

Lab4 Procedure Report

Xinyu Jian 201990890

Procedure (for extra credit)

1. Download FreeBSD's image for the BeagleBone Black from <ftp://ftp.freebsd.org/pub/FreeBSD/releases/arm/armv7/ISO-IMAGES/12.0/FreeBSD-12.0-RELEASE-arm-armv7-BEAGLEBONE.img.xz>

2. Extract the image by executing:

```
xz -d FreeBSD-12.0-RELEASE-arm-armv7-BEAGLEBONE.img.xz
```

Dissecting the image

1. Use the `file(1)` command to inspect the `.img` file downloaded above. Explain the results. How does the "file" command retrieve this information?

```
xy@xy-vm:~/Downloads$ file FreeBSD-12.0-RELEASE-arm-armv7-BEAGLEBONE.img
FreeBSD-12.0-RELEASE-arm-armv7-BEAGLEBONE.img: DOS/MBR boot sector;
partition 1 : ID=0xc, active, start-CHS (0x0,17,1), end-CHS (0x6,110,63),
startsector 1071, 102312 sectors; partition 2 : ID=0xa5, start-CHS
(0x6,111,1), end-CHS (0x187,158,63), startsector 103383, 6188049 sectors
```

`file(1)` is used to determine file type.

- `FreeBSD-12.0-RELEASE-arm-armv7-BEAGLEBONE.img`: the file name
- `DOS/MBR boot sector`; **DOS** stands for Disk Operating System. **MBR** stands for Master Boot Record, which is a special type of boot sector at the very beginning of partitioned computer mass storage devices¹. A **boot sector** is the sector of a persistent data storage device which contains machine code to be loaded into random-access memory (RAM) and then executed by a computer system's built-in firmware (e.g., the BIOS). Usually, the very first sector of the hard disk is the boot sector. It consists of MBR, DPT (Disk Partition Table) and Boot Record ID.
- `partition 1 : ID=0xc, active, start-CHS (0x0,17,1), end-CHS (0x6,110,63), startsector 1071, 102312 sectors`; is the information of the first disk partition.
 - `ID=0xc`: partition ID in a partition's entry in the partition table inside a master boot record (MBR) is a byte value intended to specify the file system the partition contains or to flag special access methods used to access these partitions.
 - `active`: On MBR disk, the system reserved partition is required to be active. An active partition is a partition on a hard drive set as the bootable partition containing the operating system. Only one partition on each hard drive can be set as an active partition or bootable partition.
 - `start-CHS (0x0,17,1)`: the start CHS address.
 - `end-CHS (0x6,110,63)`: the end CHS address.
 - `startsector 1071`: start sector ID.
 - `102312 sectors`: partition 1 has 102312 sectors.

`file(1)` retrieve this information by looking at the header information of the file, which is the boot sector.

2. Now inspect the image with `fdisk(1)`.

1. What command did you need to execute?

```
xy@xy-vm:~/Downloads$ fdisk -l FreeBSD-12.0-RELEASE-arm-armv7-
BEAGLEBONE.img
Disk FreeBSD-12.0-RELEASE-arm-armv7-BEAGLEBONE.img: 3 GiB, 3221225472
bytes, 6291456 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

Device                                Boot  Start      End
Sectors Size Id Type
FreeBSD-12.0-RELEASE-arm-armv7-BEAGLEBONE.img1 *    1071   103382
 102312  50M  c W95 FAT32 (LBA)
FreeBSD-12.0-RELEASE-arm-armv7-BEAGLEBONE.img2    103383 6291431
6188049  3G a5 FreeBSD
```

2. How many partitions are available in the image file?

2 partitions

3. Which partition including the boot loader? How do you know? What is its type?

the first partition. Because there is a * in the Boot column. Its type is W95 FAT32 (LBA).

4. Where is the MBR located?

The MBR is located on the first sector of a disk, i.e., boot sector.

5. Which partition holds the installed OS? What is its type?

the 2nd partition. Its type is FreeBSD.

Extracting MBR

1. Using `dd(1)`, extract 1 MiB of data from the beginning of the image to a file called `mbr.bin`.

Show the command you executed and evidence that it worked correctly.

A default block in `dd(1)` command is 512B. $1MiB/512B = 2048 = 2K$

```
xy@xy-vm:~/Downloads$ dd if=FreeBSD-12.0-RELEASE-arm-armv7-BEAGLEBONE.img
of=mbr.bin count=2K
2048+0 records in
2048+0 records out
1048576 bytes (1.0 MB, 1.0 MiB) copied, 0.00647639 s, 162 MB/s
```

2. Use the `file(1)` command to inspect `mbr.bin`. Compare with the results of inspecting the `.img` file.

```
xy@xy-vm:~/Downloads$ file mbr.bin
mbr.bin: DOS/MBR boot sector; partition 1 : ID=0xc, active, start-CHS
(0x0,17,1), end-CHS (0x6,110,63), startsector 1071, 102312 sectors;
partition 2 : ID=0xa5, start-CHS (0x6,111,1), end-CHS (0x187,158,63),
startsector 103383, 6188049 sectors
```

It has the same information as `file .img_file`, which proves that `file(1)` retrieve this information by looking at the first sector.

Mounting the Boot Partition

1. Using `dd(1)`, extract the boot partition to a file called `boot.img`. Explain the command you ran.

```
xy@xy-vm:~/Downloads$ dd if=FreeBSD-12.0-RELEASE-arm-armv7-BEAGLEBONE.img
of=boot.img skip=1071 count=102312
102312+0 records in
102312+0 records out
52383744 bytes (52 MB, 50 MiB) copied, 0.378313 s, 138 MB/s
```

Use the above file information. Since the partition 1 starts from sector 1071, the first 1071 sector is skipped(assuming the sector number starts from 0). The length of partition 1 is 102312 sectors, so we copy 102312 input blocks.

2. Make an empty directory as a mount point and mount `boot.img`, executing: `mount -o loop boot.img /mnt/your-mount-dir`. Show the content under the mounted directory.

```
xy@xy-vm:~/Downloads$ mkdir tmp
xy@xy-vm:~/Downloads$ sudo mount -o loop boot.img ./tmp
xy@xy-vm:~/Downloads$ ls ./tmp/
dtb  EFI  MLO  ubldr.bin  u-boot.img
```

3. Using `objdump(1)`, `hexdump(1)` and `file(1)`, what information can be extracted from the file `u-boot.img`? What is the entry address of the bootloader?

`objdump(1)` and `hexdump(1)` don't work.

```
xy@xy-vm:~/Downloads/tmp$ file u-boot.img
u-boot.img: u-boot legacy uImage, U-Boot 2018.09 for am335x board,
Firmware/ARM, Firmware Image (Not compressed), 409104 bytes, Fri Dec 7
01:55:55 2018, Load Address: 0x80800000, Entry Point: 0x00000000, Header
CRC: 0xD0B63EDC, Data CRC: 0x3DE7011A
xy@xy-vm:~/Downloads/tmp$ cd ..
xy@xy-vm:~/Downloads$ sudo umount ./tmp
```

The entry address of bootloader is 0x80800000.

1. https://en.wikipedia.org/wiki/Master_boot_record 