Fun With Thread Local Sto

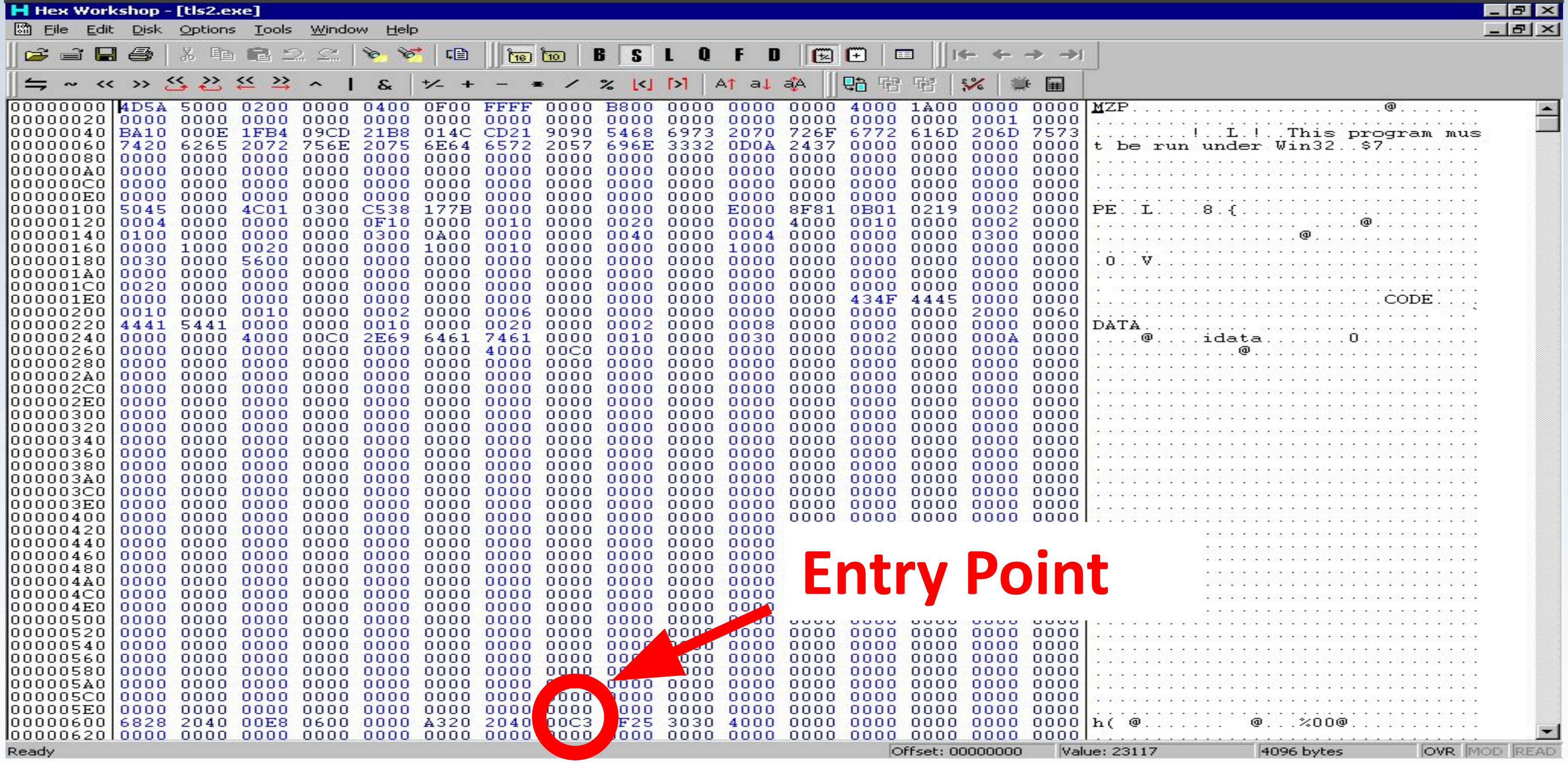
Peter Ferrie
Senior Anti-virus Researcher

26 June, 2008

You Can Call Me Al

Thread Local Storage callbacks were discovered in 2000.
However, widespread use didn't occur until 2004.
Now, it should be the first place to look for code,
since it runs before the main entrypoint.
And that can make all the difference…

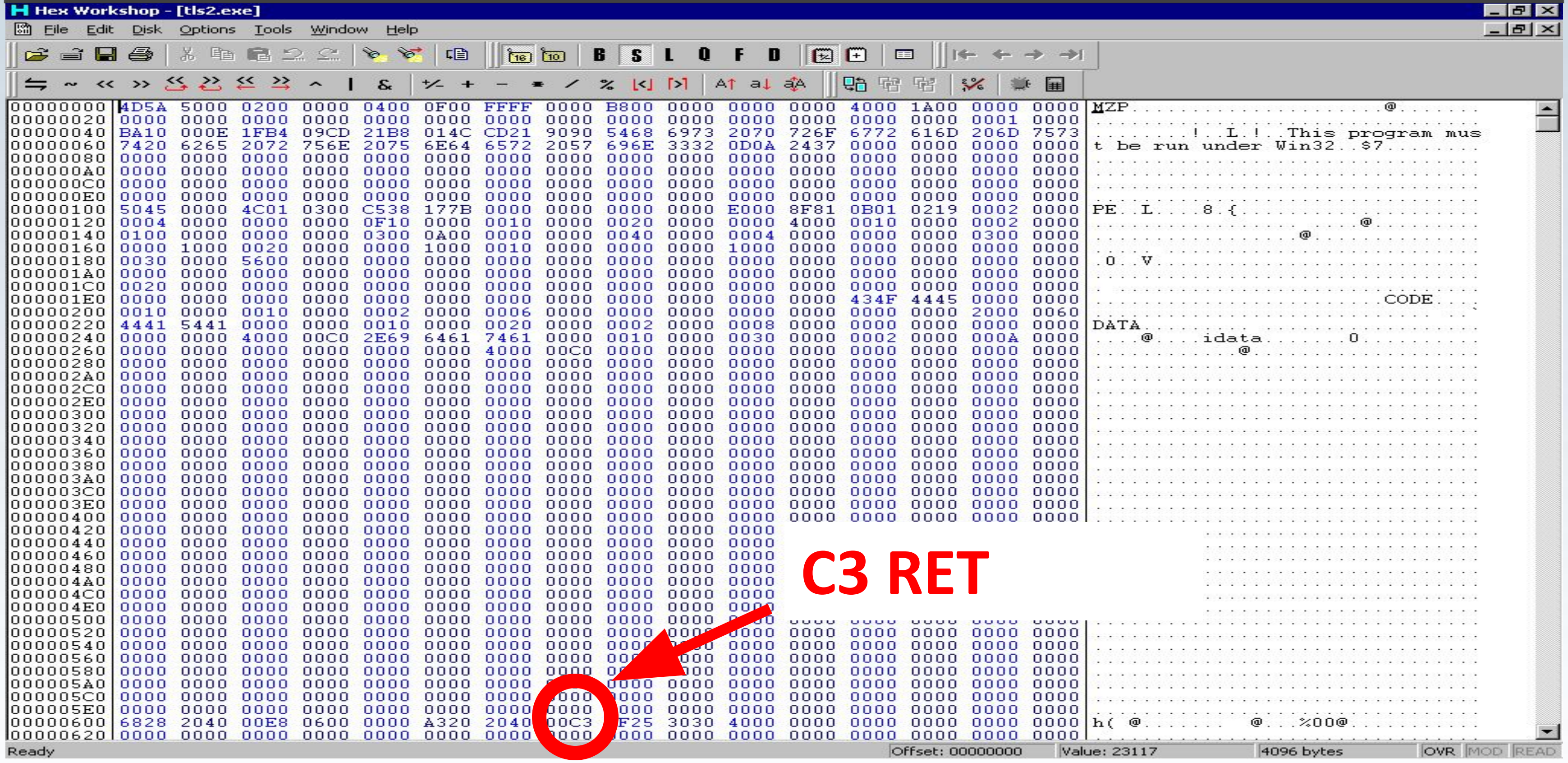
Empty!


Hex Workshop - [tls2.exe]
File Edit Disk Options Tools Window Help
Ready
Offset: 00000000
Value: 23117
4096 bytes
OVR MOD READ

```
00000000 4D5A 5000 0200 0000 0400 0F00 FFFF 0000 B800 0000 0000 0000 4000 1A00 0000 0000 MZP.....................@.......
00000020 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0001 0000 ................................
00000040 BA10 000E 1FB4 09CD 21B8 014C CD21 9090 5468 6973 2070 726F 6772 616D 206D 7573 ........!..L.!..This program mus
00000060 7420 6265 2072 756E 2075 6E64 6572 2057 696E 3332 0D0A 2437 0000 0000 0000 0000 t be run under Win32..$7........
00000080 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000000A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000000C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000000E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000100 5045 0000 4C01 0300 C538 177B 0000 0000 0000 0000 E000 8F81 0B01 0219 0002 0000 PE..L...8.{.....................
00000120 0004 0000 0000 0000 0F10 0000 0010 0000 0020 0000 0000 4000 0010 0000 0002 0000 .........................@......
00000140 0100 0000 0000 0000 0300 0A00 0000 0000 0040 0000 0004 0000 0000 0000 0300 0000 .................@..............
00000160 0000 1000 0020 0000 0000 1000 0010 0000 0000 0000 1000 0000 0000 0000 0000 0000 ................................
00000180 0030 0000 5600 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 .0..V...........................
000001A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000001C0 0020 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000001E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 434F 4445 0000 0000 ........................CODE....
00000200 0010 0000 0010 0000 0002 0000 0006 0000 0000 0000 0000 0000 0000 0000 2000 0060 ............................ ..`
00000220 4441 5441 0000 0000 0010 0000 0020 0000 0002 0000 0008 0000 0000 0000 0000 0000 DATA............................
00000240 0000 0000 4000 00C0 2E69 6461 7461 0000 0010 0000 0030 0000 0002 0000 000A 0000 .....@...idata.........0........
00000260 0000 0000 0000 0000 0000 0000 4000 00C0 0000 0000 0000 0000 0000 0000 0000 0000 .............@..................
00000280 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000002A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000002C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000002E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000300 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000320 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000340 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000360 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000380 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000003A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000003C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000003E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000400 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000420 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000440 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000460 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000480 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000004A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000004C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000004E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000500 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000520 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000540 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000560 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000580 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000005A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000005C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000005E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000600 6828 2040 00E8 0600 0000 A320 2040 00C3 FF25 3030 4000 0000 0000 0000 0000 0000 h( @........ @...%00@...........
00000620 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
```

Entry Point

Empty!


Hex Workshop - [tls2.exe]
File Edit Disk Options Tools Window Help
Ready
Offset: 00000000
Value: 23117
4096 bytes
OVR MOD READ

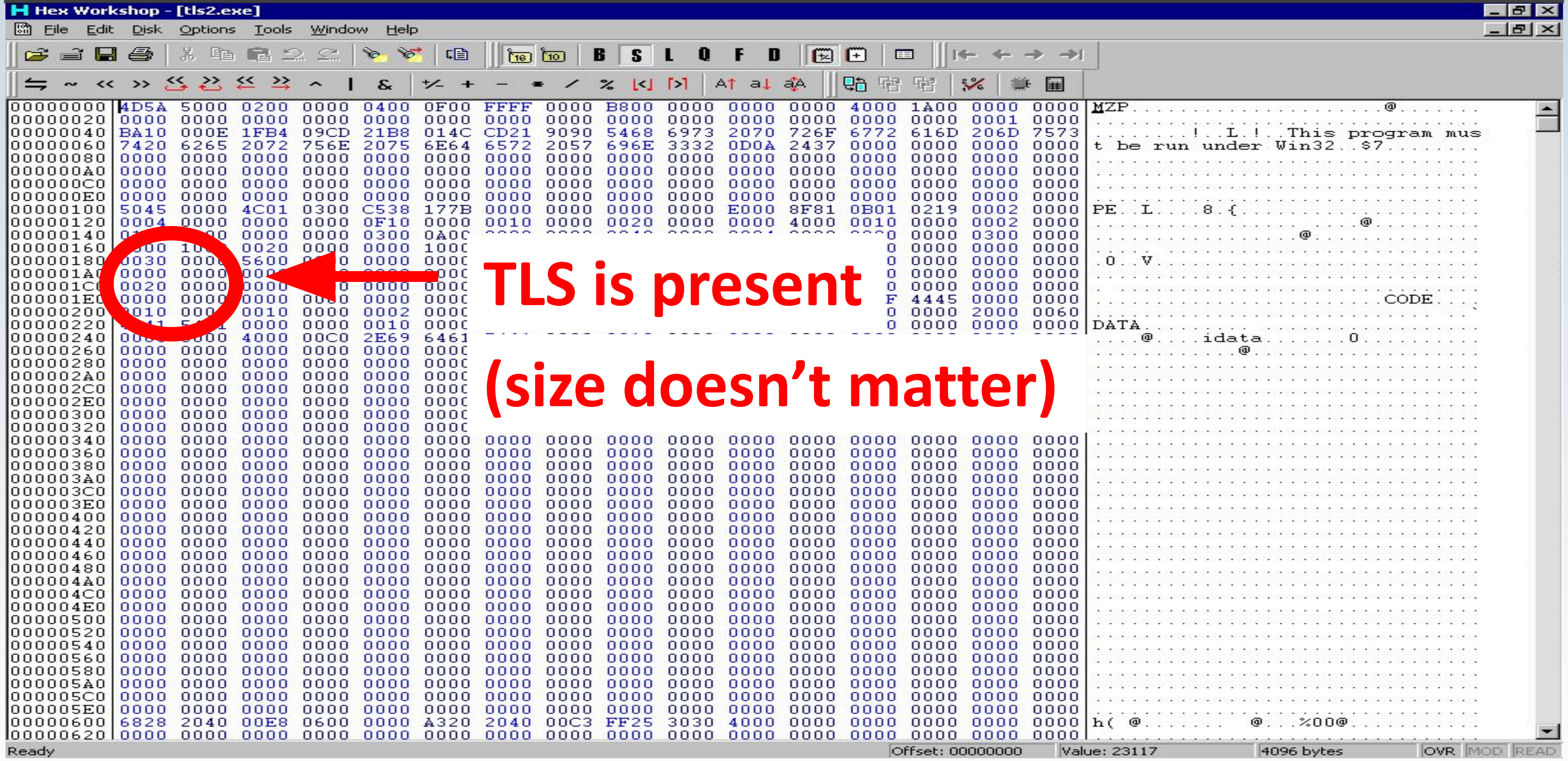
```
00000000 4D5A 5000 0200 0000 0400 0F00 FFFF 0000 B800 0000 0000 0000 4000 1A00 0000 0000 MZP.....................@.......
00000020 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0001 0000 ................................
00000040 BA10 000E 1FB4 09CD 21B8 014C CD21 9090 5468 6973 2070 726F 6772 616D 206D 7573 ........!..L.!..This program mus
00000060 7420 6265 2072 756E 2075 6E64 6572 2057 696E 3332 0D0A 2437 0000 0000 0000 0000 t be run under Win32..$7........
00000080 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000000A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000000C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000000E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000100 5045 0000 4C01 0300 C538 177B 0000 0000 0000 0000 E000 8F81 0B01 0219 0002 0000 PE..L....8.{....................
00000120 0004 0000 0000 0000 0F10 0000 0010 0000 0020 0000 0000 4000 0010 0000 0002 0000 ................. ....@.........
00000140 0100 0000 0000 0000 0300 0A00 0000 0000 0040 0000 0004 0000 0000 0000 0300 0000 .................@..............
00000160 0000 1000 0020 0000 0000 1000 0010 0000 0000 0000 1000 0000 0000 0000 0000 0000 ..... ..........................
00000180 0030 0000 5600 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 .0..V...........................
000001A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000001C0 0020 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 . ..............................
000001E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 434F 4445 0000 0000 ........................CODE....
00000200 0010 0000 0010 0000 0002 0000 0006 0000 0000 0000 0000 0000 0000 0000 2000 0060 ............................ ..`
00000220 4441 5441 0000 0000 0010 0000 0020 0000 0002 0000 0008 0000 0000 0000 0000 0000 DATA............................
00000240 0000 0000 4000 00C0 2E69 6461 7461 0000 0010 0000 0030 0000 0002 0000 000A 0000 ....@....idata.......0..........
00000260 0000 0000 0000 0000 0000 0000 4000 00C0 0000 0000 0000 0000 0000 0000 0000 0000 ............@...................
00000280 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000002A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000002C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000002E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000300 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000320 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000340 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000360 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000380 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000003A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000003C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000003E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000400 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000420 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000                          ................
00000440 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000                          ................
00000460 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000                          ................
00000480 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000                          ................
000004A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000                          ................
000004C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000                          ................
000004E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000                          ................
00000500 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000                          ................................
00000520 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000540 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000560 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000580 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000005A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000005C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000005E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000600 6828 2040 00E8 0600 0000 A320 2040 00C3 0F25 3030 4000 0000 0000 0000 0000 0000 h( @.......  @...%00@...........
00000620 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
```

C3 RET

Empty!

So the main file does nothing.
If we assume that the structure is normal,
then we could check the thread local storage table.
Just in case.

Empty!


Hex Workshop - [tls2.exe]
File Edit Disk Options Tools Window Help
B S L Q F D

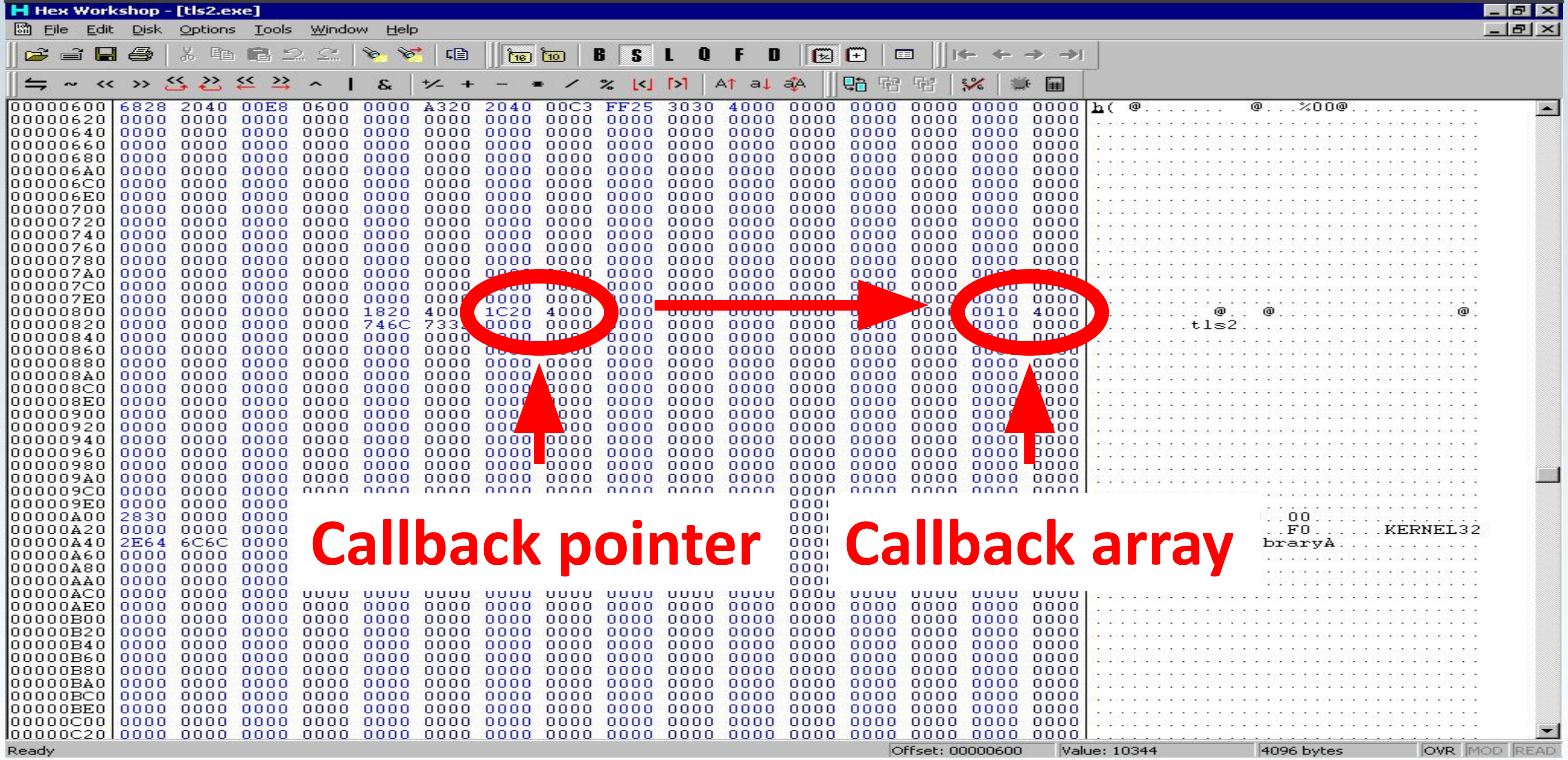
```
00000000 4D5A 5000 0200 0000 0400 0F00 FFFF 0000 B800 0000 0000 0000 4000 1A00 0000 0000 MZP.....................@.......
00000020 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0001 0000 ................................
00000040 BA10 000E 1FB4 09CD 21B8 014C CD21 9090 5468 6973 2070 726F 6772 616D 206D 7573 ........!..L.!..This program mus
00000060 7420 6265 2072 756E 2075 6E64 6572 2057 696E 3332 0D0A 2437 0000 0000 0000 0000 t be run under Win32..$7........
00000080 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000000A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000000C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000000E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000100 5045 0000 4C01 0300 C538 177B 0000 0000 0000 0000 E000 8F81 0B01 0219 0002 0000 PE..L....8.{....................
00000120 0004 0000 0000 0000 0F10 0000 0010 0000 0020 0000 0000 4000 0010 0000 0002 0000 ........................@.......
00000140                0000 0000 0300 0A00                          0000 0300 0000 ...................@............
00000160                0020 0000 0000 1000                          0000 0000 0000 ................................
00000180                5600      0000 0000                          0000 0000 0000 .0..V...........................
000001A0 0000 0000                                                   0000 0000 0000 ................................
000001C0 0020 0000                                                   0000 0000 0000 ................................
000001E0 0000 0000 0000      0000 0000                          F 4445 0000 0000 ..........................CODE....
00000200      000  0010 0000 0002 0000                          0 0000 2000 0060 ................................
00000220           0000 0000 0010 0000                          0 0000 0000 0000 DATA............................
00000240           4000 00C0 2E69 6461                                           .....@....idata........0.........
00000260 0000 0000 0000 0000 0000 0000                                           ..............@.................
00000280 0000 0000 0000 0000 0000 0000                                           ................................
000002A0 0000 0000 0000 0000 0000 0000                                           ................................
000002C0 0000 0000 0000 0000 0000 0000                                           ................................
000002E0 0000 0000 0000 0000 0000 0000                                           ................................
00000300 0000 0000 0000 0000 0000 0000                                           ................................
00000320 0000 0000 0000 0000 0000 0000                                           ................................
00000340 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000360 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000380 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000003A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000003C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000003E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000400 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000420 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000440 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000460 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000480 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000004A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000004C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000004E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000500 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000520 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000540 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000560 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000580 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000005A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000005C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
000005E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
00000600 6828 2040 00E8 0600 0000 A320 2040 00C3 FF25 3030 4000 0000 0000 0000 0000 0000 h( @.......@...%00@.............
00000620 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................
```

```
Ready    Offset: 00000000    Value: 23117    4096 bytes    OVR MOD READ
```

TLS is present

(size doesn't matter)

Empty!


Hex Workshop - [tls2.exe]
File Edit Disk Options Tools Window Help

```
00000600 6828 2040 00E8 0600 0000 A320 2040 00C3 FF25 3030 4000 0000 0000 0000 0000 0000  h( @.......@...%00@..........
00000620 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000640 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000660 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000680 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000006A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000006C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000006E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000700 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000720 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000740 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000760 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000780 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000007A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000007C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000007E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000800 0000 0000 0000 0000 1820 400  1C20 4000 0000 0000 0000 0000 0000 0000 0010 4000  ..........@...@.............@.
00000820 0000 0000 0000 0000 746C 733  0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  ........tls2....................
00000840 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000860 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000880 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000008A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000008C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000008E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000900 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000920 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000940 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000960 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000980 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000009A0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000009C0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000009E0 0000 0000 0000
00000A00 2830 0000 0000                                                                    00
00000A20 0000 0000 0000                                                                    F0.....KERNEL32
00000A40 2E64 6C6C 0000                                                                    braryA.
00000A60 0000 0000 0000
00000A80 0000 0000 0000
00000AA0 0000 0000 0000
00000AC0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000AE0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000B00 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000B20 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000B40 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000B60 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000B80 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000BA0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000BC0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000BE0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000C00 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000C20 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

Ready | Offset: 00000600 | Value: 10344 | 4096 bytes | OVR MOD READ

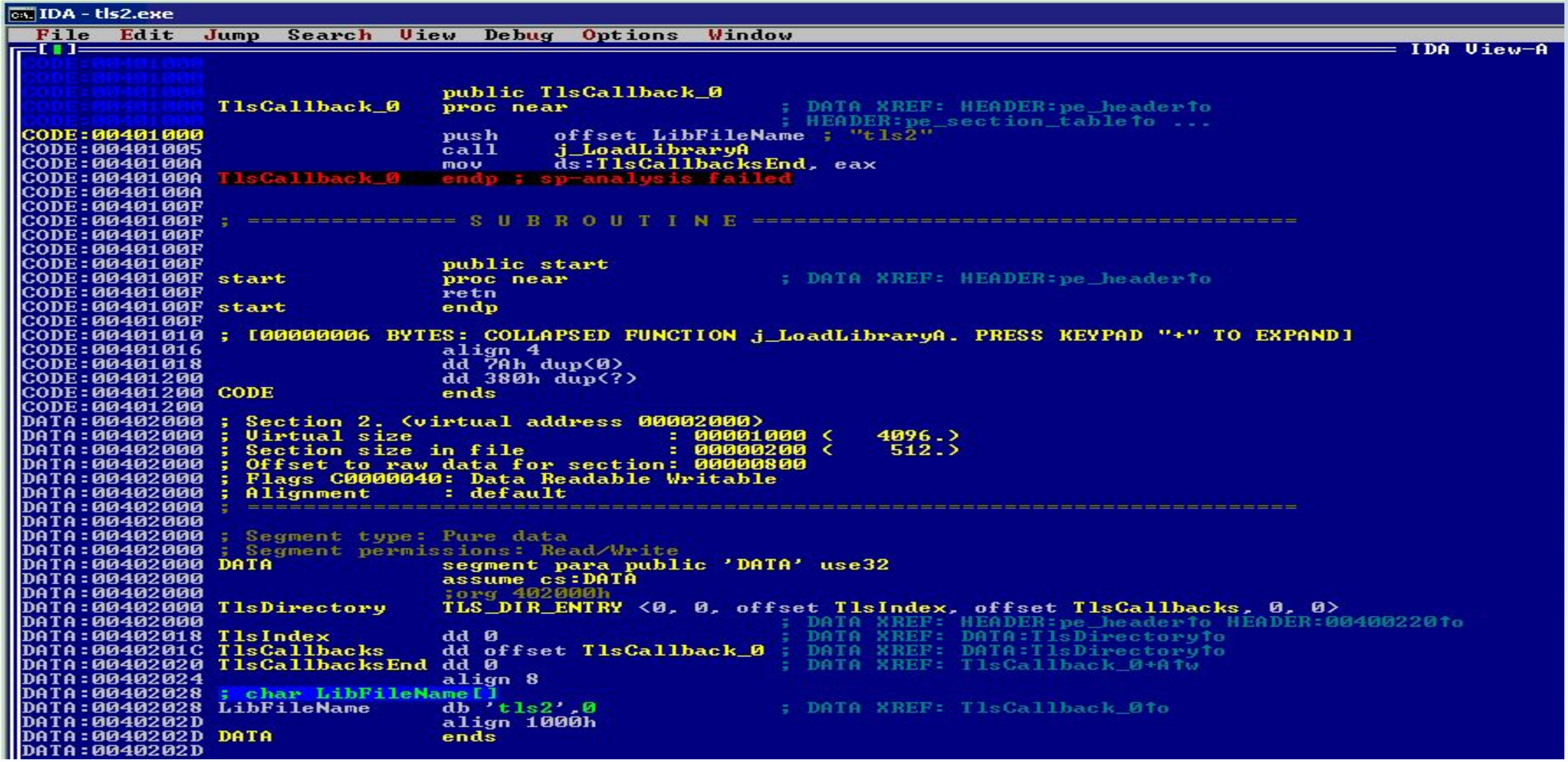
Callback pointer

Callback array

Empty!

So the search moves to the callbacks,
of which there is only one... or is there?

The One and Only



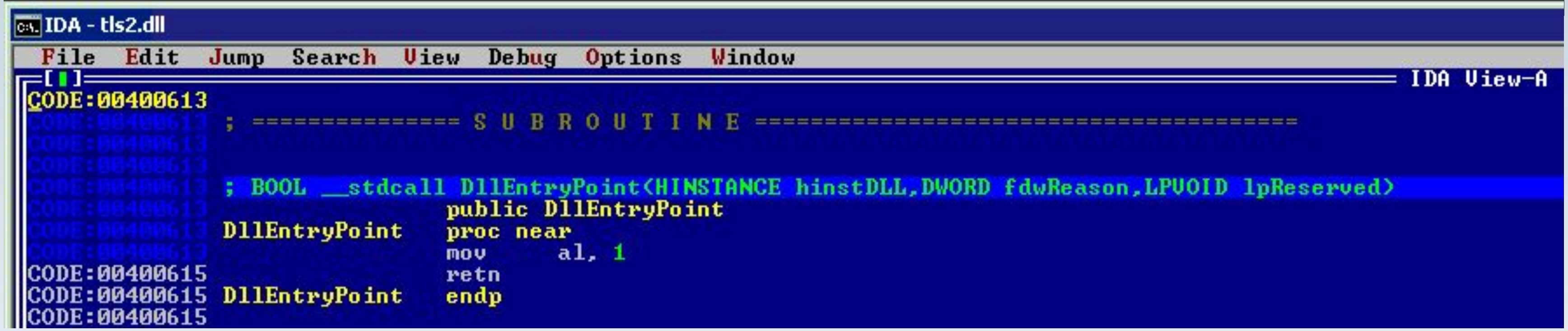
```
CODE:00401000
CODE:00401000
CODE:00401000                  public TlsCallback_0
CODE:00401000 TlsCallback_0    proc near                 ; DATA XREF: HEADER:pe_header↑o
CODE:00401000                                            ; HEADER:pe_section_table↑o ...
CODE:00401000                  push    offset LibFileName ; "tls2"
CODE:00401005                  call    j_LoadLibraryA
CODE:0040100A                  mov     ds:TlsCallbacksEnd, eax
CODE:0040100A TlsCallback_0    endp ; sp-analysis failed
CODE:0040100A
CODE:0040100F
CODE:0040100F ; =============== S U B R O U T I N E =======================================
CODE:0040100F
CODE:0040100F
CODE:0040100F                  public start
CODE:0040100F start            proc near                 ; DATA XREF: HEADER:pe_header↑o
CODE:0040100F                  retn
CODE:0040100F start            endp
CODE:0040100F
CODE:00401010 ; [00000006 BYTES: COLLAPSED FUNCTION j_LoadLibraryA. PRESS KEYPAD "+" TO EXPAND]
CODE:00401016                  align 4
CODE:00401018                  dd 7Ah dup(0)
CODE:00401200                  dd 380h dup(?)
CODE:00401200 CODE             ends
CODE:00401200
DATA:00402000 ; Section 2. (virtual address 00002000)
DATA:00402000 ; Virtual size                  : 00001000 (    4096.)
DATA:00402000 ; Section size in file          : 00000200 (     512.)
DATA:00402000 ; Offset to raw data for section: 00000800
DATA:00402000 ; Flags C0000040: Data Readable Writable
DATA:00402000 ; Alignment     : default
DATA:00402000 ; ===========================================================================
DATA:00402000
DATA:00402000 ; Segment type: Pure data
DATA:00402000 ; Segment permissions: Read/Write
DATA:00402000 DATA             segment para public 'DATA' use32
DATA:00402000                  assume cs:DATA
DATA:00402000                  ;org 402000h
DATA:00402000 TlsDirectory     TLS_DIR_ENTRY <0, 0, offset TlsIndex, offset TlsCallbacks, 0, 0>
DATA:00402000                                            ; DATA XREF: HEADER:pe_header↑o HEADER:00400220↑o
DATA:00402018 TlsIndex         dd 0                      ; DATA XREF: DATA:TlsDirectory↑o
DATA:0040201C TlsCallbacks     dd offset TlsCallback_0   ; DATA XREF: DATA:TlsDirectory↑o
DATA:00402020 TlsCallbacksEnd  dd 0                      ; DATA XREF: TlsCallback_0+A↑w
DATA:00402024                  align 8
DATA:00402028 ; char LibFileName[]
DATA:00402028 LibFileName      db 'tls2',0               ; DATA XREF: TlsCallback_0↑o
DATA:0040202D                  align 1000h
DATA:0040202D DATA             ends
DATA:0040202D
```

Am I Missing Somethi

```
CODE:00401010          push    offset LibFileName ; "tls2"
CODE:00401005          call     j_LoadLibraryA
CODE:0040100A          mov     ds:TlsCallbacksEnd, eax
```

Hmm, LoadLibrary("tls2")
Maybe DllMain contains something interesting?

I Am Missing Somethi



```
CODE:00400613
CODE:00400613 ; =============== S U B R O U T I N E =======================================
CODE:00400613
CODE:00400613
CODE:00400613 ; BOOL __stdcall DllEntryPoint(HINSTANCE hinstDLL,DWORD fdwReason,LPVOID lpReserved)
CODE:00400613                 public DllEntryPoint
CODE:00400613 DllEntryPoint   proc near
CODE:00400613                 mov     al, 1
CODE:00400615                 retn
CODE:00400615 DllEntryPoint   endp
CODE:00400615
```

No, that’s not it.

Take 2

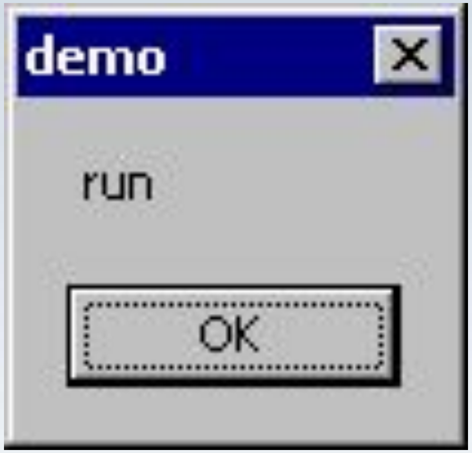
Let’s revisit the code:

```
CODE:00401010          push    offset LibFileName ; "tls2"
CODE:00401005          call     j_LoadLibraryA
CODE:0040100A          mov     ds:TlsCallbacksEnd, eax
```

It’s All About Image

It’s the TlsCallBacks extended array trick again.
Q. What value does the new callback contain?
A. The DLL’s imagebase.
Q. DEP won’t let that run, right?
A. …

Surprise!



demo

run

Not OK

Of course it will.

You just have to ask nicely.

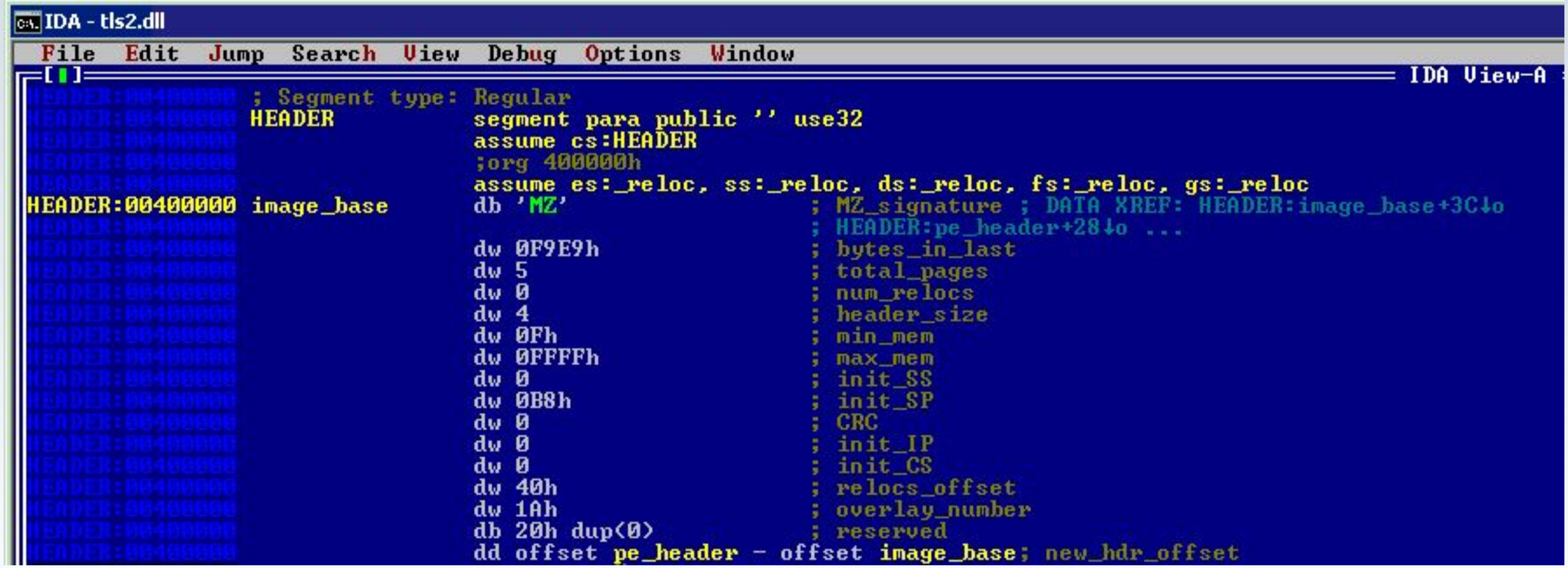
Or take a cue from a driver.

Chaotic-Evil

When the SectionAlignment value is less than 4kb, the file header is marked Writable and Executable (unless the last section characteristics override it). That turns the ImageBase into code.

Before

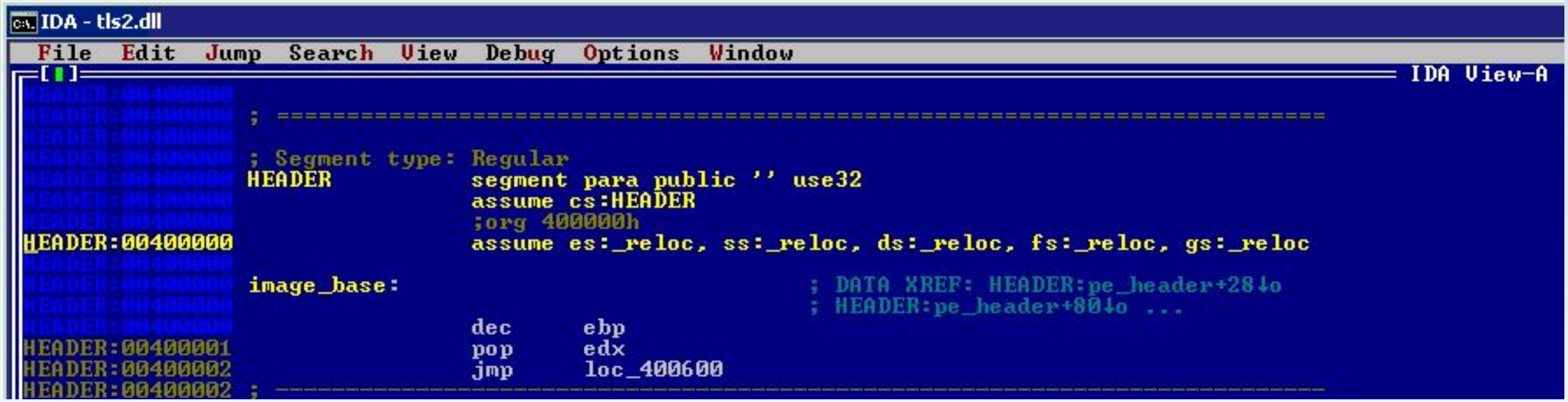
So we go from this…



```
HEADER:00400000 ; Segment type: Regular
HEADER:00400000 HEADER          segment para public '' use32
HEADER:00400000                 assume cs:HEADER
HEADER:00400000                 ;org 400000h
HEADER:00400000                 assume es:_reloc, ss:_reloc, ds:_reloc, fs:_reloc, gs:_reloc
HEADER:00400000 image_base      db 'MZ'                 ; MZ_signature ; DATA XREF: HEADER:image_base+3C↓o
HEADER:00400000                                         ; HEADER:pe_header+28↓o ...
HEADER:00400000                 dw 0F9E9h               ; bytes_in_last
HEADER:00400000                 dw 5                    ; total_pages
HEADER:00400000                 dw 0                    ; num_relocs
HEADER:00400000                 dw 4                    ; header_size
HEADER:00400000                 dw 0Fh                  ; min_mem
HEADER:00400000                 dw 0FFFFh               ; max_mem
HEADER:00400000                 dw 0                    ; init_SS
HEADER:00400000                 dw 0B8h                 ; init_SP
HEADER:00400000                 dw 0                    ; CRC
HEADER:00400000                 dw 0                    ; init_IP
HEADER:00400000                 dw 0                    ; init_CS
HEADER:00400000                 dw 40h                  ; relocs_offset
HEADER:00400000                 dw 1Ah                  ; overlay_number
HEADER:00400000                 db 20h dup(0)           ; reserved
HEADER:00400000                 dd offset pe_header - offset image_base; new_hdr_offset
```

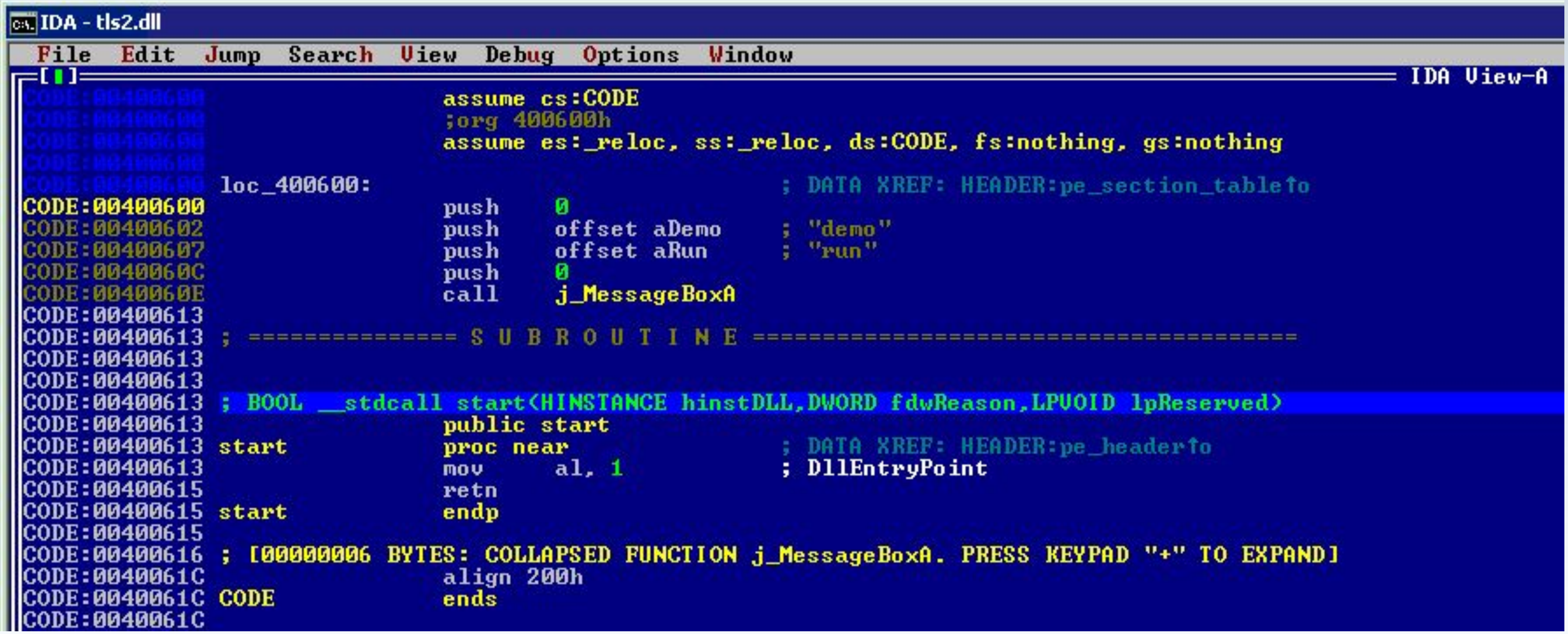
After

To this…



```
HEADER:00400000
HEADER:00400000 ; ===========================================================================
HEADER:00400000
HEADER:00400000 ; Segment type: Regular
HEADER:00400000 HEADER          segment para public '' use32
HEADER:00400000                 assume cs:HEADER
HEADER:00400000                 ;org 400000h
HEADER:00400000                 assume es:_reloc, ss:_reloc, ds:_reloc, fs:_reloc, gs:_reloc
HEADER:00400000
HEADER:00400000 image_base:                             ; DATA XREF: HEADER:pe_header+28↓o
HEADER:00400000                                         ; HEADER:pe_header+80↓o ...
HEADER:00400000
HEADER:00400000                 dec     ebp
HEADER:00400001                 pop     edx
HEADER:00400002                 jmp     loc_400600
HEADER:00400002 ; ---------------------------------------------------------------------------
```

Presto!



```
CODE:00400600                 assume cs:CODE
CODE:00400600                 ;org 400600h
CODE:00400600                 assume es:_reloc, ss:_reloc, ds:CODE, fs:nothing, gs:nothing
CODE:00400600
CODE:00400600 loc_400600:                             ; DATA XREF: HEADER:pe_section_table↑o
CODE:00400600                 push    0
CODE:00400602                 push    offset aDemo    ; "demo"
CODE:00400607                 push    offset aRun     ; "run"
CODE:0040060C                 push    0
CODE:0040060E                 call    j_MessageBoxA
CODE:00400613
CODE:00400613 ; =============== S U B R O U T I N E =======================================
CODE:00400613
CODE:00400613
CODE:00400613 ; BOOL __stdcall start(HINSTANCE hinstDLL,DWORD fdwReason,LPVOID lpReserved)
CODE:00400613                 public start
CODE:00400613 start           proc near               ; DATA XREF: HEADER:pe_header↑o
CODE:00400613                 mov     al, 1           ; DllEntryPoint
CODE:00400615                 retn
CODE:00400615 start           endp
CODE:00400615
CODE:00400616 ; [00000006 BYTES: COLLAPSED FUNCTION j_MessageBoxA. PRESS KEYPAD "+" TO EXPAND]
CODE:0040061C                 align 200h
CODE:0040061C CODE            ends
CODE:0040061C
```

Really Not OK

Just a little something to add to the workload.