**# Title**:

Add verbose option to dmem command in the UEFI Shell

**# Status:**

Draft

**# Document**:

UEFI Shell Specification 2.2+

**# License**:

SPDX-License-Identifier: CC-BY-4.0

**# Submitter**:

Arm (Stuart Yoder)

Arm (Sam Kaynor)

**# Summary of the change**

When the dmem command is run in the UEFI Shell without any arguments it displays the name and address of EFI system table entries.

The proposal is to add a -verbose argument to the dmem command which will parse and provide a human readable display of the RT\_PROPERTIES, CONFORMANCE\_PROFILE, and IMAGE\_ EXECUTION\_INFO tables if they are present.

**# Benefits of the change**

The human readable display of these tables helps in debugging and evaluation of firmware.

RT\_PROPERTIES table: There are a variety of implementations of UEFI, including U-boot with EFI support. It is useful to quickly see what RT properties the firmware is advertising.

CONFORMANCE\_PROFILE table: It is useful to someone evaluating UEFI firmware to see what conformance to pre-defined profiles is advertised by the firmware.

IMAGE\_ EXECUTION\_INFO table: If AuditMode=0 the table contains a list of images that failed secure boot validation. Displaying this information is useful to someone debugging.

**# References**

<https://bugzilla.tianocore.org/show_bug.cgi?id=4352>

**# Impact of the change**

This is simply an optional extension to the existing dmem command and implementation changes are isolated to the dmem implementation.

**# Detailed description of the change [normative updates]**

GREEN add, RED DELETE, YELLOW MODIFY

**dmem**

**Summary**

Displays the contents of system, I/O register, PCI/PCIe configuration space, or device memory.

**Usage**

**dmem [-b] [***address***] [***size***] [-MMIO] | -IO | -PCI | -PCIE | -verbose]**

**Options**

*-PCIE*

PCI Express Configuration Space. The address will have the format ssssbbddffrrr, where ssss = Segment, bb = Bus, dd = Device, ff = Function and rrr = Register.

*-verbose*

Verbose. If the UEFI System Table contents are being displayed, provide a human readable display of the contents of the RT\_PROPERTIES, CONFORMANCE\_PROFILE, and IMAGE\_ EXECUTION\_INFO tables are displayed.

**Description**

This command displays the contents of system memory (volatile or persistent), I/O register, PCI/PCIe configuration space, or device memory. The *address* and *size* should be typed in hex value. If *address* is not specified, then the contents of the EFI System Table are displayed, and if the **-verbose** option is specified the contents of the RT\_PROPERTIES, CONFORMANCE\_PROFILE, and IMAGE\_ EXECUTION\_INFO tables are displayed. Otherwise, memory starting at address is displayed.

**Examples**

\* To display the EFI system table pointer entries with verbose output:

**fs0:\> dmem -verbose**

**Memory Address 000000003FF7D808 200 Bytes**

**3FF7D808: 49 42 49 20 53 59 53 54-02 00 01 00 78 00 00 00 \*IBI SYST....x...\***

**...**

**Valid EFI Header at Address 000000003FF7D808**

**--------------------------------------------**

**System: Table Structure size 00000078 revision 00010002**

**ConIn (3F1AD388) ConOut (3F1AF288) StdErr (3F1ADD08)**

**Runtime Services 000000003F3FC318**

**...**

**RT Properties Table**

**---------------------------**

**Version 0x1**

**Runtime Services Supported:**

**GET\_TIME 1**

**SET\_TIME 1**

**WAKEUP\_TIME 0**

**...**

**Conformance Profile Table**

**---------------------------**

**Version 0x1**

**Profile GUIDs:**

**UEFI\_SPEC\_GUID 523c91af-a195-4382-818d-295fe4006465**

**Image Execution Table**

**--------------------------------------------**

**EFI\BOOT\grubaa64.efi: SIG\_NOT\_FOUND**

**# Special Instructions**

Add links to referenced specs at uefi.org/uefi