

```
Freeing unused kernel memory: 1192K (ffff800010000000-ffff800010000000)
Freeing unused kernel memory: 908K (ffff800010000000-ffff800010000000)
=====
```

```
HEADS O ROM
```

```
Run './start-xen' to load the hypervisor
Run 'kexec -e' to boot it
```

```
IPM TOTP:
[ 1.664441] random: unsealfile urandom read with 8 bits of entropy available
2016-11-03 11:45:29: 438116
```

```
/bin/ash: can't access tty: job control turned off
/ # [ 2.520525] clocksource: Switched to clocksource tsc
uname -a
Linux (none) 4.7.0-heads #17 SMP Fri Oct 28 10:27:26 EDT 2016 x86_64 GNU/Linux
/ #
```

What is Heads

- open source custom firmware for laptops and servers

What is Heads

- open source custom firmware for laptops and servers
- based on coreboot

What is Heads

- open source custom firmware for laptops and servers
- based on coreboot
- using linux with initramfs as coreboot payload

What is Heads

- open source custom firmware for laptops and servers
- based on coreboot
- using linux with initramfs as coreboot payload
- uses the "Trusted Platform Module" for measurements and storage for secrets

What is Heads

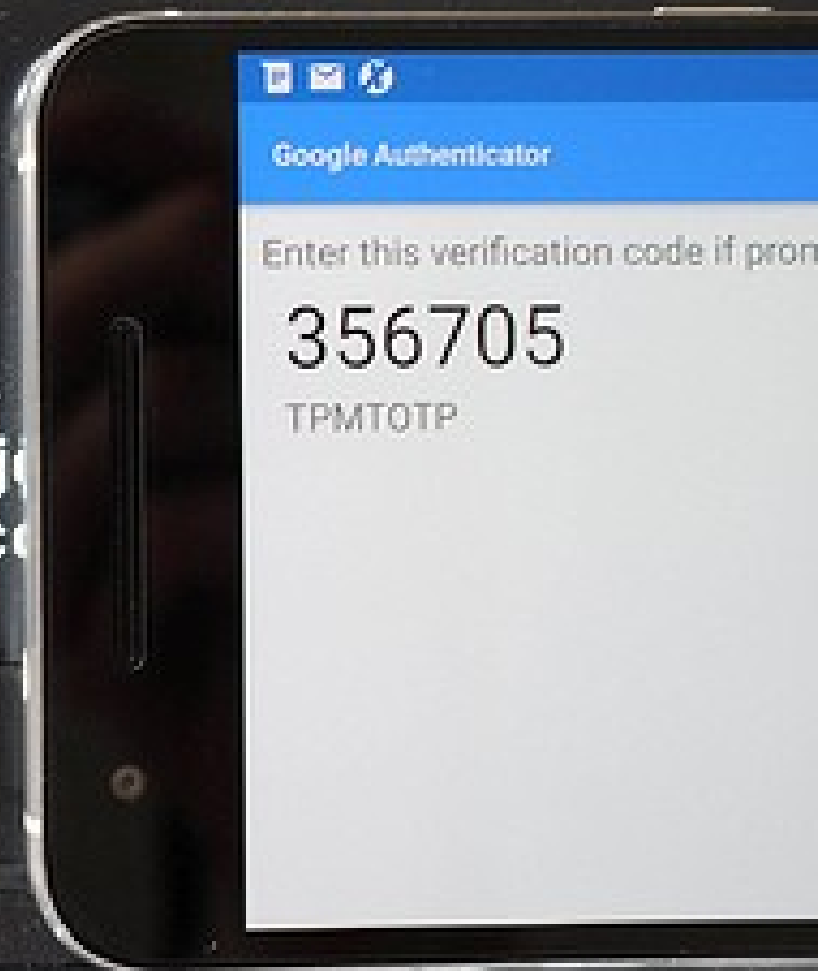
- open source custom firmware for laptops and servers
- based on coreboot
- using linux with initramfs as coreboot payload
- uses the "Trusted Platform Module" for measurements and storage for secrets
- Displays a TOTP One-Time-Password for verification

```
=====  
Run './start-xen' to load the hypervisor  
Run 'kexec -e' to boot it
```

```
Sun Jul 31 09:25:05 EDT 2016
```

```
Verify TPM PCR: 356705
```

```
/bin/ash: can't access tty; job control turned off  
/ # [ 2.451809] clocksource
```



Links / Sources

- <http://osresearch.net/>
- <https://github.com/osresearch/heads/>
- https://trmm.net/Heads_33c3