Real Insight from Code to Silicon

SourcePoint™  ScanWorks®

DCI debug of UEFI and Hypervisor technologies on the AAEON UP Whiskey Lake and Tiger Lake boards

x86 low-level debug for everyone

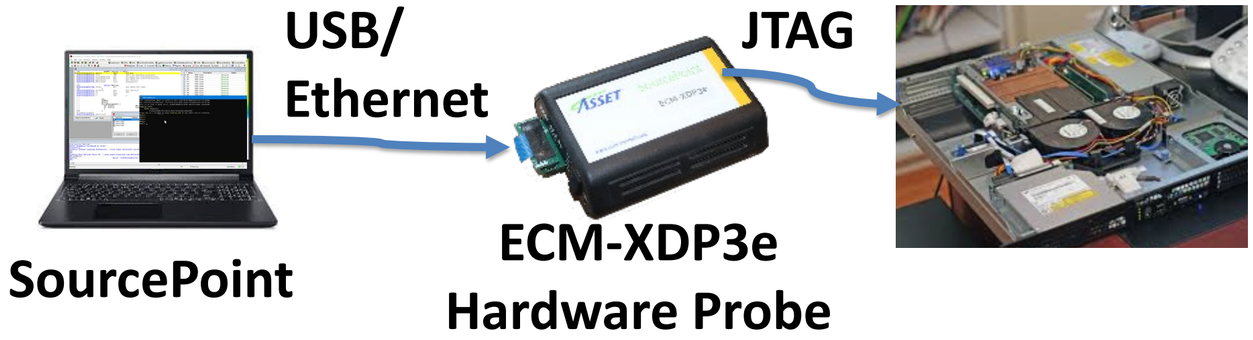
April 28, 2022

Agenda

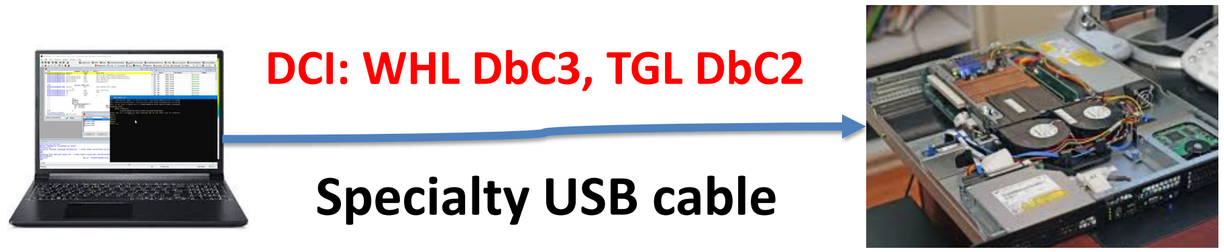
- Introduction
- SourcePoint and DCI Debug
- Whiskey Lake versus Tiger Lake
- Live demos on AAEON UP boards:
  - **UEFI** (Whiskey Lake): run-control, breakpoints, source/symbols, command language, trace, etc.
  - **Hypervisor** (Tiger Lake): Satoshi Tanda's hypervisor (MiniVisor) – VMM debug
- References/documentation
- Special offer!
- Online Q&A with ASSET Team after webinar: https://bit.ly/3K8Aseb

SourcePoint

- A very powerful JTAG-based debugger
- Optimized for UEFI and ***hypervisor*** debug
- Learning curve – lots of features



On AAEON Whiskey Lake (WHL) and Tiger Lake (TGL) boards:



SourcePoint™
Platform for Software Debug and Trace

ScanWorks®
Platform for Embedded Instruments

Whiskey Lake versus Tiger Lake

Attribute	Whiskey Lake (UP Xtreme)	Tiger Lake (UP Xtreme i11)
CPU Generation	8th	11th
DCI	DbC3	DbC2
Stability	So-so, but usable	Really good
Debug thru reset/power cycle	No (use reset vector deadloop)*	Yes
Breakpoints	Same (all)	Same (all)
Intel Processor Trace to system memory	Yes	Yes
AET to system memory	Yes	Yes
AET streaming trace to DCI USB	No	Yes
Trace Hub to system memory	Yes	Yes
Trace Hub streaming trace to DCI USB	No	Yes
Tianocore Source Code?	Yes (Aug 2021 tag)	No*
Serial console output	Yes	No*
Boot to UEFI shell	No*	Yes

***As of 4/28/2022**

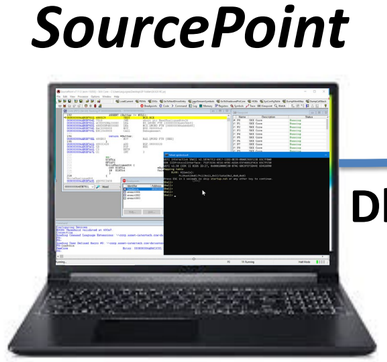
Getting Started

You'll need:

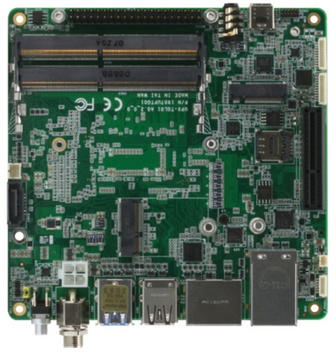
- **SourcePoint Home** license: https://www.asset-intertech.com/products/sourcepoint/sourcepoint-intel/limited-time-offer/
- AAEON UP Xtreme Celeron board (Whiskey Lake): https://up-shop.org/boards-modules/boards-modules.html
- Specialty Type-A/A DCI USB cables (no VBUS) available from DataPro, part #ITPDCIAMAM1M
- DediProg SF600
- Custom programming cable for AAEON 2x6 SPI header
- (Optional) Cable for serial out: EP-CBUSB10PFL01: www.up-shop.org/usb-2.0-pin-header-cable.html

Follow the directions here: https://www.asset-intertech.com/resources/blog/2022/03/jtag-debug-using-dci-on-the-aaeon-whiskey-lake-board/

AAEON UP Xtreme (Celeron) Whiskey Lake board



DbC2/3 Specialty USB cable



AAEON UP Xtreme i11 (i3) Tiger Lake board – version 0000

SourcePoint™ Platform for Software Debug and Trace

ScanWorks® Platform for Embedded Instruments

Demo

UEFI: Whiskey Lake

MinPlatform open-source

Full source-level and symbolic debugging using JTAG

Hypervisor: Tiger Lake

Satoshi Tanda's MiniVisor

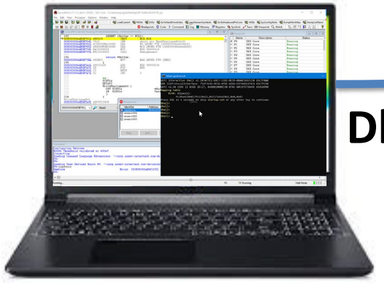
With handling of Init, (SIPI), switching the guest paging mode between 32 and 64bit modes with CR0 and EFER, access to a control register, EPT violation, misconfigured EPT entry, execution of the XSETBV instruction, execution of the CPUID instruction, etc.

Part of Training Course: https://tandasat.github.io/Hypervisor_Development_on_Intel_and_UEFI_Platform.html

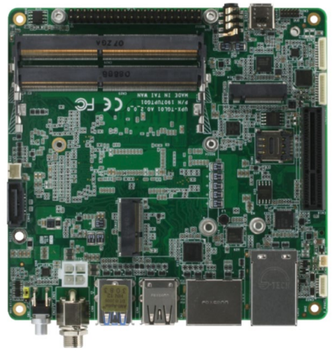
Sign up to REcon, May 30th: Hypervisor Development for Security Analysis: https://tickets.recon.cx/recon/2022/

AAEON UP Xtreme (Celeron) Whiskey Lake board

SourcePoint



DbC2/3 Specialty USB cable



AAEON UP Xtreme i11 (i3) Tiger Lake board – version 0000

Recap

- UEFI demo on AAEON Whiskey Lake board
  - Open-source MinPlatform Tianocore
  - UEFI learning, development, debug
- Hypervisor demo on AAEON Tiger Lake board
  - Open or closed-source hypervisors: MiniVisor, Bareflank, ACRN, Hyper-V, VBS, etc.
  - HV learning, cybersecurity research

Good Resources

- Tianocore new college course: https://github.com/tianocore-training/Presentation_FW using AAEON UP Xtreme Whiskey Lake board with MinPlatform UEFI
  Intel is committed to inspiring university students to work as firmware engineers in the PC industry, by directly providing hardware/firmware and course material on Intel architecture. Any academic universities interested in providing similar project and course work in the USA should submit a request to Intel academia.
- Satoshi Tanda's courses
- SourcePoint Academy: https://www.asset-intertech.com/sourcepoint-academy/
- Webinar recording with UEFI Forum: JTAG debugging with Intel Architectural Event Trace: https://www.youtube.com/watch?v=pHSvcO0ogdc

Special Offer!

- One-year subscription for SourcePoint Home license for $199 (vs. regular price $365)
- Email ai-info@asset-intertech.com with promo code ***BourbonBengal*** in Subject. Follow instructions at https://www.asset-intertech.com/products/sourcepoint/sourcepoint-intel/limited-time-offer/
- Offer valid for orders placed within two weeks of today

Wrap-Up

Questions?

Reach me at alan.sguigna@asset-intertech.com,
DM @AlanSguigna

Q&A on Teams: https://bit.ly/3K8Aseb

Real Insight from Code to Silicon

SourcePoint™
Platform for Software Debug and Trace

ScanWorks®
Platform for Embedded Instruments