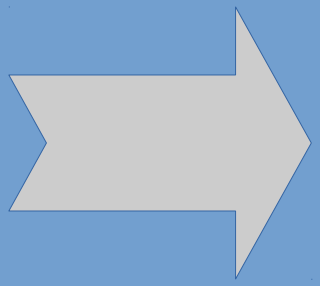
Thinkpad X230

Coreboot & ME_cleaner

freeing newer hardware

Libreboot

Thinklibre X200 (~2008)
=
Coreboot without ME
and other proprietary blobs



removing ME
=
shutdown after 30 min

new hope

me_cleaner

- python script by Nicola Corna
- insky
- „Intel
- ME

works from Nehalem
to Skylake (Kaby Lake)

mutilation / neutralization
of ME / AMT

why is Intel ME / AMT bad?

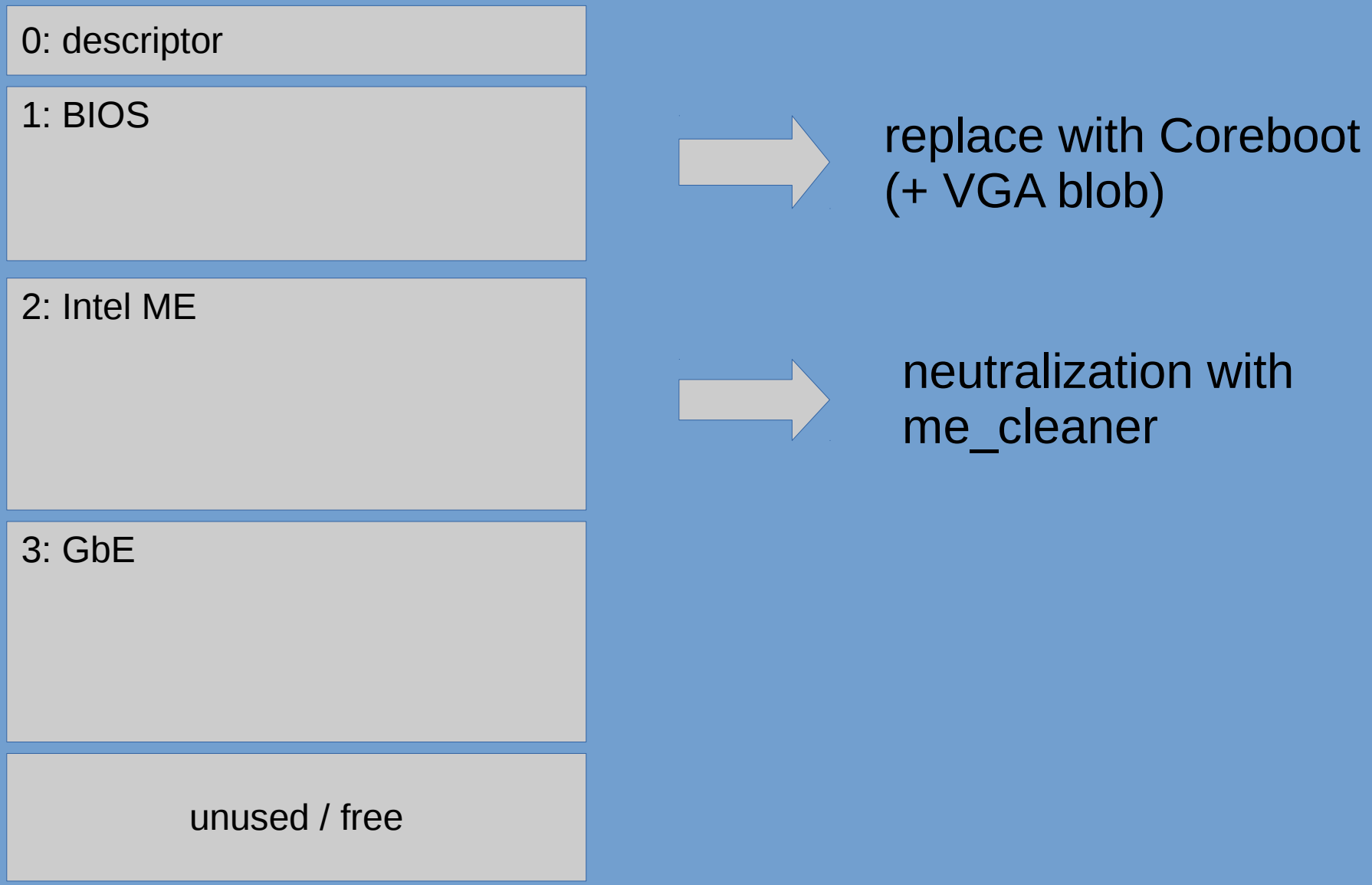
- it's proprietary software (black box, exact functionality unknown)
- it has unlimited acces to many things (network, memory, harddisk etc.)
- it is completely stealth to the main processor
- it can remotely control everything on the computer
- it contained / contains (?) severe security holes (like remote access without password in may 2017 (film))

Intel ME ist THE MAJOR SECURITY THREAT on modern platforms!

proprietary blobs & risks

• Intel ME	high!
• VGA (optional)	medium
• CPU microcode	low
• EC (embedded controller)	low
• GbE (descriptor)	low (none)

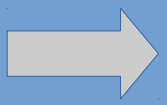
structure of firmware image



structure of ME blob

different versions from 1.5 – 5 MB

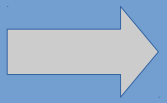
Partition table



are **NOT signed** / they only have a **checksum** and can be modified

Up to 23 partitions
of different types

examples:
BUP
ROMP
KERNEL
POLICY
HOSTCOMM
CLS
TDT etc.



cryptographically signed / cannot be modified

some of the are compressed

due to RSA key the modules cannot be modified, BUT (!) modifying the partition table it is possible de DISABLE partitions

disabling ME partitions

ROMP
BUP

ROMP = ROM bypass
BUP = Bring up

21 partitions
disabled

especially important:
network stack
JAVA-module

are disabled

depending on ME version over 90%
of code (1.5 – 5 MB) can be disabled!

< Version 11 (Skylake): only ROMP and
BUP = 90 KB of compressed code left

> Version 11: FTPR (Factory Partition,
probably for recovery) has also to be left
intact which leads to 650 KB of compressed
code

important: ME verifies RSA keys /
executes modules **ONE BY ONE**
and gets stuck after executing
the first two partitions

(most probable)

conclusion

this is
„as close
as you
can get“
to freedom

- ME starts with ROMP, makes the basic i[illegible] of ME with BUP and gets stuck immediately aft[illegible]at
- This is enough to disable the 30-min[illegible] watchdog (and keep the computer runnig)

What we know for sure: Intel AMT isn't reachable and Intel ME shows up as in „recovery state“

How to do it with the Thinkpad X230

Step 1 – what you need

- Thinkpad X230 (of course;-)
- Raspberry Pi / Beagle Bone / Bus Pirate or other flash programmer
- SOIC Clip (8 pins, but Pomona 5252 with 16 pins also works) and jumper cables
- another computer with necessary software (Coreboot, IFDTool, UEFITool ich_descriptor_tool)
- screwdrivers, time and a lot of patience ...

... and some courage

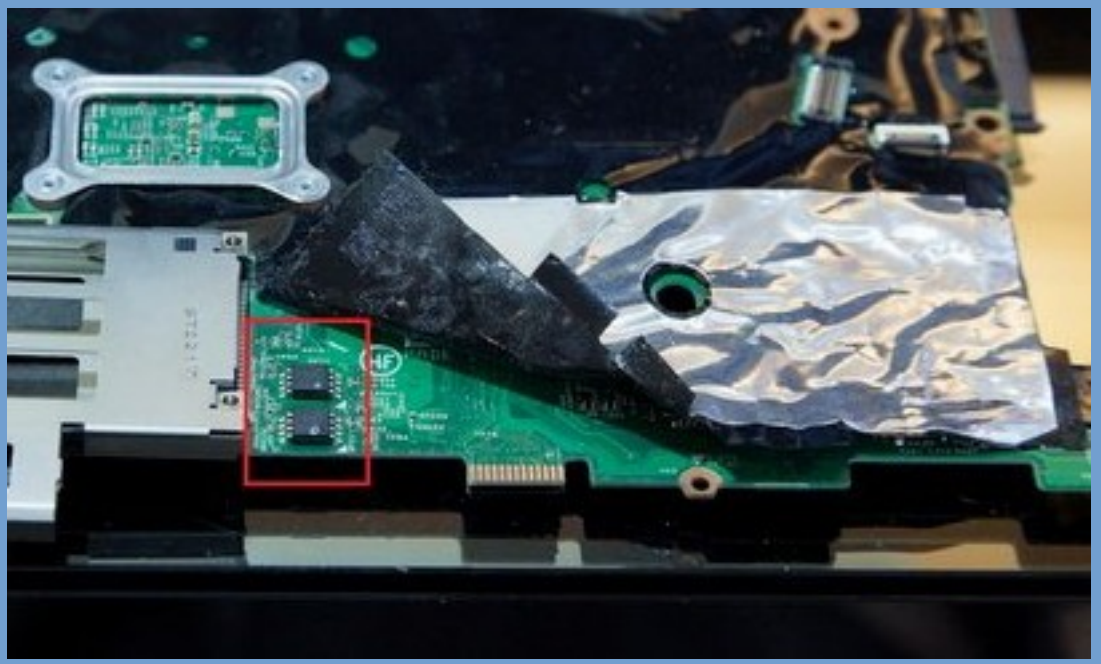
Yes, you may loose your board ... !

Step 2 – Backup the original firmware

top chip = 4MB
(lcd panel)

bottom chip = 8 MB
(near body)

Speciality: the x230 has 2 flash chips



8 MB + 4 MB = 12 MB

- You must back up INDIVIDUALLY each of the two chips with flashrom:

```
flashrom -p linux_spi:dev=/dev/spidev0.0 -r top.rom -c MX25L3206E/MX25L3208E
flashrom -p linux_spi:dev=/dev/spidev0.0 -r bottom.rom -c MX25L6406E/MX25L6408E
```

- After that you can join them to one image with cat (my recommendation):

```
cat bottom.rom top.rom > complete.rom
```

- make several copies and compare them with diff or sha512sum (if the don't match, don't proceed – you need correct images to extract the binary blobs!)

Step 3 – apply me_cleaner & extract blobs

- make image writeable (optional):

```
ifdtool -u complete.rom
```

- apply me_cleaner:

```
python me_cleaner complete.rom
```

- extract blobs:

```
ich_descriptors_tool -f complete.rom -d
```

- with ifdtool you get the four following files:

```
bios.bin / gbe.bin / me.bin / descriptor.bin
```

- use UEFITool to extract the VGA-blob from bios.bin

```
UEFITool bios.bin
```

=> deselect „unicode“, perform a text search with „VGA compatible“ and extract the hits with „extract body“

=> after that, search for a file with 64KB – with a little bit of luck this is your VGA blob ... ;-)

Step 4 – Build your coreboot.rom

- copy all the blobs to:

for me.bin, gbe.bin, descriptor.bin:
~/coreboot/3rdparty/blobs/mainboard/lenovo/x230/

for vbios.rom:
~/coreboot/

- configure coreboot:

```
cd ~/coreboot
make nconfig
```

The most important options are:

- mainboard: lenovo, x230
- flashchip-size: 12 MB
- keyboard: ps2
- blobs: indicate the correct paths!
- payload: seabios

Compile Coreboot:

```
make
```

Image = ~/coreboot/build/coreboot.rom

Step 5 – Flash new images

- split 12 MB image:

```
dd of=top.rom bs=1M if=coreboot.rom skip=8
dd of=bottom.rom bs=1M if=coreboot.rom count=8
```

- use Raspberry Pi to flash top-chip (4 MB) and test it (recommended):

```
flashrom -p linux_spi:dev=/dev/spidev0.0 -w top.rom -c MX25L3206E/MX25L3208E
```

=> your computer should boot up with seabios and Intel ME / AMT shout still be working (if you enabled it)

- flash bottom-chip (8 MB) in order to eliminate ME-functionalities:

```
flashrom -p linux_spi:dev=/dev/spidev0.0 -w bottom.rom -c MX25L6406E/MX25L6408E
```

=> Now, Intel ME / AMT should have disappeared completely

to finish the „freeing“ of the x230
you can now install a wifi-card
which is compatible with free software
(for example Atheros)
=> with coreboot the original whitelist has gone!

troubleshooting

- use a good tutorial, for example:

https://steemit.com/tutorial/@joeyd/run-don-t-walk-from-the-blob

flashing the x230 works well, however classical problems are:

- bad contact (check clip)

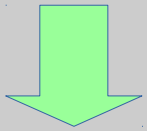
- too long cables (make them shorter)

- read / write speed too high (lower it)

conclusion – is it worth it?

Libreboot X200

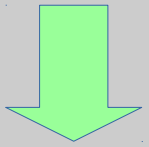
- screen quality (+ modified)
- resolution 1280x800
- keyboard
- speed (2 cores, sata2)
- RAM (8 GB)
- battery
- trackpoint
- usb 2.0 (usb 3.0 with ExpressCard)
- VGA (+ DP via Docking Station)
+ portability (smaller)
+ freedom (no proprietary blobs)



less performance, but still the best option in terms of freedom

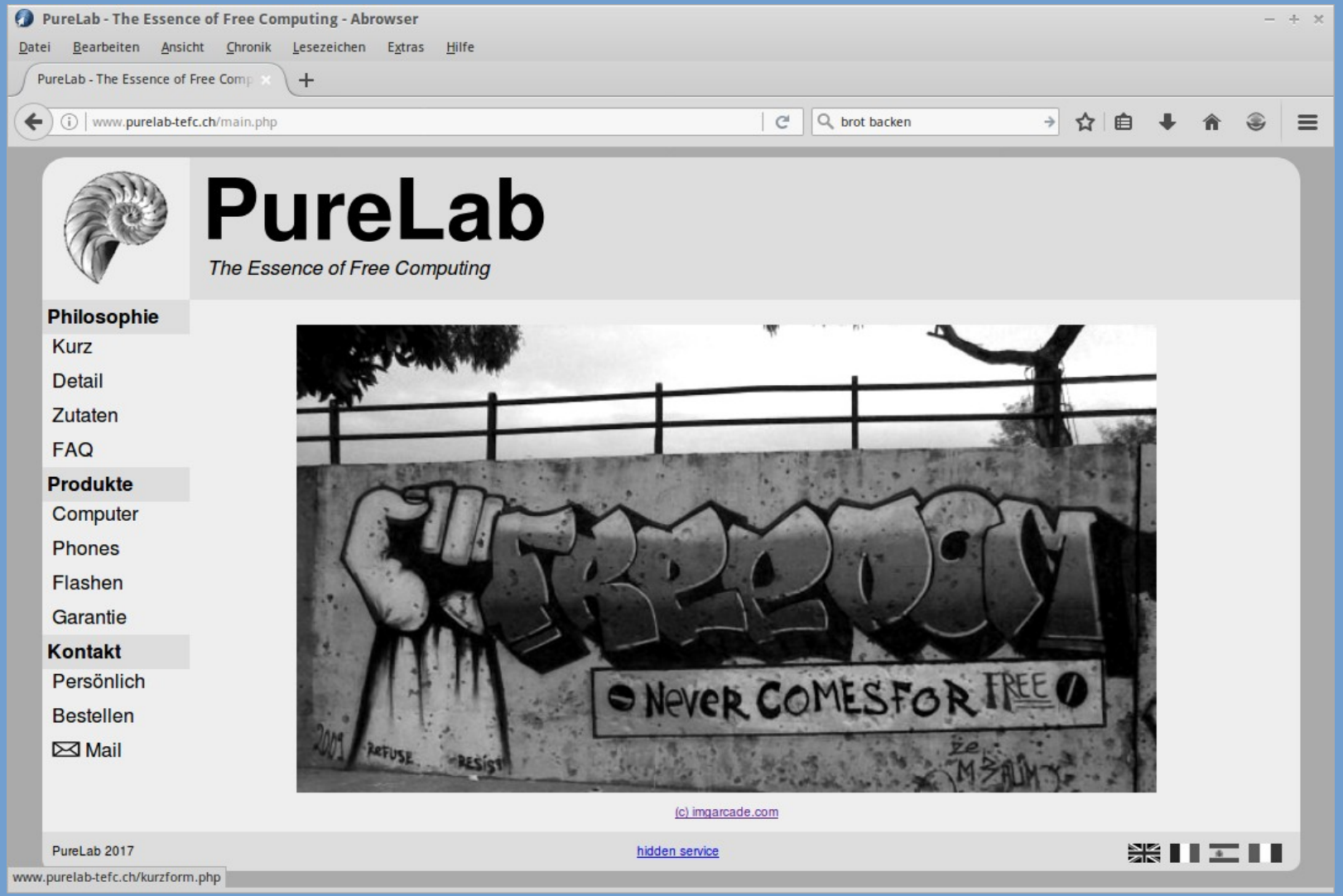
Coreboot X230 (me_cleaner)

+ screen quality
+ resolution 1366x768 (good for films)
+ keyboard
+ speed (2/4 cores, sata3)
+ RAM (16 GB)
+ battery
+ trackpoint & touchpad
+ usb 3.0
+ VGA & DisplayPort
- portability (a little bit wider)
- some proprietary blobs



technically better, but looses in terms of freedom

thx for your attention!



http://www.purelab-tefc.ch