IoT: Client Devices

Reversing: Download and Extract

Firmware Image

TP-LINK HS110 V1

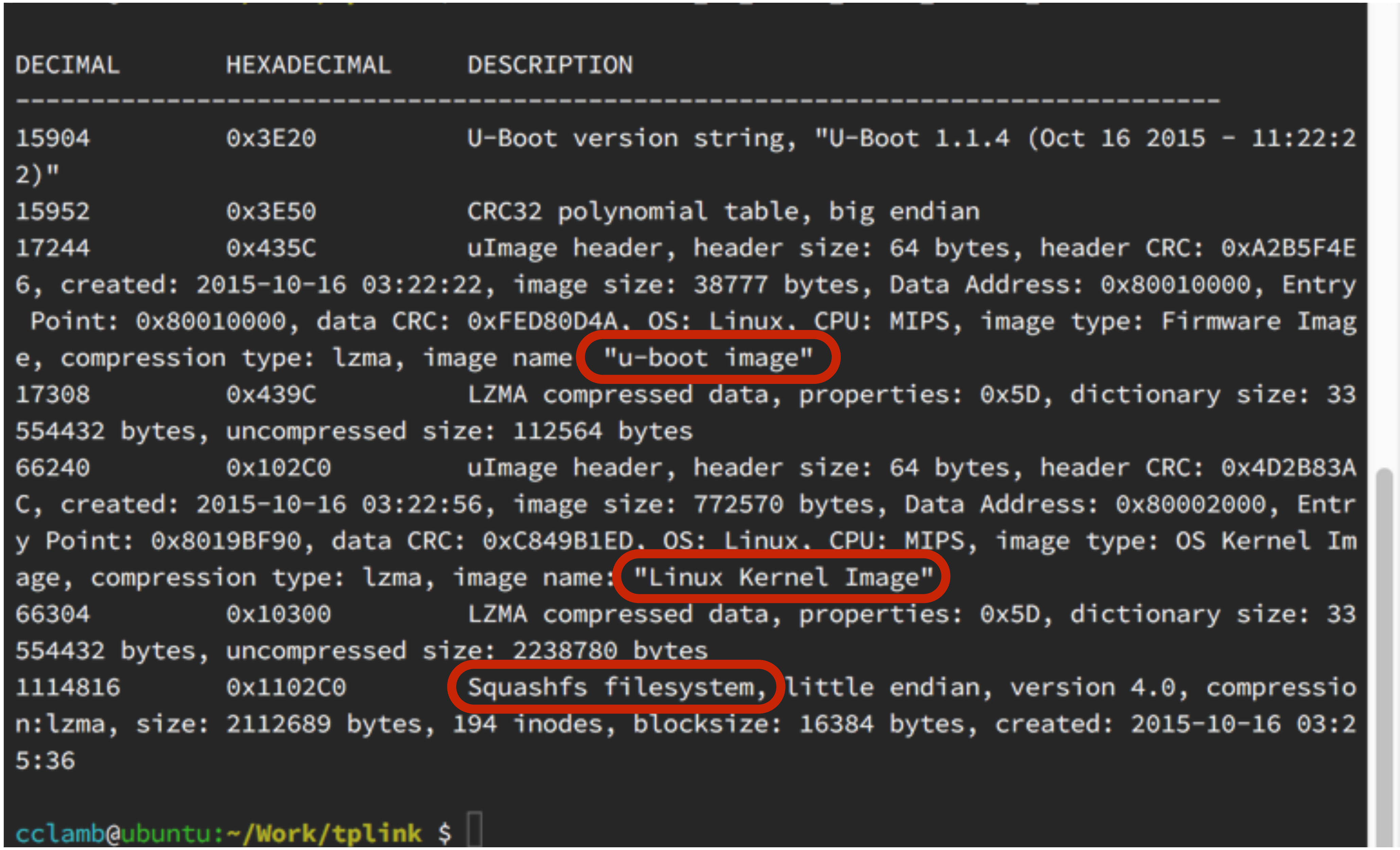
- http://www.tp-link.com/us/download/HS110.html#Firmware
- ZIP archive, go ahead and unzip
- You'll have some files and a BIN file
- BIN file is the firmware image!

What Does it Do?

Smart Plug

- Programmed via app
- Provides Usage, time used information
- uses Kasa app (see app store, google play)

Still uses full Linux!



```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
15904         0x3E20          U-Boot version string, "U-Boot 1.1.4 (Oct 16 2015 - 11:22:2
2)"
15952         0x3E50          CRC32 polynomial table, big endian
17244         0x435C          uImage header, header size: 64 bytes, header CRC: 0xA2B5F4E
6, created: 2015-10-16 03:22:22, image size: 38777 bytes, Data Address: 0x80010000, Entry
 Point: 0x80010000, data CRC: 0xFED80D4A, OS: Linux, CPU: MIPS, image type: Firmware Imag
e, compression type: lzma, image name: "u-boot image"
17308         0x439C          LZMA compressed data, properties: 0x5D, dictionary size: 33
554432 bytes, uncompressed size: 112564 bytes
66240         0x102C0         uImage header, header size: 64 bytes, header CRC: 0x4D2B83A
C, created: 2015-10-16 03:22:56, image size: 772570 bytes, Data Address: 0x80002000, Entr
y Point: 0x8019BF90, data CRC: 0xC849B1ED, OS: Linux, CPU: MIPS, image type: OS Kernel Im
age, compression type: lzma, image name: "Linux Kernel Image"
66304         0x10300         LZMA compressed data, properties: 0x5D, dictionary size: 33
554432 bytes, uncompressed size: 2238780 bytes
1114816       0x1102C0        Squashfs filesystem, little endian, version 4.0, compressio
n:lzma, size: 2112689 bytes, 194 inodes, blocksize: 16384 bytes, created: 2015-10-16 03:2
5:36

cclamb@ubuntu:~/Work/tplink $
```

Now What?

Let’s take a look inside

Onto Analysis!