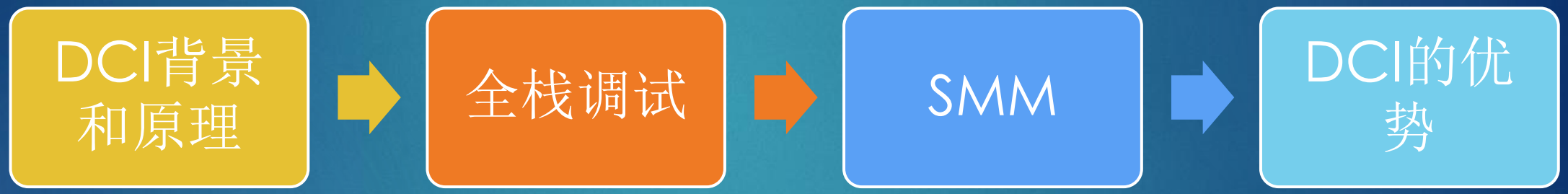
# 使用DCI技术进行全栈调试

张银奎

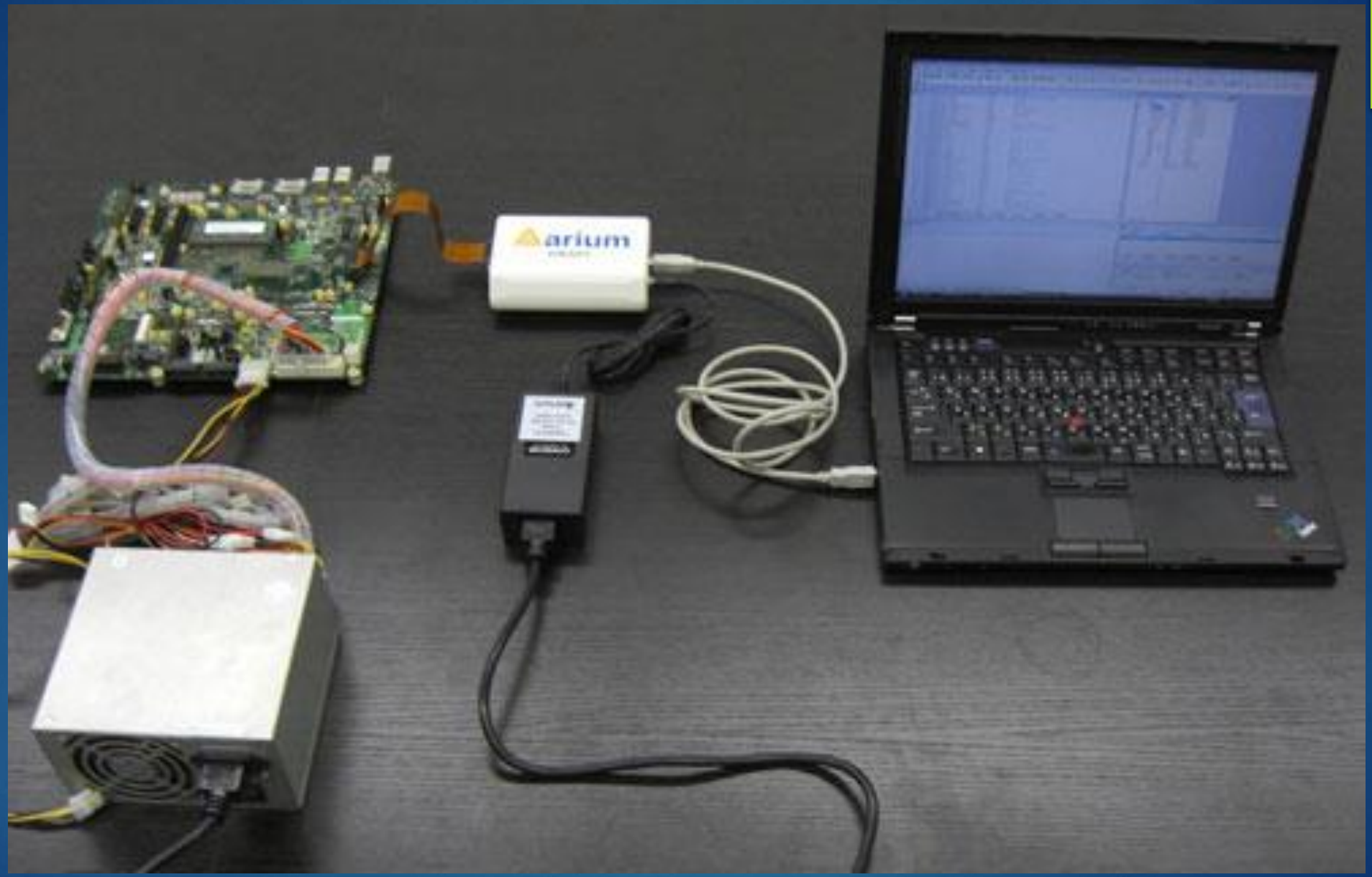
2020/7/17

张银奎，Raymond Zhang，格蠹老雷，《软件调试》和《格蠹汇编》作者
http://advdbg.org http://weibo.com/dbgger 格友公众号

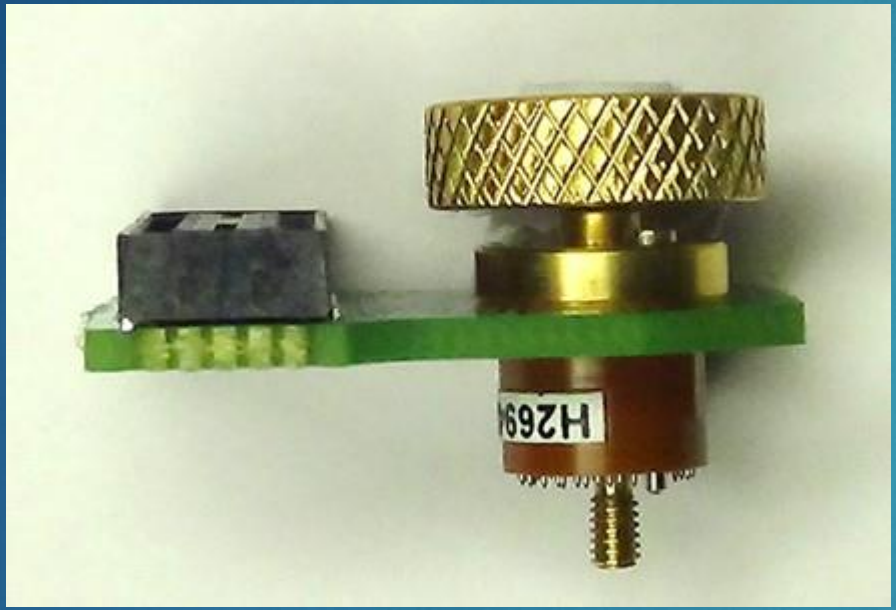

DCI背景和原理
全栈调试
SMM
DCI的优势

经典小蓝盒，XDP
Intel的JTAG技术

5000 USD




http://www.gailogic.co.jp/product/arium/LX-1000_Intel.html




CMC 35-pin ITP Adapter

CMC = Chassis Mount Connector

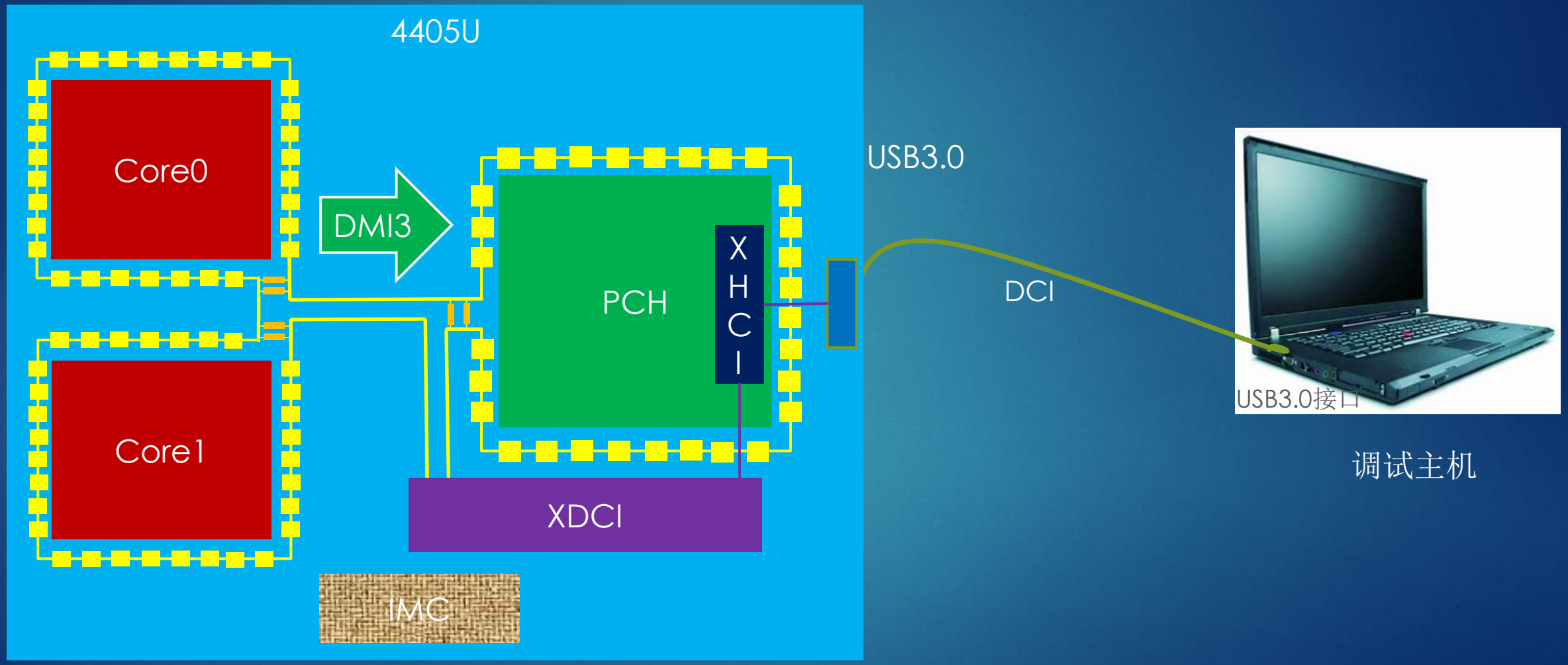
# DCI = Direct Connect Interface


http://advdbg.org/gdk/


一桌
一凳
一根线

一盅茶
一个周末！

# DCI原理图


4405U
Core0
Core1
DMI3
PCH
XHCI
XDCI
IMC
USB3.0
DCI
USB3.0接口
调试主机

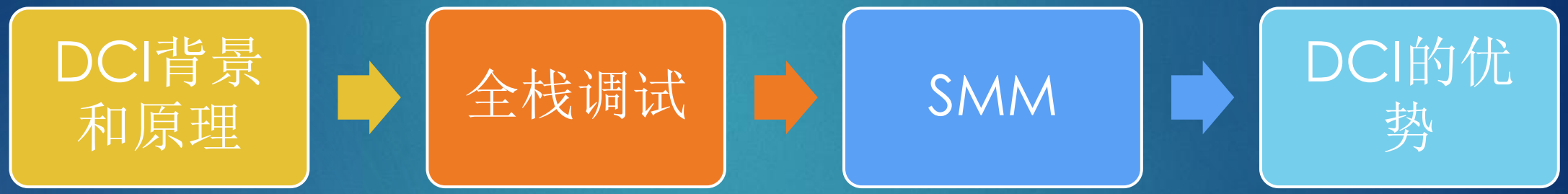
# 默认锁死

- CPU级锁死配置寄存器
- OS阶段不可改写
- 改写即触发异常
  - Windows蓝屏崩溃
  - Linux Panic重启
- 配件限制供应
- 工具的技术门槛很高

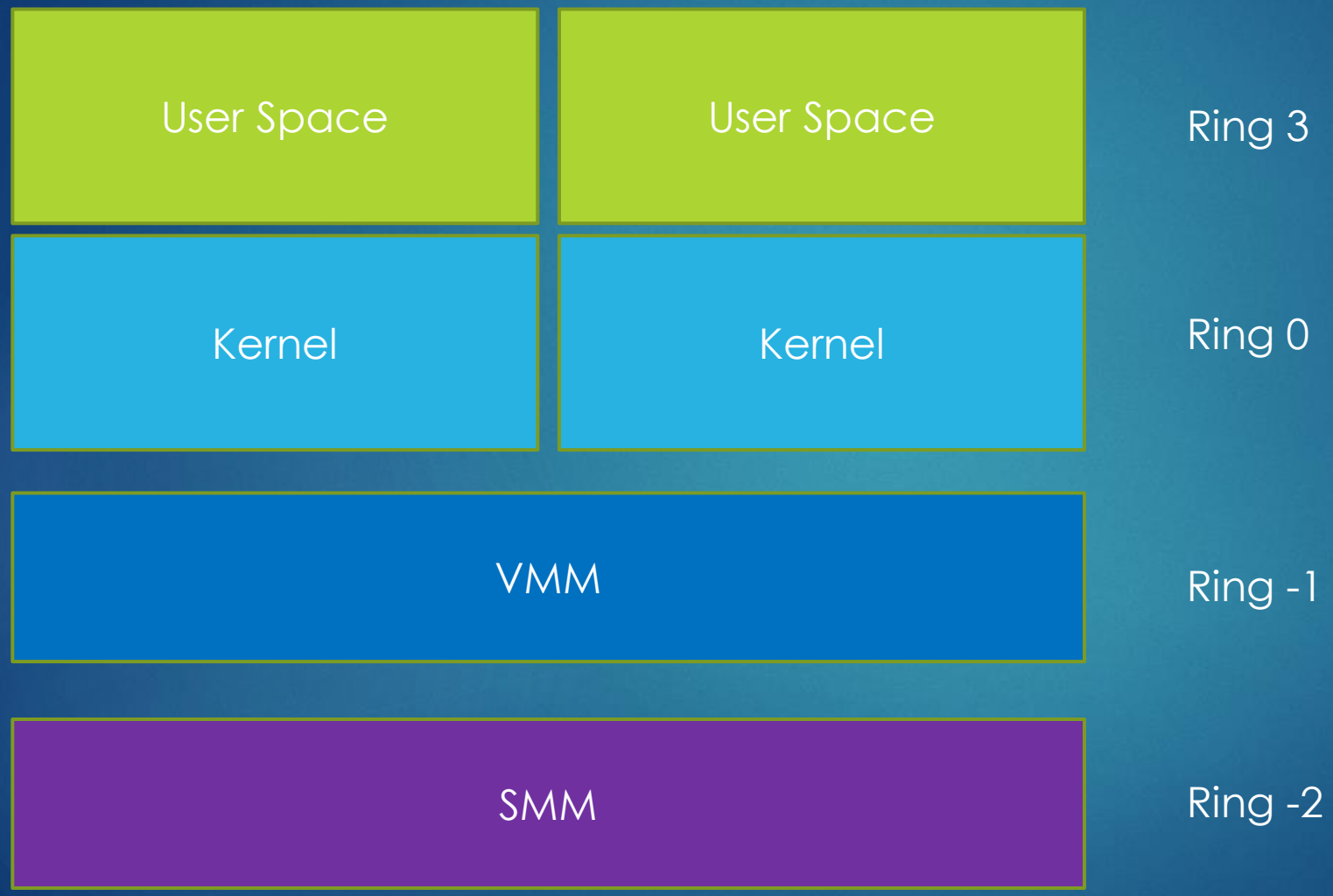

# GDK7

针对高级调试和调优设计的专业套件：硬件 + Nano Code 工具套件 + GDC社区

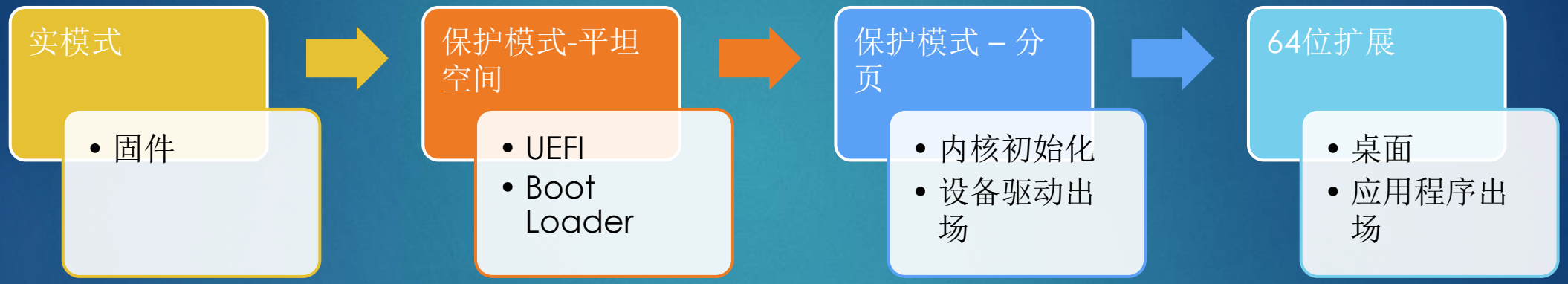
http://advdbg.org/gdk/


DCI背景和原理
全栈调试
SMM
DCI的优势

# 全栈调试


User Space
User Space
Ring 3
Kernel
Kernel
Ring 0
VMM
Ring -1
SMM
Ring -2

# 一调到底




理想情况：全能调试器，无缝对接，不需要切换调试器或者更换会话

# 十万米高空看X86架构

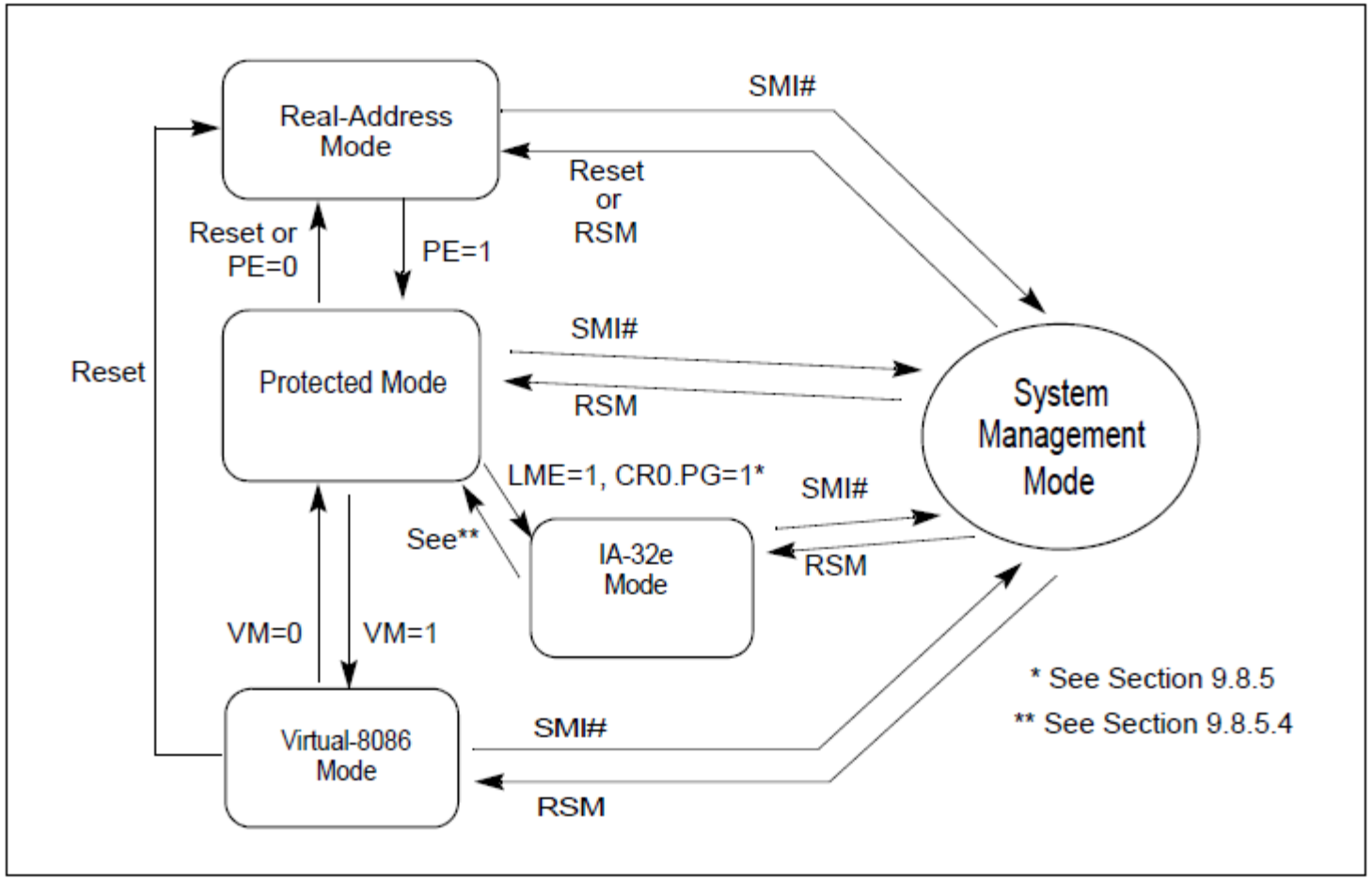
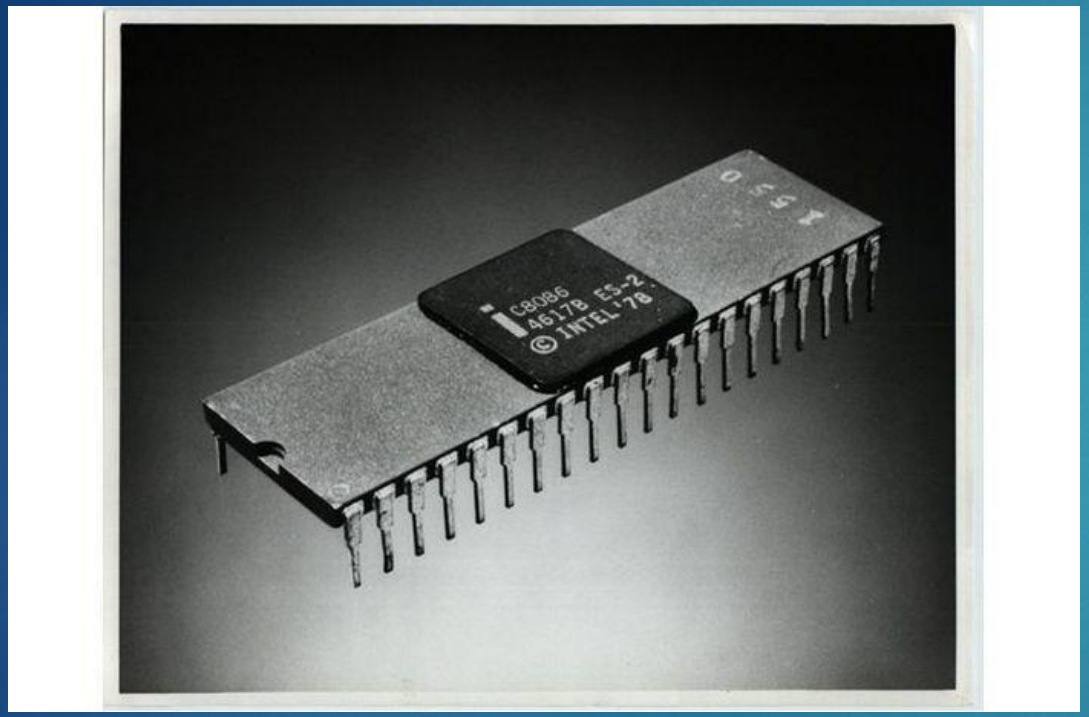
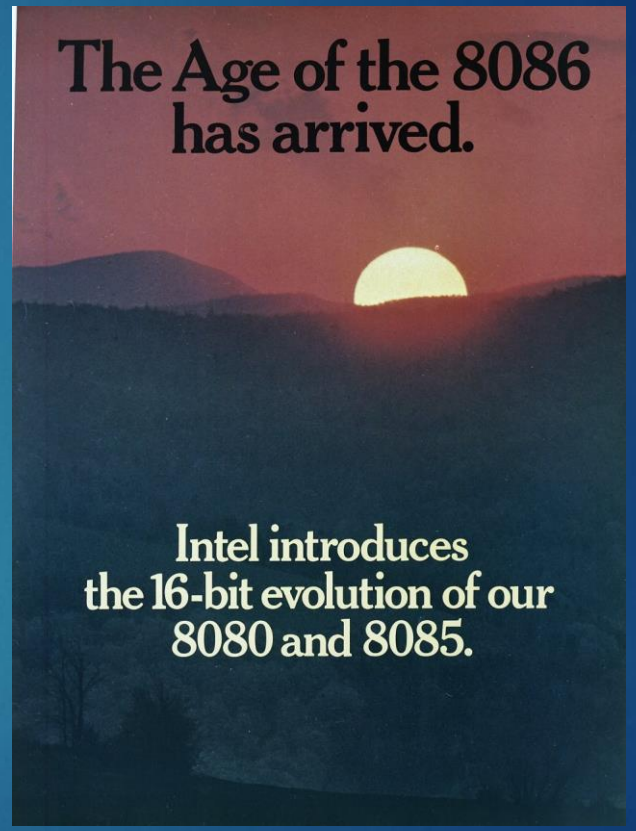



Figure 2-3. Transitions Among the Processor's Operating Modes

# 从实模式开始




June 8, 1978



# 从约定好的起跑地点出发

**0xF000:0xFFF0**

| Name | Id | State | Address | Location |
|---|---|---|---|---|
| IA | | | | |
| | 0 | Init | 0xF000:0xFFF0 | |
| | 1 | Wait for SIPI loop | 0xF000:0x0000 | |
| | 2 | Wait for SIPI loop | 0xF000:0x0000 | |
| | 3 | Shutdown | 0x0038:0x000000008D7CB172 | |

# 黑暗中崛起

此时还没有栈可用，不可以call，只能jmp

```
u f0000+fff0
00000000`000ffff0 ea5be000f03034 jmp 3430:F000E05B
00000000`000ffff7 2f das
00000000`000ffff8 30342f xor byte ptr [edi+ebp],dh
00000000`000ffffb 3136 xor dword ptr [esi],esi
00000000`000ffffd 00fc add ah,bh
00000000`000fffff 005a5a add byte ptr [edx+5Ah],bl
00000000`00100002 5a pop edx
00000000`00100003 5a pop edx
```

File Edit Selection View Go Debug Terminal Nano Help — Nano Debugger - simple-pt-master - Nano Code

NANO DEBUGGER: ...

- Open Executable
- Attach to a process
- Kernel Debugging
- Open Crash Dump

Welcome | Nano Home | Nano Debugger

File View Output Help

```
xmm0=0 0 3.22299e-044 6.60012e-043
xmm1=0 0 0 0
xmm2=-1.#QNAN 0 2.10195e-044 0
xmm3=0 2.85865e-043 6.48138e+021 -1.#QNAN
xmm4=0 0 2.10195e-044 0
xmm5=0 0 0 0
xmm6=0 6.60012e-043 -4.99956e-011 0
xmm7=0 0 0 0
cr0=00000000 cr2=00000000 cr3=00000000
dr0=00000000 dr1=00000000 dr2=00000000
dr3=00000000 dr6=00000000 dr7=00000000 cr4=00000000
c000:6e76 6658 pop eax
[ndb]!db c0000+6e7a
!db c0000+6e7a
# c6e7a 80 fd 00 74 0a 8b c2 80-fd 01 74 03 66 8b c2 66 ...t......t.f..f
# c6e8a 5a 59 c3 51 b1 00 eb 1b-51 b9 80 00 eb 15 51 b9 ZY.Q....Q.....Q.
# c6e9a 80 10 eb 0f 51 b9 80 01-eb 09 51 b1 01 eb 04 51 ....Q.....Q....Q
# c6eaa b9 80 00 52 66 50 f6 c1-80 74 02 8a e5 ba f8 0c ...RfP...t......
# c6eba 66 0f b7 c0 8a e8 24 fc-66 0d 00 00 00 80 66 ef f.....$.f.....f.
# c6eca ba fc 0c 80 e5 03 0a d5-ed 92 66 58 8a c2 80 f9 ..........fX....
# c6eda 00 74 02 8b c2 5a 59 c3-50 ba da 03 ec b2 ba ec .t...ZY.P.......
# c6eea b2 c0 58 c3 52 66 56 66-57 2e f6 44 1b 20 74 2d ..X.RfVfW..D. t-
```

16.0: 0% 100%

disassembly.nd | JTAGEvents

```
;; start=0xc6e76 end=0xc6f66
c000:6e76 6658          pop     eax
c000:6e78 8ac2          mov     al,dl
c000:6e7a 80fd00        cmp     ch,0
c000:6e7d 740a          je      6E89
c000:6e7f 8bc2          mov     ax,dx
c000:6e81 80fd01        cmp     ch,1
c000:6e84 7403          je      6E89
c000:6e86 668bc2        mov     eax,edx
c000:6e89 665a          pop     edx
c000:6e8b 59            pop     cx
c000:6e8c c3            ret
c000:6e8d 51            push    cx
c000:6e8e b100          mov     cl,0
c000:6e90 eb1b          jmp     6EAD
c000:6e92 51            push    cx
c000:6e93 b98000        mov     cx,80h
c000:6e96 eb15          jmp     6EAD
c000:6e98 51            push    cx
c000:6e99 b98010        mov     cx,1080h
c000:6e9c eb0f          jmp     6EAD
c000:6e9e 51            push    cx
c000:6e9f b98001        mov     cx,180h
c000:6ea2 eb09          jmp     6EAD
c000:6ea4 51            push    cx
c000:6ea5 b101          mov     cl,1
c000:6ea7 eb04          jmp     6EAD
c000:6ea9 51            push    cx
c000:6eaa b98000        mov     cx,80h
c000:6ead 52            push    dx
c000:6eae 6650          push    eax
c000:6eb0 f6c180        test    cl,80h
```

TERMINAL DEBUG CONSOLE OUTPUT PROBLEMS — Nano Code

```
21:15:18#EXDI:vread 0x3d8 - elements 128 width 1 exits with hr=0xee000006, read=0 [REAL]
21:15:18#JTAG:The requested memory translation failed.  The 64-bit paging PDPTE is not valid. Address can't be translated.
21:15:18#EXDI:vread 0x20 - elements 128 width 1 exits with hr=0xee000006, read=0 [REAL]
21:15:18#JTAG:The requested memory translation failed.  The 64-bit paging PDPTE is not valid. Address can't be translated.
21:15:18#EXDI:vread 0x3d8 - elements 128 width 1 exits with hr=0xee000006, read=0 [REAL]
```

⊗ 0 ⚠ 0 — Nano 欢迎您-gdman 1.0.6

21:35 2020/7/16

Intel(R) System Debugger (Legacy)

File Edit View Run Debug Options Help

LoadDXEModules LoadPEIMs LoadThis

Assembler: 0xC000:0x5DED to 0xC000:0x6F7D

| Trail | Address | Opcodes | Source |
|---|---|---|---|
| | 0xC000:0x5DED | FE C4 | inc ah |
| | 0xC000:0x5DEF | 38 F4 | cmp ah, dh |
| | 0xC000:0x5DF1 | 76 A7 | jbe 0x5D9A <> |
| | 0xC000:0x5DF3 | FE 4E FA | dec byte ptr [bp-0x6] |
| | 0xC000:0x5DF6 | 75 A0 | jnz 0x5D98 <> |
| | 0xC000:0x5DF8 | EB 2B | jmp 0x5E25 <> |
| | 0xC000:0x5DFA | FE C3 | inc bl |
| | 0xC000:0x5DFC | E8 DD 02 | call 0x60DC <> |
| | 0xC000:0x5DFF | 66 AD | lodsd dword ptr [si] |
| | 0xC000:0x5E01 | FE CB | dec bl |
| | 0xC000:0x5E03 | E8 D6 02 | call 0x60DC <> |
| | 0xC000:0x5E06 | 66 AB | stosd dword ptr [di] |
| | 0xC000:0x5E08 | 83 FF 00 | cmp di, 0x0 |
| | 0xC000:0x5E0B | 75 04 | jnz 0x5E11 <> |
| | 0xC000:0x5E0D | 43 | inc bx |
| | 0xC000:0x5E0E | E8 CB 02 | call 0x60DC <> |
| | 0xC000:0x5E11 | 83 E9 03 | sub cx, 0x3 |
| | 0xC000:0x5E14 | E2 AF | loop 0x5DC5 <> |
| | 0xC000:0x5E16 | EB D1 | jmp 0x5DE9 <> |
| | 0xC000:0x5E18 | | ??? |
| | 0xC000:0x5E1A | F9 | stc |
| | 0xC000:0x5E1B | 00 75 07 | add byte ptr [di+0x7], dh |
| | 0xC000:0x5E1E | BA CE 03 | mov dx, 0x3CE |

Registers

| Register | Value | Description |
|---|---|---|
| R10 | 0x000000008C393000 | |
| R11 | 0x0000000000001800 | |
| R12 | 0x0000000000000000 | |
| R13 | 0x0000000000000004 | |
| R14 | 0x0000000000000000 | |
| R15 | 0x0000000000000080 | |
| RIP | 0x0000000000006E6B | |
| RFL | 0x0000000000010202 | RFLAGS ... |
| EAX | 0x00008200 | |
| EBX | 0x0000A000 | |
| ECX | 0x00000108 | |
| EDX | 0x0000F004 | |
| ESI | 0x000C5108 | |
| EDI | 0x0000F304 | |
| ESP | 0x00002F94 | |
| EBP | 0x00002FDC | |
| CS | 0xC000 | |
| DS | 0x0000 | |
| SS | 0x0180 | |
| ES | 0x5000 | |
| FS | 0x0180 | |
| GS | 0x0180 | |
| EIP | 0x00006E6B | |
| EFL | 0x00010202 | EFLAGS ... |

Console View | Instruction Trace [LBR] | Paging

Debugger Commands

```
IPC: DCI: A DCI device has been detected, attempting to establish connection
IPC: DCI: Target connection has been fully established
Reload done.
INFO: Target power is now: Off
INFO: Target power is now: On
WARNING: attempting to halt an unresponsive target, this operation may fail...
SPECIAL BREAK 0 ON "Init Break" : enabled  (S=0,CS=0)
SPECIAL BREAK 1 ON "Machine Check Break" : enabled  (S=0,CS=0)
SPECIAL BREAK 2 ON "Reset Break" : enabled  (S=0,CS=0)
SPECIAL BREAK 3 ON "SMM Entry Break" : enabled  (S=0,CS=0)
SPECIAL BREAK 4 ON "Shutdown Break" : enabled  (S=0,CS=0)
SPECIAL BREAK 5 ON "SMM Exit Break" : enabled  (S=0,CS=0)
xdb>
```

[0][default] IP=0xC000:0x6E6B 0xC000:0x6E6B

13:58
2020/7/11

```
u 0038:00000000`8d7dd3d6 L30
0038:00000000`8d7dd3d6 4883c408 add rsp,8
0038:00000000`8d7dd3da 488bf4 mov rsi,rsp
0038:00000000`8d7dd3dd 0fae0e fxrstor [rsi]
0038:00000000`8d7dd3e0 4881c400020000 add rsp,200h
0038:00000000`8d7dd3e7 4883c430 add rsp,30h
0038:00000000`8d7dd3eb 58 pop rax
0038:00000000`8d7dd3ec 0f22c0 mov cr0,rax
0038:00000000`8d7dd3ef 4883c408 add rsp,8
0038:00000000`8d7dd3f3 58 pop rax
0038:00000000`8d7dd3f4 0f22d0 mov cr2,rax
0038:00000000`8d7dd3f7 58 pop rax
0038:00000000`8d7dd3f8 0f22d8 mov cr3,rax
0038:00000000`8d7dd3fb 58 pop rax
0038:00000000`8d7dd3fc 0f22e0 mov cr4,rax
0038:00000000`8d7dd3ff 58 pop rax
0038:00000000`8d7dd400 440f22c0 mov cr8,rax
0038:00000000`8d7dd404 8f4528 pop qword ptr [rbp+28h]
0038:00000000`8d7dd407 4883c430 add rsp,30h
0038:00000000`8d7dd40b 8f4518 pop qword ptr [rbp+18h]
0038:00000000`8d7dd40e 58 pop rax
0038:00000000`8d7dd40f 58 pop rax
0038:00000000`8d7dd410 58 pop rax
0038:00000000`8d7dd411 488ec0 mov es,ax
0038:00000000`8d7dd414 58 pop rax
```

保护每个任务的空间，大道并行，万物共生而不相害

保护维护公共秩序的高特权空间

Modify Register CR0

Register Value: 0x0000000080000013

Original Value: 0x0000000080000013

Group Value: 0x01

PE 0:0

cr0=0000000080000033

Register Layout:

RSVD
RSVD
CD
63 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 1 0
PG
NW
AM
WP

RSVD
ET
EM
PE
MP
TS
NE

Protection Enabled: 1 = Protected mode

Description:

Control Register 0 - Contains system control flags that control operating mode and states of the processor.

0 Protection Enabled
Enables protected mode when set; enables real-address mode when clear. This flag does not enable paging directly. It only enables segment-level protection. To enable paging,

Set Restore Close

# 1:1映射

```
u
0038:00000000`8d7dd3ef 4883c408 add rsp,8
0038:00000000`8d7dd3f3 58 pop rax
0038:00000000`8d7dd3f4 0f22d0 mov cr2,rax
0038:00000000`8d7dd3f7 58 pop rax
0038:00000000`8d7dd3f8 0f22d8 mov cr3,rax
0038:00000000`8d7dd3fb 58 pop rax
0038:00000000`8d7dd3fc 0f22e0 mov cr4,rax
0038:00000000`8d7dd3ff 58 pop rax
[ndb]!db 8d7dd3ef
!db 8d7dd3ef
#8d7dd3ef 48 83 c4 08 58 0f 22 d0-58 0f 22 d8 58 0f 22 e0 H...X.".X.".X.".
#8d7dd3ff 58 44 0f 22 c0 8f 45 28-48 83 c4 30 8f 45 18 58 XD."..E(H..0.E.X
#8d7dd40f 58 58 48 8e c0 58 48 8e-d8 8f 45 20 8f 45 38 5f XXH..XH...E .E8_
#8d7dd41f 5e 48 83 c4 08 8f 45 30-5b 5a 59 58 41 58 41 59 ^H....E0[ZYXAXAY
#8d7dd42f 41 5a 41 5b 41 5c 41 5d-41 5e 41 5f 48 8b e5 5d AZA[A\A]A^A_H..]
#8d7dd43f 48 83 c4 10 48 83 7c 24-e0 00 74 14 48 83 7c 24 H...H.|$..t.H.|$
#8d7dd44f d8 01 74 04 ff 64 24 e0-48 83 ec 08 ff 64 24 e8 ..t..d$.H....d$.
#8d7dd45f 48 83 3d 09 69 ff ff 00-74 18 50 48 8b c4 48 8b H.=.i...t.PH..H.
r cr0
cr0=0000000080000033
```

Console | Registers | Problems | Executables | Platform Register Dictionary | System Debugger Console | Platform Reg

| Name | Hex | Decimal |
|---|---|---|
| rax | 0000000080fff801 | 2164258817 |
| rdx | 0000000000000cf8 | 3320 |
| rcx | 0000000000000000 | 0 |
| rbx | 000000008d3b7370 | 2369483632 |
| rsi | 000000008d351018 | 2369064984 |
| rdi | 00000000ffffff00 | 4294967040 |
| rbp | 0000000000000000 | 0 |
| rsp | 000000008d764aa8 | 2373339816 |
| r8 | 0000000000000000 | 0 |
| r9 | 0000000000000000 | 0 |
| r10 | 0000000000000034 | 52 |
| r11 | 000000008d764a30 | 2373339696 |
| r12 | 0000000000000000 | 0 |
| r13 | 0000000000000000 | 0 |
| r14 | 0000000400000000 | 17179869184 |
| r15 | 0000000000000001 | 1 |
| rip | 000000008d7fe9de | 2373970398 |
| eflags | 00010046 | 65606 |
| es | 0020 | 32 |
| cs | 0038 | 56 |
| ss | 0020 | 32 |
| ds | 0020 | 32 |
| fs | 0020 | 32 |
| gs | 0020 | 32 |

Console | Registers | Problems | Executables | Platform Register Dictionary | System Debugger Console | Platform Reg

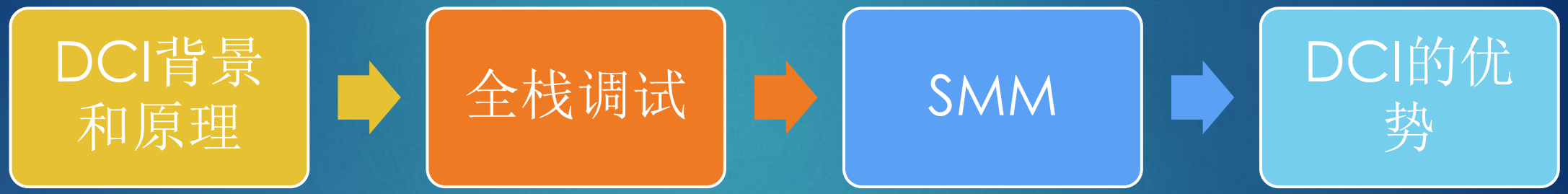
| Name | Hex | Decimal |
|---|---|---|
| rax | 0000000080fff801 | 2164258817 |
| rdx | 0000000000000cf8 | 3320 |
| rcx | 0000000000000000 | 0 |
| rbx | 000000008d3b7370 | 2369483632 |
| rsi | 000000008d351018 | 2369064984 |
| rdi | 00000000fffff00 | 4294967040 |
| rbp | 0000000000000000 | 0 |
| rsp | 000000008d764aa8 | 2373339816 |
| r8 | 0000000000000000 | 0 |
| r9 | 0000000000000000 | 0 |
| r10 | 0000000000000034 | 52 |
| r11 | 000000008d764a30 | 2373339696 |
| r12 | 0000000000000000 | 0 |
| r13 | 0000000000000000 | 0 |
| r14 | 0000000400000000 | 17179869184 |
| r15 | 0000000000000001 | 1 |
| rip | 000000008d7fe9de | 2373970398 |
| eflags | 00010046 | 65606 |
| es | 0020 | 32 |
| cs | 0038 | 56 |
| ss | 0020 | 32 |
| ds | 0020 | 32 |
| fs | 0020 | 32 |
| gs | 0020 | 32 |

| | | | |
|---|---|---|---|
| system registers | | | |
| cr0 | 0000000080000033 | 2147483699 | |
| pe | 1 | 1 | Protection Enable bit |
| mp | 1 | 1 | Monitor Coprocesor |
| em | 0 | 0 | Emulation |
| ts | 0 | 0 | Task switched |
| et | 1 | 1 | Extention type |
| ne | 1 | 1 | Numeric error |
| wp | 0 | 0 | Write protect |
| am | 0 | 0 | Alignment Mask |
| nw | 0 | 0 | Not Write-through |
| cd | 0 | 0 | Cache Disable |
| pg | 1 | 1 | Paging |
| rf | 0 | 0 | Resume Flag |
| vm | 0 | 0 | Virtual 8086 Mode |
| ac | 0 | 0 | Alignment Check |
| vif | 0 | 0 | Virtual Interrupt Flag |
| vip | 0 | 0 | Virtual Interrupt Pending |
| id | 0 | 0 | ID Flag |
| cr2 | 0000000000000000 | 0 | |
| cr3 | 000000008d735000 | 2373144576 | |
| pwt | 0 | 0 | Page-level Write-Through |
| pcd | 0 | 0 | Page-level Cache Disable |
| pdb | 0000000008d735 | 579381 | Page-Directory Base |

| | | | |
|---|---|---|---|
| cr4 | 0000000000000668 | 1640 | |
| vme | 0 | 0 | Virtual-8086 Mode Extensions |
| pvi | 0 | 0 | Protected-Mode Virtual Interrupts |
| tsd | 0 | 0 | Time Stamp Disable |
| de | 1 | 1 | Debugging Extensions |
| pse | 0 | 0 | Page Size Extensions |
| pae | 1 | 1 | Physical Address Extension |
| mce | 1 | 1 | Machine-Check Enable |
| pge | 0 | 0 | Page Global Enable |
| pce | 0 | 0 | Performance-Monitoring Counter Enable |
| osfxsr | 1 | 1 | OS Support for FXSAVE and FXRSTOR inst... |
| osxmmexcpt | 1 | 1 | OS Support for Unmasked SIMD Floating-... |
| vmxe | 0 | 0 | VMX-Enable Bit |
| smxe | 0 | 0 | SMX-Enable Bit |
| fsgsbase | 0 | 0 | FSGSBASE-Enable Bit |
| pcide | 0 | 0 | PCID-Enable Bit |
| osxsave | 0 | 0 | XSAVE and Processor Extended States-En... |
| smep | 0 | 0 | SMEP-Enable Bit |
| smap | 0 | 0 | SMAP-Enable Bit |
| pke | 0 | 0 | Protection-Key-Enable Bit |

| | | | |
|---|---|---|---|
| cr8 | 0000000000000000 | 0 | |
| tpl | 0 | 0 | Task Priority Level |
| efer | 0000000000000d00 | 3328 | |
| SYSCALL Enable | 0 | 0 | SYSCALL Enable |
| IA-32e Mode Enable | 1 | 1 | IA-32e Mode Enable |
| IA-32e Mode Active | 1 | 1 | IA-32e Mode Active |
| Execute Disable Bit Enable | 1 | 1 | Execute Disable Bit Enable |
| mxcsr | 00001f80 | 8064 | |
| ie | 0 | 0 | Invalid Operation Flag |
| de | 0 | 0 | Denormal Flag |
| ze | 0 | 0 | Divide-by-Zero Flag |
| oe | 0 | 0 | Overflow Flag |
| ue | 0 | 0 | Underflow Flag |
| pe | 0 | 0 | Precision Flag |
| daz | 0 | 0 | Denormals Are Zeros |
| im | 1 | 1 | Invalid Operation Mask |
| dm | 1 | 1 | Denormal Operation Mask |
| zm | 1 | 1 | Divide-by-Zero Mask |
| om | 1 | 1 | Overflow Mask |
| um | 1 | 1 | Underflow Mask |
| pm | 1 | 1 | Precision Mask |
| rc | 0 | 0 | Rounding Control |
| fz | 0 | 0 | Flush to Zero |

| | | | |
|---|---|---|---|
| tssbas | 8d734050 | 2373140560 | |
| tsslim | 00000067 | 103 | |
| tssar | 008b | 139 | |
| Type | b | 11 | Type |
| S | 0 | 0 | descriptor type flag |
| DPL | 0 | 0 | descriptor privilege level field |
| P | 1 | 1 | segment-present flag |
| AVL | 0 | 0 | Available for use by system software |
| L | 0 | 0 | 64-bit code segment flag |
| D/B | 0 | 0 | default operation size/default stack point... |
| G | 0 | 0 | granularity flag |
| csar | a09b | 41115 | |
| Type | b | 11 | Type |
| S | 1 | 1 | descriptor type flag |
| DPL | 0 | 0 | descriptor privilege level field |
| P | 1 | 1 | segment-present flag |
| AVL | 0 | 0 | Available for use by system software |
| L | 1 | 1 | 64-bit code segment flag |
| D/B | 0 | 0 | default operation size/default stack point... |
| G | 1 | 1 | granularity flag |


DCI背景和原理
全栈调试
SMM
DCI的优势

System Management Mode (SMM) is the most privileged CPU operation mode on x86/x86_64 architectures. It can be thought of as of "Ring -2", as the code executing in SMM has more privileges than even hardware hypervisors (VT), which are colloquially referred to as if operating in "Ring -1".

Rafal Wojtczuk, Joanna Rutkowska
*Attacking SMM Memory via Intel® CPU Cache Poisoning*

# 审视SMM

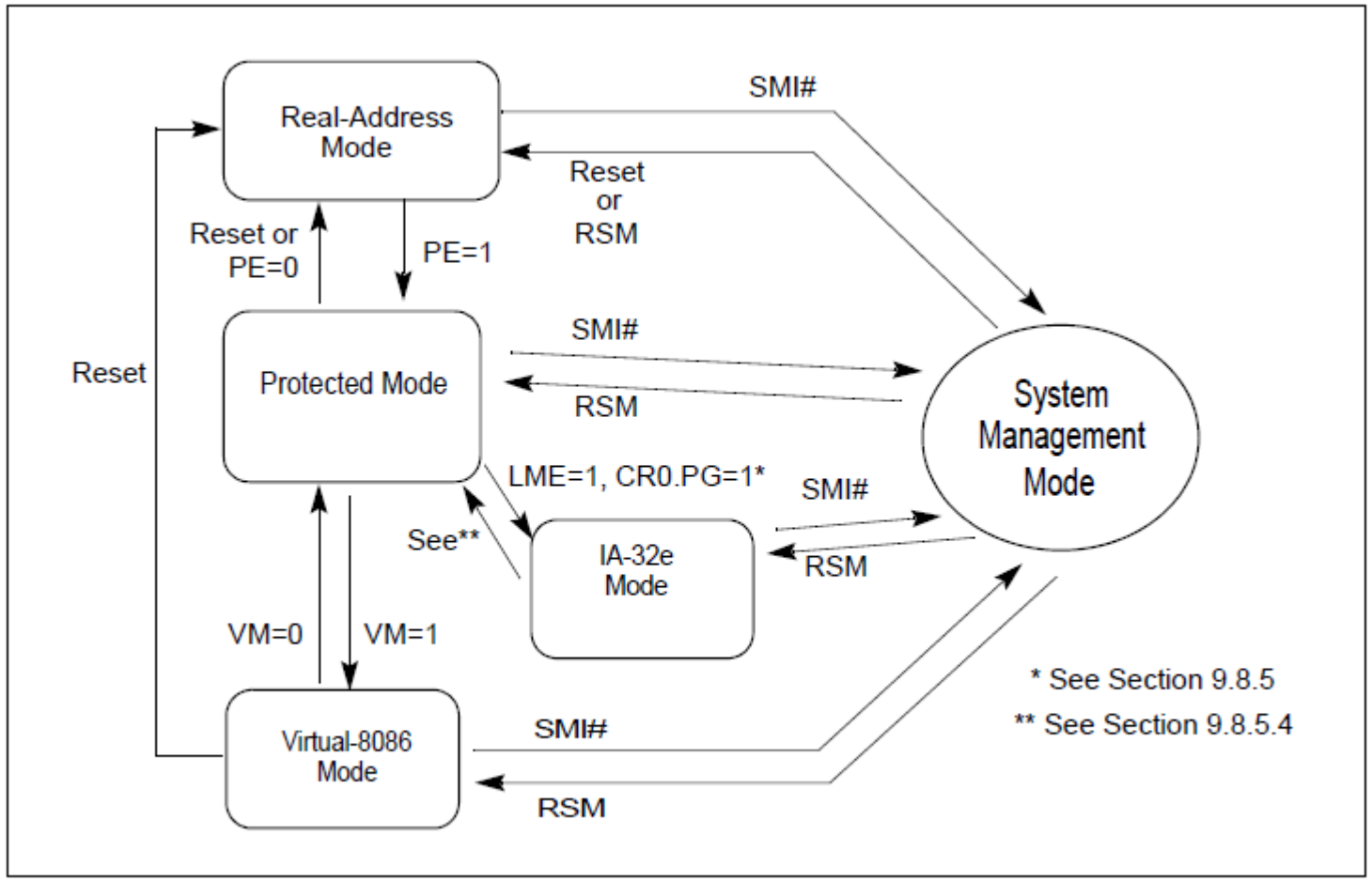



Figure 2-3. Transitions Among the Processor's Operating Modes

```
SPECIAL BREAK 3 ON "SMM Entry Break" :
enabled  (S=0,CS=0)
program stopped: SPECIAL BREAK 'SMM Entry
Break' (ID=3) at "0xC300:0x00008000"
```

Intel(R) System Debugger (Legacy)

File Edit View Run Debug Options Help

LoadDXEModules LoadPEIMs LoadThis

Assembler: 0xC300:0x00007FD2 to 0xC300:0x000080E2

| Trail | Address | Opcodes | Source |
|---|---|---|---|
| | 0xC300:0x00007FF7 | 7C 00 | jl 0x7FF9 <> |
| | 0xC300:0x00007FF9 | 7C 82 | jl 0x7F7D <> |
| | 0xC300:0x00007FFB | 38 0C | cmp byte ptr [si], cl |
| | 0xC300:0x00007FFD | 7C CC | jl 0x7FCB <> |
| | 0xC300:0x00007FFF | 76 | DB 0x76 |
| | 0xC300:0x00008000 | 00 CC | add ah, cl |
| | 0xC300:0x00008002 | 00 78 0C | add byte ptr [bx+si*1+0xC], bh |
| | 0xC300:0x00008005 | 7C CC | jl 0x7FD3 <> |
| | 0xC300:0x00008007 | 76 00 | jbe 0x8009 <> |
| | 0xC300:0x00008009 | E0 10 | loopne 0x801B <> |
| | 0xC300:0x0000800B | 78 0C | js 0x8019 <> |
| | 0xC300:0x0000800D | 7C CC | jl 0x7FDB <> |
| | 0xC300:0x0000800F | 76 00 | jbe 0x8011 <> |
| | 0xC300:0x00008011 | 30 30 | xor byte ptr [bx+si*1], dh |
| | 0xC300:0x00008013 | 78 0C | js 0x8021 <> |
| | 0xC300:0x00008015 | 7C CC | jl 0x7FE3 <> |
| | 0xC300:0x00008017 | 76 00 | jbe 0x8019 <> |
| | 0xC300:0x00008019 | 00 00 | add byte ptr [bx+si*1], al |
| | 0xC300:0x0000801B | 7C C0 | jl 0x7FDD <> |
| | 0xC300:0x0000801D | C0 7C 18 70 | sar byte ptr [si+0x18], 0x70 |
| | 0xC300:0x00008021 | 7C 82 | jl 0x7FA5 <> |
| | 0xC300:0x00008023 | 7C C6 | jl 0x7FEB <> |
| | 0xC300:0x00008025 | FE C0 | inc al |
| | 0xC300:0x00008027 | 7C 00 | jl 0x8029 <> |

Registers

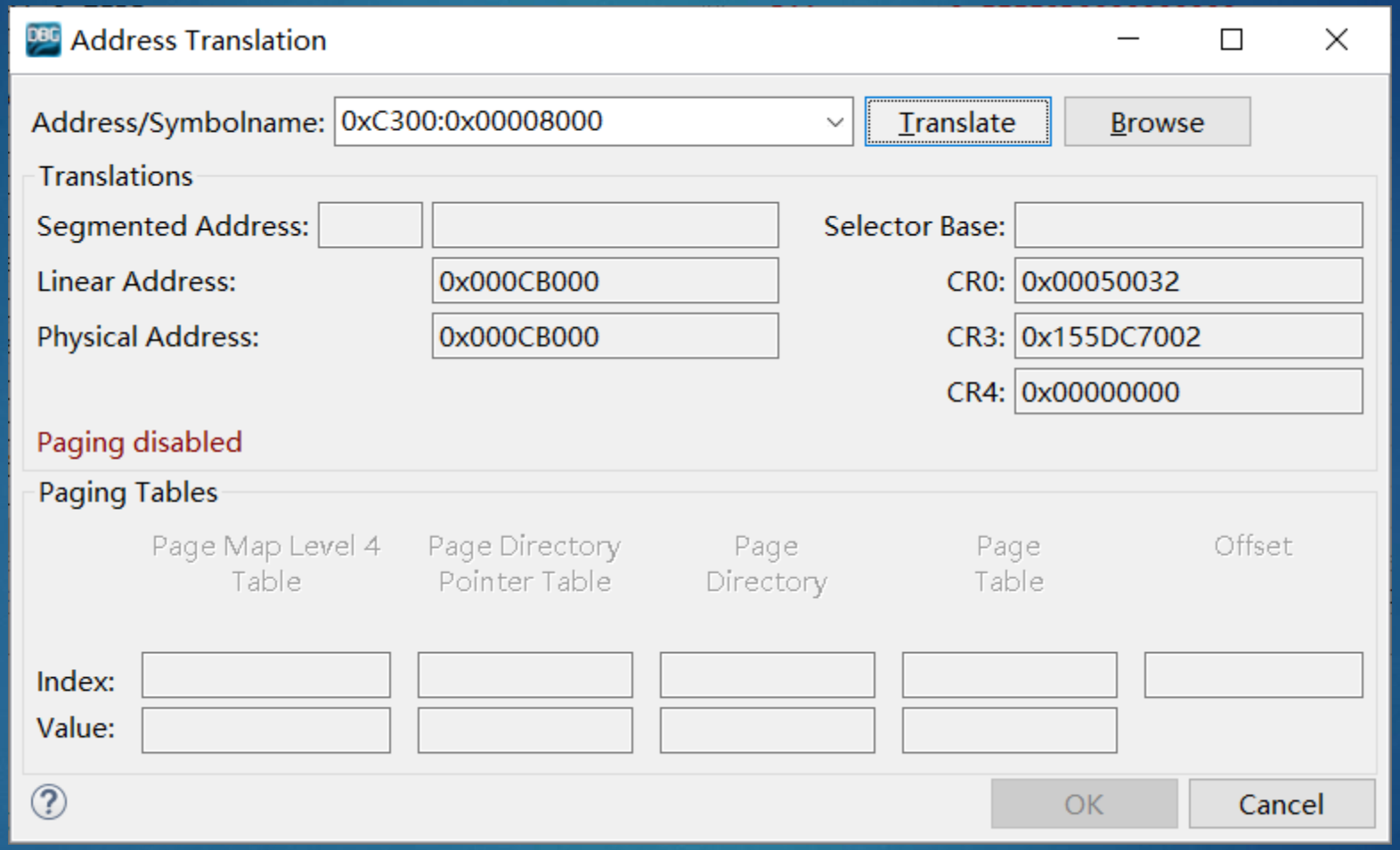
| Register | Value | Description |
|---|---|---|
| RAX | 0x8000000000000000 | |
| RBX | 0x00000000FC803080 | |
| RCX | 0xFFFF880000000000 | |
| RDX | 0x72836B300F2316F0 | |
| RSI | 0xFFFF88000354ACB0 | |
| RDI | 0x0000000000000020 | |
| RSP | 0x000000001FAF9220 | |
| RBP | 0xFFFF81861FAF92D9 | |
| R8 | 0xFFFFB70BFA971470 | |
| R9 | 0xFFFFB70BFA210000 | |
| R10 | 0x000000000000216E | |
| R11 | 0xFFFF9D0000000000 | |
| R12 | 0xFFFFB70BFCB06160 | |
| R13 | 0x0000000000000000 | |
| R14 | 0xFFFFB70BFA536900 | |
| R15 | 0xFFFF9D3FFEC4DD60 | |
| RIP | 0x0000000000008000 | |
| RFL | 0x0000000000010002 | RFLAGS ... |
| EAX | 0x00000000 | |
| EBX | 0xFC803080 | |
| ECX | 0x00000000 | |
| EDX | 0x0F2316F0 | |
| ESI | 0x0354ACB0 | |
| EDI | 0x00000020 | |
| ESP | 0x1FAF9220 | |

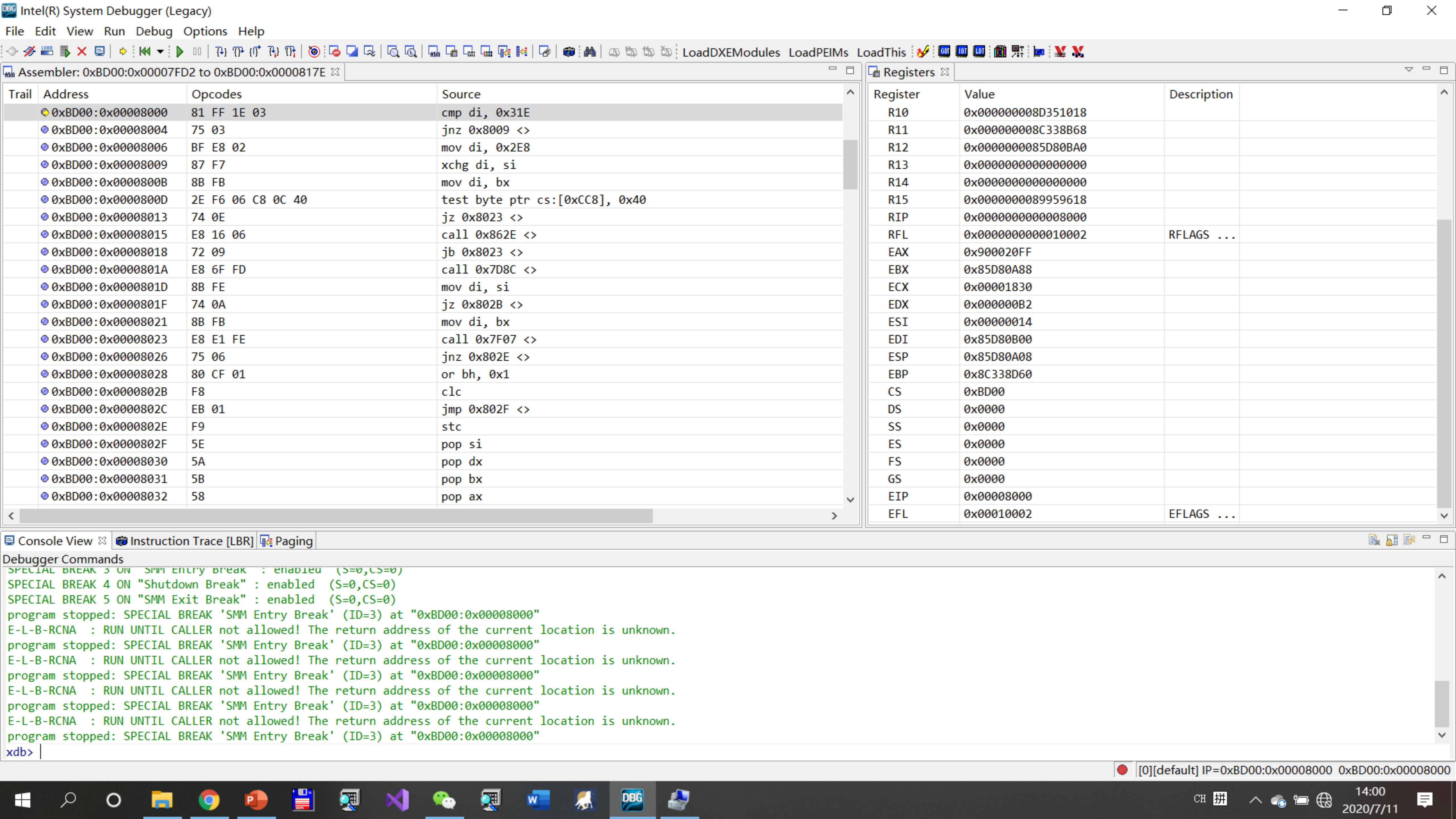
Console View | GDT: 0xffffca801c095fb0 | Instruction Trace [PT] | Paging | Memory[1] 0x0010:0x8D7C50A2 | Hardware Threads | Breakpoints | Processor Specific Registers | LDT from LDTR

| Name | Value | Description |
|---|---|---|
| SSATR | 0x8093 | SS Attributes |
| Control | | |
| CR0 | 0x0000000000050032 | Control Register 0 - System Control Flags |
| CR2 | 0x00000246799D3028 | Control Register 2 - Page Fault Address |
| CR3 | 0x0000000155DC7002 | Control Register 3 - Page Directory Base |
| CR4 | 0x0000000000000000 | Control Register 4 - Enabling Arch. Extensions |
| Debug | | |
| DR0 | 0x0000000000000000 | |
| DR1 | 0x0000000000000000 | |
| DR2 | 0x0000000000000000 | |

[3][default] IP=0xC300:0x00008000 0xC300:0x00008000

CH 拼 15:10 2020/7/11


Address Translation
Address/Symbolname: 0xC300:0x00008000
Translate
Browse
Translations
Segmented Address:
Selector Base:
Linear Address: 0x000CB000
CR0: 0x00050032
Physical Address: 0x000CB000
CR3: 0x155DC7002
CR4: 0x00000000
Paging disabled
Paging Tables
Page Map Level 4 Table
Page Directory Pointer Table
Page Directory
Page Table
Offset
Index:
Value:
OK
Cancel

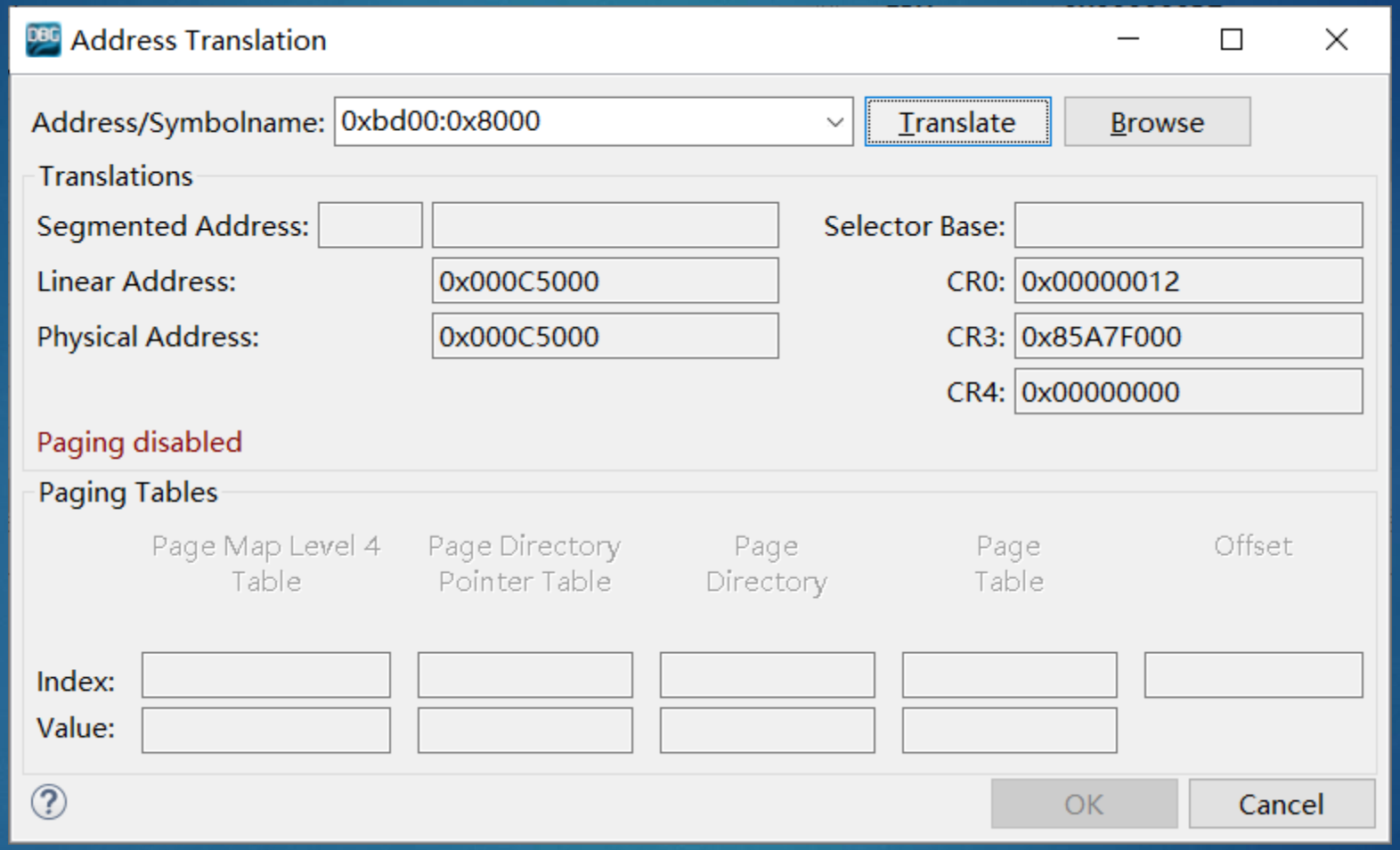


| Trail | Address | Opcodes | Source |
|---|---|---|---|
| | 0xBD00:0x00008000 | 81 FF 1E 03 | cmp di, 0x31E |
| | 0xBD00:0x00008004 | 75 03 | jnz 0x8009 <> |
| | 0xBD00:0x00008006 | BF E8 02 | mov di, 0x2E8 |
| | 0xBD00:0x00008009 | 87 F7 | xchg di, si |
| | 0xBD00:0x0000800B | 8B FB | mov di, bx |
| | 0xBD00:0x0000800D | 2E F6 06 C8 0C 40 | test byte ptr cs:[0xCC8], 0x40 |
| | 0xBD00:0x00008013 | 74 0E | jz 0x8023 <> |
| | 0xBD00:0x00008015 | E8 16 06 | call 0x862E <> |
| | 0xBD00:0x00008018 | 72 09 | jb 0x8023 <> |
| | 0xBD00:0x0000801A | E8 6F FD | call 0x7D8C <> |
| | 0xBD00:0x0000801D | 8B FE | mov di, si |
| | 0xBD00:0x0000801F | 74 0A | jz 0x802B <> |
| | 0xBD00:0x00008021 | 8B FB | mov di, bx |
| | 0xBD00:0x00008023 | E8 E1 FE | call 0x7F07 <> |
| | 0xBD00:0x00008026 | 75 06 | jnz 0x802E <> |
| | 0xBD00:0x00008028 | 80 CF 01 | or bh, 0x1 |
| | 0xBD00:0x0000802B | F8 | clc |
| | 0xBD00:0x0000802C | EB 01 | jmp 0x802F <> |
| | 0xBD00:0x0000802E | F9 | stc |
| | 0xBD00:0x0000802F | 5E | pop si |
| | 0xBD00:0x00008030 | 5A | pop dx |
| | 0xBD00:0x00008031 | 5B | pop bx |
| | 0xBD00:0x00008032 | 58 | pop ax |

| Register | Value | Description |
|---|---|---|
| R10 | 0x000000008D351018 | |
| R11 | 0x000000008C338B68 | |
| R12 | 0x0000000085D80BA0 | |
| R13 | 0x0000000000000000 | |
| R14 | 0x0000000000000000 | |
| R15 | 0x0000000089959618 | |
| RIP | 0x0000000000008000 | |
| RFL | 0x0000000000010002 | RFLAGS ... |
| EAX | 0x900020FF | |
| EBX | 0x85D80A88 | |
| ECX | 0x00001830 | |
| EDX | 0x000000B2 | |
| ESI | 0x00000014 | |
| EDI | 0x85D80B00 | |
| ESP | 0x85D80A08 | |
| EBP | 0x8C338D60 | |
| CS | 0xBD00 | |
| DS | 0x0000 | |
| SS | 0x0000 | |
| ES | 0x0000 | |
| FS | 0x0000 | |
| GS | 0x0000 | |
| EIP | 0x00008000 | |
| EFL | 0x00010002 | EFLAGS ... |

```
SPECIAL BREAK 3 ON "SMM Entry Break" : enabled  (S=0,CS=0)
SPECIAL BREAK 4 ON "Shutdown Break" : enabled  (S=0,CS=0)
SPECIAL BREAK 5 ON "SMM Exit Break" : enabled  (S=0,CS=0)
program stopped: SPECIAL BREAK 'SMM Entry Break' (ID=3) at "0xBD00:0x00008000"
E-L-B-RCNA  : RUN UNTIL CALLER not allowed! The return address of the current location is unknown.
program stopped: SPECIAL BREAK 'SMM Entry Break' (ID=3) at "0xBD00:0x00008000"
E-L-B-RCNA  : RUN UNTIL CALLER not allowed! The return address of the current location is unknown.
program stopped: SPECIAL BREAK 'SMM Entry Break' (ID=3) at "0xBD00:0x00008000"
E-L-B-RCNA  : RUN UNTIL CALLER not allowed! The return address of the current location is unknown.
program stopped: SPECIAL BREAK 'SMM Entry Break' (ID=3) at "0xBD00:0x00008000"
E-L-B-RCNA  : RUN UNTIL CALLER not allowed! The return address of the current location is unknown.
program stopped: SPECIAL BREAK 'SMM Entry Break' (ID=3) at "0xBD00:0x00008000"
xdb>
```

[0][default] IP=0xBD00:0x00008000  0xBD00:0x00008000

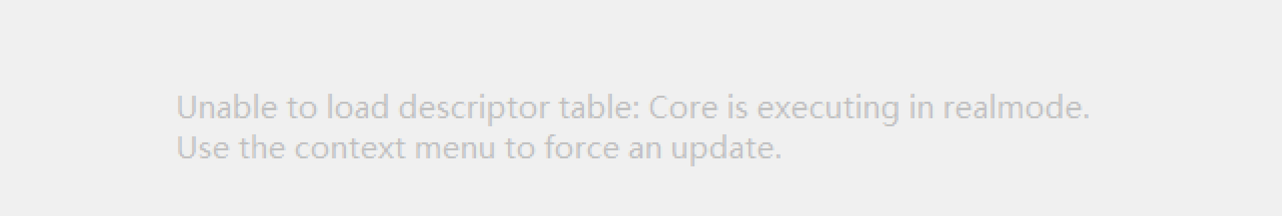

Address Translation
Address/Symbolname: 0xbd00:0x8000
Translate
Browse
Translations
Segmented Address:
Selector Base:
Linear Address: 0x000C5000
CR0: 0x00000012
Physical Address: 0x000C5000
CR3: 0x85A7F000
CR4: 0x00000000
Paging disabled
Paging Tables
Page Map Level 4 Table
Page Directory Pointer Table
Page Directory
Page Table
Offset
Index:
Value:
OK
Cancel

```
-----------------------------------------
#   c5000 031eff81 e8bf0375 8bf78702 06f62efb
#   c5010 74400cc8 0616e80e 6fe80972 74fe8bfd
#   c5020 e8fb8b0a 0675fee1 f801cf80 5ef901eb
#   c5030 c3585b5a 56526651 26d23366 2558458b
#   c5040 2c744ba5 be0008b9 ee834d3c 44852604
#   c5050 74f7e102 348b261b a8e8f787 45f626fc
#   c5060 02748011 f787e3d1 c166d38b d08b10e2
#   c5070 c683f78b 0008b948 04b60f26 01f88346
```

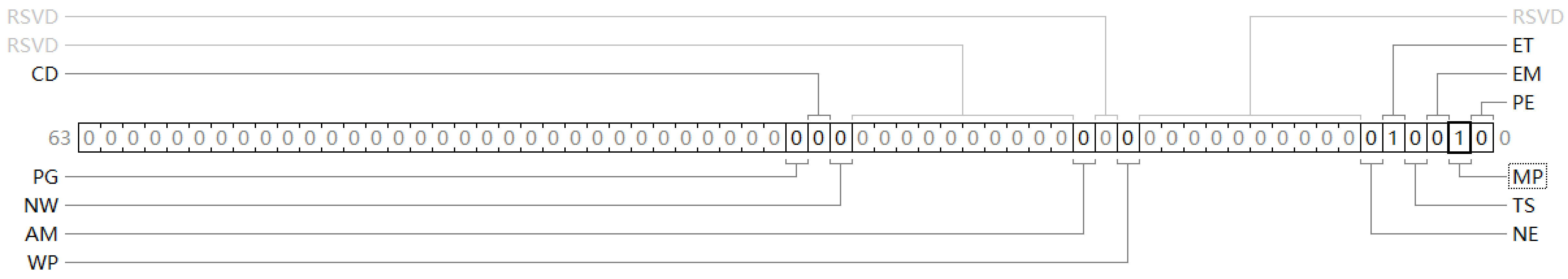
Console View | GDT | Instruction Trace [LBR] | Paging | Hardware Threads | Processor Specific Registers | LDT from LDTR

| Name | Value | Description |
|---|---|---|
| Memory Management | | |
| GDTBAS | 0x000000008C3DFAD0 | Global Descriptor Table Register Base |
| GDTLIM | 0x0047 | Global Descriptor Table Register Limit |
| IDTBAS | 0x000000008C3E60C0 | Interrupt Descriptor Table Register Base |
| IDTLIM | 0x0000 | Interrupt Descriptor Table Register Limit |
| LDTR | 0x0000 | Local Descriptor Table Register |
| LDTBAS | 0x0000000000000000 | Local Descriptor Table Base |
| LDTLIM | 0xFFFF | Local Descriptor Table Limit |
| LDTAR | 0x00 | Local Descriptor Table Attributes |
| TR | <invalid> | Task Register |
| TSSBAS | 0x0000000000000000 | Task Base |
| TSSLIM | 0xFFFF | Task Limit |
| TSSAR | 0x8B | Task Attributes |
| Shadow | | |
| CSBAS | 0x8D7BD000 | CS Base |
| CSLIM | 0xFFFFFFFF | CS Limit |
| CSATR | 0x809B | CS Attributes |
| DSBAS | 0x00000000 | DS Base |
| DSLIM | 0xFFFFFFFF | DS Limit |
| DSATR | 0x8093 | DS Attributes |
| ESBAS | 0x00000000 | ES Base |
| ESLIM | 0xFFFFFFFF | ES Limit |
| ESATR | 0x8093 | ES Attributes |
| FSBAS | 0x00000000 | FS Base |
| FSLIM | 0xFFFFFFFF | FS Limit |
| FSATR | 0x8093 | FS Attributes |
| GSBAS | 0x00000000 | GS Base |
| GSLIM | 0xFFFFFFFF | GS Limit |
| GSATR | 0x8093 | GS Attributes |
| SSBAS | 0x00000000 | SS Base |
| SSLIM | 0xFFFFFFFF | SS Limit |
| SSATR | 0x8093 | SS Attributes |
| Control | | |
| CR0 | 0x0000000000000012 | Control Register 0 - System Control Flags |
| CR2 | 0x0000000000000000 | Control Register 2 - Page Fault Address |
| CR3 | 0x0000000085A7F000 | Control Register 3 - Page Directory Base |
| CR4 | 0x0000000000000000 | Control Register 4 - Enabling Arch. Extensions |

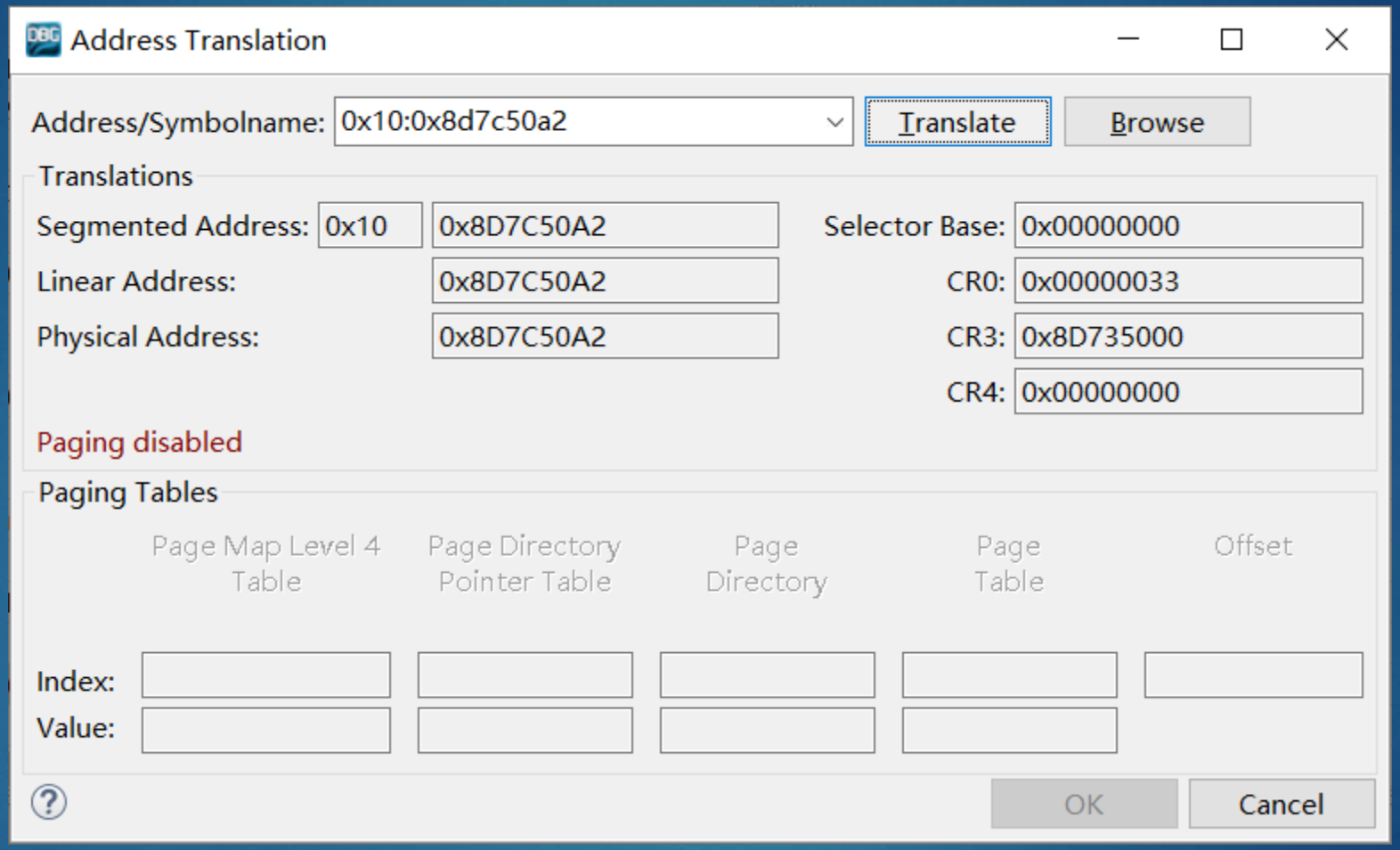
- ISD访问GDT时失败
- CR0的值位0x12



Unable to load descriptor table: Core is executing in realmode.
Use the context menu to force an update.



```
program stopped: SPECIAL BREAK 'SMM Entry Break' (ID=3) at "0xBD00:0x00008000"
program stopped: SPECIAL BREAK 'SMM Exit Break' (ID=5) at "0xBD00:0x0000801A"
```


Address Translation
Address/Symbolname: 0x10:0x8d7c50a2
Translate
Browse
Translations
Segmented Address: 0x10
0x8D7C50A2
Selector Base: 0x00000000
Linear Address: 0x8D7C50A2
CR0: 0x00000033
Physical Address: 0x8D7C50A2
CR3: 0x8D735000
CR4: 0x00000000
Paging disabled
Paging Tables
Page Map Level 4 Table
Page Directory Pointer Table
Page Directory
Page Table
Offset
Index:
Value:
OK
Cancel

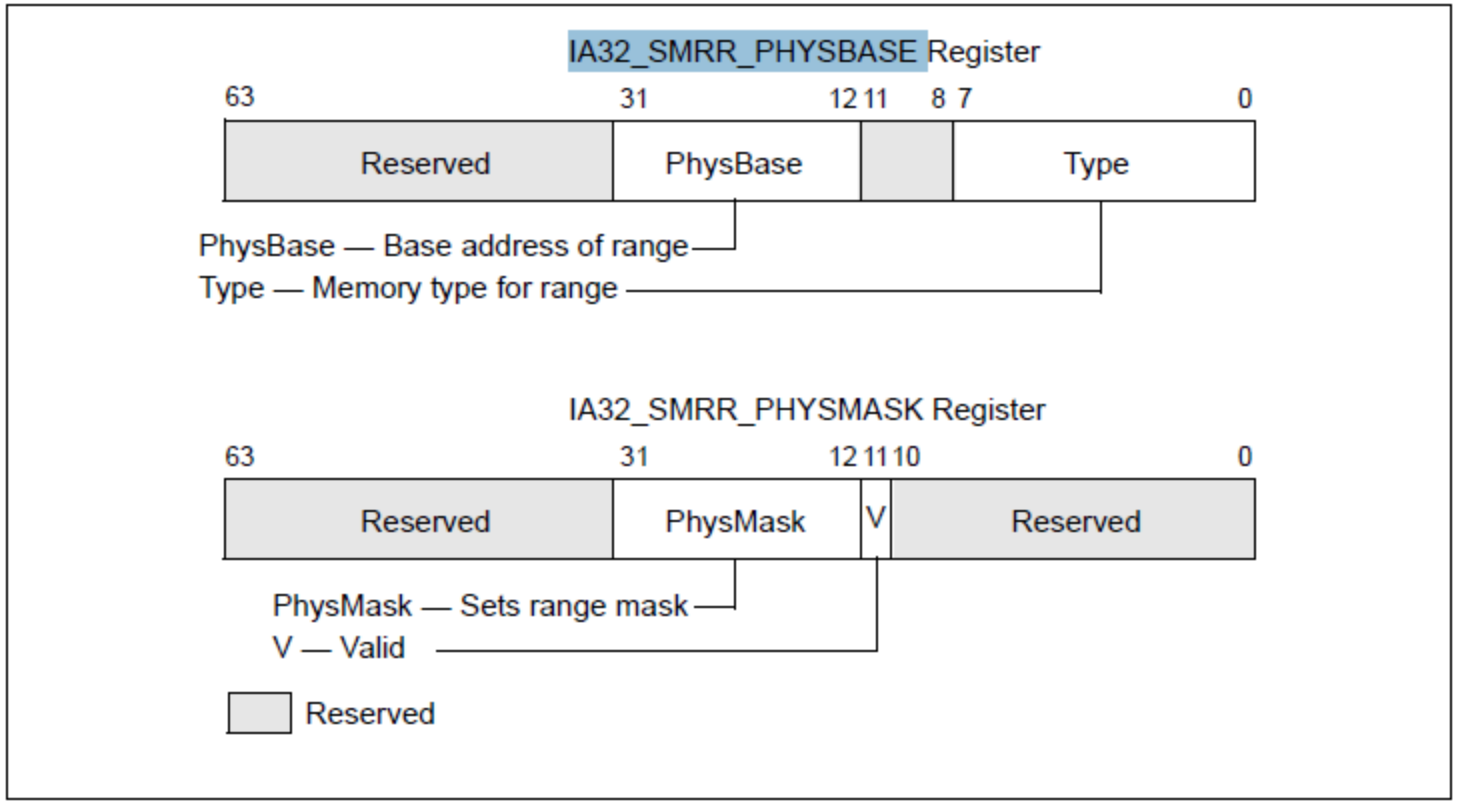



Figure 11-8. IA32_SMRR_PHYSBASE and IA32_SMRR_PHYSMASK SMRR Pair

# IA32_SMRR_PHYSBASE

```
rdmsr 1f2
msr[1f2] = 00000000`8d400006

rdmsr 1f3
msr[1f3] = 00000000`ffc00800

? ffc00800&8d400006
Evaluate expression: -1925185536 = 8d400000
```

Intel(R) System Debugger (Legacy)

File Edit View Run Debug Options Help

LoadDXEModules LoadPEIMs LoadThis

Assembler: 0xBD00:0x00007FD2 to 0xBD00:0x0000811F

| Trail | Address | Opcodes | Source |
|---|---|---|---|
| | 0xBD00:0x00007FF6 | E8 58 06 | call 0x8651 <> |
| | 0xBD00:0x00007FF9 | 72 10 | jb 0x800B <> |
| | 0xBD00:0x00007FFB | E8 94 F2 | call 0x7292 <> |
| | 0xBD00:0x00007FFE | 72 2E | jb 0x802E <> |
| | 0xBD00:0x00008000 | 81 FF 1E 03 | cmp di, 0x31E |
| | 0xBD00:0x00008004 | 75 03 | jnz 0x8009 <> |
| | 0xBD00:0x00008006 | BF E8 02 | mov di, 0x2E8 |
| | 0xBD00:0x00008009 | 87 F7 | xchg di, si |
| | 0xBD00:0x0000800B | 8B FB | mov di, bx |
| | 0xBD00:0x0000800D | 2E F6 06 C8 0C 40 | test byte ptr cs:[0xCC8], 0x40 |
| | 0xBD00:0x00008013 | 74 0E | jz 0x8023 <> |
| | 0xBD00:0x00008015 | E8 16 06 | call 0x862E <> |
| | 0xBD00:0x00008018 | 72 09 | jb 0x8023 <> |
| | 0xBD00:0x0000801A | E8 6F FD | call 0x7D8C <> |
| | 0xBD00:0x0000801D | 8B FE | mov di, si |
| | 0xBD00:0x0000801F | 74 0A | jz 0x802B <> |
| | 0xBD00:0x00008021 | 8B FB | mov di, bx |
| | 0xBD00:0x00008023 | E8 E1 FE | call 0x7F07 <> |
| | 0xBD00:0x00008026 | 75 06 | jnz 0x802E <> |
| | 0xBD00:0x00008028 | 80 CF 01 | or bh, 0x1 |
| | 0xBD00:0x0000802B | F8 | clc |
| | 0xBD00:0x0000802C | EB 01 | jmp 0x802F <> |
| | 0xBD00:0x0000802E | F9 | stc |
| | 0xBD00:0x0000802F | 5E | pop si |

Registers

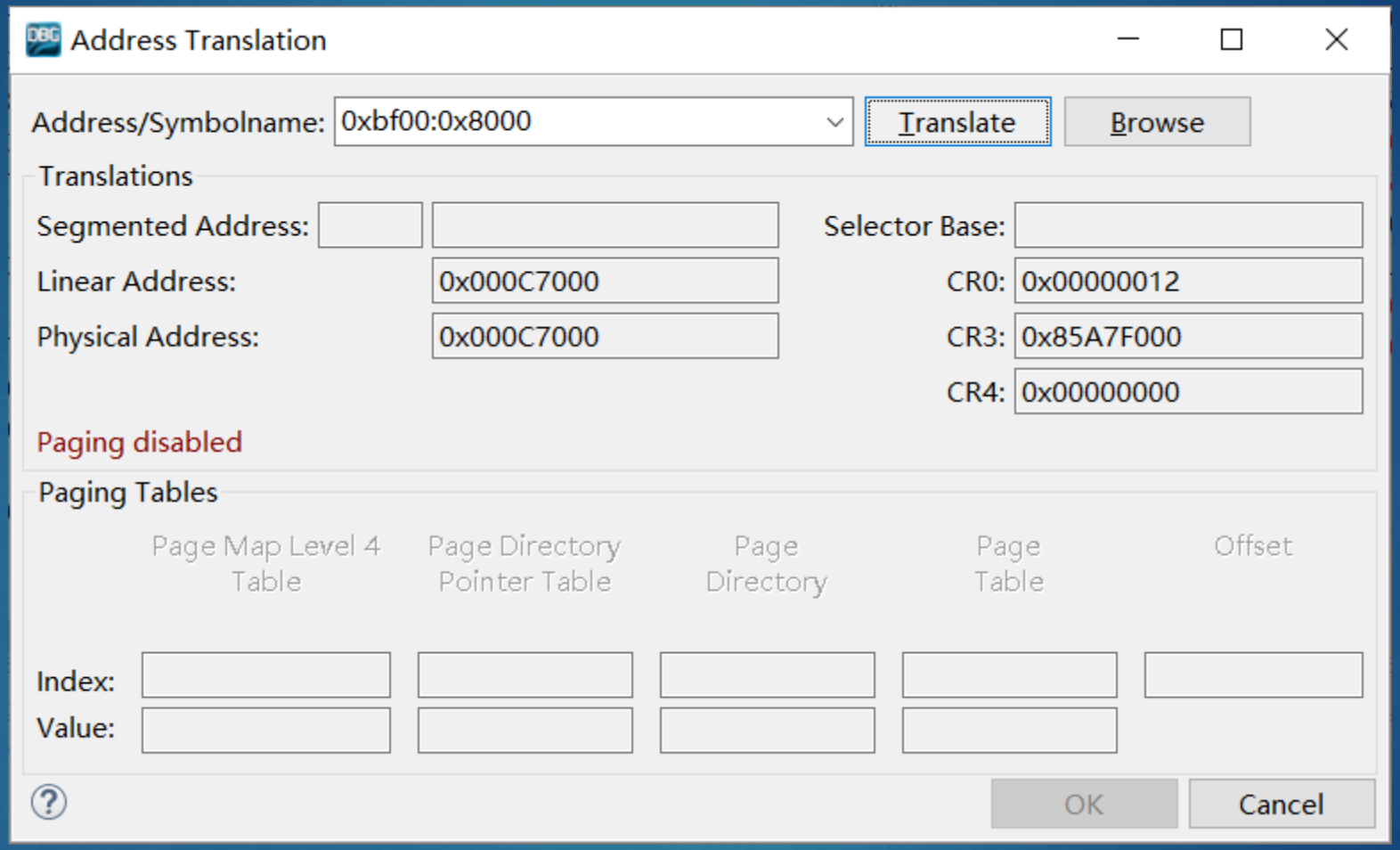
| Register | Value | Description |
|---|---|---|
| RAX | 0x00000000900020FF | |
| RBX | 0x0000000085D80AC8 | |
| RCX | 0x0000000000001830 | |
| RDX | 0x00000000000000B2 | |
| RSI | 0x000000008C338B68 | |
| RDI | 0x0000000000000000 | |
| RSP | 0x0000000085D80A48 | |
| RBP | 0x000000008D351018 | |
| R8 | 0x00000000000000FF | |
| R9 | 0x0000000000000000 | |
| R10 | 0x000000008D351018 | |
| R11 | 0x000000008C338B68 | |
| R12 | 0x0000000000000006 | |
| R13 | 0x000000008C338D60 | |
| R14 | 0x0000000000000000 | |
| R15 | 0x0000000089959618 | |
| RIP | 0x0000000000008000 | |
| RFL | 0x0000000000010002 | RFLAGS ... |
| EAX | 0x900020FF | |
| EBX | 0x85D80AC8 | |
| ECX | 0x00001830 | |
| EDX | 0x000000B2 | |
| ESI | 0x8C338B68 | |
| EDI | 0x00000000 | |
| ESP | 0x85D80A48 | |

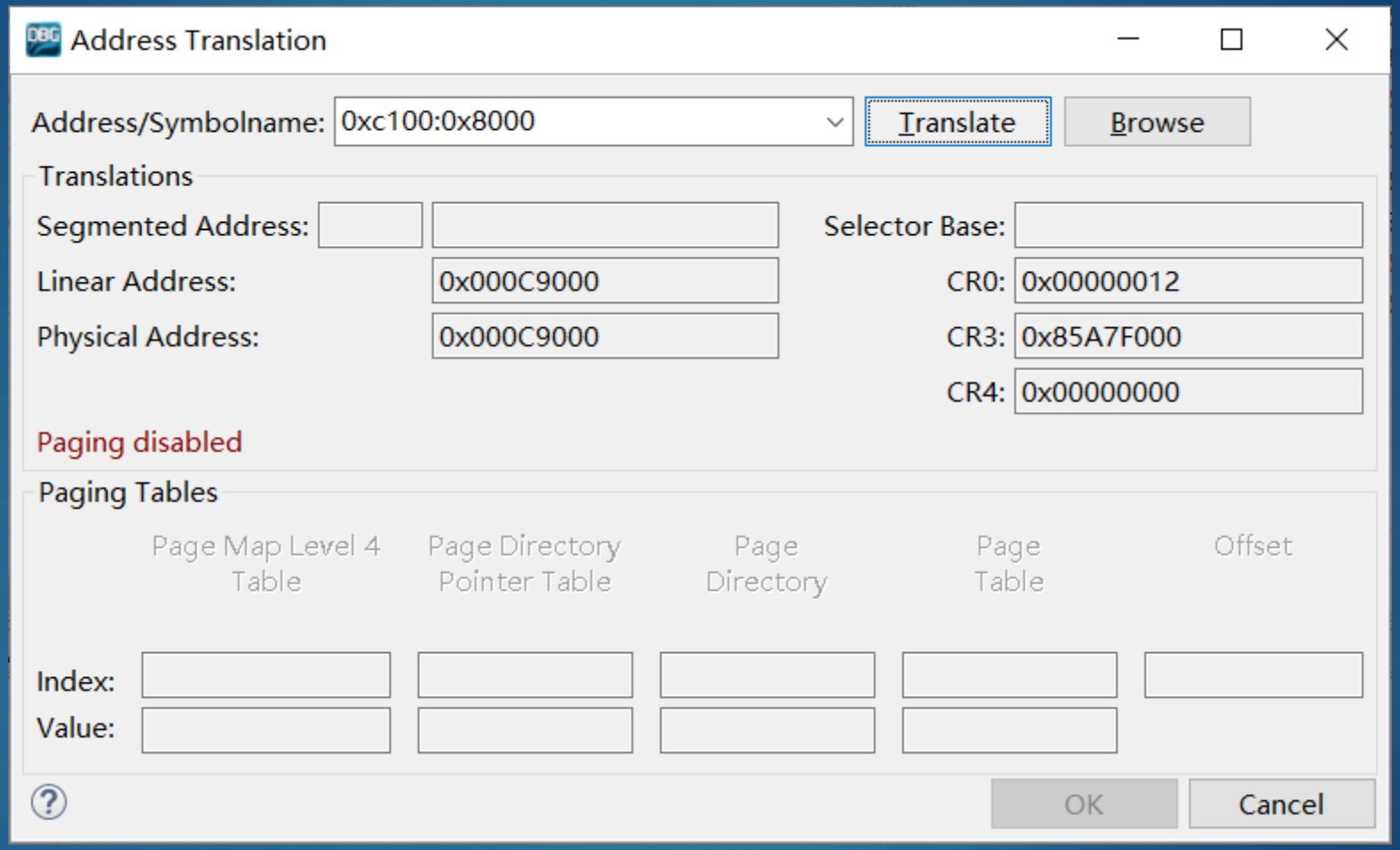
Console View | Instruction Trace [LBR] | Paging | Memory[1] 0x0010:0x8D7C50A2 | Hardware Threads

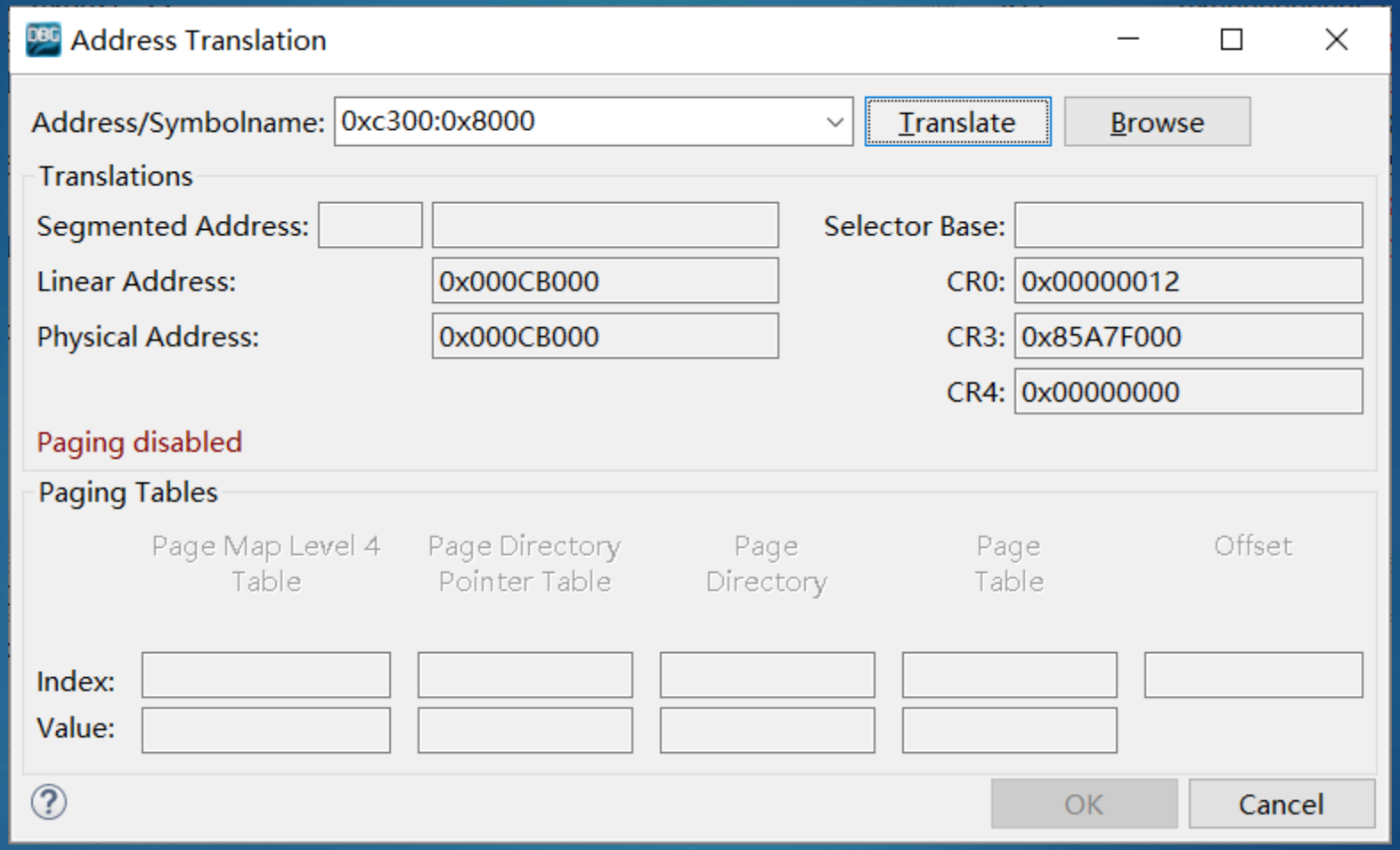
| Name | Id | State | Address | Location | File |
|---|---|---|---|---|---|
| IA | | | | | |
| | 0 | SMM entry | 0xBD00:0x00008000 | | |
| | 1 | SMM entry | 0xBF00:0x00008000 | | |
| | 2 | SMM entry | 0xC100:0x00008000 | | |
| | 3 | SMM entry | 0xC300:0x00008000 | | |

[0][default] IP=0xBD00:0x00008000 0xBD00:0x00008000

CH 拼 14:11 2020/7/11


Address Translation
Address/Symbolname: 0xbf00:0x8000
Translate
Browse
Translations
Segmented Address:
Selector Base:
Linear Address: 0x000C7000
CR0: 0x00000012
Physical Address: 0x000C7000
CR3: 0x85A7F000
CR4: 0x00000000
Paging disabled
Paging Tables
Page Map Level 4 Table
Page Directory Pointer Table
Page Directory
Page Table
Offset
Index:
Value:
OK
Cancel


Address Translation
Address/Symbolname: 0xc100:0x8000
Translate
Browse
Translations
Segmented Address:
Selector Base:
Linear Address: 0x000C9000
CR0: 0x00000012
Physical Address: 0x000C9000
CR3: 0x85A7F000
CR4: 0x00000000
Paging disabled
Paging Tables
Page Map Level 4 Table
Page Directory Pointer Table
Page Directory
Page Table
Offset
Index:
Value:
OK
Cancel


Address Translation
Address/Symbolname: 0xc300:0x8000
Translate
Browse
Translations
Segmented Address:
Selector Base:
Linear Address: 0x000CB000
CR0: 0x00000012
Physical Address: 0x000CB000
CR3: 0x85A7F000
CR4: 0x00000000
Paging disabled
Paging Tables
Page Map Level 4 Table
Page Directory Pointer Table
Page Directory
Page Table
Offset
Index:
Value:
OK
Cancel

# SMM下的寄存器

Console View | Instruction Trace [LBR] | Paging | Memory[1] 0x0010:0x8D7C50A2 | Hardware Threads

| Name | Value | Description |
|---|---|---|
| CSATR | 0x809B | CS Attributes |
| DSBAS | 0x00000000 | DS Base |
| DSLIM | 0xFFFFFFFF | DS Limit |
| DSATR | 0x8093 | DS Attributes |
| ESBAS | 0x00000000 | ES Base |
| ESLIM | 0xFFFFFFFF | ES Limit |
| ESATR | 0x8093 | ES Attributes |
| FSBAS | 0x00000000 | FS Base |
| FSLIM | 0xFFFFFFFF | FS Limit |
| FSATR | 0x8093 | FS Attributes |
| GSBAS | 0x00000000 | GS Base |
| GSLIM | 0xFFFFFFFF | GS Limit |
| GSATR | 0x8093 | GS Attributes |
| SSBAS | 0x00000000 | SS Base |
| SSLIM | 0xFFFFFFFF | SS Limit |
| SSATR | 0x8093 | SS Attributes |
| Control | | |
| CR0 | 0x0000000000000012 | Control Register 0 - Sy... |
| CR2 | 0x0000000000000000 | Control Register 2 - Pa... |
| CR3 | 0x0000000085A7F000 | Control Register 3 - Pa... |
| CR4 | 0x0000000000000000 | Control Register 4 - En... |

Intel(R) System Debugger (Legacy)

File Edit View Run Debug Options Help

LoadDXEModules LoadPEIMs LoadThis

Assembler: 0x0038:0x000000008D7CB144 to 0x0038:0x000000008D7CB2A2

| Trail | Address | Opcodes | Source |
|---|---|---|---|
| | 0x0038:0x0000000... | 0F AA | rsm |
| | 0x0038:0x0000000... | 66 66 66 66 0F 1F 84 00 00 00 00 00 | nop word ptr [rax+rax*1], ax |
| | 0x0038:0x0000000... | F8 | clc |
| | 0x0038:0x0000000... | 4F 7C 8D | jl 0x8D7CB111 |
| | 0x0038:0x0000000... | 18 00 | sbb byte ptr [rax], al |
| | 0x0038:0x0000000... | 00 00 | add byt |
| | 0x0038:0x0000000... | F3 01 28 | add dwo |
| | 0x0038:0x0000000... | 7C DB | jl 0x8D |
| | 0x0038:0x0000000... | 22 A0 9F D2 01 FC | and ah, |
| | 0x0038:0x0000000... | BC E8 62 A0 0D | mov esp |
| | 0x0038:0x0000000... | 82 | DB 0x82 |

Registers

| Register | Value | Description |
|---|---|---|
| RAX | 0x000000008D7D8DFC | |
| RBX | 0x0000000000000003 | |
| RCX | 0x0000000000000003 | |
| RDX | 0x000000008D744120 | |
| RSI | 0x0000000000058C40 | |

Console View | Instruction Trace [PT] | Paging | Memory[1] 0x0010:0x8D7C50

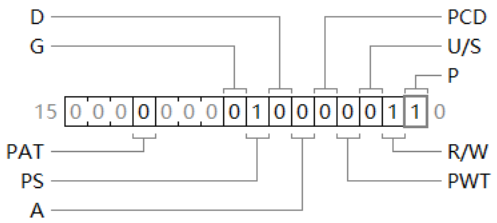
| Index | Virtual Memory Range | Physi | |
|---|---|---|---|
| PML4 [0] | 0x0000000000000000 to 0x0000007FFFFFFFFF | 0x00 | |
| PDPT [0] | 0x0000000000000000 to 0x000000003FFFFFFF | 0x00 | 1 XD=0 |
| PD [0] | 0x0000000000000000 to 0x00000000001FFFFF | 0x00 | 0 XD=0 |
| PD [1] | 0x0000000000200000 to 0x00000000003FFFFF | 0x00 | 0 XD=0 |
| PD [2] | 0x0000000000400000 to 0x00000000005FFFFF | 0x00 | 0 XD=0 |
| PD [3] | 0x0000000000600000 to 0x00000000007FFFFF | 0x00 | 0 XD=0 |
| PD [4] | 0x0000000000800000 to 0x00000000009FFFFF | 0x00 | 0 XD=0 |
| PD [5] | 0x0000000000A00000 to 0x0000000000BFFFFF | 0x00 | 0 XD=0 |
| PD [6] | 0x0000000000C00000 to 0x0000000000DFFFFF | 0x00 | 0 XD=0 |
| PD [7] | 0x0000000000E00000 to 0x0000000000FFFFFF | 0x00 | 0 XD=0 |
| PD [8] | 0x0000000001000000 to 0x00000000011FFFFF | 0x00 | 0 XD=0 |
| PD [9] | 0x0000000001200000 to 0x00000000013FFFFF | 0x00 | 0 XD=0 |
| PD [10] | 0x0000000001400000 to 0x00000000015FFFFF | 0x00 | 0 XD=0 |
| PD [11] | 0x0000000001600000 to 0x00000000017FFFFF | 0x00 | 0 XD=0 |
| PD [12] | 0x0000000001800000 to 0x00000000019FFFFF | 0x00 | 0 XD=0 |
| PD [13] | 0x0000000001A00000 to 0x0000000001BFFFFF | 0x00 | 0 XD=0 |
| PD [14] | 0x0000000001C00000 to 0x0000000001DFFFFF | 0x00 | 0 XD=0 |
| PD [15] | 0x0000000001E00000 to 0x0000000001FFFFFF | 0x00 | 0 XD=0 |
| PD [16] | 0x0000000002000000 to 0x00000000021FFFFF | 0x0000000002000000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |
| PD [17] | 0x0000000002200000 to 0x00000000023FFFFF | 0x0000000002200000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |
| PD [18] | 0x0000000002400000 to 0x00000000025FFFFF | 0x0000000002400000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |
| PD [19] | 0x0000000002600000 to 0x00000000027FFFFF | 0x0000000002600000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |
| PD [20] | 0x0000000002800000 to 0x00000000029FFFFF | 0x0000000002800000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |

Modify Page-Directory Attributes

Register Value: 0x0083 Original Value: 0x0083

Group Value: 0x01 P 0:0

Register Layout:




Page is present in memory

Description:

Page-Directory Attributes

Present Bit (P Bit)
The Present Bit indicates whether the page frame address in a page table entry maps to a page in physical memory. If the bit is set, the page is in memory.

Set Restore Close

[3][default] IP=0x0038:0x000000008D7CB172 0x0038:0x000000008D7CB172

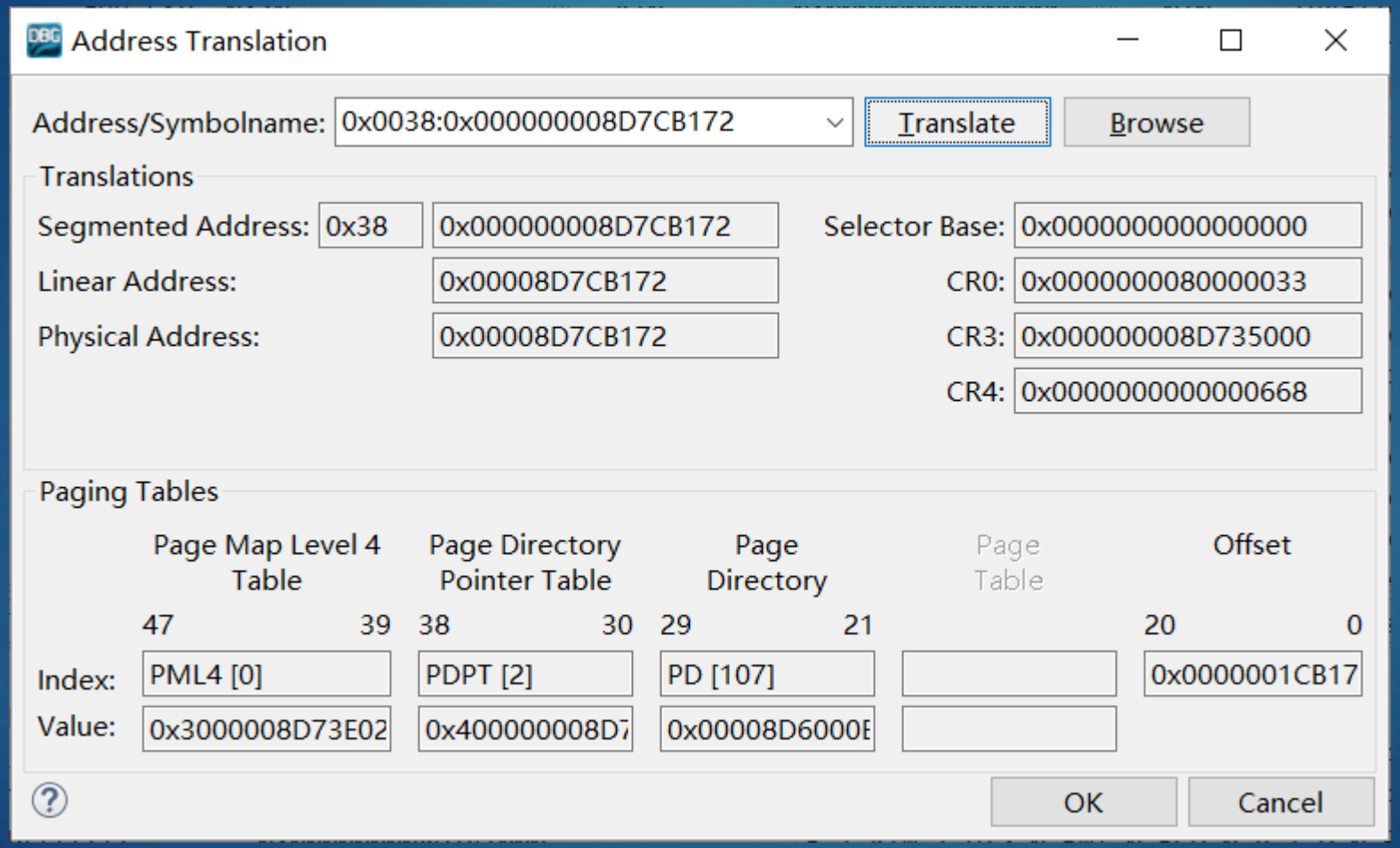
14:23 2020/7/11

# GDT

Console View | GDT: 0x000000008d734228 | Instruction Trace [PT] | Paging | Memory[1] 0x0010:0x8D7C50A2 | Hardware Threads | Breakpoints | Processor Specific F

| Index | Selector | Type | Description |
|---|---|---|---|
| 0001 | 0008 | CODE SEG | base=0x00000000 limit=0x000FFFFF (pages 0xFFFFFFFF bytes) G=4k AVL=0 P=1 DPL=0 USE32 attr=NRA |
| 0002 | 0010 | CODE SEG | base=0x00000000 limit=0x000FFFFF (pages 0xFFFFFFFF bytes) G=4k AVL=0 P=1 DPL=0 USE32 attr=NRA |
| 0003 | 0018 | DATA SEG | base=0x00000000 limit=0x000FFFFF (pages 0xFFFFFFFF bytes) G=4k AVL=0 P=1 DPL=0 attr=UWA |
| 0004 | 0020 | DATA SEG | base=0x00000000 limit=0x000FFFFF (pages 0xFFFFFFFF bytes) G=4k AVL=0 P=1 DPL=0 attr=UWA |
| 0005 | 0028 | CODE SEG | base=0x00000000 limit=0x000FFFFF (pages 0xFFFFFFFF bytes) G=4k AVL=0 P=1 DPL=0 USE16 attr=NRA |
| 0006 | 0030 | DATA SEG | base=0x00000000 limit=0x000FFFFF (pages 0xFFFFFFFF bytes) G=4k AVL=0 P=1 DPL=0 attr=UWA |
| 0007 | 0038 | CODE SEG | base=0x00000000 limit=0x000FFFFF (pages 0xFFFFFFFF bytes) G=4k AVL=0 P=1 DPL=0 64BIT attr=NRA |
| 0008+ | 0040 | BUTSS64 | base=0x000000008D734278 limit=0x00000067 bytes G=1b AVL=0 P=1 DPL=0 |

# 1:1 Paging


Address Translation
Address/Symbolname: 0x0038:0x000000008D7CB172
Translate
Browse
Translations
Segmented Address: 0x38
0x000000008D7CB172
Selector Base: 0x0000000000000000
Linear Address: 0x00008D7CB172
CR0: 0x0000000080000033
Physical Address: 0x00008D7CB172
CR3: 0x000000008D735000
CR4: 0x0000000000000668
Paging Tables
Page Map Level 4 Table
Page Directory Pointer Table
Page Directory
Page Table
Offset
47 39
38 30
29 21
20 0
Index:
PML4 [0]
PDPT [2]
PD [107]
0x0000001CB17
Value:
0x3000008D73E02
0x400000008D7
0x00008D6000E
OK
Cancel

Intel(R) System Debugger (Legacy)

File Edit View Run Debug Options Help

LoadDXEModules LoadPEIMs LoadThis

Assembler: 0x0038:0x000000008D7CB144 to 0x0038:0x000000008D7CB2A2

| Trail | Address | Opcodes | Source |
|---|---|---|---|
| | 0x0038:0x000000008D7CB144 | 8D 00 | lea eax, ptr [rax] |
| | 0x0038:0x000000008D7CB146 | 00 00 | add byte ptr [rax], al |
| | 0x0038:0x000000008D7CB148 | 00 FF | add bh, bh |
| | 0x0038:0x000000008D7CB14A | D0 48 8B | ror byte ptr [rax-0x75], 0x |
| | 0x0038:0x000000008D7CB14D | CB | ret far |
| | 0x0038:0x000000008D7CB14E | 48 B8 14 7C 7D ... | mov rax, 0x8D |
| | 0x0038:0x000000008D7CB158 | FF D0 | call rax |
| | 0x0038:0x000000008D7CB15A | 48 8B CB | mov rcx, rbx |
| | 0x0038:0x000000008D7CB15D | 48 B8 FC 8D 7D ... | mov rax, 0x8D |
| | 0x0038:0x000000008D7CB167 | FF D0 | call rax |
| | 0x0038:0x000000008D7CB169 | 48 83 C4 20 | add rsp, 0x20 |
| | 0x0038:0x000000008D7CB16D | 48 0F AE 0C 24 | fxrstor64 ptr [rsp] |
| | 0x0038:0x000000008D7CB172 | 0F AA | rsm |
| | 0x0038:0x000000008D7CB174 | 66 66 66 66 0F ... | nop word ptr [rax+rax*1], a |
| | 0x0038:0x000000008D7CB180 | F8 | clc |
| | 0x0038:0x000000008D7CB181 | 4F 7C 8D | jl 0x8D7CB111 <> |
| | 0x0038:0x000000008D7CB184 | 18 00 | sbb byte ptr [rax], al |
| | 0x0038:0x000000008D7CB186 | 00 00 | add byte ptr [rax], al |
| | 0x0038:0x000000008D7CB188 | F3 01 28 | add dword ptr [rax], ebp |
| | 0x0038:0x000000008D7CB18B | 7C DB | jl 0x8D7CB168 <> |
| | 0x0038:0x000000008D7CB18D | 22 A0 9F D2 01 FC | and ah, byte ptr [rax-0x3FE |
| | 0x0038:0x000000008D7CB193 | BC E8 62 A0 0D | mov esp, 0xDA062E8 |
| | 0x0038:0x000000008D7CB198 | 82 | DB 0x82 |
| | 0x0038:0x000000008D7CB199 | 09 7F 32 | or dword ptr [rsi+0x32], ec |

RSM

Registers

| Register | Value |
|---|---|
| RAX | 0x000000008D7D8DF |
| RBX | 0x0000000000000000 |
| RCX | 0x0000000000000000 |
| RDX | 0x000000008D74417 |
| | 0x0000000000058C4 |
| | 0x000000008D7C300 |
| | 0x000000008D7C4DF |
| | 0x00000000000581F |
| | 0x0000000000000000 |
| | 0x0000000000000000 |
| R11 | 0x000000008D74300 |
| R12 | 0x0000000000000000 |
| R13 | 0x0000000000000000 |
| R14 | 0x0000000000000000 |
| R15 | 0x0000000000000000 |
| RIP | 0x000000008D7CB17 |
| RFL | 0x0000000000001000 |
| EAX | 0x8D7D8DFC |
| EBX | 0x00000003 |
| ECX | 0x00000003 |
| EDX | 0x8D744120 |
| ESI | 0x00058C40 |
| EDI | 0x8D7C3000 |

IDT: 0x000000008d7d3280

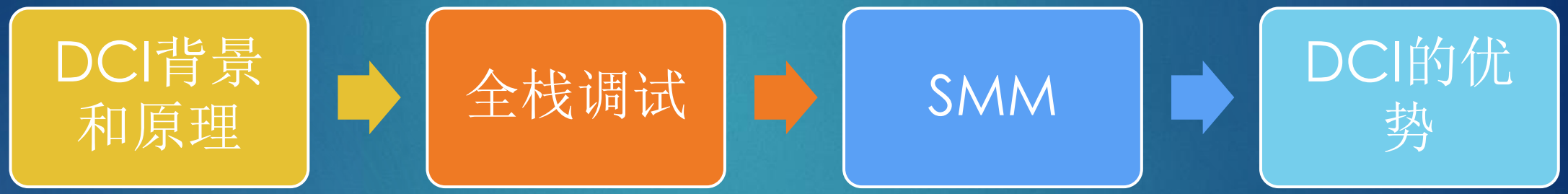
| Index | Name | Type | Description |
|---|---|---|---|
| 000 | Divide Error | IN... | sel=0x0038 off=0x000000008D7DD0B0 ti=GDT rpl=0 IST=... |
| 001 | Reserved | IN... | sel=0x0038 off=0x000000008D7DD0BF ti=GDT rpl=0 IST=... |
| 002 | NMI | IN... | sel=0x0038 off=0x000000008D7DD0CE ti=GDT rpl=0 IST=... |
| 003 | Breakpoint | IN... | sel=0x0038 off=0x000000008D7DD0DD ti=GDT rpl=0 IST=... |
| 004 | Overflow | IN... | sel=0x0038 off=0x000000008D7DD0EC ti=GDT rpl=0 IST=... |
| 005 | BOUND Range | IN... | sel=0x0038 off=0x000000008D7DD0FB ti=GDT rpl=0 IST=... |
| 006 | Invalid Op... | IN... | sel=0x0038 off=0x000000008D7DD10A ti=GDT rpl=0 IST=... |
| 007 | Device Una... | IN... | sel=0x0038 off=0x000000008D7DD119 ti=GDT rpl=0 IST=... |
| 008 | Double Fault | IN... | sel=0x0038 off=0x000000008D7DD128 ti=GDT rpl=0 IST=... |
| 009 | Reserved | IN... | sel=0x0038 off=0x000000008D7DD137 ti=GDT rpl=0 IST=... |
| 010 | Invalid TSS | IN... | sel=0x0038 off=0x000000008D7DD146 ti=GDT rpl=0 IST=... |
| 011 | Segment No... | IN... | sel=0x0038 off=0x000000008D7DD155 ti=GDT rpl=0 IST=... |
| 012 | Stack Fault | IN... | sel=0x0038 off=0x000000008D7DD164 ti=GDT rpl=0 IST=... |
| 013 | General Pr... | IN... | sel=0x0038 off=0x000000008D7DD173 ti=GDT rpl=0 IST=... |
| 014 | Page Fault | IN... | sel=0x0038 off=0x000000008D7DD182 ti=GDT rpl=0 IST=... |
| 015 | Reserved | IN... | sel=0x0038 off=0x000000008D7DD191 ti=GDT rpl=0 IST=... |
| 016 | FPU Error | IN... | sel=0x0038 off=0x000000008D7DD1A0 ti=GDT rpl=0 IST=... |
| 017 | Alignment ... | IN... | sel=0x0038 off=0x000000008D7DD1AF ti=GDT rpl=0 IST=... |
| 018 | Machine Check | IN... | sel=0x0038 off=0x000000008D7DD1BE ti=GDT rpl=0 IST=... |
| 019 | SIMD Excep... | IN... | sel=0x0038 off=0x000000008D7DD1CD ti=GDT rpl=0 IST=... |
| 020 | Reserved | IN... | sel=0x0038 off=0x000000008D7DD1DC ti=GDT rpl=0 IST=... |
| 021 | Reserved | IN... | sel=0x0038 off=0x000000008D7DD1EB ti=GDT rpl=0 IST=... |
| 022 | Reserved | IN... | sel=0x0038 off=0x000000008D7DD1FA ti=GDT rpl=0 IST=... |
| 023 | Reserved | IN... | sel=0x0038 off=0x000000008D7DD209 ti=GDT rpl=0 IST=... |
| 024 | Reserved | IN... | sel=0x0038 off=0x000000008D7DD218 ti=GDT rpl=0 IST=... |

Console View | GDT: 0x000000008d734228 | Instruction Trace [PT] | Paging | Memory[1] 0x0010:0x8D7C50A2 | Hardware Threads | Breakpoints | Processor Specific Registers | LDT from LDTR

| Index | Virtual Memory Range | Physical Base Address | Description |
|---|---|---|---|
| PD [7] | 0x0000000000E00000 to 0x0000000000FFFFFF | 0x0000000000E00000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |
| PD [8] | 0x0000000001000000 to 0x00000000011FFFFF | 0x0000000001000000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |
| PD [9] | 0x0000000001200000 to 0x00000000013FFFFF | 0x0000000001200000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |
| PD [10] | 0x0000000001400000 to 0x00000000015FFFFF | 0x0000000001400000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |
| PD [11] | 0x0000000001600000 to 0x00000000017FFFFF | 0x0000000001600000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |
| PD [12] | 0x0000000001800000 to 0x00000000019FFFFF | 0x0000000001800000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |
| PD [13] | 0x0000000001A00000 to 0x0000000001BFFFFF | 0x0000000001A00000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |
| PD [14] | 0x0000000001C00000 to 0x0000000001DFFFFF | 0x0000000001C00000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |
| PD [15] | 0x0000000001E00000 to 0x0000000001FFFFFF | 0x0000000001E00000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |
| PD [16] | 0x0000000002000000 to 0x00000000021FFFFF | 0x0000000002000000 | P=1 R/W=1 U/S=0 PWT=0 PCD=0 A=0 D=0 PS=1(2MB) G=0 PAT=0 XD=0 |

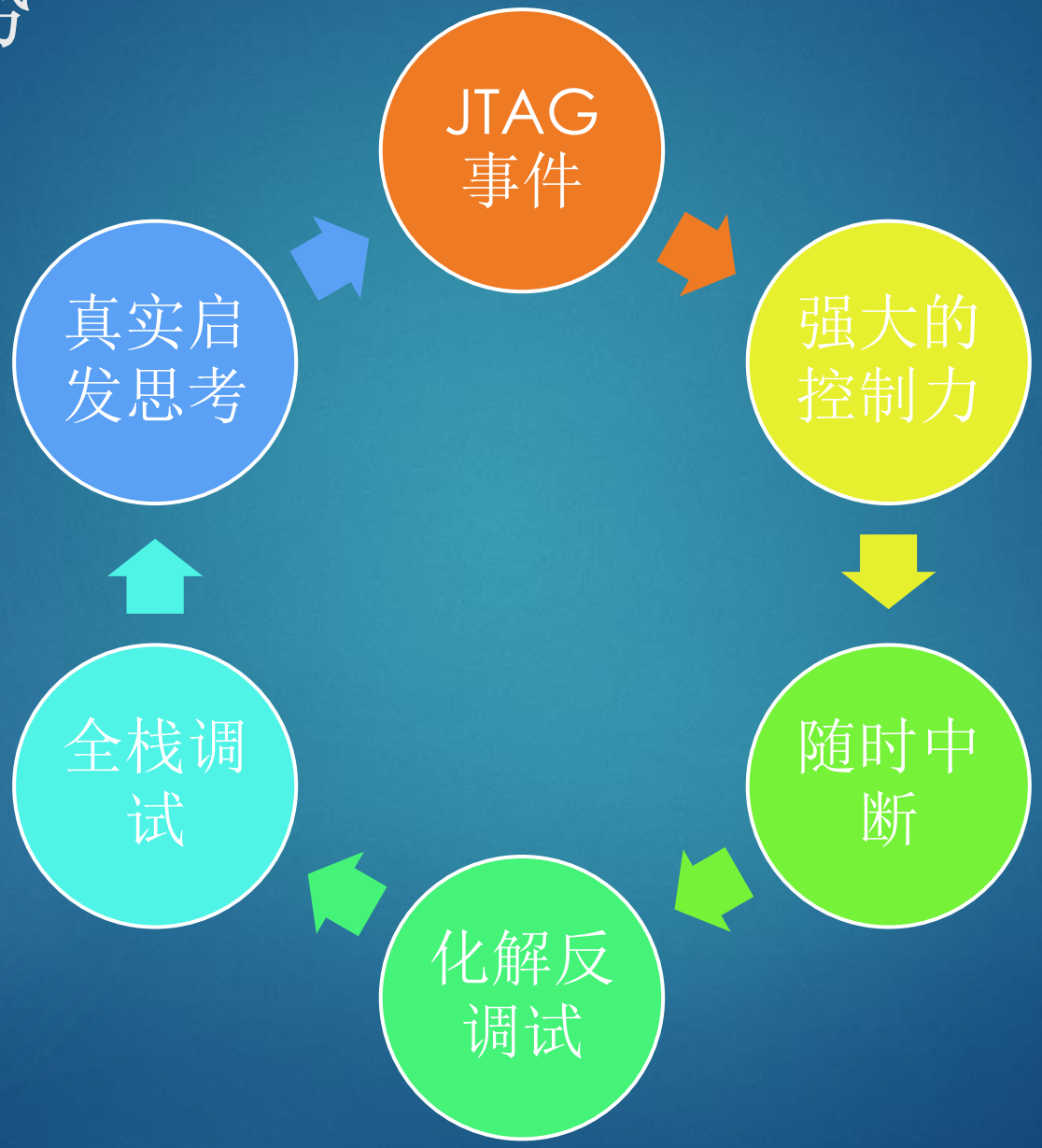
[3][default] IP=0x0038:0x000000008D7CB172 0x0038:0x000000008D7CB172

CH 拼 14:49 2020/7/11


DCI背景和原理
全栈调试
SMM
DCI的优势

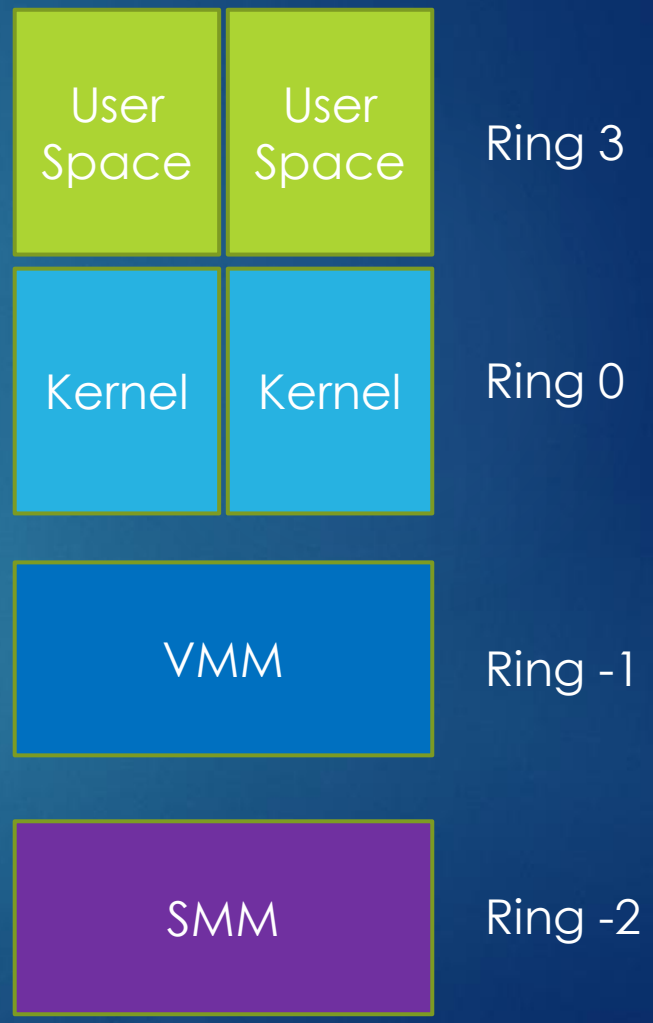
# DCI的使用场景

# DCI的优势



# 总结

- DCI技术大大降低了XDP的使用门槛
  - 价格降低，依赖减少
  - 市场上的x86系统一般不行，DCI功能默认是锁死的
- 软件的境界在于深度
  - 越是技术深处，越是魅力无穷
  - 沿着软件栈一层层探索，努力成为“全栈人才”
- 养成调试的习惯，日积月累，功到自然成
- 让一切皆可调试
  - 附加上去
  - 写一个可调试的来调试
- 一旦能够调试，便由不可控，变得可控



# 切问而近思

欢迎关注格友公众号

ffff810b`789923c8 410f23ff mov dr7,r15

JTAGEvents | disassembly.nd

```
;; start=0xffff810b789923c8 end=0xffff810b78992552
ffff810b`789923c8 410f23ff        mov     dr7,r15
ffff810b`789923cc 0f015d07        lidt    tbyte ptr [rbp+7]
ffff810b`789923d0 fb              sti
ffff810b`789923d1 8187280800002006 0000 add dword ptr [rdi+828h],620h
ffff810b`789923db 488d8f20060000  lea     rcx,[rdi+620h]
ffff810b`789923e2 8bb7c4000000    mov     esi,dword ptr [rdi+0C4h]
ffff810b`789923e8 4c8bcf          mov     r9,rdi
ffff810b`789923eb 448b9714080000  mov     r10d,dword ptr [rdi+814h]
ffff810b`789923f2 488bc7          mov     rax,rdi
ffff810b`789923f5 4c8b9f18080000  mov     r11,qword ptr [rdi+818h]
ffff810b`789923fc 41bd40000000    mov     r13d,40h
ffff810b`78992402 4489bfc4000000  mov     dword ptr [rdi+0C4h],r15d
ffff810b`78992409 483bf9          cmp     rdi,rcx
ffff810b`7899240c 730b            jae     ffff810b`78992419
ffff810b`7899240e 0f1800          prefetchnta [rax]
ffff810b`78992411 4903c5          add     rax,r13
ffff810b`78992414 483bc1          cmp     rax,rcx
ffff810b`78992417 72f5            jb      ffff810b`7899240e
ffff810b`78992419 4d8bc3          mov     r8,r11
ffff810b`7899241c bb0c000000      mov     ebx,0Ch
ffff810b`78992421 49bd0120000480001070 mov r13,7010008004002001h
ffff810b`7899242b 498bd6          mov     rdx,r14
ffff810b`7899242e 498b01          mov     rax,qword ptr [r9]
ffff810b`78992431 418bca          mov     ecx,r10d
ffff810b`78992434 4933c0          xor     rax,r8
ffff810b`78992437 4d03ce          add     r9,r14
ffff810b`7899243a 48d3c0          rol     rax,cl
ffff810b`7899243d 4d8b01          mov     r8,qword ptr [r9]
```

```
0038:00000000`8d7d9c72 488b442440      mov     rax,qword ptr [rsp+40h] ss:0020:000
00000`8d764580=0000000000000000
0038:00000000`8d7d9c77 4885c0          test    rax,rax
0038:00000000`8d7d9c7a 74f6            je      00000000`8d7d9c72
```