



## Fun With Thread Local Sto

Peter Ferrie

Senior Anti-virus Researcher

2 July, 2008



## You Can Call Me AI

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 - [ts3.exe]

File Edit Disk Options Tools Window Help

B S L O F D

00000000 MDSA 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 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..\$?  
00000080 0000 0000 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 0000 0000  
000000C0 0000 0000 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 0000 0000  
00000100 5045 0000 4C01 0300 C538 DC81 0000 0000 0000 0000 0000 E000 8F81 0E01 0219 0002 0000 0000  
00000120 0004 0000 0000 0000 0010 0000 0010 0000 0020 0000 0000 4000 0010 0000 0000 0002 0000 0000  
00000140 0100 0000 0000 0000 0300 0A00 0000 0000 0040 0000 0000 0004 0000 0000 0000 0300 0000 0000  
00000160 0000 1000 0020 0000 0000 1000 0010 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000  
00000180 0030 0000 4800 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
000001A0 0000 0000 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 0000 0000  
000001E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 434F 4445 0000 0000 0000 0000 0000  
00000200 0010 0000 0010 0000 0002 0000 0006 0000 0000 0000 0000 0000 0000 0000 2000 0000 0000 0060  
00000220 4441 5441 0000 0000 0010 0000 0020 0000 0002 0000 0008 0000 0000 0000 0000 0000 0000 0000  
00000240 0000 0000 4000 00C0 2E69 6461 7461 0000 0010 0000 0030 0000 0002 0000 000A 0000 0000 0000  
00000260 0000 0000 0000 0000 0000 0000 4000 00C0 0000 0000 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 0000 0000  
000002A0 0000 0000 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 0000 0000  
000002E0 0000 0000 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 0000 0000  
00000320 0000 0000 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 0000 0000  
00000360 0000 0000 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 0000 0000  
000003A0 0000 0000 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 0000 0000  
000003E0 0000 0000 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 0000 0000  
00000420 0000 0000 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 0000 0000  
00000460 0000 0000 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 0000 0000  
000004A0 0000 0000 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 0000 0000  
000004E0 0000 0000 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 0000 0000  
00000520 0000 0000 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 0000 0000  
00000560 0000 0000 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 0000 0000  
000005A0 0000 0000 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 0000 0000  
000005E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
00000600 C30 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
00000620 0000 0000 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

Entry Point



# Empty!

Hex Workshop - [ts3.exe]

File Edit Disk Options Tools Window Help

B S L O 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	B410	000E	1FB4	09CD	21B8	014C	CD21	9090	5468	6973	2070	726F	6772	616D	206D	7573	.....
00000060	7420	6265	2072	756E	2075	6E64	6572	2057	696E	3332	0D0A	2437	0000	0000	0000	0000	.....
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	DC81	0000	0000	0000	0000	E000	8F81	0E01	0219	0002	0000	PE . I . . . . .
00000120	0004	0000	0000	0000	0010	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	4800	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	.....
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	434F	4445	0000	0000	0000	.....
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	.....
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	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	C3	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	.....
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



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 - [tls3.exe]

File Edit Disk Options Tools Window Help

B S L O 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 0001 0000  
00000040 BA10 000E 1FB4 09CD 21B8 014C CD21 9090 5468 6973 2070 726F 6772 616D 206D 7573  
00000060 7420 6265 2072 756E 2075 6E64 6572 2057 696E 3332 0D0A 2437 0000 0000 0000 0000  
00000080 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  
000000C0 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  
00000100 5045 0000 4C01 0300 C538 DC81 0000 0000 0000 0000 E000 8F81 0E01 0219 0002 0000  
00000120 0004 0000 0000 0000 0000 0010 0000 0010 0000 0020 0000 0000 0000 0002 0000  
00000140 0000 0160 0000 0020 0000 0000 0300 0A0C 0000 0000 0000 0000 0000 0300 0000  
00000160 0000 0160 0000 0020 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
00000180 0030 0000 4800 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
000001A0 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  
000001E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 F 4445 0000 0000 0000 0000  
00000200 0010 0000 0010 0000 0002 000C 0000 0000 0000 0000 0000 0000 2000 0060  
00000220 0011 5000 0000 0000 0010 000C 0000 0000 0000 0000 0000 0000 0000 0000  
00000240 0000 0000 4000 00C0 2E69 6461 0000 0000 0000 0000 0000 0000 0000 0000 0000  
00000260 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
00000280 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  
000002C0 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  
00000300 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  
00000340 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  
00000380 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  
000003C0 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  
00000400 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  
00000440 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  
00000480 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  
000004C0 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  
00000500 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  
00000540 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  
00000580 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  
000005C0 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  
00000600 C300 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
00000620 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





Empty!

So the search moves to the callbacks,  
of which there is only one, but it looks peculiar.  
It's not a virtual address.





## The One and Only

```
C:\IDA - tls3.exe
File Edit Jump Search View Debug Options Window
[ ] IDA View-A
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 ; 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 ;
DATA:0040201C ; Imports from TLS3.dll
DATA:0040201C ;
DATA:0040201C TlsCallbacks dd 3042h ; DATA XREF: DATA:TlsDirectory!o
DATA:0040201C ; .idata:import_directory!o
DATA:00402020 TlsCallbacksEnd dd 0
DATA:00402024 align 1000h
DATA:00402024 DATA ends
DATA:00402024
```



## Imported TLS callbac

We know that the TLS callback array can be altered at runtime.  
We know that the TLS callbacks can point outside of the image.  
Now we are looking at a new way to achieve that.  
Imports are resolved before TLS callbacks are called.  
So TLS callbacks can be imported addresses!  
Let's check the import table.



### The Search Goes On

The screenshot shows the Hex Workshop interface with a memory dump. The address range is from 00000600 to 00000C20. The dump contains hexadecimal data and ASCII characters. A red arrow points from the text 'TLS3.DLL' to a red circle containing 'TLS3.dll' in the ASCII column. The status bar at the bottom indicates 'Offset: 00000600', 'Value: 195', and '4096 bytes'.

Address	Hex	ASCII
00000600	C300 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	
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 4000 1C20 4000 0000 0000 0000 0000 0000 0000 4230 0000	@ @ B0
00000820	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	
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 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	
00000A00	2830 0000 0000 0000 0000 0000 3830 0000 1C20 0000 0000 0000 0000 0000 0000 0000	
00000A20	0000 0000 0000 0000 0000 0000 4230 0000 0000 0000 0000 0000 0000 0000 0000 0000	
00000A40	0000 0000 6100 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	
00000A60	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	
00000A80	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	
00000AA0	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 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	





## The Search Goes On

So the search moves to TLS3.DLL,  
and the mysterious function called 'a'.





### 'A' function

```
IDA - tls3.dll
File Edit Jump Search View Debug Options Window IDA View-A
[ ]
CODE:00401000 ; File Name : C:\Users\Peter\z\tls3.dll
CODE:00401000 ; Format : Portable executable for 80386 <PE>
CODE:00401000 ; Imagebase : 400000
CODE:00401000 ; Section 1. (virtual address 00001000)
CODE:00401000 ; Virtual size : 00001000 ( 4096.)
CODE:00401000 ; Section size in file : 00000200 ( 512.)
CODE:00401000 ; Offset to raw data for section: 00000600
CODE:00401000 ; Flags 60000020: Text Executable Readable
CODE:00401000 ; Alignment : default
CODE:00401000 ; Exported entry 1. a
CODE:00401000 ;
CODE:00401000 ; =====
CODE:00401000 ; Segment type: Pure code
CODE:00401000 ; Segment permissions: Read/Execute
CODE:00401000 CODE segment para public 'CODE' use32
CODE:00401000 assume cs:CODE
CODE:00401000 org 401000h
CODE:00401000 assume es:_reloc, ss:_reloc, ds:CODE, fs:nothing, gs:nothing
CODE:00401000 ; ===== SUBROUTINE =====
CODE:00401000
CODE:00401000 public a
CODE:00401000 a proc near ; DATA XREF: HEADER:pe_headerfo
CODE:00401000 ; HEADER:pe_section_tablefo ...
CODE:00401000 push 0 ; uType
CODE:00401000 push offset Caption ; "demo"
CODE:00401000 push offset Text ; "run"
CODE:00401000 push 0 ; hWnd
CODE:00401000 call j_MessageBoxA
CODE:00401000 a endp ; sp-analysis failed
CODE:00401000 ; ===== SUBROUTINE =====
CODE:00401000 ; BOOL __stdcall start(HINSTANCE hinstDLL,DWORD fdwReason,LPUOID lpReserved)
CODE:00401000 public start
CODE:00401000 start proc near ; DATA XREF: HEADER:pe_headerfo
CODE:00401000 mov al, 1 ;DllEntryPoint
CODE:00401000 ret
CODE:00401000 start endp
CODE:00401015
```



## The 'Aha' Moment

So that's how it's done.  
If we let it run...



Surprise!





Not OK

The code runs.



Really Not OK

Just a little something to add to the workload.