IoT: Client Devices

Reversing: Image Analysis

So Far…

U-Boot boot loader

- Version 1.1.4, built in late 2015

Linux Kernel

- Also built in late 2015

Filesystem

- Squash-fs filesystem, late 2015

Extracting

Now let's use binwalk to extract the files

- binwalk -e -C extracted -M <imagename>

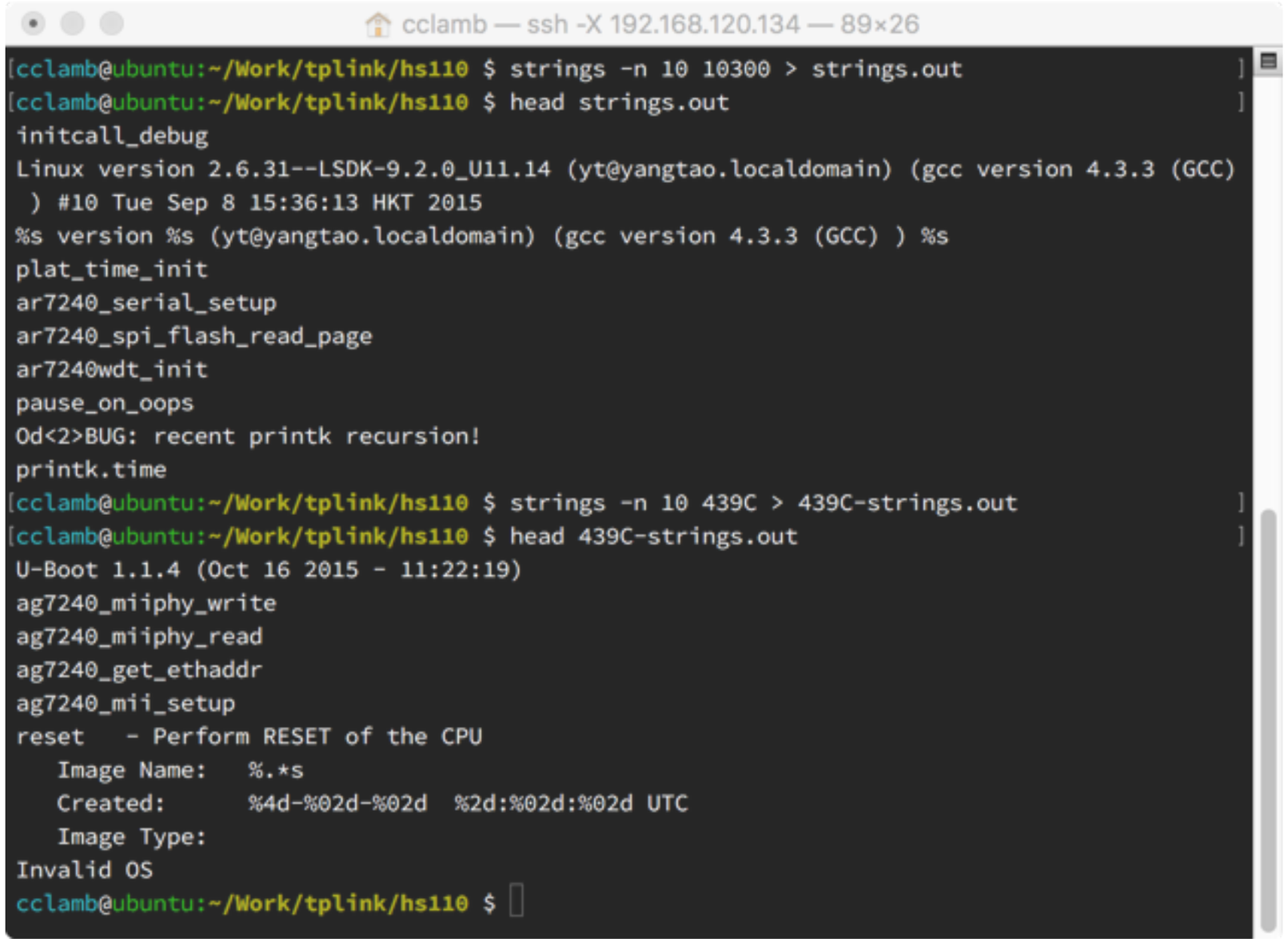
What does this do?

- -e: extract the contents of the image
- -C: place the results in the 'extracted' subdirectory
- -M: recursively scan extracted stuff

cclamb — ssh -X 192.168.120.134 — 89×26

```
[cclamb@ubuntu:~/Work/tplink/extracted/_hs110v1_us_1.0.7_Build_151016_Rel.24186.bin.extrac]
ted $ ls
10300  10300.7z  _10300.extracted  1102C0.squashfs  439C  439C.7z  squashfs-root
[cclamb@ubuntu:~/Work/tplink/extracted/_hs110v1_us_1.0.7_Build_151016_Rel.24186.bin.extrac]
ted $ binwalk ../../hs110v1_us_1.0.7_Build_151016_Rel.24186.bin

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
```



Strings

Seems to confirm binwalk results, but now we have a kernel version (released in 2009!)

```
[cclamb@ubuntu:~/Work/tplink/hs110 $ ls
 10300      _10300.extracted  439C      439C-strings.out  squashfs-root
 10300.7z   1102C0.squashfs   439C.7z   hex.out           strings.out
[cclamb@ubuntu:~/Work/tplink/hs110 $ cd squashfs-root/
[cclamb@ubuntu:~/Work/tplink/hs110/squashfs-root $ ls
 bin  dev  etc  lib  linuxrc  mnt  proc  root  sbin  sys  tmp  usr
 cclamb@ubuntu:~/Work/tplink/hs110/squashfs-root $
```

The filesystem

Take a look at squashes-root; it has a complete filesystem!