IoT: Client Devices

Running Application Executables

Application Analysis

REGULAR APPLICATIONS

- GDB, LLDB
- Binutils
- Tracing Tools (DTrace, STrace, etc.)

CROSS-COMPILATION PROBLEMS

- Cross-compiled binutils

But What about dynamic analysis?

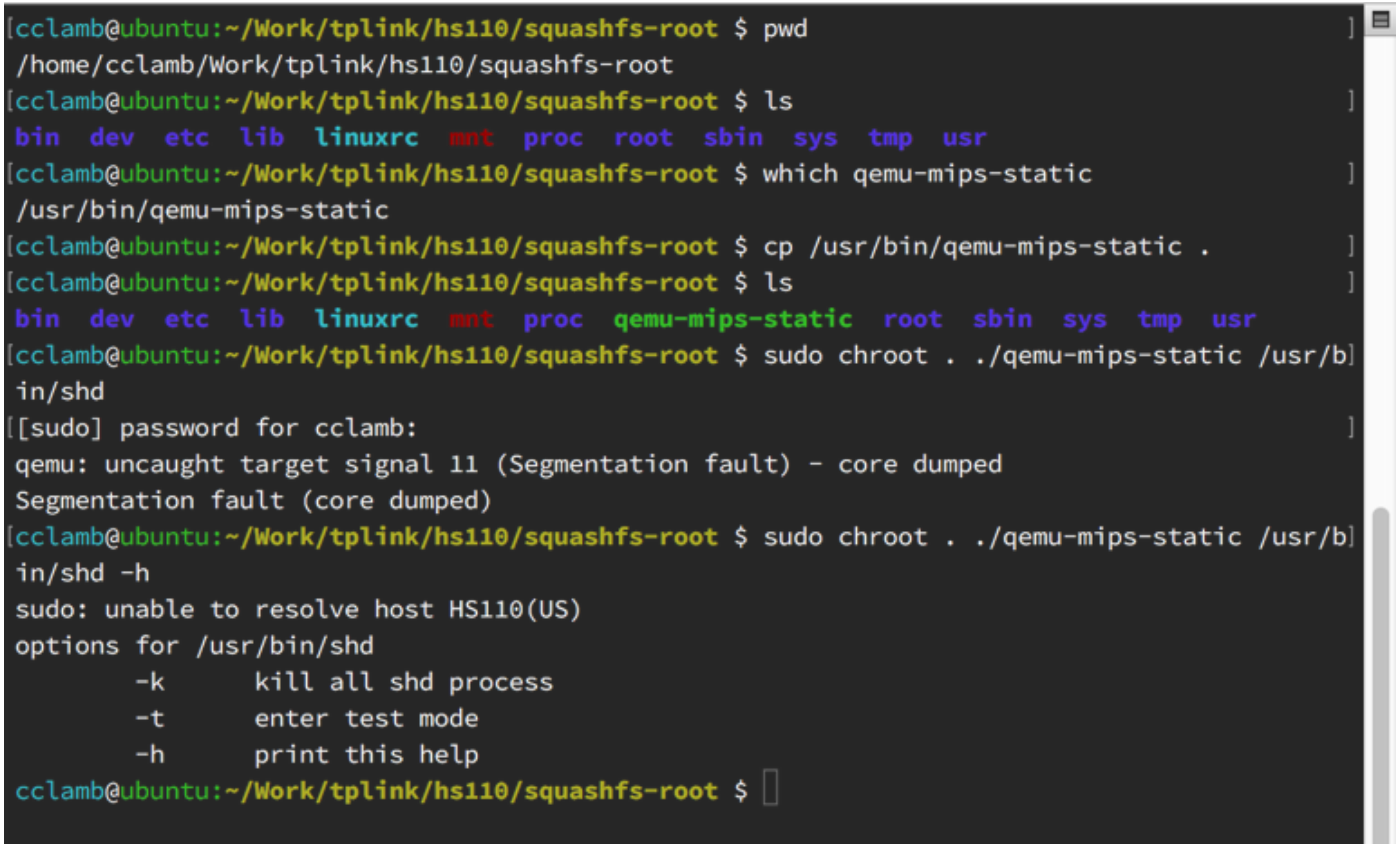
QEMU to the Rescue!

QEMU CAN RUN APPLICATIONS LOCALLY

- chroot
- qemu-*-static (e.g. qemu-mips-static)

HOW TO USE

- Easiest if you use the extracted filesystem
- copy the appropriate static execution utility
- run cross-compiled



```
[cclamb@ubuntu:~/Work/tplink/hs110/squashfs-root $ pwd                                    ]
 /home/cclamb/Work/tplink/hs110/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 $ which qemu-mips-static                 ]
 /usr/bin/qemu-mips-static
[cclamb@ubuntu:~/Work/tplink/hs110/squashfs-root $ cp /usr/bin/qemu-mips-static .         ]
[cclamb@ubuntu:~/Work/tplink/hs110/squashfs-root $ ls                                     ]
 bin  dev  etc  lib  linuxrc  mnt  proc  qemu-mips-static  root  sbin  sys  tmp  usr
[cclamb@ubuntu:~/Work/tplink/hs110/squashfs-root $ sudo chroot . ./qemu-mips-static /usr/b]
 in/shd
[[sudo] password for cclamb:                                                              ]
 qemu: uncaught target signal 11 (Segmentation fault) - core dumped
 Segmentation fault (core dumped)
[cclamb@ubuntu:~/Work/tplink/hs110/squashfs-root $ sudo chroot . ./qemu-mips-static /usr/b]
 in/shd -h
 sudo: unable to resolve host HS110(US)
 options for /usr/bin/shd
         -k      kill all shd process
         -t      enter test mode
         -h      print this help
 cclamb@ubuntu:~/Work/tplink/hs110/squashfs-root $ 
```

Running /usr/bin/shd

with flags and without!

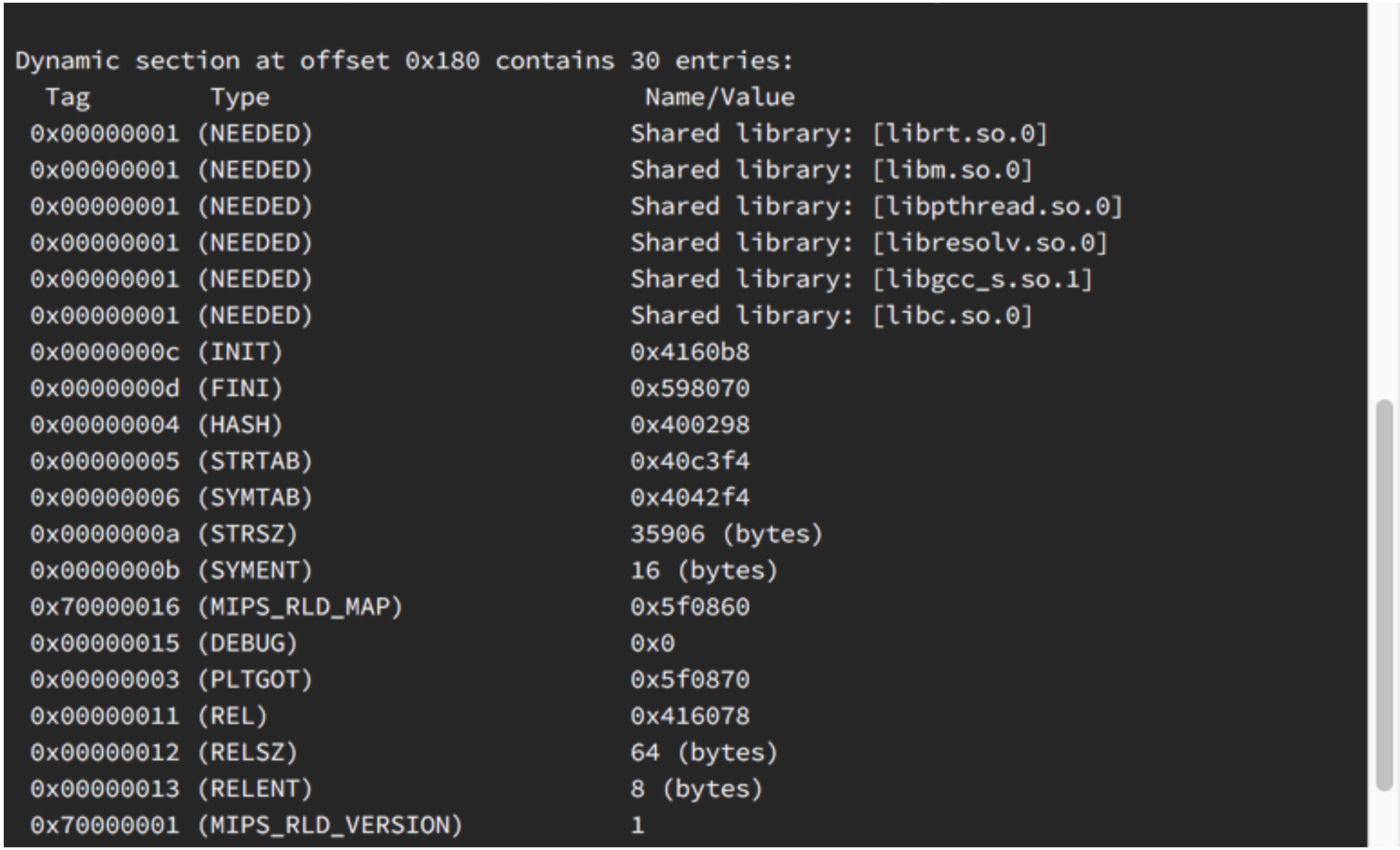
Why chroot?

YOU MAY NOT ALWAYS NEED IT

- statically linked applications

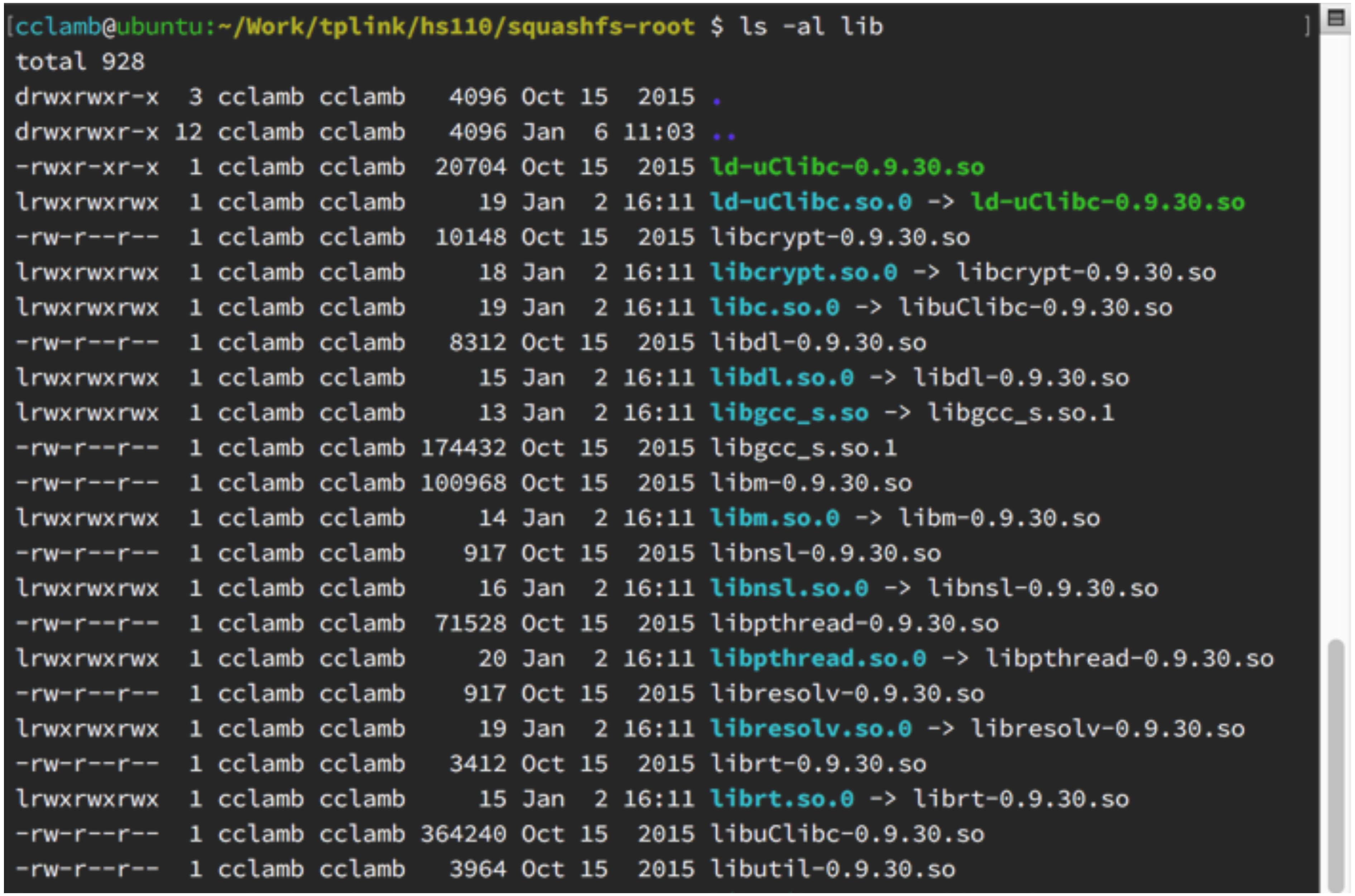
USING LIBRARIES? YOU NEED CHROOT

- shd uses a few
- how do we know?



```
Dynamic section at offset 0x180 contains 30 entries:
  Tag        Type                         Name/Value
 0x00000001 (NEEDED)                     Shared library: [librt.so.0]
 0x00000001 (NEEDED)                     Shared library: [libm.so.0]
 0x00000001 (NEEDED)                     Shared library: [libpthread.so.0]
 0x00000001 (NEEDED)                     Shared library: [libresolv.so.0]
 0x00000001 (NEEDED)                     Shared library: [libgcc_s.so.1]
 0x00000001 (NEEDED)                     Shared library: [libc.so.0]
 0x0000000c (INIT)                       0x4160b8
 0x0000000d (FINI)                       0x598070
 0x00000004 (HASH)                       0x400298
 0x00000005 (STRTAB)                     0x40c3f4
 0x00000006 (SYMTAB)                     0x4042f4
 0x0000000a (STRSZ)                      35906 (bytes)
 0x0000000b (SYMENT)                     16 (bytes)
 0x70000016 (MIPS_RLD_MAP)               0x5f0860
 0x00000015 (DEBUG)                      0x0
 0x00000003 (PLTGOT)                     0x5f0870
 0x00000011 (REL)                        0x416078
 0x00000012 (RELSZ)                      64 (bytes)
 0x00000013 (RELENT)                     8 (bytes)
 0x70000001 (MIPS_RLD_VERSION)           1
```

Shared Libraries



```
cclamb@ubuntu:~/Work/tplink/hs110/squashfs-root $ ls -al lib
total 928
drwxrwxr-x  3 cclamb cclamb   4096 Oct 15  2015 .
drwxrwxr-x 12 cclamb cclamb   4096 Jan  6 11:03 ..
-rwxr-xr-x  1 cclamb cclamb  20704 Oct 15  2015 ld-uClibc-0.9.30.so
lrwxrwxrwx  1 cclamb cclamb     19 Jan  2 16:11 ld-uClibc.so.0 -> ld-uClibc-0.9.30.so
-rw-r--r--  1 cclamb cclamb  10148 Oct 15  2015 libcrypt-0.9.30.so
lrwxrwxrwx  1 cclamb cclamb     18 Jan  2 16:11 libcrypt.so.0 -> libcrypt-0.9.30.so
lrwxrwxrwx  1 cclamb cclamb     19 Jan  2 16:11 libc.so.0 -> libuClibc-0.9.30.so
-rw-r--r--  1 cclamb cclamb   8312 Oct 15  2015 libdl-0.9.30.so
lrwxrwxrwx  1 cclamb cclamb     15 Jan  2 16:11 libdl.so.0 -> libdl-0.9.30.so
lrwxrwxrwx  1 cclamb cclamb     13 Jan  2 16:11 libgcc_s.so -> libgcc_s.so.1
-rw-r--r--  1 cclamb cclamb 174432 Oct 15  2015 libgcc_s.so.1
-rw-r--r--  1 cclamb cclamb 100968 Oct 15  2015 libm-0.9.30.so
lrwxrwxrwx  1 cclamb cclamb     14 Jan  2 16:11 libm.so.0 -> libm-0.9.30.so
-rw-r--r--  1 cclamb cclamb    917 Oct 15  2015 libnsl-0.9.30.so
lrwxrwxrwx  1 cclamb cclamb     16 Jan  2 16:11 libnsl.so.0 -> libnsl-0.9.30.so
-rw-r--r--  1 cclamb cclamb  71528 Oct 15  2015 libpthread-0.9.30.so
lrwxrwxrwx  1 cclamb cclamb     20 Jan  2 16:11 libpthread.so.0 -> libpthread-0.9.30.so
-rw-r--r--  1 cclamb cclamb    917 Oct 15  2015 libresolv-0.9.30.so
lrwxrwxrwx  1 cclamb cclamb     19 Jan  2 16:11 libresolv.so.0 -> libresolv-0.9.30.so
-rw-r--r--  1 cclamb cclamb   3412 Oct 15  2015 librt-0.9.30.so
lrwxrwxrwx  1 cclamb cclamb     15 Jan  2 16:11 librt.so.0 -> librt-0.9.30.so
-rw-r--r--  1 cclamb cclamb 364240 Oct 15  2015 libuClibc-0.9.30.so
-rw-r--r--  1 cclamb cclamb   3964 Oct 15  2015 libutil-0.9.30.so
```

Packaged Libraries

/usr/bin/shd needs to find these to run!