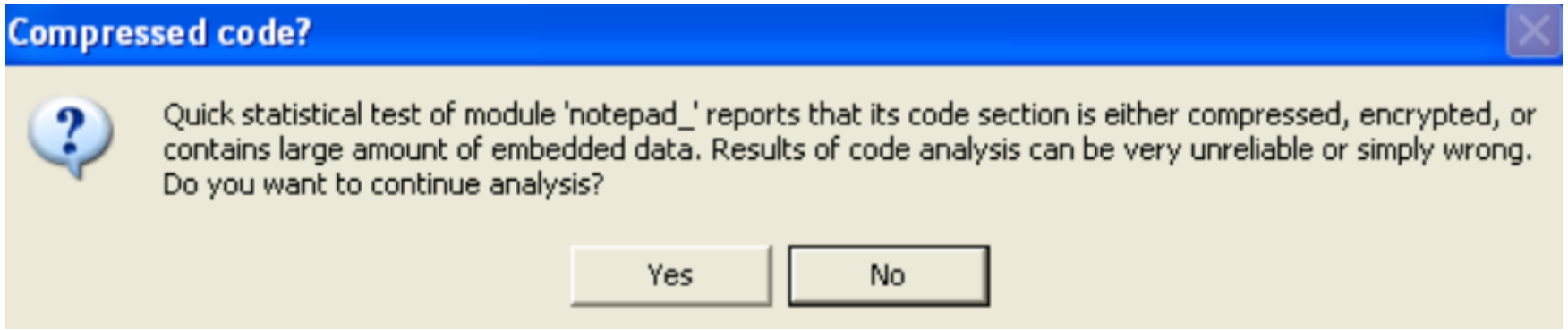

PEview - C:\Documents and Settings\notepad.exe
File View Go Help
notepad.exe
IMAGE_DOS_HEADE
MS-DOS Stub Prograr
IMAGE_NT_HEADER:
IMAGE_SECTION_HE
IMAGE_SECTION_HE
pFile Data Description
000001D8 2E 74 65 78 Name
000001DC 74 00 00 00
000001E0 00007748 Virtual Size
000001E4 00001000 RVA
000001E8 00007800 Size of Raw Data


PEview - C:\Documents and Settings\notepad_upx.exe
File View Go Help
notepad_upx.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER UPX0
IMAGE_SECTION_HEADER UPX1
pFile Data Description
000001D8 55 50 58 30 Name
000001DC 00 00 00 00
000001E0 00010000 Virtual Size
000001E4 00001000 RVA
000001E8 00000000 Size of Raw Data

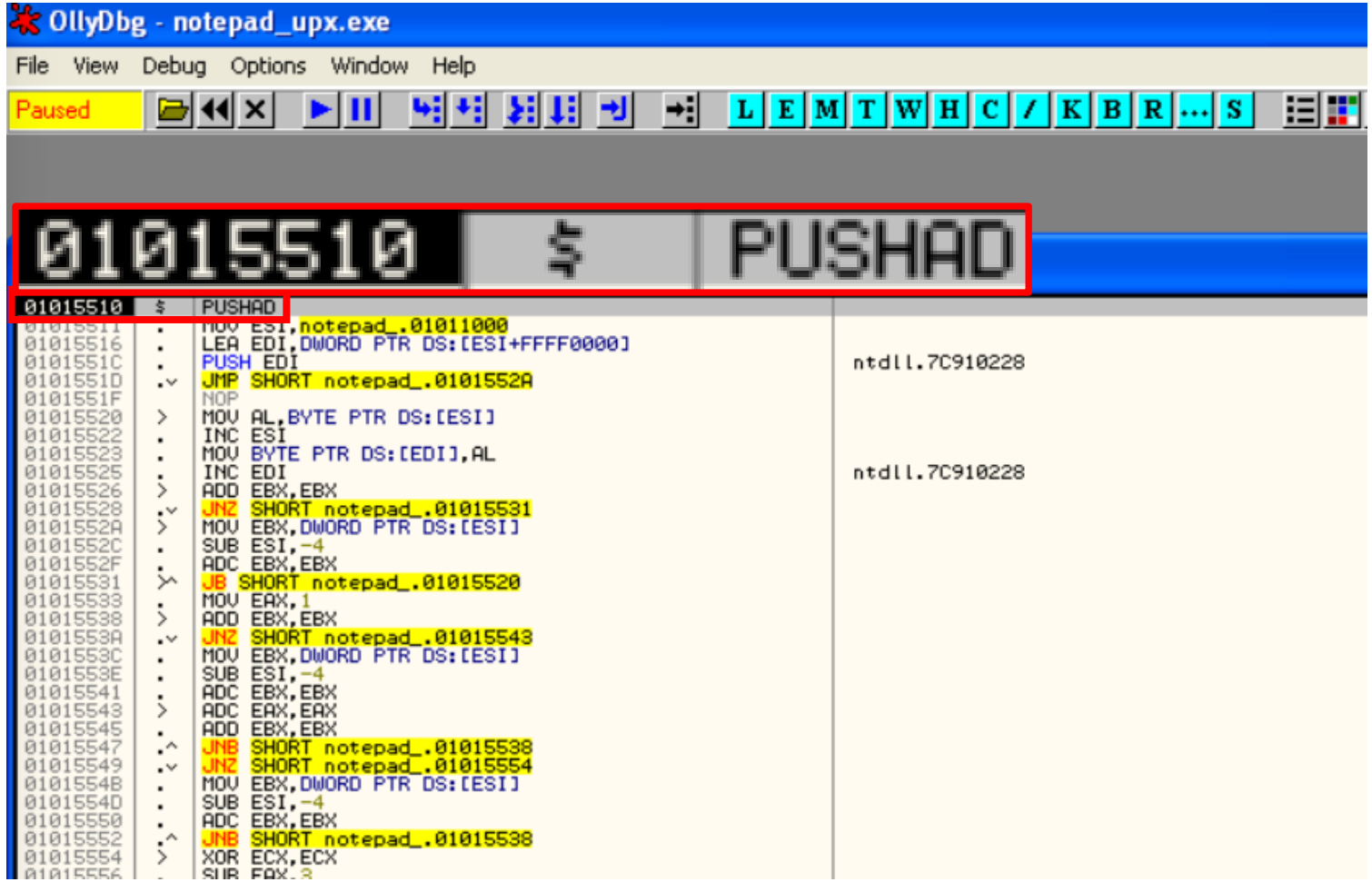
실습


OllyDbg - notepad.exe
File View Debug Options Window Help
Paused
01007390 PUSH 70
CPU - main thread, module notepad
010073AC . MOV EDI,DWORD PTR DS:[<&KERNEL32.GetModuleHandleA>]
010073B2 . CALL EDI
kernel32.GetModuleHandleA
GetModuleHandleA
010073B4 . CMP WORD PTR DS:[EAX],5A4D
010073C0 . CMP DWORD PTR DS:[ECX],4550
010073BB . MOV ECX,DWORD PTR DS:[EAX+3C]
010073C8 . MOVZX EAX,WORD PTR DS:[ECX+18]
010073CC . CMP EAX,10B
010073D1 . JE SHORT notepad.010073F2
010073D3 . CMP EAX,20B
010073D8 . JE SHORT notepad.010073DF
010073DA > MOV DWORD PTR SS:[EBP-1C],EBX
010073DD . JMP SHORT notepad.01007406
010073DF > CMP DWORD PTR DS:[ECX+84],0E
010073E6 . JBE SHORT notepad.010073DA
010073E8 . XOR EAX,EAX
010073EA . CMP DWORD PTR DS:[ECX+F8],EBX
010073F0 . JMP SHORT notepad.01007400
010073F2 > CMP DWORD PTR DS:[ECX+74],0E
010073F6 . JBE SHORT notepad.010073DA
010073F8 . XOR EAX,EAX
010073FA . CMP DWORD PTR DS:[ECX+E8],EBX
01007400 > SETNE AL
01007403 . MOV DWORD PTR SS:[EBP-1C],EAX

실습


Compressed code?
Quick statistical test of module 'notepad_' reports that its code section is either compressed, encrypted, or contains large amount of embedded data. Results of code analysis can be very unreliable or simply wrong. Do you want to continue analysis?
Yes
No

실습


OllyDbg - notepad_upx.exe
File View Debug Options Window Help
Paused
01015510 $ PUSHAD
01015510 $ PUSHAD
01015511 . MOV ESI,notepad_.01011000
01015516 . LEA EDI,DWORD PTR DS:[ESI+FFFF0000]
0101551C . PUSH EDI
0101551D .v JMP SHORT notepad_.0101552A
0101551F NOP
01015520 > MOV AL,BYTE PTR DS:[ESI]
01015522 . INC ESI
01015523 . MOV BYTE PTR DS:[EDI],AL
01015525 . INC EDI
01015526 > ADD EBX,EBX
01015528 .v JNZ SHORT notepad_.01015531
0101552A > MOV EBX,DWORD PTR DS:[ESI]
0101552C . SUB ESI,-4
0101552F . ADC EBX,EBX
01015531 >^ JB SHORT notepad_.01015520
01015533 . MOV EAX,1
01015538 > ADD EBX,EBX
0101553A .v JNZ SHORT notepad_.01015543
0101553C . MOV EBX,DWORD PTR DS:[ESI]
0101553E . SUB ESI,-4
01015541 . ADC EBX,EBX
01015543 > ADC EAX,EAX
01015545 . ADD EBX,EBX
01015547 .^ JNB SHORT notepad_.01015538
01015549 .v JNZ SHORT notepad_.01015554
0101554B . MOV EBX,DWORD PTR DS:[ESI]
0101554D . SUB ESI,-4
01015550 . ADC EBX,EBX
01015552 .^ JNB SHORT notepad_.01015538
01015554 > XOR ECX,ECX
ntdll.7C910228
ntdll.7C910228

실습

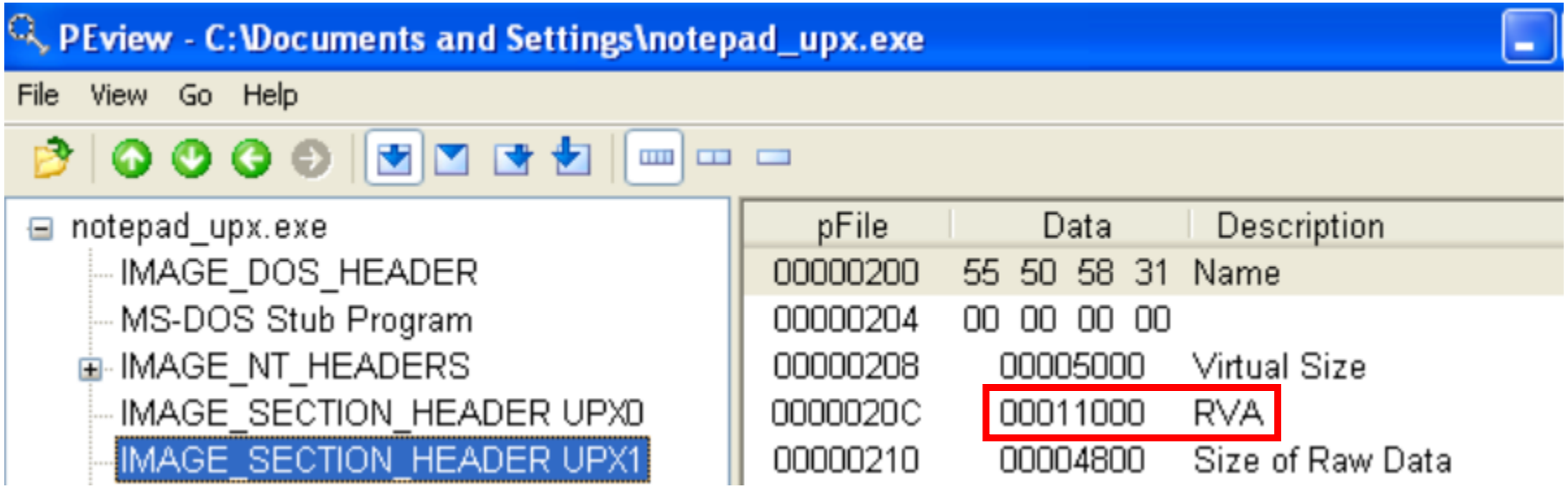
```
Registers (FPU)
EAX 00000000
ECX 0006FFB0
EDX 7C90E514 ntdll.KiFastSystemCallRet
EBX 7FFDB000
ESP 0006FFC4
EBP 0006FFF0
ESI FFFFFFFF
EDI 7C910228 ntdll.7C910228
```

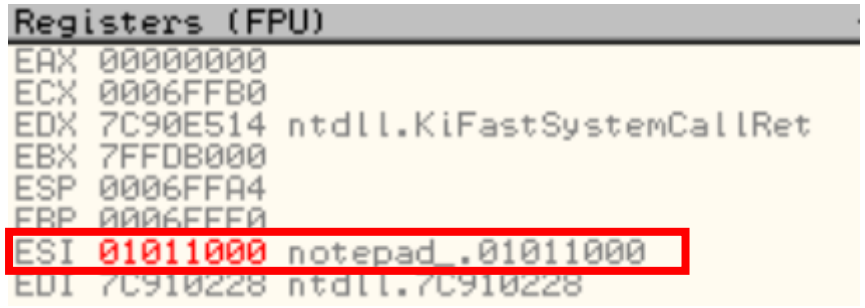
```
0006FFC4  7C816037  RETURN to kernel32.7C816037
0006FFC8  7C910228  ntdll.7C910228
0006FFCC  FFFFFFFF
0006FFD0  7FFDB000
0006FFD4  8054B6ED
0006FFD8  0006FFC8
0006FFDC  82470D10
0006FFE0  FFFFFFFF  End of SEH chain
0006FFE4  7C839B48  SE handler
0006FFE8  7C816040  kernel32.7C816040
0006FFEC  00000000
0006FFF0  00000000
0006FFF4  00000000
0006FFF8  01015510  notepad_.<ModuleEntryPoint>
0006FFFC  00000000
```

```
0006FFA4  7C910228  ntdll.7C910228
0006FFA8  FFFFFFFF
0006FFAC  0006FFF0
0006FFB0  0006FFC4
0006FFB4  7FFDB000
0006FFB8  7C90E514  ntdll.KiFastSystemCallRet
0006FFBC  0006FFB0
0006FFC0  00000000
0006FFC4  7C816037  RETURN to kernel32.7C816037
0006FFC8  7C910228  ntdll.7C910228
0006FFCC  FFFFFFFF
0006FFD0  7FFDB000
0006FFD4  8054B6ED
0006FFD8  0006FFC8
0006FFDC  82470D10
0006FFE0  FFFFFFFF  End of SEH chain
0006FFE4  7C839B48  SE handler
0006FFE8  7C816040  kernel32.7C816040
0006FFEC  00000000
```

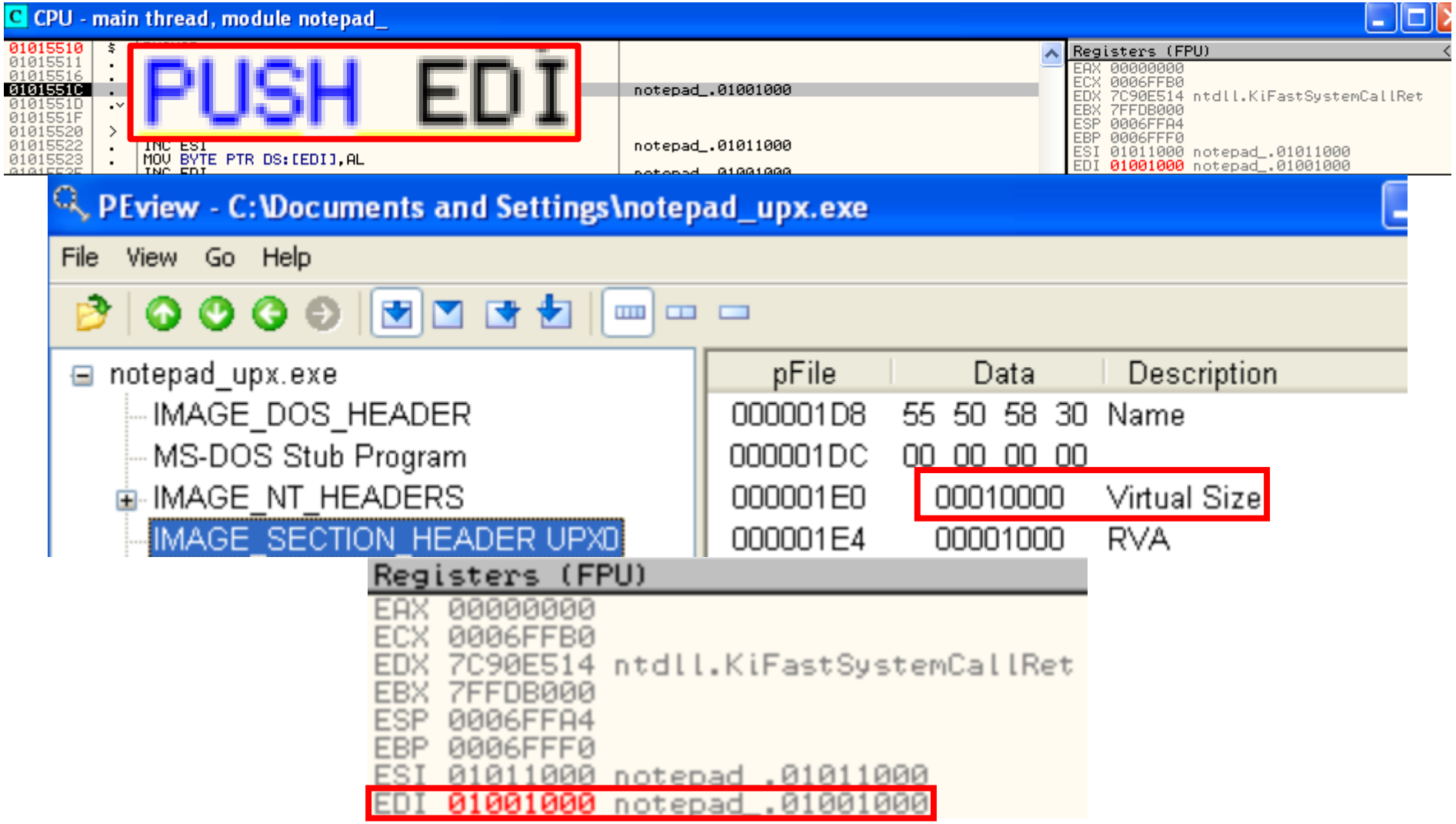
실습


CPU - main thread, module notepad_
LEA EDI,DWORD PTR DS:[ESI+FFFF0000]
MOV AL,BYTE PTR DS:[ESI]
INC ESI
MOV BYTE PTR DS:[EDI],AL
notepad_.01011000
EBP 0006FFF0
ESI 01011000 notepad_.01011000
EDI 7C910228 ntdll.7C910228


PEview - C:\Documents and Settings\notepad_upx.exe
File View Go Help
notepad_upx.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER UPX0
IMAGE_SECTION_HEADER UPX1
pFile Data Description
00000200 55 50 58 31 Name
00000204 00 00 00 00
00000208 00005000 Virtual Size
0000020C 00011000 RVA
00000210 00004800 Size of Raw Data


Registers (FPU)
EAX 00000000
ECX 0006FFB0
EDX 7C90E514 ntdll.KiFastSystemCallRet
EBX 7FFDB000
ESP 0006FFA4
EBP 0006FFF0
ESI 01011000 notepad_.01011000
EDI 7C910228 ntdll.7C910228

실습


CPU - main thread, module notepad_
PUSH EDI
notepad_.01001000
notepad_.01011000
INC ESI
MOV BYTE PTR DS:[EDI],AL
Registers (FPU)
EAX 00000000
ECX 0006FFB0
EDX 7C90E514 ntdll.KiFastSystemCallRet
EBX 7FFDB000
ESP 0006FFA4
EBP 0006FFF0
ESI 01011000 notepad_.01011000
EDI 01001000 notepad_.01001000
PEview - C:\Documents and Settings\notepad_upx.exe
File View Go Help
notepad_upx.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER UPX0
pFile Data Description
000001D8 55 50 58 30 Name
000001DC 00 00 00 00
000001E0 00010000 Virtual Size
000001E4 00001000 RVA
Registers (FPU)
EAX 00000000
ECX 0006FFB0
EDX 7C90E514 ntdll.KiFastSystemCallRet
EBX 7FFDB000
ESP 0006FFA4
EBP 0006FFF0
ESI 01011000 notepad_.01011000
EDI 01001000 notepad_.01001000

실습

```
01015520  >  8A06          MOV AL,BYTE PTR DS:[ESI]
01015522  .  46            INC ESI
01015523  .  8807          MOV BYTE PTR DS:[EDI],AL
01015525  .  47            INC EDI
```

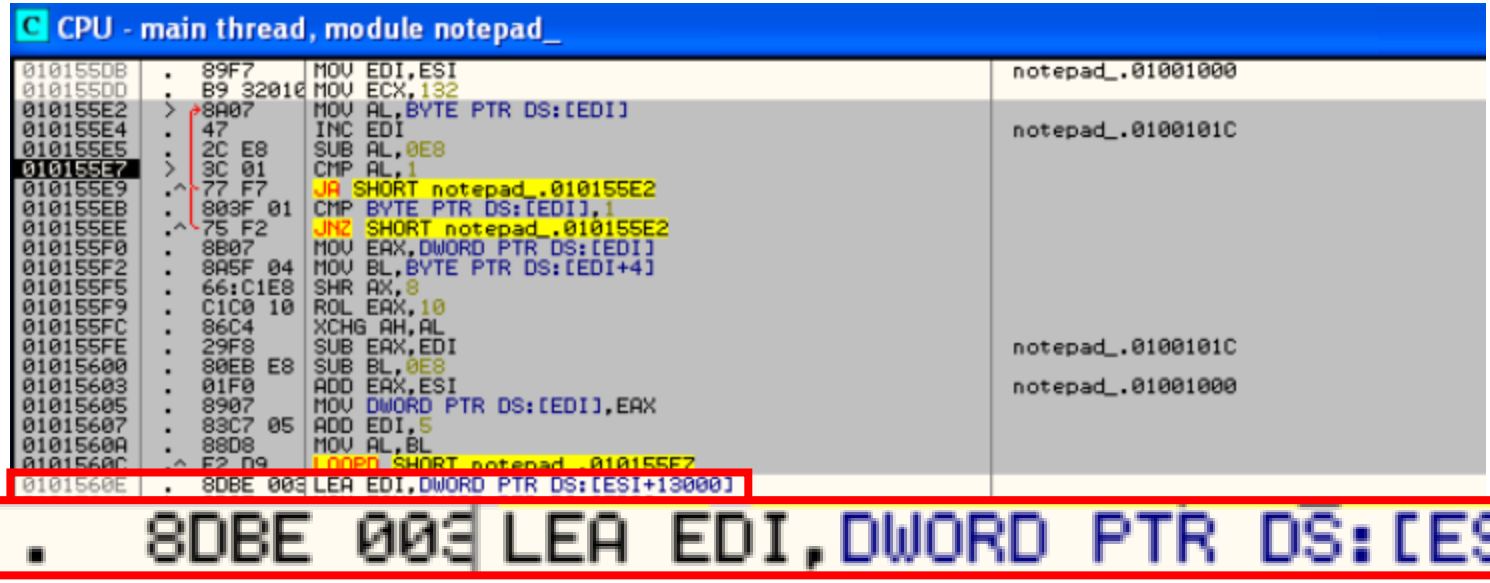
```
010155C9  .  8907          MOV DWORD PTR DS:[EDI],EAX
010155CB  .  83C7 04       ADD EDI,4
010155CE  .  83E9 04       SUB ECX,4
010155D1  .^ 77 F1         JA SHORT notepad_.010155C4
010155D3  .  01CF          ADD EDI,ECX
010155D5  .^ E9 4CFFF      JMP notepad_.01015526
010155DA  >  5E            POP ESI
```

실습

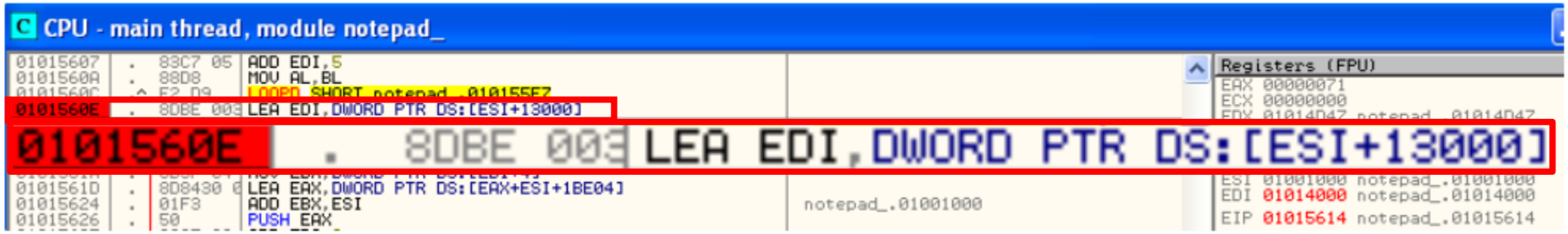
Address	Hex dump	ASCII
01001000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01001010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01001020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01001030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01001040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01001050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01001060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01001070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01001080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01001090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
010010A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
010010B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
010010C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
010010D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
010010E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
010010F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01001100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
01001110	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....

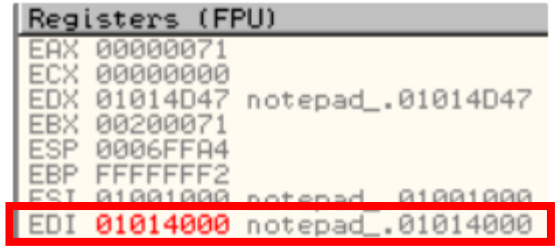
Address	Hex dump	ASCII
01001000	A2 7C 00 00 B6 7C 00 00 C4 7C 00 00 D4 7C 00 00	ó¦..╢¦..─¦..╘¦..
01001010	E4 7C 00 00 F8 7C 00 00 90 7C 00 00 00 00 00 00	Σ¦..°¦..╔¦......
01001020	48 7B 00 00 00 00 00 00 D0 81 00 00 C4 81 00 00	H{......╨ü..─ü..
01001030	BA 81 00 00 AE 81 00 00 DA 81 00 00 8A 81 00 00	╢ü..«ü..┌ü..èü..
01001040	7E 81 00 00 F2 81 00 00 5E 81 00 00 A2 81 00 00	~ü..≥ü..^ü..óü..
01001050	E6 81 00 00 50 81 00 00 3E 81 00 00 30 81 00 00	µü..Pü..>ü..0ü..
01001060	20 81 00 00 0A 81 00 00 FA 80 00 00 02 82 00 00	ü...ü..·Ç..☻é..
01001070	14 82 00 00 20 82 00 00 2A 82 00 00 3C 82 00 00	¶é.. é..*é..<é..
01001080	50 82 00 00 6E 81 00 00 00 00 00 00 24 80 00 00	Pé..nü.......$Ç..
01001090	14 80 00 00 FA 7F 00 00 EA 7F 00 00 D4 7F 00 00	¶Ç..·⌂..Ω⌂..╘⌂..
010010A0	C2 7F 00 00 B0 7F 00 00 A2 7F 00 00 92 7F 00 00	┬⌂..░⌂..ó⌂..Æ⌂..
010010B0	74 7F 00 00 5E 7F 00 00 3A 80 00 00 54 80 00 00	t⌂..^⌂..:Ç..TÇ..
010010C0	68 80 00 00 98 80 00 00 B6 80 00 00 C6 80 00 00	hÇ..ÿÇ..╢Ç..╞Ç..
010010D0	DA 80 00 00 16 7D 00 00 24 7D 00 00 36 7D 00 00	┌Ç...▬}..$}..6}..
010010E0	42 7D 00 00 50 7D 00 00 5C 7D 00 00 6A 7D 00 00	B}..P}..\}..j}..
010010F0	7C 7D 00 00 88 7D 00 00 96 7D 00 00 A4 7D 00 00	|}..ê}..û}..ñ}..
01001100	B0 7D 00 00 BC 7D 00 00 CA 7D 00 00 D6 7D 00 00	░}..╜}..╩}..╓}..
01001110	EC 7D 00 00 FE 7D 00 00 10 7E 00 00 1C 7E 00 00	∞}..■}..►~..└~..

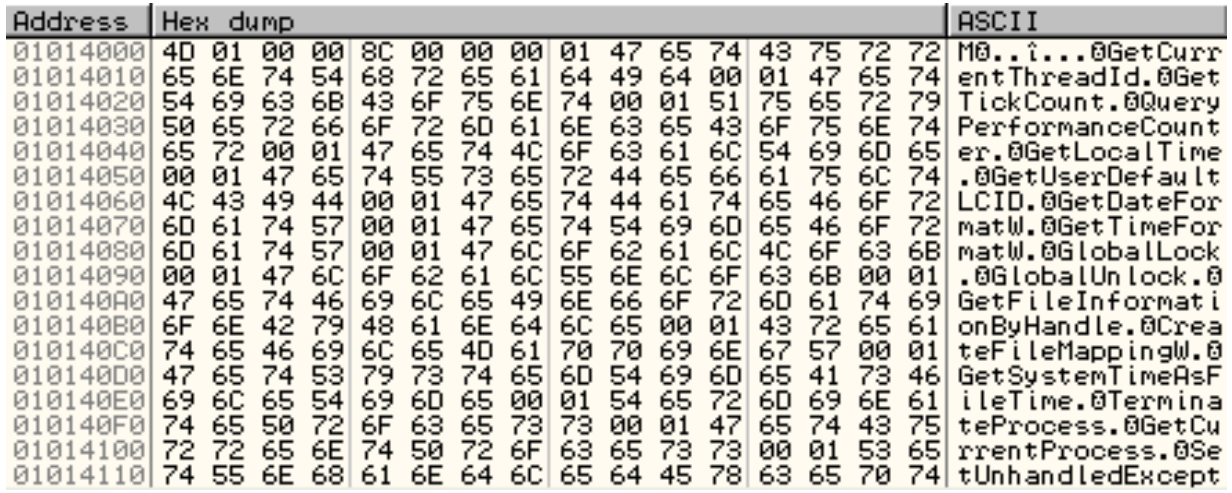
실습


CPU - main thread, module notepad_
010155DB . 89F7 MOV EDI,ESI
010155DD . B9 32010 MOV ECX,132
010155E2 > 8A07 MOV AL,BYTE PTR DS:[EDI]
010155E4 . 47 INC EDI
010155E5 . 2C E8 SUB AL,0E8
010155E7 > 3C 01 CMP AL,1
010155E9 .^77 F7 JA SHORT notepad_.010155E2
010155EB . 803F 01 CMP BYTE PTR DS:[EDI],1
010155EE .^75 F2 JNZ SHORT notepad_.010155E2
010155F0 . 8B07 MOV EAX,DWORD PTR DS:[EDI]
010155F2 . 8A5F 04 MOV BL,BYTE PTR DS:[EDI+4]
010155F5 . 66:C1E8 SHR AX,8
010155F9 . C1C0 10 ROL EAX,10
010155FC . 86C4 XCHG AH,AL
010155FE . 29F8 SUB EAX,EDI
01015600 . 80EB E8 SUB BL,0E8
01015603 . 01F0 ADD EAX,ESI
01015605 . 8907 MOV DWORD PTR DS:[EDI],EAX
01015607 . 83C7 05 ADD EDI,5
0101560A . 88D8 MOV AL,BL
0101560C .^E2 D9 LOOPD SHORT notepad_.010155E7
0101560E . 8DBE 003 LEA EDI,DWORD PTR DS:[ESI+13000]
notepad_.01001000
notepad_.0100101C
notepad_.0100101C
notepad_.01001000
0101560E . 8DBE 003 LEA EDI,DWORD PTR DS:[ESI+13000]

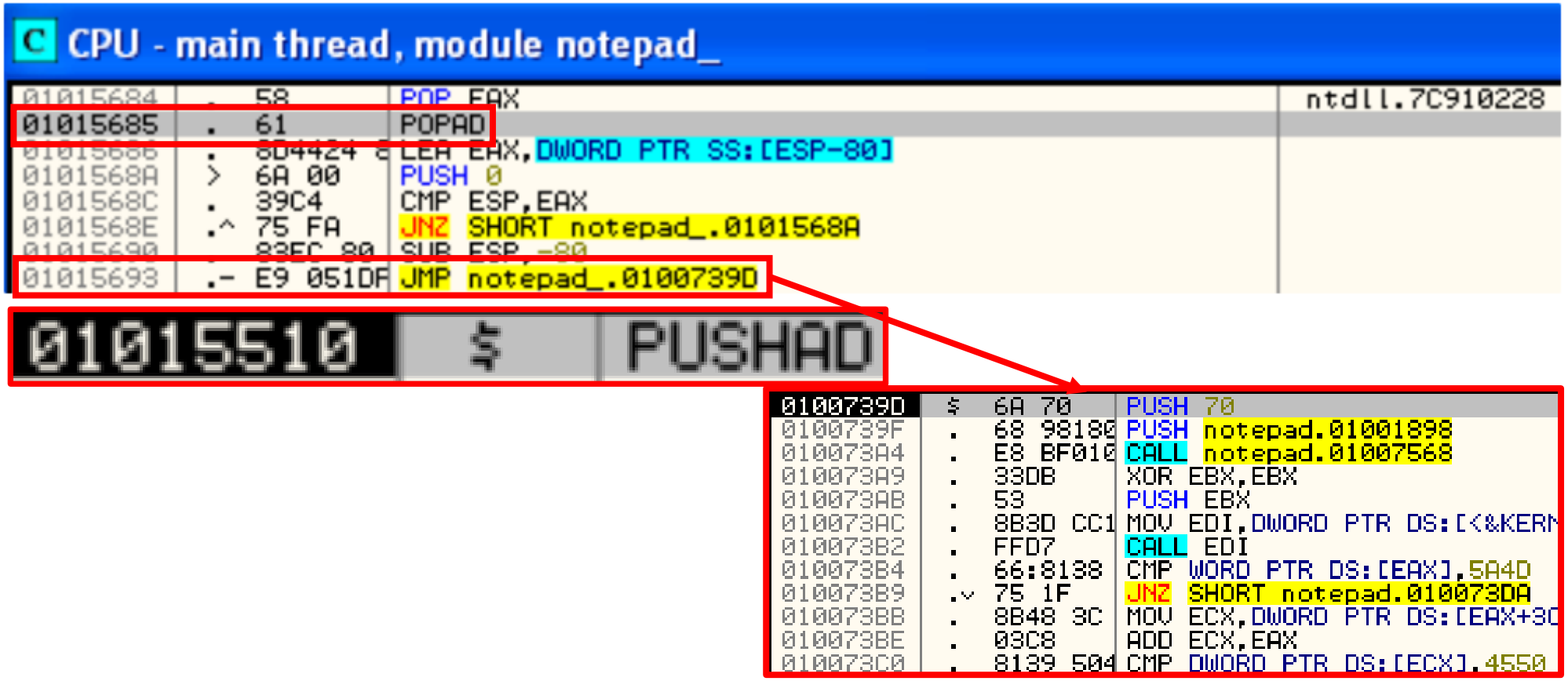
실습


CPU - main thread, module notepad_
01015607 . 83C7 05 ADD EDI,5
0101560A . 88D8 MOV AL,BL
0101560C . E2 D9 LOOPD SHORT notepad_.010155E7
0101560E . 8DBE 003 LEA EDI,DWORD PTR DS:[ESI+13000]
0101561D . 8D8430 0 LEA EAX,DWORD PTR DS:[EAX+ESI+1BE04]
01015624 . 01F3 ADD EBX,ESI
01015626 . 50 PUSH EAX
notepad_.01001000
Registers (FPU)
EAX 00000071
ECX 00000000
EDI 01014000 notepad_.01014000
EIP 01015614 notepad_.01015614


Registers (FPU)
EAX 00000071
ECX 00000000
EDX 01014D47 notepad_.01014D47
EBX 00200071
ESP 0006FFA4
EBP FFFFFFF2
EDI 01014000 notepad_.01014000


Address Hex dump ASCII
01014000 4D 01 00 00 8C 00 00 00 01 47 65 74 43 75 72 72 M0..î...0GetCurr
01014010 65 6E 74 54 68 72 65 61 64 49 64 00 01 47 65 74 entThreadId.0Get
01014020 54 69 63 6B 43 6F 75 6E 74 00 01 51 75 65 72 79 TickCount.0Query
01014030 50 65 72 66 6F 72 6D 61 6E 63 65 43 6F 75 6E 74 PerformanceCount
01014040 65 72 00 01 47 65 74 4C 6F 63 61 6C 54 69 6D 65 er.0GetLocalTime
01014050 00 01 47 65 74 55 73 65 72 44 65 66 61 75 6C 74 .0GetUserDefault
01014060 4C 43 49 44 00 01 47 65 74 44 61 74 65 46 6F 72 LCID.0GetDateFor
01014070 6D 61 74 57 00 01 47 65 74 54 69 6D 65 46 6F 72 matW.0GetTimeFor
01014080 6D 61 74 57 00 01 47 6C 6F 62 61 6C 4C 6F 63 6B matW.0GlobalLock
01014090 00 01 47 6C 6F 62 61 6C 55 6E 6C 6F 63 6B 00 01 .0GlobalUnlock.0
010140A0 47 65 74 46 69 6C 65 49 6E 66 6F 72 6D 61 74 69 GetFileInformati
010140B0 6F 6E 42 79 48 61 6E 64 6C 65 00 01 43 72 65 61 onByHandle.0Crea
010140C0 74 65 46 69 6C 65 4D 61 70 70 69 6E 67 57 00 01 teFileMappingW.0
010140D0 47 65 74 53 79 73 74 65 6D 54 69 6D 65 41 73 46 GetSystemTimeAsF
010140E0 69 6C 65 54 69 6D 65 00 01 54 65 72 6D 69 6E 61 ileTime.0Termina
010140F0 74 65 50 72 6F 63 65 73 73 00 01 47 65 74 43 75 teProcess.0GetCu
01014100 72 72 65 6E 74 50 72 6F 63 65 73 73 00 01 53 65 rrentProcess.0Se
01014110 74 55 6E 68 61 6E 64 6C 65 64 45 78 63 65 70 74 tUnhandledExcept

실습


CPU - main thread, module notepad_
01015684 58 POP EAX
ntdll.7C910228
01015685 61 POPAD
LEA EAX,DWORD PTR SS:[ESP-80]
0101568A 6A 00 PUSH 0
0101568C 39C4 CMP ESP,EAX
0101568E 75 FA JNZ SHORT notepad_.0101568A
SUB ESP,-80
01015693 E9 051DF JMP notepad_.0100739D
01015510 $ PUSHAD
0100739D $ 6A 70 PUSH 70
0100739F 68 98180 PUSH notepad.01001898
010073A4 E8 BF010 CALL notepad.01007568
010073A9 33DB XOR EBX,EBX
010073AB 53 PUSH EBX
010073AC 8B3D CC1 MOV EDI,DWORD PTR DS:[<&KERN
010073B2 FFD7 CALL EDI
010073B4 66:8138 CMP WORD PTR DS:[EAX],5A4D
010073B9 75 1F JNZ SHORT notepad.010073DA
010073BB 8B48 3C MOV ECX,DWORD PTR DS:[EAX+3C
010073BE 03C8 ADD ECX,EAX
010073C0 8139 504 CMP DWORD PTR DS:[ECX],4550

감사합니다.