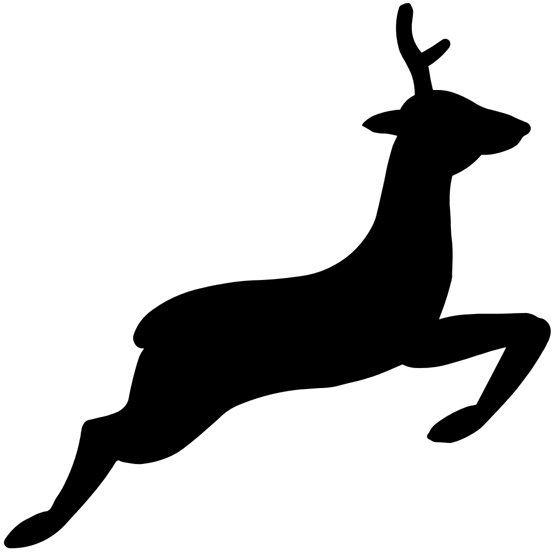
Coreboot / Libreboot



Coreboot / Libreboot

Fast, secure and flexible OpenSource firmware

Coreboot / Libreboot

Fast, secure and flexible OpenSource firmware

Replacement for your BIOS / (U)EFI

Why should I use coreboot / libreboot?

- Open Source

Why should I use coreboot / libreboot?

- Open Source
- Security - minimal Trusted Computing Base

Why should I use coreboot / libreboot?

- Open Source
- Security - minimal Trusted Computing Base
- Performance - Boot Time

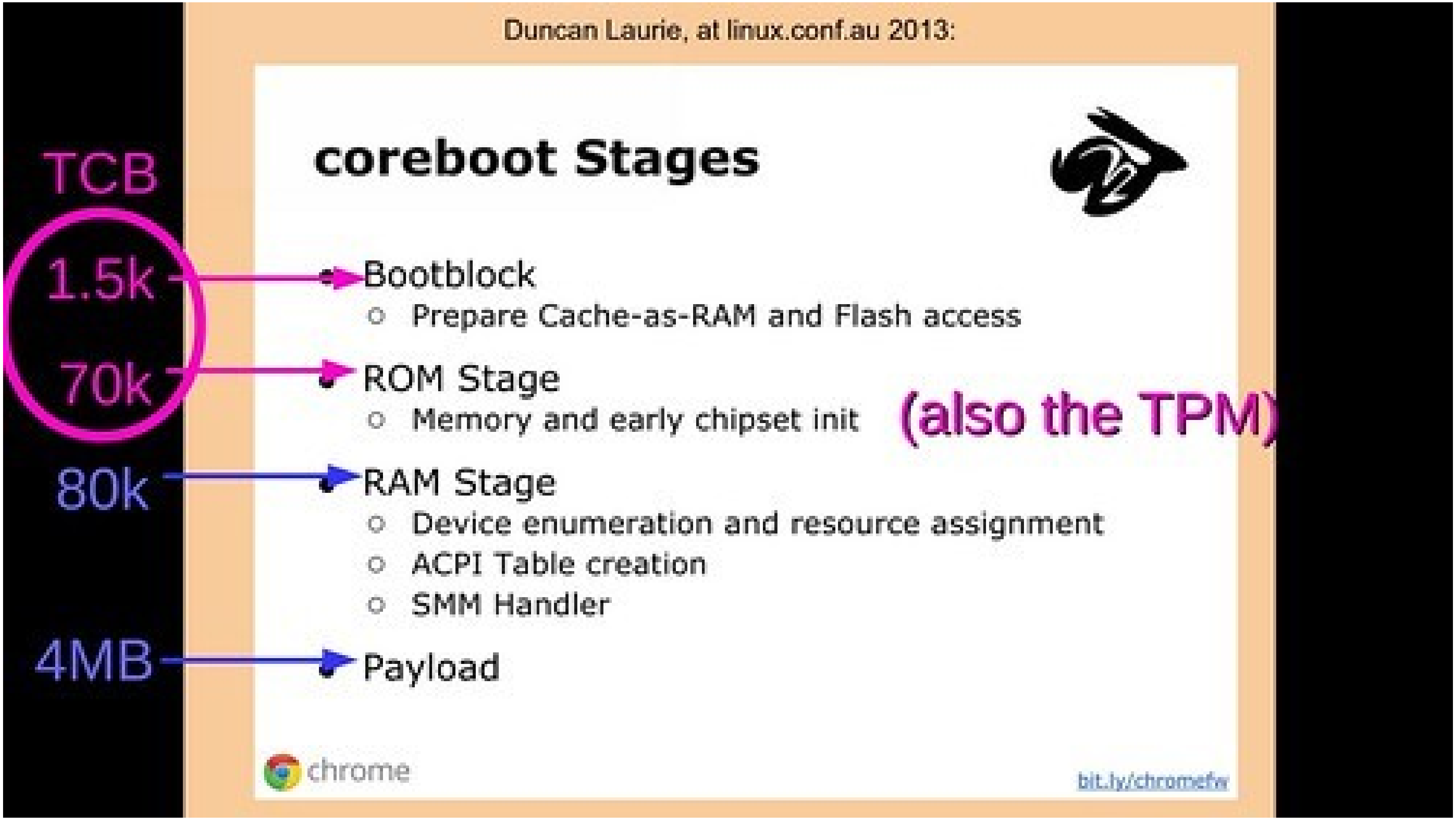
Why should I use coreboot / libreboot?

- Open Source
- Security - minimal Trusted Computing Base
- Performance - Boot Time
- Flexibility - many (customizable) payloads available

Payloads

- SeaBIOS
- TianoCore (UEFI)
- Grub2
- Linux Kernel
- Memtest86+
- Games (Invaders / Tetris)

Boot Process



Duncan Laurie, at linux.conf.au 2013:

coreboot Stages

- Bootblock
  - ○ Prepare Cache-as-RAM and Flash access
- ROM Stage
  - ○ Memory and early chipset init
- RAM Stage
  - ○ Device enumeration and resource assignment
  - ○ ACPI Table creation
  - ○ SMM Handler
- Payload

Supported Hardware

- old Thinkpads
- Chromebooks
- some Mainboards (Server and Desktop)

- Can be bought
  - https://tehnoetic.com
  - https://puri.sm
  - https://minifree.org
  - ...

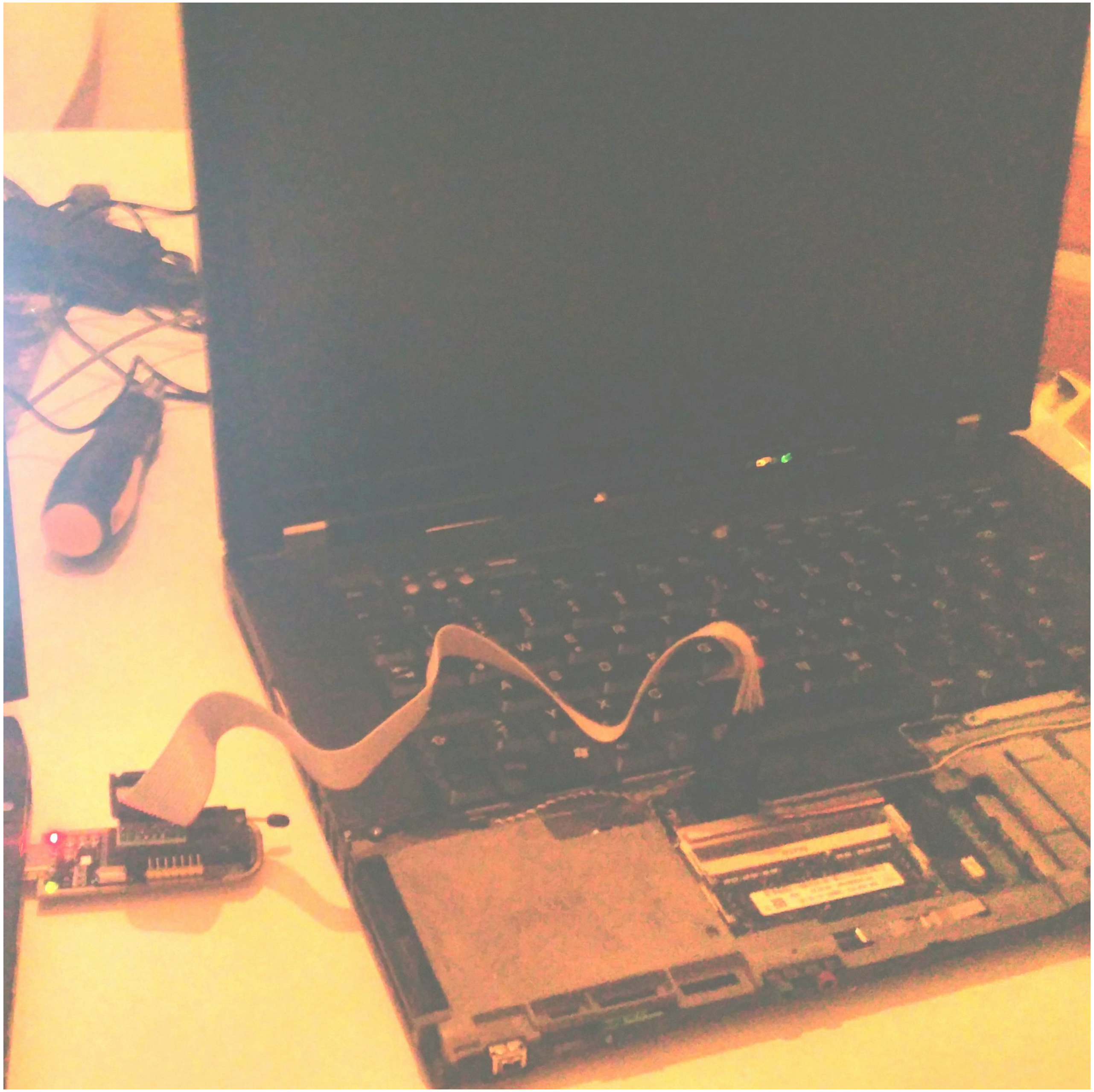
Installation

- Using an external SPI-Flasher to write directoy

Installation

1st Installation:

- Write to EEPROM using a SPI-Flasher



Links

- https://libreboot.org/
- https://www.coreboot.org/