Security of BIOS/UEFI System Firmware from Attacker and Defender Perspectives

Miscellaneous Training Materials

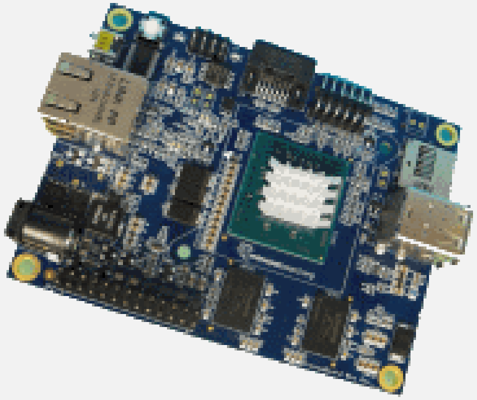
Yuriy Bulygin *
Alex Bazhaniuk *
Andrew Furtak *
John Loucaides **

* Advanced Threat Research, McAfee
** Intel

License

MinnowMax Platform and EDKII

MinnowMax



Open hardware platform

Baytrail single or dual core

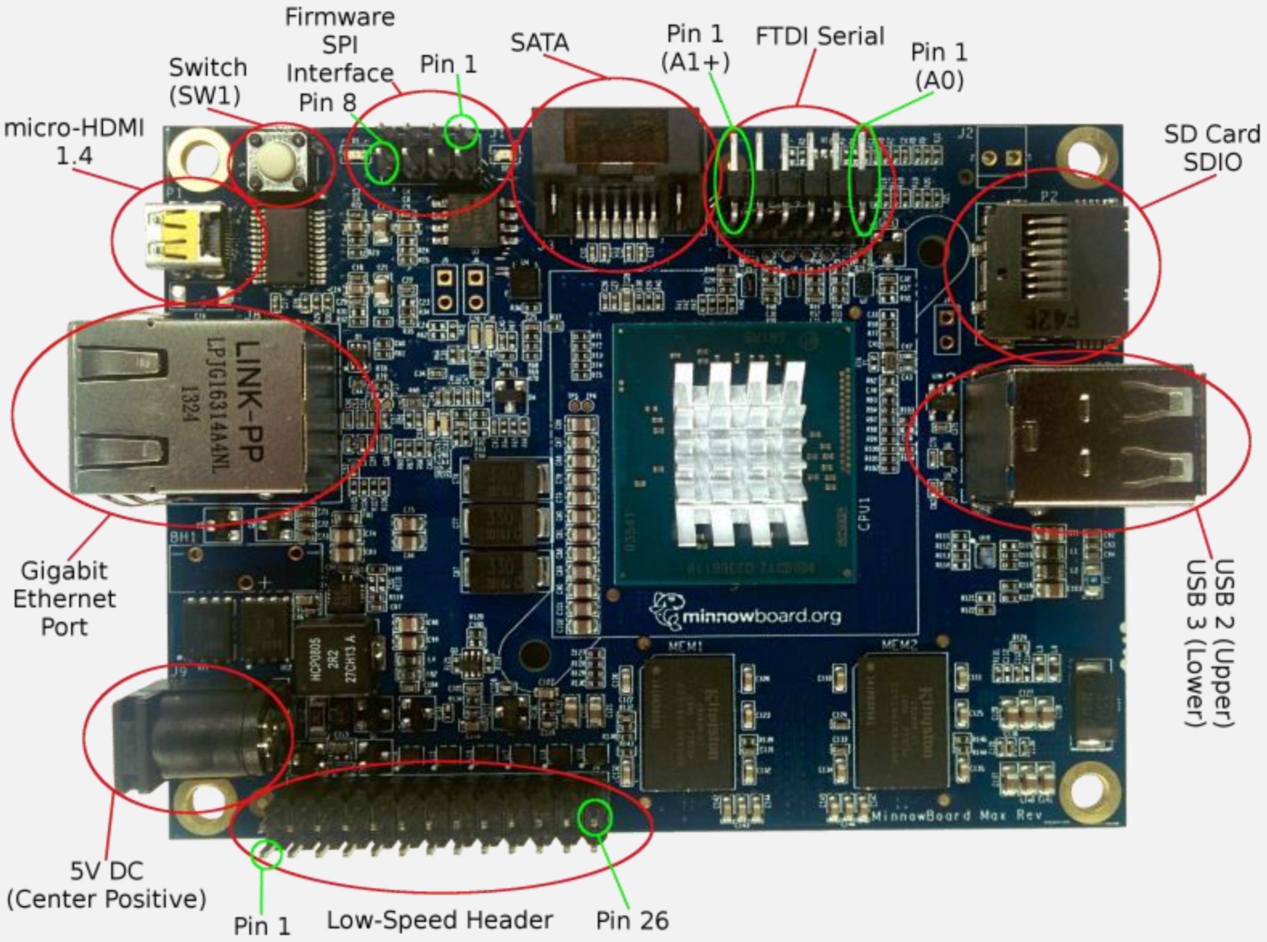
From http://firmware.intel.com/projects

This project focus in on the firmware source code (and binary modules) required to create the boot firmware image for the MinnowBoard MAX. The UEFI Open Source (EDKII project) packages for MinnowBoard MAX are available at http://tianocore.sourceforge.net/wiki/EDK2. To learn more about getting involved in the UEFI EDKII project visit the How to Contribute page.

The source code builds using Microsoft Visual Studios and GNU C Compiler (for both 32 and 64 bit images) - production and debug execution environments. The source code builds the same UEFI firmware image shipping on MinnowBoard MAX.

- See more at: http://firmware.intel.com/projects#sthash.1oOc8srY.dpuf

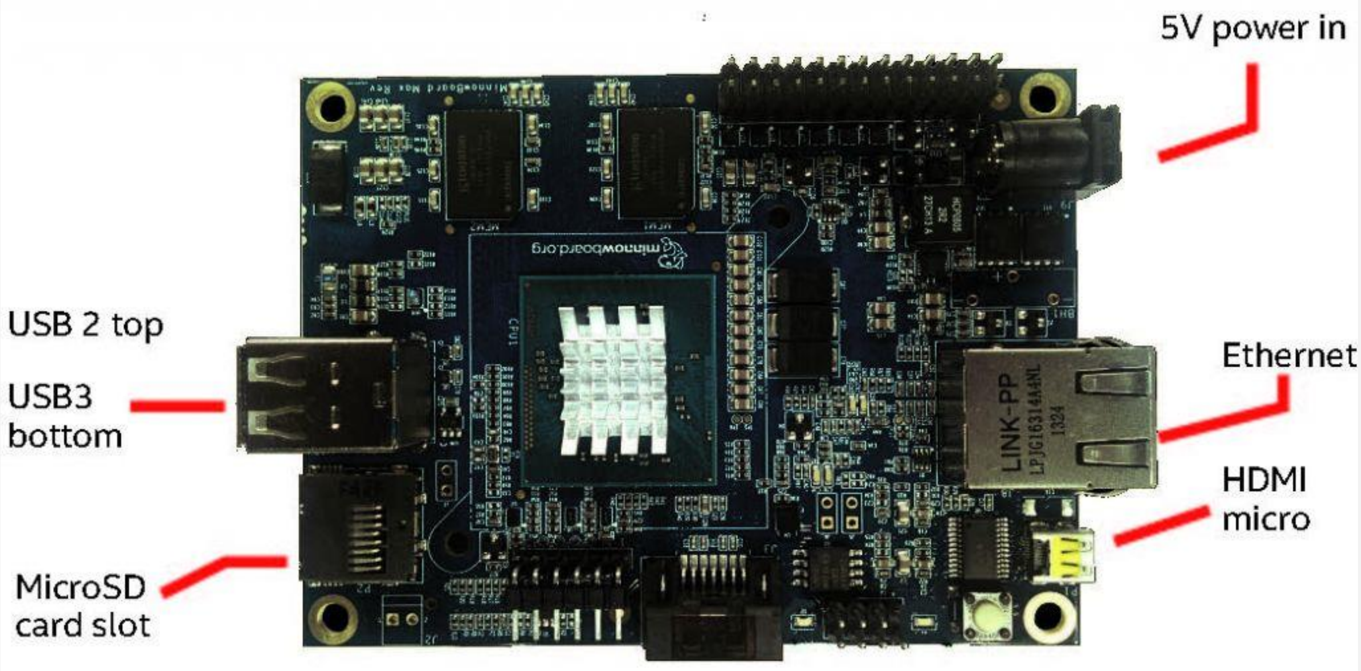
MinnowBoard Interfaces



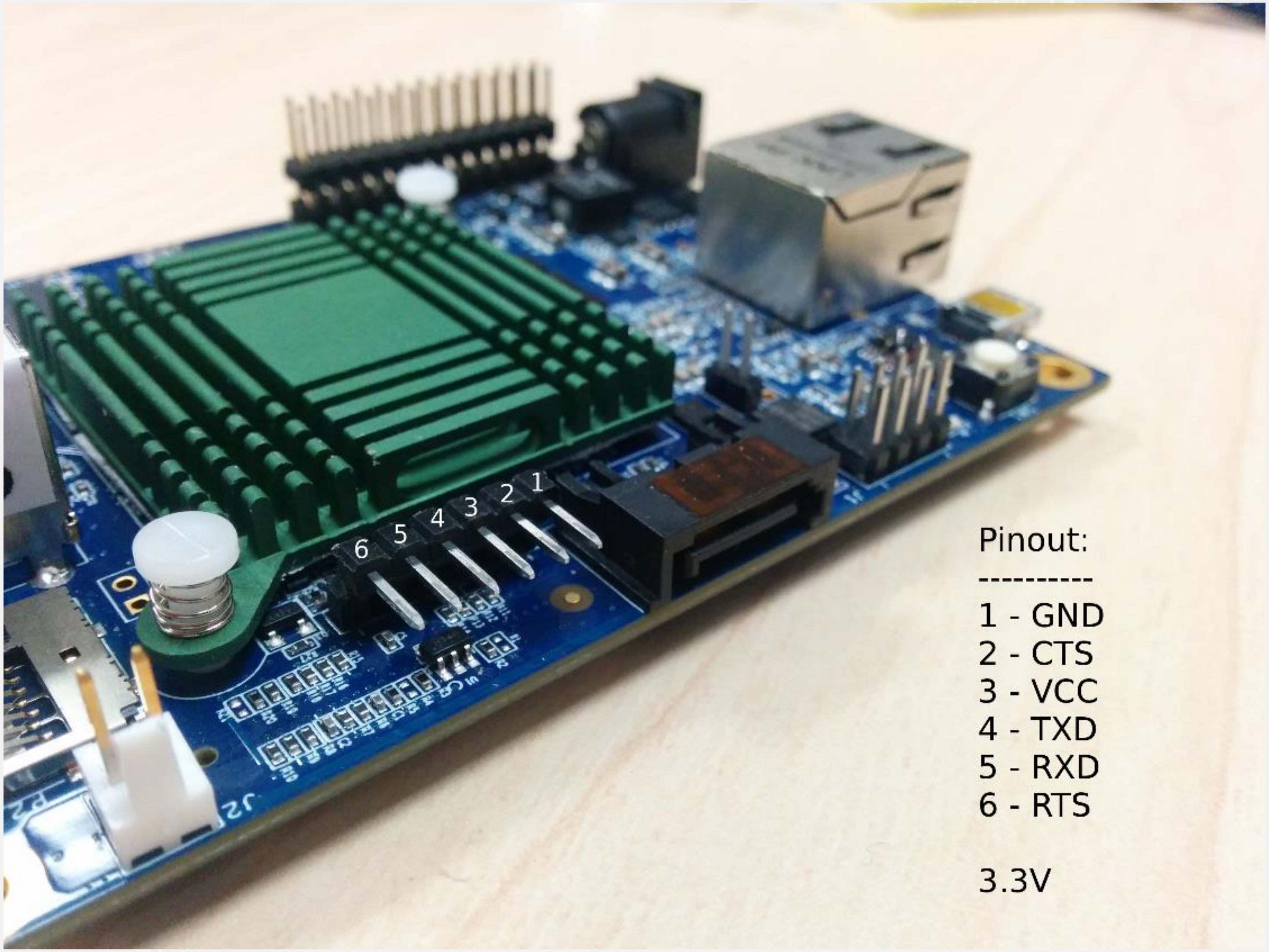
Source: https://01.org/android-ia/guides/android-5.x-lollipop-bring-guide

USB Ports in MinnowBoard

2 USB ports: USB3 on bottom and USB2 on top



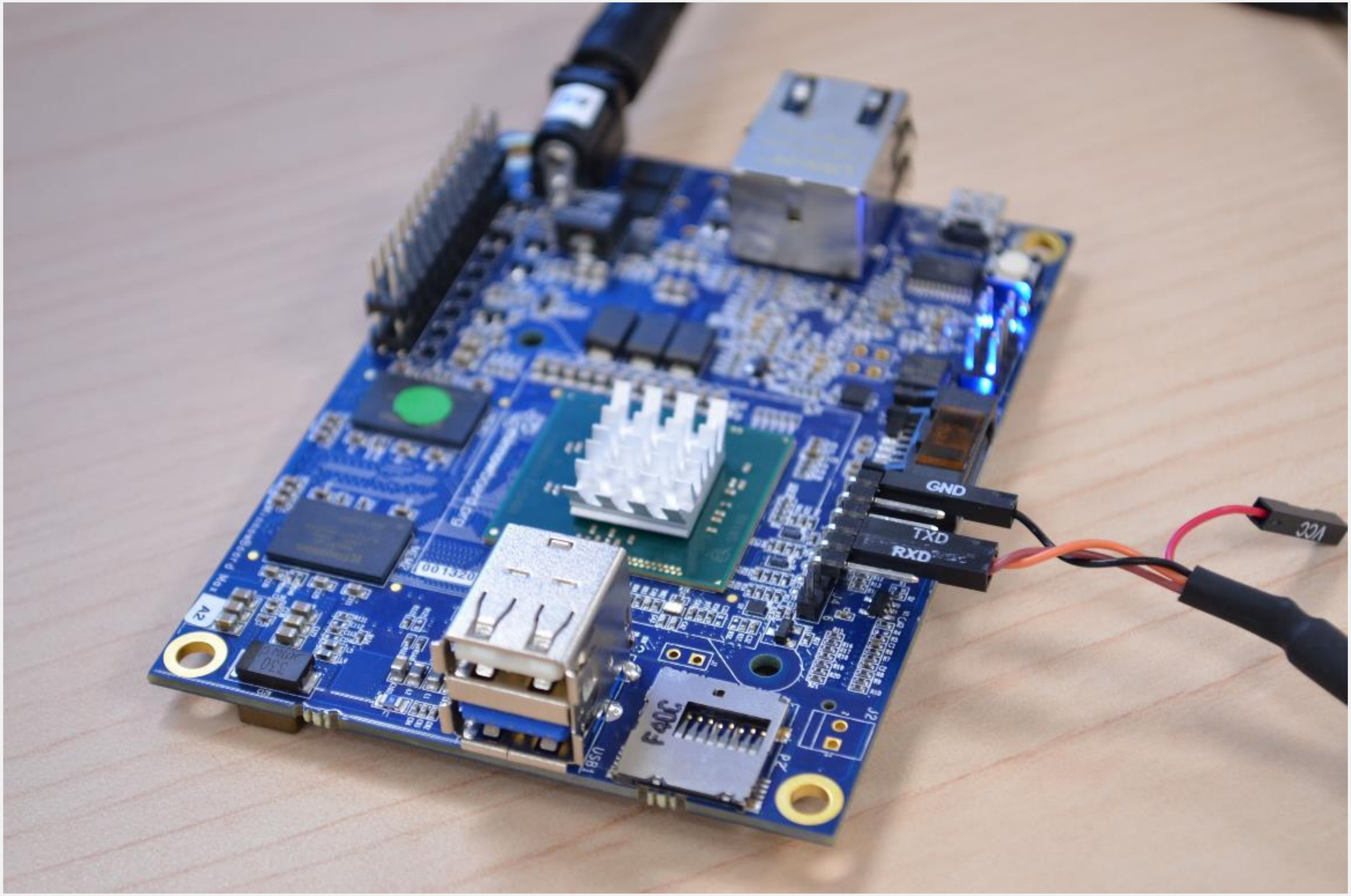
UART Pinout Configuration



Pinout:
----
1 - GND
2 - CTS
3 - VCC
4 - TXD
5 - RXD
6 - RTS

3.3V

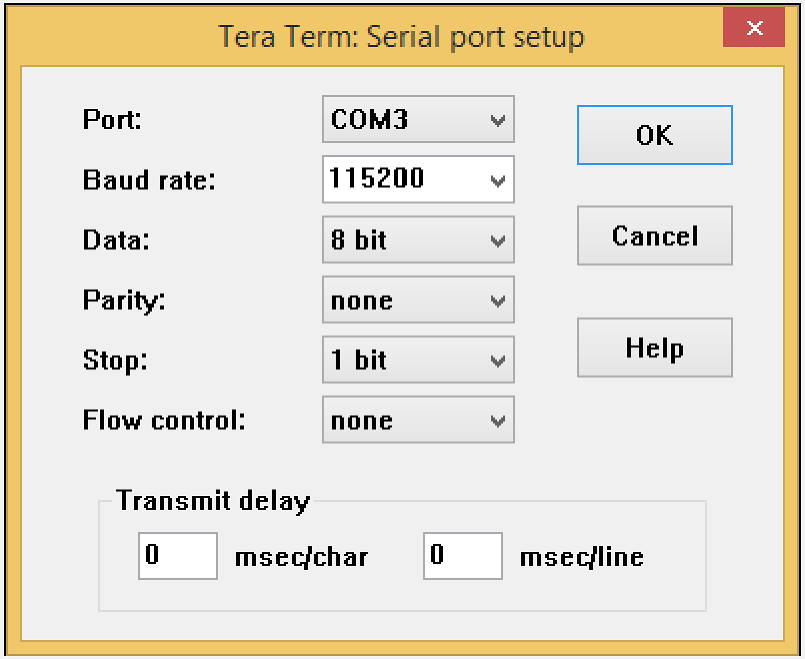
Connect to UART port



UART configuration

Baud rate - 115200

Flow control - 0



Tera Term: Serial port setup

Port: COM3

Baud rate: 115200

Data: 8 bit

Parity: none

Stop: 1 bit

Flow control: none

Transmit delay

0 msec/char

0 msec/line

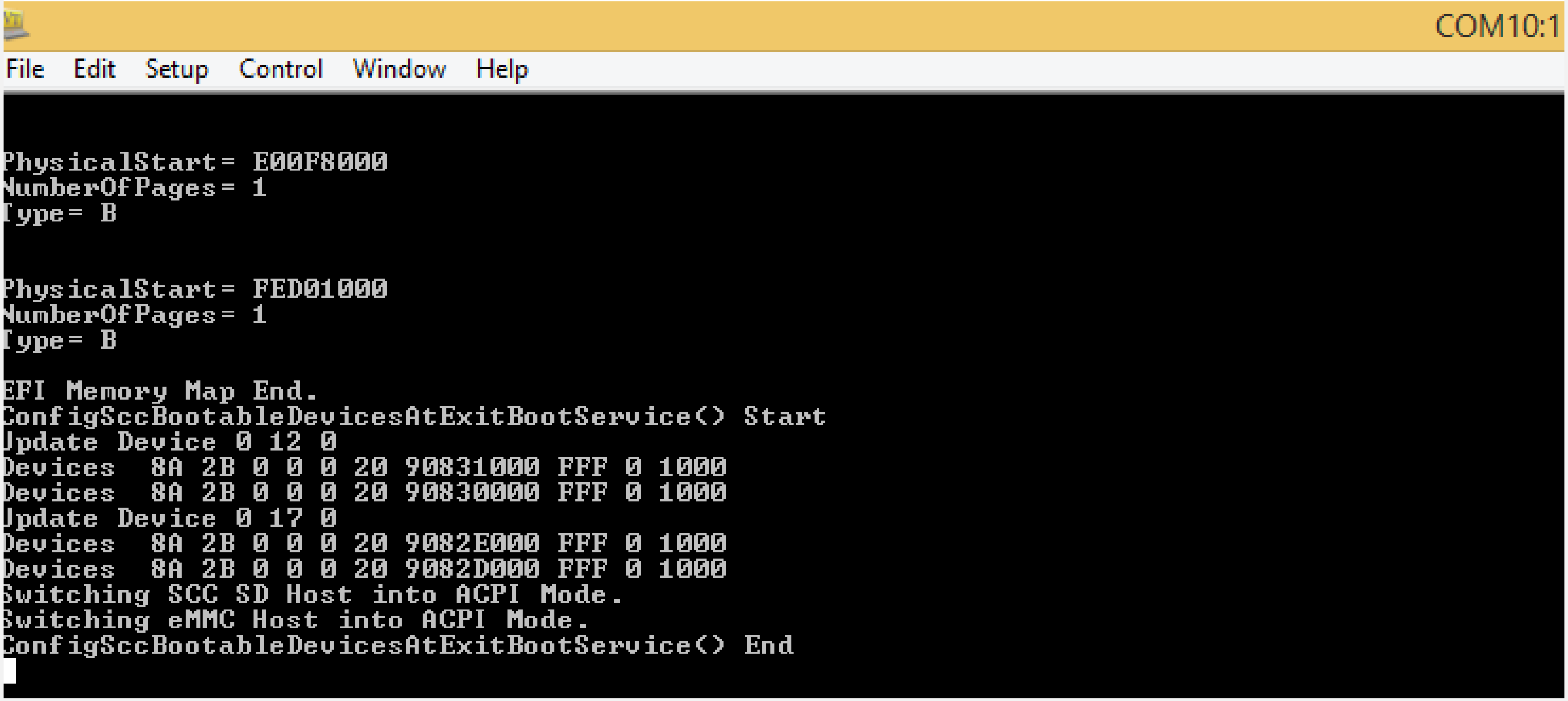
To read UART output

On Windows use: PUTTY or Tera Term

On Linux run minicom:

```
$minicom -D /dev/ttyUSB0
```

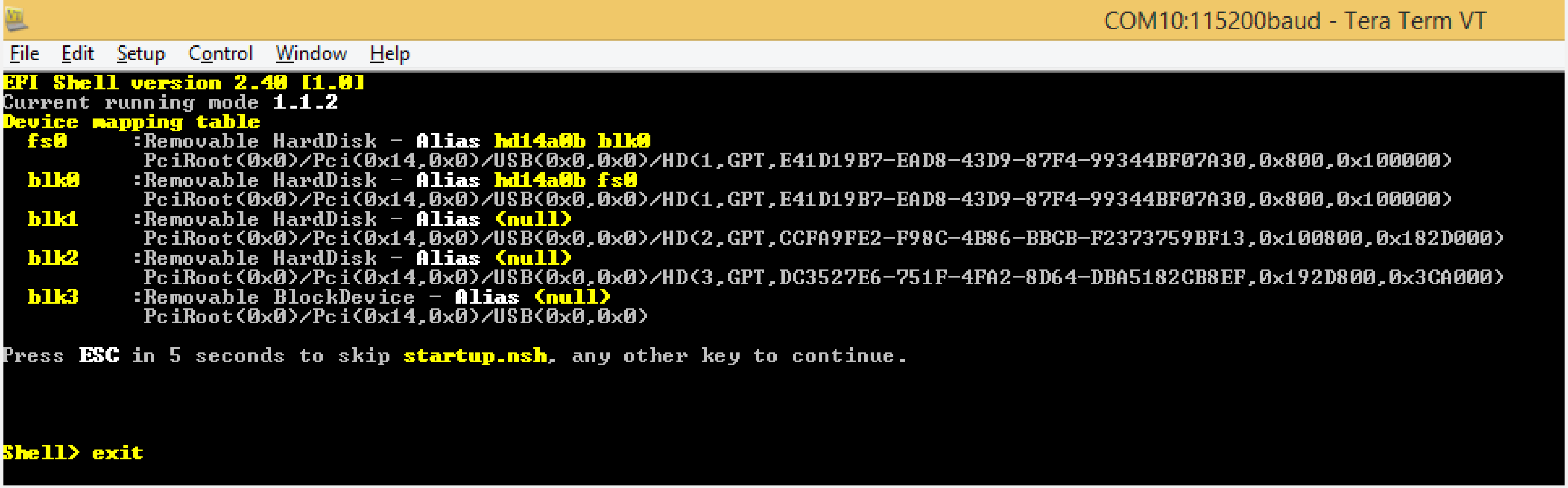
Successfully launch Linux



```
PhysicalStart= E00F8000
NumberOfPages= 1
Type= B


PhysicalStart= FED01000
NumberOfPages= 1
Type= B

EFI Memory Map End.
ConfigSccBootableDevicesAtExitBootService() Start
Update Device 0 12 0
Devices  8A 2B 0 0 0 20 90831000 FFF 0 1000
Devices  8A 2B 0 0 0 20 90830000 FFF 0 1000
Update Device 0 17 0
Devices  8A 2B 0 0 0 20 9082E000 FFF 0 1000
Devices  8A 2B 0 0 0 20 9082D000 FFF 0 1000
Switching SCC SD Host into ACPI Mode.
Switching eMMC Host into ACPI Mode.
ConfigSccBootableDevicesAtExitBootService() End
```

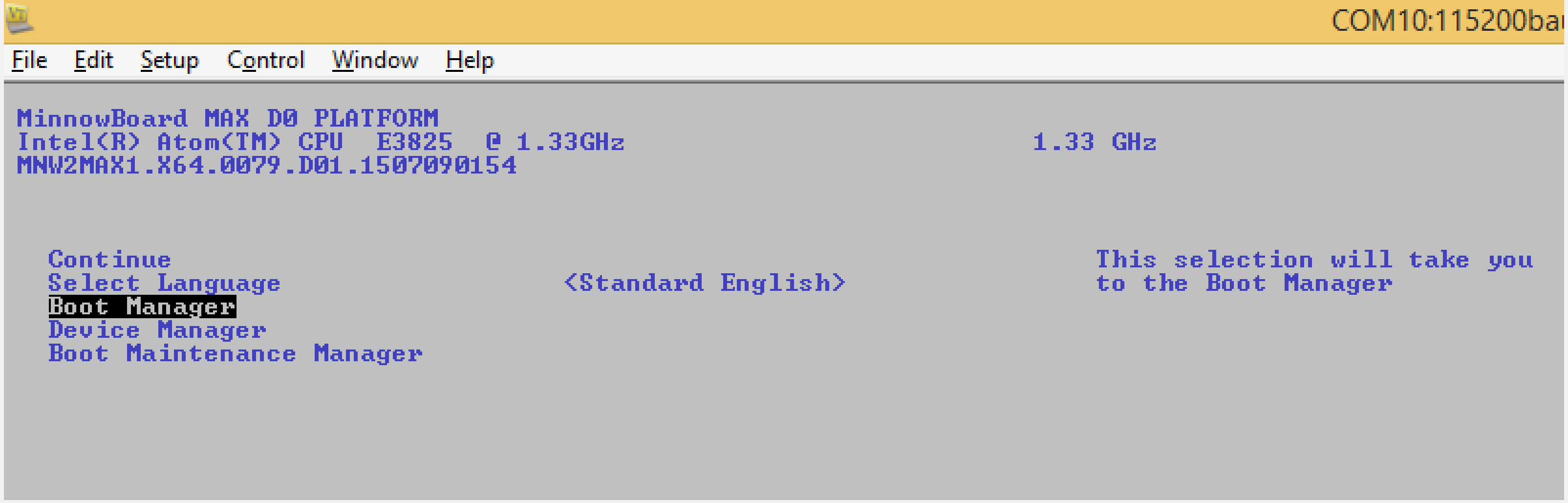
UEFI shell

For come to Setup Screen type `exit` & **enter** in the UEFI shell:

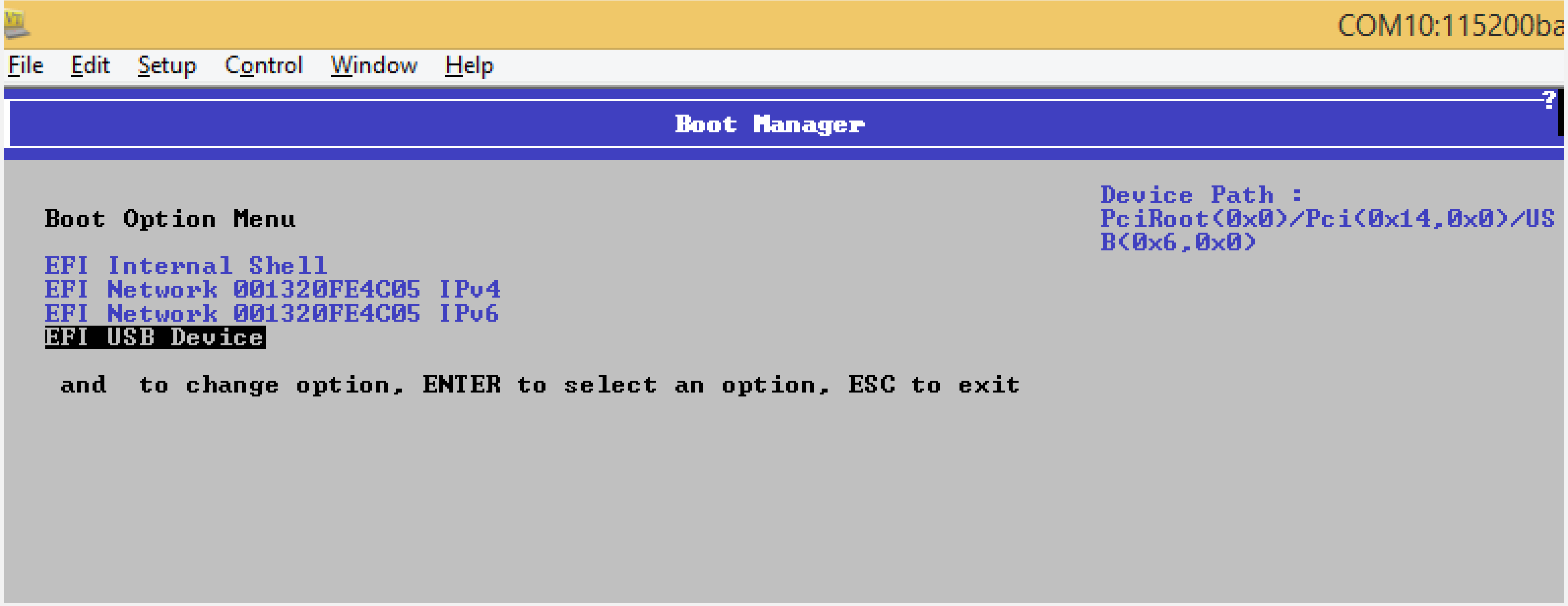


```
EFI Shell version 2.40 [1.0]
Current running mode 1.1.2
Device mapping table
  fs0      :Removable HardDisk - Alias hd14a0b blk0
           PciRoot(0x0)/Pci(0x14,0x0)/USB(0x0,0x0)/HD(1,GPT,E41D19B7-EAD8-43D9-87F4-99344BF07A30,0x800,0x100000)
  blk0     :Removable HardDisk - Alias hd14a0b fs0
           PciRoot(0x0)/Pci(0x14,0x0)/USB(0x0,0x0)/HD(1,GPT,E41D19B7-EAD8-43D9-87F4-99344BF07A30,0x800,0x100000)
  blk1     :Removable HardDisk - Alias (null)
           PciRoot(0x0)/Pci(0x14,0x0)/USB(0x0,0x0)/HD(2,GPT,CCFA9FE2-F98C-4B86-BBCB-F2373759BF13,0x100800,0x182D000)
  blk2     :Removable HardDisk - Alias (null)
           PciRoot(0x0)/Pci(0x14,0x0)/USB(0x0,0x0)/HD(3,GPT,DC3527E6-751F-4FA2-8D64-DBA5182CB8EF,0x192D800,0x3CA000)
  blk3     :Removable BlockDevice - Alias (null)
           PciRoot(0x0)/Pci(0x14,0x0)/USB(0x0,0x0)

Press ESC in 5 seconds to skip startup.nsh, any other key to continue.



Shell> exit
```

Boot from USB Device



```
MinnowBoard MAX D0 PLATFORM
Intel(R) Atom(TM) CPU  E3825  @ 1.33GHz                         1.33 GHz
MNW2MAX1.X64.0079.D01.1507090154


  Continue                                                          This selection will take you
  Select Language                   <Standard English>              to the Boot Manager
  Boot Manager
  Device Manager
  Boot Maintenance Manager
```



```
                                     Boot Manager

                                                                   Device Path :
  Boot Option Menu                                                 PciRoot(0x0)/Pci(0x14,0x0)/US
                                                                   B(0x6,0x0)
  EFI Internal Shell
  EFI Network 001320FE4C05 IPv4
  EFI Network 001320FE4C05 IPv6
  EFI USB Device

   and  to change option, ENTER to select an option, ESC to exit
```

MinnowBoard Configuration

Students need to configure Ethernet card in laptops with `192.168.1.1/24` IP address

Access to MinnowBoard board through SSH (`22` port).

Recommended clients: PUTTY, MobaXterm

MinnowBoard Network configuration:

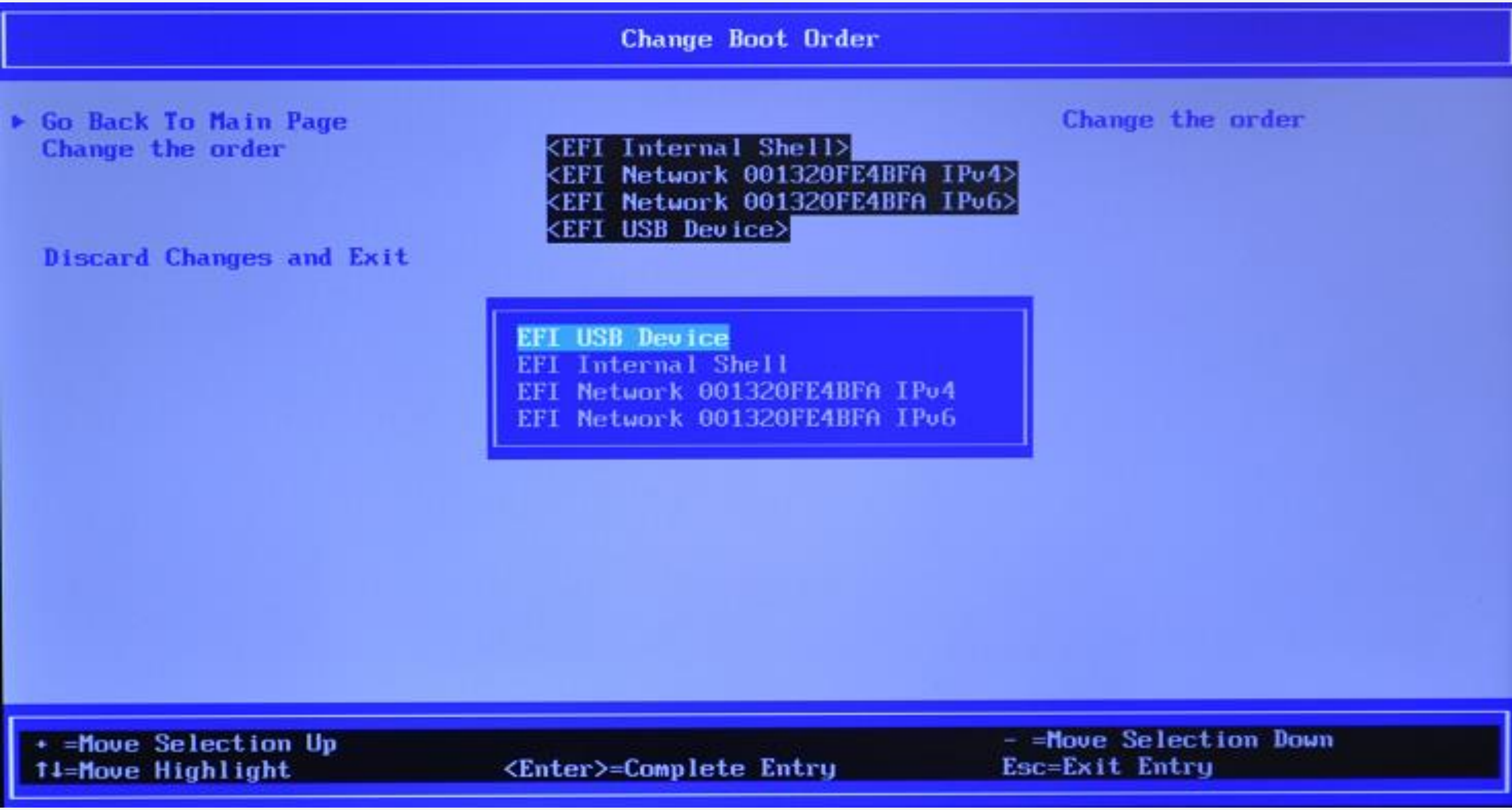
```
IP address: 192.168.1.2

Gateway:    192.168.1.1
```

MinnowBoard File System

~/Desktop/bios	- MinnowBoard EDK2 FW sources
~/Desktop/chipsec	- CHIPSEC framework
~/Desktop/image	- binary BIOS images
~/Desktop/udk-debugger	- udk-debugger installer & config
~/Desktop/patches	- BIOS patches
~/Desktop/tools	- misc useful BIOS/UEFI utilities
~/Desktop/exercises	- materials for exercises

Useful UEFI Setup Options

Changing Boot Order On MinnowMax



Change Boot Order

▶ Go Back To Main Page
Change the order

<EFI Internal Shell>
<EFI Network 001320FE4BFA IPv4>
<EFI Network 001320FE4BFA IPv6>
<EFI USB Device>

Discard Changes and Exit

Change the order

EFI USB Device
EFI Internal Shell
EFI Network 001320FE4BFA IPv4
EFI Network 001320FE4BFA IPv6

+ =Move Selection Up
↑↓=Move Highlight
<Enter>=Complete Entry
- =Move Selection Down
Esc=Exit Entry

Training materials are available on Github

https://github.com/advanced-threat-research/firmware-security-training

Yuriy Bulygin	@c7zero
Alex Bazhaniuk	@ABazhaniuk
Andrew Furtak	@a_furtak
John Loucaides	@JohnLoucaides