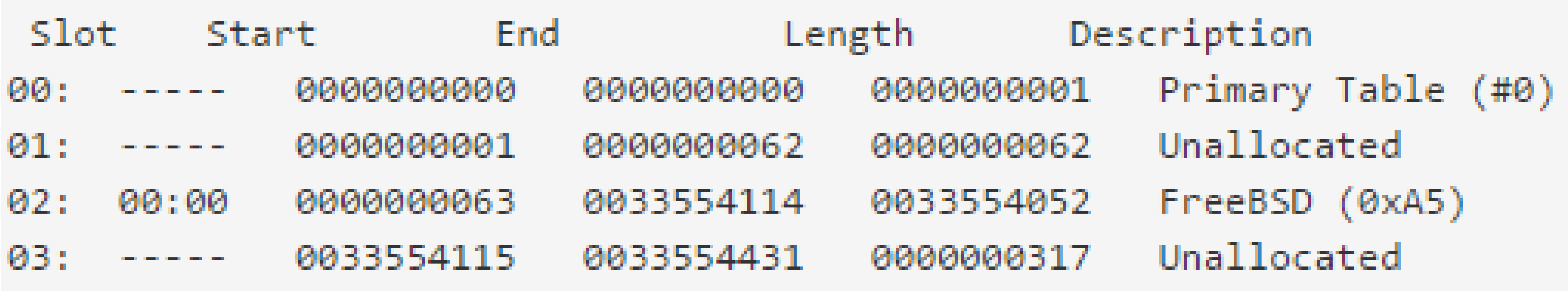
VOLUME ANALYSIS - PART III

COMP 597 – Computer Forensics

BSD Server Partitioning

- FreeBSD
- NetBSD
- OpenBSD

BSD Partition System



```
     Slot      Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000062   0000000062   Unallocated
02:  00:00   0000000063   0033554114   0033554052   FreeBSD (0xA5)
03:  -----   0033554115   0033554431   0000000317   Unallocated
```

From: https://digital-forensics.sans.org/blog/2010/02/10/freebsd-computer-forensic-tips-tricks/

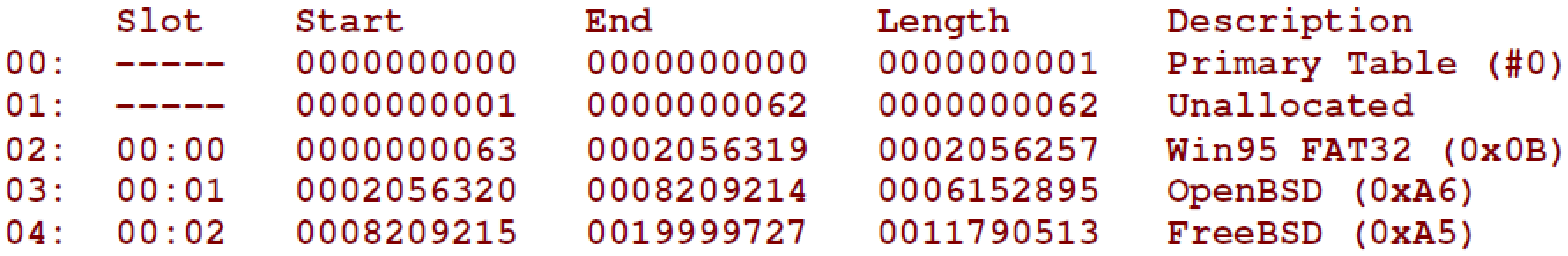
BSD Partition System

- Can be integrated inside a DOS partition
- Uses only 1 sector
- Located in the 2nd sector of BSD partition

BSD Partition System

Value	Partition Type
0xa5	FreeBSD
0xa6	OpenBSD
0xa9	NetBSD

BSD Partition System



```
      Slot      Start        End          Length       Description
00:   -----     0000000000   0000000000   0000000001   Primary Table (#0)
01:   -----     0000000001   0000000062   0000000062   Unallocated
02:   00:00     0000000063   0002056319   0002056257   Win95 FAT32 (0x0B)
03:   00:01     0002056320   0008209214   0006152895   OpenBSD (0xA6)
04:   00:02     0008209215   0019999727   0011790513   FreeBSD (0xA5)
```

From: File System Forensic Analysis, 2nd edition, Brian Carrier

BSD Disk Label

Byte Range	Description
0–3	0x82564557
4–131	Drive Information
132–135	0x82564557
136–137	Checksum
138–139	Number of partitions
140–143	Size of boot area
144–147	Maximum size of file system boot super block
148–163	BSD Partition #1
164–179	BSD Partition #2
180-371	BSD Partitions 3 to 14
372–387	BSD Partition #15
388–403	BSD Partition #16
404–511	Unused

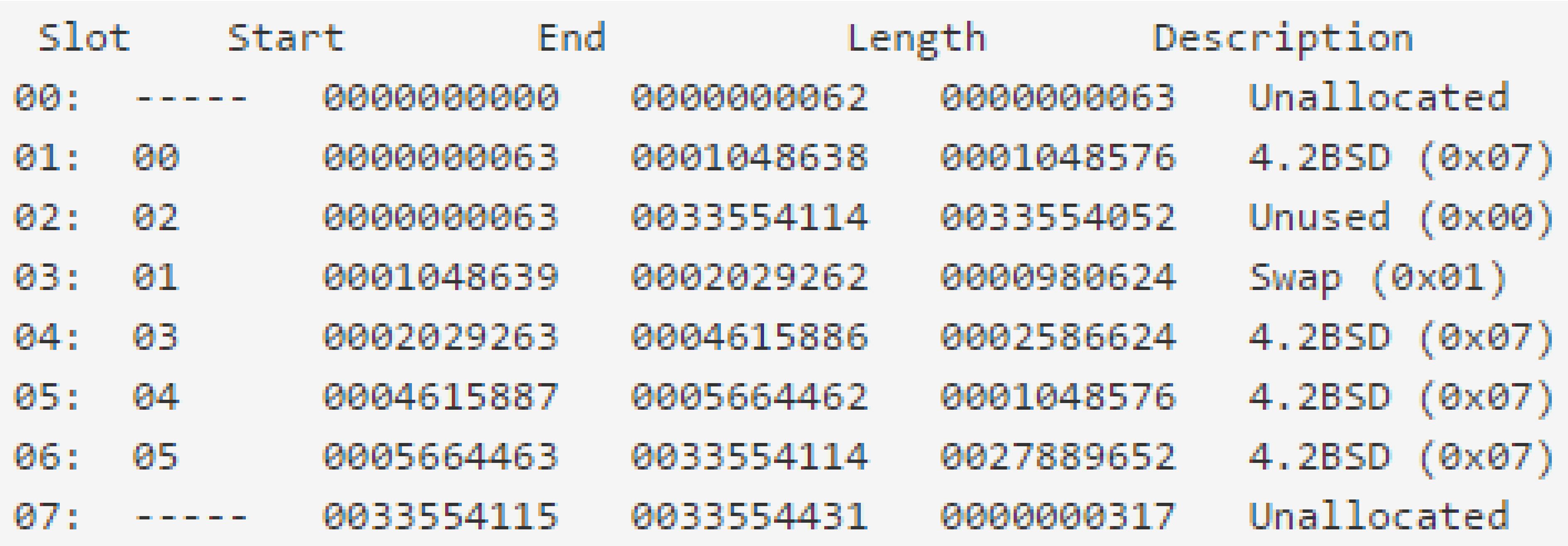
BSD Disk Label - Entry

Bytes	Description
4	Size of BSD partition
4	Start of the BSD partition
4	UFS File system fragment size
1	Partition Type
1	UFS File system fragments per block
2	UFS File system cylinders per group

BSD Disk Label - Entry

Type	Description
0	Unused Slot
1	Swap space
5	4.1BSD
7	4.2BSD fast file system (FFS)
8	MSDOS file system (FAT)
10	In use, but unknown
12	CD-ROM (ISO9660)

BSD Disk Label - Entry



```
 Slot     Start        End          Length       Description
00:   -----     0000000000   0000000062   0000000063    Unallocated
01:   00        0000000063   0001048638   0001048576    4.2BSD (0x07)
02:   02        0000000063   0033554114   0033554052    Unused (0x00)
03:   01        0001048639   0002029262   0000980624    Swap (0x01)
04:   03        0002029263   0004615886   0002586624    4.2BSD (0x07)
05:   04        0004615887   0005664462   0001048576    4.2BSD (0x07)
06:   05        0005664463   0033554114   0027889652    4.2BSD (0x07)
07:   -----     0033554115   0033554431   0000000317    Unallocated
```

From: https://digital-forensics.sans.org/blog/2010/02/10/freebsd-computer-forensic-tips-tricks/

BSD Partition System

- What happens to the non-BSD partitions?

BSD Partition System

- FreeBSD
  - Reads DOS & its own partition information
- OpenBSD & NetBSD
  - Only partitions listed in its disk label are visible

BSD Partition System

Suppose we have the following configuration:

Hard Disk 1

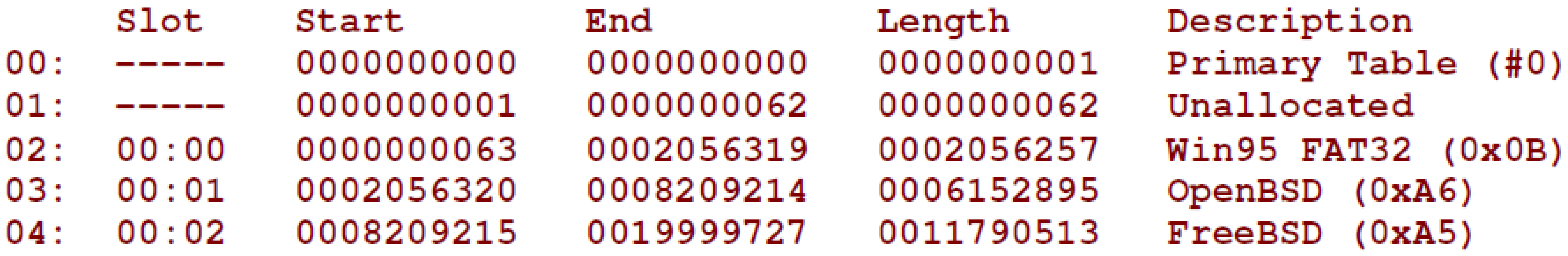
- Dos system:
  - Three partitions
  - Including FreeBSD
- FreeBSD system:
  - Four partitions

Hard Disk 2

- OpenBSD system:
  - Five partitions

OpenBSD

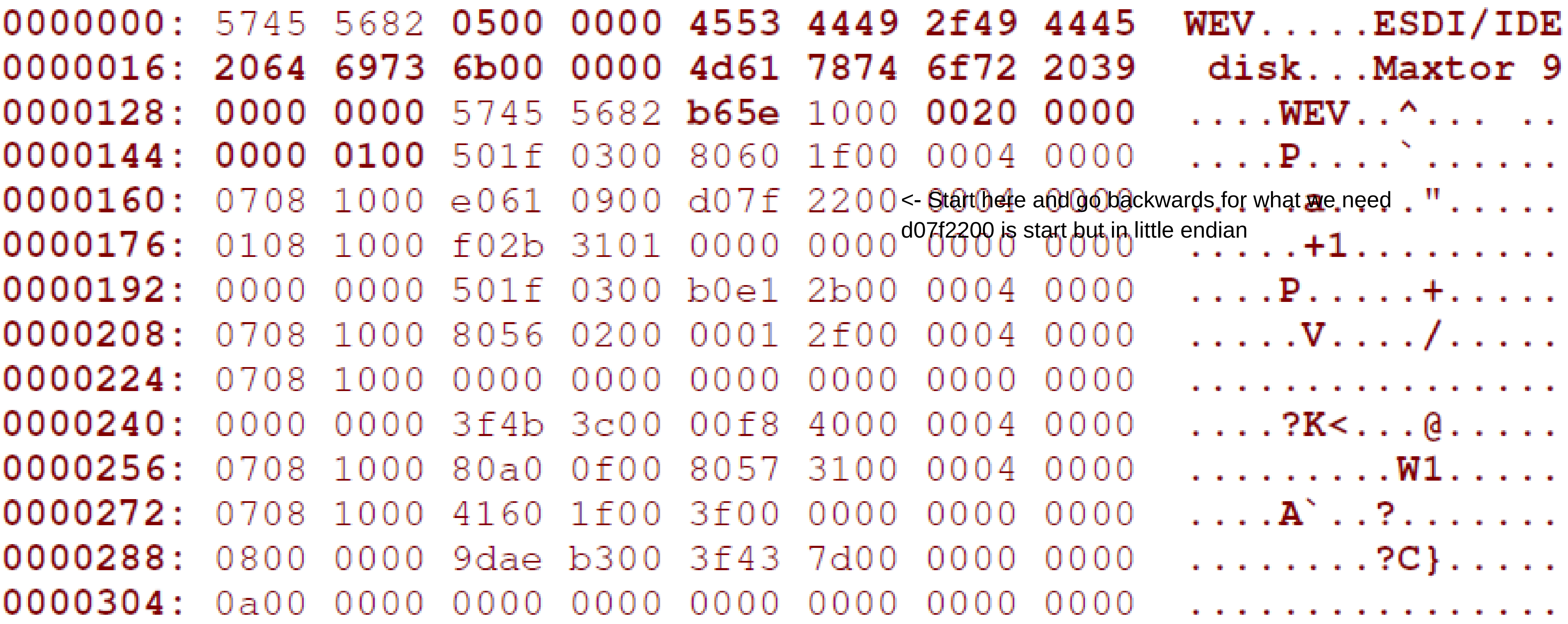
OpenBSD Example



```
     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000062   0000000062   Unallocated
02:  00:00   0000000063   0002056319   0002056257   Win95 FAT32 (0x0B)
03:  00:01   0002056320   0008209214   0006152895   OpenBSD (0xA6)
04:  00:02   0008209215   0019999727   0011790513   FreeBSD (0xA5)
```

From: File System Forensic Analysis, 2nd edition, Brian Carrier

OpenBSD Example

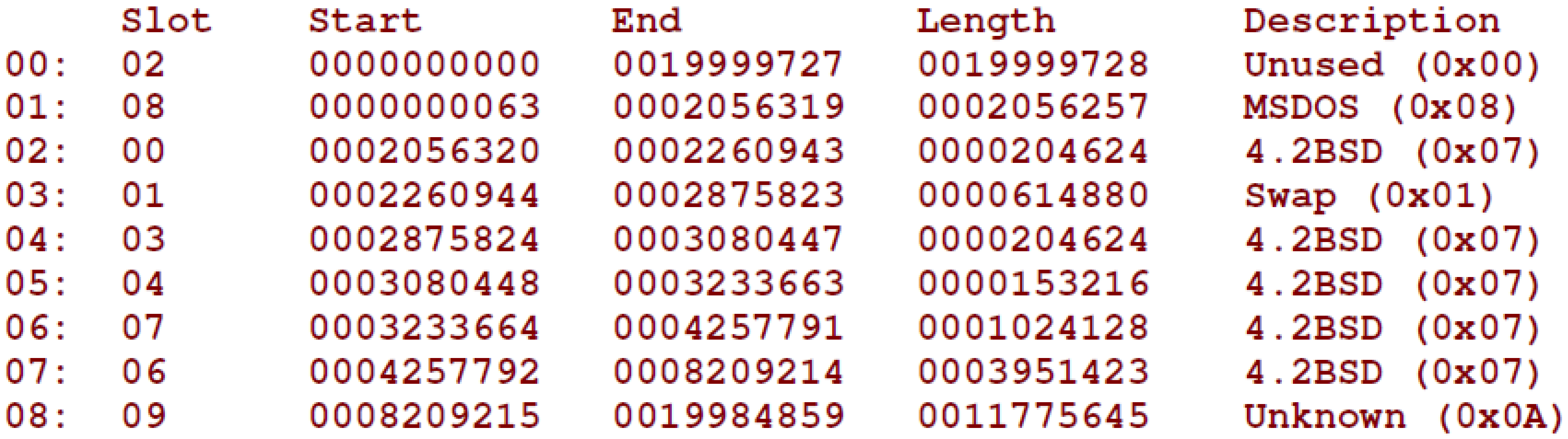


```
0000000: 5745 5682 0500 0000 4553 4449 2f49 4445  WEV.....ESDI/IDE
0000016: 2064 6973 6b00 0000 4d61 7874 6f72 2039   disk...Maxtor 9
0000128: 0000 0000 5745 5682 b65e 1000 0020 0000  ....WEV..^... ..
0000144: 0000 0100 501f 0300 8060 1f00 0004 0000  ....P....`......
0000160: 0708 1000 e061 0900 d07f 2200 0004 0000  .....a....".....
0000176: 0108 1000 f02b 3101 0000 0000 0000 0000  .....+1.........
0000192: 0000 0000 501f 0300 b0e1 2b00 0004 0000  ....P.....+.....
0000208: 0708 1000 8056 0200 0001 2f00 0004 0000  .....V..../.....
0000224: 0708 1000 0000 0000 0000 0000 0000 0000  ................
0000240: 0000 0000 3f4b 3c00 00f8 4000 0004 0000  ....?K<...@.....
0000256: 0708 1000 80a0 0f00 8057 3100 0004 0000  .........W1.....
0000272: 0708 1000 4160 1f00 3f00 0000 0000 0000  ....A`..?.......
0000288: 0800 0000 9dae b300 3f43 7d00 0000 0000  ........?C}.....
0000304: 0a00 0000 0000 0000 0000 0000 0000 0000  ................
```

<- Start here and go backwards for what we need
d07f2200 is start but in little endian

From: File System Forensic Analysis, 2nd edition, Brian Carrier

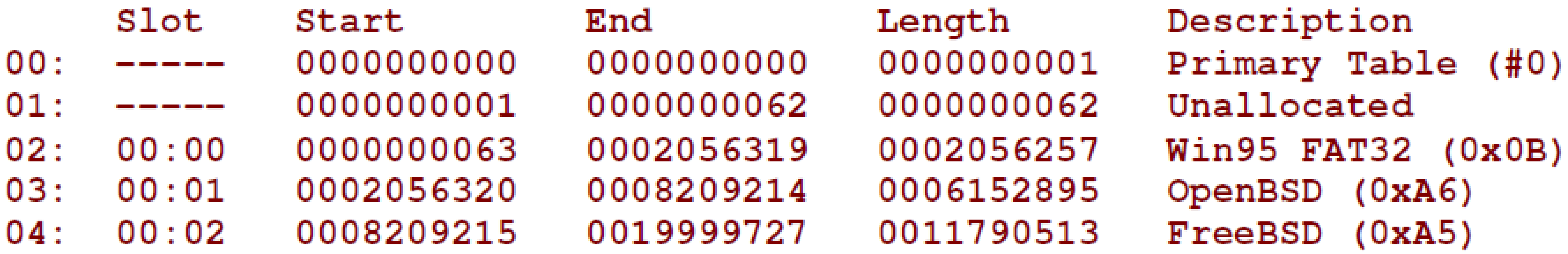
OpenBSD Example



```
      Slot    Start        End          Length       Description
00:   02      0000000000   0019999727   0019999728   Unused (0x00)
01:   08      0000000063   0002056319   0002056257   MSDOS (0x08)
02:   00      0002056320   0002260943   0000204624   4.2BSD (0x07)
03:   01      0002260944   0002875823   0000614880   Swap (0x01)
04:   03      0002875824   0003080447   0000204624   4.2BSD (0x07)
05:   04      0003080448   0003233663   0000153216   4.2BSD (0x07)
06:   07      0003233664   0004257791   0001024128   4.2BSD (0x07)
07:   06      0004257792   0008209214   0003951423   4.2BSD (0x07)
08:   09      0008209215   0019984859   0011775645   Unknown (0x0A)
```

FreeBSD

FreeBSD Example

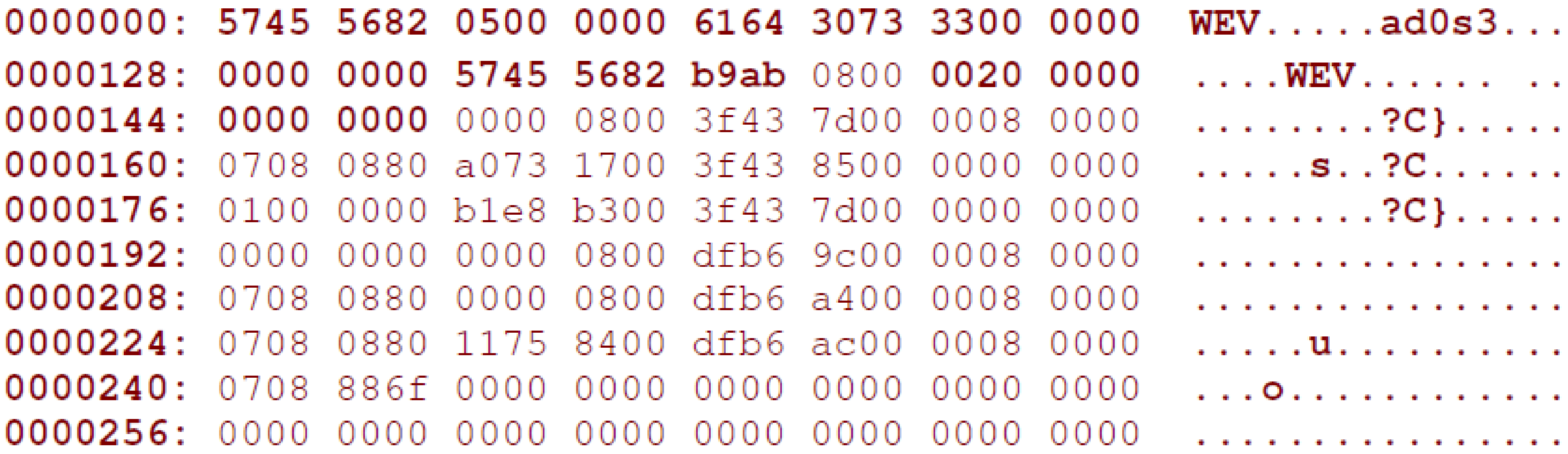


```
     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000062   0000000062   Unallocated
02:  00:00   0000000063   0002056319   0002056257   Win95 FAT32 (0x0B)
03:  00:01   0002056320   0008209214   0006152895   OpenBSD (0xA6)
04:  00:02   0008209215   0019999727   0011790513   FreeBSD (0xA5)
```

Look for partition table at 0008209216

From: File System Forensic Analysis, 2nd edition, Brian Carrier

FreeBSD Example

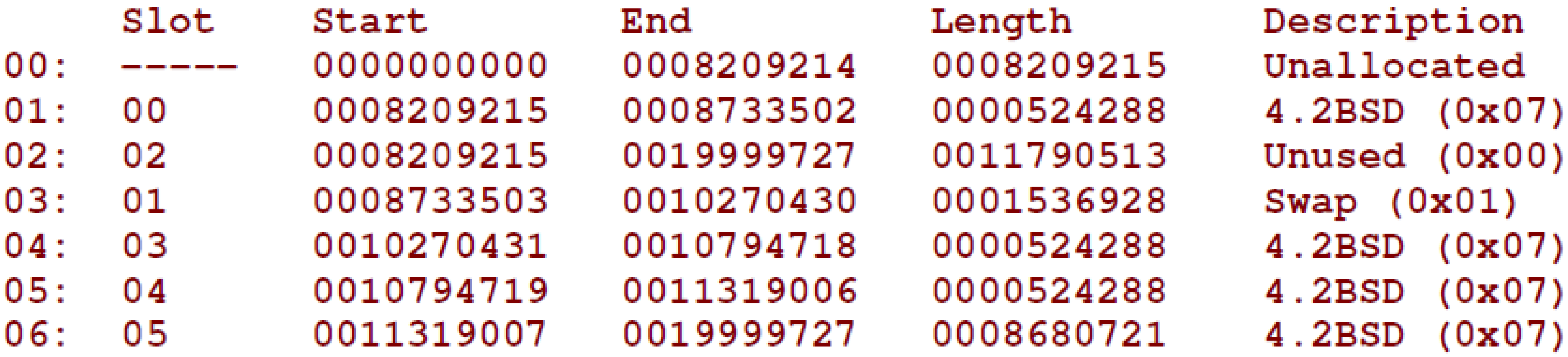


```
0000000: 5745 5682 0500 0000 6164 3073 3300 0000  WEV.....ad0s3...
0000128: 0000 0000 5745 5682 b9ab 0800 0020 0000  ....WEV...... ..
0000144: 0000 0000 0000 0800 3f43 7d00 0008 0000  ........?C}.....
0000160: 0708 0880 a073 1700 3f43 8500 0000 0000  .....s..?C......
0000176: 0100 0000 b1e8 b300 3f43 7d00 0000 0000  ........?C}.....
0000192: 0000 0000 0000 0800 dfb6 9c00 0008 0000  ................
0000208: 0708 0880 0000 0800 dfb6 a400 0008 0000  ................
0000224: 0708 0880 1175 8400 dfb6 ac00 0008 0000  .....u..........
0000240: 0708 886f 0000 0000 0000 0000 0000 0000  ...o............
0000256: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

Types are far left two

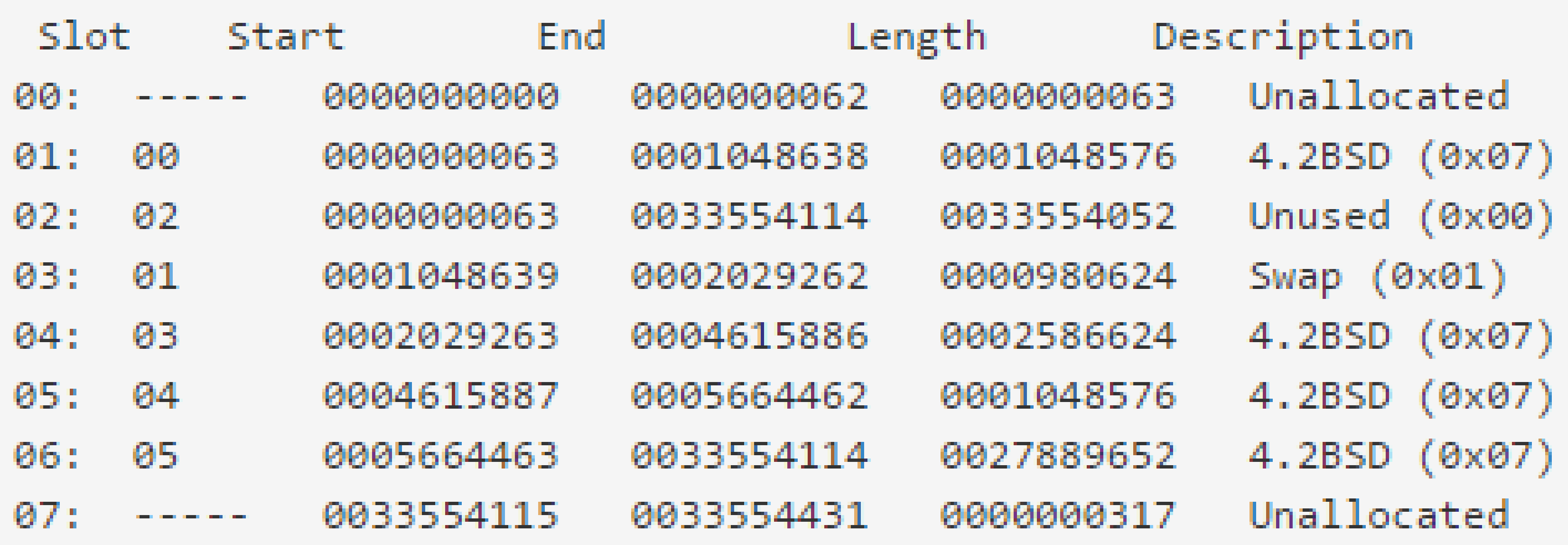
From: File System Forensic Analysis, 2nd edition, Brian Carrier

FreeBSD Example



```
     Slot    Start        End          Length       Description
00:  -----   0000000000   0008209214   0008209215   Unallocated
01:  00      0008209215   0008733502   0000524288   4.2BSD (0x07)
02:  02      0008209215   0019999727   0011790513   Unused (0x00)
03:  01      0008733503   0010270430   0001536928   Swap (0x01)
04:  03      0010270431   0010794718   0000524288   4.2BSD (0x07)
05:  04      0010794719   0011319006   0000524288   4.2BSD (0x07)
06:  05      0011319007   0019999727   0008680721   4.2BSD (0x07)
```

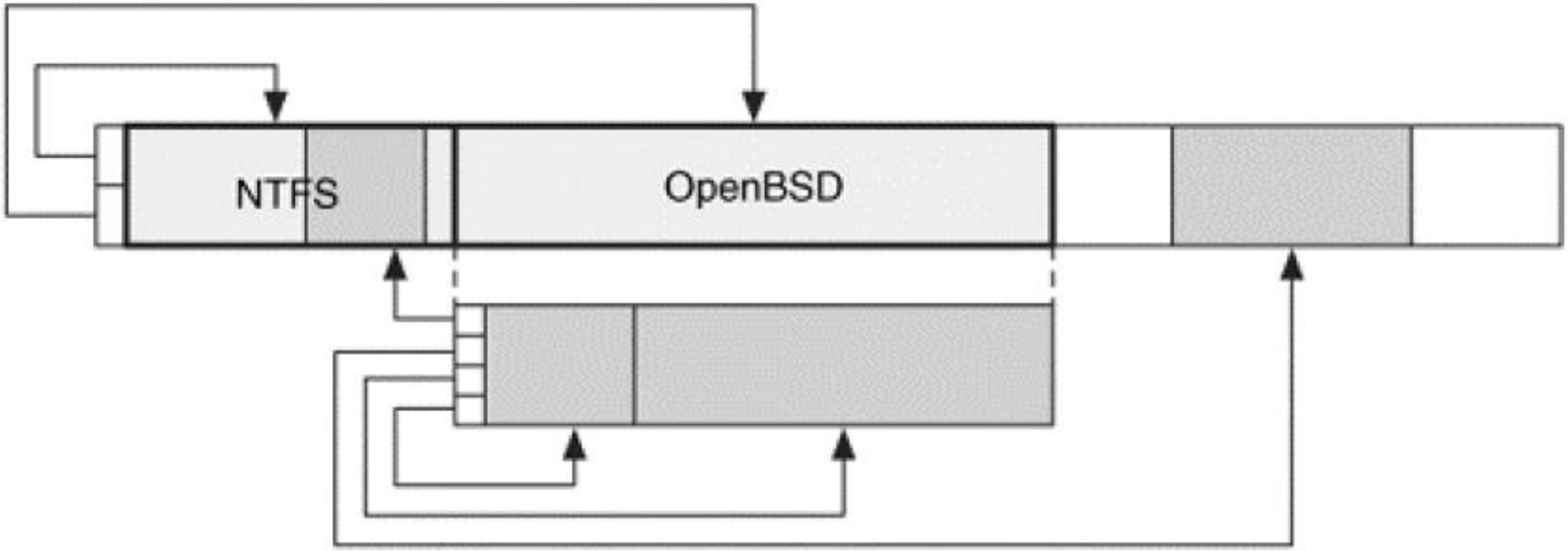
Exercise 1



```
 Slot    Start        End          Length       Description
00:  -----   0000000000   0000000062   0000000063   Unallocated
01:  00      0000000063   0001048638   0001048576   4.2BSD (0x07)
02:  02      0000000063   0033554114   0033554052   Unused (0x00)
03:  01      0001048639   0002029262   0000980624   Swap (0x01)
04:  03      0002029263   0004615886   0002586624   4.2BSD (0x07)
05:  04      0004615887   0005664462   0001048576   4.2BSD (0x07)
06:  05      0005664463   0033554114   0027889652   4.2BSD (0x07)
07:  -----   0033554115   0033554431   0000000317   Unallocated
```

From: https://digital-forensics.sans.org/blog/2010/02/10/freebsd-computer-forensic-tips-tricks/

Exercise 2



From: File System Forensic Analysis, 2nd edition, Brian Carrier

Dos partition with OpenBSD partition, NTF, and unused space
OpenBSD with first pointer to part of NTFS (****this isnt good, huge red flag that someone modified something), The second pointer is not pointing to the entire allocated space, this is a huge sign that someone modified something, also you cant point to unallocated space
Purpose of root is the hierarchy of the file system

References

1. File System Forensic Analysis, 2nd edition, Brian Carrier, 2005.