Libreboot

freedom und *privacy*
von Kopf bis Fuss?

If you can't hack it

You don't own it.

Who **owns / controls** your computer ?

free software

The freedom to:

(0) **run** the program for any purpose you want.

(1) **study** how the program works, and change it to make it do what you wish.

(2) **redistribute** and make copies so you can help your neighbor.

(3) **improve** the program, and release your improvements (and modified versions in general) to the public, so that the whole community benefits.

freedom 1 & 3 = source code !!!

... to make copies
so you can
help your neighbor.

philosophical

improve the program,
and release
your improvements
(and modified versions in general)
to the public, **so that**
the whole community benefits.

free software
(>) !! (==)
open source

study the source code and know what the program does

verschiedene
Lizenzen

practical

open source

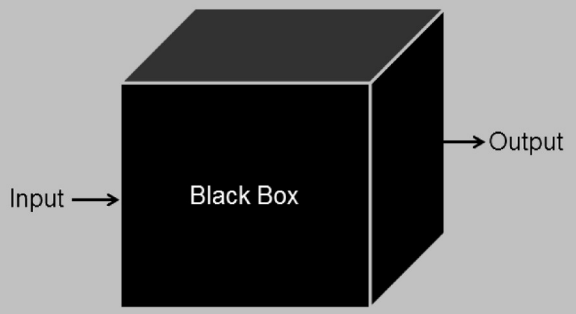
trusted

secure

trustworthy

trust

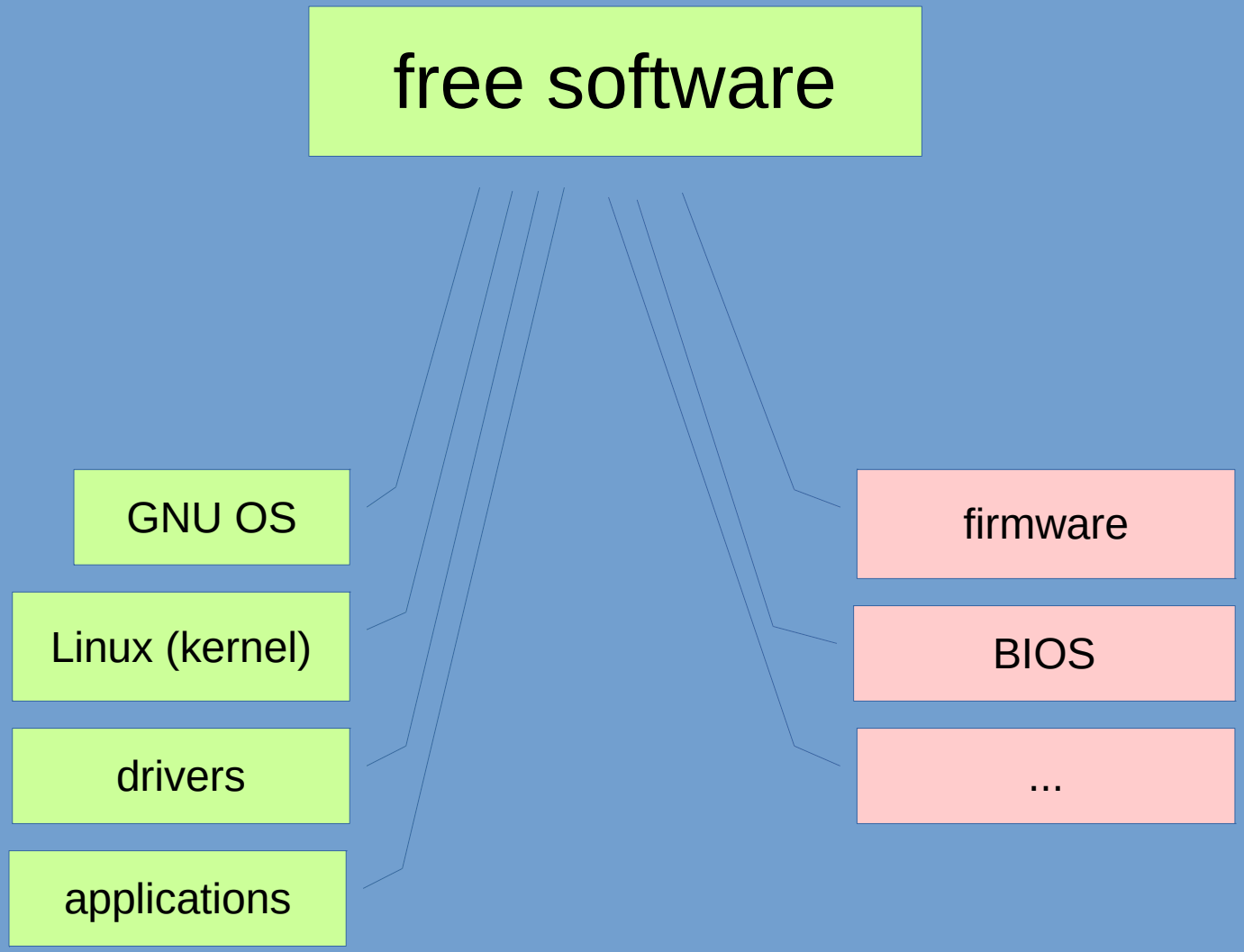
free software
open source



Internal behavior of the code is unknown

impossible to know what it does

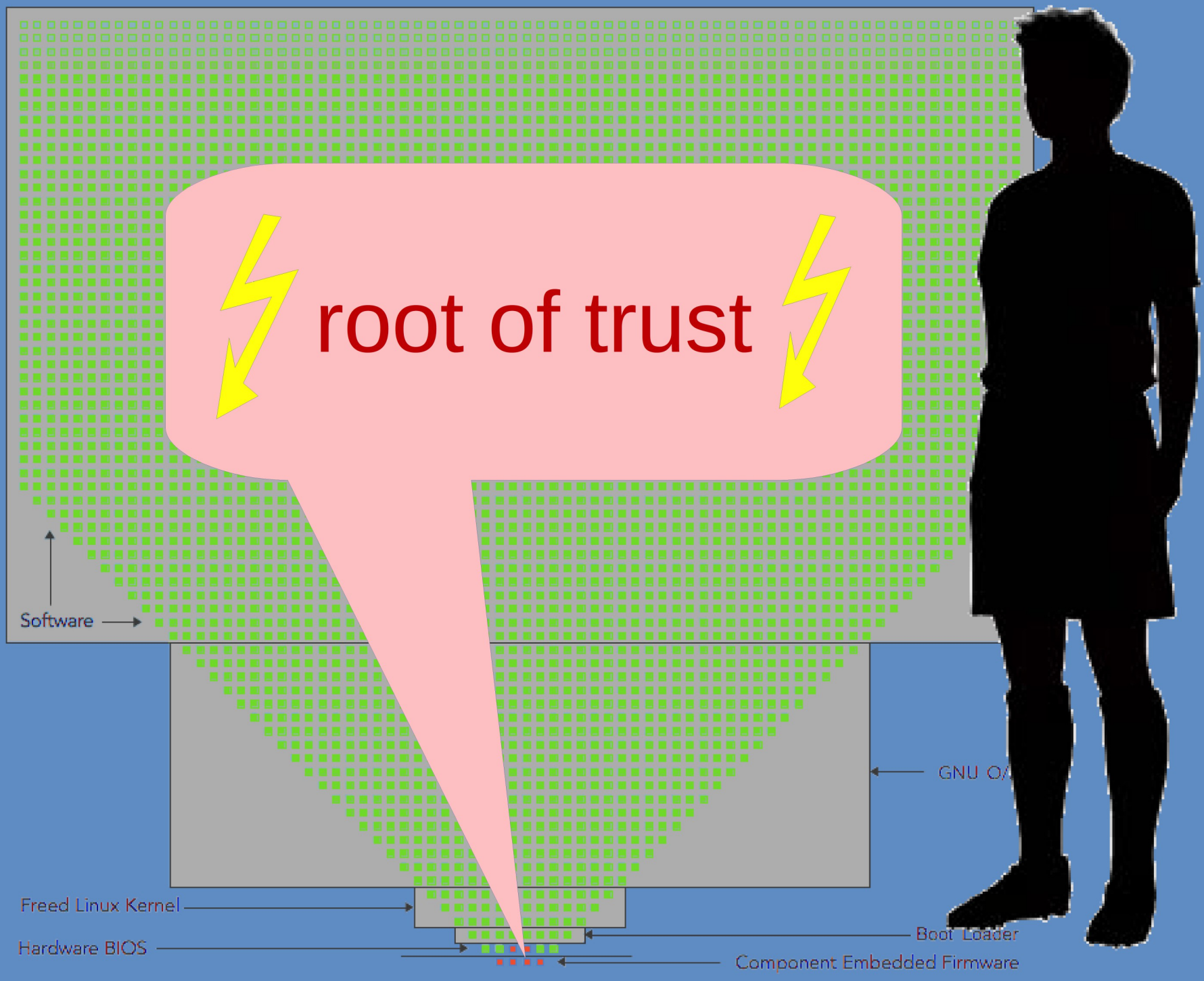
proprietary software
closed source

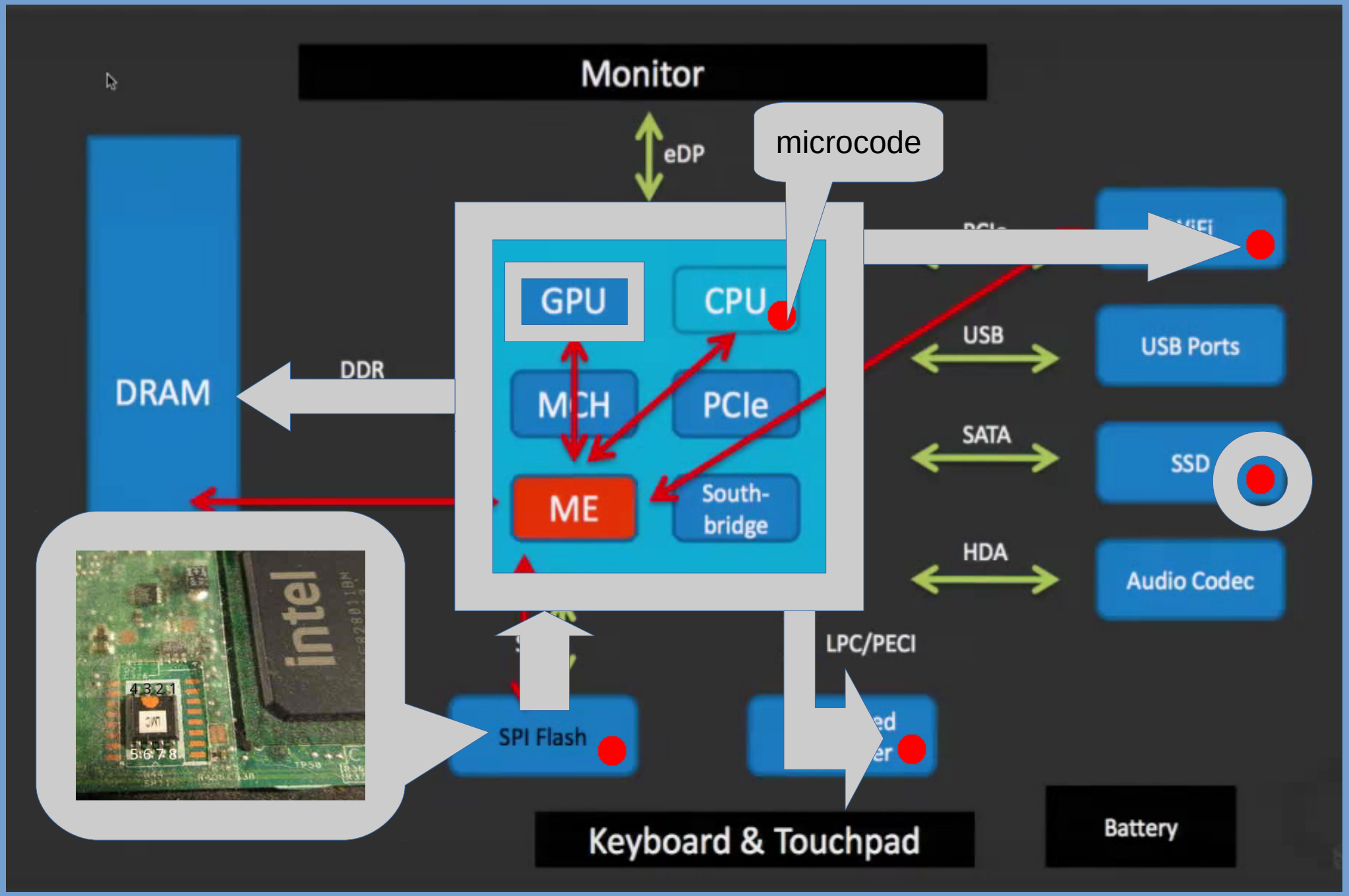

free software
GNU OS
Linux (kernel)
drivers
applications
firmware
BIOS
...

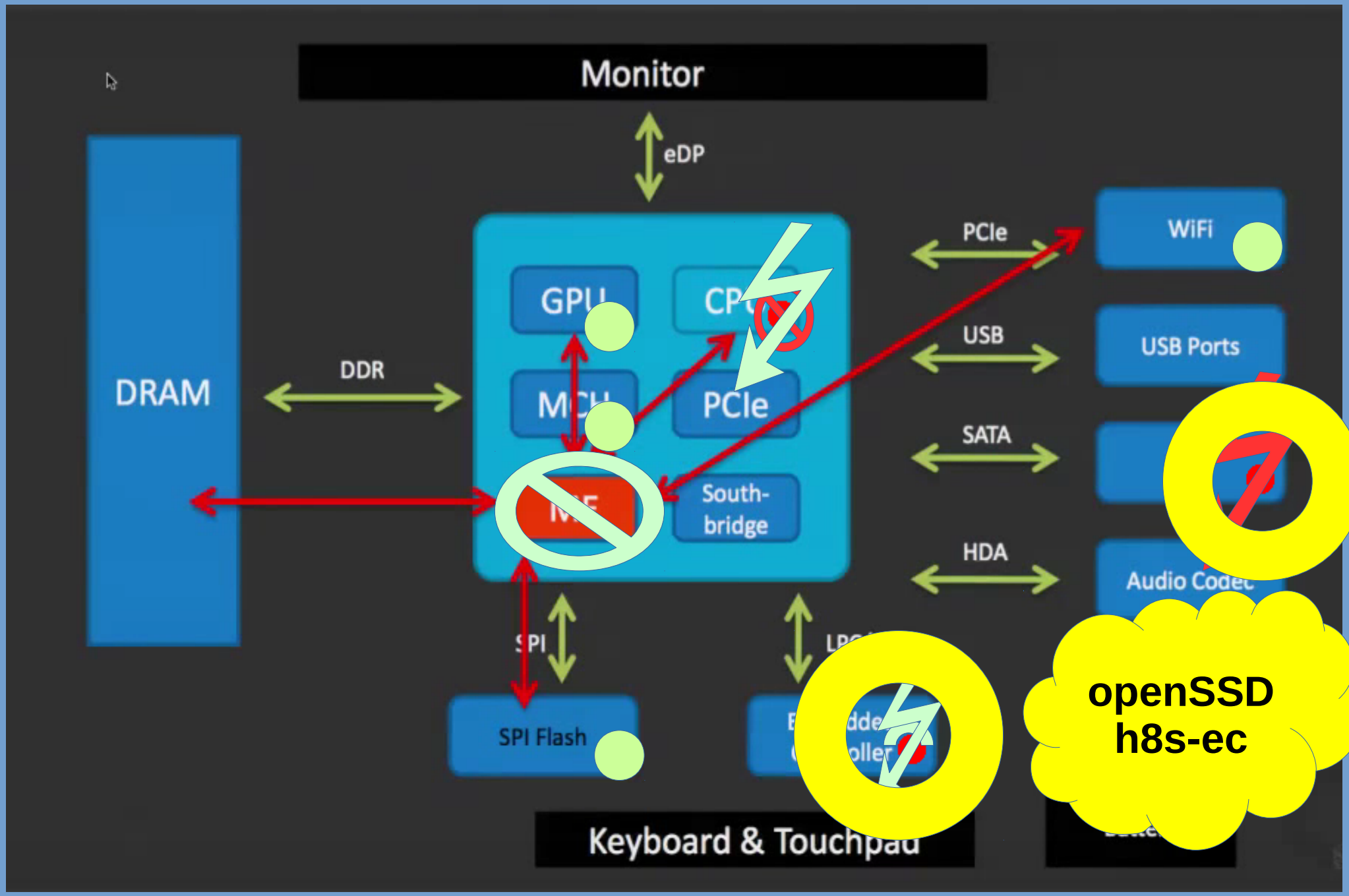
Purism Librem 15 Laptop: Graphical representation relative to size of the completely freed kernel, operating system, and all software applications.

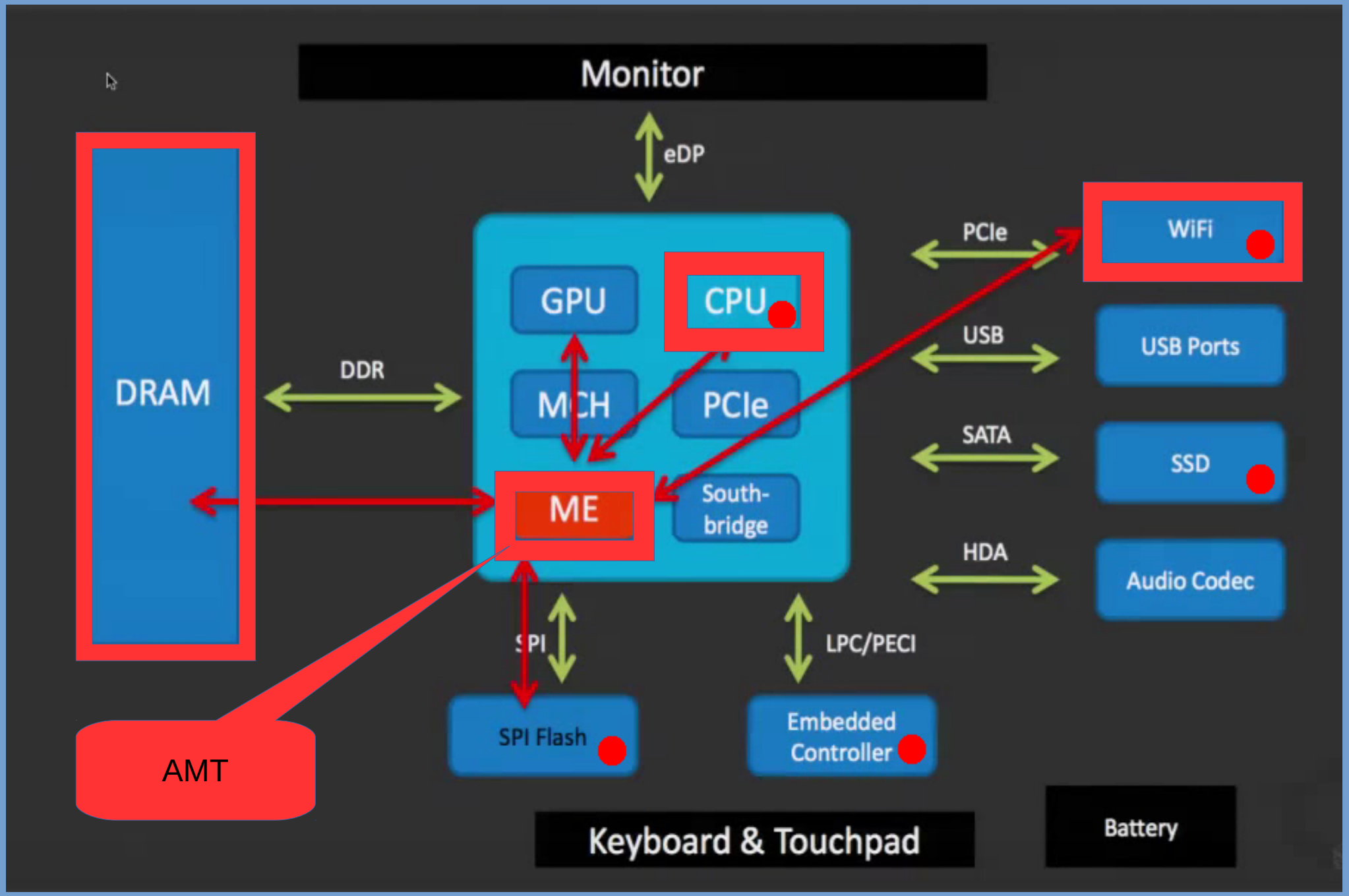
Completely Freed
Binary Firmware

Purism Laptop




Monitor
eDP
microcode
DRAM
DDR
GPU
CPU
MCH
PCIe
ME
South-
bridge
USB
USB Ports
SATA
SSD
HDA
Audio Codec
LPC/PECI
SPI Flash
Keyboard & Touchpad
Battery
intel
4 3 2 1
5 6 7 8


Monitor
eDP
DRAM
DDR
GPU
CPU
MCH
PCIe
ME
South-
bridge
PCIe
USB
SATA
HDA
WiFi
USB Ports
Audio Codec
SPI
SPI Flash
Keyboard & Touchpad
openSSD
h8s-ec


Monitor
eDP
DRAM
DDR
GPU
CPU
MCH
PCIe
ME
South-
bridge
PCIe
WiFi
USB
USB Ports
SATA
SSD
HDA
Audio Codec
SPI
LPC/PECI
SPI Flash
Embedded
Controller
AMT
Keyboard & Touchpad
Battery

Intel ME

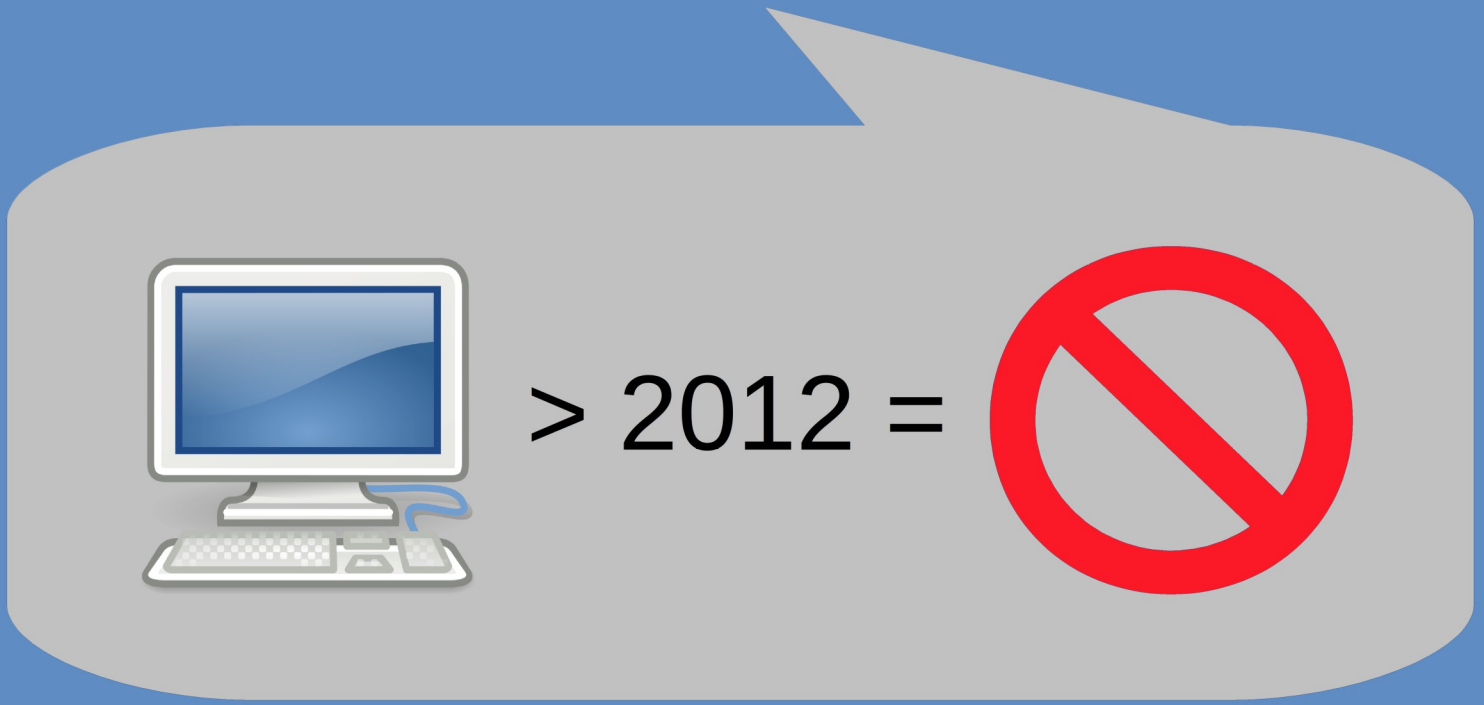
- 2006: separate computing environment (can be disabled)
- 2009: integrate Core i3/i5/i7 (can't be disabled)

> 2008 =

- firmware
- computer min
- no cooperation from Intel

AMD PSP

- Private Security Platform = Intel ME on AMD
- Introduced in 2013
- same issues: cryptographically signed / system refuses to boot / cannot be disabled



arm
(Chromebooks ...)

OpenPOWER
(server, desktop)

OPEN HARDWARE !!!

This is as close as you can get to free software

Richard Stallmann

levels of privacy

0	**Windows / Mac OS X**
1	**Standard-GNU/Linux (Ubuntu, SuSE, LinuxMint, Debian ...)**
2	**Freies GNU/Linux (Trisquel, GnewSense, Parabola ...)**
3	**Coreboot**
4	**Libreboot**
5	**Gehärteter Hacker-Computer**

SeaBIOS
(legacy, e.g. Windows)

CoreBoot + payload (e.g. GRUB)
(minimal init, Linux)

binary
blobs

Coreboot

=

free BIOS

Libreboot

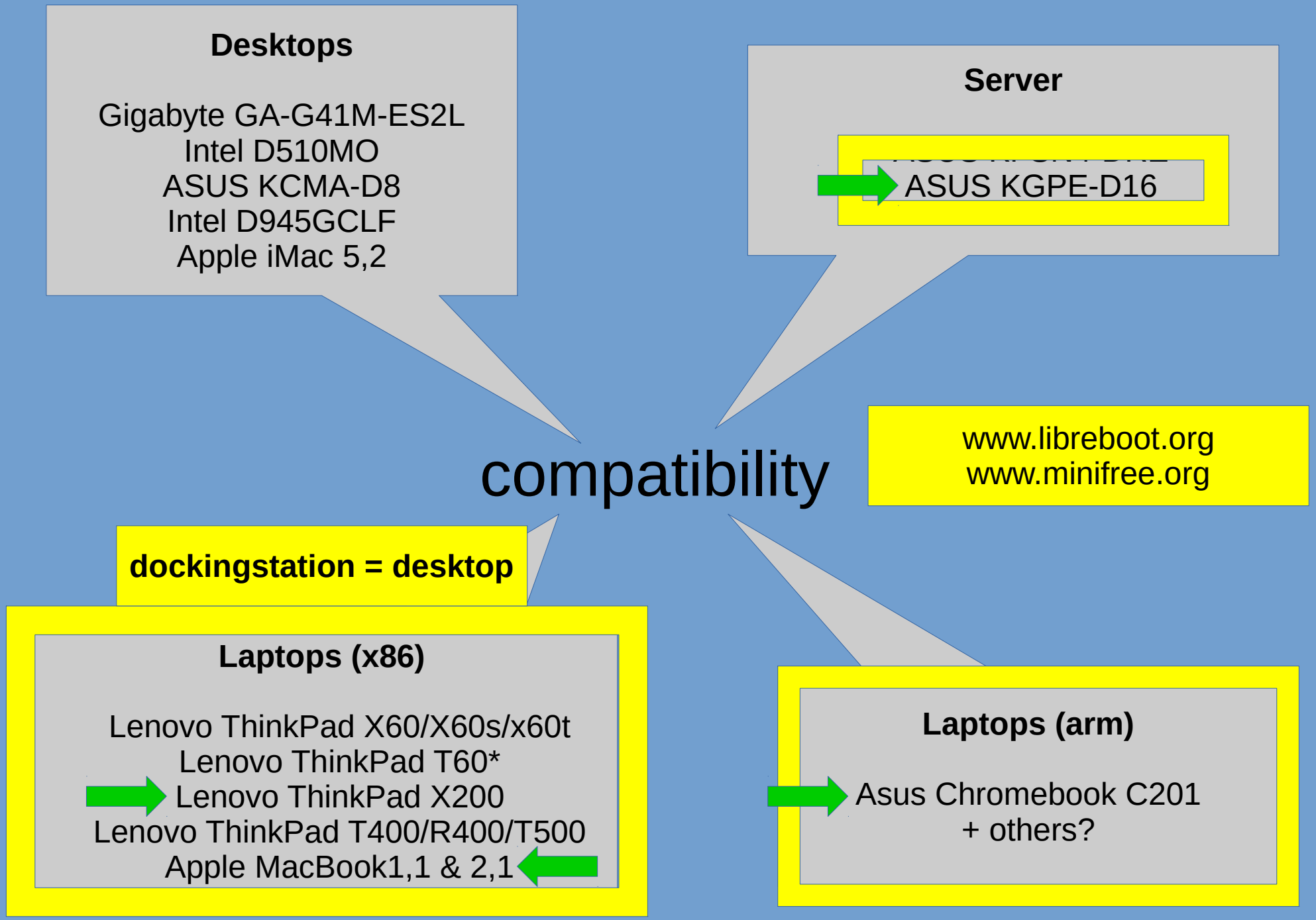
100%

"free distribution"

fast
configurable

many systems
binary blobs
complicated

few systems
100% free
precompiled images


Desktops
Gigabyte GA-G41M-ES2L
Intel D510MO
ASUS KCMA-D8
Intel D945GCLF
Apple iMac 5,2
Server
ASUS KGPE-D16
compatibility
www.libreboot.org
www.minifree.org
dockingstation = desktop
Laptops (x86)
Lenovo ThinkPad X60/X60s/x60t
Lenovo ThinkPad T60*
Lenovo ThinkPad X200
Lenovo ThinkPad T400/R400/T500
Apple MacBook1,1 & 2,1
Laptops (arm)
Asus Chromebook C201
+ others?

Best option for
a modern & stylish
laptop !

romebook C201

11.6" 16:9 HD (1366x768)
Rockchip Quad-Core RK3288C Processor
OnBoard Memory 2 GB / 4 GB
16GB eMMC
card reader (Micro SD/SDXC/SDHC)
HD Web Camera
Integrated 802.11 a/b/g/n/ac
Built-in Bluetooth™ V4.0
1 x COMBO audio jack / 2 x USB 2.0 / 1 x micro HDMI
287 x 194 x 17.9 mm (WxDxH)
0.98 kg (with Polymer Battery)

recommended

lightweight / beautiful / only model with 4 cores / free EC firmware
computing power? / SSD capacity? / flashing? / wifi dongle
sold by: www.minifree.org

Best option to
run a free
tor node !

pad x60/x60s

Intel Core Duo processor L2300 (1.5Ghz) /
T2300(1.66GHz) / T2400(1.83GHz)
Memory 2GB (evtl. 4 GB)
12" display (1024 x 768)
32-bit system
small & lightweight
docking station (DVD-RW, but only vga)

=> partial compatibility for tablets

generally not recommended

old / bad display / computing power?
easy to flash (internally)
=> can be used to run a tor node (instead of RPi)

Best option if you don't want to flash externally !

cbook 2,1

partially recomm ed

beautiful / good display / touchpad computing power?
polycarbonat case? / runs hot under Libreboot / keyboard?
iSight not compatible / wifi compatible out of the box (Atheros)
easy to flash (internally)

ad T400 / T500

Best option if you want big screen and some computing power !

I dont like it ...
(heavy, ugly ...)

Intel Core 2 Duo (1.83-2.93 Ghz) – socket!
14"/15" Display (1280 x 800 / 1440x900 // 1680 x 1050 / 1920 x 1200)
[illegible]M
[illegible]emovable (2nd HDD)
[illegible]ressCard/54, VGA
[illegible]SB 2.0, Modem, LAN
4-pin FireWire
Docking station (DVI)

partially recommended

computing power / screen size (quality?) / heavy! / touchpad & trackpoint / webcam works / digital video out?
must be flashed externally & a lot of work (50 screws)!

nkpad x200

Best option of all!
Can be used as
laptop & desktop!

Intel Core 2 Duo (1.2-2.8 Ghz)
12" display (1280 x 800) – crap!
4 GB RAM (8 GB?)
2 x USB 2.0, [illegible]Bus, CardReader, VGA,
[illegible]ng station

vBoe-Hydis:
HV121WX5-100 (glossy)
HV121WX4-110 (glossy)
HV121WX4-120 (matte)
Samsung:
LTN121AP02 FRU 42T0563 (matte)

Don't buy:
x200s
x200t

recommended (best opti [illegible] !

computing power / portability (mesu[illegible]es & weight)
only trackpoint / webcam works / digital video via DP!
must be flashed externally but is relatively easy

X200 – affs/ips-screen

colors
viewing angle
brightness
contrast

"lamp contains mercury"

1:1 re[illegible]ent:

- HV[illegible]X5-10[illegible]
- HV12[illegible]X4-11[illegible]
- HV121[illegible]4-120 (matte)
- LTN121[illegible]02 FRU 42T056[illegible]atte)

change inverter

only CCFL-models
(not possible with led)

problems ...

China

shipping

language

„compatible one“

specifications ?

quality ?

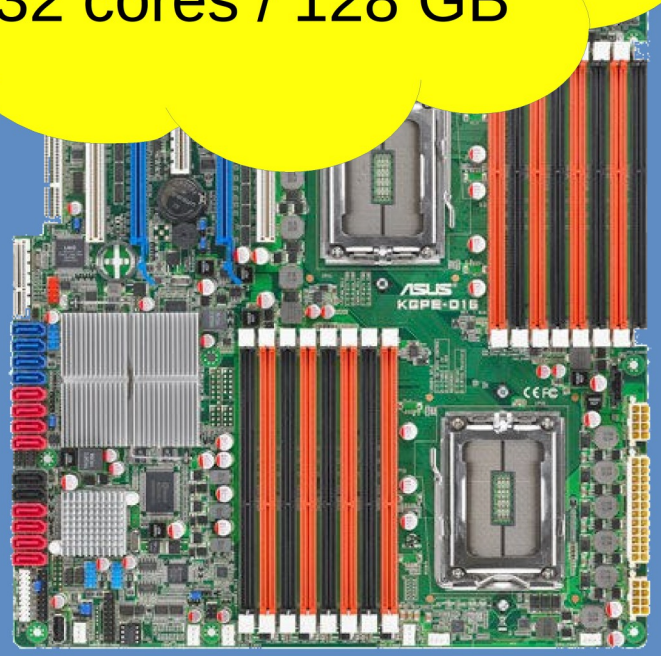
calibration

Colormunki / ArgyllCMS / DisplayCal

=> icc-profile

KPGE-D16

Best option for
server and desktop
32 cores / 128 GB



Socket: 2xG34 - AMD Opteron 6000 series
Memory: DDR3 DIMM 800 - 1333 MHz;
Memory type: ECC/non-ECC
Number of memory slots:
Maximum memory:
0 x IDE: no / 6 x 3
x8, 1xPCI
7 USB, 1xFireWire (IEEE1394a), 2xCOM, D-Sub,
2xEthernet, PS/2 (keyboard), PS/2 (mouse);
Main power connector: 24-pin;
Processor power connector: 8-pin + 8-pin;
Form factor: S

6200 recommended

instable > 128 GB

recommended

power (up to 2x16 cores) / memory (up to 128 GB) / connectivity
virtualization works / expensive
must be flashed externally

installation

internal flashing

if it fails:
don't shut down your computer!
retry or get help via IRC

if you brick
your computer
you need an external
programmer to reflash
the chip

1) downloa boot (www.libreboot.org)

2) backup o l BIOS

3) flash

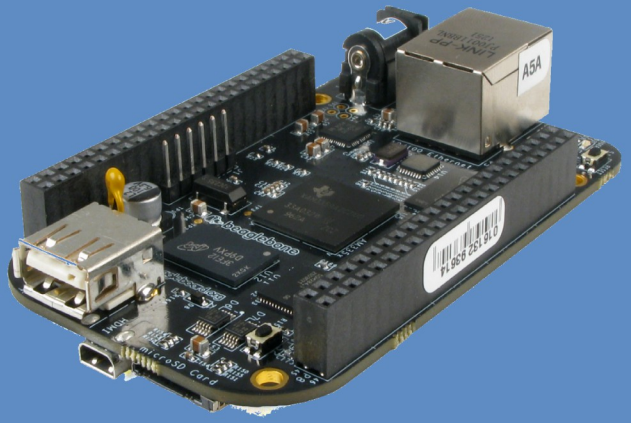
```
sudo ./lenovobios_firstflash bin/YOURBOARD/YOURROM
sudo ./lenovobios_secondflash /path/to/libreboot.rom
```

Backup:

```
sudo ./flashrom_lenovobios_sst -p internal -r factory.bin
sudo ./flashrom_lenovobios_macronix -p internal -r factory.bin
```

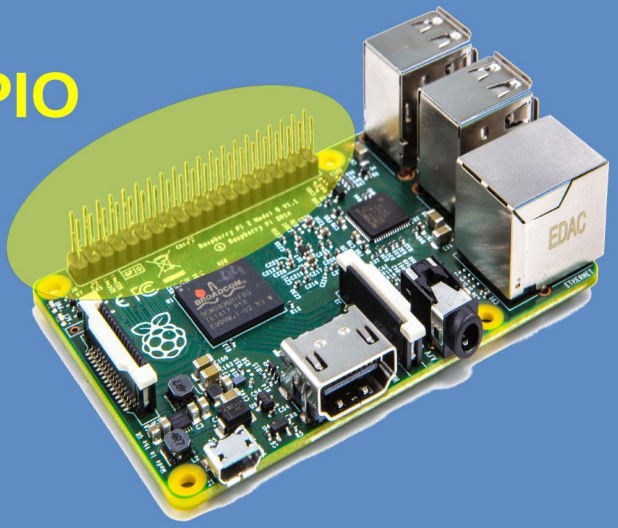
original BIOS is unique to every laptop!

external flashing

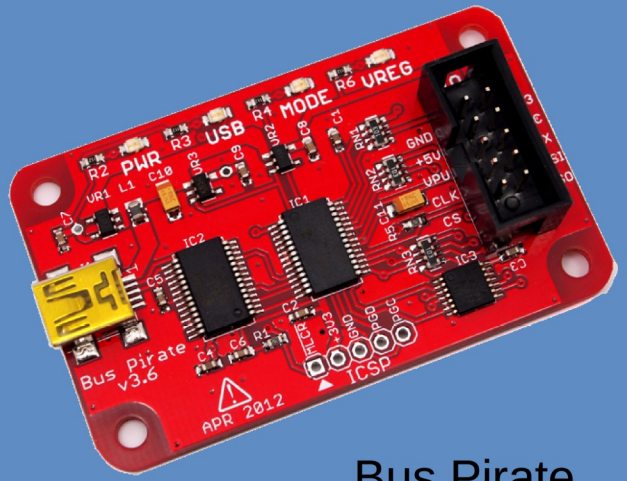


Beagle Bone

GPIO

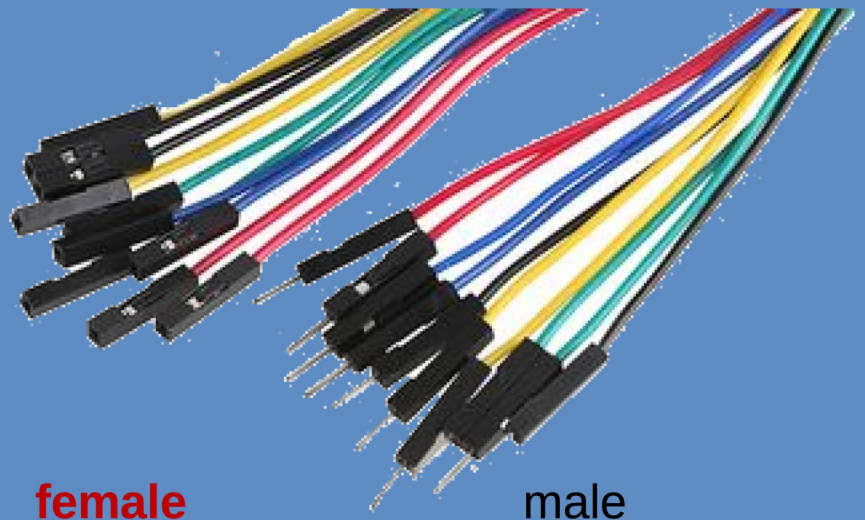


Raspberry Pi



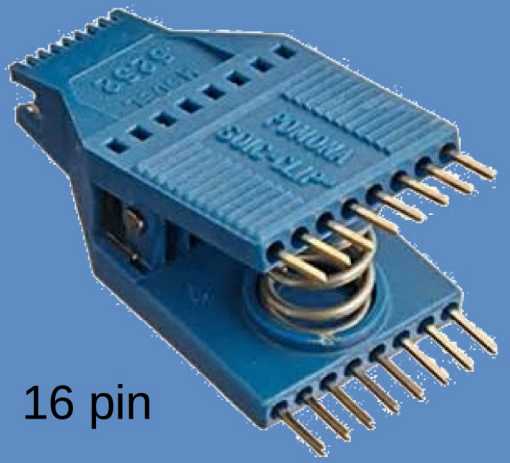
Bus Pirate

other material



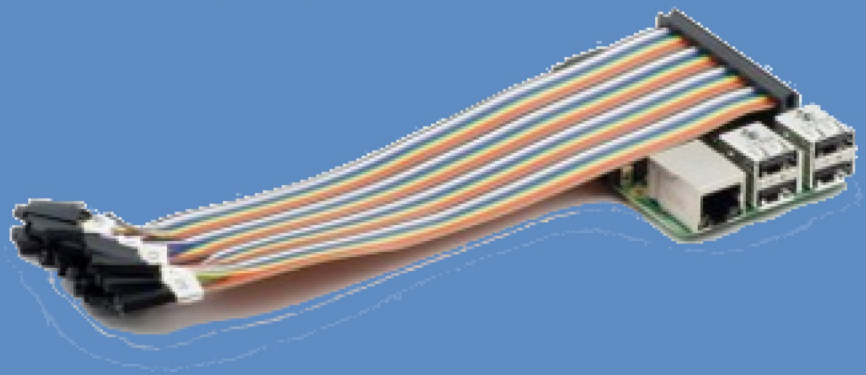
female male

Pomona clip

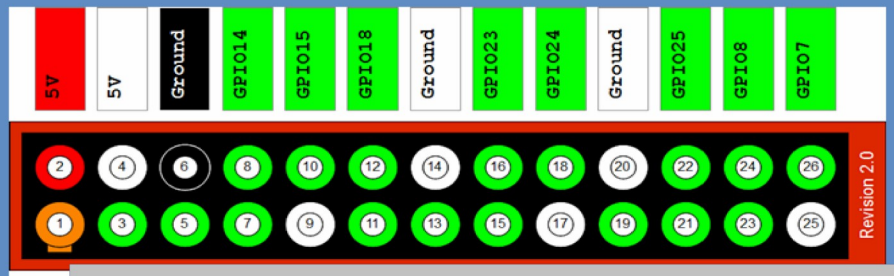


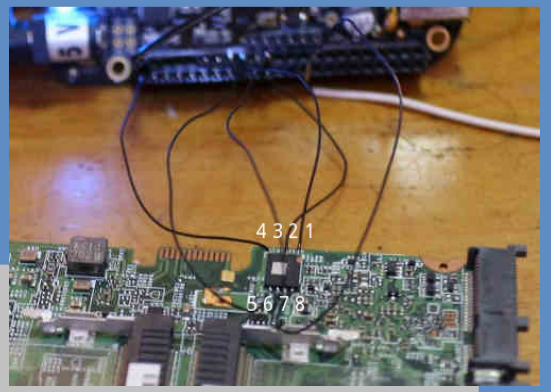
16 pin

jumper cables



8 pin





1) download image (www.libreboot.or

2) configure image

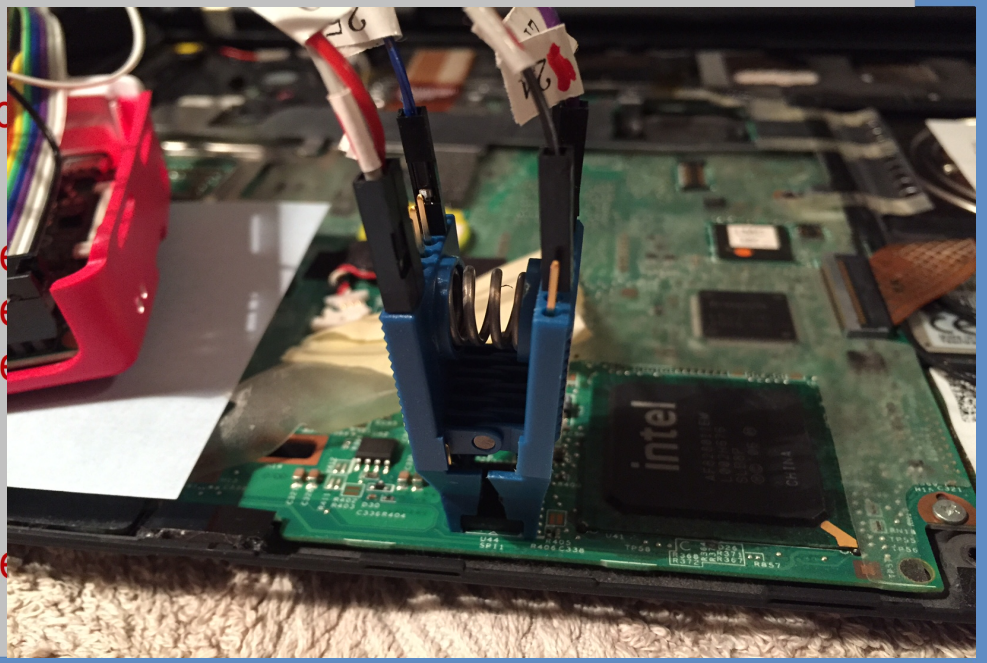
```
./ich9gen --macaddress XX:XX:XX:XX:XX:XX
dd if=ich9fdgbe_8m.bin of=libreboot.rom bs=1 co
```

3) backup & check original BIOS

```
./flashrom -p linux_spi:dev=/dev/spidev1.0,spispe
./flashrom -p linux_spi:dev=/dev/spidev1.0,spispe
./flashrom -p linux_spi:dev=/dev/spidev1.0,spispe
sha512sum factory*.rom
```

4) flash libreboot

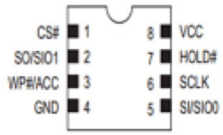
```
./flashrom -p linux_spi:dev=/dev/spidev1.0,spispe
```



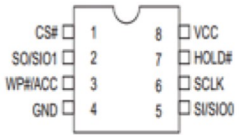
Pin #
1
2
3
4
5
6
7
8

16-PIN

8-LAND WSON (8x6mm, 6x5mm), USON (4x4mm)



8-PIN PDIP (300mil)



disconnect cmos-battery !

tipps & tricks

- insert spidev-device

modprobe spidev

- always control twice
- check images
- if it doesn't work: re[illegible]gain and again ...) !
  - change spidev-number
  - change read/write-speed
  - specify flash-chip (with -c option)

./flashrom -p linux_spi:dev=/dev/spidev**1.0**,spispeed=**512** -r libreboot.rom

be prepared for worst case ;-)
(i.e. to lose your board ...)

- can take hours!

./flashrom **-c "MX25L6405"** -p linux_spi:dev=/dev/spidev1.0,spispeed=512 -r libreboot.rom

wifi

incompatible with Lenovo-BIOS

full height
(x60)

half height
(all other)

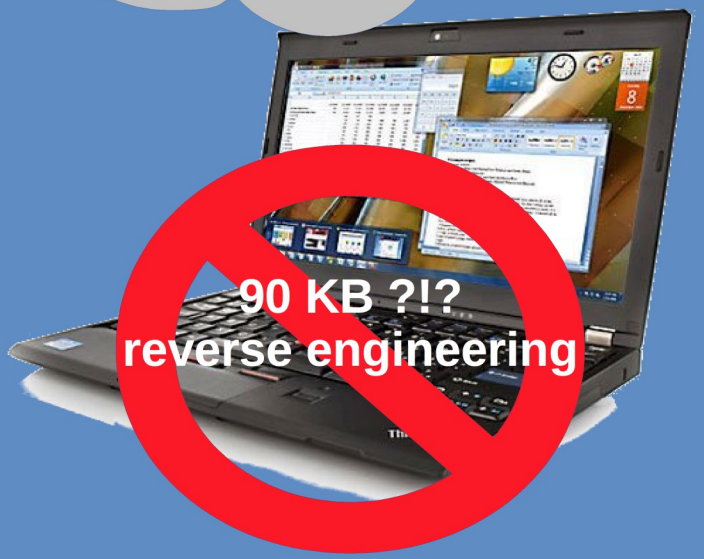
www.h-node.org

PERSPECTIVES ?

negotiation
with Intel

Purism

disable portions
(partitions) of ME
me_cleaner
(skript)



Thinkpad x220

DuckDuckGo

Google

Twitter

Gnu Social

Facebook

Debian

more freedom & liberty

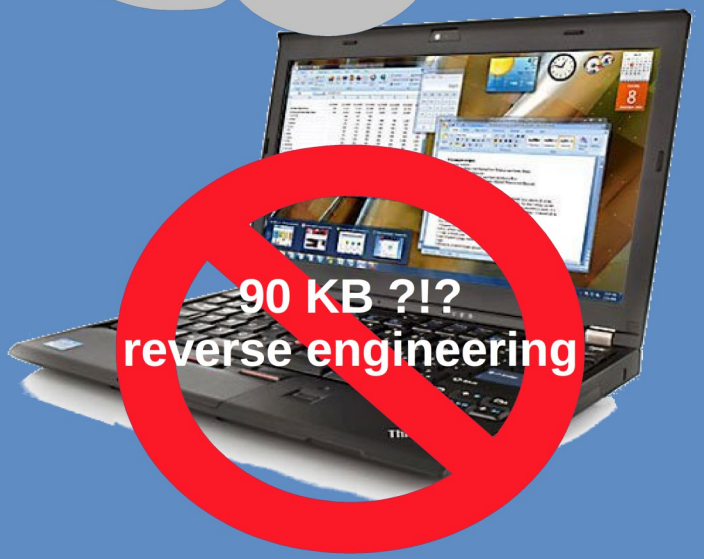
Heirloom aka Novena

PERSPECTIVES ?

negotiation
with Intel

Purism

disable portions
(partitions) of ME
me_cleaner
(skript)



Thinkpad x220

Thx & happy hacking! ;-)

contact: elpinguino@gmx.ch

Copyrights & Sources

Logos: taken from www.libreboot.org / www.coreboot.org

Slide 3: https://en.wikipedia.org/wiki/Richard_Stallman

Slide 7: boot sequence (c) www.puri.sm

Slides 8-10: underlying graphic (c) Joanna Rutkowska (presentation link: https://www.youtube.com/watch?v=rcwngbUrZNg)

Slide 24: http://thinkwiki.de/X200_Displayumbau

Slide 37: http://mottweilerstudio.com/novena-heirloom-first-complete-example/ and https://www.crowdsupply.com/sutajio-kosagi/novena