presented by

JTAG-based UEFI Debug and Trace

UEFI 2020 Virtual Plugfest

July 14, 2020

Presented by Alan Sguigna, ASSET InterTech, Inc.

Meet the Presenter

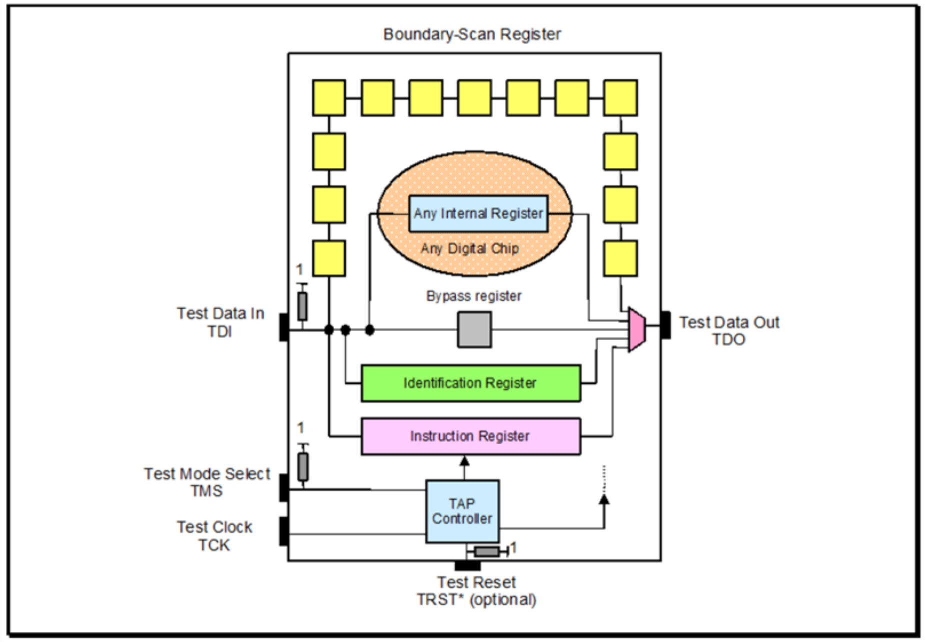
Alan Sguigna
Vice President, Sales &
Customer Service
Member Company:
ASSET InterTech, Inc.

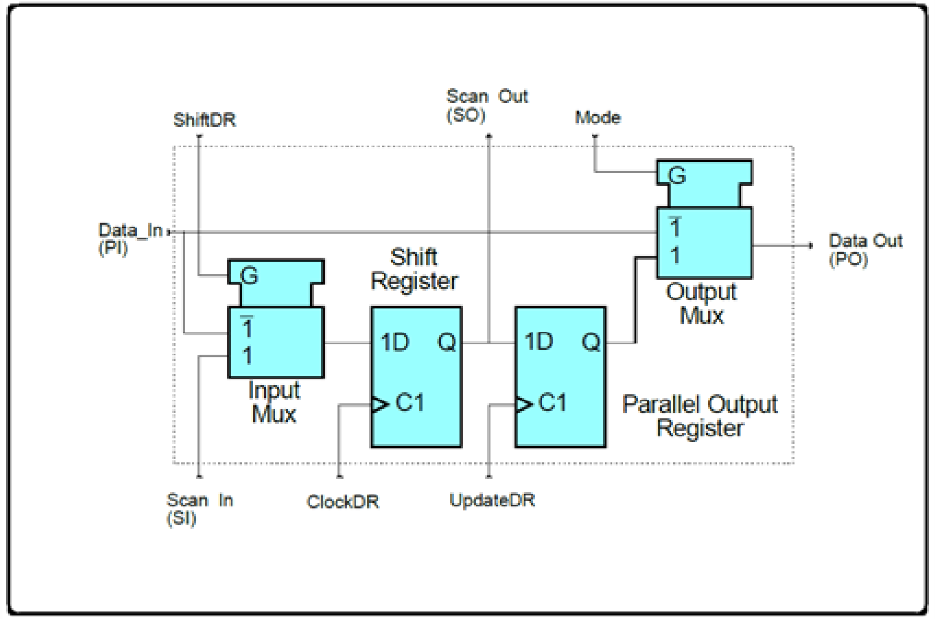
Agenda

- What is JTAG? Debug use case
- Access mechanisms (platform-dependent)
- Tools of the Trade: Run-control, Trace, scripting
- Examples/ Demo:
  - Run-control: halt, go, single-step, breakpoint
  - Trace: Last Branch Record (LBR), Branch Trace Store (BTS), Instruction Trace, Architectural Event Trace, ME trace
  - Intel CScripts
- Call to Action

What is JTAG?

- Celebrated its 30th Anniversary on February 15, 2020
- “Joint Test Access Group”
- IEEE 1149.1 and subsequent standards – ingrained within much of today’s commercial silicon
- Specifies a dedicated debug port with a serial communications interface
- Test Access Port implements a stateful protocol with test registers that connect with a chip’s system logic
- An “engine” within chips that drives embedded instrumentation for a plethora of applications





JTAG Applications

Test

Boundary-Scan Test, JTAG-based functional test

Debug

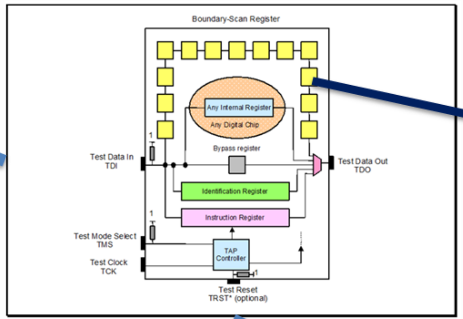
Run-control (Intel ITP, AMD HDT, Arm CoreSight)

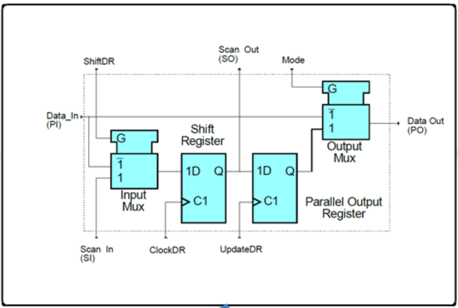
Validation

Hardware perform-ance / conform-ance

Programming

SVF, STAPL, JAM, and at-speed flash IP





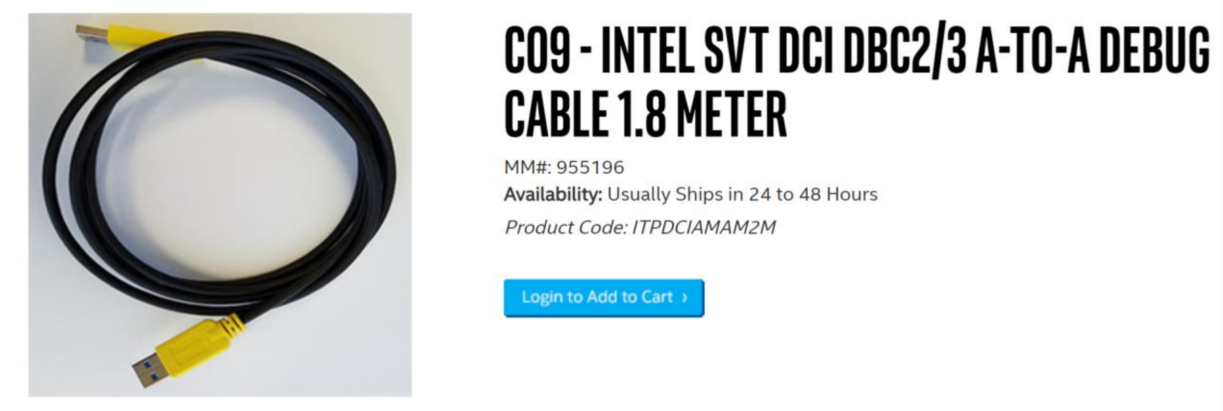
Why is JTAG Useful for Debugging?

- “Bare-metal” debugging at the interface between the hardware and the software
- Essential for debug on wedged platforms
- Use same tools as used in silicon validation

Access Mechanisms (Intel)

- XDP (eXtended Debug Port)

- DbC/ DCI (Debug Class)



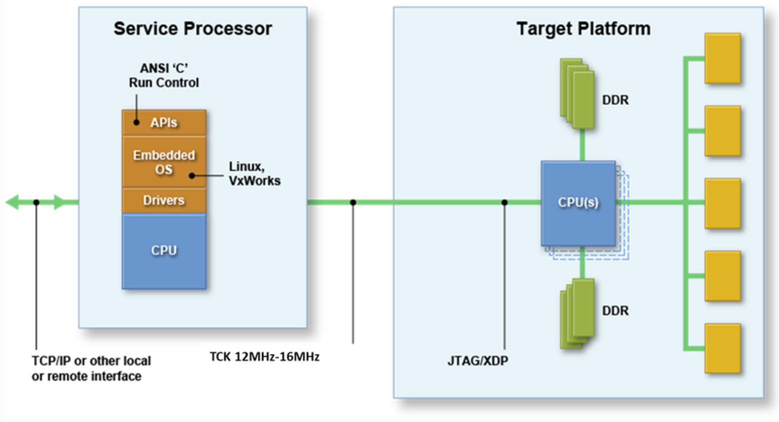
C09 - INTEL SVT DCI DBC2/3 A-TO-A DEBUG CABLE 1.8 METER

MM#: 955196

Availability: Usually Ships in 24 to 48 Hours

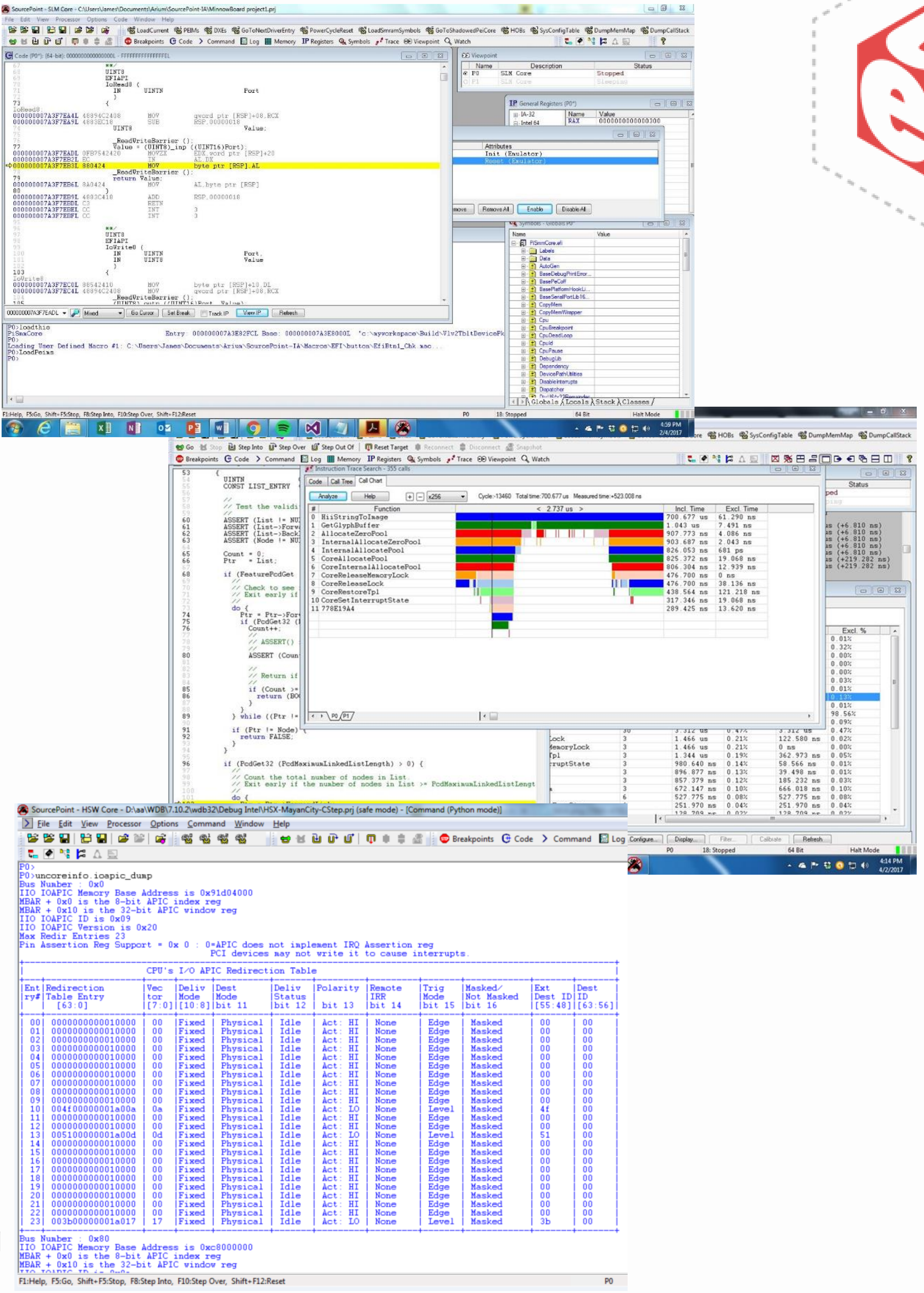
Product Code: ITPDCIAMAM2M

- BMC



Tools of the Trade

- Run-control
- Trace
- Scripting



SourcePoint - SLM Core - C:\Users\James\Documents\Arium\SourcePoint-IA\MinnowBoard project1.prj

Code (P0*): (64-bit): 0000000000000000L - FFFFFFFFFFFFFFFFL

```
                 **/
                 UINT8
                 EFIAPI
                 IoRead8 (
                   IN      UINTN                    Port
                   )
                 {
IoRead8:
000000007A3F7EA4L 48894C2408     MOV     qword ptr [RSP]+08,RCX
000000007A3F7EA9L 4883EC18       SUB     RSP,00000018
                   UINT8                            Value;

                   _ReadWriteBarrier ();
                   Value = (UINT8)_inp ((UINT16)Port);
000000007A3F7EADL 0FB7542420     MOVZX   EDX,word ptr [RSP]+20
000000007A3F7EB2L EC             IN      AL,DX
000000007A3F7EB3L 880424         MOV     byte ptr [RSP],AL
                   _ReadWriteBarrier ();
                   return Value;
000000007A3F7EB6L 8A0424         MOV     AL,byte ptr [RSP]
                 }
000000007A3F7EB9L 4883C418       ADD     RSP,00000018
000000007A3F7EBDL C3             RETN
000000007A3F7EBEL CC             INT     3
000000007A3F7EBFL CC             INT     3

                 **/
                 UINT8
                 EFIAPI
                 IoWrite8 (
                   IN      UINTN                    Port,
                   IN      UINT8                    Value
                   )
                 {
IoWrite8:
000000007A3F7EC0L 88542410       MOV     byte ptr [RSP]+10,DL
000000007A3F7EC4L 48894C2408     MOV     qword ptr [RSP]+08,RCX
```

Instruction Trace Search - 355 calls

Cycle:-13460 Total time:700.677 us Measured time:+523.008 ns

#	Function	< 2.737 us >	Incl. Time	Excl. Time
0	HiiStringToImage		700.677 us	61.290 ns
1	GetGlyphBuffer		1.043 us	7.491 ns
2	AllocateZeroPool		907.773 ns	4.086 ns
3	InternalAllocateZeroPool		903.687 ns	2.043 ns
4	InternalAllocatePool		826.053 ns	681 ps
5	CoreAllocatePool		825.372 ns	19.068 ns
6	CoreInternalAllocatePool		806.304 ns	12.939 ns
7	CoreReleaseMemoryLock		476.700 ns	0 ns
8	CoreReleaseLock		476.700 ns	38.136 ns
9	CoreRestoreTpl		438.564 ns	121.218 ns
10	CoreSetInterruptState		317.346 ns	19.068 ns
11	778E19A4		289.425 ns	13.620 ns

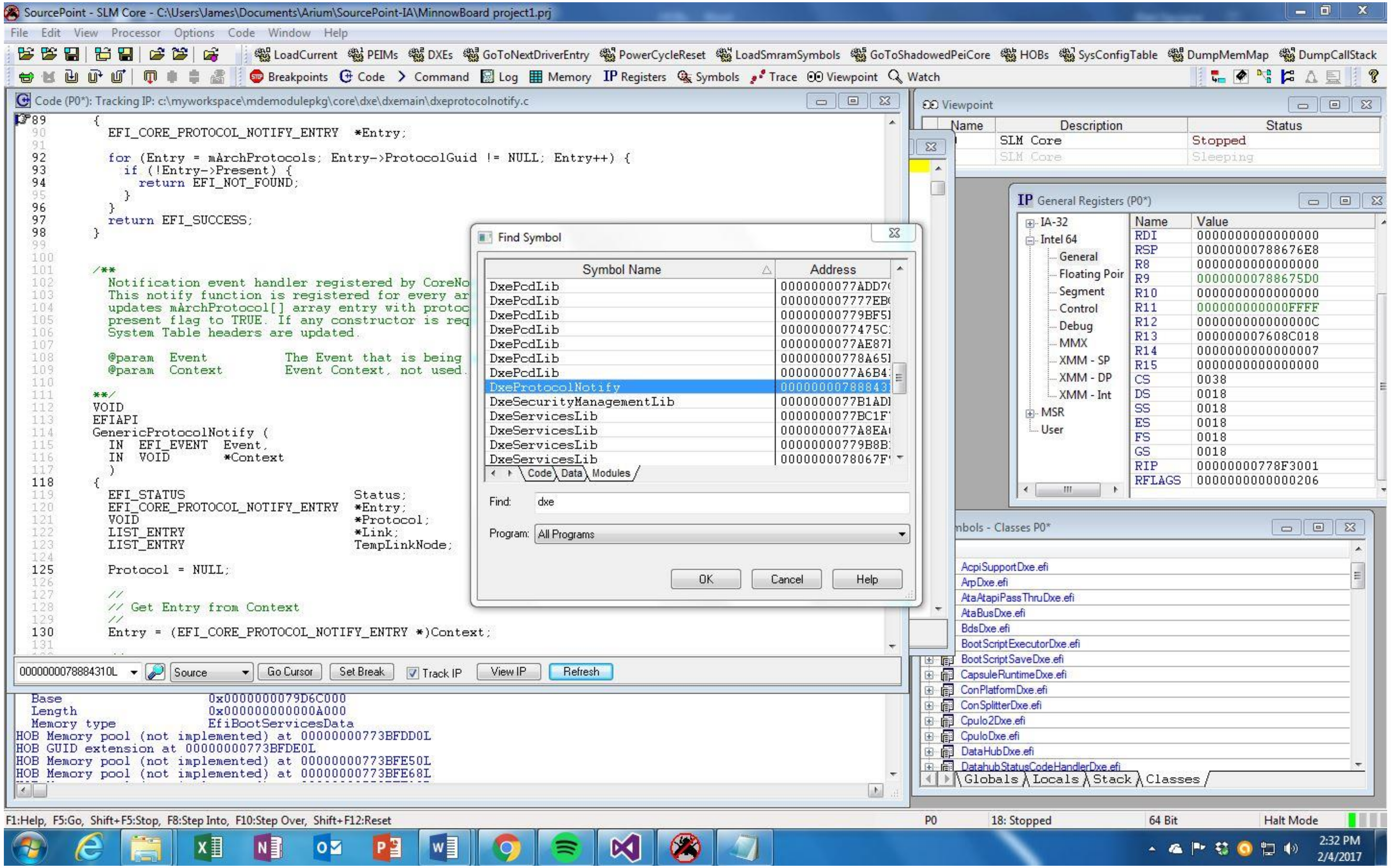
SourcePoint - HSW Core - D:\aa\WDB\7.10.2\wdb32\Debug Intel\HSX-MayanCity-CStep.prj (safe mode) - [Command (Python mode)]

```
P0>
P0>uncoreinfo.ioapic_dump
Bus Number : 0x0
IIO IOAPIC Memory Base Address is 0x91d04000
MBAR + 0x0 is the 8-bit APIC index reg
MBAR + 0x10 is the 32-bit APIC window reg
IIO IOAPIC ID is 0x09
IIO IOAPIC Version is 0x20
Max Redir Entries 23
Pin Assertion Reg Support = 0x 0 : 0=APIC does not implement IRQ Assertion reg
                                   PCI devices may not write it to cause interrupts.
+---------------------------------------------------------------------------------------------------------+
|                       CPU's I/O APIC Redirection Table                                                  |
+---+----------------+----+-----+--------+------+--------+--------+-------+------------+-------+-------+
|Ent|Redirection     |Vec |Deliv|Dest    |Deliv |Polarity|Remote  |Trig   |Masked/     |Ext    |Dest   |
|ry#|Table Entry     |tor |Mode |Mode    |Status|        |IRR     |Mode   |Not Masked  |Dest ID|ID     |
|   |  [63:0]        |[7:0]|[10:8]|bit 11 |bit 12| bit 13 |bit 14  |bit 15 |bit 16      |[55:48]|[63:56]|
+---+----------------+----+-----+--------+------+--------+--------+-------+------------+-------+-------+
| 00| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 01| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 02| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 03| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 04| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 05| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 06| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 07| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 08| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 09| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 10| 004f00000001a00a | 0a |Fixed | Physical | Idle | Act: LO | None | Level | Masked | 4f | 00 |
| 11| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 12| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 13| 005100000001a00d | 0d |Fixed | Physical | Idle | Act: LO | None | Level | Masked | 51 | 00 |
| 14| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 15| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 16| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 17| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 18| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 19| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 20| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 21| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 22| 0000000000010000 | 00 |Fixed | Physical | Idle | Act: HI | None | Edge | Masked | 00 | 00 |
| 23| 003b00000001a017 | 17 |Fixed | Physical | Idle | Act: LO | None | Level | Masked | 3b | 00 |
+---+----------------+----+-----+--------+------+--------+--------+-------+------------+-------+-------+
Bus Number : 0x80
IIO IOAPIC Memory Base Address is 0xc8000000
MBAR + 0x0 is the 8-bit APIC index reg
MBAR + 0x10 is the 32-bit APIC window reg
```

File Edit View Processor Options Code Window Help
LoadCurrent PEIMs DXEs GoToNextDriverEntry PowerCycleReset LoadSmramSymbols GoToShadowedPeiCore HOBs SysConfigTable DumpMemMap DumpCallStack
Breakpoints Code Command Log Memory IP Registers Symbols Trace Viewpoint Watch
Step Over Step Out Of Reset Target Reconnect Disconnect Snapshot
Code Call Tree Call Chart
Analyze Help x256
Globals Locals Stack Classes
P0 18: Stopped 64 Bit Halt Mode
4:59 PM 2/4/2017
File Edit View Processor Options Command Window Help
F1:Help, F5:Go, Shift+F5:Stop, F8:Step Into, F10:Step Over, Shift+F12:Reset P0

Examples

Basic Run-Control – MinnowBoard



SourcePoint - SLM Core - C:\Users\James\Documents\Arium\SourcePoint-IA\MinnowBoard project1.prj
File Edit View Processor Options Code Window Help
LoadCurrent PEIMs DXEs GoToNextDriverEntry PowerCycleReset LoadSmramSymbols GoToShadowedPeiCore HOBs SysConfigTable DumpMemMap DumpCallStack
Breakpoints Code Command Log Memory Registers Symbols Trace Viewpoint Watch

Code (P0*): Tracking IP: c:\myworkspace\mdemodulepkg\core\dxe\dxemain\dxeprotocolnotify.c

```
{
  EFI_CORE_PROTOCOL_NOTIFY_ENTRY  *Entry;

  for (Entry = mArchProtocols; Entry->ProtocolGuid != NULL; Entry++) {
    if (!Entry->Present) {
      return EFI_NOT_FOUND;
    }
  }
  return EFI_SUCCESS;
}


/**
  Notification event handler registered by CoreNo
  This notify function is registered for every ar
  updates mArchProtocol[] array entry with protoc
  present flag to TRUE. If any constructor is req
  System Table headers are updated.

  @param  Event          The Event that is being
  @param  Context        Event Context, not used.

**/
VOID
EFIAPI
GenericProtocolNotify (
  IN  EFI_EVENT  Event,
  IN  VOID       *Context
  )
{
  EFI_STATUS                      Status;
  EFI_CORE_PROTOCOL_NOTIFY_ENTRY  *Entry;
  VOID                            *Protocol;
  LIST_ENTRY                      *Link;
  LIST_ENTRY                      TempLinkNode;

  Protocol = NULL;

  //
  // Get Entry from Context
  //
  Entry = (EFI_CORE_PROTOCOL_NOTIFY_ENTRY *)Context;
```

0000000078884310L Source | Go Cursor | Set Break | ☑ Track IP | View IP | Refresh

```
  Base                    0x0000000079D6C000
  Length                  0x000000000000A000
  Memory type             EfiBootServicesData
HOB Memory pool (not implemented) at 00000000773BFDD0L
HOB GUID extension at 00000000773BFDE0L
HOB Memory pool (not implemented) at 00000000773BFE50L
HOB Memory pool (not implemented) at 00000000773BFE68L
```

Find Symbol

Symbol Name	Address
DxePcdLib	000000077ADD7(
DxePcdLib	000000007777EB(
DxePcdLib	00000000779BF5I
DxePcdLib	000000077475C:
DxePcdLib	0000000077AE87I
DxePcdLib	00000000778A65I
DxePcdLib	00000000077A6B4:
DxeProtocolNotify	000000007888431
DxeSecurityManagementLib	0000000077B1ADI
DxeServicesLib	0000000077BC1F'
DxeServicesLib	0000000077A8EA(
DxeServicesLib	00000000779B8B:
DxeServicesLib	0000000078067F'

Code | Data | Modules

Find: dxe

Program: All Programs

OK | Cancel | Help

Viewpoint

Name	Description	Status
	SLM Core	Stopped
	SLM Core	Sleeping

General Registers (P0*)

- IA-32
- Intel 64
  - General
  - Floating Poir
  - Segment
  - Control
  - Debug
  - MMX
  - XMM - SP
  - XMM - DP
  - XMM - Int
- MSR
- User

Name	Value
RDI	0000000000000000
RSP	00000000788676E8
R8	0000000000000000
R9	00000000788675D0
R10	0000000000000000
R11	000000000000FFFF
R12	000000000000000C
R13	000000007608C018
R14	0000000000000007
R15	0000000000000000
CS	0038
DS	0018
SS	0018
ES	0018
FS	0018
GS	0018
RIP	00000000778F3001
RFLAGS	0000000000000206

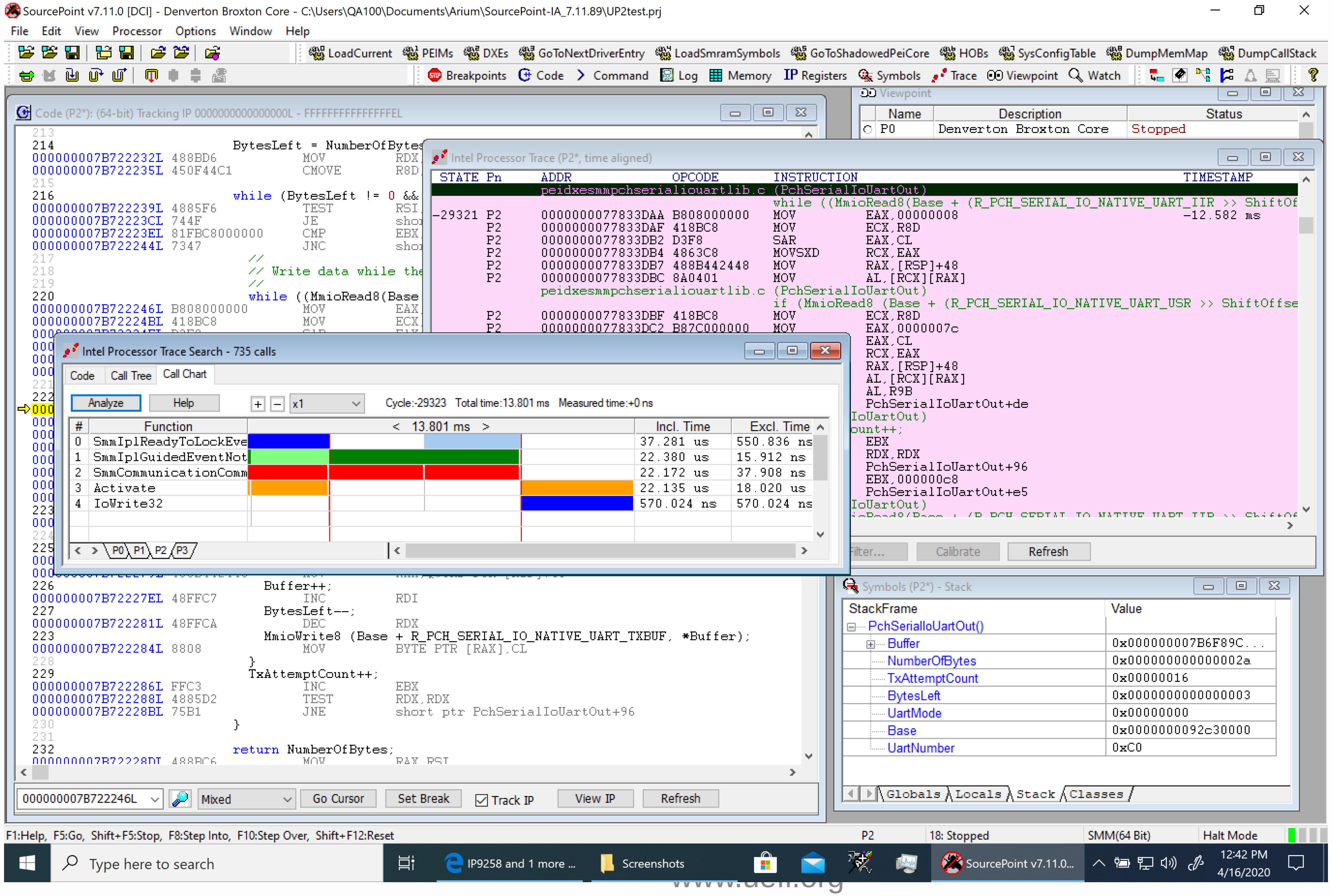
mbols - Classes P0*

- AcpiSupportDxe.efi
- ArpDxe.efi
- AtaAtapiPassThruDxe.efi
- AtaBusDxe.efi
- BdsDxe.efi
- BootScriptExecutorDxe.efi
- BootScriptSaveDxe.efi
- CapsuleRuntimeDxe.efi
- ConPlatformDxe.efi
- ConSplitterDxe.efi
- CpuIo2Dxe.efi
- CpuIoDxe.efi
- DataHubDxe.efi
- DatahubStatusCodeHandlerDxe.efi

Globals | Locals | Stack | Classes

F1:Help, F5:Go, Shift+F5:Stop, F8:Step Into, F10:Step Over, Shift+F12:Reset | P0 | 18: Stopped | 64 Bit | Halt Mode

Intel Processor Trace – Apollo Lake



SourcePoint v7.11.0 [DCI] - Denverton Broxton Core - C:\Users\QA100\Documents\Arium\SourcePoint-IA_7.11.89\UP2test.prj
File Edit View Processor Options Window Help
LoadCurrent PEIMs DXEs GoToNextDriverEntry LoadSmramSymbols GoToShadowedPeiCore HOBs SysConfigTable DumpMemMap DumpCallStack
Breakpoints Code Command Log Memory IP Registers Symbols Trace Viewpoint Watch

Code (P2*): (64-bit) Tracking IP 0000000000000000L - FFFFFFFFFFFFFFFEL

```
213
214                              BytesLeft = NumberOfBytes
000000007B72232L 488BD6            MOV          RDX
000000007B722235L 450F44C1         CMOVE        R8D
215
216                              while (BytesLeft != 0 &&
000000007B722239L 4885F6           TEST         RSI
000000007B72223CL 744F             JE           shor
000000007B72223EL 81FBC8000000     CMP          EBX
000000007B722244L 7347             JNC          shor
217                                //
218                                // Write data while the
219                                //
220                                while ((MmioRead8(Base
000000007B722246L B808000000       MOV          EAX
000000007B72224BL 418BC8           MOV          ECX
...
226                                  Buffer++;
000000007B72227EL 48FFC7           INC          RDI
227                                  BytesLeft--;
000000007B722281L 48FFCA           DEC          RDX
223                                  MmioWrite8 (Base + R_PCH_SERIAL_IO_NATIVE_UART_TXBUF, *Buffer);
000000007B722284L 8808             MOV          BYTE PTR [RAX],CL
228                                }
229                                TxAttemptCount++;
000000007B722286L FFC3             INC          EBX
000000007B722288L 4885D2           TEST         RDX,RDX
000000007B72228BL 75B1             JNE          short ptr PchSerialIoUartOut+96
230                              }
231
232                              return NumberOfBytes;
000000007B72228DL 488BC6           MOV          RAX,RSI
```

000000007B722246L | Mixed | Go Cursor | Set Break | ☑ Track IP | View IP | Refresh

Viewpoint

Name	Description	Status
○ P0	Denverton Broxton Core	Stopped

Intel Processor Trace (P2*, time aligned)

```
STATE  Pn     ADDR              OPCODE       INSTRUCTION                                               TIMESTAMP
              peidxesmmpchserialiouartlib.c  (PchSerialIoUartOut)
                                             while ((MmioRead8(Base + (R_PCH_SERIAL_IO_NATIVE_UART_IIR >> ShiftOf
-29321 P2     0000000077833DAA  B808000000   MOV       EAX,00000008                                   -12.582 ms
       P2     0000000077833DAF  418BC8       MOV       ECX,R8D
       P2     0000000077833DB2  D3F8         SAR       EAX,CL
       P2     0000000077833DB4  4863C8       MOVSXD    RCX,EAX
       P2     0000000077833DB7  488B442448   MOV       RAX,[RSP]+48
       P2     0000000077833DBC  8A0401       MOV       AL,[RCX][RAX]
              peidxesmmpchserialiouartlib.c  (PchSerialIoUartOut)
                                             if (MmioRead8 (Base + (R_PCH_SERIAL_IO_NATIVE_UART_USR >> ShiftOffse
       P2     0000000077833DBF  418BC8       MOV       ECX,R8D
       P2     0000000077833DC2  B87C000000   MOV       EAX,0000007c
                                                       EAX,CL
                                                       RCX,EAX
                                                       RAX,[RSP]+48
                                                       AL,[RCX][RAX]
                                                       AL,R9B
                                                       PchSerialIoUartOut+de
                                             IoUartOut)
                                             ount++;
                                                       EBX
                                                       RDX,RDX
                                                       PchSerialIoUartOut+96
                                                       EBX,000000c8
                                                       PchSerialIoUartOut+e5
                                             IoUartOut)
```

Filter... | Calibrate | Refresh

Intel Processor Trace Search - 735 calls

Code | Call Tree | Call Chart

Analyze | Help | + | − | x1 | Cycle:-29323 Total time:13.801 ms Measured time:+0 ns

#	Function	< 13.801 ms >	Incl. Time	Excl. Time
0	SmmIplReadyToLockEve		37.281 us	550.836 ns
1	SmmIplGuidedEventNot		22.380 us	15.912 ns
2	SmmCommunicationComm		22.172 us	37.908 ns
3	Activate		22.135 us	18.020 us
4	IoWrite32		570.024 ns	570.024 ns

P0 P1 P2 P3

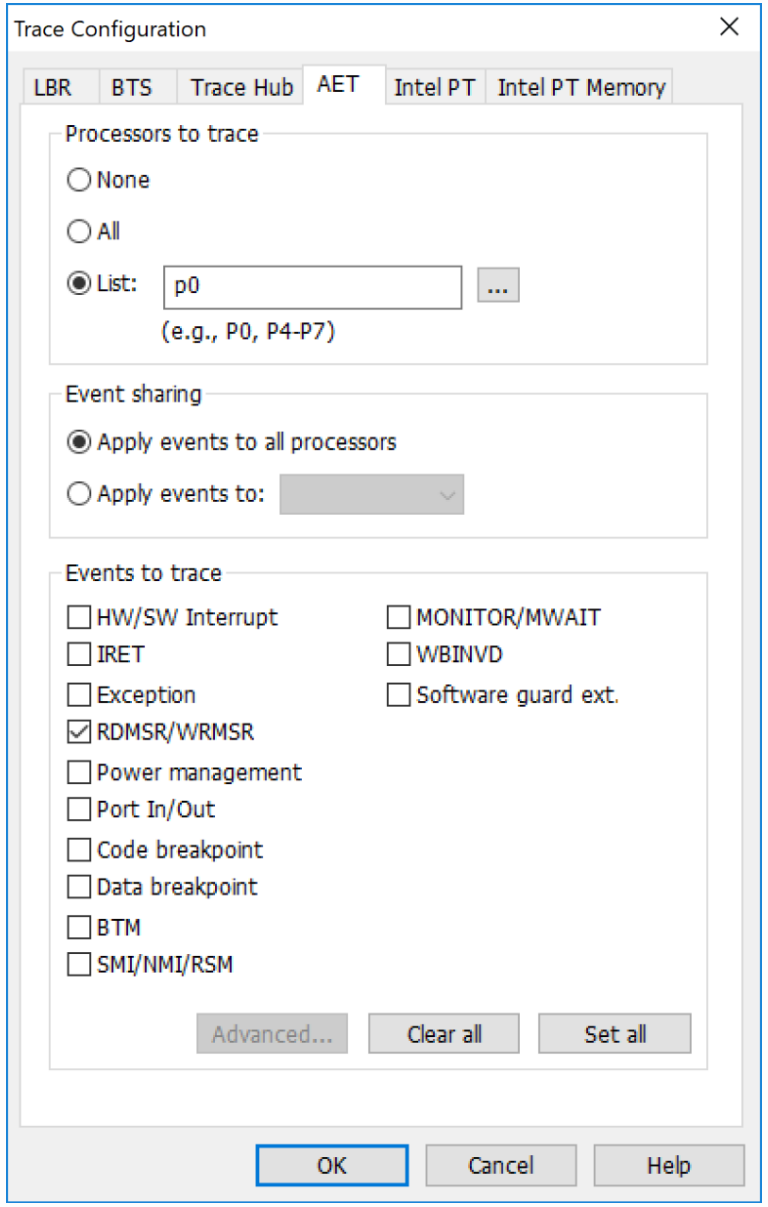
Symbols (P2*) - Stack

StackFrame	Value
PchSerialIoUartOut()	
Buffer	0x000000007B6F89C...
NumberOfBytes	0x000000000000002a
TxAttemptCount	0x00000016
BytesLeft	0x0000000000000003
UartMode	0x00000000
Base	0x0000000092c30000
UartNumber	0xC0

Globals | Locals | Stack | Classes

F1:Help, F5:Go, Shift+F5:Stop, F8:Step Into, F10:Step Over, Shift+F12:Reset | P2 | 18: Stopped | SMM(64 Bit) | Halt Mode

Intel AET – Skylake-SP



Trace Configuration

Processors to trace

○ None

○ All

● List: p0

(e.g., P0, P4-P7)

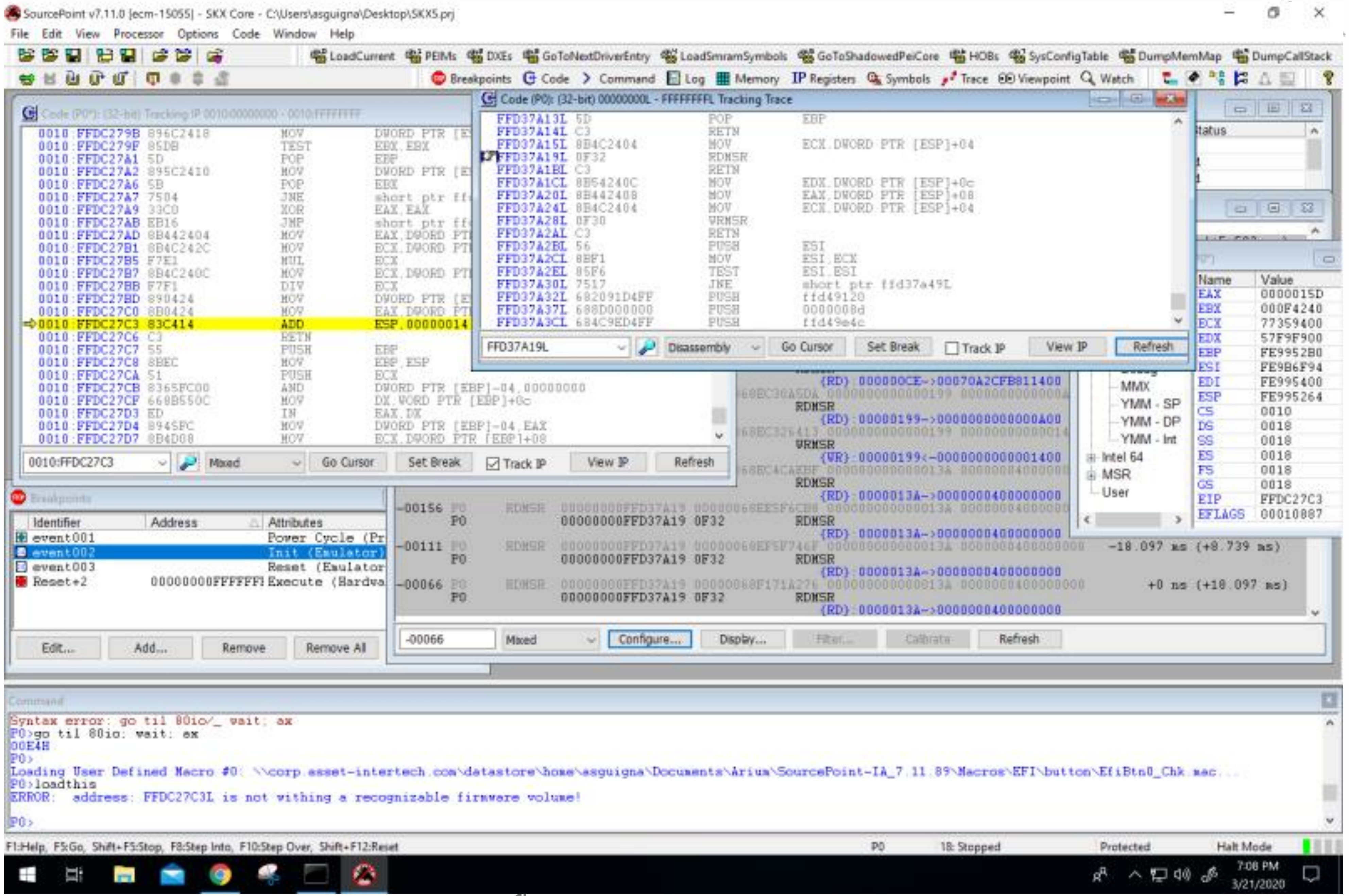
Event sharing

● Apply events to all processors

○ Apply events to:

Events to trace

- ☐ HW/SW Interrupt
- ☐ IRET
- ☐ Exception
- ☑ RDMSR/WRMSR
- ☐ Power management
- ☐ Port In/Out
- ☐ Code breakpoint
- ☐ Data breakpoint
- ☐ BTM
- ☐ SMI/NMI/RSM
- ☐ MONITOR/MWAIT
- ☐ WBINVD
- ☐ Software guard ext.



SourcePoint v7.11.0 [ecm-15055] - SKX Core - C:\Users\asguigna\Desktop\SKX5.prj

Code (P0*): (32-bit) Tracking IP 0010:00000000 - 0010:FFFFFFFF

```
0010:FFDC279B 896C2418   MOV    DWORD PTR [E
0010:FFDC279F 85DB       TEST   EBX,EBX
0010:FFDC27A1 5D         POP    EBP
0010:FFDC27A2 895C2410   MOV    DWORD PTR [E
0010:FFDC27A6 5B         POP    EBX
0010:FFDC27A7 7504       JNE    short ptr ff
0010:FFDC27A9 33C0       XOR    EAX,EAX
0010:FFDC27AB EB16       JMP    short ptr ff
0010:FFDC27AD 8B442404   MOV    EAX,DWORD PT
0010:FFDC27B1 8B4C242C   MOV    ECX,DWORD PT
0010:FFDC27B5 F7E1       MUL    ECX
0010:FFDC27B7 8B4C240C   MOV    ECX,DWORD PT
0010:FFDC27BB F7F1       DIV    ECX
0010:FFDC27BD 890424     MOV    DWORD PTR [E
0010:FFDC27C0 8B0424     MOV    EAX,DWORD PT
0010:FFDC27C3 83C414     ADD    ESP,00000014
0010:FFDC27C6 C3         RETN
0010:FFDC27C7 55         PUSH   EBP
0010:FFDC27C8 8BEC       MOV    EBP,ESP
0010:FFDC27CA 51         PUSH   ECX
0010:FFDC27CB 8365FC00   AND    DWORD PTR [EBP]-04,00000000
0010:FFDC27CF 668B550C   MOV    DX,WORD PTR [EBP]+0c
0010:FFDC27D3 ED         IN     EAX,DX
0010:FFDC27D4 8945FC     MOV    DWORD PTR [EBP]-04,EAX
0010:FFDC27D7 8B4D08     MOV    ECX,DWORD PTR [EBP]+08
```

0010:FFDC27C3 | Mixed | Go Cursor | Set Break | ☑ Track IP | View IP | Refresh

Code (P0): (32-bit) 0000000L - FFFFFFFFL Tracking Trace

```
FFD37A13L 5D         POP    EBP
FFD37A14L C3         RETN
FFD37A15L 8B4C2404   MOV    ECX,DWORD PTR [ESP]+04
FFD37A19L 0F32       RDMSR
FFD37A1BL C3         RETN
FFD37A1CL 8B54240C   MOV    EDX,DWORD PTR [ESP]+0c
FFD37A20L 8B442408   MOV    EAX,DWORD PTR [ESP]+08
FFD37A24L 8B4C2404   MOV    ECX,DWORD PTR [ESP]+04
FFD37A28L 0F30       WRMSR
FFD37A2AL C3         RETN
FFD37A2BL 56         PUSH   ESI
FFD37A2CL 8BF1       MOV    ESI,ECX
FFD37A2EL 85F6       TEST   ESI,ESI
FFD37A30L 7517       JNE    short ptr ffd37a49L
FFD37A32L 682091D4FF PUSH   ffd49120
FFD37A37L 688D000000 PUSH   0000008d
FFD37A3CL 684C9ED4FF PUSH   ffd49e4c
```

FFD37A19L | Disassembly | Go Cursor | Set Break | ☐ Track IP | View IP | Refresh

Breakpoints

Identifier	Address	Attributes
event001		Power Cycle (Pr
event002		Init (Emulator)
event003		Reset (Emulator
Reset+2	00000000FFFFFFF(	Execute (Hardwa

```
                                       {RD} 000000CE->00070A2CFB811400
                  68EC30A5DA 0000000000000199 000000000000A
                                  RDMSR
                                       {RD} 00000199->0000000000000A00
                  68EC326413 0000000000000199 00000000000014
                                  WRMSR
                                       {WR} 00000199<-0000000000001400
                  68EC4CAEBF 000000000000013A 00000004000000
                                  RDMSR
                                       {RD} 0000013A->0000000400000000
-00156 P0   RDMSR 00000000FFD37A19 00000068EE5F6CB8 000000000000013A 000000040000000
       P0         00000000FFD37A19 0F32       RDMSR
                                       {RD} 0000013A->0000000400000000
-00111 P0   RDMSR 00000000FFD37A19 00000068EF5F746F 000000000000013A 0000000400000000   -18.097 ms (+8.739 ms)
       P0         00000000FFD37A19 0F32       RDMSR
                                       {RD} 0000013A->0000000400000000
-00066 P0   RDMSR 00000000FFD37A19 00000068F171A276 000000000000013A 0000000400000000   +0 ns (+18.097 ms)
       P0         00000000FFD37A19 0F32       RDMSR
                                       {RD} 0000013A->0000000400000000
```

-00066 | Mixed | Configure... | Display... | Filter... | Calibrate | Refresh

Name	Value
EAX	0000015D
EBX	000F4240
ECX	77359400
EDX	57F9F900
EBP	FE9952B0
ESI	FE9B6F94
EDI	FE995400
ESP	FE995264
CS	0010
DS	0018
SS	0018
ES	0018
FS	0018
GS	0018
EIP	FFDC27C3
EFLAGS	00010887

Command

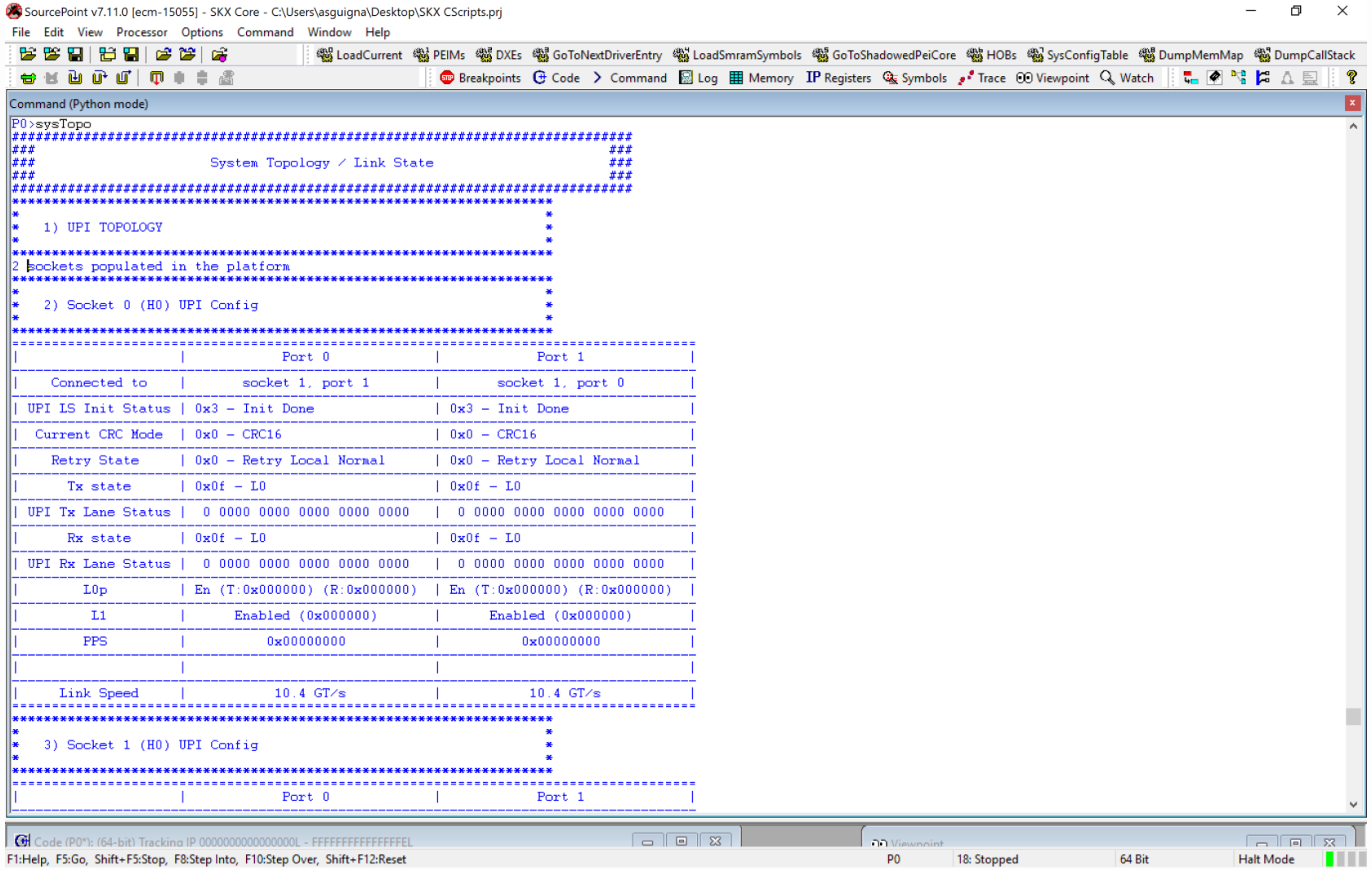
```
Syntax error: go til 80io/_ wait; ax
P0>go til 80io; wait; ex
00E4H
P0>
Loading User Defined Macro #0: \\corp.asset-intertech.com\datastore\home\asguigna\Documents\Arium\SourcePoint-IA_7.11.89\Macros\EFI\button\EfiBtn0_Chk.mac...
P0>loadthis
ERROR:  address: FFDC27C3L is not withing a recognizable firmware volume!

P0>
```

F1:Help, F5:Go, Shift+F5:Stop, F8:Step Into, F10:Step Over, Shift+F12:Reset   P0   18: Stopped   Protected   Halt Mode

7:08 PM
3/21/2020

CScripts – Skylake-SP

bkc	Best Known Configuration checker
coreinfo	Processor Core Information
edk2	UEFI Development Kit 2
ei	Error Injection
error	System Errors
mc	Memory Controller
pch	Platform Control Hub
pci	Peripheral Component Interconnect
pcie	Peripheral Component Interconnect (PCIe) base class
pm	Power Management
ras	Reliability, Availability, Serviceability
skx	Model Specific Registers (MSR)
uncoreinfo	SKX uncore implementation
upi	UPI module implementation


SourcePoint v7.11.0 [ecm-15055] - SKX Core - C:\Users\asguigna\Desktop\SKX CScripts.prj
File Edit View Processor Options Command Window Help
LoadCurrent PEIMs DXEs GoToNextDriverEntry LoadSmramSymbols GoToShadowedPeiCore HOBs SysConfigTable DumpMemMap DumpCallStack
Breakpoints Code Command Log Memory Registers Symbols Trace Viewpoint Watch
Command (Python mode)
Code (P0*): (64-bit) Tracking IP 0000000000000000L - FFFFFFFFFFFFFFFEL
Viewpoint
F1:Help, F5:Go, Shift+F5:Stop, F8:Step Into, F10:Step Over, Shift+F12:Reset
P0
18: Stopped
64 Bit
Halt Mode

```
P0>sysTopo
##############################################################################
###                                                                        ###
###                      System Topology / Link State                      ###
###                                                                        ###
##############################################################################
********************************************************************
*                                                                  *
*   1) UPI TOPOLOGY                                                *
*                                                                  *
********************************************************************
2 sockets populated in the platform
********************************************************************
*                                                                  *
*   2) Socket 0 (H0) UPI Config                                    *
*                                                                  *
********************************************************************
=====================================================================================
|                    |             Port 0              |             Port 1              |
-------------------------------------------------------------------------------------
|    Connected to    |          socket 1, port 1       |          socket 1, port 0       |
-------------------------------------------------------------------------------------
| UPI LS Init Status | 0x3 - Init Done                 | 0x3 - Init Done                 |
-------------------------------------------------------------------------------------
|  Current CRC Mode  | 0x0 - CRC16                     | 0x0 - CRC16                     |
-------------------------------------------------------------------------------------
|    Retry State     | 0x0 - Retry Local Normal        | 0x0 - Retry Local Normal        |
-------------------------------------------------------------------------------------
|      Tx state      | 0x0f - L0                       | 0x0f - L0                       |
-------------------------------------------------------------------------------------
| UPI Tx Lane Status |  0 0000 0000 0000 0000 0000     |  0 0000 0000 0000 0000 0000     |
-------------------------------------------------------------------------------------
|      Rx state      | 0x0f - L0                       | 0x0f - L0                       |
-------------------------------------------------------------------------------------
| UPI Rx Lane Status |  0 0000 0000 0000 0000 0000     |  0 0000 0000 0000 0000 0000     |
-------------------------------------------------------------------------------------
|        L0p         | En (T:0x000000) (R:0x000000)    | En (T:0x000000) (R:0x000000)    |
-------------------------------------------------------------------------------------
|         L1         |      Enabled (0x000000)         |      Enabled (0x000000)         |
-------------------------------------------------------------------------------------
|        PPS         |          0x00000000             |          0x00000000             |
-------------------------------------------------------------------------------------
|                    |                                 |                                 |
-------------------------------------------------------------------------------------
|     Link Speed     |           10.4 GT/s             |           10.4 GT/s             |
=====================================================================================
********************************************************************
*                                                                  *
*   3) Socket 1 (H0) UPI Config                                    *
*                                                                  *
********************************************************************
=====================================================================================
|                    |             Port 0              |             Port 1              |
-------------------------------------------------------------------------------------
```

Call to Action

- Take advantage of open source learning/ development opportunities
  - The MinnowBoard Chronicles
  - Debugging Intel Firmware using DCI & USB 3.0
  - Intel Firmware site

Questions?

Thanks for attending the UEFI 2020 Virtual Plugfest

For more information on UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by ASSET™