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

*As of 4/28/2022
You’ll need:

- **SourcePoint Home** license: [https://www.asset-intertech.com/products/sourcepoint/sourcepoint-intel/limited-time-offer/](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](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

Follow the directions here: [https://www.asset-intertech.com/resources/blog/2022/03/jtag-debug-using-dci-on-the-aaeon-whiskey-lake-board/](https://www.asset-intertech.com/resources/blog/2022/03/jtag-debug-using-dci-on-the-aaeon-whiskey-lake-board/)
**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/
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
Tianocore new college course: [https://github.com/tianocore-training/Presentation_FW](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/](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](https://www.youtube.com/watch?v=pHSvcO0ogdc)
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
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

© 2022, ASSET InterTech, Inc.