Sunucu Tabanlı Partitionlar

Dosya Sistem Analizi Hafta 6

Yrd. Doç. Dr. Erhan AKBAL

Giriş

- Bu bölüm ve bir önceki bölümün temel kavramları aynıdır.
- İntel 64 Bit GPT sistemlerine,
- FreeBSD, NetBSD ve OpenBSD bölümleme sistemlerine,
- Sun Solaris bölüm sistemlerine bakılacaktır.

I64 Sistemler - GPT (Guid Partition Table)

Giriş

- **BIOS**, bilgisayarlarınızda bulunan bir **CMOS** yongasında yerleşik olarak bulunan ve bilgisayarınızı açtığınızda işletim sistemini başlatan bir programdır.
- BIOS, bilgisayarınızın donanımının bir parçasıdır ve **Windows**'dan **ayrı bir programdır.**
- **UEFI** ise, **BIOS**'un *(temel giriş/çıkış sistemi)* yerine koyulmak için tasarlanmıştır.
- **UEFI** standardı **Microsoft** dahil **140'**tan fazla teknoloji şirketi tarafından oluşturulmuştur. Yazılım birlikte çalışılabilirliğini ve **BIOS**'un adres sınırlamalarını iyileştirmek için tasarlanmıştır.
- Bu spesifikasyonun ilk versiyonu **EFI** olarak adlandırılmıştır ve **EFI 1.10 ismi ile duyurulmuştur.**
- **2005** yılında **EFI Spesifikasyonu'**nun daha yaygın olarak benimsenmesi ve geliştirilmeye devam edilmesini sağlamak için sektör genelinde bir organizasyon olarak **Evrensel EFI Forumu** gerçekleştirildi.
- Bu grup, **EFI 1.10 Spesifikasyonu**'ndan yola çıkarak yeni spesifikasyonlar hazırladı ve bunları **Evrensel EFI Spesifikasyonu (UEFI)** adıyla duyurdu.

Basit Disk ve GPT

- Basit diskler **Windows**'ta en çok kullandığımız disk birimleridir.
- **Basit Disk** terimi, bölümler içeren *(Birincil veya Mantıksal)* disk anlamında kullanılır.
- **MBR** ile tanımlanan **Basit** disklerin aksine **GPT** ile tanımlanan **Basit** diskler **3** veya **4** bölüme ihtiyaç duyarlar:
- **Kurtarma, ESP (EFI System Partition), MSR (Microsoft Reserved Partition)** ve **Sistem (DATA)** bölümü.
  - **ESP** bölümü **100 MB** büyüklüğündedir. **NTLDR, HAL, Boot.txt** ve **sistemin ön yüklenebilmesi için gerekli sürücüler** gibi diğer bazı sistem dosyalarını barındırır. **ESP** mutlaka **MSR, OEM** ve **DATA** bölümlerinden **önce olmalıdır.**
  - **MSR Bölümü:** Her **GPT** disk mutlaka bir **Sistem Ayrıldı** bölümü barındırmak zorundadır. **MSR**'nin dikteki sırası **ESP**'den sonradır. **ESP** ile **MSR** arasında bir **OEM** bölüntü olabilir ama **MSR** mutlaka **işletim sisteminin yüklü olduğu bölüntüden önce yer almalıdır. MSR** bölümü **Windows** kurulumu esnasında kurulum tarafından otomatik olarak oluşturulur. **MSR, 128 MB** büyüklüğündedir.

- **GPT** diskte, işletim sisteminin kurulabileceği **en az 1 DATA bölümü bulunmalıdır.**
- **UEFI, MBR** ya da benzeri bir veriye gerek duymadan diski kendi başına başlatabilir ancak geriye yönelik uyuşmayı sağlayabilmek için **UEFI**'nin kullandığı disk bölümlendirme tablosu olan **GPT**, kendi başlangıcı olan **Birincil Bölüm Tablo Başlığı**'ndan önce **MBR** girdisini disk üzerinde ilk sektörde saklar.
- **MBR**'yi diskin başlangıcında tutmak, **MBR** tabanlı disk uygulamalarının *(Örneğin, **Microsoft MS-DOS FDISK**)* **GPT** disklerini yanlış tanımlamalarını ve üzerine yazmalarını engellemek içindir

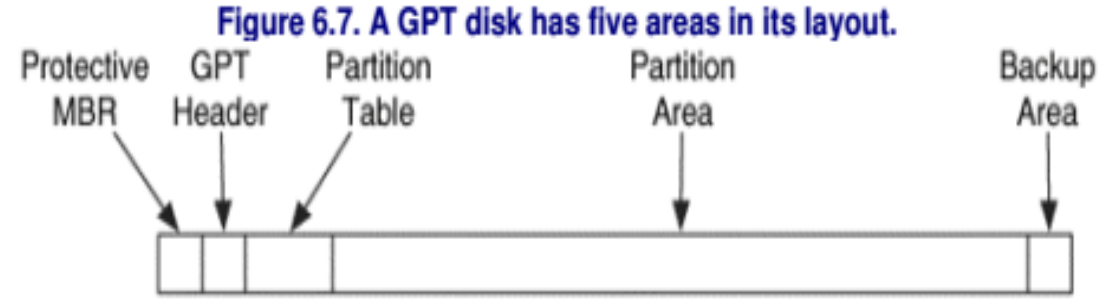
Genel Bakış

- 64-bit Intel Itanium işlemcileri olan sistemler (IA64) IA32 sistemleri gibi bir BIOS'a sahip değillerdir.
- Bunun yerine, Extensible Firmware Interface (EFI) özelliklerine sahiptirler.
- EFI (http://www.intel.com/technology/efi), Sun Sparc sistemleri gibi Intel dışı platformlar tarafından da kullanılır. EFI, 128 bölüm destekleyebilen ve 64 bit LBA adreslerini kullanan GUID Bölme Tablosu (GPT) adlı bir partition sistemi kullanır.
- Başarısızlık durumunda önemli veri yapılarının yedek kopyaları saklanır.
- UEFI standardına sahip olan bu sistem, diskin bölümlerini düzenleyen en güncel sistemdir.
- Yani UEFI tabanlı bir sisteminiz varsa MBR yerine GPT kullanılması gerekmektedir. MBR'nin aksine, GPT'de teorik olarak sınırsız bölüm oluşturulabilir.
- GPT, depolama alanı olarak da MBR'den bir adım öndedir. MBR'de bulunan her bir bölüm için 2TB sınırı, GPT'de 9.44ZB gibi boyutlara ulaşabilmektedir. Elbette bu değer sadece teorik olarak mümkün. Zira Windows işletim sistemlerinde her bir bölümün maksimum kapasitesi 256TB olarak sabitlenmiştir.

GPT Destekleri

OS	Support Version	Boot from GPT on EFI
Windows 2003	Since SP1 64bit only	No
Windows XP	64bit only	Only 64bit
Windows Vista	Both 32 bit and 64bit	Yes
Windows 2008	Both 32 bit and 64bit	Yes
Windows 2008R2	64bit only	Yes
Windows 7	Both 32 bit and 64bit	Yes
Windows 8 / 8.1	Both 32 bit and 64bit	Yes
Windows 2012 / 2012R2	64bit only	Yes
Solaris	Since Solaris 10 Both 32 bit and 64 bit	No
FreeBSD	Since 7.0 Both 32 bit and 64 bit	Yes
Mac OS X	Since 10.4.0 (some features Since 10.4.6) Both 32 bit and 64 bit	Yes
Linux	Most of the Linux OS Both 32 bit and 64 bit	Yes
VMware ESXi	Since ESXi 5.0	Yes

GPT Yapısı



- GPT diskinin beş ana alanı vardır.
- **İlk alan** Koruyucu MBR'dir ve diskin ilk sektöründe başlar ve bir girişli bir DOS bölüm tablosu içerir. Tek giriş, tüm diski kapsayan 0xEE tipi bir bölüm içindir. Bu bölüm, eski bilgisayarların diski kullandığı gibi algılayabilmesi ve biçimlendirmeye çalışmaması için vardır.
- **ikinci kısmı,** sektör 1'de başlar ve GPT başlığını içerir. Başlık, GPT diski oluşturulduğunda sabitlenen bölüm tablosunun boyutunu ve konumunu tanımlar. Windows, partition tablosundaki girdilerin sayısını 128 [Microsoft 2004] olarak sınırlar. Başlık (header) ayrıca, başlık ve partition tablosunun bir sağlama toplamı içerir, böylece hatalar veya değişiklikler tespit edilebilir.
- **Üçüncü bölüm** partition tablosunu içerir. Partition tablosundaki her girdi, bir başlangıç ve bitiş adresi, bir tür değeri, bir ad, özellik bayrakları ve bir GUID değeri içerir. 128 bit GUID, bu sistem için benzersiz olmayı desteklemektedir ve bölüm tablosu oluşturulduğunda ayarlanır.
- **Diskin dördüncü bölümü** partition alanıdır. Partition alanı en geniş alandır ve bölümlere ayrılan sektörleri içerir. Bu alanın başlangıç ve bitiş sektörleri GPT başlığında tanımlanmıştır.
- **Diskin son bölümü** GPT başlığının ve bölüm tablosunun bir yedek kopyasını içerir. Bölme alanını takiben sektörde yer almaktadır.

Veri Yapıları

- GPT diskinin ilk alanı, standart bir DOS bölüm tablosu kullanır. Bir GPT diskin, tüm diski kapsayan tek girişli bir DOS bölüm tablosu vardır. Burada bir örnek gösterilmektedir.

```
# mmls -t dos gpt-disk.dd
DOS Partition Table
Units are in 512-byte sectors
     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  00:00   0000000001   0120103199   0120103199   GPT Safety Partition (0xEE)
```

- Sektör 1 GPT başlığını içeriyor. GPT başlığı diskin düzenini açıklar. Veri yapısı Tablo 6.16'da verilmiştir.

Table 6.16. Data structure for the GPT header.

Byte Range	Description	Essential
0–7	Signature value ("EFI PART")	No
8–11	Version	Yes
12–15	Size of GPT header in bytes	Yes
16–19	CRC32 checksum of GPT header	No
20–23	Reserved	No
24–31	LBA of current GPT header structure	No
32–39	LBA of the other GPT header structure	No
40–47	LBA of start of partition area	Yes
48–55	LBA of end of partition area	No
56–71	Disk GUID	No
72–79	LBA of the start of the partition table	Yes
80–83	Number of entries in partition table	Yes
84–87	Size of each entry in partition table	Yes
88–91	CRC32 checksum of partition table	No
92–End of Sector	Reserved	No

- Bu değerleri kullanarak, bölüm tablosunun, bölüm alanının ve GPT başlığının ve bölüm tablosunun yedek kopyalarının bulunduğu disk düzeni belirlenebilir.
- Örnek bir disk görüntüsü için GPT başlığı burada gösterilmiştir:

```
# dd if=gpt-disk.dd bs=512 skip=1 count=1 | xxd
0000000: 4546 4920 5041 5254 0000 0100 5c00 0000  EFI PART....\...
0000016: 8061 a3b0 0000 0000 0100 0000 0000 0000  .a..............
0000032: 1fa1 2807 0000 0000 2200 0000 0000 0000  ..(.....".......
0000048: fea0 2807 0000 0000 7e5e 4da1 1102 5049  ..(.....~^M...PI
0000064: ab2a 79a6 3ea6 3659 0200 0000 0000 0000  .*y.>.8Y........
0000080: 8000 0000 8000 0000 69a5 7180 0000 0000  ........i.q.....
0000096: 0000 0000 0000 0000 0000 0000 0000 0000  ................
[REMOVED]
```

- İmza değerini ilk 8 baytta görebiliriz ve bayt 12 ila 15 bize GPT başlığının 96 bayt (0x5c) olduğunu gösterir.
- Bayt 32 - 39, üstbilginin yedek kopyasının sektör 120.103.199'da (0x0728a1af) bulunduğu göstermektedir. Bunun, DOS koruma bölümünün son sektörü olarak gördüğümüz aynı sektör olduğunu unutmayın.
- 40'dan 47'ye kadar olan baytlar bölüm alanının sektör 34'de (0x22) başladığını ve sektör 120, 103, 166'da (0x0728a0fe) bittiğini göstermektedir.
- 72 - 79 baytları, bölüm tablosunun 2. sektörde başladığını ve 80 - 83 baytlarının tabloda 128 (0x80) girdi olduğunu göstermektedir.
- 84'ten 87'ye kadar olan baytlar, her girişin 128 (0x80) bayt olduğunu gösterir;

Partition Tablo Kayıtlarının Veri Yapıları

- 128 bitlik tür değeri bölümün içeriğini tanımlar.
- Bir GPT diski ile bölümler hem sistem bilgisini hem de dosya sistemlerini tutmak için kullanılır.
- Örneğin, EFI kullanan her bilgisayarın, sistemin donanımını ve yazılımını başlatmak için gerekli dosyaları içeren bir EFI Sistem Bölümüne sahip olması gerekir.

Table 6.17. Data structure for each GPT partition table entry.

Byte Range	Description	Essential
0–15	Partition type GUID	No
16–31	Unique partition GUID	No
32–39	Starting LBA of partition	Yes
40–47	Ending LBA of partition	Yes
48–55	Partition attributes	No
56–127	Partition name in Unicode	No

GPT Partition Türleri

Operating system	Partition type	Globally unique identifier (GUID)[4]
(None)	Unused entry	00000000-0000-0000-0000-000000000000
	MBR partition scheme	024DEE41-33E7-11D3-9D69-0008C781F39F
	EFI System partition	C12A7328-F81F-11D2-BA4B-00A0C93EC93B
	BIOS boot partition[e]	21686148-6449-6E6F-744E-656564454649
	Intel Fast Flash (iFFS) partition (for Intel Rapid Start technology)[23][24]	D3BFE2DE-3DAF-11DF-BA40-E3A556D89593
	Sony boot partition[f]	F4019732-066E-4E12-8273-346C5641494F
	Lenovo boot partition[g]	BFBFAFE7-A34F-448A-9A5B-6213EB736C22
Windows	Microsoft Reserved Partition (MSR)	E3C9E316-0B5C-4DB8-817D-F92DF00215AE
	Basic data partition[9]	EBD0A0A2-B9E5-4433-87C0-68B6B72699C7
	Logical Disk Manager (LDM) metadata partition	5808C8AA-7E8F-42E0-85D2-E1E90434CFB3
	Logical Disk Manager data partition	AF9B60A0-1431-4F62-BC68-3311714A69AD
	Windows Recovery Environment	DE94BBA4-06D1-4D40-A16A-BFD50179D6AC
	IBM General Parallel File System (GPFS) partition	37AFFC90-EF7D-4E96-91C3-2D7AE055B174
	Storage Spaces partition	E75CAF8F-F680-4CEE-AFA3-B001E56EFC2D
HP-UX	Data partition	75894C1E-3AEB-11D3-B7C1-7B03A0000000
	Service Partition	E2A1E728-32E3-11D6-A682-7B03A0000000
Linux	Linux filesystem data[h]	0FC63DAF-8483-4772-8E79-3D69D8477DE4
	RAID partition	A19D880F-05FC-4D3B-A006-743F0F84911E
	Root partition (x86)[27]	44479540-F297-41B2-9AF7-D131D5F0458A
	Root partition (x86-64)[27]	4F68BCE3-E8CD-4DB1-96E7-FBCAF984B709
	Root partition (32-bit ARM)[27]	69DAD710-2CE4-4E3C-B16C-21A1D49ABED3
	Root partition (64-bit ARM/AArch64)[27]	B921B045-1DF0-41C3-AF44-4C6F280D3FAE
	Swap partition	0657FD6D-A4AB-43C4-84E5-0933C84B4F4F
	Logical Volume Manager (LVM) partition	E6D6D379-F507-44C2-A23C-238F2A3DF928
	/home partition[27]	933AC7E1-2EB4-4F13-B844-0E14E2AEF915
	/srv (server data) partition[27]	3B8F8425-20E0-4F3B-907F-1A25A76F98E8
	Plain dm-crypt partition[28][29]	7FFEC5C9-2D00-49B7-8941-3EA10A5586B7
	LUKS partition[28][29]	CA7D7CCB-63ED-4C53-861C-1742536059CC

Table 6.18. GPT partition types defined by Intel.

GUID Type Value	Description
00000000-0000-0000-0000-000000000000	Unallocated entry
C12A7328-F81F-11D2-BA4B-00A0C93EC93B	EFI system partition
024DEE41-33E7-11d3-9D69-0008C781F39F	Partition with DOS partition table inside

Microsoft has defined some of the type values that it uses, and they are given in Table 6.19.

Table 6.19. GPT partition types that Microsoft has defined.

GUID Type Value	Description
E3C9E316-0B5C-4DB8-817D-f92DF00215AE	Microsoft Reserved Partition (MRP)
EBD0A0A2-B9E5-4433-87C0-68B6B72699C7	Primary partition (basic disk)
5808C8AA-7E8F-42E0-85D2-E1E90434CFB3	LDM metadata partition (dynamic disk)
AF9B60A0-1431-4F62-BC68-3311714A69AD	LDM data partition (dynamic disk)

GPT

GUID Partition Table
Globally Unique Identifier

Protective MBR (LBA 0)

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
16	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
32	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
48	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
64	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
96	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
144	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
304	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
336	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
368	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
400	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
448	02	00	EE	FF	FF	FF	01	00	00	00	FF	FF	FF	FF	00	00
464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA

GUID Protective MBR	
Bytes	**Description**
0-440	Unused by UEFI systems
440-443	Unused and set to Zero
444-445	Unused and set to Zero
446-509	MBR partition records that only have one entry pointing to the EFI Partition
510-511	Set to AA55
512	The rest of the logical block, if any, is reserved. Set to Zero

432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
448	02	00	EE	FF	FF	FF	01	00	00	00	FF	FF	FF	FF	00	00
464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA

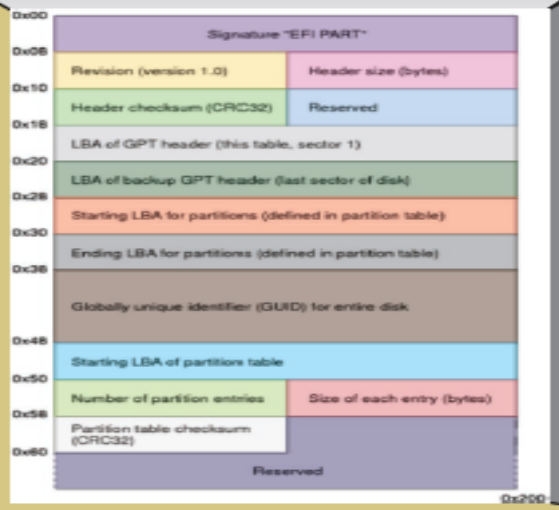
GUID protected MBR entry format	
Bytes	**Purpose**
0	Set to 0x00 to indicate a non-bootable partition. If set to any value other than 0x00 the behavior of this flag on non-UEFI systems is undefined. Must be ignored by UFI implementations
1-3	Set to 0x0002000, corresponding to the Starting LBA field
4	Partition type set to "EE" with indicates the EFI partition
5-7	Set to the CHS address of the last logical block on the disk. Set to 0xFFFFFF if it is not possible to represent the value in this field
8-11	Set to 0x00000001 (i.e., the LBA of the GPT Partition Header).
12-15	Set to the size of the disk minus one. Set to 0xFFFFFFFF if the size of the disk is too large to be represented in this field.

GPT header (LBA 1)

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
512	45	46	49	20	50	41	52	54	00	00	01	00	5C	00	00	00	EFI PART
528	C1	70	1B	FA	00	00	00	00	01	00	00	00	00	00	00	00	Áp ú
544	FF	37	76	00	00	00	00	00	22	00	00	00	09	00	00	00	ÿ7v "
560	DE	37	76	00	00	00	00	00	8B	21	AD	7E	A0	1D	F0	48	Þ7v ‹!-~ ðH
576	BC	FA	B7	E9	A4	BD	63	07	02	00	00	00	00	00	00	00	¼ú·é¤½c
592	80	00	00	00	80	00	00	00	D5	82	B6	FD	00	00	00	00	€ € Õ‚¶ý
608	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
624	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
640	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
656	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
672	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
688	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
704	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
720	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
736	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
752	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
768	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
784	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
800	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
816	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
832	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
848	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
864	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
880	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
896	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
912	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
928	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
944	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
960	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
976	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
992	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
1008	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

GPT vs MBR

MBR = 32bit, GPT = 64bit
GPT has a backup Partition Table located at Last LBA n-1 and a backup GPT Header located at Last LBA n
MBR has a maximum of 4 partitions
GPT has a maximum of 128 partitions
MBR Partition Table allows for up to 2.2 TB (2.20×10^{12} bytes)
GPT allows for up to 9.4 ZB (9.4×10^{21} bytes)
GPT allows for each partition to have a 36 character Unicode name
The odds of generated two identical guids is 1 in 5,316,911,983,139,663,491,615,228,241,121,400,000
GUIDs are stored as 128-bit values, and are displayed as 32 hexadecimal digits



GPT Header				
Mnemonic	**Byte Offset**	**Byte Legnth**	**Bytes**	**Purpose**
Signature	0	8	0-7	Identifies EFI-compatible partition table header. This value must contain the ASCII string "EFI PART", encoded as the 64-bit constant 0x5452415020494645
Revision	8	4	8-11	The revision number for this header. This revision value is not related to the UEFI Specification version. This header is version 1.0, so the correct value is 0x00010000.
Headersize	12	4	12-15	Size in bytes of the GPT Header. The HeaderSize must be greater than 92 and must be less than or equal to the logical block size.
HeaderCRC32	16	4	16-19	CRC32 checksum for the GPT Header structure. This value is computed by setting this field to 0, and computing the 32-bit CRC for HeaderSize bytes.
Reserved	20	4	20-23	Must be Zero
MyLBA	24	8	24-31	The LBA that contains this data structure.
AlternateLBA	32	8	32-39	LBA address of the alternate GPT Header.
FirstUsableLBA	40	8	40-47	The first usable logical block that may be used by a partition described by a GUID Partition Entry.
LastUsableLBA	48	8	48-55	The last usable logical block that may be used by a partition described by a GUID Partition Entry.
DiskGUID	56	16	56-71	GUID that can be used to uniquely identify the disk.
PartitionEntryLBA	72	8	72-79	The starting LBA of the GUID Partition Entry array.
NumberOfPartitionEntries	80	4	80-83	The number of Partition Entries in the GUID Partition Entry array.
SizeOfPartitionEntry	84	4	84-87	The size, in bytes, of each the GUID Partition Entry structures in the GUID Partition Entry array. This field shall be set to a value of 128 x 2n where n is an integer greater than or equal to zero (e.g., 128, 256, 512, etc.). NOTE: Previous versions of this specification allowed any multiple of 8..
PartitionEntryArrayCRC32	88	4	88-92	The CRC32 of the GUID Partition Entry array. Starts at PartitionEntryLBA and is computed over a byte length of NumberOfPartitionEntries * SizeOfPartitionEntry.
Reserved	92	Blocksize-92	92-	The rest of the block is reserved by UEFI andmust be zero.

Partition table (LBA 2)

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1024	A2	A0	D0	EB	E5	B9	33	44	87	C0	68	B6	B7	26	99	C7
1040	3A	E1	A9	FD	37	D2	00	43	8B	87	D9	69	A0	53	BC	BD
1056	80	00	00	00	00	00	00	00	7F	37	76	00	00	00	00	00
1072	00	00	00	00	00	00	00	80	42	00	61	00	73	00	69	00
1088	63	00	20	00	64	00	61	00	74	00	61	00	20	00	70	00
1104	61	00	72	00	74	00	69	00	74	00	69	00	6F	00	6E	00
1120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
1136	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

GUID partition table entry format	
Bytes	**Purpose**
0-15	Partition type GUID
16-31	Unique partition GUID
32-39	Starting LBA of partition
40-47	Ending LBA of partition
48-55	Partition Attributes
56-127	Partition name in Unicode

Table 18. Defined GPT Partition Entry - Partition Type GUIDs

Description	GUID Value
Unused Entry	00000000-0000-0000-0000-000000000000
EFI System Partition	C12A7328-F81F-11D2-BA4B-00A0C93EC93B
Partition containing a legacy MBR	024DEE41-33E7-11D3-9D69-0008C781F39F

GPT Partition Entry

Mnemonic	Byte Offset	Byte Legnth	Bytes	Purpose
PartitionTypeGUID	0	16	0-15	Unique ID that defines the purpose and type of this Partition. A value of zero defines that this partition entry is not being used.
UniquePartitionGUID	16	16	16	GUID that is unique for every partition entry. Every partition ever created will have a unique GUID. This GUID must be assigned when the GPT Partition Entry is created. The GPT Partition Entry is created whenever the NumberOfPartitionEntries in the GPT Header is increased to include a larger rangeof addresses.
StartingLBA	32	8	32-39	Starting LBA of the partition defined by this entry.
EndingLBA	40	8	40-47	Ending LBA of the partition defined by this entry.
Attributes	48	8	48-55	Attribute bits, all bits reserved by UEFI
PartitionName	56	72	56-127	Null-terminated string containing a human-readable name of the partition.
Reserved	128	SizeOfPartition Entry - 128	32-39	The rest of the GPT Partition Entry, if any, is reserved by UEFI and must be zero.

Defined GPT Partition Entry - Attributes

Bits	Name	Description
Bit 0	Required Partition	If this bit is set, the partition is required for the platform to function. The owner/creator of the partition indicates that deletion or modification of the contents can result in loss of platform features or failure for the platform to boot or operate. The system cannot function normally if this partition is removed, and it should be considered part of the hardware of the system. Actions such as running diagnostics, system recovery, or even OS install or boot could potentially stop working if this partition is removed. Unless OS software or firmware recognizes this partition, it should never be removed or modified as the UEFI firmware or platform hardware may become non-functional.
Bit 1	No Block IO Protocol	If this bit is set, then firmware must not produce an EFI_BLOCK_IO_PROTOCOL device for this partition. By not producing an EFI_BLOCK_IO_PROTOCOL partition, file system mappings will not be created for this partition in UEFI.
Bit 2	Legacy BIOS Bootable	This bit is set aside by this specification to let systems with traditional PC-AT BIOS firmware implementations inform certain limited, special-purpose software running on these systems that a GPT partition may be bootable. For systems with firmware implementations conforming to this pecification, the UEFI boot manager (see chapter 3) must ignore this bit when selecting a UEFI compliant application, e.g., an OS loader (see 2.1.3). Therefore there is no need for this specification to define the exact meaning of this bit.
Bits 3-47		Undefined and must be zero. Reserved for expansion by future versions of the UEFI specification.
Bits 48-63		Reserved for GUID specific use. The use of these bits will vary depending on the PartitionTypeGUID. Only the owner of the PartitionTypeGUID is allowed to modify these bits. They must be preserved if Bits 0–47 are modified.

Analiz

- GPT disklerinde, bölüm tablosunun yedek kopyası bulunur; böylece, orijinal tablo bozulduğunda veriler daha kolay kurtarılabilir.
- Sektör 0, sektör 1'in kullanılmayan bölümleri ve bölüm girdilerinin herhangi biri verileri gizlemek için kullanılabilir.

BSD İşletim Sistemi

- BSD “Berkeley Software Distribution” 'ın kısaltılmışıdır. Bu isim California Üniversitesi, Berkeley 'in kaynak kodu dağıtımı olan AT&T 'nin UNIX® 'i için bir eklentiler zinciridir.
- BSD 'in içeriği:
  - BSD çekirdeği işlem zamanlama, hafıza yönetimi, simetrik çoklu işlemci(SMP), aygıt sürücüleri ve diğerlerini kapsar.
  - *Linux çekirdeğinden farklı olarak kapasite ve güçte birçok farklı BSD çekirdeği vardır.*
  - C kütüphanesi, sistem API 'sinin temellidir
  - *BSD C Kütüphanesi GNU projesi tabanlı değildir, Berkeley kodu temellidir.*
  - Kabuk, dosya araçları derleyiciler ve linkerler gibi araçlar bulundurur.
  - X Window sistemi grafik ekran arabirimi.

BSD Türleri

- FreeBSD yüksek performans ve son kullanıcılar için kullanım kolaylığı amacını güder. ISP firmaları için favori işletim sistemdir. PCler ve Compaq'ın Alpha işlemcileri üzerinde çalışır. FreeBSD açık bir farkla diğer projelere oranla daha fazla kişi tarafından kullanılır.
- NetBSD azami seviyede taşınabilirlilik hedefler. Ek olarak sade dizayna sahiptir. NetBSD palmlerden büyük serverlara kadar her yerde çalışır ve NASA'nın uzay çalışmalarında da kullanılmıştır. Özel olarakda Intel-olmayan donanımlar için iyi seçimdir.
- OpenBSD kod temizliğini ve güvenliğini hedef alır. Açık kaynak kod geliştirim modeli ve sıkı kod incelemesini içerir ve ABD hükümet bakanlıkları, hisse senedi kurumları gibi güvenlik temelli işletmeler için bir işletim sistemi olmayı hedefler. NetBSD gibi birçok platformda çalışabilir.

BSD Partitionları

- Bilgisayar incelemeleri için FreeBSD (http://www.freebsd.org), OpenBSD (http://www.openbsd.org) ve NetBSD gibi BSD UNIX sunucularıyla karşılaşmak yaygındır. Bu sistemler kendi partition sistemini kullanır ve bu partition yapılarının detaylarını inceleme için bilmek gerekir.
- Bir inceleme sırasında bir Linux sistemi ile karşılaşmak daha genel bir şeydir, ancak Linux sadece DOS tabanlı bölümleri kullanır ve herhangi bir özel veri yapısı yoktur.
- Pek çok BSD sistemi IA32 tabanlı bir donanım kullanır (yani x86 / i386) ve Microsoft ürünleri ile aynı diskte bulunabilecekleri şekilde tasarlanmıştır.
- Bu nedenle dos bölümleme yapısını bilmek gerekir.
- IA32 olmayan bir donanım üzerinde çalışan bir BSD sistemi büyük olasılıkla DOS bölümlerini kullanmaz ve kendine özeldir.

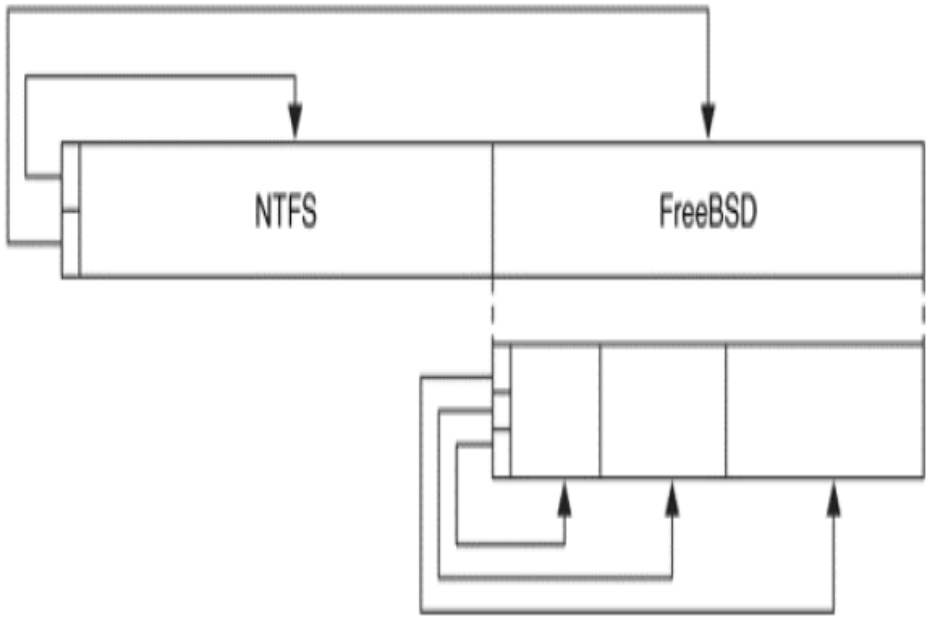
BSD Partitionları

- Bu bölüme başlamadan önce anlaşılması gereken önemli kavram, bir işletim sistemi çalışırken hangi bölüme kullanıcının erişebileceğini seçebilmesidir.
- Gösterildiği gibi, FreeBSD işletim sistemi DOS ve BSD bölüm sistemlerini kullanır ancak OpenBSD ve NetBSD yalnızca BSD bölümleme sistemini kullanır. DOS bölümlerinin yapısının bilinmesi FreeBSD için gereklidir.

Genel Bakış

- BSD bölümleme sistemi DOS bölümlerinden daha basit ancak Apple bölüm haritasından daha karmaşıktır.
- Gerekli verileri içeren yalnızca bir sektör vardır ve Şekil 6.1'de gösterildiği gibi bir DOS bölümü içerisinde bulunmaktadır.
- Sistemin aynı diskte Windows'a sahip olabilmesi ve kullanıcının hangi işletim sistemini yükleyebileceğini seçebilmesi için bir DOS bölümü bulunur.
- DOS partition tablosu, sırasıyla FreeBSD, OpenBSD veya NetBSD türü- 0xa5, 0xa6 ve 0xa9 olan bir bölüm kayıtına sahip olacaktır. BSD bölümü, birincil DOS bölmelerinden biri olacaktır.

Figure 6.1. A disk with two DOS partitions and three BSD partitions inside the FreeBSD-type DOS partition.



Genel Bakış - Devam

- BSD bölümleri için bir DOS bölümü tarafından oluşturulan bir volüm içerisinde bulunduğunu söyleyebiliriz.
- Merkezi veri yapısı disk etiketidir.
- En az 276 bayt boyutundadır ve BSD bölümünün ikinci sektöründe bulunur.
- IA32 dışı bazı sistemlerde, ilk sektörde olabilir.
- FreeBSD, OpenBSD ve NetBSD aynı yapıyı kullanır ancak uygulamada biraz farklıdır.

Disk Etiket (Label) Yapısı

- Disk etiket yapısı, diskin donanım özelliklerini ve sekiz veya onaltı BSD partitionları için bir partition tablosu içerir.
- Apple bölümlerinin aksine, bölüm tablosu sabit bir boyuttadır ve DOS bölümlerinin aksine, yalnızca bir bölüm tablosu vardır.
- BSD partition tablosundaki her entry aşağıdaki alanları içerir.

- Starting sector of the BSD partition
- Size of the BSD partition
- Partition type
- Size of the UFS file system fragment
- Number of UFS file system fragments per block
- Number of cylinders per UFS Cylinder group

Disk Etiket (label) Yapısı

- **Başlangıç sektör adresi** disk etiketine veya DOS bölümüne göre değil disk başlangıcına göre verilir.
- **Partition türü alanı** UFS, Swap alanı, FAT ve kullanılmayan gibi BSD bölümünde olması gereken dosya sistemi türünü tanımlar.
- Son üç değer yalnızca bölüm bir UFS dosya sistemi içerdiğinde kullanılır. UFS Dosya sisteminde açıklanacaktır.

- Starting sector of the BSD partition
- Size of the BSD partition
- Partition type
- Size of the UFS file system fragment
- Number of UFS file system fragments per block
- Number of cylinders per UFS Cylinder group

Analiz Şartları

- BSD partitionlarının temel teorisi basittir.
- Tek yapı okunur ve paritionların listesi kolayca işlenebilir.
- Bununla birlikte, bir inceleme uzmanı için zorluk, kullanıcının hangi bölümlere erişebildiğini bilmektir.
- Örneğin, çift önyükleme sistemi olması durumunda, araştırmacı kullanıcının Windows bölümüne ve BSD bölümlerine erişimi olup olmadığını bilmelidir.
- FreeBSD bunu OpenBSD ve NetBSD'den farklı şekilde halleder. Her bir işletim sisteminin, uygulama düzeyinde analiz olarak düşünülse de, disk etiketindeki verileri nasıl kullandığı gösterilecektir.

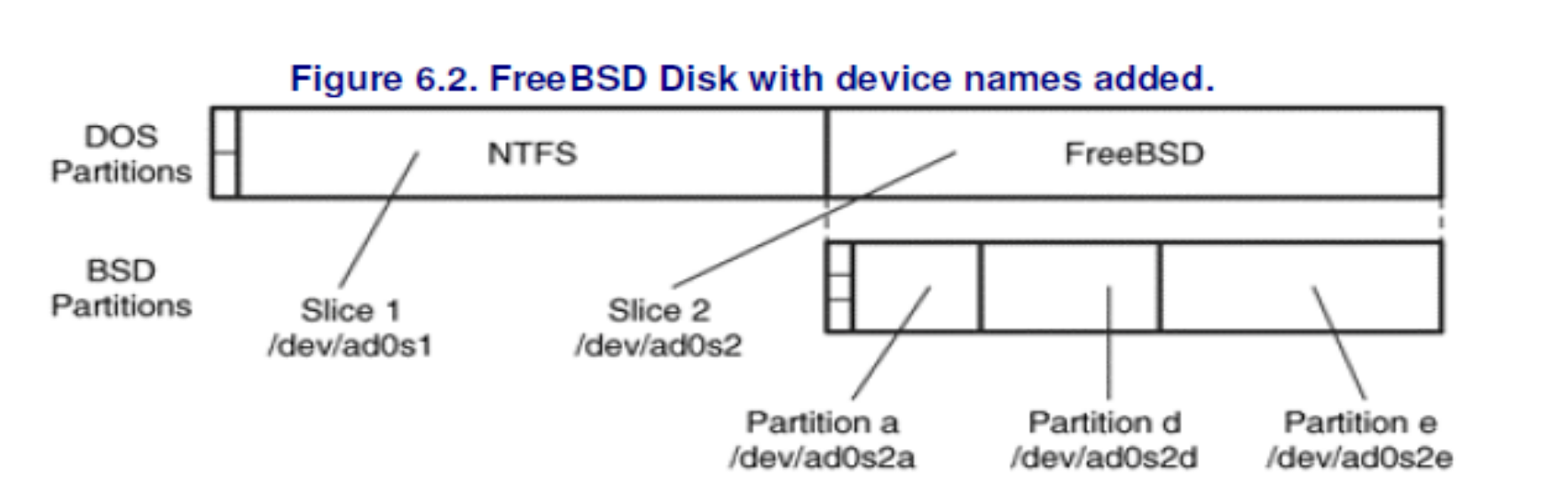
FreeBSD

Genel Bakış

- FreeBSD, kullanıcıya disk üzerindeki tüm DOS ve BSD bölümlerine erişim hakkı tanır.
- FreeBSD, her bir DOS bölümüne işaret etmek için "slice-dilim" terimini kullanır.
- BSD partitionlarını belirtmek için "partition" terimini kullanır. Bu nedenle, bir sistemin hem Windows hem de FreeBSD yüklü olduğu durumlarda, kullanıcının FreeBSD'yi çalıştırırken Windows dilimlerine erişmesi gerekir.
- FreeBSD'deki disk etiket yapısı, sadece FreeBSD DOS partitionındaki sektörleri düzenlemek için kullanılır.
- Ancak OpenBSD uygulamasının FreeBSD uygulamasından farklı olduğu bilinmelidir.

Bölümleme Yapısı

- Şekile bakarsak, disk etiketi FreeBSD içinde DOS partitionı tipinde üç partition tanımlamaktadır, ancak NTFS tipinde partitionın tanımlanmasına gerek yoktur.



Etiketleme Yapısı

- FreeBSD, diğer UNIX türleri gibi, her bir partition ve slice a özel bir aygıt dosyası tanımlar.
- Dosya, DOS bölüm numarasına ve BSD bölüm numarasına göre adlandırılır.
- Birincil ATA diskin temel adı **/dev/ad0** 'dır.
- DOS partitionı olarak da adlandırılan her slice (dilim), temel isme **'s'** harfini ve **dilim numarasını** ekler.
- Örneğin, ilk slice **/dev/ad0s1** ve ikinci slice **/dev/ d0s2** 'dir.
- FreeBSD partition türüne sahip herhangi bir slice, disk etiket yapısı için işlenir.
- Dilimdeki bölümlere disk etiketi bölüm tablosundaki girdilerine dayanarak harfler verilir.
- Örneğin, ikinci DOS bölümü FreeBSD ise, ilk BSD bölümü **/dev/ad0s2a** olur ve ikinci BSD bölümü **/dev/ad0s2b** olur. Dilim (slice) sayısını içermeyen ikinci bir cihaz seti BSD bölümleri için de oluşturulabilir.
- Örneğin, **/dev/ad0a**, FreeBSD bölümü DOS bölümü 2 ise, **/dev/ad0s2a** bölümünün bir kısayolu olacaktır.

Etiket Anlamları

- BSD bölümlerinden bazıları özel anlam taşır.
- **'a'** bölümü genellikle önyükleme kodunun bulunduğu kök bölüm içindir.
- **'b'** bölümü genellikle sistemin swap alanı içindir,
- **'c'** bölümü genellikle tüm slice için
- **'d'** ile başlayan bölümler ise herhangi bir şey olabilir. "**Genel**" terimi kullanılır, çünkü BSD bölümleme araçlarının kaç tanesinin bölüm oluşturduğu tam bilinmez, ancak herhangi bir kullanıcı disk etiket bölüm tablosunu bir hex editörle düzenleyebilir ve girdileri değiştirebilir.

- **Swap alanı**, sabit disk üzerinde işletim sistemi tarafından ayrılmış bir bölümdür.
- İşlenecek veriler RAM'e sığmadığı zaman bu bölüm RAM gibi kullanılır ve böylece işlemlerin devam etmesi sağlanır. Sabit disklerin veri okuma/yazma hızları RAM'lerden çok daha düşük olduğu için **swap** alanının kullanılması işlemleri yavaşlatır.
- Özetle, bir FreeBSD sistemi tüm DOS bölümlerine ve BSD bölümlerine erişim sağlar. **Araştırmacı, sistemi tam olarak analiz etmek için disk etiketindeki DOS bölmelerini ve BSD bölümlerini analiz etmelidir.**

NetBSD ve OpenBSD

Genel Bakış

- OpenBSD ve NetBSD kullanıcıya yalnızca BSD disk label yapısındaki kayıtlara erişim hakkı verir.
- FreeBSD disk etiket yapısı, diğerlerinden farklıdır.
- OpenBSD ve NetBSD disk etiket yapısı disk üzerindeki herhangi bir partitionı tanımlayabilir. Başka bir deyişle, disk etiketi bulunduğu DOS bölümünün sınırlarının dışındaki bölümleri tanımlayabilir. Bu bölümün geri kalan kısmı için yalnızca OpenBSD'ye göre açıklanacak, fakat gerçekte hem OpenBSD hem de NetBSD'yi kastedilmektedir.
- OpenBSD kodu yıllar önce NetBSD kodundan ayrılmıştır.

Genel Bakış

- OpenBSD çekirdeği yüklendikten sonra DOS bölümleri yok sayılır.
- DOS bölümleri sadece OpenBSD partitionının başlangıcını bulmak için kullanılır. Bu nedenle eğer bir sistem üzerinde hem Windows hem de OpenBSD varsa ve kullanıcılar OpenBSD'den bir FAT bölümüne eriştiyse, FAT bölümü hem DOS partition tablosunda hem de BSD disk etiketinde olacaktır.
- Bunu önceki şekilde gördüğümüz gibi aynı DOS bölümlerine sahip olduğumuz yandaki şekilde de görebiliriz.
- Ancak bu durumda, NTFS tipi DOS bölümüne erişebilmemiz için disk etiketinde ek bir kayıt olması gerekmektedir

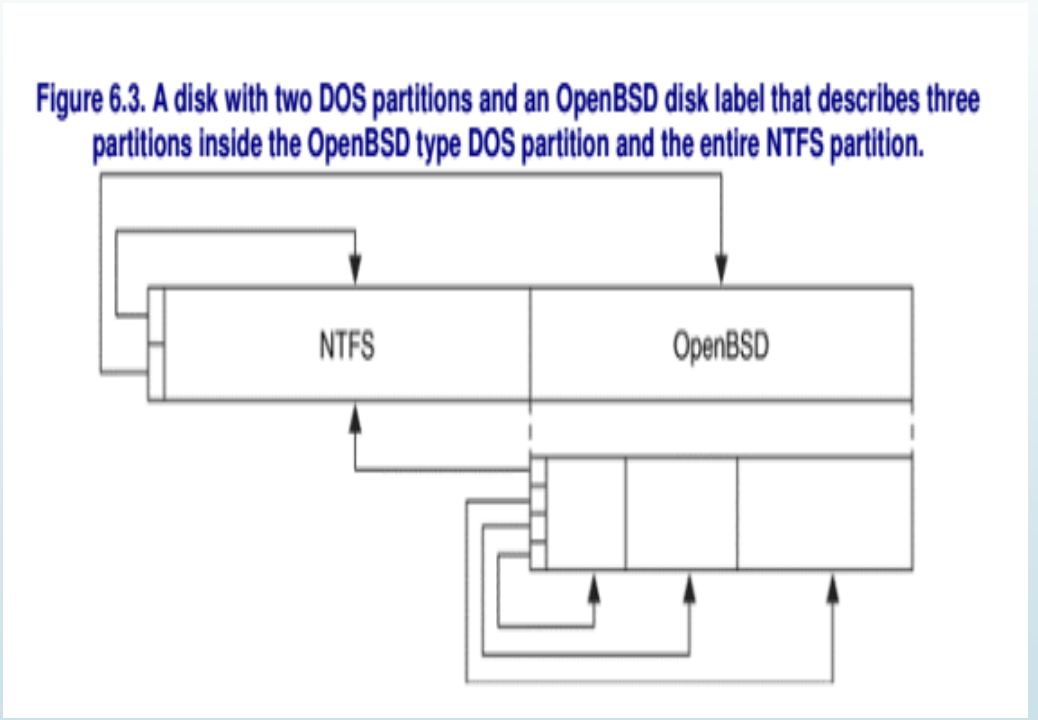


Figure 6.3. A disk with two DOS partitions and an OpenBSD disk label that describes three partitions inside the OpenBSD type DOS partition and the entire NTFS partition.

Etiketleme Yapısı

- OpenBSD, FreeBSD'nin partition aygıtları için kullandığı dosya adlarına benzer dosya adları kullanır.
- Birincil ATA aygıtının temel adı **"/dev/wd0"**'dır. **Dilim(Slice)** kavramı yoktur ve BSD bölümleri harflerle isimlendirilir.
- Bu nedenle, ilk BSD bölümü **/dev/wd0a** ve ikincisi **/dev/wd0b**'dir.
- FreeBSD gibi ilk partition genellikle root bölüm için, ikinci bölüm ise swap alanı içindir.
- Örneğimizdeki üçüncü bölüm, **/dev/wd0c**, kayıt diski için kullanılan cihazdır.
- FreeBSD'nin üçüncü bölümünün yalnızca **Slice** veya **DOS** bölümü olduğunu hatırlayın.
- Özetle, bir OpenBSD sistemi yalnızca OpenBSD disk etiketinde açıklanan bölümlere erişim sağlar. Bir OpenBSD sisteminin analizi yapılırken, disk etiketinde listelenen bölümlere odaklanmalıdır.

Boot Kodu

- Bir BSD sistemi için boot kodu, volümün sektör1'e ait disk etiket yapısını çevrelemektedir.
- Sektör0 önyükleme kodunu içerir ve MBR'deki önyükleme kodu ön yüklenebilir BSD türü bölümü bulduğunda boot edilir.
- Tüm önyükleme kodları sector0'a sığamayabilir, bu nedenle sektör 2'ye atlar ve genelde sektör 16'daki dosya sistemi verileri başlayana kadar önyükleme kodu mevcut olabilir.

Veri Yapıları

Bu bölüm BSD disk etiketi veri yapısını ve FreeBSD ve OpenBSD sistemlerinden örnek disk imaj örneklerini açıklayacaktır.

Örnek disk görüntüleri üzerinde çalışan analiz araçlarının çıktısı da verilmektedir

Disk Etiket Veri Yapısı

- Disk etiketi Tablo da verilen düzene sahiptir.
- Gerekli olmayan olarak işaretlenen verilerin diğer disk işlemleri için önemli olabileceğini ancak diskin düzenini belirlemek için gerekli olmadığını unutmayın.

Byte Range	Description	Essential
0–3	Signature value (0x82564557)	No
4–5	Drive type	No
6–7	Drive subtype	No
8–23	Drive type name	No
24–39	Pack identifier name	No
40–43	Size of a sector in bytes	Yes
44–47	Number of sectors per track	No
48–51	Number of tracks per cylinder	No
52–55	Number of cylinders per unit	No
56–59	Number of sectors per cylinder	No
60–63	Number of sectors per unit	No
64–65	Number of spare sectors per track	No
66–67	Number of spare sectors per cylinder	No
68–71	Number of alternate cylinders per unit	No
72–73	Rotational speed of disk	No
74–75	Hardware sector interleave	No
76–77	Track skew	No
78–79	Cylinder skew	No
80–83	Head switch time in microseconds	No
84–87	Track-to-track seek time in microseconds	No
88–91	Flags	No
92–111	Drive specific information	No
112–131	Reserved	No
132–135	Signature value (0x82564557)	No
136–137	Checksum	No
138–139	Number of partitions	Yes
140–143	Size of boot area	No
144–147	Maximum size of file system boot super block	No
148–163	BSD Partition #1 (see Table 6.2)	Yes
164–179	BSD Partition #2 (see Table 6.2)	Yes
180–195	BSD Partition #3 (see Table 6.2)	Yes
196–211	BSD Partition #4 (see Table 6.2)	Yes
212–227	BSD Partition #5 (see Table 6.2)	Yes
228–243	BSD Partition #6 (see Table 6.2)	Yes
244–259	BSD Partition #7 (see Table 6.2)	Yes
260–275	BSD Partition #8 (see Table 6.2)	Yes
276–291	BSD Partition #9 (see Table 6.2)	Yes
292–307	BSD Partition #10 (see Table 6.2)	Yes
308–323	BSD Partition #11 (see Table 6.2)	Yes
324–339	BSD Partition #12 (see Table 6.2)	Yes
340–355	BSD Partition #13 (see Table 6.2)	Yes
356–371	BSD Partition #14 (see Table 6.2)	Yes
372–387	BSD Partition #15 (see Table 6.2)	Yes
388–403	BSD Partition #16 (see Table 6.2)	Yes
404–511	Unused	No

BSD bölüm etiket tablosu kayıtları ve Partition Tipleri

Table 6.2. Data structure for BSD disk label entry.

Byte Range	Description	Essential
0–3	Size of BSD partition in sectors	Yes
4–7	Starting sector of BSD partition	Yes
8–11	File system fragment size	No
12–12	File system type (see Table 6.3)	No
13–13	File system fragments per block	No
14–15	File system cylinders per group	No

Table 6.3. BSD partition type values.

Type	Description
0	Unused Slot
1	Swap space
2	Version 6
3	Version 7
4	System V
5	4.1BSD
6	Eighth edition
7	4.2BSD fast file system (FFS)
8	MSDOS file system (FAT)
9	4.4BSD log-structured file system (4.4LFS)
10	In use, but unknown or unsupported
11	OS/2 HPFS
12	CD-ROM (ISO9660)
13	Bootstrap
14	Vinum drive

Örnek Sistem

- FreeBSD ve OpenBSD için en yaygın dosya hızlı dosya sistemi (FFS) 'dir.
- Sistemin ayrıca en az bir swap partitionı olacaktır.
- Diskin bir 1GB FAT bölümü, 3GB'lık bir OpenBSD bölümü ve 6GB'lık bir FreeBSD bölümü olduğunu görebiliyoruz.
- OpenBSD ve FreeBSD bölümlerinin her birinde, ek bölümleri tanımlayan disk etiket yapıları bulunur.

```
# mmls -t dos bsd-disk.dd
Units are in 512-byte sectors

     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)
```

OpenBSD Örnek İmajı

- Partition 2,056,320 sektöründe başlıyor ve disk etiketi ikinci sektörde yer almaktadır.
- İki imza değerini (0x82564557, bayt 0 ila 3 ve 132 ila 135) görebiliriz.
- İkinci imza değerini 138 ila 139 bayt arasında, 16 (0x0010) bölüm tablosu girdisi olduğunu gösterir.
- Bölümleme tablosu, bayt 148 de başlar ve 16 baytlık yapıdadır.
- 11 ila 16 arasındaki kayıtlar kullanılmaz ve 0'ları içerir. Sektörün geri kalan kısmı disk etiketi yapısı tarafından kullanılmaz.

```
# dd if=bsd-disk.dd skip=2056321 bs=512 count=1 | xxd
0000000: 5745 5682 0500 0000 4553 4449 2f49 4445  WEV.....ESDI/IDE
0000016: 2064 6973 6b00 0000 4d61 7874 6f72 2039   disk...Maxtor 9
0000032: 3130 3234 4434 2020 0002 0000 3f00 0000  1024D4  ....?...
0000048: 1000 0000 ff3f 0000 f003 0000 f02b 3101  .....?.......+1.
0000064: 0000 0000 0000 0000 100e 0100 0000 0000  ................
[REMOVED - ZEROS]
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  ................
0000320: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000336: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000352: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000368: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000384: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000400: 0000 0000 0000 0000 0000 0000 0000 0000  ................
[REMOVED]
```

OpenBSD Örnek İmaj Yapısı

Table 6.4. The contents of the BSD disk label structure in our example OpenBSD disk image.

	Start	Size	Type
1	0x001f6080 (2,056,320)	0x00031f50 (204,624)	0x07 (7)
2	0x00227fd0 (2,260,944)	0x000961e0 (614,880)	0x01 (1)
3	0x00000000 (0)	0x01312bf0 (19,999,728)	0x00 (0)
4	0x002be1b0 (2,875,824)	0x00031f50 (204,624)	0x07 (7)
5	0x002f0100 (3,080,448)	0x00025680 (153,216)	0x07 (7)
6	0x00000000 (0)	0x00000000 (0)	0x00 (0)
7	0x0040f800 (4,257,792)	0x003c4b3f (3,951,423)	0x07 (7)
8	0x00315780 (3,233,664)	0x000fa080 (1,024,128)	0x07 (7)
9	0x0000003f (63)	0x001f6041 (2,056,257)	0x08 (8)
10	0x007d433f (8,209,215)	0x00b3ae9d (11,775,645)	0x0a (10)

```
# dd if=bsd-disk.dd skip=2056321 bs=512 count=1 | xxd
0000000: 5745 5682 0500 0000 4553 4449 2f49 4445  WEV.....ESDI/IDE
0000016: 2064 6973 6b00 0000 4d61 7874 6f72 2039   disk...Maxtor 9
0000032: 3130 3234 4434 2020 0002 0000 3f00 0000  1024D4  ....?...
0000048: 1000 0000 ff3f 0000 f003 0000 f02b 3101  .....?.......+1.
0000064: 0000 0000 0000 0000 100e 0100 0000 0000  ................
[REMOVED - ZEROS]
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  ................
0000320: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000336: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000352: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000368: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000384: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000400: 0000 0000 0000 0000 0000 0000 0000 0000  ................
[REMOVED]
```

OpenBSD Örnek İmaj Yapısı

- İlk bölüm kök bölüm içindir ve önyükleme kodunu içerir.
- İkinci bölüm takas alanı içindir
- Üçüncü bölüm tüm diskin bölümüdür ve bölümler dört ve yukarı bölümler herhangi bir BSD bölümü içindir.
- Örnek imajı bu yönergeleri takip etmektedir ve ilk partition DOS partition başlangıcında başlar, bu da sektör 2.056.320'dir.
- İkinci partition, swap alanına dönüştürmek için kullanılan 1 değerine sahiptir.
- Üçüncü partition, sektör 0'da başlar ve kayıt diskinin boyutudur.
- Partitiion 4, 5, 7 ve 8'in 4.2BSD FFS tipindedir ve partitionların başlangıç sektörü, bölüm 9'a kadardır.
- Partition 9'un başlangıç sektörü 63'tür ve türü bir FAT dosya sistemi içindir.
- Bu bölüm, DOS bölme tablosunun ilk kayıtında tanımlanan FAT bölümü için BSD disk etiketi girdisidir.
- Partition 10 bilinmeyen bir tür değerine sahip ve daha önce gördüğümüz DOS bölüm tablosundaki üçüncü giriş olan FreeBSD bölümü için BSD disk etiketi girişidir.
- Bölüm 9, 'i' olarak etiketlendiğinden, kullanıcı FAT bölümüne aygıt /dev/wd0i ile erişebilir. OpenBSD, yüklendikten sonra DOS bölüm tablosu içeriğini yok saydığını unutmayın.

OpenBSD Örnek İmajın Çıktı Hali

Table 6.5. A summary of the file systems the OpenBSD system could access.

Device	Description	Mounting Point	Starting sector	Ending Sector
/dev/wd0a	4.2FFS BSD	/	2,056,320	2,260,943
/dev/wd0b	swap	N/A	2260944	2875823
/dev/wd0c	entire disk	N/A	0	19999727
/dev/wd0d	4.2FFS BSD	/tmp/	2875824	3080447
/dev/wd0e	4.2FFS BSD	/home/	3080448	3233663
/dev/wd0g	4.2FFS BSD	/var/	4257792	820921
/dev/wd0h	4.2FFS BSD	/usr/	3233664	4257791
/dev/wd0i	FAT	user's discretion	63	2056319
/dev/wd0j	FreeBSD Partition	N/A	8209215	19984859

OpenBSD Mmls Çıktısı

```
# mmls -t bsd -o 20563210 bsd-disk.dd
BSD Disk Label
Units are in 512-byte sectors

     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)
```

Mmls aracı, çıktıyı partitionın başlangıç sektörüne göre sıralayacağını unutmayın; bu nedenle, FAT partitionı, partition tablosundaki sekizinci kayıta rağmen çıktının başına yerleştirilir. Slot sütunu, bölümün nerede olduğunu gösterir.

FreeBSD Örnek İmajı

```
# dd if=bsd-disk.dd skip=8209216 bs=512 count=1 | xxd
0000000: 5745 5682 0500 0000 6164 3073 3300 0000  WEV.....ad0s3...
0000016: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000032: 0000 0000 0000 0000 0002 0000 3f00 0000  ............?...
0000048: 1000 0000 814d 0000 f003 0000 f02b 3101  .....M.......+1.
0000064: 0000 0000 0000 0000 100e 0100 0000 0000  ................
[REMOVED - ZEROS]
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  ................
0000272: 0000 0000 eb0e 4254 5801 0180 f60f 8007  ......BTX.......
0000288: 0020 0000 fa31 c08e d0bc 0018 8ec0 8ed8  . ...1..........
0000304: 666a 0266 9dbf 001e b900 3957 f3ab 5fbe  fj.f......9W.._.
0000320: e296 ac98 91e3 1dac 92ad 93ad b608 d1eb  ................
0000336: 730b 8905 8875 0288 5505 83c0 048d 7d08  s....u..U.....}.
0000352: e2ec ebde c645 0518 c645 0810 c645 0d1e  .....E...E...E..
0000368: c645 6668 bb20 28e8 bb00 0f01 1ed6 960f  .Efh. (.........
0000384: 0116 d096 0f20 c066 83c8 010f 22c0 ea7f  ..... .f....".."...
0000400: 9008 0031 c9b1 108e d1b1 380f 00d9 ba00  ...1......8.....
0000416: a000 0036 0fb7 0513 0400 00c1 e00a 2d00  ...6..........-.
0000432: 1000 0029 d0b1 3351 5068 0202 0000 6a2b  ...)..3QPh....j+
0000448: ff35 0c90 0000 5151 5151 52b1 076a 00e2  .5....QQQQR..j..
0000464: fc61 071f 0fa1 0fa9 cffa bc00 1800 000f  .a..............
0000480: 20c0 25ff ffff 7f0f 22c0 31c9 0f22 d90f   .%.....".1..".."
0000496: 0115 d096 0000 66ea e890 1800 b120 8ed1  ......f...... ..
```

- Partition 8,209,215 sektöründen başlar ve ikinci sektörde disk etiketleri vardır.

FreeBSD Örnek İmajı

Table 6.6. The contents of the BSD disk label in our FreeBSD example disk image.

	Start	Size	Type
1	0x007d433f (8,209,215)	0x00080000 (524,288)	0x07 (7)
2	0x0085433f (8,733,503)	0x001773a0 (1,536,928)	0x01 (1)
3	0x007d433f (8,209,215)	0x00b3e8b1 (11,790,513)	0x00 (0)
4	0x009cb6df (10,270,431)	0x00080000 (524,288)	0x07 (7)
5	0x00a4b6df (10,794,719)	0x00080000 (524,288)	0x07 (7)
6	0x00acb6df (11,319,007)	0x00847511 (8,680,721)	0x07 (7)
7	0x00000000 (0)	0x00000000 (0)	0x00 (0)
8	0x00000000 (0)	0x00000000 (0)	0x00 (0)

```
# dd if=bsd-disk.dd skip=8209216 bs=512 count=1 | xxd
0000000: 5745 5682 0500 0000 6164 3073 3300 0000  WEV.....ad0s3...
0000016: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000032: 0000 0000 0000 0000 0002 0000 3f00 0000  ............?...
0000048: 1000 0000 814d 0000 f003 0000 f02b 3101  .....M.......+1.
0000064: 0000 0000 0000 0000 100e 0100 0000 0000  ................
[REMOVED - ZEROS]
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  ................
0000272: 0000 0000 eb0e 4254 5801 0180 f60f 8007  ......BTX.......
0000288: 0020 0000 fa31 c08e d0bc 0018 8ec0 8ed8  . ...1..........
0000304: 666a 0266 9dbf 001e b900 3957 f3ab 5fbe  fj.f......9W.._.
0000320: e296 ac98 91e3 1dac 92ad 93ad b608 d1eb  ................
0000336: 730b 8905 8875 0288 5505 83c0 048d 7d08  s....u..U.....}.
0000352: e2ec ebde c645 0518 c645 0810 c645 0d1e  .....E...E...E..
0000368: c645 6668 bb20 28e8 bb00 0f01 1ed6 960f  .Efh. (.........
0000384: 0116 d096 0f20 c066 83c8 010f 22c0 ea7f  ..... .f....".."...
0000400: 9008 0031 c9b1 108e d1b1 380f 00d9 ba00  ...1......8.....
0000416: a000 0036 0fb7 0513 0400 00c1 e00a 2d00  ...6..........-.
0000432: 1000 0029 d0b1 3351 5068 0202 0000 6a2b  ...)..3QPh....j+
0000448: ff35 0c90 0000 5151 5151 52b1 076a 00e2  .5....QQQQR..j..
0000464: fc61 071f 0fa1 0fa9 cffa bc00 1800 000f  .a..............
0000480: 20c0 25ff ffff 7f0f 22c0 31c9 0f22 d90f   .%.....".1.."..
0000496: 0115 d096 0000 66ea e890 1800 b120 8ed1  ......f...... ..
```

138'den 139'a kadar olan değerden sekiz partition olduğunu görüyoruz. Sekiz partition tablosu kayıtları, 148 ile 275 bayt arasındadır ve parantez içinde verilmiş olan onluk değerlerin karşılığı Tablo 6.6'da gösterilen alanlara ayrıştırılabilir.

FreeBSD Örnek İmajın Çıktı Hali

Table 6.6. The contents of the BSD disk label in our FreeBSD example disk image.

	Start	Size	Type
1	0x007d433f (8,209,215)	0x00080000 (524,288)	0x07 (7)
2	0x0085433f (8,733,503)	0x001773a0 (1,536,928)	0x01 (1)
3	0x007d433f (8,209,215)	0x00b3e8b1 (11,790,513)	0x00 (0)
4	0x009cb6df (10,270,431)	0x00080000 (524,288)	0x07 (7)
5	0x00a4b6df (10,794,719)	0x00080000 (524,288)	0x07 (7)
6	0x00acb6df (11,319,007)	0x00847511 (8,680,721)	0x07 (7)
7	0x00000000 (0)	0x00000000 (0)	0x00 (0)
8	0x00000000 (0)	0x00000000 (0)	0x00 (0)

İlk BSD partitionının, disk etiketinin bulunduğu DOS bölümü ile aynı başlangıç sektörüne sahip olduğunu ve 4.2BSD FFS türüne sahip olduğunu görüyoruz. İkinci kayıt swap alanı içindir ve üçüncü kayıt yalnızca DOS bölümündeki sektörler içindir. Giriş 4, 5 ve 6, FFS dosya sistemi bölümleridir. Özetlemek gerekirse, bir FreeBSD kullanıcısının erişebileceği her bölümün aygıt adı ve konumu aşağıda verilmiştir.

Table 6.7. A summary of the file systems the FreeBSD system could access.

Device	Description	Mounting Point	Starting sector	Ending Sector
/dev/ad0s1	FAT DOS partition	User's discretion	63	2056319
/dev/ad0s2	OpenBSD DOS partition	N/A	2056320	8209214
/dev/ad0s3a	4.2BSD FFS partition	/	8209215	8733502
/dev/ad0s3b	swap	N/A	8733503	10270430
/dev/ad0s3c	Entire FreeBSD DOS partition	N/A	8209215	19999727
/dev/ad0s3d	4.2BSD FFS partition	/tmp	10270431	10794718
/dev/ad0s3e	4.2BSD FFS partition	/var	10794719	11319006
/dev/ad0s3f	4.2BSD FFS partition	/usr	11319007	19999727

FreeBSD Mmls Aracı Çıktısı

```
# mmls -t bsd -o 82092165 bsd-disk.dd
BSD Disk Label
Units are in 512-byte sectors

      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)
```

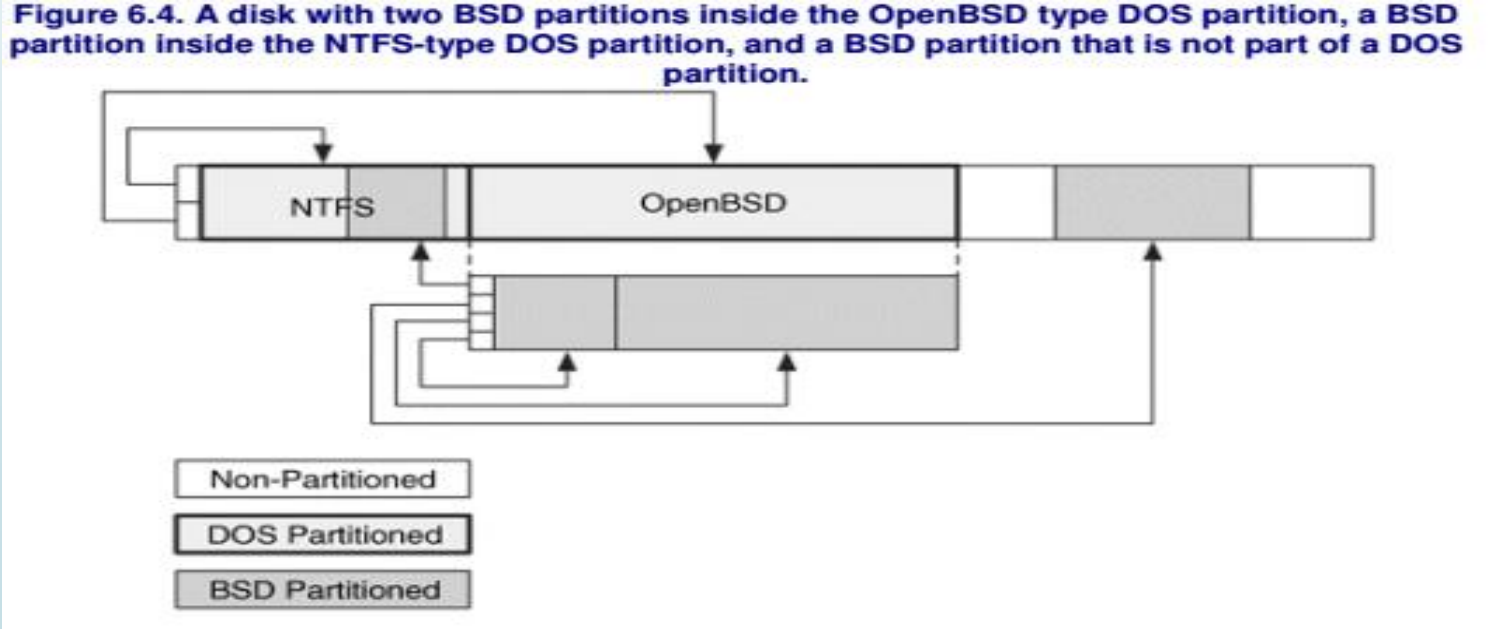
FAT ve OpenBSD partitionlarına ayrılan alanın, bu alan için disk etiketi kayıtları olduğundan 'Ayrılmamış' olarak işaretlenmiştir. DOS partition tablosu, bu verileri partition içinde bölmek için gereklidir.

Analiz Hususları

- Disk etiket yapısındaki her BSD partitionı bir tür alanına sahiptir.
- BSD sistemleri Windows'tan daha az uygulanır, çünkü Windows bölüm alanını bir sürücü harfine sahip olup olmamasını belirlemek için kullanır.
- Bir BSD sistemi ile her disk etiketi girişi için bir aygıt oluşturulur, bu yüzden partitionlar herhangi bir tür olarak mount edilebilir.
- Disk etiket yapısı en fazla 404 bayt'tır. Yalnızca sekiz kayıtı olan disk etiketleri için disk etiket yapısı sadece 276 bayttır. Bu nedenle, 512 baytlık sektörün geri kalanı veriyi gizlemek için kullanılabilir, ancak çok fazla veri saklanamaz.
- DOS bölüm tablosu bozuksa ve BSD türü bölümün konumu belirlenemiyorsa, 0x82564557 imza değeri araması yapılabilir. İmza değeri, disk etiket yapısının bayt 0 ve bayt 132'de bulunmalıdır.
- Bir FreeBSD sistemi ile kullanıcının hem DOS bölümlerine hem de BSD bölümlerine erişebildiğini unutmayın. Bu nedenle, soruşturma tüm DOS bölümlerinin ve BSD bölümlerinin analizini içermelidir.
- Bir OpenBSD sistemi ile kullanıcının sadece disk etiketindeki partitionlara erişebildiğini unutmayın. OpenBSD, DOS partition tablosunu başlattığında yok saydığından, DOS bölüm tablosunun içeriğini BSD disk etiketi ile karşılaştırmak yararlı olabilir.
- BSD partitionlarından biri NTFS tipi DOS bölümü içerisindedir. NTFS bölümü içinde bir NTFS dosya sistemi varsa, bu olası bir senaryondur ve araştırılması gerekir.

Analiz Hususları

- Şekilde, bir DOS partitiona ayrılmayan uzayda bulunan bir BSD partitionı gösterilmektedir. Bu, sistem yönetim açısından iyi bir uygulama değildir, çünkü başka bir program alana bir DOS bölümüne tahsis edebilir ve BSD verilerini üzerine yazabilir.



Sun Solaris

Giriş

- Sun Microsystems'in Solaris işletim sistemi büyük sunucularda ve masaüstü sistemlerde kullanılır.
- Diskin boyutuna ve Solaris sürümüne bağlı olarak iki farklı bölümleme sistemi kullanır.
- Solaris 9, 1- terrabyte'dan daha büyük dosya sistemlerini destekler ve 64-bit adres alanına sahip oldukları için EFI bölme tablolarını kullanıyor [Sun 2003].
- Solaris'in diğer tüm sürümleri, sadece baktığımız BSD disk etiketine benzer veri yapıları kullanır. Aslında, birincil veri yapısına disk etiketi denir, ancak yapının gerçek düzeni farklıdır.
- Sparc tabanlı Solaris ve i386 tabanlı Solaris için düzen farklıdır.
- Solaris veri yapılarının adları BSD ile aynıdır, ancak ortam bölmelerinin adları farklıdır.
- Solaris, partitionlarının her biri için "slice-dilim" terimini kullanmaktadır.
- Öncelikle Solaris mimarisinin genel özellikleri, ardından Sparc veri yapısı detayları ve son olarak i386 veri yapısı spesifikasyonlarını gösterilecektir.

Genel Bakış

- Solaris'i kurduğunuzda, disk üzerinde bir disk etiket yapısı oluşturulur.
- Kesin konumu donanım platformuna bağlıdır. Disk etiketi, destekleyebileceği maksimum disk partition sayısına sahiptir ve, Sparc sistemleri için maksimum 8, i386 için 16'dır.
- Disk etiketindeki her partitionın **başlangıç konumu, boyutu, bayraklar dizisi ve bir tür** ile tanımlanır. Bayraklar, bölümün salt okunur olup olmadığını ve takas alanı olarak kullanılıp kullanmayacağını size söyler.
- Bu derste gördüğümüz diğer partition sistemlerinde, dosya alanı türü açıklanmak için tür alanı kullanılmıştır, ancak Solaris'te genellikle bölümün mount noktasını tanımlamaktadır.
- Örneğin, bazı türler **home**, **usr** veya **var** bölümlerini belirtir ve diğerleri **swap** alanını veya atanmamış olanları belirtir.

Partition Adlandırma

- Solaris, partitionlar için ölçeklendirilebilir bir adlandırma kuralı kullanmaktadır.
- Bir Solaris ortamındayken, blok aygıtları /dev/dsk/ dizininde bulunabilir ve raw aygıtlar /dev/rdsk/ dizininde bulunabilir.
- Bu dizinlerde, Solaris bölümleri (veya dilimlerin) bir Sparc sisteminde c**W**t**X**d**Y**s**Z** ve i386 sisteminde c**W**d**Y**s**Z** gibi isimleri vardır. **W**'nin yerini denetleyici numarası alır, **X**'i fiziksel veri yolu hedef numarası (SCSI ID) alır, **Y**, veri yolundaki sürücü numarasını alır ve **Z**, sürücüdeki dilim numarası ile değiştirilir.
- Örneğin, Sparc sisteminizde yalnızca bir denetleyici varsa, disk SCSI KİMLİĞİ 6'dır ve dilim 5'i istiyorsanız, ham aygıta **/dev/rdsk/c0t6d0s5** adresinden erişirsiniz.
- Solaris ile bir partition için, disk etiketi tablosunda, mount noktasına dayalı bir konuma sahip olmak yaygındır.

Adlandırma Kuralları

Table 6.8. The typical partition that is created in each table entry.

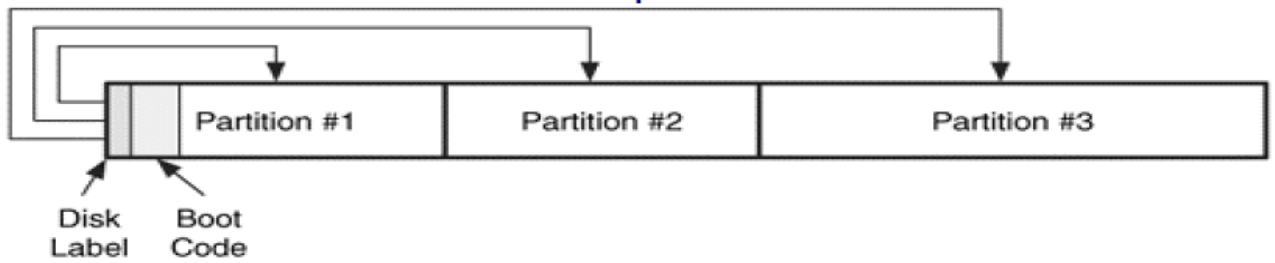
Table Entry	Description
0	/root/partition—The operating system and kernel
1	Swap space
2	The entire disk, including the disk label and all partitions
3	/export/ partition
4	/export/swap/ partition
5	/opt/ partition
6	/usr/ partition
7	/home/ partition

Sisteme eklenen ek diskler üzerinde yalnızca bir tane bölüm olabilir ve bu bölüm girişi 5, 6 veya 7'yi kullanabilir.

Sparc Veri Yapıları

- Bir Sparc sisteminde, disk etiket yapısı, 0 olan ilk sektörde oluşturulur.
- Sektör 1-15, sistemin önyükleme kodu olan "bootblock" 'u içerir ve 16 ve daha yukarı sektörler Dosya sistemleri ve takas alanı saklamak üzere bölümlenmiştir.
- Solaris, bir UFS dosya sistemi kullanmaktadır.
- Disk bölümünün düzenleri kafa karıştırıcı olabilir çünkü Solaris bölümleri için düzen bilgileri bir yerde değildir.
- Disk etiket yapısında, partition verisini tutan iki veri yapısı vardır. VTOC (**Volume Table of Content**) yapısı bölüm sayısını, her biri için tür, izin ve zaman damgalarını içerir, ancak her bölümün başlangıç konumu ve boyutu disk haritası yapısında saklanır.

Figure 6.5. The layout of a Sun Sparc disk where the disk label and boot code are located in the first partition.



Disk Etiketi İçeriği

Table 6.9. Data structure for the Sun Sparc disk label.

Byte Range	Description	Essential
0–127	ASCII Label	No
128–261	Spare VTOC (see Table 6.10)	Yes
262–263	Sectors to skip, writing	No
264–265	Sectors to skip, reading	No
266–419	Reserved	No
420–421	Disk speed	No
422–423	Number of physical cylinders	No
424–425	Alternates per cylinder	No
426–429	Reserved	No
430–431	Interleave	No
432–433	Number of data cylinders	No
434–435	Number of alternate cylinders	No
436–437	Number of heads	Yes
438–439	Number of sectors per track	Yes
440–443	Reserved	No
444–451	Partition #1 disk map (see Table 6.13)	Yes
452–459	Partition #2 disk map (see Table 6.13)	Yes
460–467	Partition #3 disk map (see Table 6.13)	Yes
468–475	Partition #4 disk map (see Table 6.13)	Yes
476–483	Partition #5 disk map (see Table 6.13)	Yes
484–491	Partition #6 disk map (see Table 6.13)	Yes
492–499	Partition #7 disk map (see Table 6.13)	Yes
500–507	Partition #8 disk map (see Table 6.13)	Yes
508–509	Signature Value (0xDABE)	No
510–511	Checksum	No

VTOC, 128 ile 261 arasındaki baytlarda bulunur. Bu yapı size bölüm sayısının (bayt 12-13) ve bayraklar, tür ve her bölüm için bir zaman damgası olduğunu söyler.

VTOC İçeriği

Table 6.10. Data structure for the VTOC in Sun Sparc disk labels.

Byte Range	Description	Essential
0–3	Version (0x01)	No
4–11	Volume Name	No
12–13	Number of Partitions	Yes
14–15	Partition #1 type (see Table 6.11)	No
16–17	Partition #1 flags (see Table 6.12)	No
18–19	Partition #2 type (see Table 6.11)	No
20–21	Partition #2 flags (see Table 6.12)	No
22–23	Partition #3 type (see Table 6.11)	No
24–25	Partition #3 flags (see Table 6.12)	No
26–27	Partition #4 type (see Table 6.11)	No
28–29	Partition #4 flags (see Table 6.12)	No
30–31	Partition #5 type (see Table 6.11)	No
32–33	Partition #5 flags (see Table 6.12)	No
34–35	Partition #6 type (see Table 6.11)	No
36–37	Partition #6 flags (see Table 6.12)	No
38–39	Partition #7 type (see Table 6.11)	No
40–41	Partition #7 flags (see Table 6.12)	No
42–43	Partition #8 type (see Table 6.11)	No
44–45	Partition #8 flags (see Table 6.12)	No
46–57	Boot info	No
58–59	Reserved	No
60–63	Signature Value (0x600DDEEE)	No
64–101	Reserved	No
102–105	Partition #1 timestamp	No
106–109	Partition #2 timestamp	No
110–113	Partition #3 timestamp	No
114–117	Partition #4 timestamp	No
118–121	Partition #5 timestamp	No
122–125	Partition #6 timestamp	No
126–129	Partition #7 timestamp	No
130–133	Partition #8 timestamp	No

- VTOC'daki bölümlerin her biri için alan türü, bölümün ne için kullanıldığını ve nereye mount edileceğini belirtir.
- Aslında dosya sistemlerini mount etme zamanı geldiğinde işletim sistemi farklı bir yapılandırma dosyası kullanacaktır.
- Bu nedenle, tür /usr/ partition için ayarlandığı için /usr/ olarak mount edileceği anlamına gelmez.
- Solaris disk etiket yapısı, diğer bölüm sistemleri gibi her bölüm için dosya sistemi türünü belirtmez.

Sun Partition Türleri ve Bayrak Değerleri

Table 6.11. Type values for each Sun partition (used for both Sparc and i386).

Value	Description
0	Unassigned
1	partition /boot/
2	/ partition
3	Swap
4	/usr/ partition
5	The entire disk
6	/stand/ partition
7	/var/ partition
8	/home/ partition
9	Alternate sector partition
10	cachefs partition

Table 6.12. Flag values of each Sun partition (used for both Sparc and i386).

Value	Description
1	The partition cannot be mounted
128	The partition is read-only

Table 6.13. Data structure for the Sun Sparc disk label disk map.

Byte Range	Description	Essential
0–3	Starting Cylinder	Yes
4–7	Size	Yes

Örnek İmaj

```
# dd if=sparc-disk.dd bs=512 count=1 | xxd
0000000: 4d61 7874 6f72 2038 3532 3530 4136 2063  Maxtor 85250A6 c
0000016: 796c 2031 3038 3534 2061 6c74 2032 2068  yl 10854 alt 2 h
0000032: 6420 3135 2073 6563 2036 3300 0000 0000  d 15 sec 63.....
0000048: 0000 0000 0000 0000 0000 0000 0000 0000  ................
[REMOVED - ZEROS]
0000128: 0000 0001 0000 0000 0000 0000 0008 0002  ................
0000144: 0000 0003 0001 0005 0000 0000 0000 0000  ................
0000160: 0000 0007 0000 0004 0000 0008 0000 0000  ................
0000176: 0000 0000 0000 0000 0000 0000 600d deee  ............`...
[REMOVED - ZEROS]
0000416: 0000 0000 1518 2a68 0000 0000 0000 0001  ......*h........
0000432: 2a66 0002 000f 003f 0000 0000 0000 0826  *f.....?.......&
0000448: 0020 b06b 0000 0000 0010 0176 0000 0000  . .k.......v....
0000464: 009c 8286 0000 0000 0000 0000 0000 0000  ................
0000480: 0000 0000 0000 0609 0007 cd0d 0000 1101  ................
0000496: 005d bdd5 0000 0458 0006 3e61 dabe 1ffe  .]....x..>a....
```

- İlk 128 bayt ASCII etiketini gösterir.
- VTOC 128'den başlar.
- 140'dan 141'e kadar olan baytlar yapıda 8 bölüm olduğunu gösterir.
- 142 ile 173 arasındaki baytlardan her bölüm için 2 baytlı ve 2 baytlık bayrak alanlarını görebiliriz.
- Örneğin, ilk bölüm 142 ile 143 arasındaki baytlarda tür değerine sahiptir ve 2'dir, bu / bölümüdür.
- Bayrak değeri bayt 144 ile 145 arasındadır ve 0'dır.
- Bayt 146 - 147, ikinci bölümün bir tür 3'tür (takas alanı)
- Bayt 148 - 149, bayrağı 1'dir (bağlanamayan) gösterir.
- Bayt 436 - 437, 15 (0x0f) kafalar olduğunu
- 438 - 439 baytlarının, parça başına 63 (0x3f) sektör olduğunu gösteriyor.
- Silindir adreslerini dönüştürmek için buna ihtiyacımız var. Yerleşim bilgisi bayt 444'te başlar ve başlangıç silindiri ve boyutu hem 4 bayt değerleridir. İlk bölüm 2,086 (0x00000826) ve 2,142,315 (0x0020b06b) boyutlarında bir başlangıç silindirine sahiptir.

Mmls Çıktısı

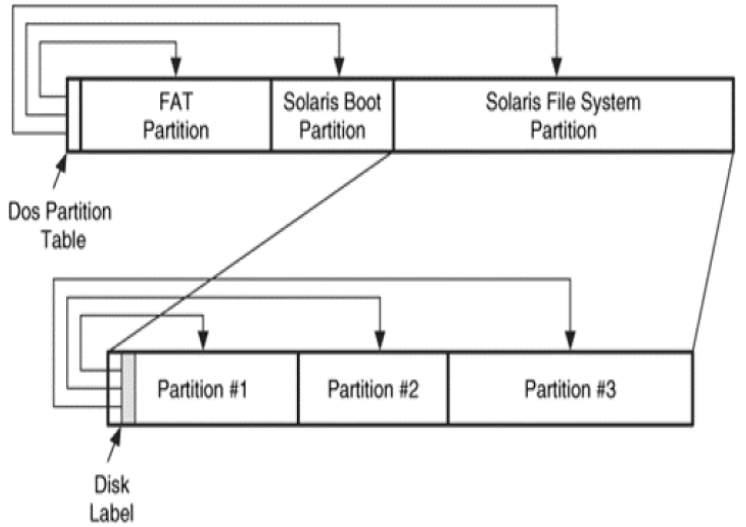
```
# mmls -t sun sparc-disk.dd
Sun VTOC
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  01      0000000000   0001048949   0001048950   swap (0x03)
01:  02      0000000000   0010257029   0010257030   backup (0x05)
02:  07      0001050840   0001460024   0000409185   /home/ (0x08)
03:  05      0001460025   0001971269   0000511245   /var/ (0x07)
04:  00      0001971270   0004113584   0002142315   / (0x02)
05:  06      0004113585   0010257029   0006143445   /usr/ (0x04)
```

İ386 Veri Yapıları

- Solaris bir i386 sistemine kurulduğunda, bir veya daha fazla DOS tabanlı bölüm oluşturulmalıdır.
- Tipik bir kurulum, bir önyükleme bölümü (DOS bölüm tipi 0xBE) ve dosya sistemleriyle bir bölüm (DOS bölüm tipi 0x82) oluşturacaktır.
- Önyükleme bölümü, sistemi başlatmak için gereken önyükleme kodunu içerir ve gerçek bir dosya sistemi içermez.
- Disk etiketi yapısı dosya sistemi DOS bölümünün (tür 0x82) ikinci sektöründe bulunur ve bu DOS bölümü içindeki Sun bölümlerinin düzenini tanımlar.
- Tüm Sun bölümleri, DOS bölümünün başlangıcından sonra başlamalıdır.

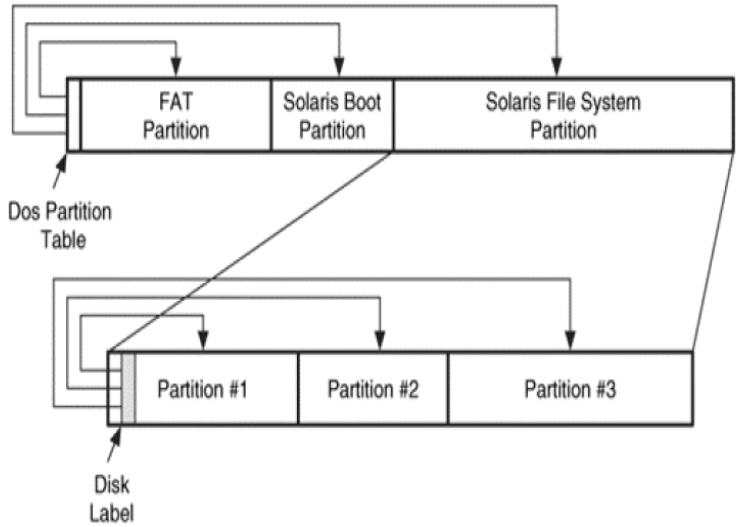
Figure 6.6. An i386 Sun disk with three DOS partitions. The final one contains a disk label and three Sun partitions.



İ386 Veri Yapıları

- Burada üç DOS bölümlü bir disk bulunur ve son bölüm bir disk etiketi ve üç adet Sun bölümü içerir.
- Disk etiket yapısı 512 bayt boyutundadır ve tüm bölüm bilgileri tek bir konumdadır çünkü Sparc sürümünden daha iyi düzenlenmiştir.
- I386 sürümünün bir başka yararı, bilginin CHS değil LBA adresleri kullanılarak depolanmasıdır.
- Bu farklılıklar dışında iki yapı da birbirine çok benzer. Disk etiketinin ilk 456 baytına İçindekiler Topluluk Tablosu (VTOC) denir ve burada bölümler, disk etiketi, sektör boyutu ve bölüm sayısı bulunur.

Figure 6.6. An i386 Sun disk with three DOS partitions. The final one contains a disk label and three Sun partitions.



Disk Etiket Yapısı

Table 6.14. Data structure for the Sun i386 disk label.

Byte Range	Description	Essential
0–11	Bootinfo	No
12–15	Signature Value (0x600DDEEE)	No
16–19	Version	No
20–27	Volume Name	No
28–29	Sector size	Yes
30–31	Number of Partitions	Yes
32–71	Reserved	No
72–83	Partition #1 (see Table 6.15)	Yes
84–95	Partition #2 (see Table 6.15)	Yes
96–107	Partition #3 (see Table 6-15)	Yes
108–119	Partition #4 (see Table 6.15)	Yes
120–131	Partition #5 (see Table 6.15)	Yes
132–143	Partition #6 (see Table 6.15)	Yes
144–155	Partition #7 (see Table 6.15)	Yes
156–167	Partition #8 (see Table 6.15)	Yes
168–179	Partition #9 (see Table 6.15)	Yes
180–191	Partition #10 (see Table 6.15)	Yes
192–203	Partition #11 (see Table 6.15)	Yes
204–215	Partition #12 (see Table 6.15)	Yes
216–227	Partition #13 (see Table 6.15)	Yes
228–239	Partition #14 (see Table 6.15)	Yes
240–251	Partition #15 (see Table 6.15)	Yes
252–263	Partition #16 (see Table 6.15)	Yes
264–327	Timestamps (not used)	No
328–455	Volume Label	No
456–507	Hardware Details	No
508–509	Signature Value (0xDABE)	No
510–511	Checksum	No

Table 6.15. Data structure for the Sun i386 disk label partition entry.

Byte Range	Description	Essential
0–1	Partition Type (see Table 6.11)	No
2–3	Flag (see Table 6.12)	No
4–7	Starting Sector	Yes
8–11	Size in Sectors	Yes

Table 6.11. Type values for each Sun partition (used for both Sparc and i386).

Value	Description
0	Unassigned
1	partition /boot/
2	/ partition
3	Swap
4	/usr/ partition
5	The entire disk
6	/stand/ partition
7	/var/ partition
8	/home/ partition
9	Alternate sector partition
10	cachefs partition

Table 6.12. Flag values of each Sun partition (used for both Sparc and i386).

Value	Description
1	The partition cannot be mounted
128	The partition is read-only

Örnek İmaj Çıktısı

```
# dd if=i386-disk.dd bs=512 skip=22497 | xxd
0000000: 0000 0000 0000 0000 0000 0000 eede 0d60  ...............'
0000016: 0100 0000 0000 0000 0000 0000 0002 1000  ................
0000032: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000048: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000064: 0000 0000 0000 0000 0200 0000 c00e 1000  ................
0000080: 0082 3e00 0300 0100 d00b 0000 f002 1000  ..>.............
0000096: 0500 0000 0000 0000 309a 7001 0000 0000  ........0.p.....
0000112: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000128: 0000 0000 0400 0000 c090 4e00 2000 fa00  ..........N. ...
0000144: 0000 0000 0000 0000 0000 0000 0800 0000  ................
0000160: e090 4801 0041 1f00 0100 0100 0000 0000  ..H..A..........
0000176: f003 0000 0900 0100 f003 0000 e007 0000  ................
[REMOVED - ZEROS]
0000320: 0000 0000 0000 0000 4445 4641 554c 5420  ........DEFAULT
0000336: 6379 6c20 3233 3936 3420 616c 7420 3220  cyl 23964 alt 2
0000352: 6864 2031 3620 7365 6320 3633 0000 0000  hd 16 sec 63....
[REMOVED - ZEROS]
0000448: 0000 0000 0000 0000 9e5d 0000 9c5d 0000  .........]...]..
0000464: 0200 0000 1000 0000 3f00 0000 0100 0000  ........?.......
0000480: 0000 100e 0000 0000 0000 0000 0000 0000  ................
0000496: 0000 0000 0000 0000 0000 0000 beda a24a  ..............J
```

- Bu bir i386 little-endian sıralamasında saklar.
- 30. baytta 16 (0x10) bölüm olduğunu görüyoruz.
- İlk bölüm girişi 72 numaralı bayttan başlar ve 83'te biter.
- Byte 72 ila 73, kök bölüm olan 0x02 tipi olduğunu gösterir.
- Başlangıç sektörü 76 ile 79 bayt arasında verilir ve 1.052.352 (0x00100EC0) görürüz.
- 80 ila 83 baytları bölüm boyutunu verir ve 4,096,512 (0x003e8200) görürüz.
- Bu disk etiketinde kullanılan 10 bölüm var ve sonuncusu 180 ile 191 arasındaki baytlarda yer alıyor.
- Zaman damgaları hepsi sıfır ve birim adı disk geometri bilgisiyle "DEFAULT".