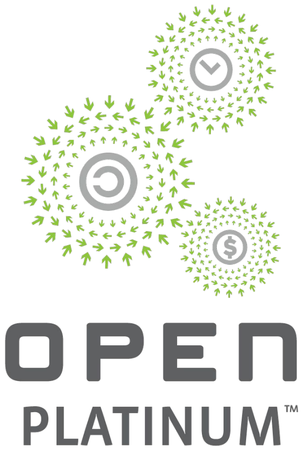
Open. Together.

OCP
SUMMIT

Go Forth and Modify: Fiano

Gan Shun Lim Software Engineer, Google
Ryan O'Leary Software Engineer, Google



Many thanks to

OPEN SYSTEMS FIRMWARE

- Ron Minnich — Google
- Julien Viard de Galbert — Splitted-Desktop Systems
- Andrea Barberio — Facebook

References taken from

- Nikolaj Schlej — UEFITool
- Teddy Reed — UEFI Firmware Parser

Embedded Software

The problem

OPEN SYSTEMS FIRMWARE

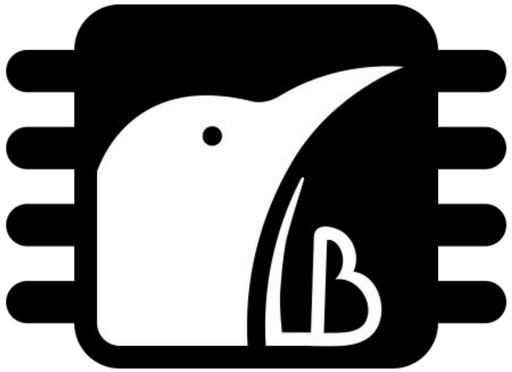
- Vendors provide binary UEFI blobs without source
- Want to edit binary UEFI firmware images
- UEFI was designed to be modular, should be easy in theory
- Applications:
  - LinuxBoot (see Chris Koch's talk)
  - Removing unnecessary DXEs to reduce attack surface
  - Security forensics
  - Debugging
  - Rapid prototyping

Embedded Software

LinuxBoot

OPEN SYSTEMS FIRMWARE

- LinuxBoot adds Linux to your UEFI firmware image.
- Netboot and diskboot are performed by Linux.
- See Chris Koch’s talk for specifics



https://www.linuxboot.org

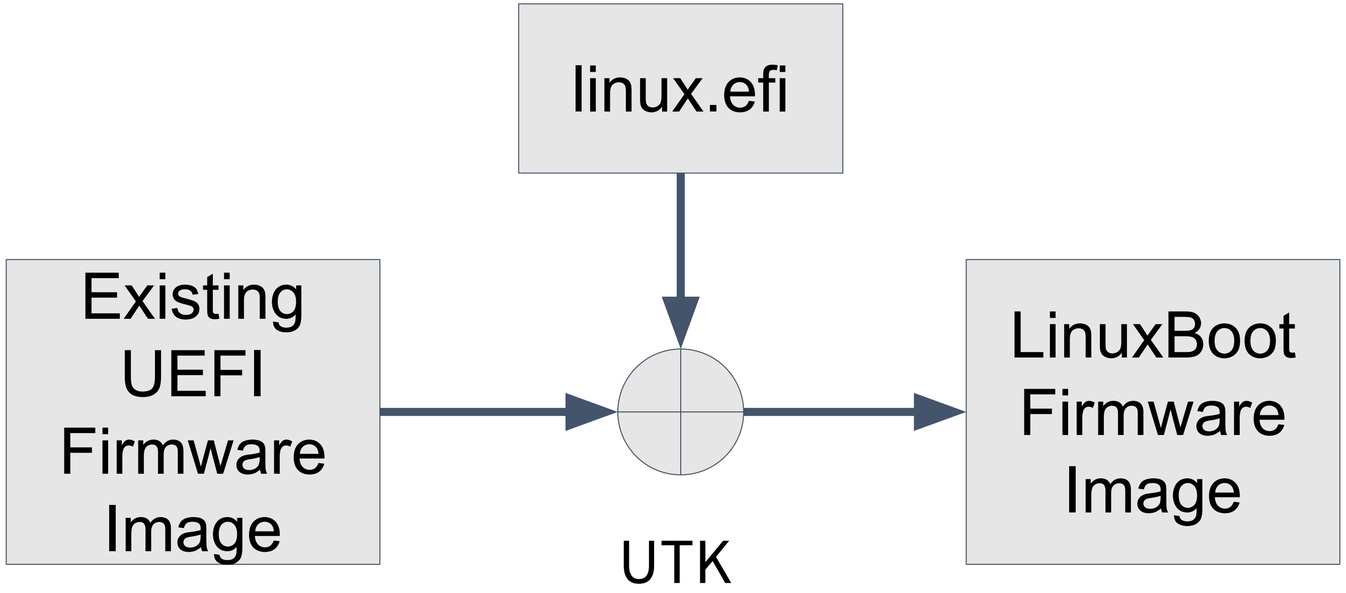
Embedded Software

UTK as a Build Tool for LinuxBoot

OPEN SYSTEMS FIRMWARE

tianocore

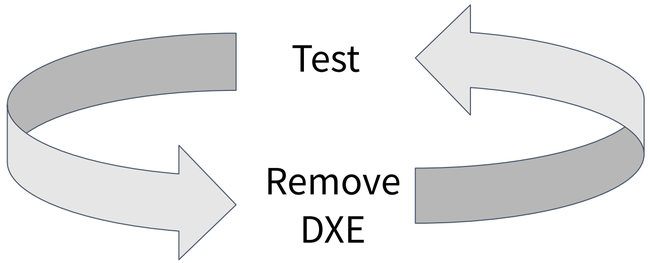
Flashrom



utk old.bios replace_pe32 Shell linux.efi save linuxboot.bios

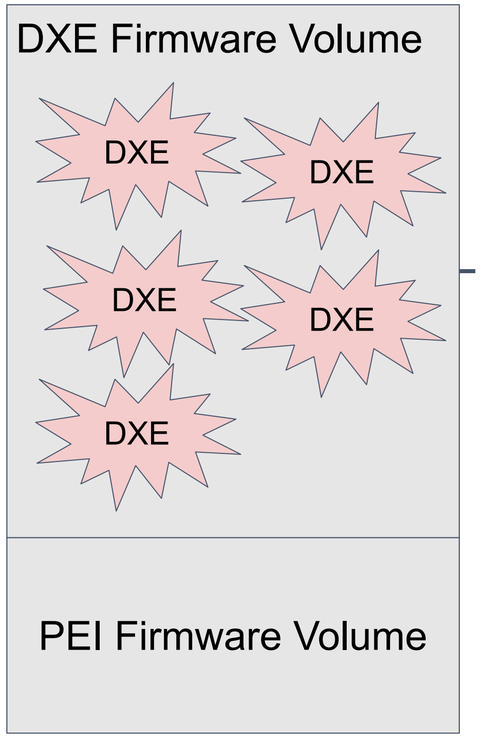
Embedded Software

DXECleaner



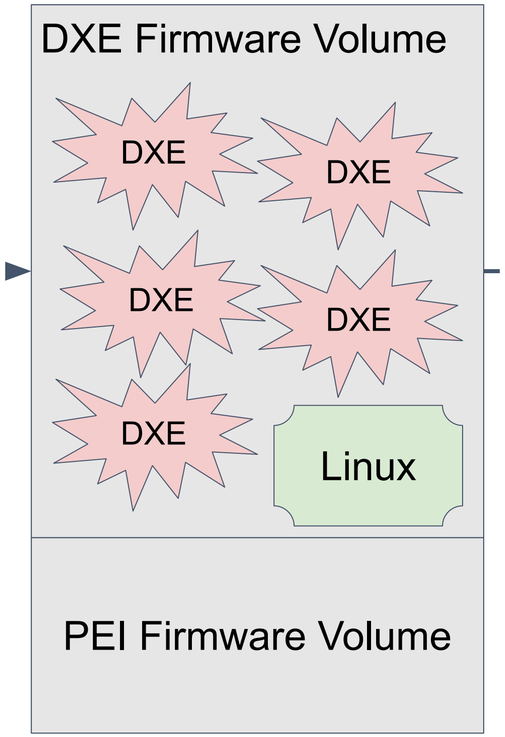
OPEN SYSTEMS FIRMWARE

Original UEFI Image



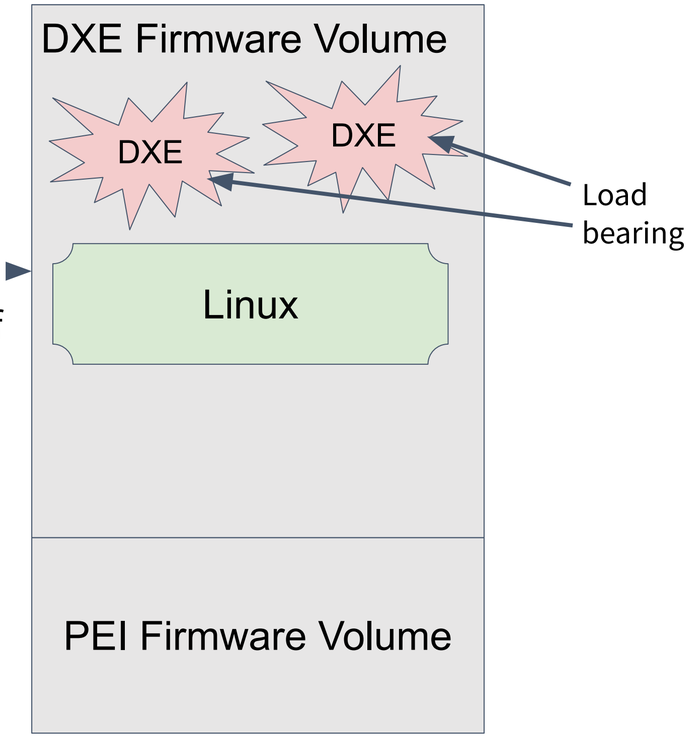
Insert Linux kernel

LinuxBoot Image



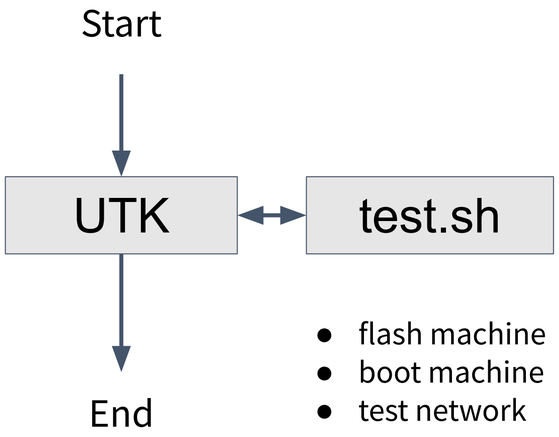
Removal of Unneeded DXEs

Cleaned Image



Embedded Software

Demo of DXECleaner



- flash machine
- boot machine
- test network
- ...

```
~/go/src/github.com/linuxboot/fiano/dxecleaner-demo$ ls
demo.cast  OVMF.rom  serial  test.sh
~/go/src/github.com/linuxboot/fiano/dxecleaner-demo$ vim test.sh
~/go/src/github.com/linuxboot/fiano/dxecleaner-demo$ utk OVMF.rom dxecleaner $PWD/test.sh
Beginning of round 1
Trying to remove D93CE3D8-A7EB-4730-8C8E-CC466A9ECC3C
Successfully booted in QEMU!
  Success D93CE3D8-A7EB-4730-8C8E-CC466A9ECC3C!
Trying to remove 6C2004EF-4E0E-4BE4-B14C-340EB4AA5891
Successfully booted in QEMU!
  Success 6C2004EF-4E0E-4BE4-B14C-340EB4AA5891!
Trying to remove 80CF7257-87AB-47F9-A3FE-D50B76D89541
Failed to boot in QEMU!
  Failed 80CF7257-87AB-47F9-A3FE-D50B76D89541!
Trying to remove B601F8C4-43B7-4784-95B1-F4226CB40CEE
Failed to boot in QEMU!
  Failed B601F8C4-43B7-4784-95B1-F4226CB40CEE
Trying to remove F80697E9-7FD6-4665-8646-88E33EF71DFC
```

DEMO

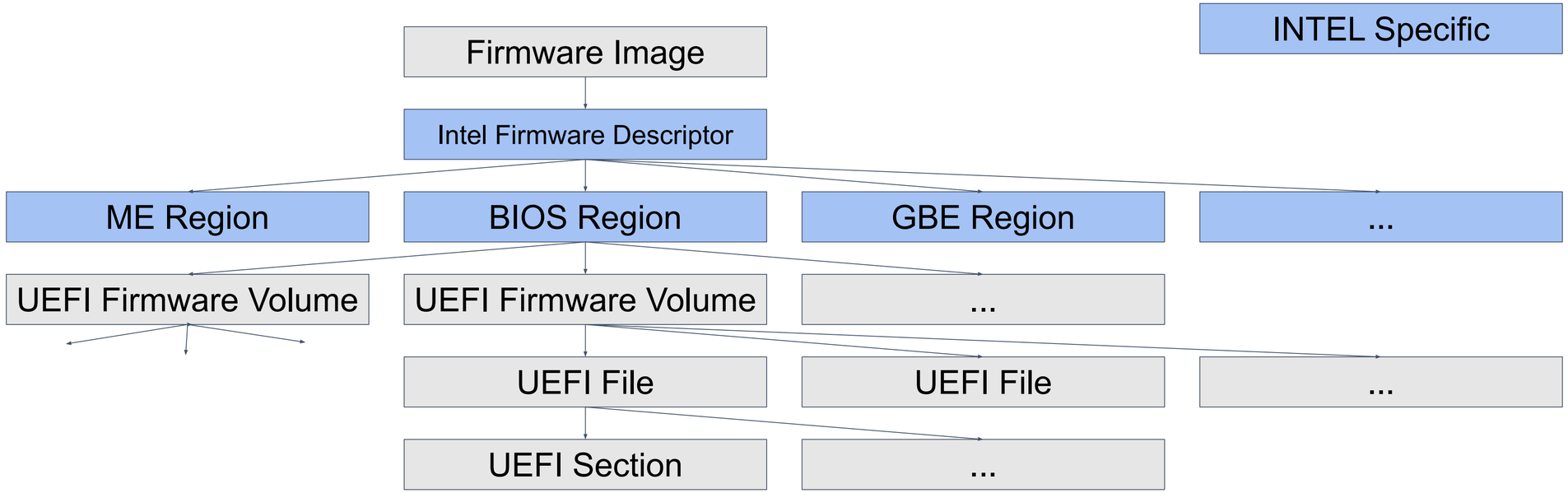
DEMO

https://asciinema.org/a/OjPGXgyINGreaAbsaJM4bVTsj

OPEN SYSTEMS FIRMWARE

Embedded Software

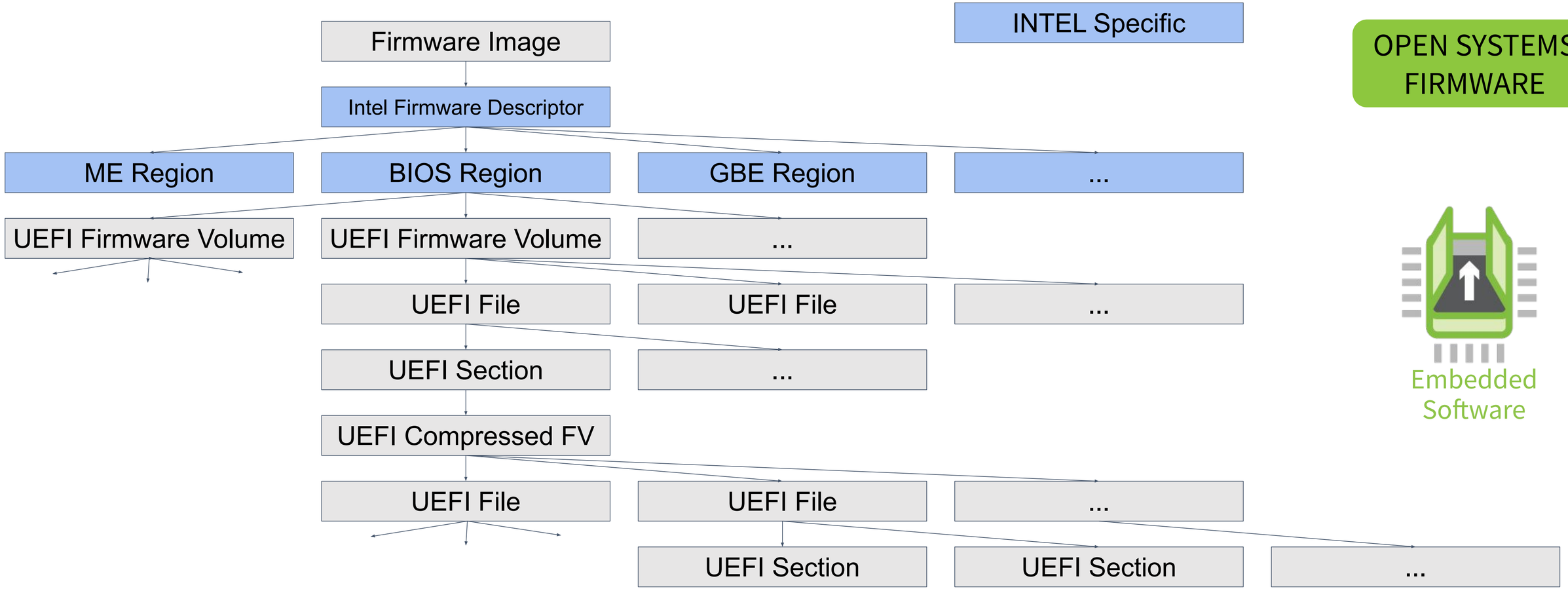
Anatomy of a UEFI Image



OPEN SYSTEMS FIRMWARE

Embedded Software

Anatomy of a UEFI Image



OPEN SYSTEMS FIRMWARE

Embedded Software

What can utk do?

OPEN SYSTEMS FIRMWARE

- Poke around
- Extract files
- Modify files in memory and save.

Embedded Software

utk <rom> table | less

```
Node         GUID/Name                              Type                                  Size
BIOS                                                                                      0x400000
 FV          FFF12B8D-7696-4C8B-A985-2747075B4F50                                          0x84000
  Free                                                                                        0x0
 FV          8C8CE578-8A3D-4F1C-9935-896185C32DD3                                         0x348000
  File       9E21FD93-9C72-4C15-8C4B-E77F1DB2D792  EFI_FV_FILETYPE_FIRMWARE_VOLUME_IMAGE  0x1256a7
   Sec                                              EFI_SECTION_GUID_DEFINED              0x12568f
    Sec                                             EFI_SECTION_RAW                          0x7c
    Sec                                             EFI_SECTION_FIRMWARE_VOLUME_IMAGE     0xe0004
     FV        8C8CE578-8A3D-4F1C-9935-896185C32DD3                                        0xe0000
      File     1B45CC0A-156A-428A-AF62-49864DA0E6E6  EFI_FV_FILETYPE_FREEFORM                 0x2c
       Sec                                           EFI_SECTION_RAW                         0x14
      File     FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF  EFI_FV_FILETYPE_FFS_PAD                 0x40
      File     52C05B14-0B98-496C-BC3B-04B50211D680  EFI_FV_FILETYPE_PEI_CORE              0xc4fa
       Sec                                           EFI_SECTION_RAW                         0x3c
       Sec                                           EFI_SECTION_PE32                      0xc484
       Sec     PeiCore                               EFI_SECTION_USER_INTERFACE              0x14
       Sec     Version 1.0                           EFI_SECTION_VERSION                      0xe
      File     9B3ADA4F-AE56-4C24-8DEA-F03B7558AE50  EFI_FV_FILETYPE_PEIM                  0x4f3a
      File     FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF  EFI_FV_FILETYPE_FFS_PAD                 0x40
      File     A3610442-E69F-4DF3-82CA-2360C4031A23  EFI_FV_FILETYPE_PEIM                  0x211e
      File     FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF  EFI_FV_FILETYPE_FFS_PAD                 0x60
      File     9D225237-FA01-464C-A949-BAABC02D31D0  EFI_FV_FILETYPE_PEIM                  0x21d6
      File     FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF  EFI_FV_FILETYPE_FFS_PAD                 0x28
```

OPEN SYSTEMS FIRMWARE

Embedded Software

More commands for poking around

OPEN SYSTEMS FIRMWARE

- **`utk <romimage> find .*Shell.*`**
  - Takes a regexp, dumps json about the struct in question
- **`utk <romimage> find 7C04A583-9E3E-4f1c-AD65-E05268D0B4D1`**
  - Find can also take a GUID, (in this case it's the EFI Shell GUID)

- **`utk <romimage> dump .*Shell.* shell.bin`**
  - dump uses find to search for the requested ffs, and dumps the whole ffs to a binary
- **`utk <romimage> count`**
  - Counts the number of each type of firmware.

Embedded Software

Let’s change things!

OPEN SYSTEMS FIRMWARE

- **`utk <romimage> remove .*Shell.* save <newromimage>`**
  - Removes an FFS, could be Dxe, or Pei
  - Remove takes the same arguments as Find.

- **`utk <romimage> replace_pe32 .*Shell.* bzImage save <newromimage>`**
  - Replaces the PE32 executable in the Shell with another PE32 executable. In the case of Linuxboot, it can just be a Linux kernel!

Embedded Software

Chain commands together

OPEN SYSTEMS FIRMWARE

- `utk <romimage> \`
  - `remove .*Ip.* \`
  - `remove .*Dhcp.* \`
  - `replace_pe32 .*Shell.* bzImage \`
  - `save <newromimage>`

- Commands can be chained together for more complex operations

Embedded Software

TLDR

OPEN SYSTEMS FIRMWARE

- Easily scriptable UEFI image editing tool
- Written in Go, unit-tested, type safe
- Avoids rebuilding entire UEFI images.
  - Speed
  - Availability of source
- Automated DXE removal

Embedded Software

Call to Action

UTK

https://github.com/linuxboot/fiano

Try utk

```
sudo apt-get install go
go get github.com/linuxboot/fiano/cmds/utk
utk --help
```

Take a look at the issue tracker. help wanted tags are great to start. File bugs, create pull-requests, update documentation, ...

LinuxBoot Book

https://github.com/linuxboot/book
See the UTK chapter.

New Firmware

Let use know if you want to try UTK on your firmware. We're always excited about seeing UTK work for new firmware!

Laptop Stickers

Get them now!


Open. Together.
OCP Global Summit | March 14–15, 2019
OCP
SUMMIT