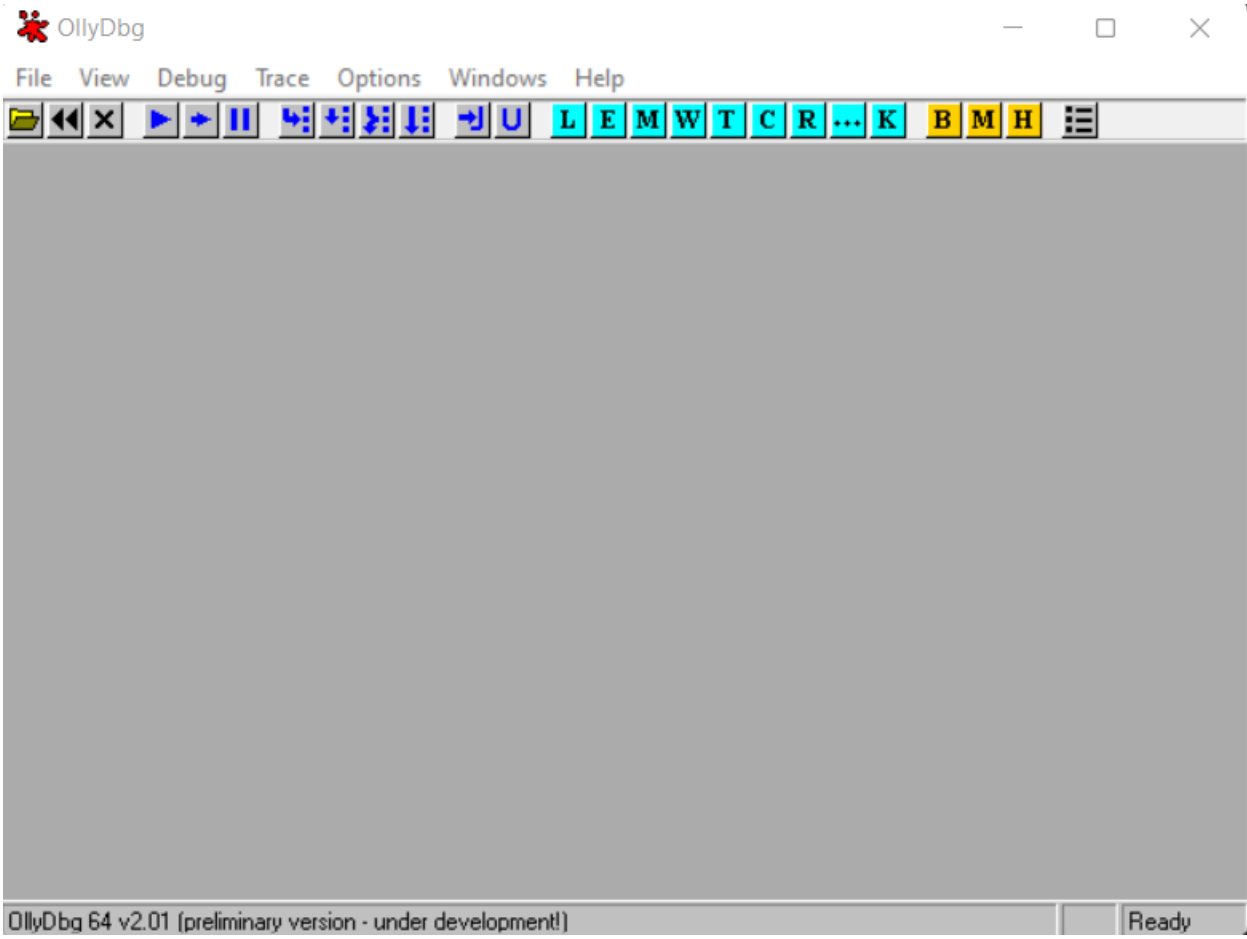
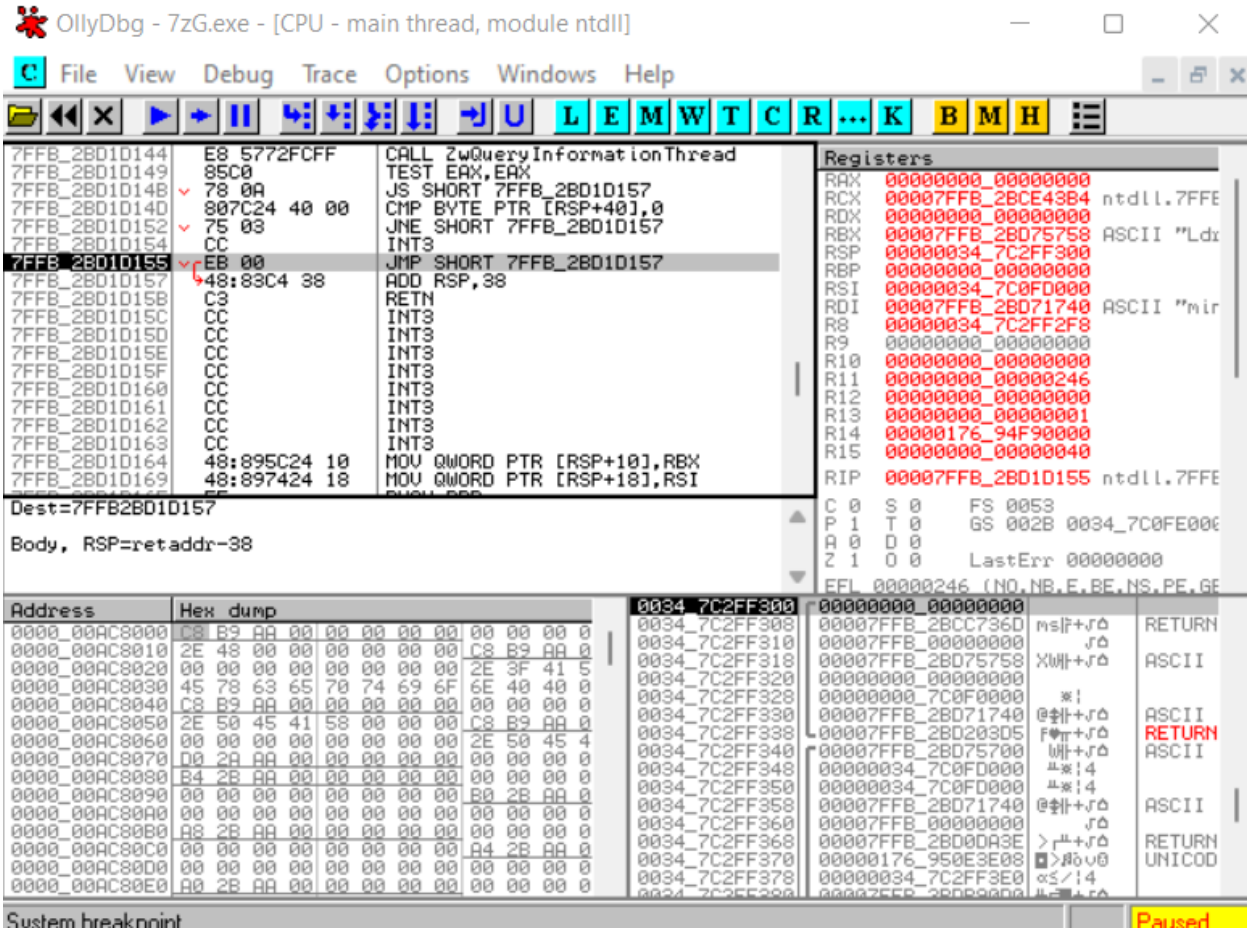
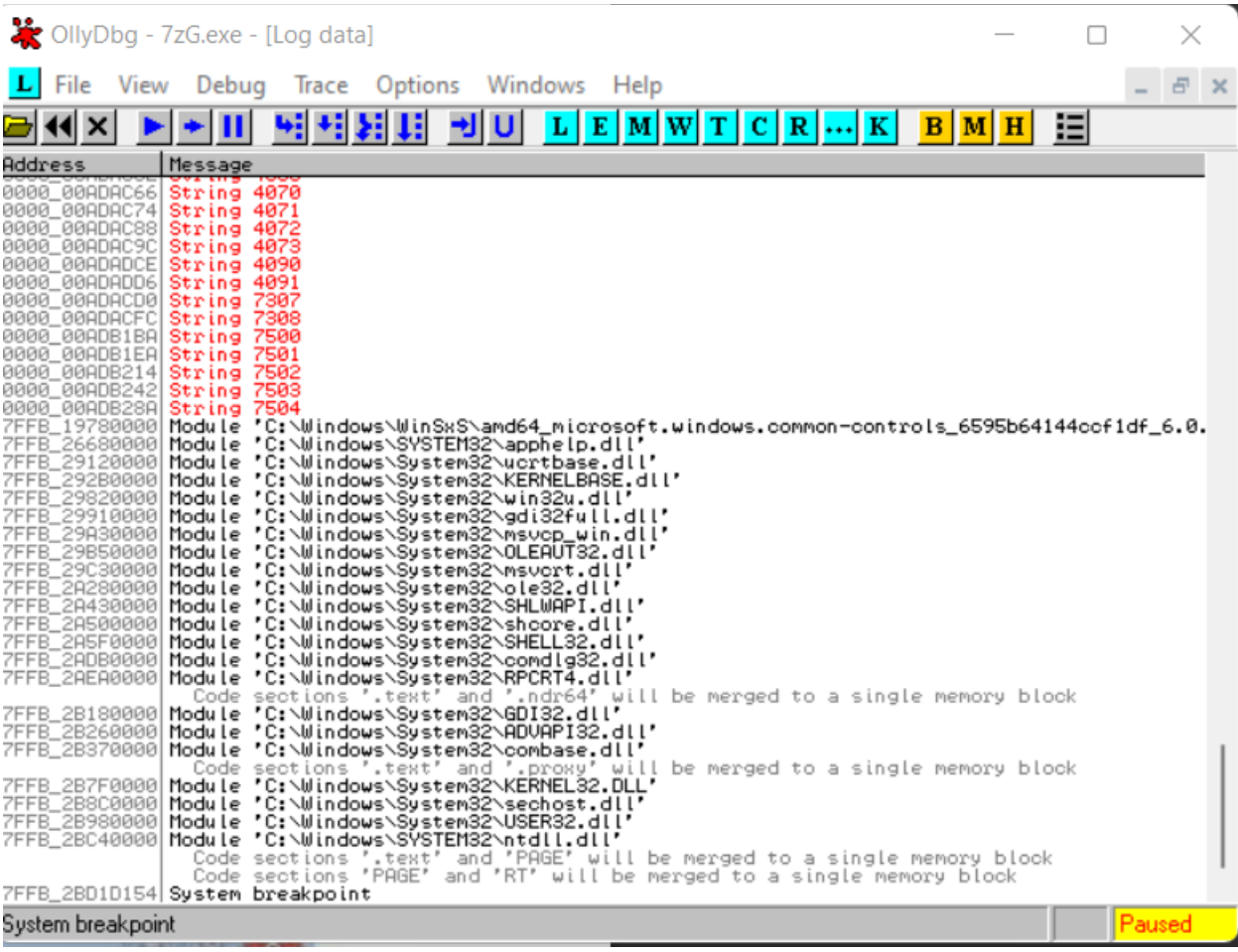
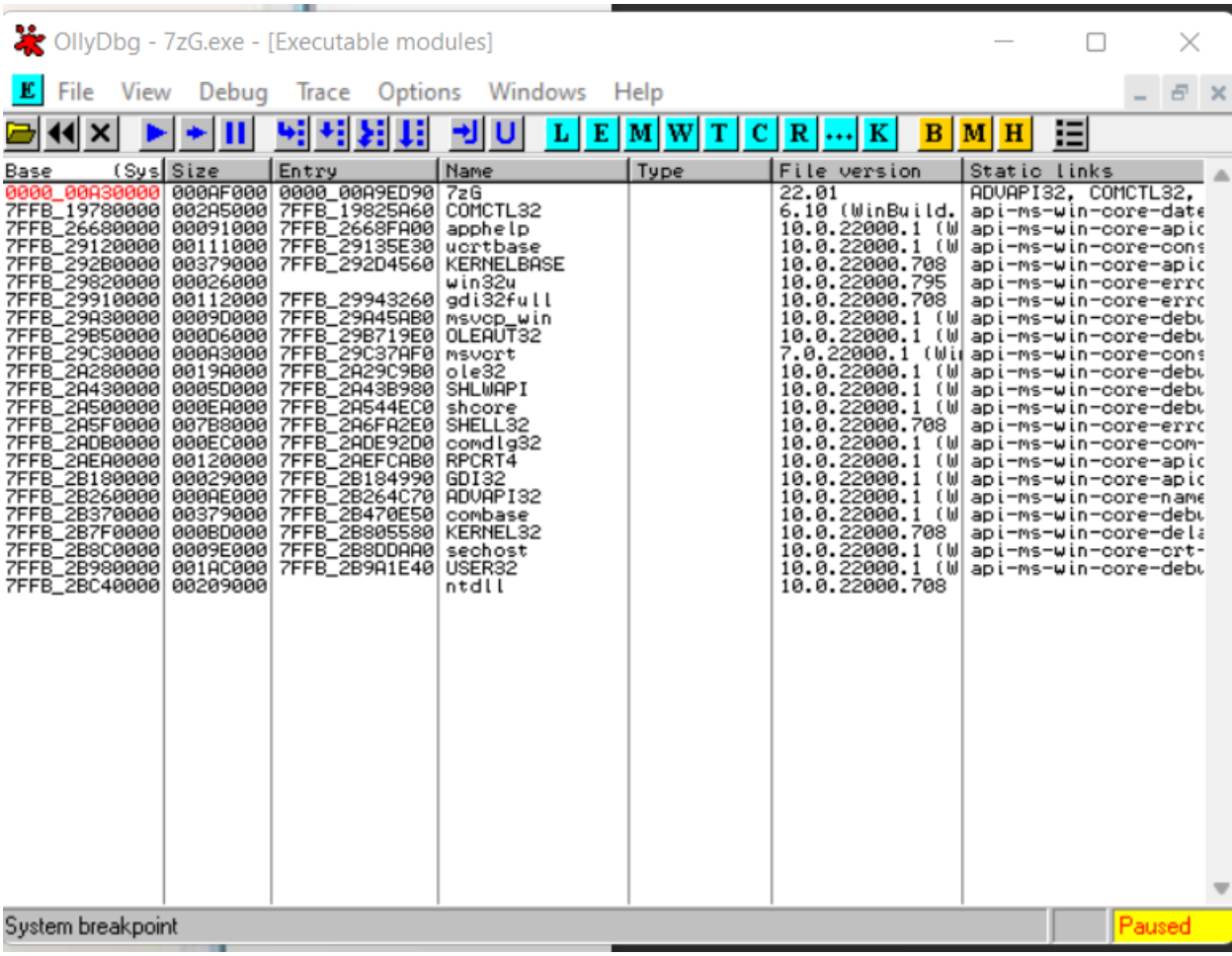
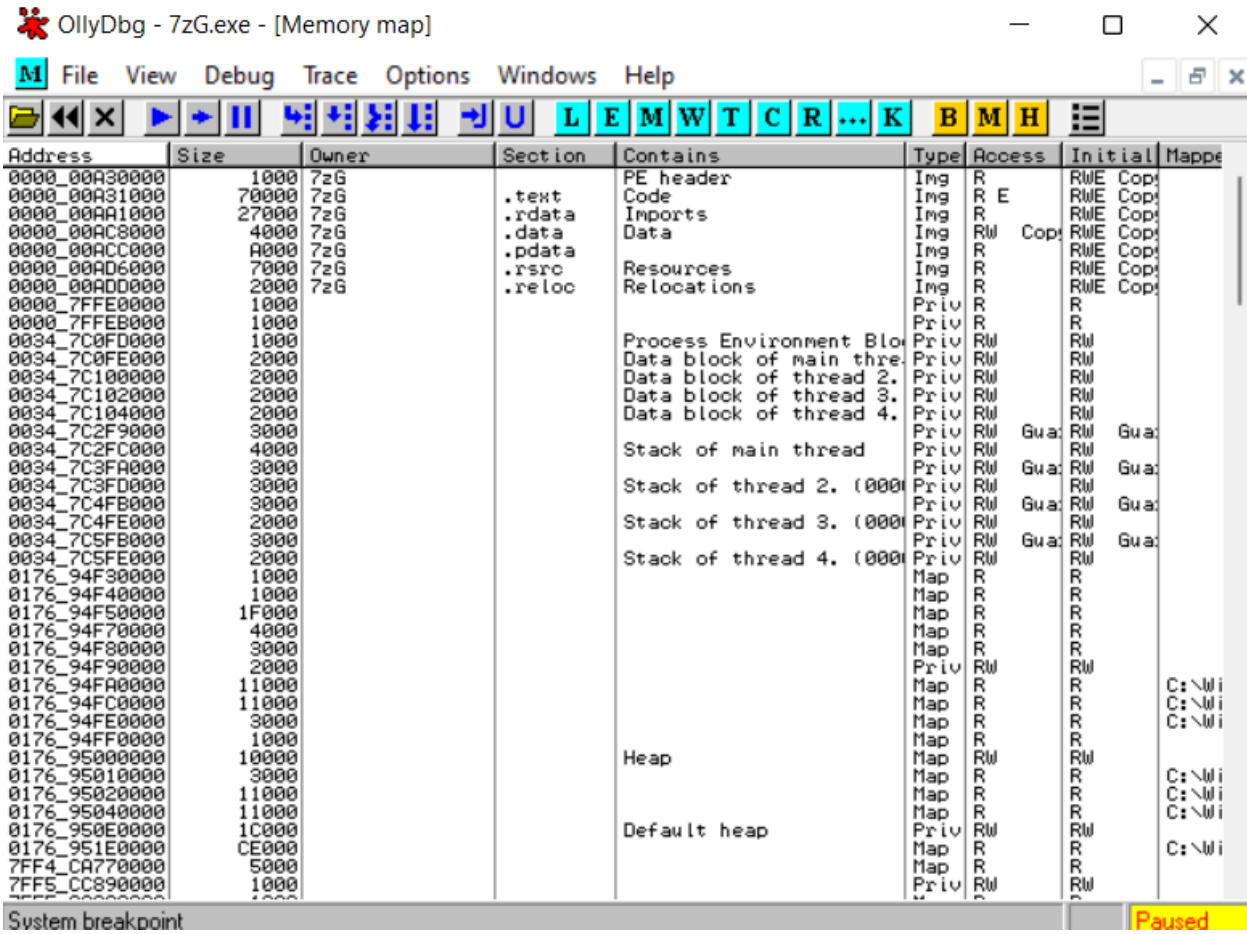
EX. NO. 16 - Virus Analysis using OllyDb

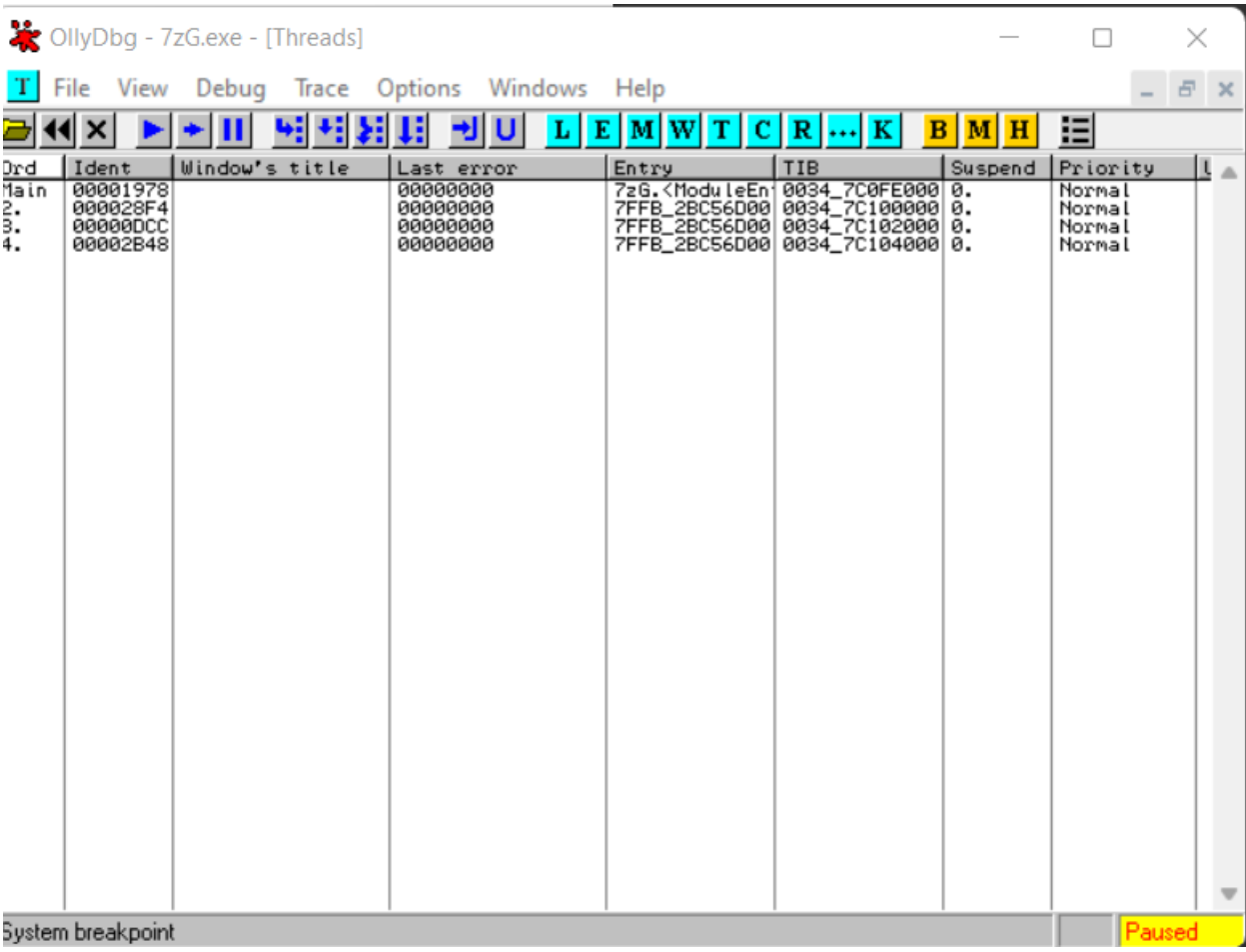



OllyDbg - 7zG.exe - [CPU - main thread, module ntdll]
File View Debug Trace Options Windows Help
7FFB_2BD1D144 E8 5772FCFF CALL ZwQueryInformationThread
7FFB_2BD1D149 85C0 TEST EAX,EAX
7FFB_2BD1D14B 78 0A JS SHORT 7FFB_2BD1D157
7FFB_2BD1D14D 807C24 40 00 CMP BYTE PTR [RSP+40],0
7FFB_2BD1D152 75 03 JNE SHORT 7FFB_2BD1D157
7FFB_2BD1D154 CC INT3
7FFB_2BD1D155 EB 00 JMP SHORT 7FFB_2BD1D157
7FFB_2BD1D157 48:83C4 38 ADD RSP,38
7FFB_2BD1D15B C3 RETN
Dest=7FFB2BD1D157
Body, RSP=retaddr-38
Registers
RAX 00000000_00000000
RCX 00007FFB_2BCE43B4 ntdll.7FFE
RDX 00000000_00000000
RBX 00007FFB_2BD75758 ASCII "Ldr
RSP 00000034_7C2FF300
RBP 00000000_00000000
RSI 00000034_7C0FD000
RDI 00007FFB_2BD71740 ASCII "mir
R8 00000034_7C2FF2F8
R9 00000000_00000000
R10 00000000_00000000
R11 00000000_00000246
R12 00000000_00000000
R13 00000000_00000001
R14 00000176_94F90000
R15 00000000_00000040
RIP 00007FFB_2BD1D155 ntdll.7FFE
C 0 S 0 FS 0053
P 1 T 0 GS 002B 0034_7C0FE000
A 0 D 0
Z 1 O 0 LastErr 00000000
EFL 00000246 (NO,NB,E,BE,NS,PE,GE
Address Hex dump
0034_7C2FF300 00000000_00000000
System breakpoint
Paused


OllyDbg - 7zG.exe - [Log data]
File View Debug Trace Options Windows Help
Address Message
0000_00ADAC66 String 4070
0000_00ADAC74 String 4071
0000_00ADAC88 String 4072
0000_00ADAC9C String 4073
0000_00ADADCE String 4090
0000_00ADADD6 String 4091
0000_00ADACD0 String 7307
0000_00ADACFC String 7308
0000_00ADB1BA String 7500
0000_00ADB1EA String 7501
0000_00ADB214 String 7502
0000_00ADB242 String 7503
0000_00ADB28A String 7504
7FFB_19780000 Module 'C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.
7FFB_26680000 Module 'C:\Windows\SYSTEM32\apphelp.dll'
7FFB_29120000 Module 'C:\Windows\System32\ucrtbase.dll'
7FFB_292B0000 Module 'C:\Windows\System32\KERNELBASE.dll'
7FFB_29820000 Module 'C:\Windows\System32\win32u.dll'
7FFB_29910000 Module 'C:\Windows\System32\gdi32full.dll'
7FFB_29A30000 Module 'C:\Windows\System32\msvcp_win.dll'
7FFB_29B50000 Module 'C:\Windows\System32\OLEAUT32.dll'
7FFB_29C30000 Module 'C:\Windows\System32\msvcrt.dll'
7FFB_2A280000 Module 'C:\Windows\System32\ole32.dll'
7FFB_2A430000 Module 'C:\Windows\System32\SHLWAPI.dll'
7FFB_2A500000 Module 'C:\Windows\System32\shcore.dll'
7FFB_2A5F0000 Module 'C:\Windows\System32\SHELL32.dll'
7FFB_2ADB0000 Module 'C:\Windows\System32\comdlg32.dll'
7FFB_2AEA0000 Module 'C:\Windows\System32\RPCRT4.dll'
Code sections '.text' and '.ndr64' will be merged to a single memory block
7FFB_2B180000 Module 'C:\Windows\System32\GDI32.dll'
7FFB_2B260000 Module 'C:\Windows\System32\ADVAPI32.dll'
7FFB_2B370000 Module 'C:\Windows\System32\combase.dll'
Code sections '.text' and '.proxy' will be merged to a single memory block
7FFB_2B7F0000 Module 'C:\Windows\System32\KERNEL32.DLL'
7FFB_2B8C0000 Module 'C:\Windows\System32\sechost.dll'
7FFB_2B980000 Module 'C:\Windows\System32\USER32.dll'
7FFB_2BC40000 Module 'C:\Windows\SYSTEM32\ntdll.dll'
Code sections '.text' and 'PAGE' will be merged to a single memory block
Code sections 'PAGE' and 'RT' will be merged to a single memory block
7FFB_2BD1D154 System breakpoint
System breakpoint
Paused


OllyDbg - 7zG.exe - [Executable modules]
File View Debug Trace Options Windows Help
L E M W T C R ... K B M H
Base (Sys Size Entry Name Type File version Static links
0000_00A30000 000AF000 0000_00A9ED90 7zG 22.01 ADVAPI32, COMCTL32,
7FFB_19780000 002A5000 7FFB_19825A60 COMCTL32 6.10 (WinBuild. api-ms-win-core-date
7FFB_26680000 00091000 7FFB_2668FA00 apphelp 10.0.22000.1 (W api-ms-win-core-apic
7FFB_29120000 00111000 7FFB_29135E30 ucrtbase 10.0.22000.1 (W api-ms-win-core-cons
7FFB_292B0000 00379000 7FFB_292D4560 KERNELBASE 10.0.22000.708 api-ms-win-core-apic
7FFB_29820000 00026000 win32u 10.0.22000.795 api-ms-win-core-erro
7FFB_29910000 00112000 7FFB_29943260 gdi32full 10.0.22000.708 api-ms-win-core-erro
7FFB_29A30000 0009D000 7FFB_29A45AB0 msvcp_win 10.0.22000.1 (W api-ms-win-core-debu
7FFB_29B50000 000D6000 7FFB_29B719E0 OLEAUT32 10.0.22000.1 (W api-ms-win-core-debu
7FFB_29C30000 000A3000 7FFB_29C37AF0 msvcrt 7.0.22000.1 (Wi api-ms-win-core-cons
7FFB_2A280000 0019A000 7FFB_2A29C9B0 ole32 10.0.22000.1 (W api-ms-win-core-debu
7FFB_2A430000 0005D000 7FFB_2A43B980 SHLWAPI 10.0.22000.1 (W api-ms-win-core-debu
7FFB_2A500000 000EA000 7FFB_2A544EC0 shcore 10.0.22000.1 (W api-ms-win-core-debu
7FFB_2A5F0000 007B8000 7FFB_2A6FA2E0 SHELL32 10.0.22000.708 api-ms-win-core-erro
7FFB_2ADB0000 000EC000 7FFB_2ADE92D0 comdlg32 10.0.22000.1 (W api-ms-win-core-com-
7FFB_2AEA0000 00120000 7FFB_2AEFCAB0 RPCRT4 10.0.22000.1 (W api-ms-win-core-apic
7FFB_2B180000 00029000 7FFB_2B184990 GDI32 10.0.22000.1 (W api-ms-win-core-apic
7FFB_2B260000 000AE000 7FFB_2B264C70 ADVAPI32 10.0.22000.1 (W api-ms-win-core-name
7FFB_2B370000 00379000 7FFB_2B470E50 combase 10.0.22000.1 (W api-ms-win-core-debu
7FFB_2B7F0000 000BD000 7FFB_2B805580 KERNEL32 10.0.22000.708 api-ms-win-core-dela
7FFB_2B8C0000 0009E000 7FFB_2B8DDAA0 sechost 10.0.22000.1 (W api-ms-win-core-crt-
7FFB_2B980000 001AC000 7FFB_2B9A1E40 USER32 10.0.22000.1 (W api-ms-win-core-debu
7FFB_2BC40000 00209000 ntdll 10.0.22000.708
System breakpoint
Paused


OllyDbg - 7zG.exe - [Memory map]
File View Debug Trace Options Windows Help
L E M W T C R ... K B M H
Address Size Owner Section Contains Type Access Initial Mappe
0000_00A30000 1000 7zG PE header Img R RWE Cop
0000_00A31000 70000 7zG .text Code Img R E RWE Cop
0000_00AA1000 27000 7zG .rdata Imports Img R RWE Cop
0000_00AC8000 4000 7zG .data Data Img RW Cop RWE Cop
0000_00ACC000 A000 7zG .pdata Img R RWE Cop
0000_00AD6000 7000 7zG .rsrc Resources Img R RWE Cop
0000_00ADD000 2000 7zG .reloc Relocations Img R RWE Cop
0000_7FFE0000 1000 Priv R R
0000_7FFEB000 1000 Priv R R
0034_7C0FD000 1000 Process Environment Blo Priv RW RW
0034_7C0FE000 2000 Data block of main thre Priv RW RW
0034_7C100000 2000 Data block of thread 2. Priv RW RW
0034_7C102000 2000 Data block of thread 3. Priv RW RW
0034_7C104000 2000 Data block of thread 4. Priv RW RW
0034_7C2F9000 3000 Priv RW Gua RW Gua
0034_7C2FC000 4000 Stack of main thread Priv RW RW
0034_7C3FA000 3000 Priv RW Gua RW Gua
0034_7C3FD000 3000 Stack of thread 2. (000 Priv RW RW
0034_7C4FB000 3000 Priv RW Gua RW Gua
0034_7C4FE000 2000 Stack of thread 3. (000 Priv RW RW
0034_7C5FB000 3000 Priv RW Gua RW Gua
0034_7C5FE000 2000 Stack of thread 4. (000 Priv RW RW
0176_94F30000 1000 Map R R
0176_94F40000 1000 Map R R
0176_94F50000 1F000 Map R R
0176_94F70000 4000 Map R R
0176_94F80000 3000 Map R R
0176_94F90000 2000 Priv RW RW
0176_94FA0000 11000 Map R R C:\Wi
0176_94FC0000 11000 Map R R C:\Wi
0176_94FE0000 3000 Map R R C:\Wi
0176_94FF0000 1000 Map R R
0176_95000000 10000 Heap Map RW RW
0176_95010000 3000 Map R R C:\Wi
0176_95020000 11000 Map R R C:\Wi
0176_95040000 11000 Map R R C:\Wi
0176_950E0000 1C000 Default heap Priv RW RW
0176_951E0000 CE000 Map R R C:\Wi
7FF4_CA770000 5000 Map R R
7FF5_CC890000 1000 Priv RW RW
System breakpoint
Paused


OllyDbg - 7zG.exe - [Threads]
File View Debug Trace Options Windows Help
Ord Ident Window's title Last error Entry TIB Suspend Priority
Main 00001978 00000000 7zG.<ModuleEn 0034_7C0FE000 0. Normal
2. 000028F4 00000000 7FFB_2BC56D00 0034_7C100000 0. Normal
3. 00000DCC 00000000 7FFB_2BC56D00 0034_7C102000 0. Normal
4. 00002B48 00000000 7FFB_2BC56D00 0034_7C104000 0. Normal
System breakpoint
Paused