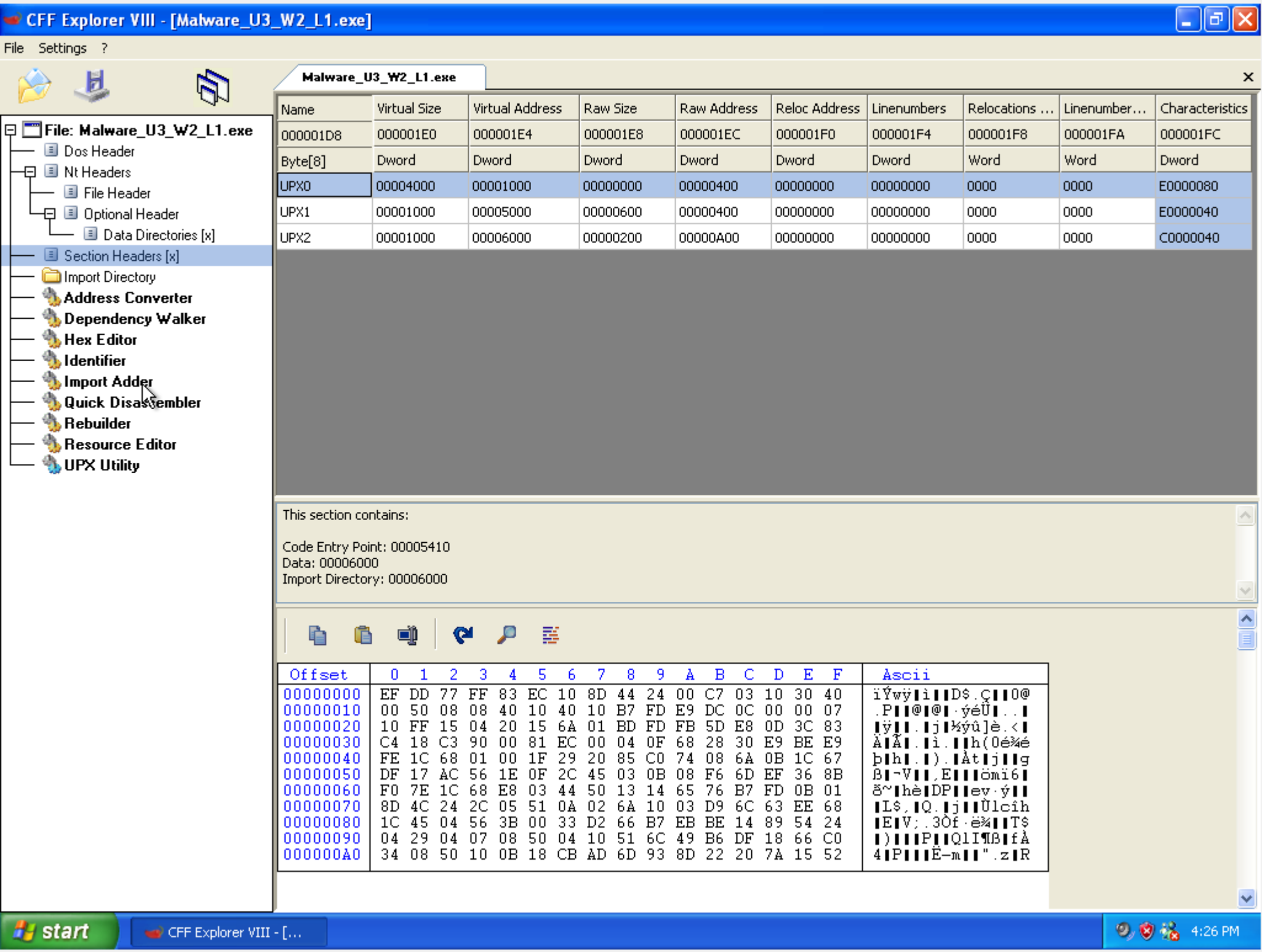
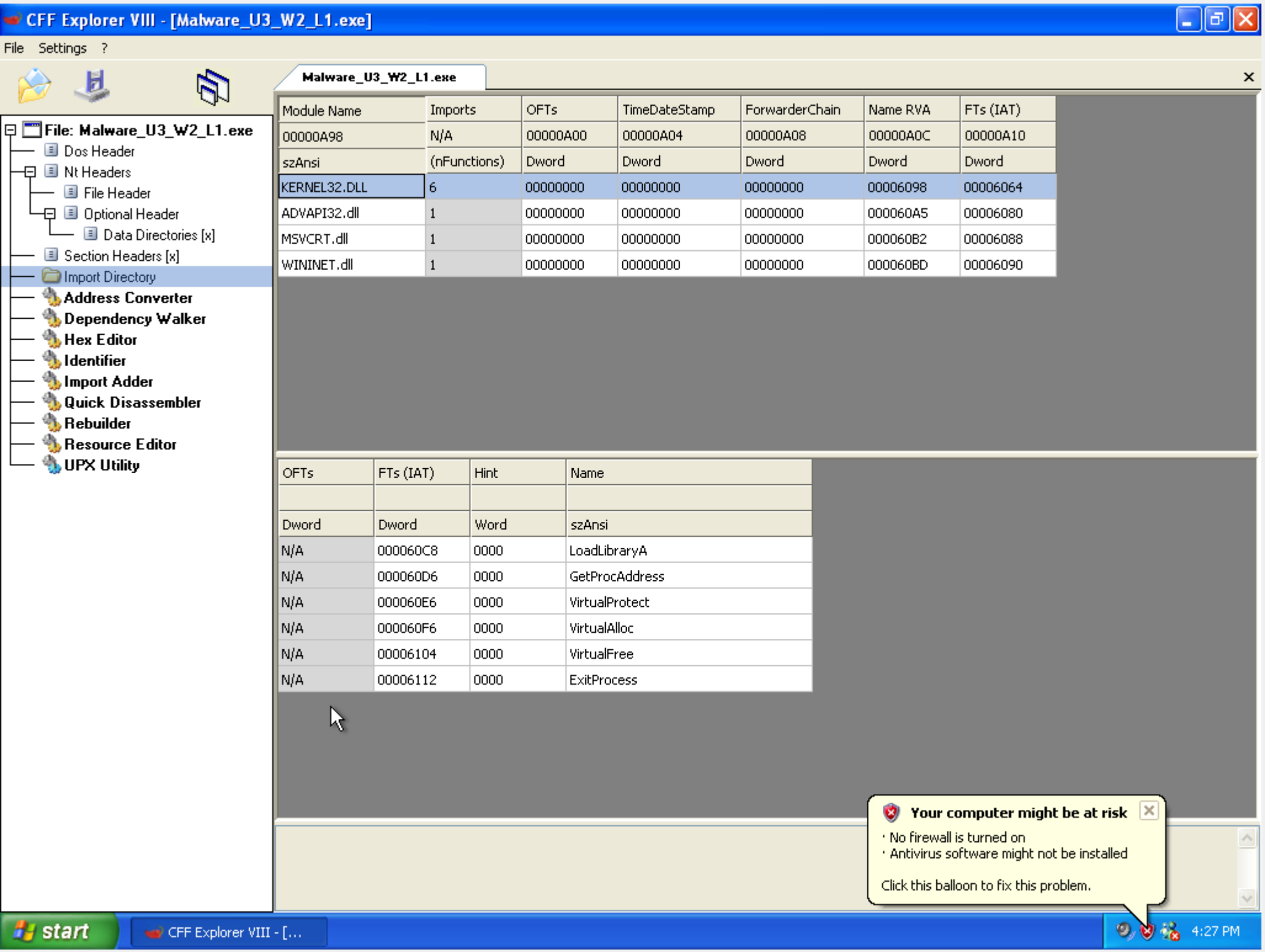
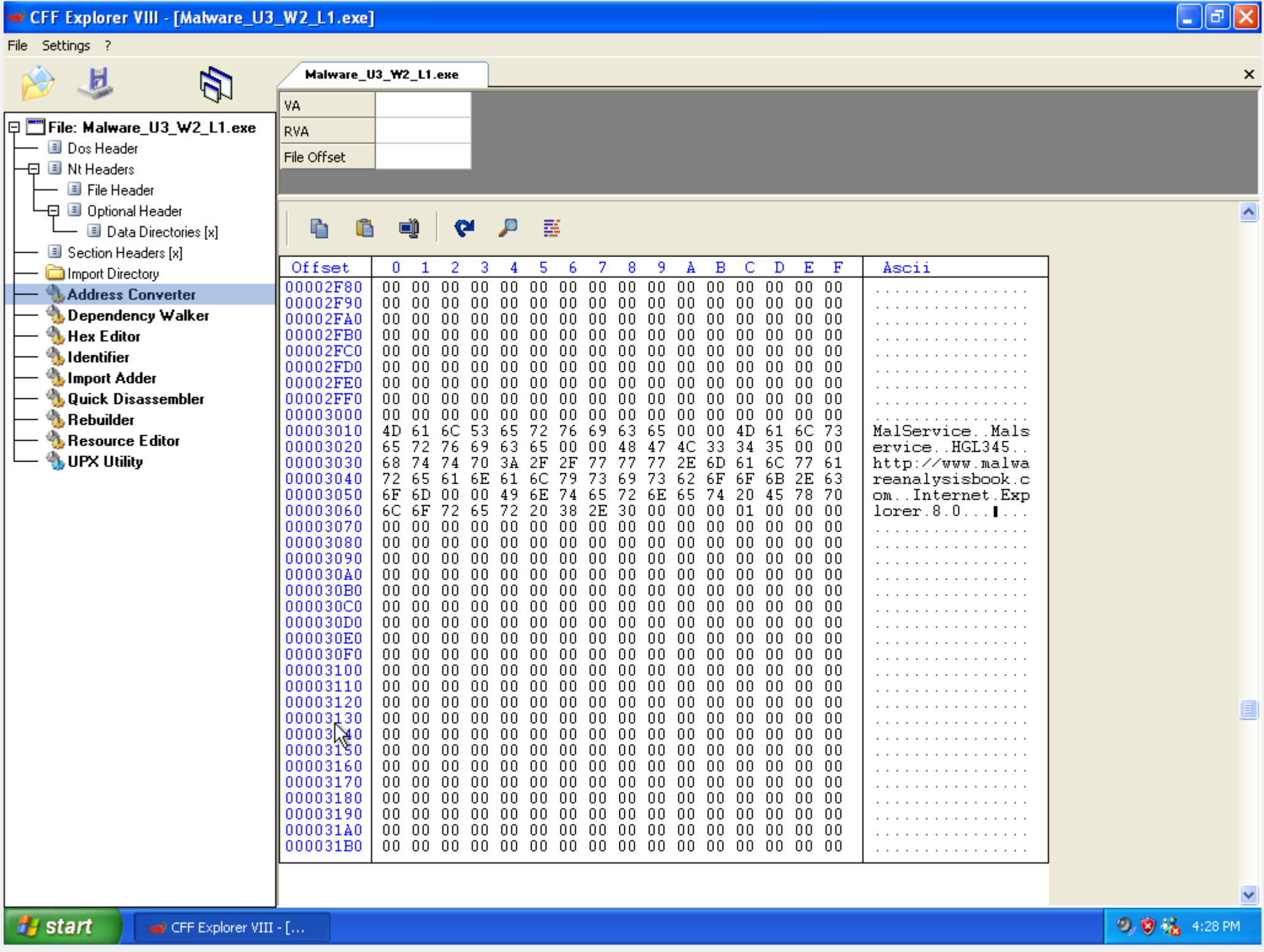

CFF Explorer VIII - [Malware_U3_W2_L1.exe]
File Settings ?
Malware_U3_W2_L1.exe
File: Malware_U3_W2_L1.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Name Virtual Size Virtual Address Raw Size Raw Address Reloc Address Linenumbers Relocations ... Linenumber... Characteristics
000001D8 000001E0 000001E4 000001E8 000001EC 000001F0 000001F4 000001F8 000001FA 000001FC
Byte[8] Dword Dword Dword Dword Dword Dword Word Word Dword
UPX0 00004000 00001000 00000000 00000400 00000000 00000000 0000 0000 E0000080
UPX1 00001000 00005000 00000600 00000400 00000000 00000000 0000 0000 E0000040
UPX2 00001000 00006000 00000200 00000A00 00000000 00000000 0000 0000 C0000040
This section contains:
Code Entry Point: 00005410
Data: 00006000
Import Directory: 00006000
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F Ascii
00000000 EF DD 77 FF 83 EC 10 8D 44 24 00 C7 03 10 30 40
00000010 00 50 08 08 40 10 40 10 B7 FD E9 DC 0C 00 00 07
00000020 10 FF 15 04 20 15 6A 01 BD FD FB 5D E8 0D 3C 83
00000030 C4 18 C3 90 00 81 EC 00 04 0F 68 28 30 E9 BE E9
00000040 FE 1C 68 01 00 1F 29 20 85 C0 74 08 6A 0B 1C 67
00000050 DF 17 AC 56 1E 0F 2C 45 03 0B 08 F6 6D EF 36 8B
00000060 F0 7E 1C 68 E8 03 44 50 13 14 65 76 B7 FD 0B 01
00000070 8D 4C 24 2C 05 51 0A 02 6A 10 03 D9 6C 63 EE 68
00000080 1C 45 04 56 3B 00 33 D2 66 B7 EB BE 14 89 54 24
00000090 04 29 04 07 08 50 04 10 51 6C 49 B6 DF 18 66 C0
000000A0 34 08 50 10 0B 18 CB AD 6D 93 8D 22 20 7A 15 52
start
CFF Explorer VIII - [...
4:26 PM


CFF Explorer VIII - [Malware_U3_W2_L1.exe]
File Settings ?
Malware_U3_W2_L1.exe
File: Malware_U3_W2_L1.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT)
00000A98 | N/A | 00000A00 | 00000A04 | 00000A08 | 00000A0C | 00000A10
szAnsi | (nFunctions) | Dword | Dword | Dword | Dword | Dword
KERNEL32.DLL | 6 | 00000000 | 00000000 | 00000000 | 00006098 | 00006064
ADVAPI32.dll | 1 | 00000000 | 00000000 | 00000000 | 000060A5 | 00006080
MSVCRT.dll | 1 | 00000000 | 00000000 | 00000000 | 000060B2 | 00006088
WININET.dll | 1 | 00000000 | 00000000 | 00000000 | 000060BD | 00006090
OFTs | FTs (IAT) | Hint | Name
Dword | Dword | Word | szAnsi
N/A | 000060C8 | 0000 | LoadLibraryA
N/A | 000060D6 | 0000 | GetProcAddress
N/A | 000060E6 | 0000 | VirtualProtect
N/A | 000060F6 | 0000 | VirtualAlloc
N/A | 00006104 | 0000 | VirtualFree
N/A | 00006112 | 0000 | ExitProcess
Your computer might be at risk
· No firewall is turned on
· Antivirus software might not be installed
Click this balloon to fix this problem.
start
CFF Explorer VIII - [...
4:27 PM


CFF Explorer VIII - [Malware_U3_W2_L1.exe]
File Settings ?
Malware_U3_W2_L1.exe
File: Malware_U3_W2_L1.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
VA
RVA
File Offset
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F Ascii
00002F80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00002F90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00002FA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00002FB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00002FC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00002FD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00002FE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00002FF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003010 4D 61 6C 53 65 72 76 69 63 65 00 00 4D 61 6C 73 MalService..Mals
00003020 65 72 76 69 63 65 00 00 48 47 4C 33 34 35 00 00 ervice..HGL345..
00003030 68 74 74 70 3A 2F 2F 77 77 77 2E 6D 61 6C 77 61 http://www.malwa
00003040 72 65 61 6E 61 6C 79 73 69 73 62 6F 6F 6B 2E 63 reanalysisbook.c
00003050 6F 6D 00 00 49 6E 74 65 72 6E 65 74 20 45 78 70 om..Internet.Exp
00003060 6C 6F 72 65 72 20 38 2E 30 00 00 00 01 00 00 00 lorer.8.0.......
00003070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000030A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000030B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000030C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000030D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000030E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000030F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00003190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000031A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000031B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
start
CFF Explorer VIII - [...
4:28 PM