Introduction to coreboot

coreboot

- What is coreboot?
- How can I try it out?
- How can I contribute?

What is coreboot?

Firmware

coreboot is firmware targeting multiple mainboards and processor architectures, including x86.

By default, Google's Chromebooks are running coreboot.

You can get coreboot on laptops from System76, Purism, and some refurbished Thinkpads.

Payloads

coreboot itself only initializes hardware and will need a payload to execute.

The default payload of coreboot is SeaBIOS, an open implementation of a legacy BIOS.

You can use any ELF binary as a payload, including a Linux kernel or a DOOM port.

Stages

coreboot consists of multiple stages.

1. Boot Block (CAR / Cache As RAM)
2. Verification (TPM, vboot)
3. ROM stage (memory init, ucode update)
4. RAM stage (PCIe, SMM, ACPI)
5. Payload

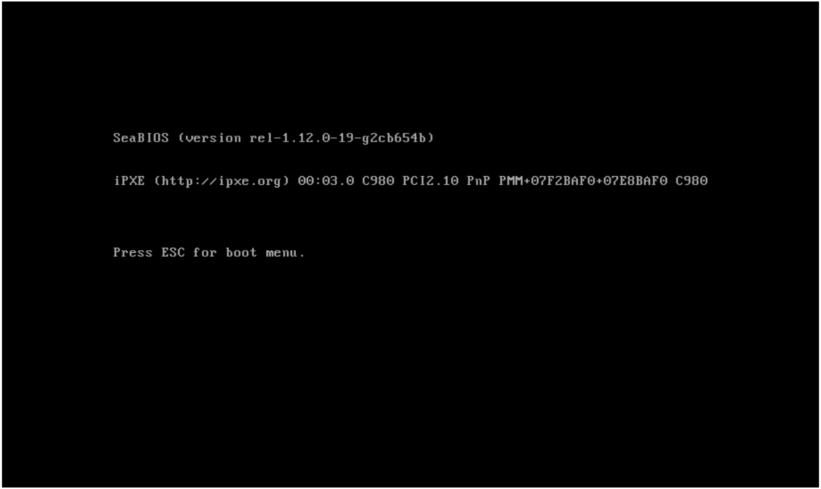
How can I try it out?

Run coreboot in an emulator

See the end users docs at https://coreboot.org/users.html.

1. clone the repo: `git clone https://review.coreboot.org/coreboot.git && cd coreboot`
2. build the toolchain: `make toolchain-i386 CPUS=4 && make iasl`
3. generate a generic config: `make defconfig`
4. build it: `make -j4`
5. run it in QEMU `qemu-system-x86_64 -bios build/coreboot.rom -serial stdio`

Demo



```
SeaBIOS (version rel-1.12.0-19-g2cb654b)

iPXE (http://ipxe.org) 00:03.0 C980 PCI2.10 PnP PMM+07F2BAF0+07E8BAF0 C980


Press ESC for boot menu.
```

Output

```
coreboot-4.9-2-g96374e7978-dirty Mon Mar 18 17:28:15 UTC 2019 bootblock starting...
CBFS: 'Master Header Locator' located CBFS at [200:40000)
CBFS: Locating 'fallback/romstage'
CBFS: Found @ offset 80 size 3c04


coreboot-4.9-2-g96374e7978-dirty Mon Mar 18 17:28:15 UTC 2019 romstage starting...
CBMEM:
IMD: root @ 07fff000 254 entries.
IMD: root @ 07ffec00 62 entries.
```

Output (continued)

```
CBFS: 'Master Header Locator' located CBFS at [200:40000)
CBFS: Locating 'fallback/ramstage'
CBFS: Found @ offset 3d00 size aca9
Decompressing stage fallback/ramstage @ 0x07fbcfc0 (128664 bytes)
Loading module at 07fbd000 with entry 07fbd000. filesize: 0x15750 memsize: 0x1f658
Processing 1257 relocs. Offset value of 0x071bd000


coreboot-4.9-2-g96374e7978-dirty Mon Mar 18 17:28:15 UTC 2019 ramstage starting...
Enumerating buses...
```

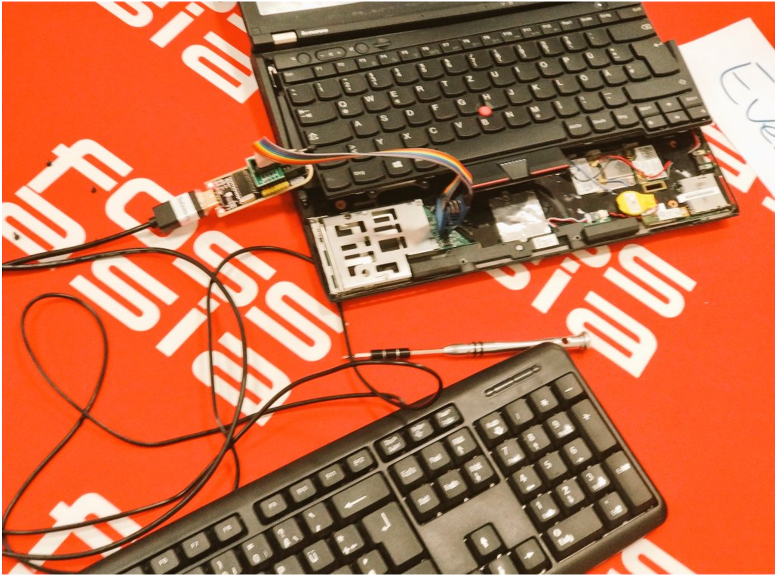
Output (continued)

```
CBFS: Locating 'fallback/payload'
CBFS: Found @ offset 1c080 size 12ba8
[...]
Loading segment from ROM address 0xfffdc2d4
  Entry Point 0x000fd258
Jumping to boot code at 000fd258(07fb4000)
SeaBIOS (version rel-1.12.0-19-g2cb654b)
```

Run coreboot on real hardware

1. get a fully supported device, e.g., Thinkpad X230, T430 etc
2. get a SOIC8 test clip and an SPI programmer, e.g., CH341A
3. open the laptop and read out the old ROM using flashrom
4. configure coreboot for your device and build it
5. flash it

Demo? Come to our workshop! :)



How can I contribute?

Ways to contribute

- fix bugs, implement features
- write documentation
- port to new hardware
- get board schematics and other docs
- work on coreboot utils
- reverse engineering

Thanks! :)