COMPX508 – Malware Analysis

Week 11

Lecture 2: Dynamic Analysis with a debugger

Vimal Kumar

Debugging in malware analysis

- Interactive debugging
  - A debugger offers the ability to monitor the behaviour of code as it is being executed.
  - Can pause the execution where-ever we want
    - Helps us slow the execution down to study the behaviour

- There are several open-source debuggers for executables
  - x64dbg
  - windbg
  - ollydbg
  - Ghidra
  - etc.

https://help.x64dbg.com/en/latest/introduction/index.html

Objectives

- General Objectives
  - Understand malware behaviour
  - Bypass obfuscation and sandbox detection
  - Extract meaningful information like keys, IP addresses, domain names

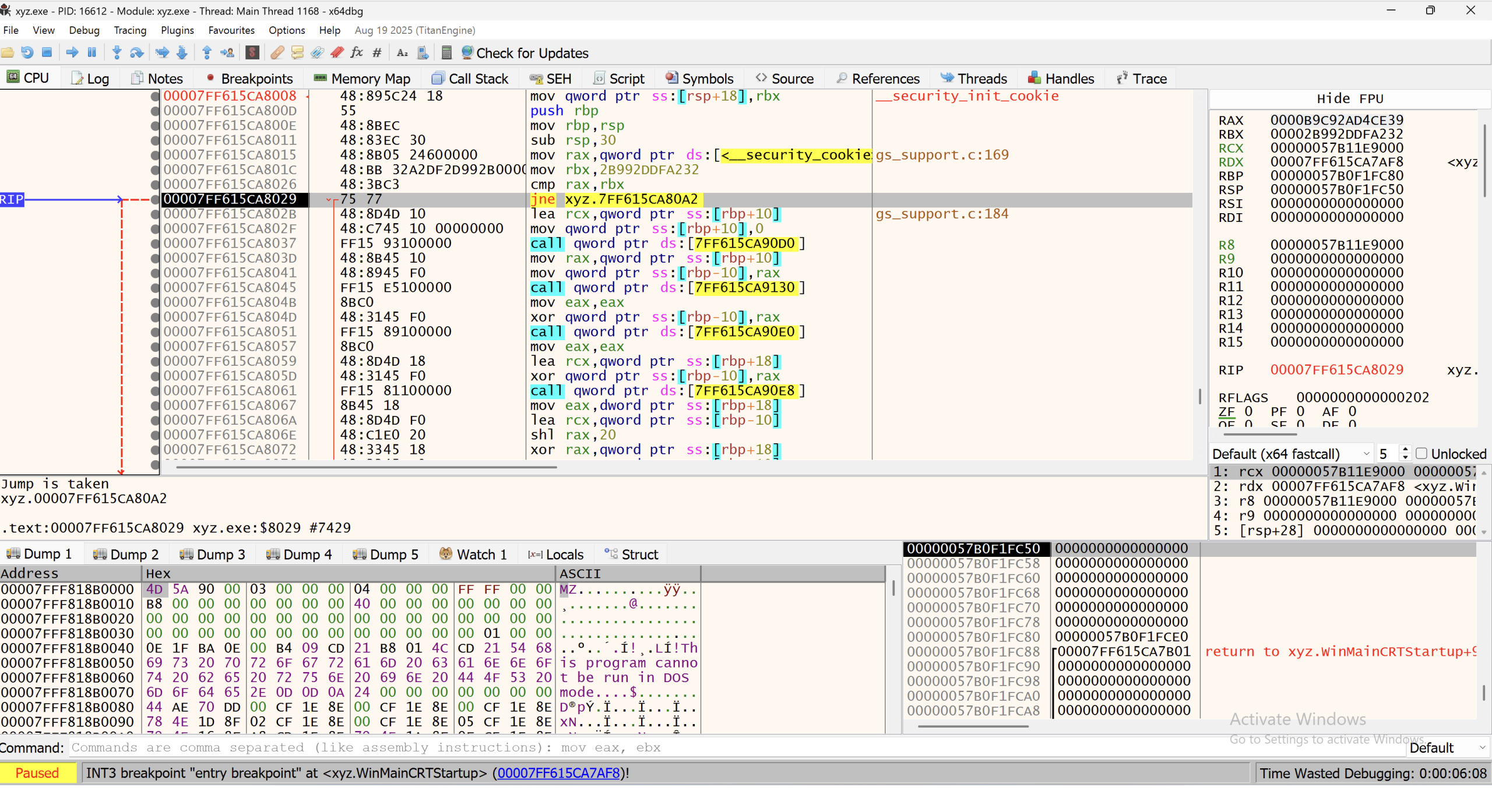
- Specific Objectives
  - Modify code to make the malware work the way we want
    - Identify and bypass anti-analysis code
  - Track register values and memory locations (variables) to extract information such as keys, domain names, IP addresses etc.
  - Trace execution flow
  - Unpack, packed malware – before it is executed.

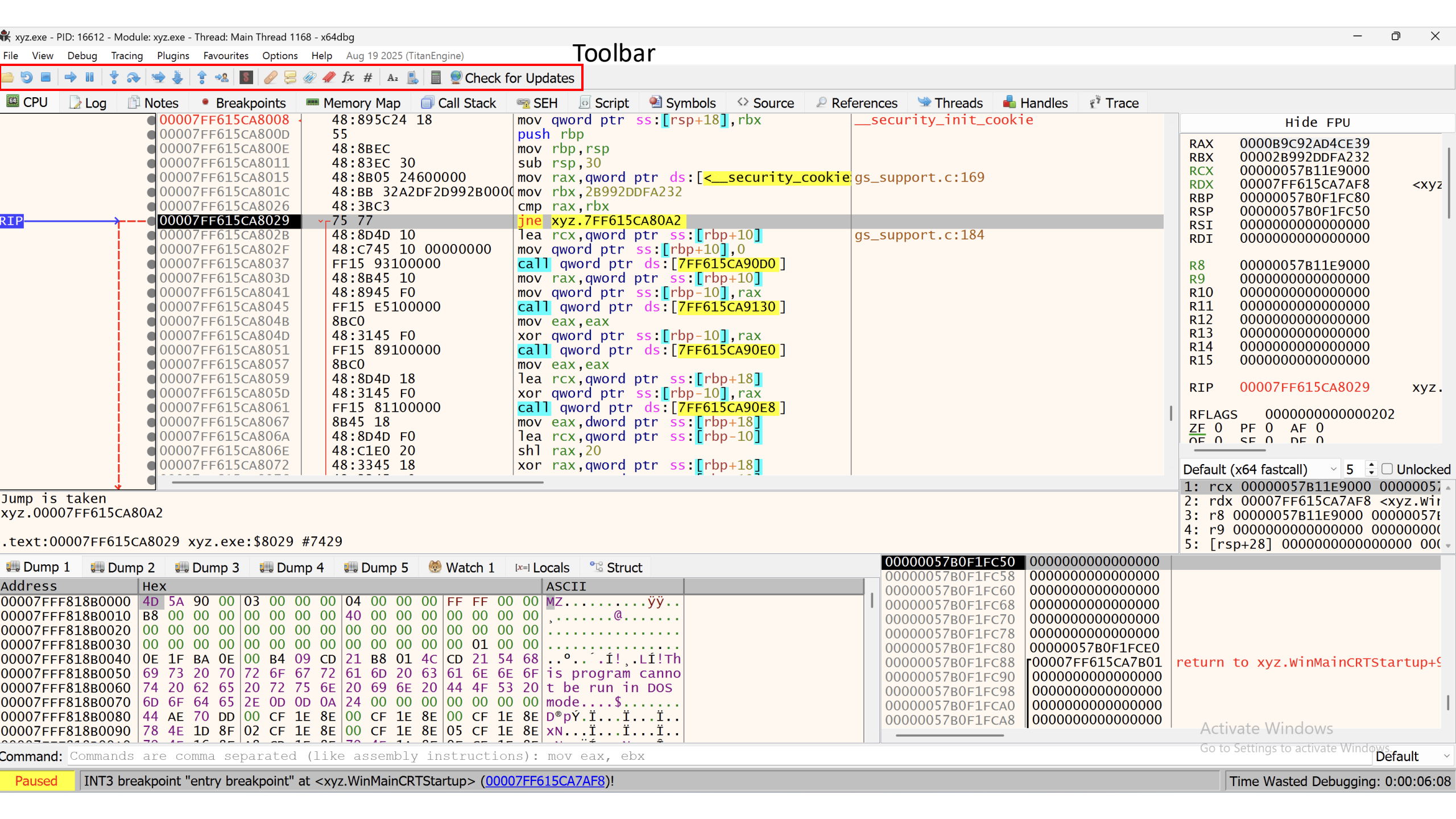
Breakpoints

- Used for pausing the execution of the program
- There are many kinds of breakpoints
- Entry Breakpoint
  - Breaks at the entry point of the application
  - Usually this is where we want to start
- Execution Breakpoint
  - Most common breakpoint.
  - When you toggle a breakpoint on a specific address, this tell the debugger to stop when that address is reached in the execution.
- Memory Breakpoint
  - Breaks when a particular memory address is read, written to or accessed.

Using x64dbg

- Open a file
- Restart debugging the file
- Stop Execution
- Start Execution
- Pause Execution
- Step into
  - Go to the next instruction
  - If there is a function call go to the first instruction of the function call
- Step over
  - Go to the next instruction
  - If there is a function call execute the entire functionand go to the instruction just after it


xyz.exe - PID: 16612 - Module: xyz.exe - Thread: Main Thread 1168 - x64dbg
File View Debug Tracing Plugins Favourites Options Help Aug 19 2025 (TitanEngine)
Check for Updates
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
00007FF615CA8008 48:895C24 18 mov qword ptr ss:[rsp+18],rbx __security_init_cookie
00007FF615CA800D 55 push rbp
00007FF615CA800E 48:8BEC mov rbp,rsp
00007FF615CA8011 48:83EC 30 sub rsp,30
00007FF615CA8015 48:8B05 24600000 mov rax,qword ptr ds:[<__security_cookie gs_support.c:169
00007FF615CA801C 48:BB 32A2DF2D992B0000 mov rbx,2B992DDFA232
00007FF615CA8026 48:3BC3 cmp rax,rbx
RIP 00007FF615CA8029 75 77 jne xyz.7FF615CA80A2
00007FF615CA802B 48:8D4D 10 lea rcx,qword ptr ss:[rbp+10] gs_support.c:184
00007FF615CA802F 48:C745 10 00000000 mov qword ptr ss:[rbp+10],0
00007FF615CA8037 FF15 93100000 call qword ptr ds:[7FF615CA90D0]
00007FF615CA803D 48:8B45 10 mov rax,qword ptr ss:[rbp+10]
00007FF615CA8041 48:8945 F0 mov qword ptr ss:[rbp-10],rax
00007FF615CA8045 FF15 E5100000 call qword ptr ds:[7FF615CA9130]
00007FF615CA804B 8BC0 mov eax,eax
00007FF615CA804D 48:3145 F0 xor qword ptr ss:[rbp-10],rax
00007FF615CA8051 FF15 89100000 call qword ptr ds:[7FF615CA90E0]
00007FF615CA8057 8BC0 mov eax,eax
00007FF615CA8059 48:8D4D 18 lea rcx,qword ptr ss:[rbp+18]
00007FF615CA805D 48:3145 F0 xor qword ptr ss:[rbp-10],rax
00007FF615CA8061 FF15 81100000 call qword ptr ds:[7FF615CA90E8]
00007FF615CA8067 8B45 18 mov eax,dword ptr ss:[rbp+18]
00007FF615CA806A 48:8D4D F0 lea rcx,qword ptr ss:[rbp-10]
00007FF615CA806E 48:C1E0 20 shl rax,20
00007FF615CA8072 48:3345 18 xor rax,qword ptr ss:[rbp+18]
Hide FPU
RAX 0000B9C92AD4CE39
RBX 00002B992DDFA232
RCX 00000057B11E9000
RDX 00007FF615CA7AF8 <xyz
RBP 00000057B0F1FC80
RSP 00000057B0F1FC50
RSI 0000000000000000
RDI 0000000000000000
R8 00000057B11E9000
R9 0000000000000000
R10 0000000000000000
R11 0000000000000000
R12 0000000000000000
R13 0000000000000000
R14 0000000000000000
R15 0000000000000000
RIP 00007FF615CA8029 xyz.
RFLAGS 0000000000000202
ZF 0 PF 0 AF 0
Default (x64 fastcall) 5 Unlocked
1: rcx 00000057B11E9000
2: rdx 00007FF615CA7AF8 <xyz.Wi
3: r8 00000057B11E9000
4: r9 0000000000000000
5: [rsp+28] 0000000000000000
Jump is taken
xyz.00007FF615CA80A2
.text:00007FF615CA8029 xyz.exe:$8029 #7429
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Address Hex ASCII
00007FFF818B0000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..
00007FFF818B0010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
00007FFF818B0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00007FFF818B0030 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ....
00007FFF818B0040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..º..´.Í!¸.LÍ!Th
00007FFF818B0050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00007FFF818B0060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00007FFF818B0070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
00007FFF818B0080 44 AE 70 DD 00 CF 1E 8E 00 CF 1E 8E 00 CF 1E 8E D®pÝ.Ï...Ï...Ï..
00007FFF818B0090 78 4E 1D 8F 02 CF 1E 8E 00 CF 1E 8E 05 CF 1E 8E xN...Ï...Ï...Ï..
00000057B0F1FC50 0000000000000000
00000057B0F1FC58 0000000000000000
00000057B0F1FC60 0000000000000000
00000057B0F1FC68 0000000000000000
00000057B0F1FC70 0000000000000000
00000057B0F1FC78 0000000000000000
00000057B0F1FC80 00000057B0F1FCE0
00000057B0F1FC88 00007FF615CA7B01 return to xyz.WinMainCRTStartup+9
00000057B0F1FC90 0000000000000000
00000057B0F1FC98 0000000000000000
00000057B0F1FCA0 0000000000000000
00000057B0F1FCA8 0000000000000000
Activate Windows
Go to Settings to activate Windows.
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Default
Paused
INT3 breakpoint "entry breakpoint" at <xyz.WinMainCRTStartup> (00007FF615CA7AF8)!
Time Wasted Debugging: 0:00:06:08


xyz.exe - PID: 16612 - Module: xyz.exe - Thread: Main Thread 1168 - x64dbg
File View Debug Tracing Plugins Favourites Options Help Aug 19 2025 (TitanEngine)
Toolbar
Check for Updates
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
00007FF615CA8008 48:895C24 18 mov qword ptr ss:[rsp+18],rbx __security_init_cookie
00007FF615CA800D 55 push rbp
00007FF615CA800E 48:8BEC mov rbp,rsp
00007FF615CA8011 48:83EC 30 sub rsp,30
00007FF615CA8015 48:8B05 24600000 mov rax,qword ptr ds:[<__security_cookie gs_support.c:169
00007FF615CA801C 48:BB 32A2DF2D992B0000 mov rbx,2B992DDFA232
00007FF615CA8026 48:3BC3 cmp rax,rbx
RIP 00007FF615CA8029 75 77 jne xyz.7FF615CA80A2
00007FF615CA802B 48:8D4D 10 lea rcx,qword ptr ss:[rbp+10] gs_support.c:184
00007FF615CA802F 48:C745 10 00000000 mov qword ptr ss:[rbp+10],0
00007FF615CA8037 FF15 93100000 call qword ptr ds:[7FF615CA90D0]
00007FF615CA803D 48:8B45 10 mov rax,qword ptr ss:[rbp+10]
00007FF615CA8041 48:8945 F0 mov qword ptr ss:[rbp-10],rax
00007FF615CA8045 FF15 E5100000 call qword ptr ds:[7FF615CA9130]
00007FF615CA804B 8BC0 mov eax,eax
00007FF615CA804D 48:3145 F0 xor qword ptr ss:[rbp-10],rax
00007FF615CA8051 FF15 89100000 call qword ptr ds:[7FF615CA90E0]
00007FF615CA8057 8BC0 mov eax,eax
00007FF615CA8059 48:8D4D 18 lea rcx,qword ptr ss:[rbp+18]
00007FF615CA805D 48:3145 F0 xor qword ptr ss:[rbp-10],rax
00007FF615CA8061 FF15 81100000 call qword ptr ds:[7FF615CA90E8]
00007FF615CA8067 8B45 18 mov eax,dword ptr ss:[rbp+18]
00007FF615CA806A 48:8D4D F0 lea rcx,qword ptr ss:[rbp-10]
00007FF615CA806E 48:C1E0 20 shl rax,20
00007FF615CA8072 48:3345 18 xor rax,qword ptr ss:[rbp+18]
Hide FPU
RAX 0000B9C92AD4CE39
RBX 00002B992DDFA232
RCX 00000057B11E9000
RDX 00007FF615CA7AF8 <xyz
RBP 00000057B0F1FC80
RSP 00000057B0F1FC50
RSI 0000000000000000
RDI 0000000000000000
R8 00000057B11E9000
R9 0000000000000000
R10 0000000000000000
R11 0000000000000000
R12 0000000000000000
R13 0000000000000000
R14 0000000000000000
R15 0000000000000000
RIP 00007FF615CA8029 xyz.
RFLAGS 0000000000000202
ZF 0 PF 0 AF 0
Default (x64 fastcall) 5 Unlocked
1: rcx 00000057B11E9000
2: rdx 00007FF615CA7AF8 <xyz.wi
3: r8 00000057B11E9000
4: r9 0000000000000000
5: [rsp+28] 0000000000000000
Jump is taken
xyz.00007FF615CA80A2
.text:00007FF615CA8029 xyz.exe:$8029 #7429
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Address Hex ASCII
00007FFF818B0000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..
00007FFF818B0010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
00007FFF818B0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00007FFF818B0030 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ....
00007FFF818B0040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..º..´.Í!¸.LÍ!Th
00007FFF818B0050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00007FFF818B0060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00007FFF818B0070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
00007FFF818B0080 44 AE 70 DD 00 CF 1E 8E 00 CF 1E 8E 00 CF 1E 8E D®pÝ.Ï...Ï...Ï..
00007FFF818B0090 78 4E 1D 8F 02 CF 1E 8E 00 CF 1E 8E 05 CF 1E 8E xN...Ï...Ï...Ï..
00000057B0F1FC50 0000000000000000
00000057B0F1FC58 0000000000000000
00000057B0F1FC60 0000000000000000
00000057B0F1FC68 0000000000000000
00000057B0F1FC70 0000000000000000
00000057B0F1FC78 0000000000000000
00000057B0F1FC80 00000057B0F1FCE0
00000057B0F1FC88 00007FF615CA7B01 return to xyz.WinMainCRTStartup+9
00000057B0F1FC90 0000000000000000
00000057B0F1FC98 0000000000000000
00000057B0F1FCA0 0000000000000000
00000057B0F1FCA8 0000000000000000
Activate Windows
Go to Settings to activate Windows.
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Default
Paused
INT3 breakpoint "entry breakpoint" at <xyz.WinMainCRTStartup> (00007FF615CA7AF8)!
Time Wasted Debugging: 0:00:06:08

Program execution views

xyz.exe - PID: 16612 - Module: xyz.exe - Thread: Main Thread 1168 - x64dbg

File View Debug Tracing Plugins Favourites Options Help Aug 19 2025 (TitanEngine)

Check for Updates

CPU | Log | Notes | Breakpoints | Memory Map | Call Stack | SEH | Script | Symbols | Source | References | Threads | Handles | Trace

```
00007FF615CA8008   48:895C24 18      mov qword ptr ss:[rsp+18],rbx      __security_init_cookie
00007FF615CA800D   55                push rbp
00007FF615CA800E   48:8BEC           mov rbp,rsp
00007FF615CA8011   48:83EC 30        sub rsp,30
00007FF615CA8015   48:8B05 24600000  mov rax,qword ptr ds:[<__security_cookie  gs_support.c:169
00007FF615CA801C   48:BB 32A2DF2D992B0000 mov rbx,2B992DDFA232
00007FF615CA8026   48:3BC3           cmp rax,rbx
RIP 00007FF615CA8029   75 77         jne xyz.7FF615CA80A2
00007FF615CA802B   48:8D4D 10        lea rcx,qword ptr ss:[rbp+10]      gs_support.c:184
00007FF615CA802F   48:C745 10 00000000 mov qword ptr ss:[rbp+10],0
00007FF615CA8037   FF15 93100000     call qword ptr ds:[7FF615CA90D0]
00007FF615CA803D   48:8B45 10        mov rax,qword ptr ss:[rbp+10]
00007FF615CA8041   48:8945 F0        mov qword ptr ss:[rbp-10],rax
00007FF615CA8045   FF15 E5100000     call qword ptr ds:[7FF615CA9130]
00007FF615CA804B   8BC0              mov eax,eax
00007FF615CA804D   48:3145 F0        xor qword ptr ss:[rbp-10],rax
00007FF615CA8051   FF15 89100000     call qword ptr ds:[7FF615CA90E0]
00007FF615CA8057   8BC0              mov eax,eax
00007FF615CA8059   48:8D4D 18        lea rcx,qword ptr ss:[rbp+18]
00007FF615CA805D   48:3145 F0        xor qword ptr ss:[rbp-10],rax
00007FF615CA8061   FF15 81100000     call qword ptr ds:[7FF615CA90E8]
00007FF615CA8067   8B45 18           mov eax,dword ptr ss:[rbp+18]
00007FF615CA806A   48:8D4D F0        lea rcx,qword ptr ss:[rbp-10]
00007FF615CA806E   48:C1E0 20        shl rax,20
00007FF615CA8072   48:3345 18        xor rax,qword ptr ss:[rbp+18]
```

Hide FPU

```
RAX   0000B9C92AD4CE39
RBX   00002B992DDFA232
RCX   00000057B11E9000
RDX   00007FF615CA7AF8   <xyz
RBP   00000057B0F1FC80
RSP   00000057B0F1FC50
RSI   0000000000000000
RDI   0000000000000000

R8    00000057B11E9000
R9    0000000000000000
R10   0000000000000000
R11   0000000000000000
R12   0000000000000000
R13   0000000000000000
R14   0000000000000000
R15   0000000000000000

RIP   00007FF615CA8029   xyz.

RFLAGS   0000000000000202
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
```

Default (x64 fastcall) 5 Unlocked

```
1: rcx 00000057B11E9000 0000005
2: rdx 00007FF615CA7AF8 <xyz.Wi
3: r8 00000057B11E9000 00000057
4: r9 0000000000000000 00000000
5: [rsp+28] 0000000000000000 00
```

```
Jump is taken
xyz.00007FF615CA80A2

.text:00007FF615CA8029 xyz.exe:$8029 #7429
```

Dump 1 | Dump 2 | Dump 3 | Dump 4 | Dump 5 | Watch 1 | Locals | Struct

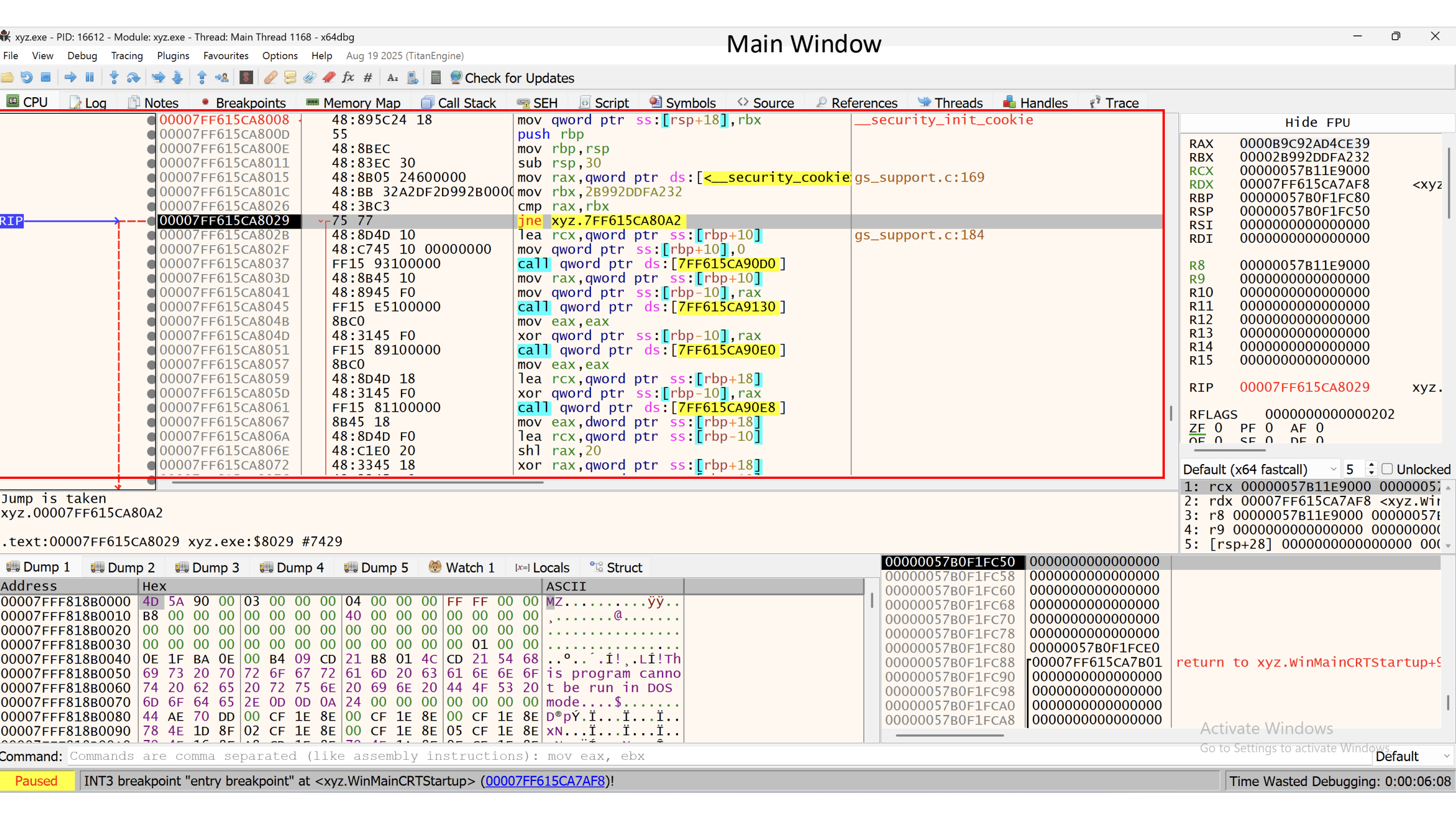
Address	Hex	ASCII
00007FFF818B0000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....ÿÿ..
00007FFF818B0010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	¸.......@.......
00007FFF818B0020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00007FFF818B0030	00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00	....
00007FFF818B0040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	..º..´.Í!¸.LÍ!Th
00007FFF818B0050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
00007FFF818B0060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
00007FFF818B0070	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode....$.......
00007FFF818B0080	44 AE 70 DD 00 CF 1E 8E 00 CF 1E 8E 00 CF 1E 8E	D®pÝ.Ï...Ï...Ï..
00007FFF818B0090	78 4E 1D 8F 02 CF 1E 8E 00 CF 1E 8E 05 CF 1E 8E	xN...Ï...Ï...Ï..

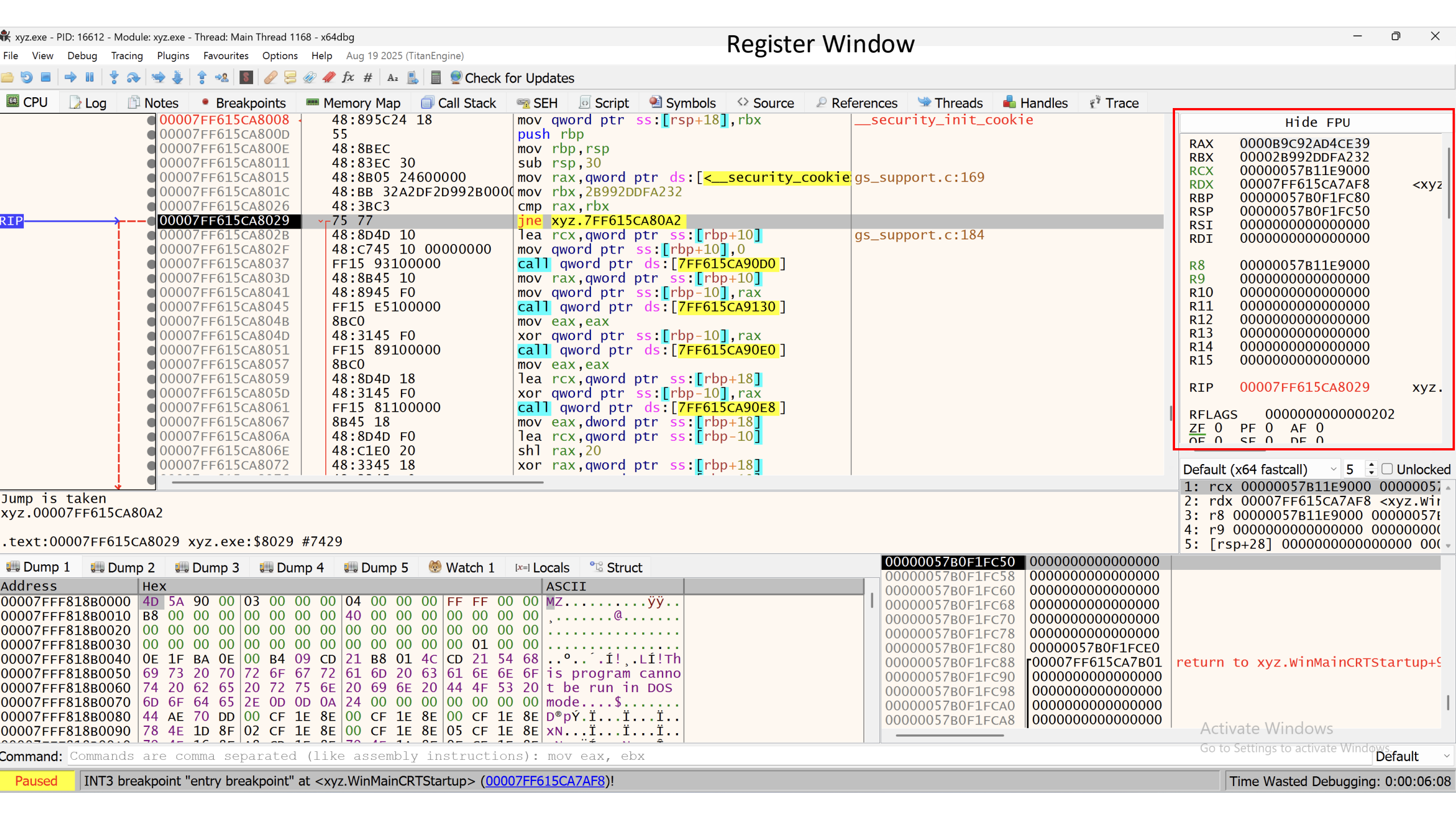
```
00000057B0F1FC50   0000000000000000
00000057B0F1FC58   0000000000000000
00000057B0F1FC60   0000000000000000
00000057B0F1FC68   0000000000000000
00000057B0F1FC70   0000000000000000
00000057B0F1FC78   0000000000000000
00000057B0F1FC80   00000057B0F1FCE0
00000057B0F1FC88   00007FF615CA7B01   return to xyz.WinMainCRTStartup+9
00000057B0F1FC90   0000000000000000
00000057B0F1FC98   0000000000000000
00000057B0F1FCA0   0000000000000000
00000057B0F1FCA8   0000000000000000
```


Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Default

Paused | INT3 breakpoint "entry breakpoint" at <xyz.WinMainCRTStartup> (00007FF615CA7AF8)! | Time Wasted Debugging: 0:00:06:08


xyz.exe - PID: 16612 - Module: xyz.exe - Thread: Main Thread 1168 - x64dbg
Main Window
File View Debug Tracing Plugins Favourites Options Help Aug 19 2025 (TitanEngine)
Check for Updates
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
00007FF615CA8008 48:895C24 18 mov qword ptr ss:[rsp+18],rbx __security_init_cookie
00007FF615CA800D 55 push rbp
00007FF615CA800E 48:8BEC mov rbp,rsp
00007FF615CA8011 48:83EC 30 sub rsp,30
00007FF615CA8015 48:8B05 24600000 mov rax,qword ptr ds:[<__security_cookie gs_support.c:169
00007FF615CA801C 48:BB 32A2DF2D992B0000 mov rbx,2B992DDFA232
00007FF615CA8026 48:3BC3 cmp rax,rbx
RIP 00007FF615CA8029 75 77 jne xyz.7FF615CA80A2
00007FF615CA802B 48:8D4D 10 lea rcx,qword ptr ss:[rbp+10] gs_support.c:184
00007FF615CA802F 48:C745 10 00000000 mov qword ptr ss:[rbp+10],0
00007FF615CA8037 FF15 93100000 call qword ptr ds:[7FF615CA90D0]
00007FF615CA803D 48:8B45 10 mov rax,qword ptr ss:[rbp+10]
00007FF615CA8041 48:8945 F0 mov qword ptr ss:[rbp-10],rax
00007FF615CA8045 FF15 E5100000 call qword ptr ds:[7FF615CA9130]
00007FF615CA804B 8BC0 mov eax,eax
00007FF615CA804D 48:3145 F0 xor qword ptr ss:[rbp-10],rax
00007FF615CA8051 FF15 89100000 call qword ptr ds:[7FF615CA90E0]
00007FF615CA8057 8BC0 mov eax,eax
00007FF615CA8059 48:8D4D 18 lea rcx,qword ptr ss:[rbp+18]
00007FF615CA805D 48:3145 F0 xor qword ptr ss:[rbp-10],rax
00007FF615CA8061 FF15 81100000 call qword ptr ds:[7FF615CA90E8]
00007FF615CA8067 8B45 18 mov eax,dword ptr ss:[rbp+18]
00007FF615CA806A 48:8D4D F0 lea rcx,qword ptr ss:[rbp-10]
00007FF615CA806E 48:C1E0 20 shl rax,20
00007FF615CA8072 48:3345 18 xor rax,qword ptr ss:[rbp+18]
Hide FPU
RAX 0000B9C92AD4CE39
RBX 00002B992DDFA232
RCX 00000057B11E9000
RDX 00007FF615CA7AF8 <xyz
RBP 00000057B0F1FC80
RSP 00000057B0F1FC50
RSI 0000000000000000
RDI 0000000000000000
R8 00000057B11E9000
R9 0000000000000000
R10 0000000000000000
R11 0000000000000000
R12 0000000000000000
R13 0000000000000000
R14 0000000000000000
R15 0000000000000000
RIP 00007FF615CA8029 xyz.
RFLAGS 0000000000000202
ZF 0 PF 0 AF 0
Default (x64 fastcall) 5 Unlocked
1: rcx 00000057B11E9000 0000005
2: rdx 00007FF615CA7AF8 <xyz.Wi
3: r8 00000057B11E9000 00000057
4: r9 0000000000000000 00000000
5: [rsp+28] 0000000000000000 00
Jump is taken
xyz.00007FF615CA80A2
.text:00007FF615CA8029 xyz.exe:$8029 #7429
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Address Hex ASCII
00007FFF818B0000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..
00007FFF818B0010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
00007FFF818B0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00007FFF818B0030 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ....
00007FFF818B0040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..º..´.Í!¸.LÍ!Th
00007FFF818B0050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00007FFF818B0060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00007FFF818B0070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
00007FFF818B0080 44 AE 70 DD 00 CF 1E 8E 00 CF 1E 8E 00 CF 1E 8E D®pÝ.Ï...Ï...Ï..
00007FFF818B0090 78 4E 1D 8F 02 CF 1E 8E 00 CF 1E 8E 05 CF 1E 8E xN...Ï...Ï...Ï..
00000057B0F1FC50 0000000000000000
00000057B0F1FC58 0000000000000000
00000057B0F1FC60 0000000000000000
00000057B0F1FC68 0000000000000000
00000057B0F1FC70 0000000000000000
00000057B0F1FC78 0000000000000000
00000057B0F1FC80 00000057B0F1FCE0
00000057B0F1FC88 00007FF615CA7B01 return to xyz.WinMainCRTStartup+9
00000057B0F1FC90 0000000000000000
00000057B0F1FC98 0000000000000000
00000057B0F1FCA0 0000000000000000
00000057B0F1FCA8 0000000000000000
Activate Windows
Go to Settings to activate Windows.
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Default
Paused
INT3 breakpoint "entry breakpoint" at <xyz.WinMainCRTStartup> (00007FF615CA7AF8)!
Time Wasted Debugging: 0:00:06:08


xyz.exe - PID: 16612 - Module: xyz.exe - Thread: Main Thread 1168 - x64dbg
Register Window
File View Debug Tracing Plugins Favourites Options Help Aug 19 2025 (TitanEngine)
Check for Updates
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
00007FF615CA8008 48:895C24 18 mov qword ptr ss:[rsp+18],rbx __security_init_cookie
00007FF615CA800D 55 push rbp
00007FF615CA800E 48:8BEC mov rbp,rsp
00007FF615CA8011 48:83EC 30 sub rsp,30
00007FF615CA8015 48:8B05 24600000 mov rax,qword ptr ds:[<__security_cookie gs_support.c:169
00007FF615CA801C 48:BB 32A2DF2D992B0000 mov rbx,2B992DDFA232
00007FF615CA8026 48:3BC3 cmp rax,rbx
RIP 00007FF615CA8029 75 77 jne xyz.7FF615CA80A2
00007FF615CA802B 48:8D4D 10 lea rcx,qword ptr ss:[rbp+10] gs_support.c:184
00007FF615CA802F 48:C745 10 00000000 mov qword ptr ss:[rbp+10],0
00007FF615CA8037 FF15 93100000 call qword ptr ds:[7FF615CA90D0]
00007FF615CA803D 48:8B45 10 mov rax,qword ptr ss:[rbp+10]
00007FF615CA8041 48:8945 F0 mov qword ptr ss:[rbp-10],rax
00007FF615CA8045 FF15 E5100000 call qword ptr ds:[7FF615CA9130]
00007FF615CA804B 8BC0 mov eax,eax
00007FF615CA804D 48:3145 F0 xor qword ptr ss:[rbp-10],rax
00007FF615CA8051 FF15 89100000 call qword ptr ds:[7FF615CA90E0]
00007FF615CA8057 8BC0 mov eax,eax
00007FF615CA8059 48:8D4D 18 lea rcx,qword ptr ss:[rbp+18]
00007FF615CA805D 48:3145 F0 xor qword ptr ss:[rbp-10],rax
00007FF615CA8061 FF15 81100000 call qword ptr ds:[7FF615CA90E8]
00007FF615CA8067 8B45 18 mov eax,dword ptr ss:[rbp+18]
00007FF615CA806A 48:8D4D F0 lea rcx,qword ptr ss:[rbp-10]
00007FF615CA806E 48:C1E0 20 shl rax,20
00007FF615CA8072 48:3345 18 xor rax,qword ptr ss:[rbp+18]
Hide FPU
RAX 0000B9C92AD4CE39
RBX 00002B992DDFA232
RCX 00000057B11E9000
RDX 00007FF615CA7AF8 <xyz
RBP 00000057B0F1FC80
RSP 00000057B0F1FC50
RSI 0000000000000000
RDI 0000000000000000
R8 00000057B11E9000
R9 0000000000000000
R10 0000000000000000
R11 0000000000000000
R12 0000000000000000
R13 0000000000000000
R14 0000000000000000
R15 0000000000000000
RIP 00007FF615CA8029 xyz.
RFLAGS 0000000000000202
ZF 0 PF 0 AF 0
Default (x64 fastcall) 5 Unlocked
1: rcx 00000057B11E9000
2: rdx 00007FF615CA7AF8 <xyz.Wi
3: r8 00000057B11E9000
4: r9 0000000000000000
5: [rsp+28] 0000000000000000
Jump is taken
xyz.00007FF615CA80A2
.text:00007FF615CA8029 xyz.exe:$8029 #7429
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Address Hex ASCII
00007FFF818B0000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..
00007FFF818B0010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
00007FFF818B0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00007FFF818B0030 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ....
00007FFF818B0040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..º..´.Í!¸.LÍ!Th
00007FFF818B0050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00007FFF818B0060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00007FFF818B0070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
00007FFF818B0080 44 AE 70 DD 00 CF 1E 8E 00 CF 1E 8E 00 CF 1E 8E D®pÝ.Ï...Ï...Ï..
00007FFF818B0090 78 4E 1D 8F 02 CF 1E 8E 00 CF 1E 8E 05 CF 1E 8E xN...Ï...Ï...Ï..
00000057B0F1FC50 0000000000000000
00000057B0F1FC58 0000000000000000
00000057B0F1FC60 0000000000000000
00000057B0F1FC68 0000000000000000
00000057B0F1FC70 0000000000000000
00000057B0F1FC78 0000000000000000
00000057B0F1FC80 00000057B0F1FCE0
00000057B0F1FC88 00007FF615CA7B01 return to xyz.WinMainCRTStartup+9
00000057B0F1FC90 0000000000000000
00000057B0F1FC98 0000000000000000
00000057B0F1FCA0 0000000000000000
00000057B0F1FCA8 0000000000000000
Activate Windows
Go to Settings to activate Windows.
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Default
Paused
INT3 breakpoint "entry breakpoint" at <xyz.WinMainCRTStartup> (00007FF615CA7AF8)!
Time Wasted Debugging: 0:00:06:08

Parameters last pushed on the stack

xyz.exe - PID: 16612 - Module: xyz.exe - Thread: Main Thread 1168 - x64dbg

File View Debug Tracing Plugins Favourites Options Help Aug 19 2025 (TitanEngine)

Check for Updates

CPU | Log | Notes | Breakpoints | Memory Map | Call Stack | SEH | Script | Symbols | Source | References | Threads | Handles | Trace

```
00007FF615CA8008   48:895C24 18        mov qword ptr ss:[rsp+18],rbx      __security_init_cookie
00007FF615CA800D   55                  push rbp
00007FF615CA800E   48:8BEC             mov rbp,rsp
00007FF615CA8011   48:83EC 30          sub rsp,30
00007FF615CA8015   48:8B05 24600000    mov rax,qword ptr ds:[<__security_cookie  gs_support.c:169
00007FF615CA801C   48:BB 32A2DF2D992B0000 mov rbx,2B992DDFA232
00007FF615CA8026   48:3BC3             cmp rax,rbx
RIP 00007FF615CA8029   75 77           jne xyz.7FF615CA80A2
00007FF615CA802B   48:8D4D 10          lea rcx,qword ptr ss:[rbp+10]      gs_support.c:184
00007FF615CA802F   48:C745 10 00000000 mov qword ptr ss:[rbp+10],0
00007FF615CA8037   FF15 93100000       call qword ptr ds:[7FF615CA90D0]
00007FF615CA803D   48:8B45 10          mov rax,qword ptr ss:[rbp+10]
00007FF615CA8041   48:8945 F0          mov qword ptr ss:[rbp-10],rax
00007FF615CA8045   FF15 E5100000       call qword ptr ds:[7FF615CA9130]
00007FF615CA804B   8BC0                mov eax,eax
00007FF615CA804D   48:3145 F0          xor qword ptr ss:[rbp-10],rax
00007FF615CA8051   FF15 89100000       call qword ptr ds:[7FF615CA90E0]
00007FF615CA8057   8BC0                mov eax,eax
00007FF615CA8059   48:8D4D 18          lea rcx,qword ptr ss:[rbp+18]
00007FF615CA805D   48:3145 F0          xor qword ptr ss:[rbp-10],rax
00007FF615CA8061   FF15 81100000       call qword ptr ds:[7FF615CA90E8]
00007FF615CA8067   8B45 18             mov eax,dword ptr ss:[rbp+18]
00007FF615CA806A   48:8D4D F0          lea rcx,qword ptr ss:[rbp-10]
00007FF615CA806E   48:C1E0 20          shl rax,20
00007FF615CA8072   48:3345 18          xor rax,qword ptr ss:[rbp+18]
```

Jump is taken
xyz.00007FF615CA80A2

.text:00007FF615CA8029 xyz.exe:$8029 #7429

Hide FPU

```
RAX   0000B9C92AD4CE39
RBX   00002B992DDFA232
RCX   00000057B11E9000
RDX   00007FF615CA7AF8   <xyz
RBP   00000057B0F1FC80
RSP   00000057B0F1FC50
RSI   0000000000000000
RDI   0000000000000000

R8    00000057B11E9000
R9    0000000000000000
R10   0000000000000000
R11   0000000000000000
R12   0000000000000000
R13   0000000000000000
R14   0000000000000000
R15   0000000000000000

RIP   00007FF615CA8029   xyz.

RFLAGS   0000000000000202
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
```

Default (x64 fastcall) 5 Unlocked

```
1: rcx 00000057B11E9000 0000005
2: rdx 00007FF615CA7AF8 <xyz.Wi
3: r8 00000057B11E9000 00000057
4: r9 0000000000000000 00000000
5: [rsp+28] 0000000000000000 00
```

Dump 1 | Dump 2 | Dump 3 | Dump 4 | Dump 5 | Watch 1 | Locals | Struct

Address	Hex	ASCII
00007FFF818B0000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....ÿÿ..
00007FFF818B0010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	¸.......@.......
00007FFF818B0020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00007FFF818B0030	00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00	....
00007FFF818B0040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	..º..´.Í!¸.LÍ!Th
00007FFF818B0050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
00007FFF818B0060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
00007FFF818B0070	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode....$.......
00007FFF818B0080	44 AE 70 DD 00 CF 1E 8E 00 CF 1E 8E 00 CF 1E 8E	D®pÝ.Ï...Ï...Ï..
00007FFF818B0090	78 4E 1D 8F 02 CF 1E 8E 00 CF 1E 8E 05 CF 1E 8E	xN...Ï...Ï...Ï..

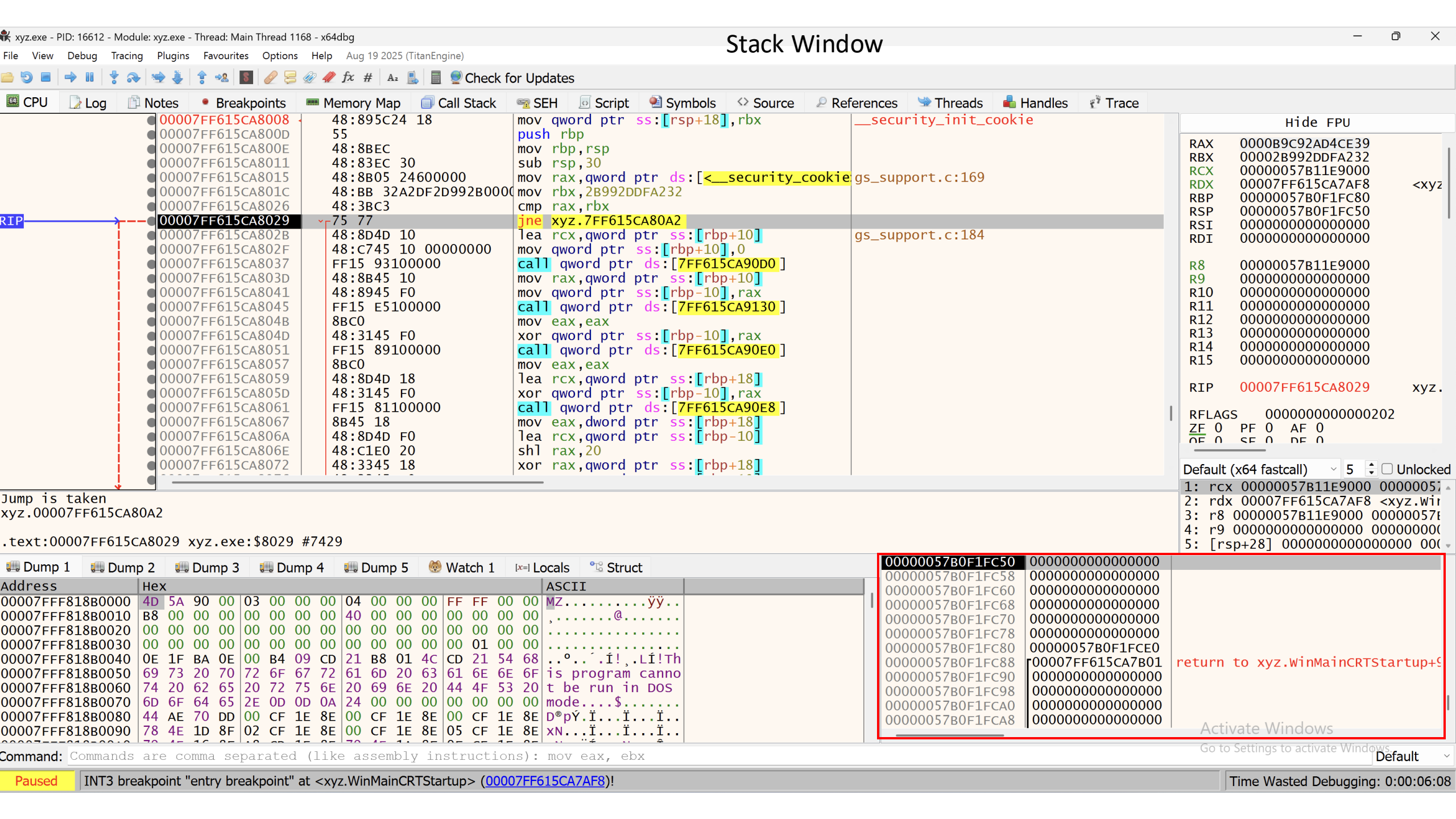
```
00000057B0F1FC50   0000000000000000
00000057B0F1FC58   0000000000000000
00000057B0F1FC60   0000000000000000
00000057B0F1FC68   0000000000000000
00000057B0F1FC70   0000000000000000
00000057B0F1FC78   0000000000000000
00000057B0F1FC80   00000057B0F1FCE0
00000057B0F1FC88   00007FF615CA7B01   return to xyz.WinMainCRTStartup+9
00000057B0F1FC90   0000000000000000
00000057B0F1FC98   0000000000000000
00000057B0F1FCA0   0000000000000000
00000057B0F1FCA8   0000000000000000
```

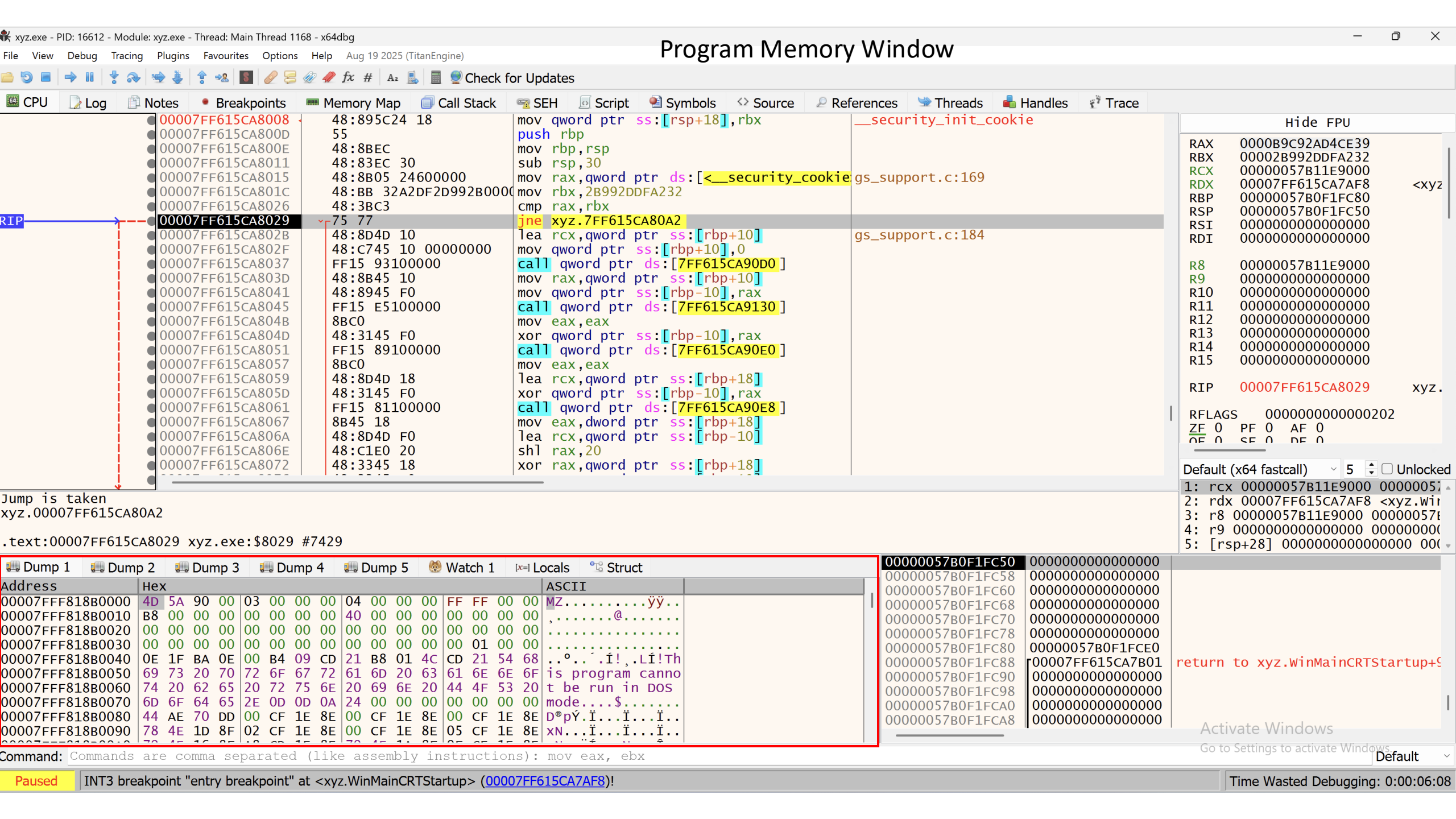
Activate Windows
Go to Settings to activate Windows.

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Default

Paused | INT3 breakpoint "entry breakpoint" at <xyz.WinMainCRTStartup> (00007FF615CA7AF8)! | Time Wasted Debugging: 0:00:06:08


Stack Window
xyz.exe - PID: 16612 - Module: xyz.exe - Thread: Main Thread 1168 - x64dbg
File View Debug Tracing Plugins Favourites Options Help Aug 19 2025 (TitanEngine)
Check for Updates
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
00007FF615CA8008 48:895C24 18 mov qword ptr ss:[rsp+18],rbx __security_init_cookie
00007FF615CA800D 55 push rbp
00007FF615CA800E 48:8BEC mov rbp,rsp
00007FF615CA8011 48:83EC 30 sub rsp,30
00007FF615CA8015 48:8B05 24600000 mov rax,qword ptr ds:[<__security_cookie gs_support.c:169
00007FF615CA801C 48:BB 32A2DF2D992B0000 mov rbx,2B992DDFA232
00007FF615CA8026 48:3BC3 cmp rax,rbx
RIP 00007FF615CA8029 75 77 jne xyz.7FF615CA80A2
00007FF615CA802B 48:8D4D 10 lea rcx,qword ptr ss:[rbp+10] gs_support.c:184
00007FF615CA802F 48:C745 10 00000000 mov qword ptr ss:[rbp+10],0
00007FF615CA8037 FF15 93100000 call qword ptr ds:[7FF615CA90D0]
00007FF615CA803D 48:8B45 10 mov rax,qword ptr ss:[rbp+10]
00007FF615CA8041 48:8945 F0 mov qword ptr ss:[rbp-10],rax
00007FF615CA8045 FF15 E5100000 call qword ptr ds:[7FF615CA9130]
00007FF615CA804B 8BC0 mov eax,eax
00007FF615CA804D 48:3145 F0 xor qword ptr ss:[rbp-10],rax
00007FF615CA8051 FF15 89100000 call qword ptr ds:[7FF615CA90E0]
00007FF615CA8057 8BC0 mov eax,eax
00007FF615CA8059 48:8D4D 18 lea rcx,qword ptr ss:[rbp+18]
00007FF615CA805D 48:3145 F0 xor qword ptr ss:[rbp-10],rax
00007FF615CA8061 FF15 81100000 call qword ptr ds:[7FF615CA90E8]
00007FF615CA8067 8B45 18 mov eax,dword ptr ss:[rbp+18]
00007FF615CA806A 48:8D4D F0 lea rcx,qword ptr ss:[rbp-10]
00007FF615CA806E 48:C1E0 20 shl rax,20
00007FF615CA8072 48:3345 18 xor rax,qword ptr ss:[rbp+18]
Hide FPU
RAX 0000B9C92AD4CE39
RBX 00002B992DDFA232
RCX 00000057B11E9000
RDX 00007FF615CA7AF8 <xyz
RBP 00000057B0F1FC80
RSP 00000057B0F1FC50
RSI 0000000000000000
RDI 0000000000000000
R8 00000057B11E9000
R9 0000000000000000
R10 0000000000000000
R11 0000000000000000
R12 0000000000000000
R13 0000000000000000
R14 0000000000000000
R15 0000000000000000
RIP 00007FF615CA8029 xyz.
RFLAGS 0000000000000202
ZF 0 PF 0 AF 0
Default (x64 fastcall) 5 Unlocked
1: rcx 00000057B11E9000
2: rdx 00007FF615CA7AF8 <xyz.wi
3: r8 00000057B11E9000
4: r9 0000000000000000
5: [rsp+28] 0000000000000000
Jump is taken
xyz.00007FF615CA80A2
.text:00007FF615CA8029 xyz.exe:$8029 #7429
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Address Hex ASCII
00007FFF818B0000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..
00007FFF818B0010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
00007FFF818B0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00007FFF818B0030 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ....
00007FFF818B0040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..º..´.Í!¸.LÍ!Th
00007FFF818B0050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00007FFF818B0060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00007FFF818B0070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
00007FFF818B0080 44 AE 70 DD 00 CF 1E 8E 00 CF 1E 8E 00 CF 1E 8E D®pÝ.Ï...Ï...Ï..
00007FFF818B0090 78 4E 1D 8F 02 CF 1E 8E 00 CF 1E 8E 05 CF 1E 8E xN...Ï...Ï...Ï..
00000057B0F1FC50 0000000000000000
00000057B0F1FC58 0000000000000000
00000057B0F1FC60 0000000000000000
00000057B0F1FC68 0000000000000000
00000057B0F1FC70 0000000000000000
00000057B0F1FC78 0000000000000000
00000057B0F1FC80 00000057B0F1FCE0
00000057B0F1FC88 00007FF615CA7B01 return to xyz.WinMainCRTStartup+9
00000057B0F1FC90 0000000000000000
00000057B0F1FC98 0000000000000000
00000057B0F1FCA0 0000000000000000
00000057B0F1FCA8 0000000000000000
Activate Windows
Go to Settings to activate Windows.
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Default
Paused
INT3 breakpoint "entry breakpoint" at <xyz.WinMainCRTStartup> (00007FF615CA7AF8)!
Time Wasted Debugging: 0:00:06:08


Program Memory Window
xyz.exe - PID: 16612 - Module: xyz.exe - Thread: Main Thread 1168 - x64dbg
File View Debug Tracing Plugins Favourites Options Help Aug 19 2025 (TitanEngine)
Check for Updates
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
00007FF615CA8008 48:895C24 18 mov qword ptr ss:[rsp+18],rbx __security_init_cookie
00007FF615CA800D 55 push rbp
00007FF615CA800E 48:8BEC mov rbp,rsp
00007FF615CA8011 48:83EC 30 sub rsp,30
00007FF615CA8015 48:8B05 24600000 mov rax,qword ptr ds:[<__security_cookie gs_support.c:169
00007FF615CA801C 48:BB 32A2DF2D992B0000 mov rbx,2B992DDFA232
00007FF615CA8026 48:3BC3 cmp rax,rbx
RIP 00007FF615CA8029 75 77 jne xyz.7FF615CA80A2
00007FF615CA802B 48:8D4D 10 lea rcx,qword ptr ss:[rbp+10] gs_support.c:184
00007FF615CA802F 48:C745 10 00000000 mov qword ptr ss:[rbp+10],0
00007FF615CA8037 FF15 93100000 call qword ptr ds:[7FF615CA90D0]
00007FF615CA803D 48:8B45 10 mov rax,qword ptr ss:[rbp+10]
00007FF615CA8041 48:8945 F0 mov qword ptr ss:[rbp-10],rax
00007FF615CA8045 FF15 E5100000 call qword ptr ds:[7FF615CA9130]
00007FF615CA804B 8BC0 mov eax,eax
00007FF615CA804D 48:3145 F0 xor qword ptr ss:[rbp-10],rax
00007FF615CA8051 FF15 89100000 call qword ptr ds:[7FF615CA90E0]
00007FF615CA8057 8BC0 mov eax,eax
00007FF615CA8059 48:8D4D 18 lea rcx,qword ptr ss:[rbp+18]
00007FF615CA805D 48:3145 F0 xor qword ptr ss:[rbp-10],rax
00007FF615CA8061 FF15 81100000 call qword ptr ds:[7FF615CA90E8]
00007FF615CA8067 8B45 18 mov eax,dword ptr ss:[rbp+18]
00007FF615CA806A 48:8D4D F0 lea rcx,qword ptr ss:[rbp-10]
00007FF615CA806E 48:C1E0 20 shl rax,20
00007FF615CA8072 48:3345 18 xor rax,qword ptr ss:[rbp+18]
Hide FPU
RAX 0000B9C92AD4CE39
RBX 00002B992DDFA232
RCX 00000057B11E9000
RDX 00007FF615CA7AF8 <xyz
RBP 00000057B0F1FC80
RSP 00000057B0F1FC50
RSI 0000000000000000
RDI 0000000000000000
R8 00000057B11E9000
R9 0000000000000000
R10 0000000000000000
R11 0000000000000000
R12 0000000000000000
R13 0000000000000000
R14 0000000000000000
R15 0000000000000000
RIP 00007FF615CA8029 xyz.
RFLAGS 0000000000000202
ZF 0 PF 0 AF 0
Default (x64 fastcall) 5 Unlocked
1: rcx 00000057B11E9000
2: rdx 00007FF615CA7AF8 <xyz.Wi
3: r8 00000057B11E9000
4: r9 0000000000000000
5: [rsp+28] 0000000000000000
Jump is taken
xyz.00007FF615CA80A2
.text:00007FF615CA8029 xyz.exe:$8029 #7429
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Address Hex ASCII
00007FFF818B0000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..
00007FFF818B0010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
00007FFF818B0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00007FFF818B0030 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ....
00007FFF818B0040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..º..´.Í!¸.LÍ!Th
00007FFF818B0050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00007FFF818B0060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00007FFF818B0070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
00007FFF818B0080 44 AE 70 DD 00 CF 1E 8E 00 CF 1E 8E 00 CF 1E 8E D®pÝ.Ï...Ï...Ï..
00007FFF818B0090 78 4E 1D 8F 02 CF 1E 8E 00 CF 1E 8E 05 CF 1E 8E xN...Ï...Ï...Ï..
00000057B0F1FC50 0000000000000000
00000057B0F1FC58 0000000000000000
00000057B0F1FC60 0000000000000000
00000057B0F1FC68 0000000000000000
00000057B0F1FC70 0000000000000000
00000057B0F1FC78 0000000000000000
00000057B0F1FC80 00000057B0F1FCE0
00000057B0F1FC88 00007FF615CA7B01 return to xyz.WinMainCRTStartup+
00000057B0F1FC90 0000000000000000
00000057B0F1FC98 0000000000000000
00000057B0F1FCA0 0000000000000000
00000057B0F1FCA8 0000000000000000
Activate Windows
Go to Settings to activate Windows.
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Default
Paused
INT3 breakpoint "entry breakpoint" at <xyz.WinMainCRTStartup> (00007FF615CA7AF8)!
Time Wasted Debugging: 0:00:06:08

Starting Points

- String References
  - Help us to find points of interest.

- Function calls
  - What parameters are being passed
  - What is being returned
  - Behaviour of the program

Function calls in x64 assembly

- By default, the x64 calling convention passes the first four arguments to a function in registers.
- The registers used for these arguments depend on the position and type of the argument.
  - Remaining arguments get pushed on the stack in right-to-left order.

Parameter type	fifth and higher	fourth	third	second	leftmost
floating-point	stack	XMM3	XMM2	XMM1	XMM0
integer	stack	R9	R8	RDX	RCX
Aggregates (8, 16, 32, or 64 bits) and `__m64`	stack	R9	R8	RDX	RCX
Other aggregates, as pointers	stack	R9	R8	RDX	RCX
`__m128`, as a pointer	stack	R9	R8	RDX	RCX

https://learn.microsoft.com/en-us/cpp/build/x64-calling-convention?view=msvc-170#parameter-passing