VOLUME ANALYSIS - PART II

COMP 597 – Computer Forensics

Volume Analysis

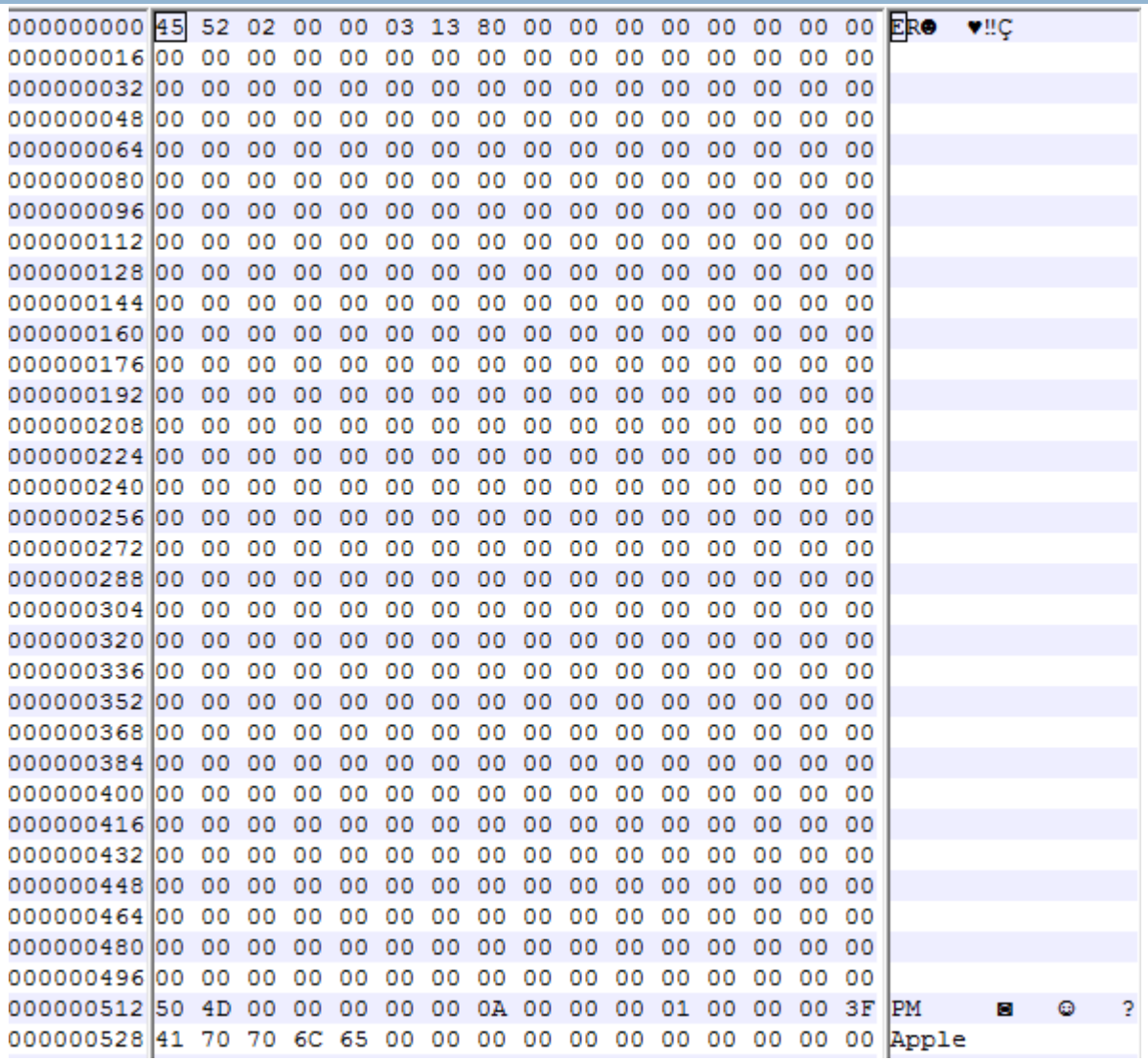
- Apple partitions
- GPT partitions

Apple Partition

Apple Partition

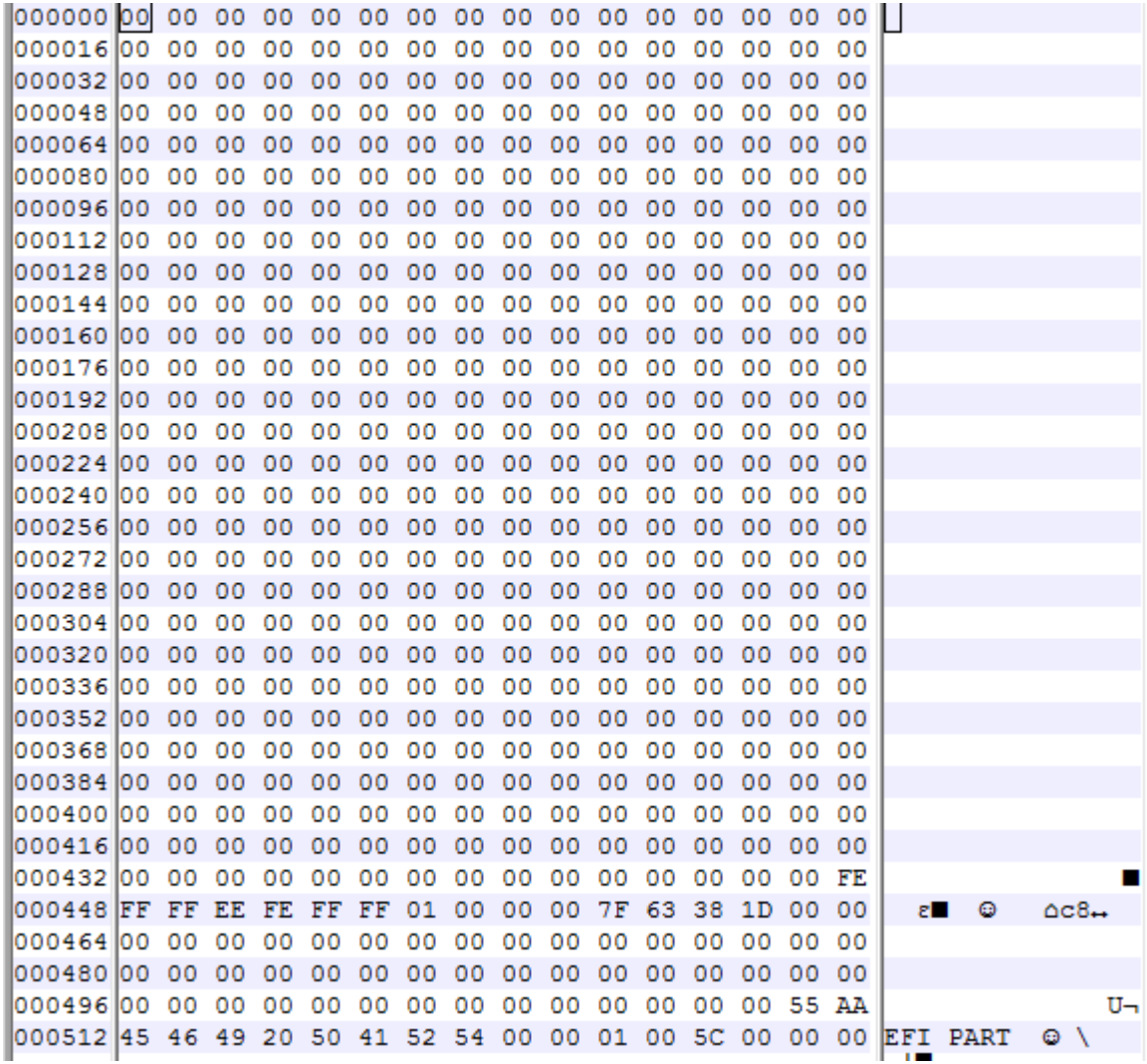
- PowerPC Mac
- Intel Mac

Apple Partition - PowerPC



```
000000000 45 52 02 00 00 03 13 80 00 00 00 00 00 00 00 00 ER☻  ♥‼Ç
000000016 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000032 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000048 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000064 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000096 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000112 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000128 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000144 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000176 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000192 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000208 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000224 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000256 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000272 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000288 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000304 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000336 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000352 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000368 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000384 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000416 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000432 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000448 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000464 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000496 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000512 50 4D 00 00 00 00 00 0A 00 00 00 01 00 00 00 3F PM      ◙    ☺    ?
000000528 41 70 70 6C 65 00 00 00 00 00 00 00 00 00 00 00 Apple
```

Apple Partition - Intel

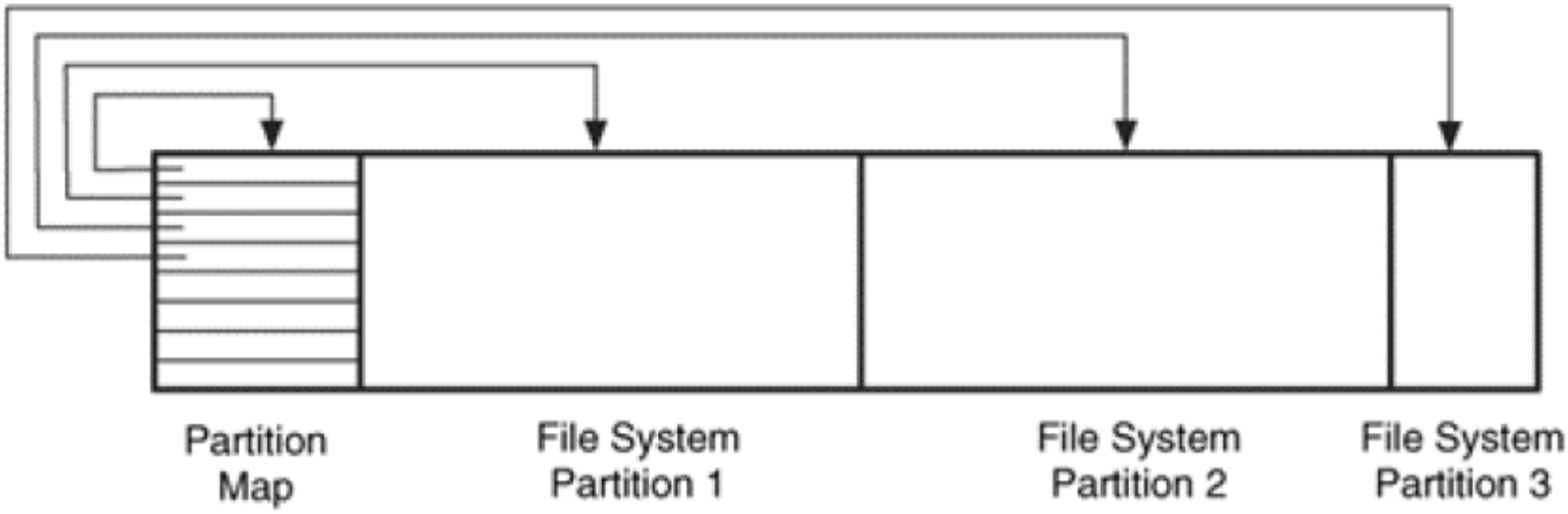


```
000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000016 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000032 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000048 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000064 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000096 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000112 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000128 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000144 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000176 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000192 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000208 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000224 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000256 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000272 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000288 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000304 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000336 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000352 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000368 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000384 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000416 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000432 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FE                 ■
000448 FF FF EE FE FF FF 01 00 00 00 7F 63 38 1D 00 00   ε■  ☺    ⌂c8↔
000464 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000496 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA               U¬
000512 45 46 49 20 50 41 52 54 00 00 01 00 5C 00 00 00 EFI PART  ☺ \
                                                        ■
```

Apple Partition Map

- Can describe any number of partitions
- Uses multiple consecutive sectors
- No boot code
- Located at the beginning of the disk

Apple Partition Map



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

Apple Partition

#	Byte Range	Entry Description
1	0–1	Signature value (0x504D)
2	2–3	Reserved
3	4–7	Total Number of partitions
4	8–11	Starting sector of partition
5	12–15	Size of partition in sectors
6	16–47	Name of partition in ASCII
7	48–79	Type of partition in ASCII
8	80–83	Starting sector of data area in partition
9	84–87	Size of data area in sectors
10	88–91	Status of partition (see table 5-8)
11	92–95	Starting sector of boot code
12	96–99	Size of boot code in sectors
13	100–103	Address of boot loader code
14	104–107	Reserved
15	108–111	Boot code entry point
16	112–115	Reserved
17	116–119	Boot code checksum
18	120–135	Processor type
19	136–511	Reserved

Apple Partition Map

#	Type
1	Apple_Driver43
2	Apple_Driver43_CD
3	Apple_Driver_ATA
4	Apple_Free
5	Apple_HFS
6	Apple_HFSX
7	Apple_MFS
8	Apple_Partition_Map
9	Apple_UFS

Apple Partition Map

```
000000512 50 4D 00 00 00 00 00 0A 00 00 00 01 00 00 00 3F PM      ◙    ☺    ?
000000528 41 70 70 6C 65 00 00 00 00 00 00 00 00 00 00 00 Apple
000000544 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000560 41 70 70 6C 65 5F 70 61 72 74 69 74 69 6F 6E 5F Apple_partition_
000000576 6D 61 70 00 00 00 00 00 00 00 00 00 00 00 00 00 map
000000592 00 00 00 00 00 00 00 3F 00 00 00 03 00 00 00 00        ?    ♥
000000608 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000624 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000640 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000656 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000672 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000688 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000704 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000720 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000736 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000752 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000768 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000784 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000816 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000832 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000848 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000864 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000880 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000896 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000912 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000928 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000944 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000960 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000976 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000992 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001008 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001024 50 4D 00 00 00 00 00 0A 00 00 00 40 00 00 80 B8 PM      ◙    @    Ç╕
```

Apple Partition Map

- How do we retrieve the first partition?

```
0000000: 504d 0000 0000 000a 0000 0001 0000 003f  PM.............?
0000016: 4170 706c 6500 0000 0000 0000 0000 0000  Apple...........
0000032: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000048: 4170 706c 655f 7061 7274 6974 696f 6e5f  Apple_partition_
0000064: 6d61 7000 0000 0000 0000 0000 0000 0000  map.............
0000080: 0000 0000 0000 003f 0000 0000 0000 0000  .......?........
0000096: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

Apple Partition Map

```
MAC Partition Map
Units are in 512-byte sectors

     Slot   Start       End         Length      Description
00:  -----  0000000000  0000000000  0000000001  Unallocated
01:  00     0000000001  0000000063  0000000063  Apple_partition_map
02:  -----  0000000001  0000000010  0000000010  Table
03:  -----  0000000011  0000000063  0000000053  Unallocated
04:  01     0000000064  0000000117  0000000054  Apple_Driver43
05:  02     0000000118  0000000191  0000000074  Apple_Driver43
06:  03     0000000192  0000000245  0000000054  Apple_Driver_ATA
07:  04     0000000246  0000000319  0000000074  Apple_Driver_ATA
08:  05     0000000320  0000000519  0000000200  Apple_FWDriver
09:  06     0000000520  0000001031  0000000512  Apple_Driver_IOKit
10:  07     0000001032  0000001543  0000000512  Apple_Patches
11:  08     0000001544  0039070059  0039068516  Apple_HFS
12:  09     0039070060  0039070079  0000000020  Apple_Free
```

GPT

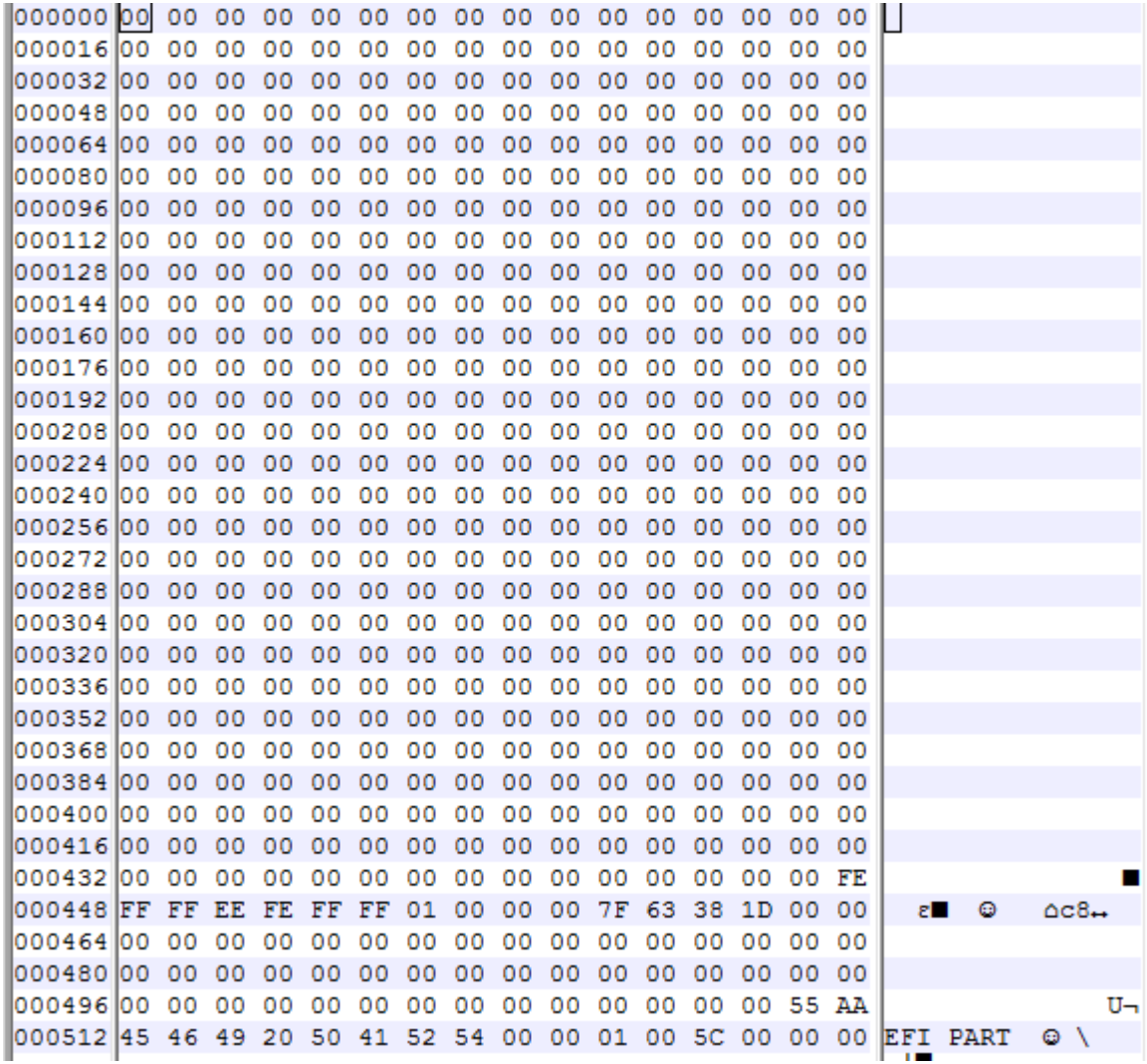
GPT

- Intel's current booting system
- *GUID Partition Table*
- Backup copy is maintained

GPT

1. Protective MBR
2. GPT header
3. Partition table
4. Partition area
5. Backup copy

GPT - Example

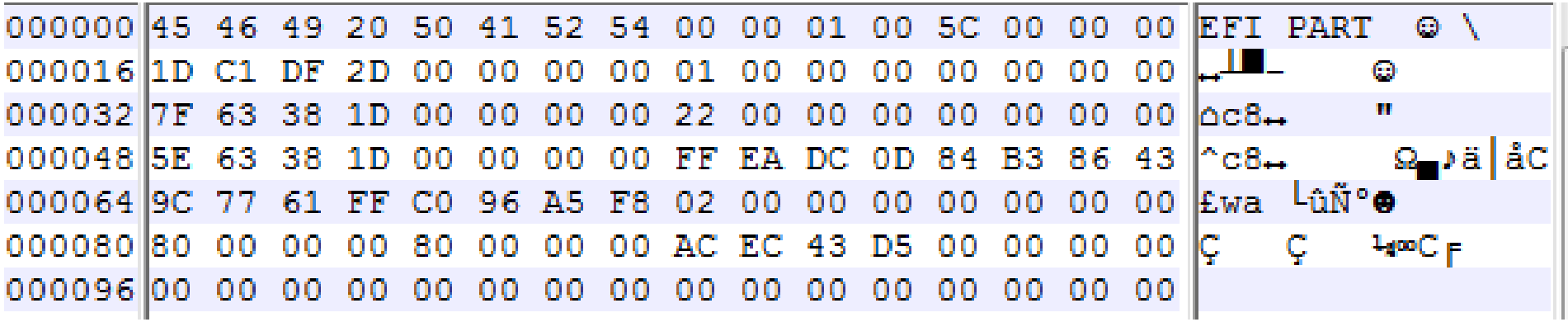


```
000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000016 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000032 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000048 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000064 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000096 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000112 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000128 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000144 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000176 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000192 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000208 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000224 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000256 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000272 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000288 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000304 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000336 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000352 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000368 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000384 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000416 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000432 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FE                                          ■
000448 FF FF EE FE FF FF 01 00 00 00 7F 63 38 1D 00 00   ε■  ☺    ⌂c8↔
000464 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000496 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA                                       U¬
000512 45 46 49 20 50 41 52 54 00 00 01 00 5C 00 00 00 EFI PART  ☺ \
                                                        ■
```

GPT Header

#	Byte Range	Entry Description
1	0–8	Signature value (0x4546492050415254)
2	8–11	Version
3	12–15	Size of GPT header in bytes
4	16–19	CRC32 checksum of GPT header
5	20–23	Reserved
6	24–31	LBA of current GPT header structure
7	32–39	LBA of the other GPT header structure
8	40–47	LBA of start of partition area
9	48–55	LBA of end of partition area
10	56–71	Disk GUID
11	72–79	LBA of the start of the partition table
12	80–83	Number of entries in partition table
13	84–87	Size of each entry in partition table
14	88–91	CRC32 checksum of partition table
15	92–511	Reserved

GPT Header



000000	45	46	49	20	50	41	52	54	00	00	01	00	5C	00	00	00
000016	1D	C1	DF	2D	00	00	00	00	01	00	00	00	00	00	00	00
000032	7F	63	38	1D	00	00	00	00	22	00	00	00	00	00	00	00
000048	5E	63	38	1D	00	00	00	00	FF	EA	DC	0D	84	B3	86	43
000064	9C	77	61	FF	C0	96	A5	F8	02	00	00	00	00	00	00	00
000080	80	00	00	00	80	00	00	00	AC	EC	43	D5	00	00	00	00
000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

EFI PART ☺ \
↔┘■– ☺
⌂c8↔ "
^c8↔ Ω▄♪ä│åC
£wa └ûÑ°☻
Ç Ç ↳∞C ƒ

GPT – Table Entry

#	Byte Range	Entry Description
1	0–15	Partition type GUID
2	16–31	Unique partition GUID
3	32–39	Starting LBA of partition
4	40–47	Ending LBA of partition
5	48–55	Partition attributes
6	56–127	Partition name in Unicode

GPT - GUID

8-4-4-4-12

```
typedef struct _GUID {
  DWORD Data1;
  WORD  Data2;
  WORD  Data3;
  BYTE  Data4[8];
} GUID;
```

GPT

001024	28	73	2A	C1	1F	F8	D2	11	BA	4B	00	A0	C9	3E	C9	3B
001040	E8	17	8B	DE	1E	7A	85	43	88	5B	B6	05	5B	67	84	DF
001056	28	00	00	00	00	00	00	00	27	40	06	00	00	00	00	00
001072	00	00	00	00	00	00	00	00	45	00	46	00	49	00	20	00
001088	53	00	79	00	73	00	74	00	65	00	6D	00	20	00	50	00
001104	61	00	72	00	74	00	69	00	74	00	69	00	6F	00	6E	00
001120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
001136	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

(s*┴▼°╥◄								K		á	╔	>	╔	;	
Φ‼ï		▌▲zàCê[						┼	♠	[	g	ä	■		
(								'	@	♠					
										E	F	I			
S	y	s	t	e	m			P							
a	r	t	i	t	i	o	n								

References

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