VOLUME ANALYSIS - PART I

COMP 597 – Computer Forensics

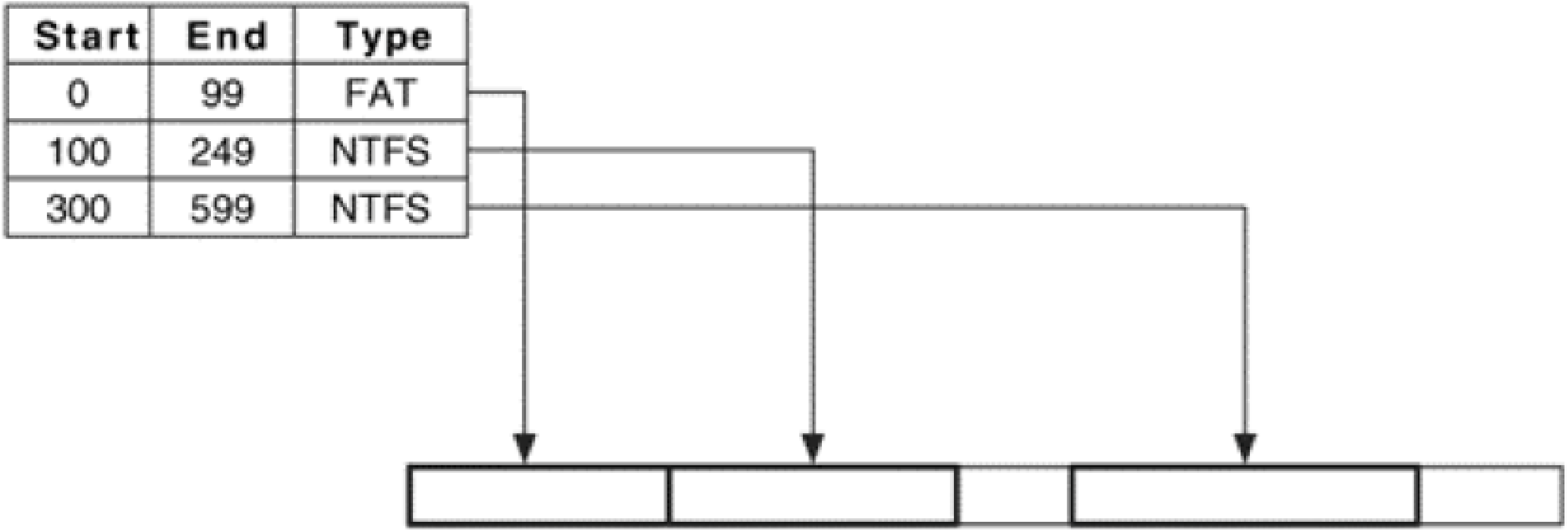
Volume Analysis

- What is volume analysis?

Volumes

- Volumes are used to:
  - assemble multiple storage devices or partitions into one
  - partition a storage device or partition into independent partitions

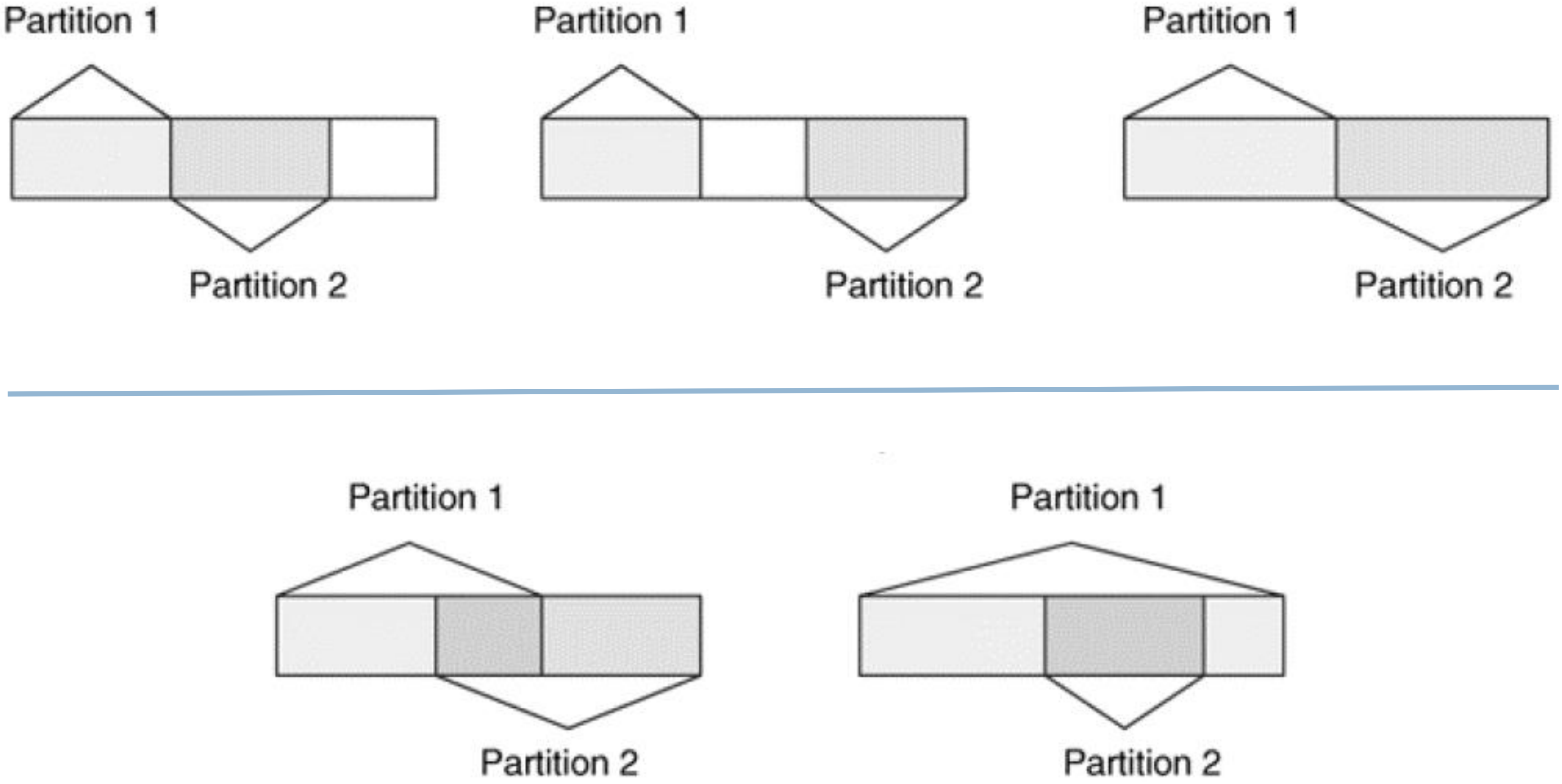
Partition System



Start	End	Type
0	99	FAT
100	249	NTFS
300	599	NTFS

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

Partition System - Example



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

PC-based Partitions

Examples:

- DOS
- Apple
- GPT

DOS partitions

- Very common
- Complicated
- Has an MBR in sector 0

DOS - Partition Table

- Flag (1 byte)
- Starting CHS address (3 bytes)
- Type of partition (1 byte)
- Ending CHS address (3 bytes)
- Starting LBA address (4 bytes)
- Number of sectors in partition (4 bytes)

DOS – Type Field

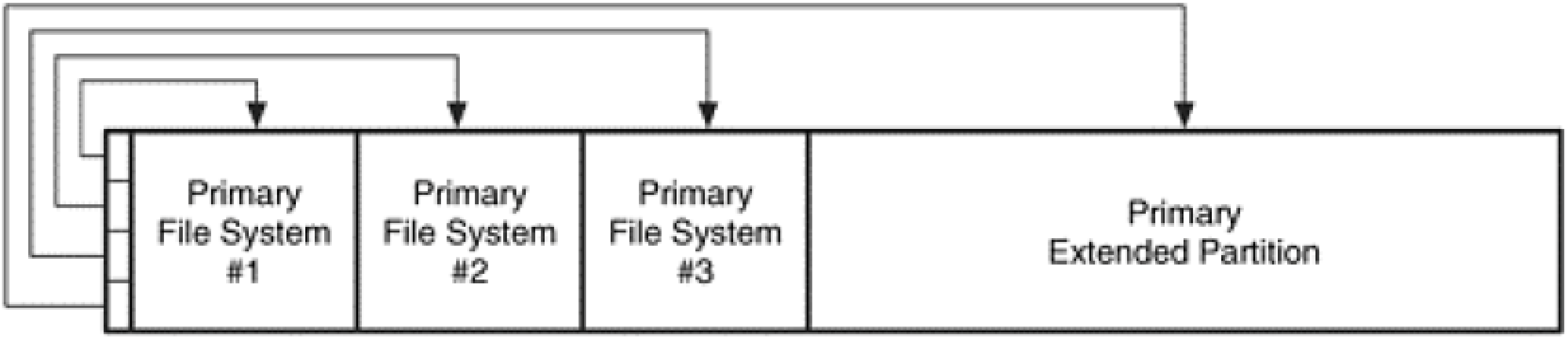
Value	Partition Type
0x01	FAT12, CHS
0x04	FAT16, 16–32 MB, CHS
0x05	Microsoft Extended, CHS
0x07	NTFS
0x0b	FAT32, CHS
0x0c	FAT32, LBA
0x0f	Microsoft Extended, LBA

Value	Partition Type
0x82	Linux Swap
0x83	Linux
0x85	Linux Extended
0xa5	FreeBSD
0xa6	OpenBSD
0xa8	Mac OSX
0xab	Mac OSX Boot

Partition Analysis Tools

- fdisk
  - fdisk –lu image.dd
- mmls
  - mmls image.dd

DOS - Extended Partition



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

DOS – Secondary Extended Partition

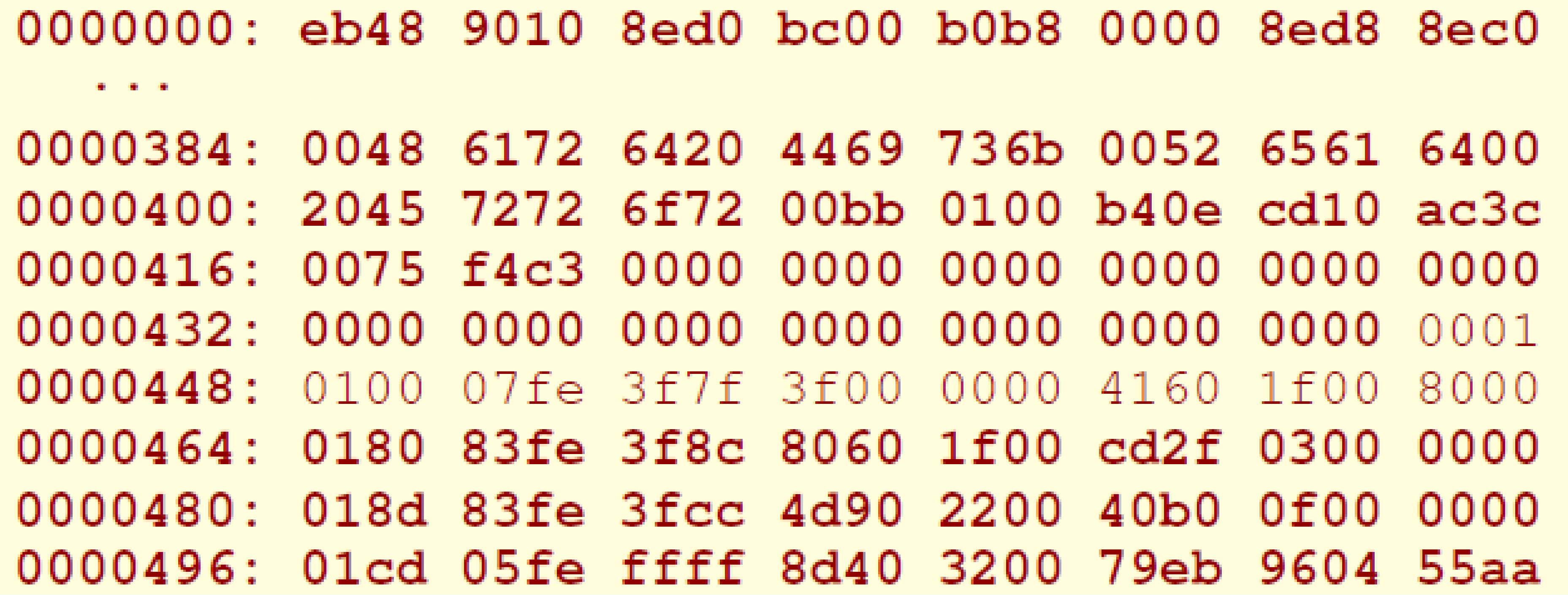
- Two entries:
  - Partition entry
  - Extended partition entry

DOS – Secondary Extended Partition

- Exercise:

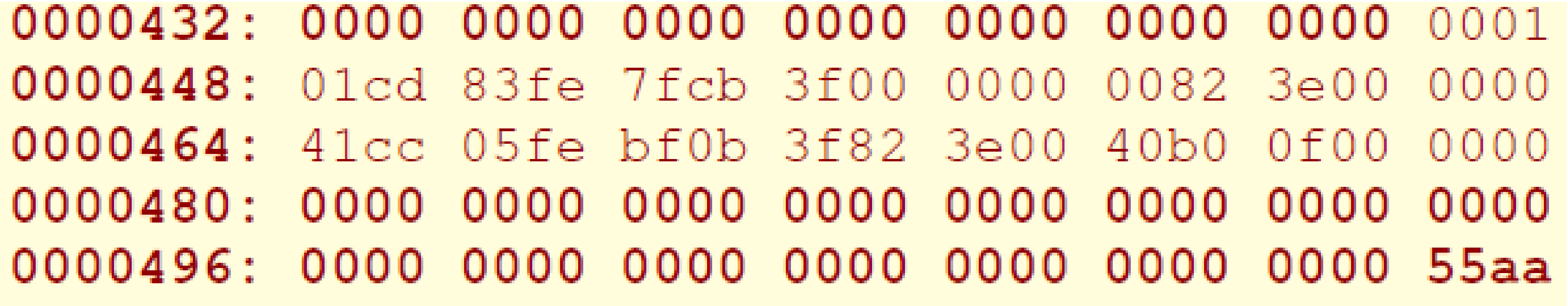
We have a 120GB hard disk and we want to have six partitions, 20GBs each

DOS – Example



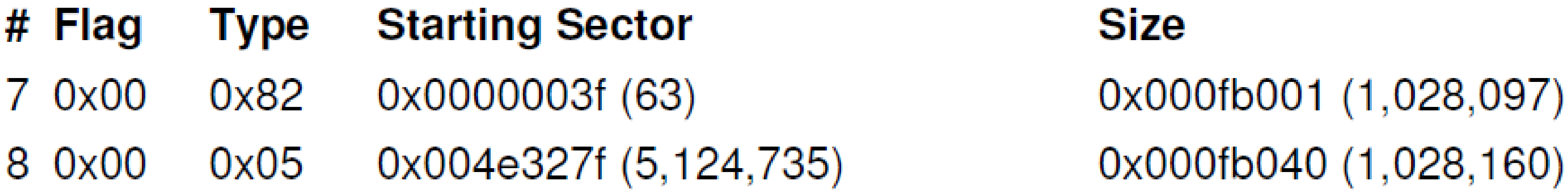
```
0000000: eb48 9010 8ed0 bc00 b0b8 0000 8ed8 8ec0
   ...
0000384: 0048 6172 6420 4469 736b 0052 6561 6400
0000400: 2045 7272 6f72 00bb 0100 b40e cd10 ac3c
0000416: 0075 f4c3 0000 0000 0000 0000 0000 0000
0000432: 0000 0000 0000 0000 0000 0000 0000 0001
0000448: 0100 07fe 3f7f 3f00 0000 4160 1f00 8000
0000464: 0180 83fe 3f8c 8060 1f00 cd2f 0300 0000
0000480: 018d 83fe 3fcc 4d90 2200 40b0 0f00 0000
0000496: 01cd 05fe ffff 8d40 3200 79eb 9604 55aa
```

DOS – Example



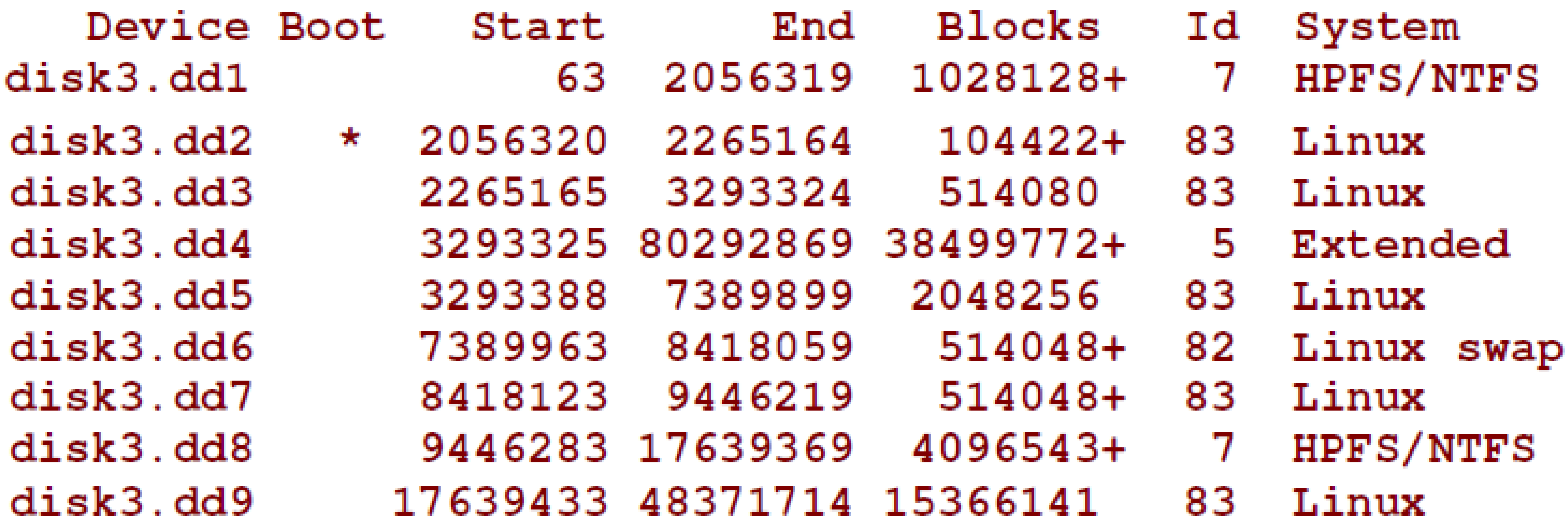
```
0000432: 0000 0000 0000 0000 0000 0000 0000 0001
0000448: 01cd 83fe 7fcb 3f00 0000 0082 3e00 0000
0000464: 41cc 05fe bf0b 3f82 3e00 40b0 0f00 0000
0000480: 0000 0000 0000 0000 0000 0000 0000 0000
0000496: 0000 0000 0000 0000 0000 0000 0000 55aa
```

DOS – Example



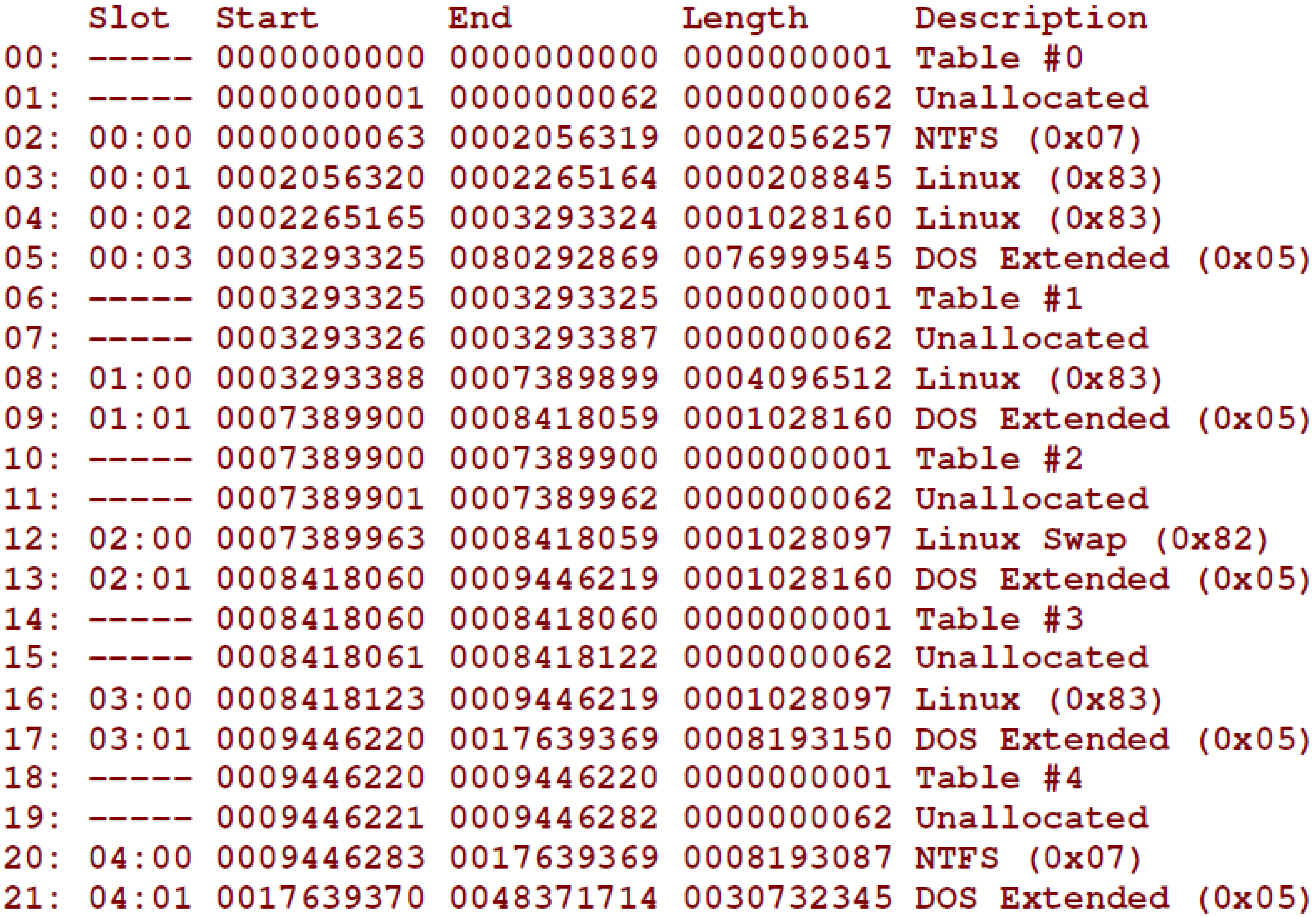
#	Flag	Type	Starting Sector	Size
7	0x00	0x82	0x0000003f (63)	0x000fb001 (1,028,097)
8	0x00	0x05	0x004e327f (5,124,735)	0x000fb040 (1,028,160)

DOS – Example (fdisk)



```
   Device Boot    Start       End    Blocks   Id  System
disk3.dd1            63   2056319  1028128+   7  HPFS/NTFS
disk3.dd2   *   2056320   2265164   104422+  83  Linux
disk3.dd3       2265165   3293324   514080   83  Linux
disk3.dd4       3293325  80292869 38499772+   5  Extended
disk3.dd5       3293388   7389899  2048256   83  Linux
disk3.dd6       7389963   8418059   514048+  82  Linux swap
disk3.dd7       8418123   9446219   514048+  83  Linux
disk3.dd8       9446283  17639369  4096543+   7  HPFS/NTFS
disk3.dd9      17639433  48371714 15366141   83  Linux
```

DOS – Example (mmls)



```
     Slot   Start        End          Length       Description
00:  -----  0000000000   0000000000   0000000001   Table #0
01:  -----  0000000001   0000000062   0000000062   Unallocated
02:  00:00  0000000063   0002056319   0002056257   NTFS (0x07)
03:  00:01  0002056320   0002265164   0000208845   Linux (0x83)
04:  00:02  0002265165   0003293324   0001028160   Linux (0x83)
05:  00:03  0003293325   0080292869   0076999545   DOS Extended (0x05)
06:  -----  0003293325   0003293325   0000000001   Table #1
07:  -----  0003293326   0003293387   0000000062   Unallocated
08:  01:00  0003293388   0007389899   0004096512   Linux (0x83)
09:  01:01  0007389900   0008418059   0001028160   DOS Extended (0x05)
10:  -----  0007389900   0007389900   0000000001   Table #2
11:  -----  0007389901   0007389962   0000000062   Unallocated
12:  02:00  0007389963   0008418059   0001028097   Linux Swap (0x82)
13:  02:01  0008418060   0009446219   0001028160   DOS Extended (0x05)
14:  -----  0008418060   0008418060   0000000001   Table #3
15:  -----  0008418061   0008418122   0000000062   Unallocated
16:  03:00  0008418123   0009446219   0001028097   Linux (0x83)
17:  03:01  0009446220   0017639369   0008193150   DOS Extended (0x05)
18:  -----  0009446220   0009446220   0000000001   Table #4
19:  -----  0009446221   0009446282   0000000062   Unallocated
20:  04:00  0009446283   0017639369   0008193087   NTFS (0x07)
21:  04:01  0017639370   0048371714   0030732345   DOS Extended (0x05)
```

Extracting Partitions

- How do we extract from an image:
  - MBR
  - Deleted partitions
  - Volume partitions

Recovering Deleted Partitions

- Why do we need to recover partitions?

Multiple Operating Systems

- Boot sector handles it
- MBR code handles it

Modified Extended Partition

Modified Extended Partition

- Can an extended partition table have more than two entries?

References

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