UEFI & EDK II Training

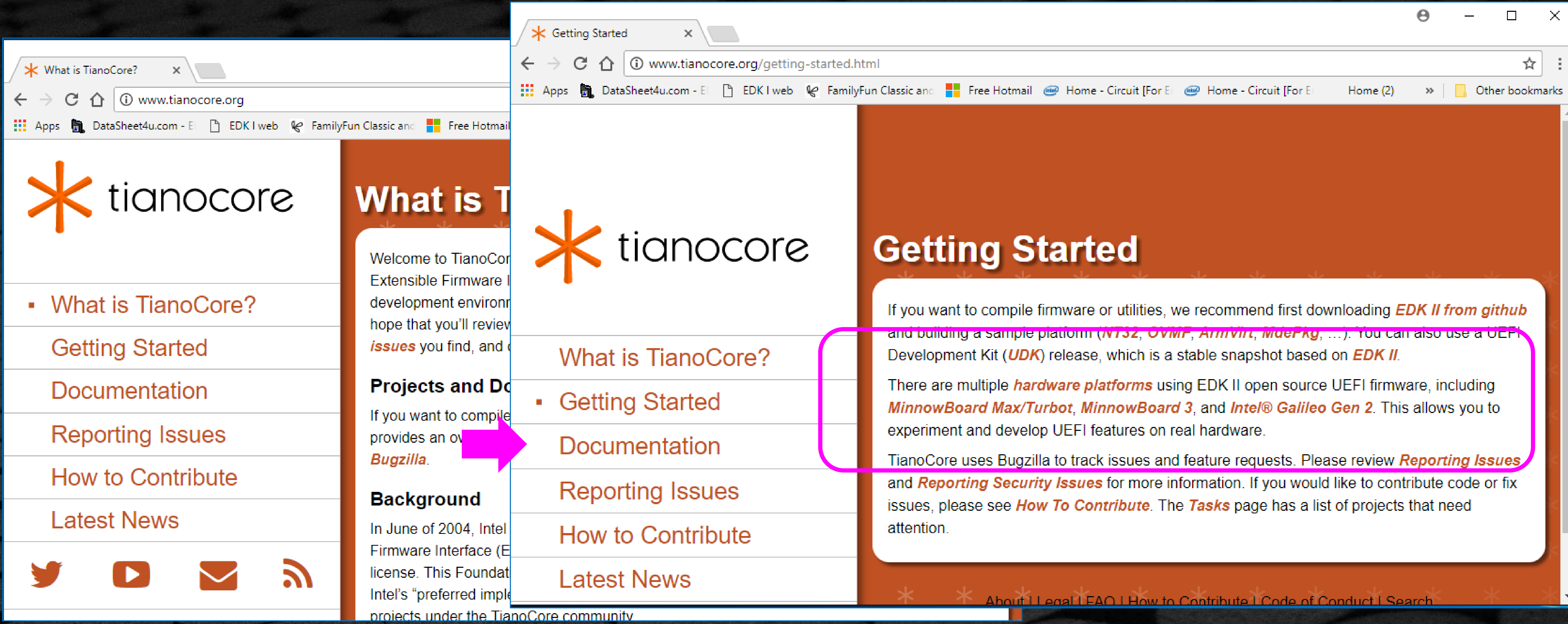
Open Source UEFI Platforms

tianocore.org

LESSON OBJECTIVE

- Chart the organization of the Tianocore.org repositories
- Recognize the various Open Source UEFI Platforms

Tianocore.org



What is T

Welcome to TianoCor
Extensible Firmware I
development environ
hope that you'll review
issues you find, and c

Projects and Do

If you want to compile
provides an ov
Bugzilla.

Background

In June of 2004, Intel
Firmware Interface (E
license. This Foundat
Intel's "preferred impl
projects under the TianoCore community

Getting Started

If you want to compile firmware or utilities, we recommend first downloading ***EDK II from github*** and building a sample platform (***NT32***, ***OVMF***, ***ArmVirt***, ***MdePkg***, ...). You can also use a UEFI Development Kit (***UDK***) release, which is a stable snapshot based on ***EDK II***.

There are multiple ***hardware platforms*** using EDK II open source UEFI firmware, including ***MinnowBoard Max/Turbot***, ***MinnowBoard 3***, and ***Intel® Galileo Gen 2***. This allows you to experiment and develop UEFI features on real hardware.

TianoCore uses Bugzilla to track issues and feature requests. Please review ***Reporting Issues*** and ***Reporting Security Issues*** for more information. If you would like to contribute code or fix issues, please see ***How To Contribute***. The ***Tasks*** page has a list of projects that need attention.

About | Legal | FAQ | How to Contribute | Code of Conduct | Search

Platforms ***Emulator***, ***OVMF***, ***ArmVirt***, ***MdePkgHardware platforms***: ***MinnowBoard Max/Turbot***, ***Up Squared***, and ***Intel® Galileo Gen 2***.

tianocore

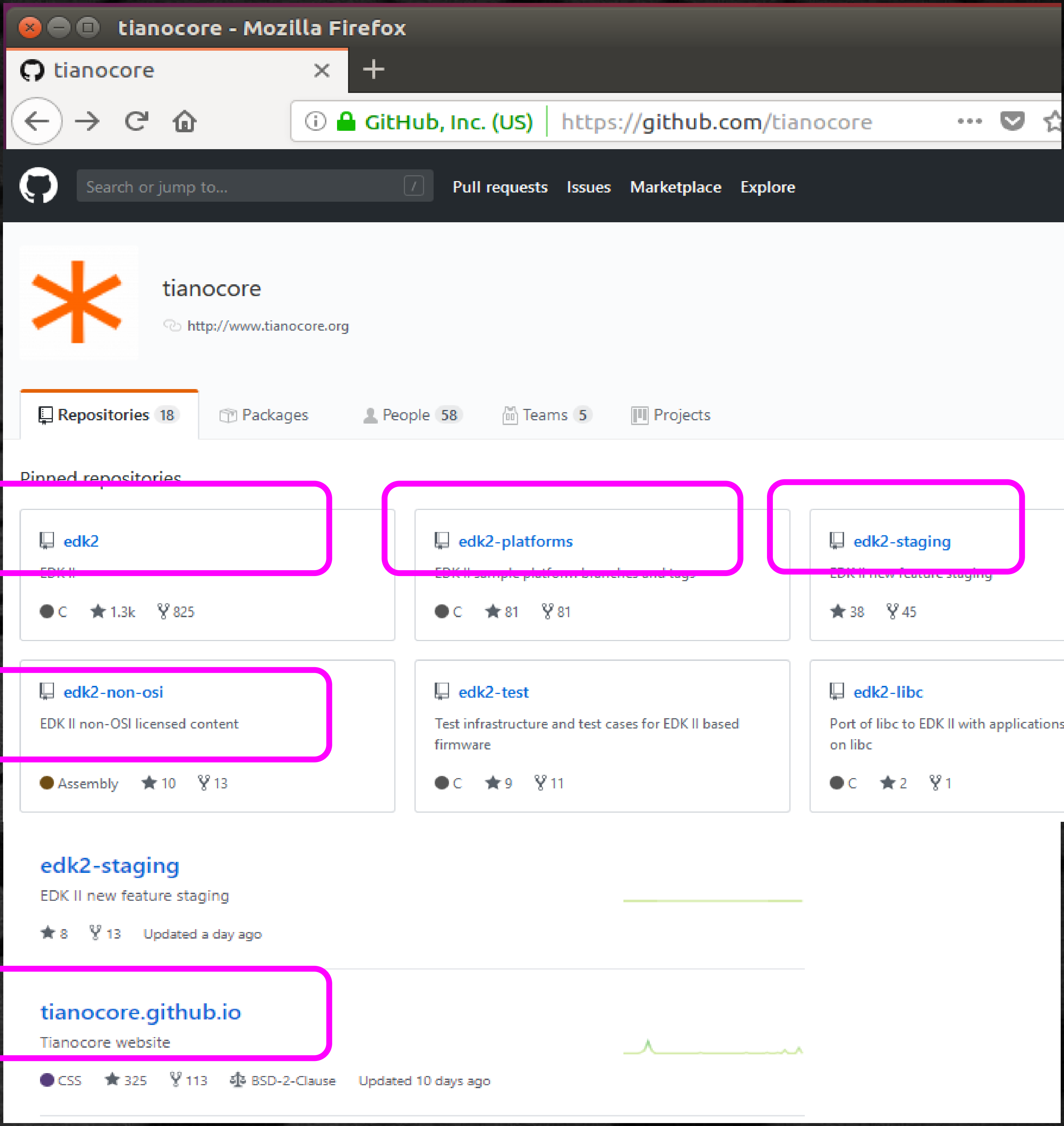
GitHub

Github/tianocore

Concept of Repositories

- Main development - edk2
- Other platforms - edk2-platforms
- Not compatible w/ edk2 & edk2-platforms licensing - edk2-non-osi
- Work in Progress - edk2-staging
- Online Info & Help (Wiki pages) tianocore.github.io

- To download use "git clone" then "git checkout"



tianocore - Mozilla Firefox

tianocore

GitHub, Inc. (US) | https://github.com/tianocore

Search or jump to... Pull requests Issues Marketplace Explore

tianocore

http://www.tianocore.org

Repositories 18 | Packages | People 58 | Teams 5 | Projects

Pinned repositories

edk2
EDK II
● C ★ 1.3k 825

edk2-platforms
EDK II sample platform branches and tags
● C ★ 81 81

edk2-staging
EDK II new feature staging
★ 38 45

edk2-non-osi
EDK II non-OSI licensed content
● Assembly ★ 10 13

edk2-test
Test infrastructure and test cases for EDK II based firmware
● C ★ 9 11

edk2-libc
Port of libc to EDK II with applications on libc
● C ★ 2 1

edk2-staging
EDK II new feature staging
★ 8 13 Updated a day ago

tianocore.github.io
Tianocore website
● CSS ★ 325 113 BSD-2-Clause Updated 10 days ago

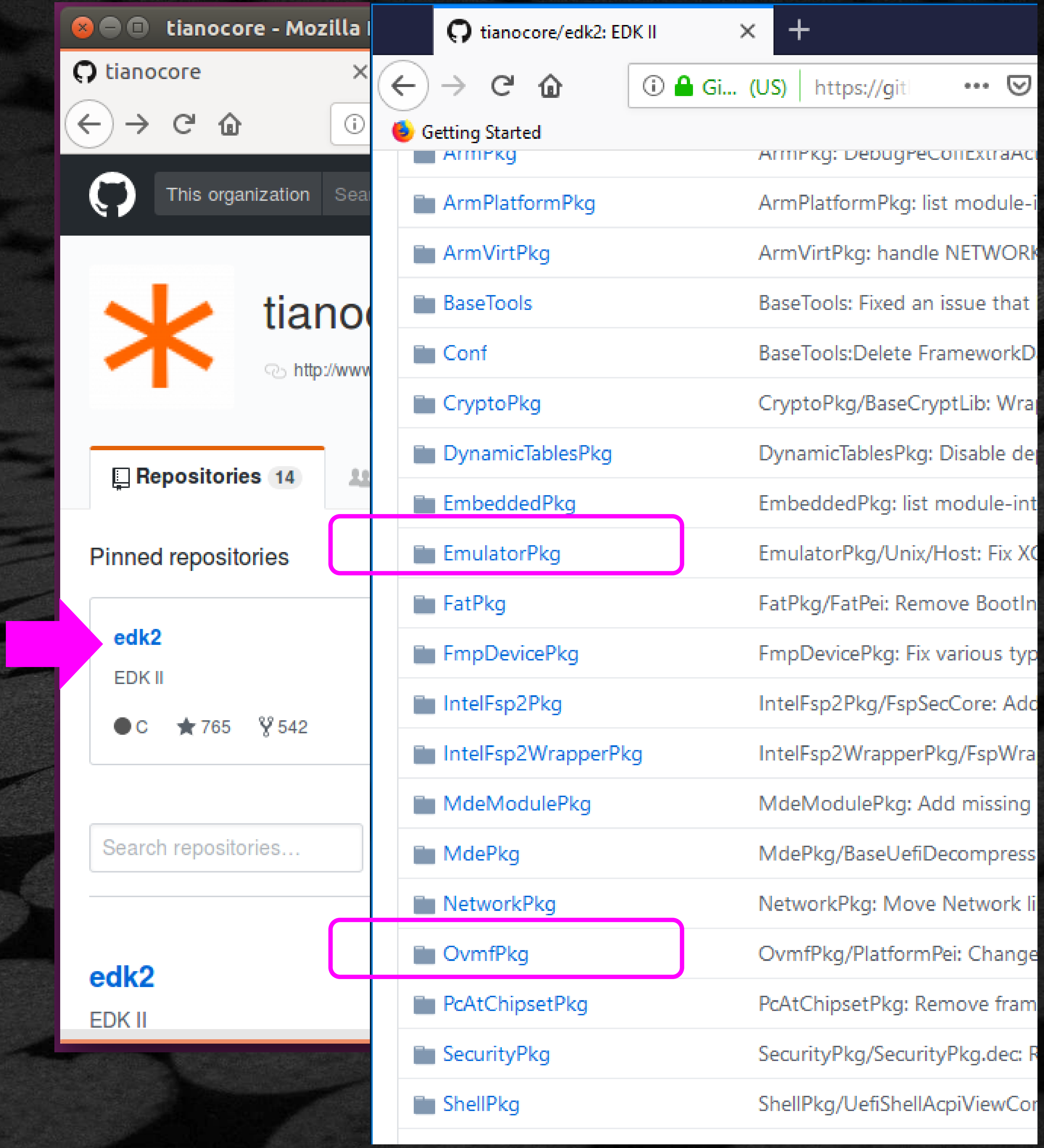
GitHub Tianocore.org

edk2 – Platforms on edk2- “**CORE**”

EmulatorPkg

OvmfPkg

See *Readme.md* files



tianocore - Mozilla

tianocore

This organization Sea

tiano

http://www

Repositories 14

Pinned repositories

edk2

EDK II

● C ★ 765 542

Search repositories…

edk2

EDK II

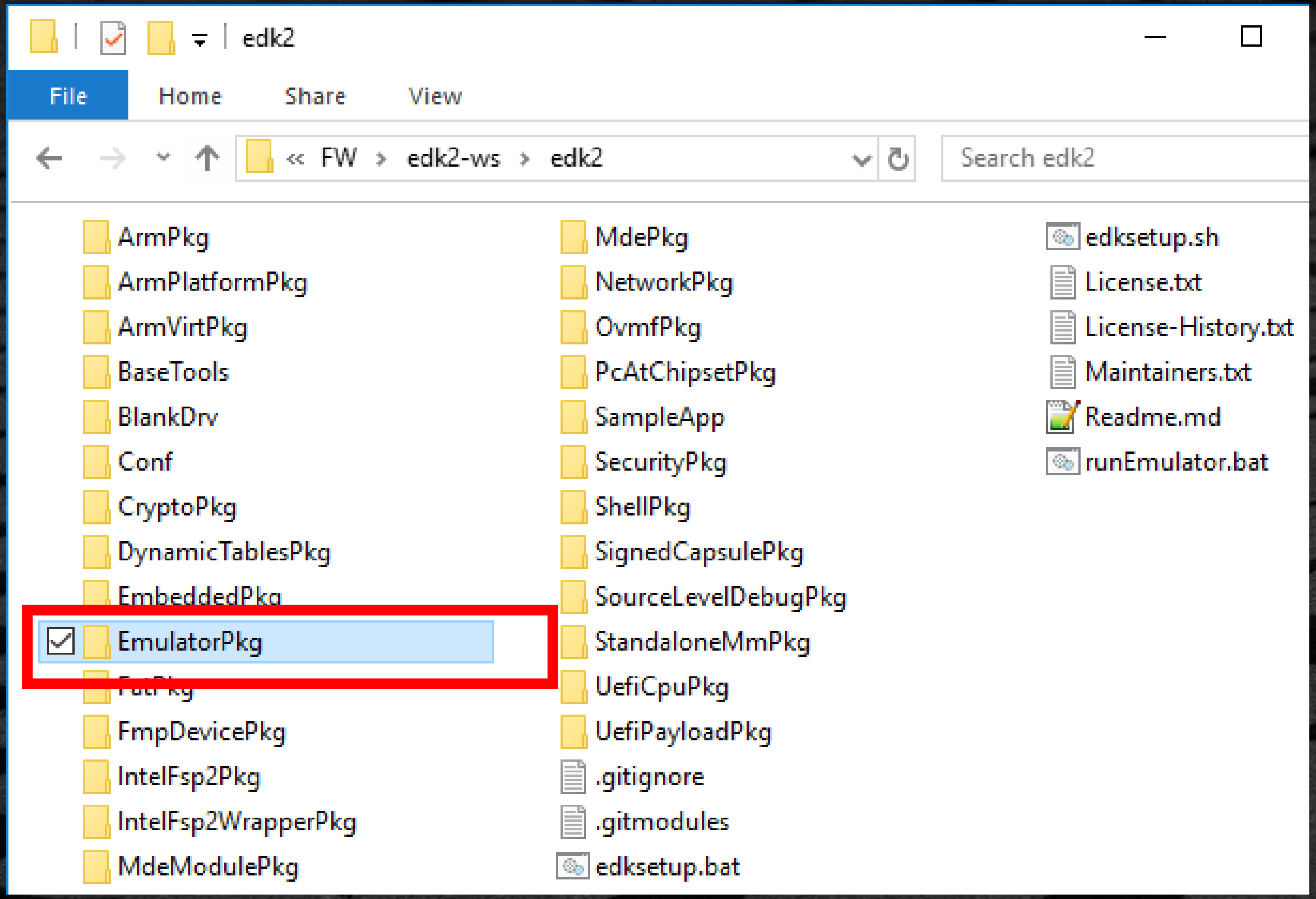
tianocore/edk2: EDK II

Gi... (US) https://git

Getting Started

ArmPkg	ArmPkg: DebugPeCoffExtraAc
ArmPlatformPkg	ArmPlatformPkg: list module-i
ArmVirtPkg	ArmVirtPkg: handle NETWORK
BaseTools	BaseTools: Fixed an issue that
Conf	BaseTools:Delete FrameworkD
CryptoPkg	CryptoPkg/BaseCryptLib: Wra
DynamicTablesPkg	DynamicTablesPkg: Disable de
EmbeddedPkg	EmbeddedPkg: list module-int
EmulatorPkg	EmulatorPkg/Unix/Host: Fix XC
FatPkg	FatPkg/FatPei: Remove BootIn
FmpDevicePkg	FmpDevicePkg: Fix various typ
IntelFsp2Pkg	IntelFsp2Pkg/FspSecCore: Add
IntelFsp2WrapperPkg	IntelFsp2WrapperPkg/FspWra
MdeModulePkg	MdeModulePkg: Add missing
MdePkg	MdePkg/BaseUefiDecompress
NetworkPkg	NetworkPkg: Move Network li
OvmfPkg	OvmfPkg/PlatformPei: Change
PcAtChipsetPkg	PcAtChipsetPkg: Remove fram
SecurityPkg	SecurityPkg/SecurityPkg.dec: R
ShellPkg	ShellPkg/UefiShellAcpiViewCor

Emulation Directory Structure

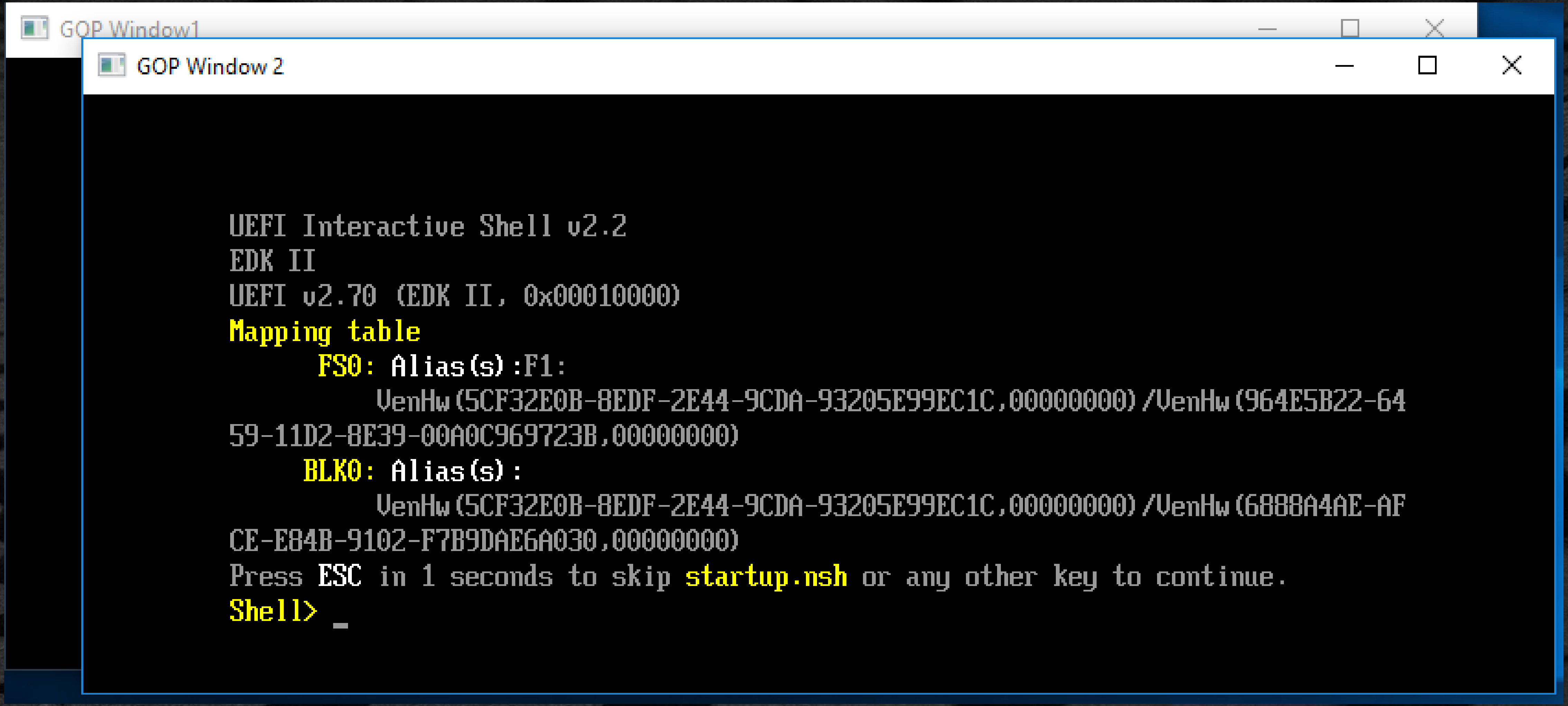


- ArmPkg
- ArmPlatformPkg
- ArmVirtPkg
- BaseTools
- BlankDrv
- Conf
- CryptoPkg
- DynamicTablesPkg
- EmbeddedPkg
- ☑ EmulatorPkg
- FatPkg
- FmpDevicePkg
- IntelFsp2Pkg
- IntelFsp2WrapperPkg
- MdeModulePkg
- MdePkg
- NetworkPkg
- OvmfPkg
- PcAtChipsetPkg
- SampleApp
- SecurityPkg
- ShellPkg
- SignedCapsulePkg
- SourceLevelDebugPkg
- StandaloneMmPkg
- UefiCpuPkg
- UefiPayloadPkg
- .gitignore
- .gitmodules
- edksetup.bat
- edksetup.sh
- License.txt
- License-History.txt
- Maintainers.txt
- Readme.md
- runEmulator.bat

EmulatorPkg files

- ✓ EmulatorPkg.dsc
- ✓ EmulatorPkg.dec
- ✓ EmulatorPkg.fdf

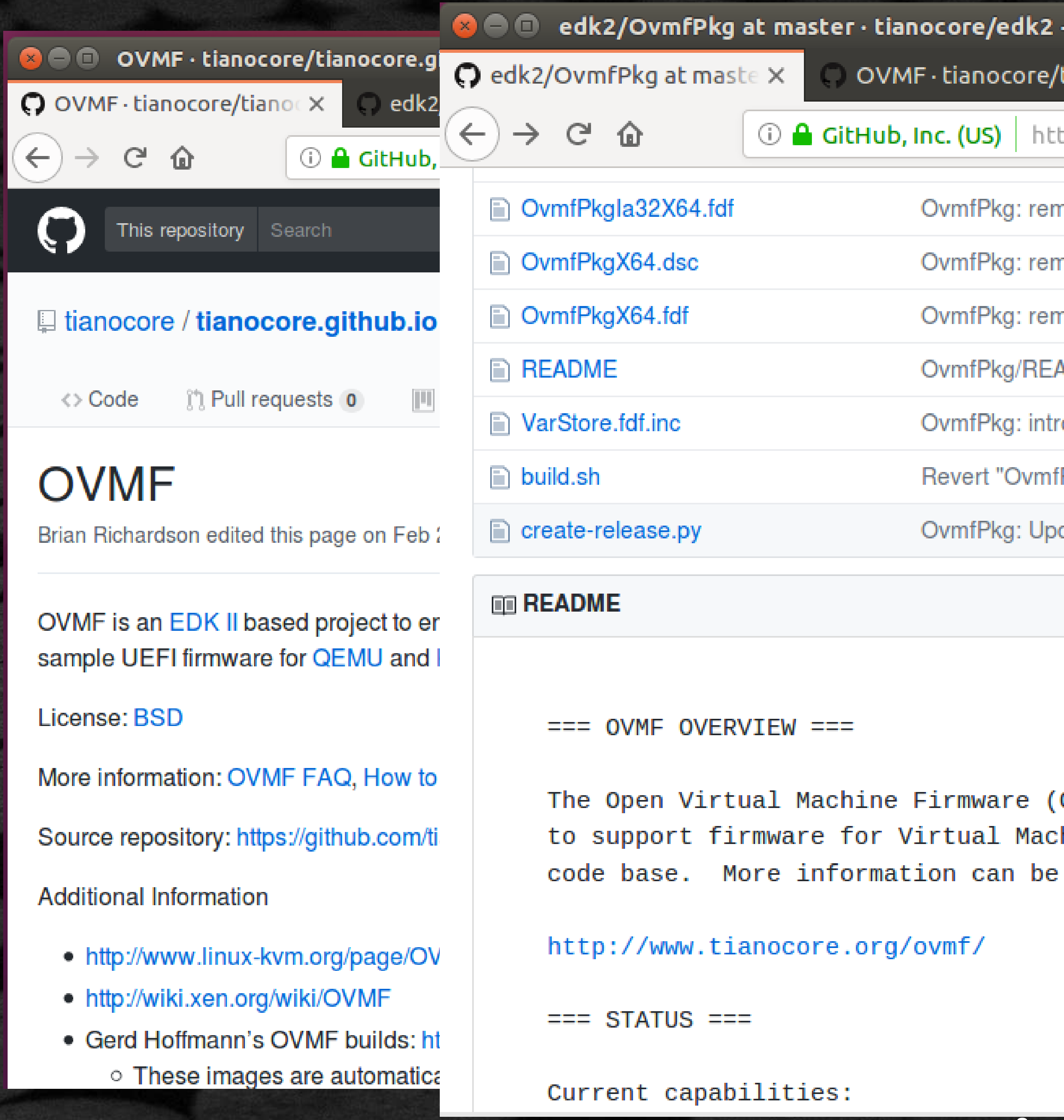
Running Emulator with Windows



```
UEFI Interactive Shell v2.2
EDK II
UEFI v2.70 (EDK II, 0x00010000)
Mapping table
      FS0: Alias(s):F1:
          VenHw(5CF32E0B-8EDF-2E44-9CDA-93205E99EC1C,00000000)/VenHw(964E5B22-64
59-11D2-8E39-00A0C969723B,00000000)
     BLK0: Alias(s):
          VenHw(5CF32E0B-8EDF-2E44-9CDA-93205E99EC1C,00000000)/VenHw(6888A4AE-AF
CE-E84B-9102-F7B9DAE6A030,00000000)
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell> _
```

Open Virtual Machine Firmware (OVMF)

- Uses EDK II to support firmware in the OvmfPkg platform package
- Supports UEFI: Helps develop/debug drivers & applications
- QEMU VM; emulates IA32 (x86)/X64 (x86-64) based system
- Exit condition → UEFI Shell
- Tool Chain/OS Support
- Information Ovmf wiki, Tianocore.org



tianocore / tianocore.github.io

OVMF

Brian Richardson edited this page on Feb

OVMF is an EDK II based project to er
sample UEFI firmware for QEMU and

License: BSD

More information: OVMF FAQ, How to

Source repository: https://github.com/ti

Additional Information

- http://www.linux-kvm.org/page/OV
- http://wiki.xen.org/wiki/OVMF
- Gerd Hoffmann's OVMF builds: ht
  - These images are automatica

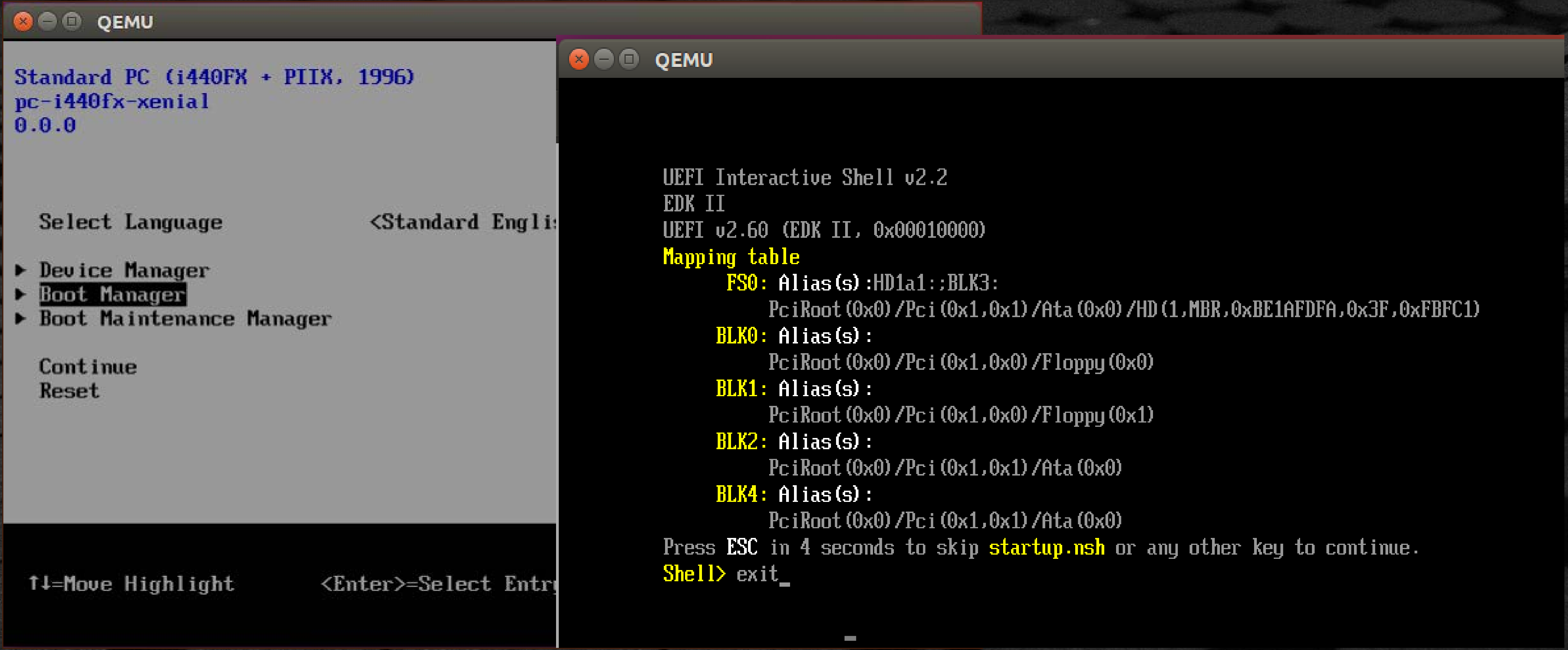
OvmfPkgIa32X64.fdf	OvmfPkg: rem
OvmfPkgX64.dsc	OvmfPkg: rem
OvmfPkgX64.fdf	OvmfPkg: rem
README	OvmfPkg/REA
VarStore.fdf.inc	OvmfPkg: intr
build.sh	Revert "Ovmf
create-release.py	OvmfPkg: Upc

README

```
=== OVMF OVERVIEW ===

The Open Virtual Machine Firmware (
to support firmware for Virtual Mac
code base.  More information can be

http://www.tianocore.org/ovmf/

=== STATUS ===

Current capabilities:
```

OVMF BIOS w/ QEMU

Boots to UEFI Shell



```
Standard PC (i440FX + PIIX, 1996)
pc-i440fx-xenial
0.0.0


  Select Language              <Standard Engli

▶ Device Manager
▶ Boot Manager
▶ Boot Maintenance Manager

  Continue
  Reset


 ↑↓=Move Highlight       <Enter>=Select Entr
```

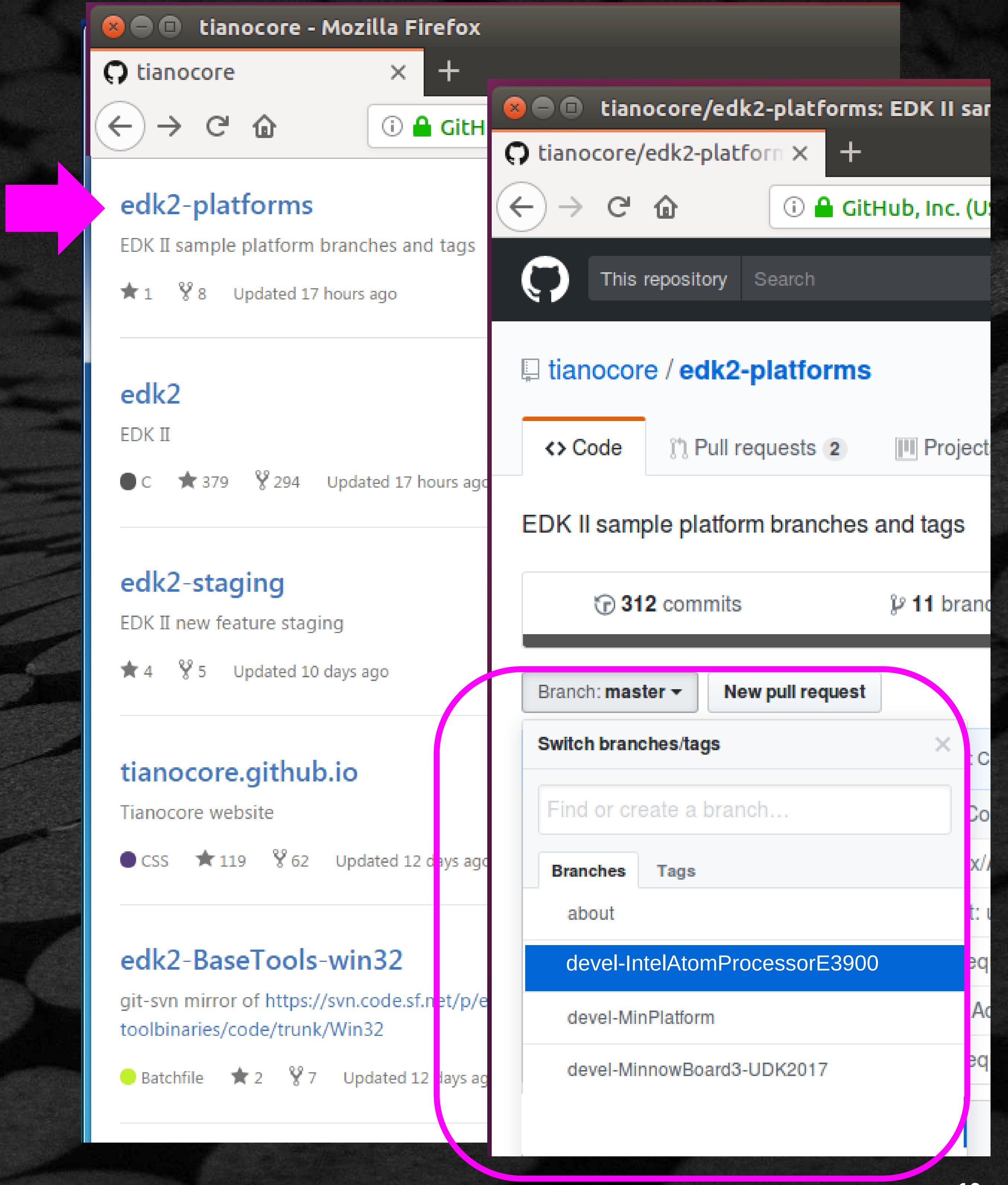
```
UEFI Interactive Shell v2.2
EDK II
UEFI v2.60 (EDK II, 0x00010000)
Mapping table
      FS0: Alias(s):HD1a1::BLK3:
          PciRoot(0x0)/Pci(0x1,0x1)/Ata(0x0)/HD(1,MBR,0xBE1AFDFA,0x3F,0xFBFC1)
     BLK0: Alias(s):
          PciRoot(0x0)/Pci(0x1,0x0)/Floppy(0x0)
     BLK1: Alias(s):
          PciRoot(0x0)/Pci(0x1,0x0)/Floppy(0x1)
     BLK2: Alias(s):
          PciRoot(0x0)/Pci(0x1,0x1)/Ata(0x0)
     BLK4: Alias(s):
          PciRoot(0x0)/Pci(0x1,0x1)/Ata(0x0)
Press ESC in 4 seconds to skip startup.nsh or any other key to continue.
Shell> exit_
```

Platforms Tianocore.org

edk2-platforms – Platforms

- devel-IntelAtomProcessorE3900 – Leaf Hill, Up Squared (Apollo Lake)
- Vlv2TbltDevicePkg – BayTrail-I
- MinPlatformPkg – (w/ FSP)
  - KabylakeOpenBoardPkg
  - WhiskeyLakeOpenBoardPkg
- How to build

  See *Readme.md* files



tianocore - Mozilla Firefox

tianocore

edk2-platforms

EDK II sample platform branches and tags

★ 1 8 Updated 17 hours ago

edk2

EDK II

C ★ 379 294 Updated 17 hours ago

edk2-staging

EDK II new feature staging

★ 4 5 Updated 10 days ago

tianocore.github.io

Tianocore website

CSS ★ 119 62 Updated 12 days ago

edk2-BaseTools-win32

git-svn mirror of https://svn.code.sf.net/p/e toolbinaries/code/trunk/Win32

Batchfile ★ 2 7 Updated 12 days ag

tianocore/edk2-platforms: EDK II sar

tianocore/edk2-platforn

GitHub, Inc. (U

This repository Search

tianocore / edk2-platforms

<> Code Pull requests 2 Project

EDK II sample platform branches and tags

312 commits 11 branc

Branch: master New pull request

Switch branches/tags

Find or create a branch…

Branches Tags

about

devel-IntelAtomProcessorE3900

devel-MinPlatform

devel-MinnowBoard3-UDK2017

Slim BootLoader (SBL) Project

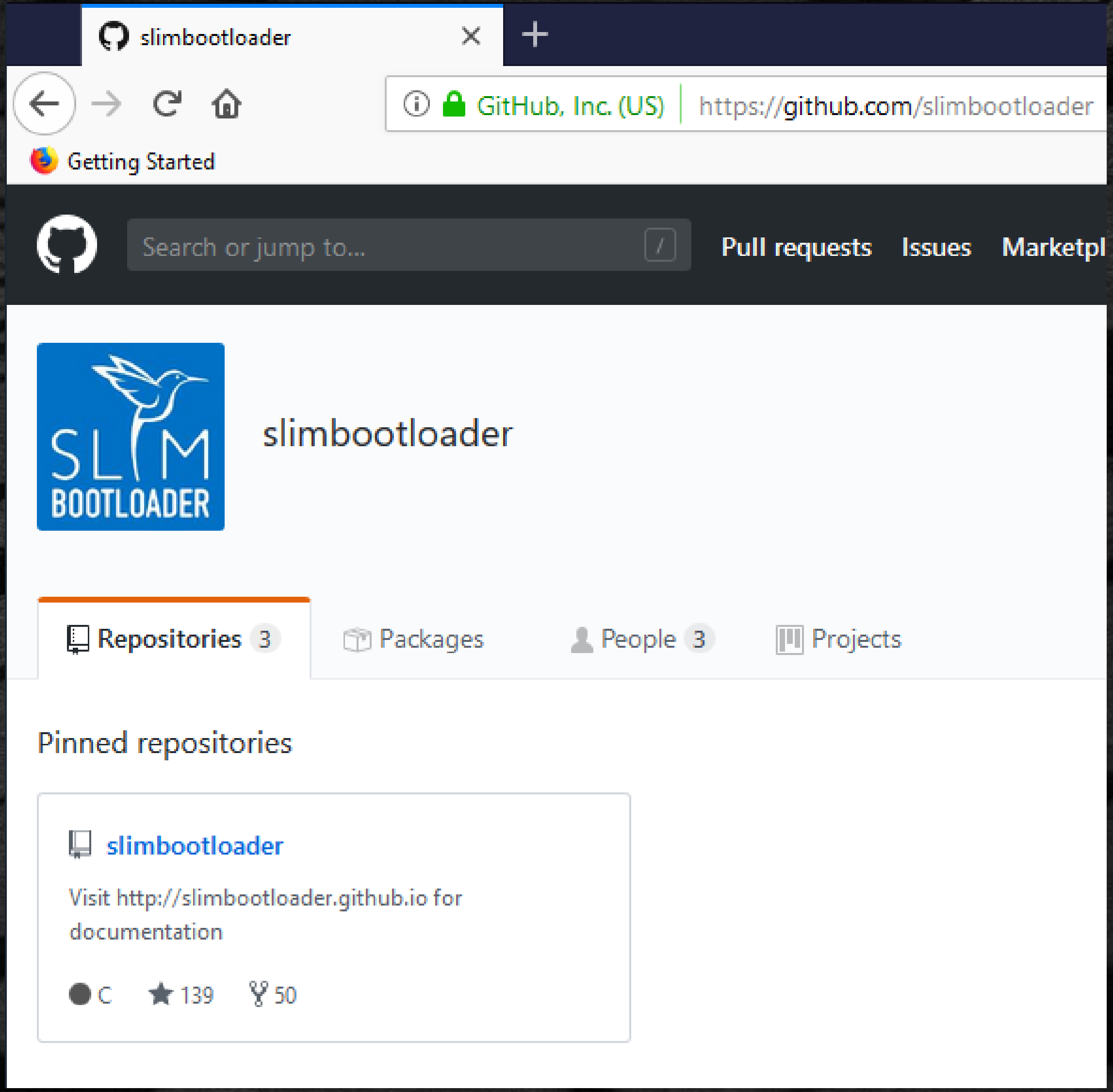
Fast & Secure Open source boot solution for IoT Use Cases

Github: https://github.com/slimbootloader

Supported Hardware:

- QEMU
- UP2 Board
- Apollo Lake CRB
- Whisky Lake CRB
- Coffee Lake Refresh CRB
- UP Xtreme Board

Documentation: Slim Bootloader Project



Visit http://slimbootloader.github.io for documentation

Intel® FSP Repository

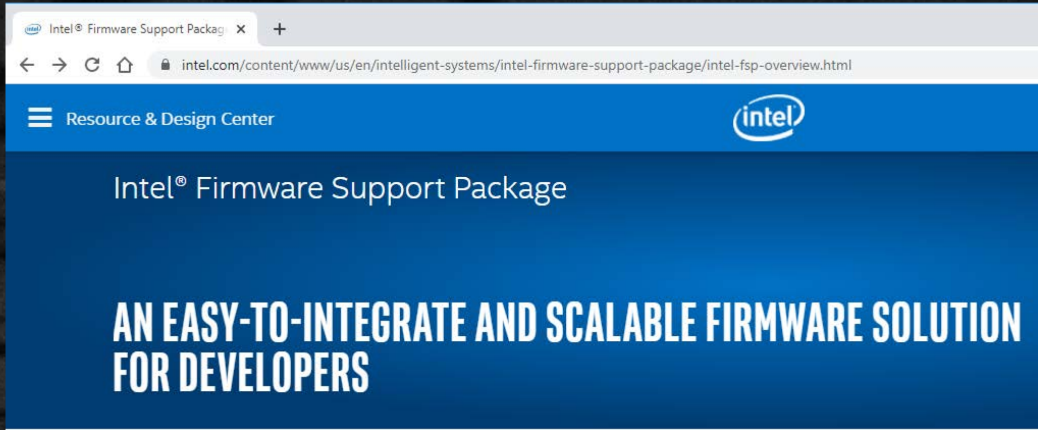
intel Intel Developer Zone Overview

Repository of Intel FSP binaries posted by Intel on github:

Includes documentation on how to integrate with various platforms: https://github.com/intel/FSP

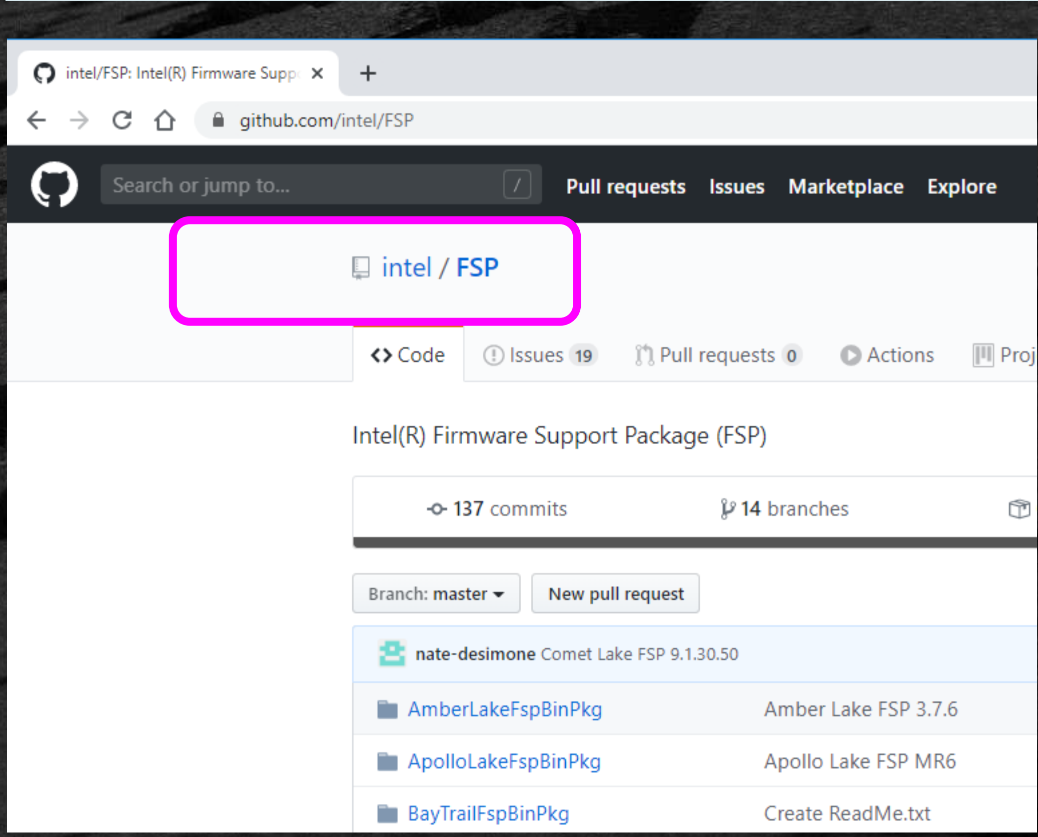
Wiki: https://github.com/intel/FSP/wiki

- current specifications


Intel® Firmware Support Packag
intel.com/content/www/us/en/intelligent-systems/intel-firmware-support-package/intel-fsp-overview.html
Resource & Design Center
intel

Intel® Firmware Support Package

AN EASY-TO-INTEGRATE AND SCALABLE FIRMWARE SOLUTION FOR DEVELOPERS



intel / FSP

Intel(R) Firmware Support Package (FSP)

137 commits 14 branches

Branch: master New pull request

nate-desimone Comet Lake FSP 9.1.30.50

AmberLakeFspBinPkg	Amber Lake FSP 3.7.6
ApolloLakeFspBinPkg	Apollo Lake FSP MR6
BayTrailFspBinPkg	Create ReadMe.txt

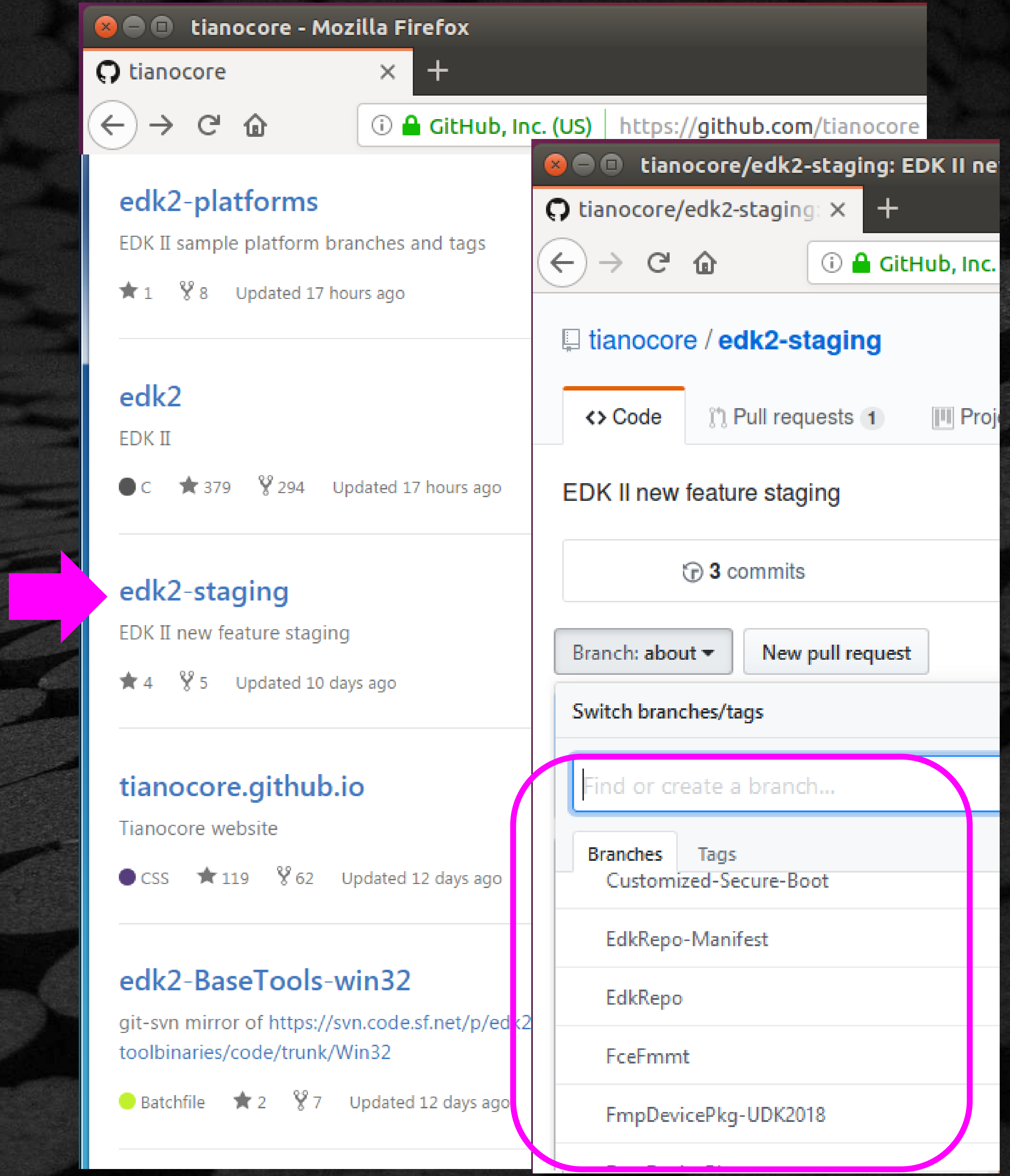
STAGING TIANOCORE.ORG

Implementations not yet Ready for EDK II Main edk2-staging

Projects on branches

- Host-based FW analysis (HBFA)
- edk2-host-test
- FceFmmt (FW Utils)
- UEFI_PCI_ENHANCE-2
- EdkRepo
- Cpu/6-level
- HTTPS-TLS
- RICS-V
- . . .

- See *Readme.md* files



tianocore - Mozilla Firefox
tianocore
GitHub, Inc. (US) https://github.com/tianocore

edk2-platforms
EDK II sample platform branches and tags
★ 1 8 Updated 17 hours ago

edk2
EDK II
● C ★ 379 294 Updated 17 hours ago

edk2-staging
EDK II new feature staging
★ 4 5 Updated 10 days ago

tianocore.github.io
Tianocore website
● CSS ★ 119 62 Updated 12 days ago

edk2-BaseTools-win32
git-svn mirror of https://svn.code.sf.net/p/edk2 toolbinaries/code/trunk/Win32
● Batchfile ★ 2 7 Updated 12 days ago

tianocore / edk2-staging

EDK II new feature staging

3 commits

Customized-Secure-Boot
EdkRepo-Manifest
EdkRepo
FceFmmt
FmpDevicePkg-UDK2018

SUMMARY

- Chart the organization of the Tianocore.org repositories
- Recognize the various Open Source UEFI Platforms

Questions?

Return to Main Training Page

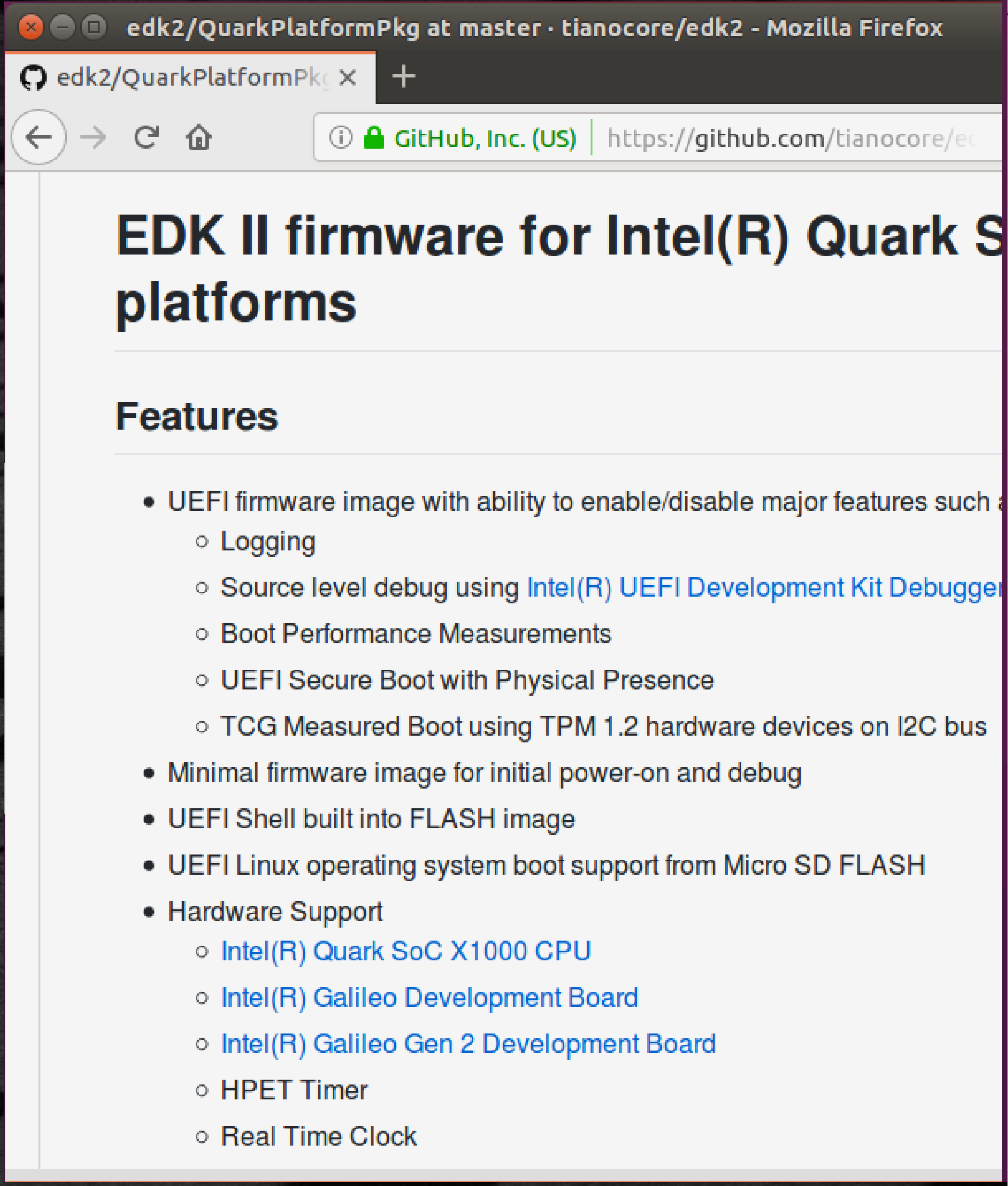
Return to Training Table of contents for next presentation link

tianocore

Back up

Intel® Quark SoC X1000 Platform Project EDK II

- Uses EDK II to support firmware
- QuarkPlatformPkg
  -Intel® Galileo Gen2
- How to Build: Quark Readme.md

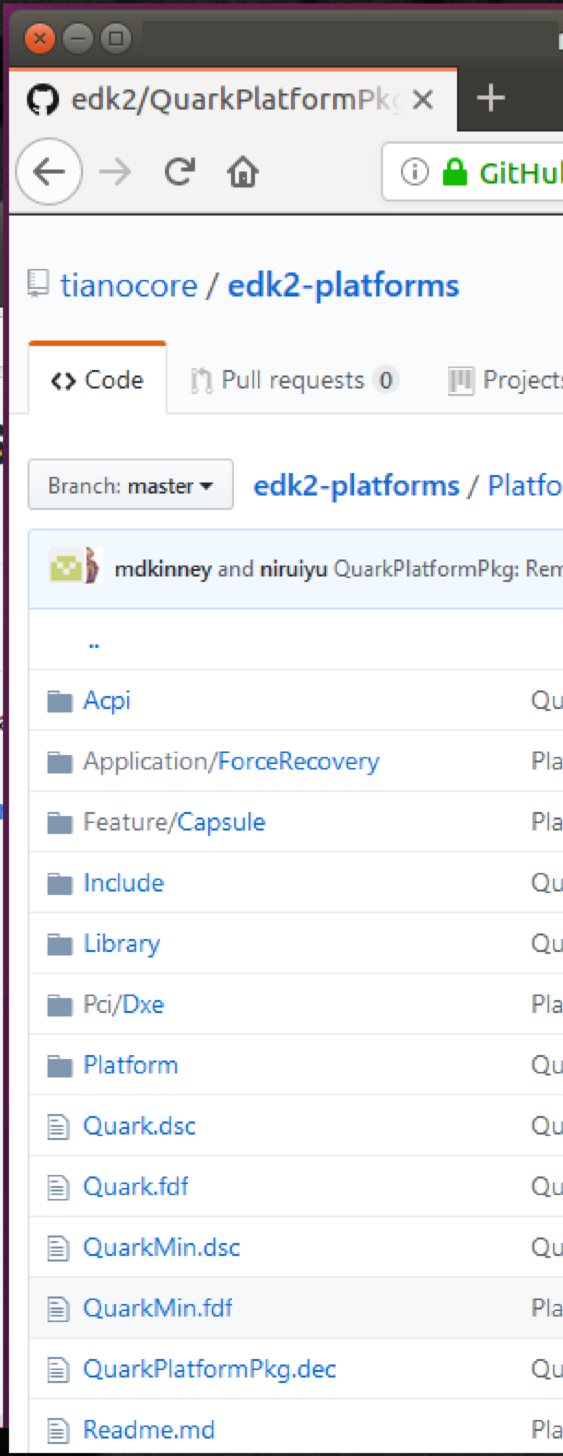


edk2/QuarkPlatformPkg at master · tianocore/edk2 - Mozilla Firefox
edk2/QuarkPlatformPk
GitHub, Inc. (US)
https://github.com/tianocore/e

EDK II firmware for Intel(R) Quark S platforms

Features

- UEFI firmware image with ability to enable/disable major features such a
  - Logging
  - Source level debug using Intel(R) UEFI Development Kit Debugger
  - Boot Performance Measurements
  - UEFI Secure Boot with Physical Presence
  - TCG Measured Boot using TPM 1.2 hardware devices on I2C bus
- Minimal firmware image for initial power-on and debug
- UEFI Shell built into FLASH image
- UEFI Linux operating system boot support from Micro SD FLASH
- Hardware Support
  - Intel(R) Quark SoC X1000 CPU
  - Intel(R) Galileo Development Board
  - Intel(R) Galileo Gen 2 Development Board
  - HPET Timer
  - Real Time Clock



mdkinney and niruiyu QuarkPlatformPkg: Ren

..

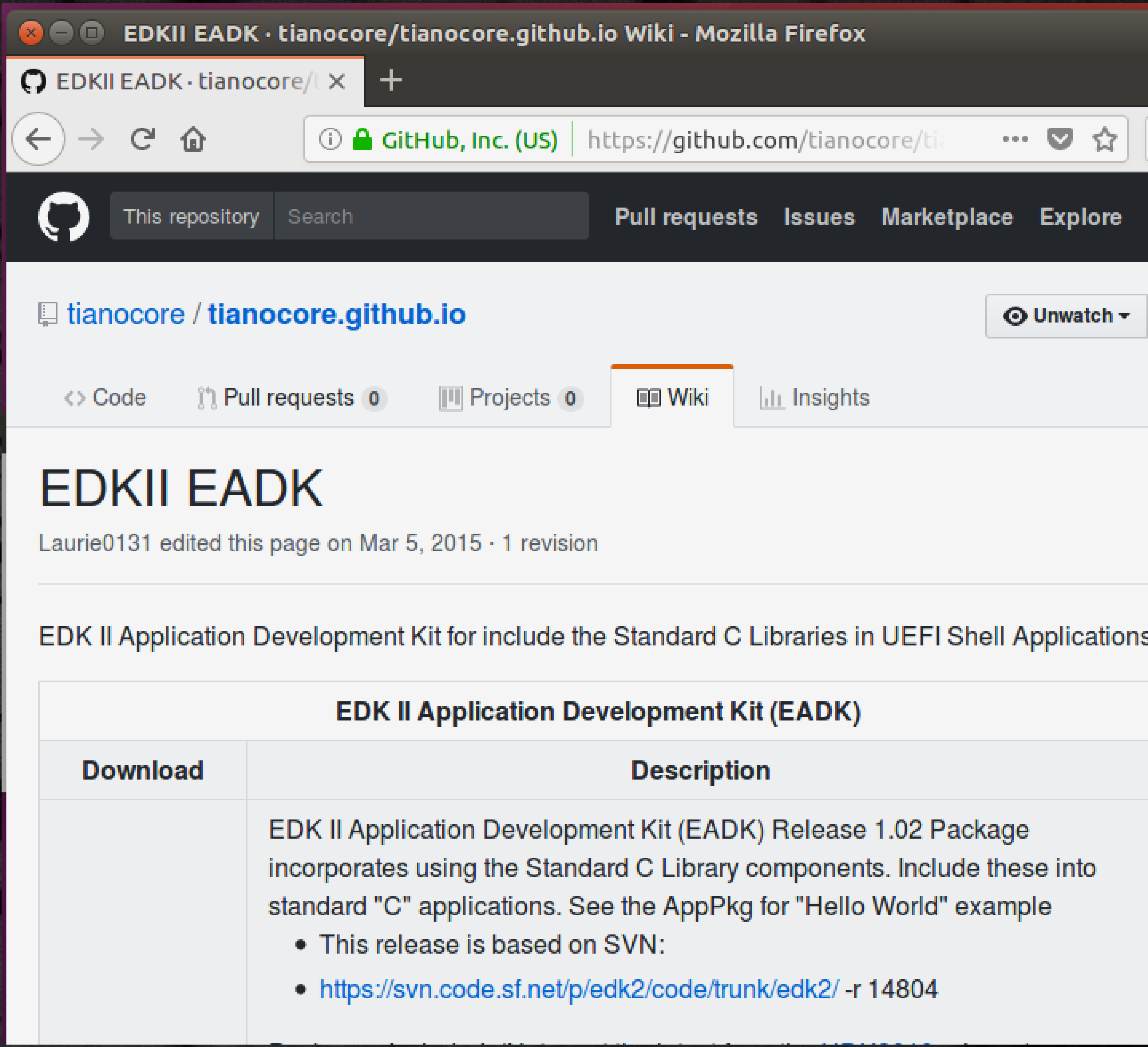
Acpi	Qu
Application/ForceRecovery	Pla
Feature/Capsule	Pla
Include	Qu
Library	Qu
Pci/Dxe	Pla
Platform	Qu
Quark.dsc	Qu
Quark.fdf	Qu
QuarkMin.dsc	Qu
QuarkMin.fdf	Pla
QuarkPlatformPkg.dec	Qu
Readme.md	Pla

EDK II EADK

EDK II Application Development Kit includes the Standard “C” Libraries in UEFI Shell Applications

Link: wiki EADK

Github: edk2-libc



tianocore / tianocore.github.io

EDKII EADK

Laurie0131 edited this page on Mar 5, 2015 · 1 revision

EDK II Application Development Kit for include the Standard C Libraries in UEFI Shell Applications

EDK II Application Development Kit (EADK)	
Download	**Description**
	EDK II Application Development Kit (EADK) Release 1.02 Package incorporates using the Standard C Library components. Include these into standard "C" applications. See the AppPkg for "Hello World" example • This release is based on SVN: • https://svn.code.sf.net/p/edk2/code/trunk/edk2/ -r 14804

tianocore

EDK II EADK COMPONENTS

EDK II Application Development Kit includes the Standard C Libraries in UEFI Shell Applications

● Components

- Utilities (Python 2.7.2, & 2.7.10 etc.)
- C Library
- BSD Socket Library
- Network Socket Library – Ipv4 / Ipv6

● Packages `/AppPkg`
`/StdLib`

tianocore

EDK II EADK – STANDARD ANSI C LIBRARY

FreeBSD Port

ANSI/POSIX compliant

System I/O	- open(), read(), write(), close(), stat()
Standard I/O	- fopen(), printf(), gets(), getchar(),. . .
String/Char	- strcmp(), isascii(), atoi(), . . .
Memory	- malloc(), free(), realloc(),. . .
Time/Date	- time(), asctime(), ctime(), . . .
Math	- sqrt(), pow(), sin(), log(), . . .