PC Tabanlı Partitionlar

Dosya Sistem Analizi Hafta 5

Yrd. Doç. Dr. Erhan AKBAL

Giriş

- Son bölümde volüm analizi genel bir bakış sunuldu ve önemi gösterildi.
- Şimdi volümlerin soyut yapısının bırakacağız ve kişisel bilgisayarlarda kullanılan bölümleme sistemlerinin ayrıntılarına bakılacak.
- Bu bölümde, DOS bölmelerini, Apple bölümlerini ve çıkarılabilir medya yapıları incelenecektir. Ayrıca, bu sistemleri analiz ederken yapılması gereken özel hususlar açıklanacaktır.
- Sonraki bölümde sunucu tabanlı partition sistemleri incelenecektir.

DOS Partitionları

- En sık görülen bölümleme sistemi DOS tarzı bölümdür. DOS bölümleri Intel IA32 donanımıyla (yani i386 / x86) yıllarca kullanılmıştır, ancak hiçbir resmi spesifikasyon bulunmamaktadır.
- Microsoft, bu tür bir bölüm sistemi için Master Boot Record Ana Önyükleme Kaydı (MBR) diskleri kullanan isimleri kullanmaktadır.
- Bu, Genişletilebilir Ürün Yazılımı Arabirimi (EFI) ve 64-bit Intel tabanlı sistemler (IA64) ile kullanılan bir GUID Bölüm Tablosu (GPT) bir sonraki bölümde açıklanacaktır.
- Windows 2000'den başlayarak Microsoft, temel ve dinamik diskleri kullanır. Temel bir disk, bir MBR veya bir GPT diskini belirtir ve disk partitionları bağımsızdır.

DOS Partitionları

- Çoklu Disk Birimleri bölümünde gösterilecek dinamik diskler MBR veya GPT kullanan disklerdir. Bölümler birleştirilebilir ve tek bir büyük bölüm oluşturulabilir. Temel diskler geleneksel olarak DOS bölümleriyle ilişkilendirilmiştir.
- DOS bölümleri, Microsoft DOS, Microsoft Windows, Linux ve IA32 tabanlı FreeBSD ve OpenBSD sistemleri ile birlikte kullanılır.
- DOS bölümleri en yaygın fakat aynı zamanda en karmaşık bölümleme sistemidir.

MBR ve GPT Kavramları

- **MBR**, disk bölümlerini yönetmek için kullanılan, nispeten eski ancak günümüzde halen pek çok kullanıcı tarafından kullanılan sistemdir.
- Depolama alanında organize edilen disk bölümlerine dair bilgiler de bu sistem tarafından tutulur. MBR ayrıca işletim sistemi için disk bölümlerini taramaya yarayan kodu barındırır.
- **GPT**, UEFI standardına sahip diskin bölümlerini düzenleyen en güncel sistemdir. Intel Mac'ler standart olarak disklerinde GPT'yi kullanır.
- Sıradan yollardan Mac OS X'i MBR sisteme yüklemek mümkün değildir.
- Ayrıca pek çok Linux kernel'i GPT desteğine sahiptir. GPT diski Linux ile kullanmak için Grub 2 bootloader'ın kullanılması gerekmektedir.
- Windows tarafında ise GPT diskler Windows XP'den bu yana destekleniyor. (32-bit XP hariç) 64-bit Windows 8 yüklü bilgisayarlar GPT'yi varsayılan olarak kullanırken, Windows 7 ve öncesi sürümlerde MBR varsayılan olarak belirlenmiş durumda.

Temel MBR Konsepti

- DOS bölmelerini kullanarak düzenlenen bir disk, ilk 512 bayt sektöründe bir MBR'ye sahiptir.
- MBR önyükleme kodunu, bir bölüm tablosunu ve imza değerini içerir.
- Önyükleme kodu, bilgisayara bölüm tablosunu nasıl işleyeceğini ve işletim sistemini bulmasını anlatan yönergeleri içerir.
- Bölüm tablosunda dört girdi bulunur ve her biri bir DOS bölümünü tanımlayabilir.

- Her Girişte aşağıdaki alanlar bulunur.

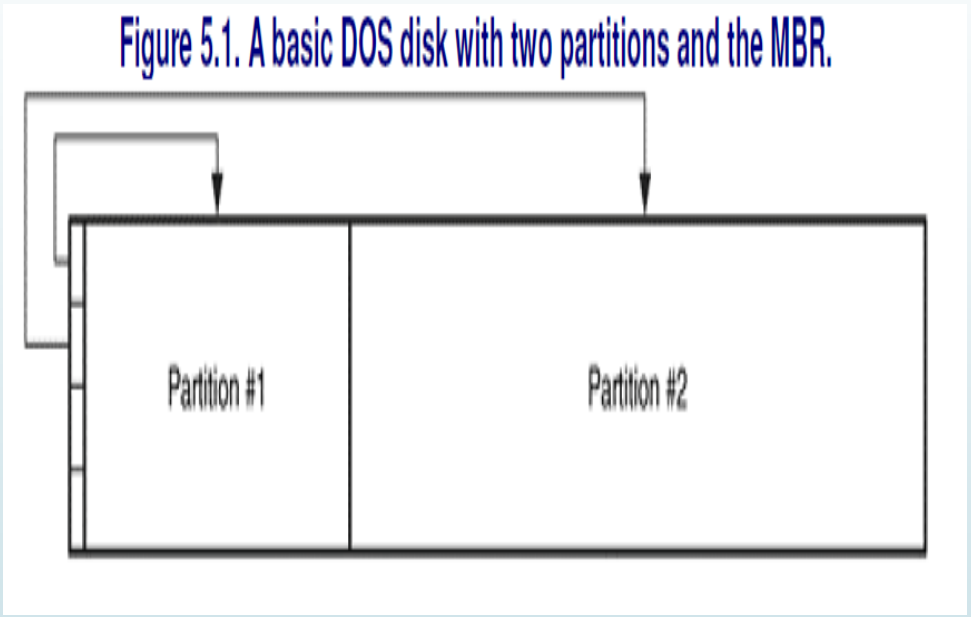
1. CHS adresi Başlangıcı
2. CHS adresi Bitişi
3. LBA adresinin başlangıcı
4. Partitionlardaki sektör sayısı
5. Partition türü
6. Bayraklar (Flags)

Temel MBR Konsepti

- Her tablo girişi, **CHS** ve **LBA** adreslerindeki bir bölümün düzenini açıklar.
- CHS adreslerinin yalnızca 8 GB'den küçük diskler için çalıştığı ancak LBA adresleri disklerin terabayta (TB) boyutta olmasına izin verdiğini unutmayın.
- Partition tür alanı, partitionda hangi veri türünün bulunması gerektiğini tanımlar. Yaygın örnekler arasında FAT, NTFS ve FreeBSD bulunmaktadır.
- Tür değeri, farklı OS'ler tarafından farklı şekilde kullanılır.
- NTFS türünde bir bölümün içine bir FAT dosya sistemi yerleştirebilir ve onu FAT olarak görürsünüz.
- Windows, bölüm türünü desteklemiyorsa, bir dosya sistemini bir bölüme mount etmeye çalışmaz.
- Bu nedenle, bir diskte bir Linux dosya sistemi türü olan bir bölümün içinde bir FAT dosya sistemi varsa, kullanıcı Windows'ta FAT dosya sistemini göremez.
- Bu davranış, Windows'tan bölümleri gizlemek için kullanılabilir.

Temel MBR Konsepti

- Tablodaki Her girdi, hangi bölümün "ön yüklenebilir" olduğunu tanımlayan bir bayrak alanı da içerir.
- Bu, bilgisayar önyükleme yaparken işletim sisteminin nerede olduğunu belirlemek için kullanılır.
- MBR'deki dört girişi kullanarak, dört bölüme kadar basit bir disk düzeni tanımlayabiliriz. Şekilde, iki bölümlü ve MBR'nin ilk bölümü olduğu basit diski göstermektedir.



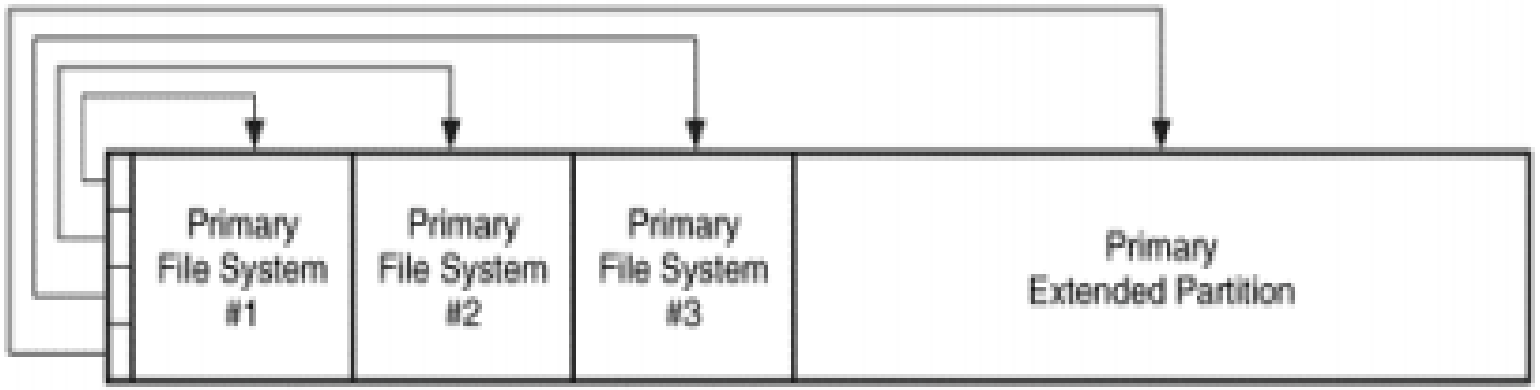
Genişletilmiş (Extended) MBR Yapısı

- MBR, dört partitiona kadar basit bir tanımlama yöntemidir.
- Bununla birlikte, birçok sistem bundan daha fazla bölüm gerektirir.
- Örneğin, kullanıcının birden fazla işletim sistemi kullanması nedeniyle altı adet 20GB bölümlemeye bölmek istediği 120GB'lık bir diski düşünün. Dört bölüm tablosu girdisini kullanarak altı bölüm tanımlayamayız.
- Bu tasarım probleminin çözümü, DOS bölmelerini bu kadar karmaşık yapan şeydir.
- Çözümün ardındaki temel teori normal bölümler için MBR'deki girdilerin bir, iki veya üçünü kullanmak ve daha sonra diskin geri kalanını dolduracak bir "genişletilmiş bölüm" oluşturmaktır.

Genişletilmiş (Extended) MBR Yapısı

- Birincil bir dosya sistemi bölümü, girişi MBR'de ve bölüm bir dosya sistemi veya başka yapılandırılmış veriler içeren bir bölümdür.
- Birincil genişletilmiş bölüm, girişi MBR'de olan ve bölüm ek bölümler içeren bir bölümdür.

Figure 5.2. A DOS disk with three primary file system partitions and one primary secondary partition.

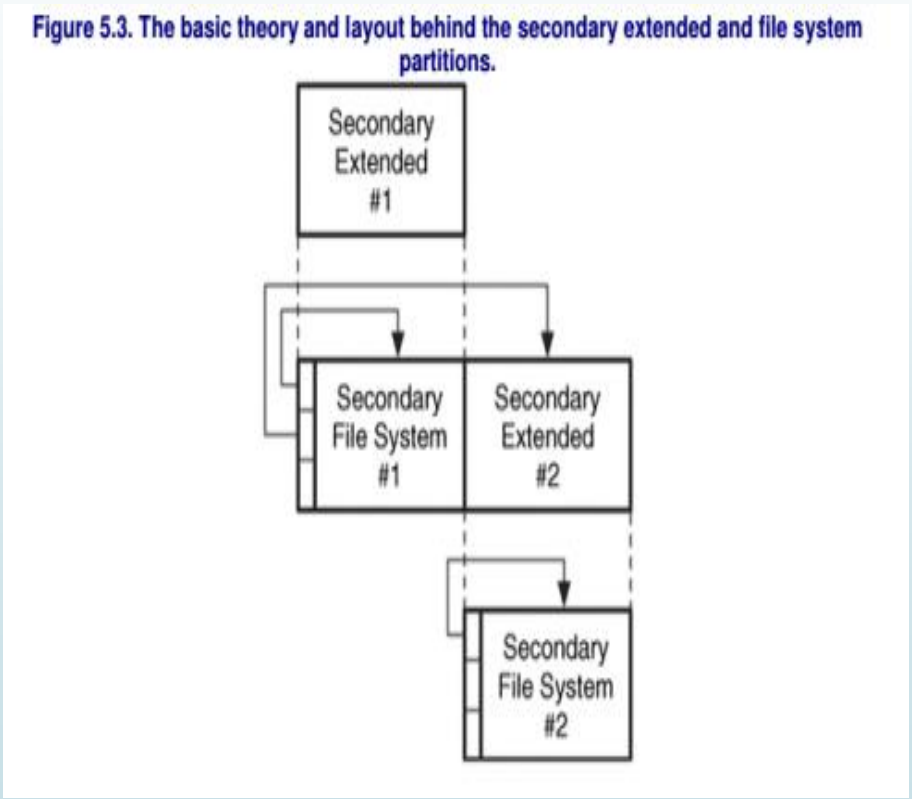


Primary Extended Partition Yapısı

- Temel teori, her dosya sistemi bölümünü, dosya sistemi bölümünün ne kadar büyük olduğunu ve bir sonraki bölümü nerede bulabileceğimizi açıklayan veriler öne çıkmaktadır.
- Tüm bu partitonlar birincil genişletilmiş partition içine yerleştirilmelidir, bu yüzden mümkün olduğunca büyük kapasitede olmalıdır.
- Windows'da mantıksal partition olarak da adlandırılan ikincil bir dosya sistemi bölümü, birincil genişletilmiş partition sınırlarının içinde bulunur ve bir dosya sistemi veya başka yapılandırılmış veriler içerir.
- İkincil dosya sistemi bölümleri, genişletilmiş bir bölümdeyken MBR'de açıklanan bölümlere eşdeğerdir.
- İkincil genişletilmiş partition, bir partition tablosu ve ikincil bir dosya sistemi partitionı içeren bir partitiondır.
- İkincil genişletilmiş partitionlar, ikincil dosya sistemi partitionlarına sarılır ve ikincil dosya sistemi partitonın bulunduğu yeri ve bir sonraki ikincil genişletilmiş bölümün nerede olduğunu açıklar.

Primary Extended Partition Yapısı

- İkincil Genişletilmiş # 1, İkincil Dosya Sistemi # 1 ve İkincil Genişletilmiş # 2'yi işaret eden bir bölüm tablosu içerir.
- İkincil Genişletilmiş # 2, İkincil Dosya Sistemi # 2'ye işaret eden bir bölüm tablosu içerir.
- Ayrıca, başka bir ikincil genişletilmiş bölüme işaret edebilir ve bu işlem, disk alanımız bitene kadar tekrarlanabilir.



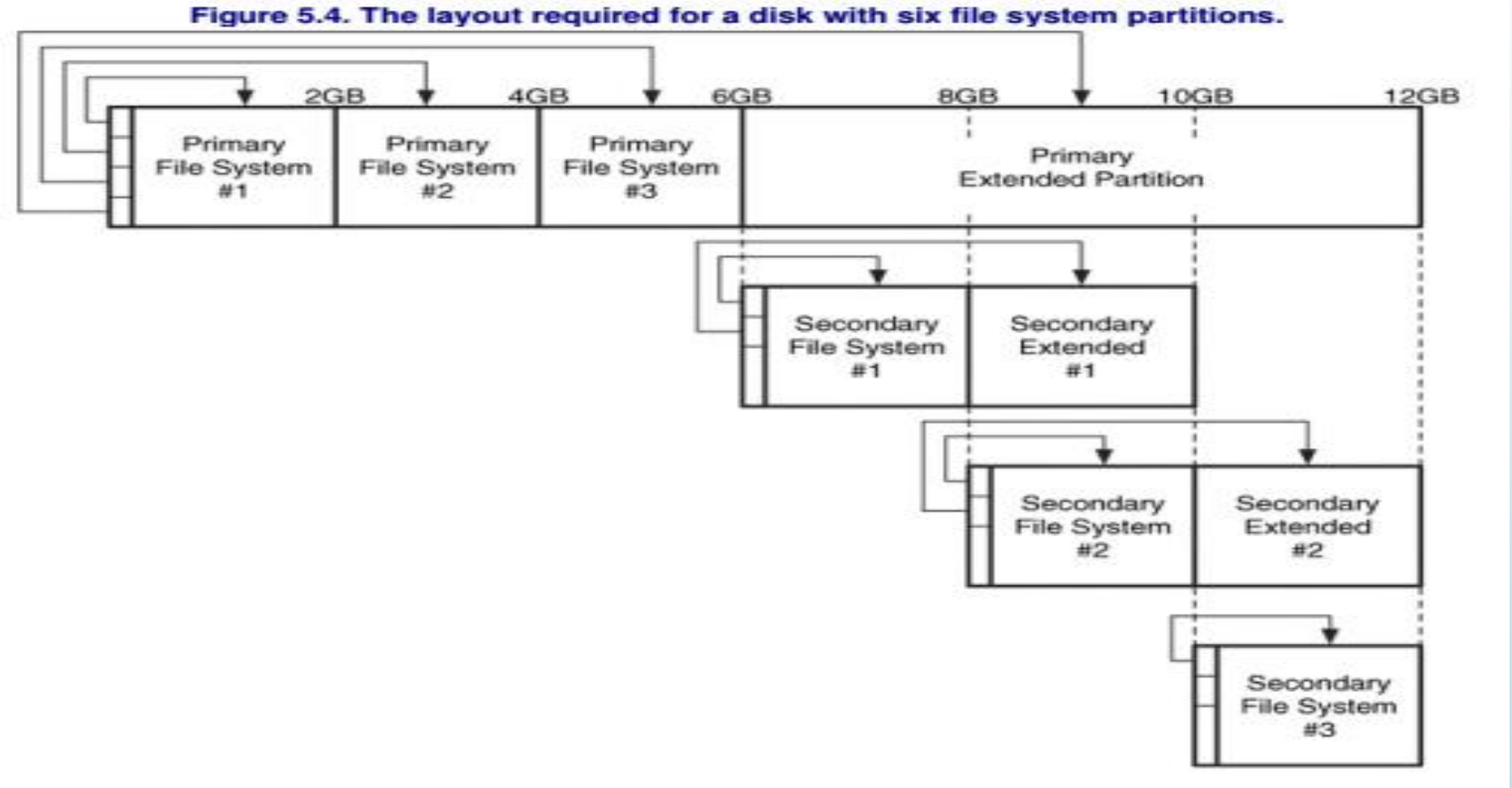
Primary ve Extended Yapılarının birarada kullanımı

- Eğer bir ile dört arasında partitiona ihtiyaç duyarsak, bunları yalnızca MBR kullanarak oluşturabiliriz ve genişletilmiş partitionlardan endişelenmemize gerek yoktur.
- Dört bölümden fazlasını istiyorsak, MBR'de üç birincil dosya sistemi bölümü oluşturmalı ve ardından geri kalan bölümü birincil genişletilmiş partitona ayırmalıyız.
- Birincil genişletilmiş bölümün içinde, bağlantılı liste bölümleme yöntemini kullanıyoruz.

Örnek Yapı

12GB'lık bir diski altı 2GB'lık bölüme ayırmak istiyoruz.

İlk 3GB bölümünü MBR'deki ilk üç girişi kullanarak oluşturuyoruz ve geri kalan 6GB'dan 12GB'a uzanan birincil genişletilmiş bölüme ayrılmıştır.



Analiz Sorunları

- Genişletilmiş bir bölüm tablosunda en fazla ikincil bir dosya sistemi bölümü için bir girdi ve ikincil bir genişletilmiş bölüm için bir girdi olmalıdır.
- Pratikte, daha fazla giriş yapılırsa, çoğu işletim sistemi bir hata oluşturmaz.
- Bazı adli araçlar, üçüncü bölüm girişini düzgün bir şekilde ele alırken, bazıları göz ardı ettiği gösterilmiştir.

Boot Kodu

- Bir DOS diskindeki önyükleme kodu, MBR olan ilk **512** baytlık sektörün ilk **446** baytında bulunur.
- Sektörün sonu bölümleme tablosunu içerir. Standart Microsoft önyükleme kodu, MBR'deki partition tablosunu işler ve hangi partifionın önyüklenebilir bayrağa sahip olduğunu tanımlar.
- Böyle bir partition bulunduğunda, partition ilk sektörüne bakar ve orada bulunan kodu çalıştırır. Partitionın başındaki kod işletim sistemine özgü olacaktır.
- Önyükleme kesici virüsleri kendilerini MBR'nin ilk 446 baytına yerleştirir, böylece bilgisayar önyüklenirken aktif olurlar.
- Bir bilgisayarda birden fazla işletim sistemine sahip olmak çok daha yaygın hale gelmektedir. Bunu halletmenin iki yolu vardır.
- Windows, önyüklenebilir bölümde bir kullanıcının hangi işletim sistemini yükleyeceğini seçmesine olanak tanıyan kodlar yükleyerek bunu çözer.
- Diğer yöntem, MBR'deki kodu değiştirmektir. Yeni MBR kodu kullanıcıya bir seçenek listesi sunar ve kullanıcı hangi bölümden önyükleneceğini seçer.

Özet

- DOS bölüm sistemi karmaşıktır, çünkü her bölüm tablosu yalnızca dört girişe sahiptir. DOS bölümleri bulunan bir diskin düzen bilgilerini listelemek için aşağıdaki üst düzey adımlar gereklidir:

1. MBR Tablosu, diskin ilk sektöründe okunur ve dört partition tablosu girişi tanımlanır ve işlenir.
2. Uzatılmış bir partition için bir girdi ile karşılaşıldığında, genişletilmiş bölümün ilk kesimi okunur ve bölüm tablosu girdileri, MBR ile aynı şekilde işlenir.
3. Genişletilmemiş bir bölüm için bir girdi işlendiğinde, başlangıç sektörü ve boyutları görüntülenir. Biten sektör adresi, başlangıç sektör adresini ve boyutunu birlikte ekleyip bir çıkararak belirlenebilir.

VERİ YAPILARI

Bu bölüm sistemin çalışmasını sağlayan veri yapıları hakkında ayrıntıların gösterecektir.

MBR Veri Yapıları

- DOS Bölme tabloları, MBR'de ve her genişletilmiş partionun ilk kesiminde bulunur.
- Öncelikle, hepsi aynı 512 baytlık yapıyı kullanır. İlk 446 bayt, assembly boot kodu için ayrılmıştır.
- Kod bilgisayarın başlatılabilmesi için gereklidir.

Table 5.1. Data structures for the DOS partition table.

Byte Range	Description	Essential
0–445	Boot Code	No
446–461	Partition Table Entry #1 (see Table 5.2)	Yes
462–477	Partition Table Entry #2 (see Table 5.2)	Yes
478–493	Partition Table Entry #3 (see Table 5.2)	Yes
494–509	Partition Table Entry #4 (see Table 5.2)	Yes
510–511	Signature value (0xAA55)	No

Partition Tablosu Yapısı

- Partiton tablosu 4 tane 16 baytlık içeriğe sahiptir.
- CHS adreslerinin temel daha eski sistemler için şart olduğunu, ancak yeni sistemlerde gerekli olmadığını unutmayın.

Table 5.2. Data structure for DOS partition entries.

Byte Range	Description	Essential
0–0	Bootable Flag	No
1–3	Starting CHS Address	Yes
4–4	Partition Type (see Table 5.3)	No
5–7	Ending CHS Address	Yes
8–11	Starting LBA Address	Yes
12–15	Size in Sectors	Yes

Partition Tablosu Yapısı

- Önyükleme bayrağı her zaman gerekli olmaz. Örneğin, üzerinde Microsoft Windows olan bir sistemin varsa ve disk iki bölüme ayrılmışsa, üzerinde işletim sistemi olan bölüm (örneğin C: \ windows) önyüklenebilir bayrağa sahip olacak.
- Öte yandan, önyükleme kodu kullanıcıdan önyüklenecek bölümü seçmesini isterse önyüklenebilir bayrak gerekli değildir.
- Bazı önyükleme programları, kullanıcı bu bölümü başlatmayı seçtikten sonra önyüklenebilir bayrağı ayarlar.
- Başlama ve bitiş CHS adresleri, 8 bit baş değeri, 6 bitlik bir sektör değeri ve 10 bitlik bir silindir değeri içerir. Teorik olarak, CHS adresleri veya LBA adresleri her bölüm için ayarlanmalıdır, ancak her ikisi birden ayarlanmamalıdır.
- Hangi değerlerin ayarlanması gerektiğini belirlemek için sistemi önyüklemek OS ve koda bağlıdır.

Partition Türleri

Partition type alanı, bölümde olması gereken dosya sistemi türünü tanımlar.

Table 5.3. Some of the type values for DOS partitions.

Type	Description
0x00	Empty
0x01	FAT12, CHS
0x04	FAT16, 16–32 MB, CHS
0x05	Microsoft Extended, CHS
0x06	FAT16, 32 MB–2GB, CHS
0x07	NTFS
0x0b	FAT32, CHS
0x0c	FAT32, LBA
0x0e	FAT16, 32 MB–2GB, LBA
0x0f	Microsoft Extended, LBA
0x11	Hidden FAT12, CHS
0x14	Hidden FAT16, 16–32 MB, CHS
0x16	Hidden FAT16, 32 MB–2GB, CHS
0x1b	Hidden FAT32, CHS
0x1c	Hidden FAT32, LBA
0x1e	Hidden FAT16, 32 MB–2GB, LBA
0x42	Microsoft MBR, Dynamic Disk
0x82	Solaris x86
0x82	Linux Swap
0x83	Linux
0x84	Hibernation
0x85	Linux Extended
0x86	NTFS Volume Set
0x87	NTFS Volume Set
0xa0	Hibernation
0xa1	Hibernation
0xa5	FreeBSD
0xa6	OpenBSD
0xa8	Mac OSX
0xa9	NetBSD
0xab	Mac OSX Boot
0xb7	BSDI
0xb8	BSDI swap
0xee	EFI GPT Disk
0xef	EFI System Partition
0xfb	Vmware File System
0xfc	Vmware swap

Partition Türleri

- 0x01 - 0x0f aralığında Microsoft dosya sistemleri için kaç bölüm türüne sahip olduğuna dikkat edin. Bunun nedeni, Microsoft işletim sistemlerinin bölümün nasıl veri okuduğunu ve yazdığını belirlemek için bölüm türünü kullanmasıdır.
- Windows, INT 13h veya genişletilmiş INT 13h BIOS yordamlarını kullanabilir.
- Genişletilmiş INT13h yordamları, 8.1GB'dan büyük disklere erişmek ve CHS yerine LBA adresleme kullanmak için gereklidir. Bu nedenle, FAT16 0x04 ve 0x0E türleri, OS'un ikinci tür için genişletilmiş yordamları kullanması dışında aynıdır.
- Benzer şekilde, 0x0B ve 0x0C FAT32'nin normal ve genişletilmiş versiyonlarını ve 0x05'in ve 0x0F'de normal ve genişletilmiş partition türlerini göstermektedir.
- Bu bölüm türlerinin "gizli" versiyonlarında üst dizinde 0 yerine 1 olur ve bunlarla çeşitli araçlar oluşturur.

Örnek Yapı

- Örnek Sistem çift önyükleme Microsoft Windows ve Linux sistemine sahiptir ve sekiz dosya sistemi bölümüne sahiptir.
- Birinci örnek, diskin ilk sektöründendir. Bu çıktı, xxd aracınındır, ancak benzer veriler, Windows veya UNIX'de bir hex editör kullanılarak bulunabilir. Aşağıdaki komut Linux'ta kullanılmıştır.

```
# dd if=disk3.dd bs=512 skip=0 count=1 | xxd
```

Soldaki sütun onluk byte ofseti, orta sekiz sütun onaltılık biçimde veridir ve son sütun ASCII'ye tercüme edilmiştir. Veriler, little-endian olan IA32 tabanlı sistemden ve en düşük anlamlı baytla en düşük adrese sahip sayıları saklar. Bu nedenle, orta sütundaki bayt sırası tersine çevrilmesi gerekebilir. Diskin MBR'si şöyledir:

```
# dd if=disk3.dd bs=512 skip=0 count=1 | xxd
0000000: eb48 9010 8ed0 bc00 b0b8 0000 8ed8 8ec0  .H..............
[REMOVED]
0000384: 0048 6172 6420 4469 736b 0052 6561 6400  .Hard Disk.Read.
0000400: 2045 7272 6f72 00bb 0100 b40e cd10 ac3c   Error........<
0000416: 0075 f4c3 0000 0000 0000 0000 0000 0000  .u..............
0000432: 0000 0000 0000 0000 0000 0000 0000 0001  ................
0000448: 0100 07fe 3f7f 3f00 0000 4160 1f00 8000  ....?.?...A`....
0000464: 0180 83fe 3f8c 8060 1f00 cd2f 0300 0000  ....?..`.../....
0000480: 018d 83fe 3fcc 4d90 2200 40b0 0f00 0000  ....?.M."."@.....
0000496: 01cd 05fe ffff 8d40 3200 79eb 9604 55aa  .......@2.y...U.
```

Örnek Yapının İncelenmesi

- İlk 446 bayt önyükleme kodunu içerir.
- 0xAA55 imza değeri, sektörün son iki baytında görülebilir (endian sıralaması nedeniyle çıktıda ters çevrilmişdir).
- Bölüm tablosu koyu renkte ve 0x0001 ile ofset 446'da başlar.
- Çıktıdaki her satır 16 bayt ve her tablo girişi 16 bayttır. Bu nedenle, ikinci giriş, ilk girdinin bir satır altında 0x8000 ile başlar.
- Daha önce özetlenen yapıyı kullanarak, dört bölüm tablosu girişi Tablo 5.4'te gösterilmektedir. Değerler, önemli değerlerin parantez içindeki onluk değerli hali ile onaltılık biçimde gösterilmiştir.

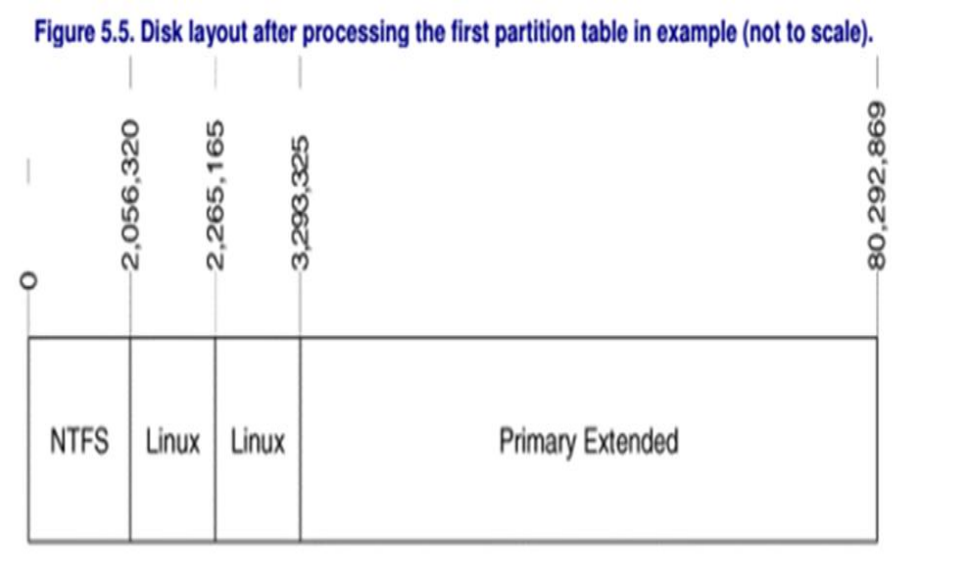
```
# dd if=disk3.dd bs=512 skip=0 count=1 | xxd
0000000: eb48 9010 8ed0 bc00 b0b8 0000 8ed8 8ec0  .H..............
[REMOVED]
0000384: 0048 6172 6420 4469 736b 0052 6561 6400  .Hard Disk.Read.
0000400: 2045 7272 6f72 00bb 0100 b40e cd10 ac3c   Error.........<
0000416: 0075 f4c3 0000 0000 0000 0000 0000 0000  .u..............
0000432: 0000 0000 0000 0000 0000 0000 0000 0001  ................
0000448: 0100 07fe 3f7f 3f00 0000 4160 1f00 8000  ....?.?...A`....
0000464: 0180 83fe 3f8c 8060 1f00 cd2f 0300 0000  ....?..`.../....
0000480: 018d 83fe 3fcc 4d90 2200 40b0 0f00 0000  ....?.M."@.....
0000496: 01cd 05fe ffff 8d40 3200 79eb 9604 55aa  .......@2.y...U.
```

Table 5.4. The contents of the primary partition table in the example disk image.

#	Flag	Type	Starting Sector	Size
1	0x00	0x07	0x0000003f (63)	0x001f6041 (2,056,257)
2	0x80	0x83	0x001f6080 (2,056,320)	0x00032fcd (208,845)
3	0x00	0x83	0x0022904d (2,265,165)	0x000fb040 (1,028,160)
4	0x00	0x05	0x0032408d (3,293,325)	0x0496eb79 (76,999,545)

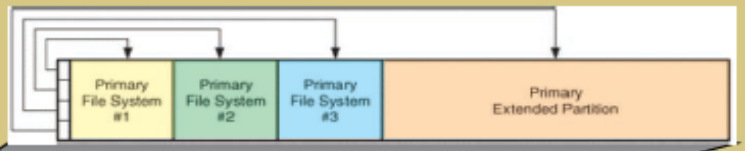
Disk Görünümü

- Tablo 5.4'te ve Tablo 5.3'deki bölüm türü alanını kullanarak, her bölümde ne tür verinin bulunduğunu tahmin edebiliriz.
- İlk bölüm NTFS dosya sistemi (tür 0x07), ikinci ve üçüncü bölümler Linux dosya sistemleri (0x83) için, dördüncü bölüm ise genişletilmiş bölüm (0x05) olmalıdır.
- İkinci giriş önyüklenebilir olarak ayarlanmıştır. Extended partition beklenmeliydi, çünkü daha önce toplamda sekiz bölüm olacağı belirtilmişti. Bu bölüm tablosundaki disk düzeni Şekil 5.5'de gösterilmiştir.



MBR

Master Boot Record



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	33	C0	8E	D0	BC	00	7C	8E	C0	8E	D8	BE	00	7C	BF	00
16	06	B9	00	02	FC	F3	A4	50	68	1C	06	CB	FB	B9	04	00
32	BD	BE	07	80	7E	00	00	7C	0B	0F	85	0E	01	83	C5	10
48	E2	F1	CD	18	88	56	00	55	C6	46	11	05	C6	46	10	00
64	B4	41	BB	AA	55	CD	13	5D	72	0F	81	FB	55	AA	75	09
80	F7	C1	01	00	74	03	FE	46	10	66	60	80	7E	10	00	74
96	26	66	68	00	00	00	00	66	FF	76	08	68	00	00	68	00
112	7C	68	01	00	68	10	00	B4	42	8A	56	00	8B	F4	CD	13
128	9F	83	C4	10	9E	EB	14	B8	01	02	BB	00	7C	8A	56	00
144	8A	76	01	8A	4E	02	8A	6E	03	CD	13	66	61	73	1C	FE
160	4E	11	75	0C	80	7E	00	80	0F	84	8A	00	B2	80	EB	84
176	55	32	E4	8A	56	00	CD	13	5D	EB	9E	81	3E	FE	7D	55
192	AA	75	6E	FF	76	00	E8	8D	00	75	17	FA	B0	D1	E6	64
208	E8	83	00	B0	DF	E6	60	E8	7C	00	B0	FF	E6	64	E8	75
224	00	FB	B8	00	BB	CD	1A	66	23	C0	75	3B	66	81	FB	54
240	43	50	41	75	32	81	F9	02	01	72	2C	66	68	07	BB	00
256	00	66	68	00	02	00	00	66	68	08	00	00	00	66	53	66
272	53	66	55	66	68	00	00	00	00	66	68	00	7C	00	00	66
288	61	68	00	00	07	CD	1A	5A	32	F6	EA	00	7C	00	00	CD
304	18	A0	B7	07	EB	08	A0	B6	07	EB	03	A0	B5	07	32	E4
320	05	00	07	8B	F0	AC	3C	00	74	09	BB	07	00	B4	0E	CD
336	10	EB	F2	F4	EB	FD	2B	C9	E4	64	EB	00	24	02	E0	F8
352	24	02	C3	49	6E	76	61	6C	69	64	20	70	61	72	74	69
368	74	69	6F	6E	20	74	61	62	6C	65	00	45	72	72	6F	72
384	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69
400	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E
416	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74
432	65	6D	00	00	00	63	7B	9A	00	00	00	00	00	00	00	02
448	03	00	06	FE	7F	E1	80	00	00	00	80	37	76	00	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

DOS partition table format	
Bytes	**Purpose**
0-445	Boot code
446-461	Partition Table Entry #1
462-477	Partition Table Entry #2
478-493	Partition Table Entry #3
494-509	Partition Table Entry #4
510-511	Signature value (0xAA55)

DOS Partition Table Entry format	
Bytes	**Purpose**
0	Bootable flag (0x80=active; else 0x00)
1-3	Starting CHS address
4	Partition type (e.g., 0x00=empty, 0x01=FAT12, 0x07=NTFS, 0x0b=FAT32 (CHS), 0x83=Linux, 0xa5=FreeBSD, 0xa8=MacOS X)*
5-7	Ending CHS address
8-11	Starting LBA address
12-15	Size (in sectors)

Flag	Starting CHS	Partition Type	Ending CHS	Starting LBA	Size
00	000302	06	E17FFE	00000080	00763780

*Data is in an IA32-based system, Little endian (least significant byte is first)

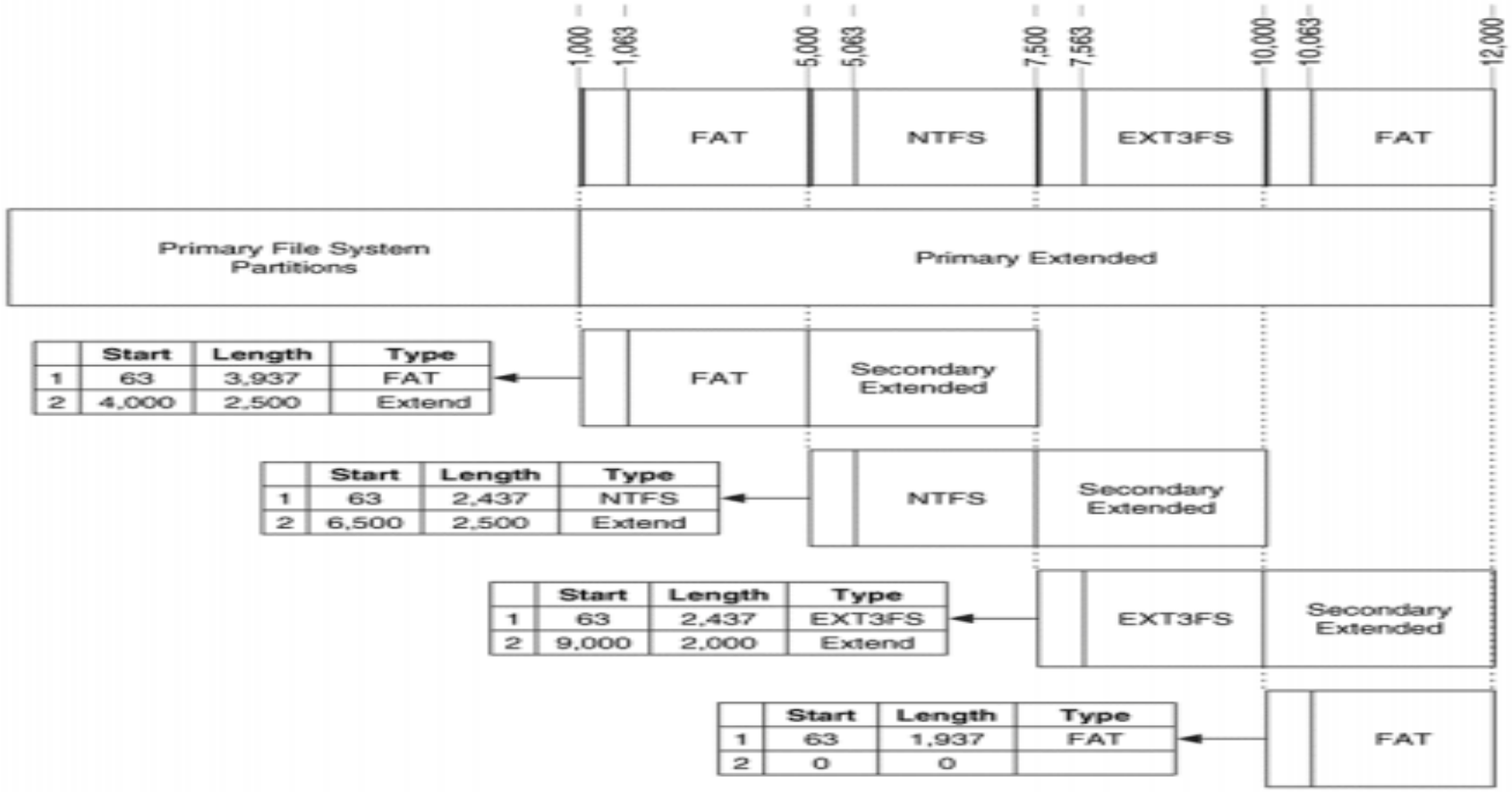
Genişletilmiş Partition Yapısı

Veri Yapısı

- Genişletilmiş bölümlerin, MBR'nin yaptığı gibi ilk sektörde aynı yapıyı kullandıklarını, ancak bunları bağlantılı bir liste yapmak için kullandıklarını hatırlayın.
- Partition tablosu verileri biraz farklı olsa da, başlangıç sektör adresleri diskin başlangıcının yanı sıra diskteki diğer yerlerle ilgilidir.
- Ayrıca, ikincil bir dosya sistemi bölümünün başlangıç sektörü, ikincil bir genişletilmiş bölümün başlangıç bölümünden farklı bir yerle bağlantılıdır.
- İkincil bir dosya sistemi kayıtı için başlangıç adresi, geçerli partition tablosuyla ilgilidir. Bu nedenle, kendilerine göre başlangıç adresleri vardır.
- Öte yandan, ikincil bir genişletilmiş partition kaydı için başlangıç adresi, birincil genişletilmiş bölümle ilişkilidir.

Örnek Yapı

Figure 5.6. Disk with three secondary extended partitions. Note that the starting location of the secondary extended partitions is relative to the start of the primary extended partition, sector 1000.



	Start	Length	Type
1	63	3,937	FAT
2	4,000	2,500	Extend

	Start	Length	Type
1	63	2,437	NTFS
2	6,500	2,500	Extend

	Start	Length	Type
1	63	2,437	EXT3FS
2	9,000	2,000	Extend

	Start	Length	Type
1	63	1,937	FAT
2	0	0	

- Birincil genişletilmiş bölümün ilk sektöre ait içeriği 3,293,325 numaralı sektörde aşağıdaki gibidir:

```
# dd if=disk3.dd bs=512 skip=3293325 count=1 | xxd
[REMOVED]
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 A.....?.>.@.....
0000480: 0000 0000 0000 0000 0000 0000 0000 0000 ................
0000496: 0000 0000 0000 0000 0000 0000 0000 55aa ..............U.
```

- Dört bölüm tablosu girdisi işaretlidir ve son iki girdinin boş olduğunu görüyoruz.

- İlk iki bölüm tablosu girişi aşağıdaki gibi olur.

Table 5.5. The contents of the primary extended partition table in the example disk image.

#	Flag	Type	Starting Sector	Size
5	0x00	0x83	0x0000003f (63)	0x003e8200 (4,096,572)
6	0x00	0x05	0x003e823f (4,096,575)	0x000fb040 (1,028,160)

- **Girdi # 5**'in bir Linux dosya sistemi (0x83) için bir türü vardır, bu yüzden ikincil bir dosya sistemi bölümüdür ve başlangıç sektörü geçerli genişletilmiş bölümün başlangıcı ile ilişkilidir (sektör 3,293,325).

```
3,293,325 + 63 = 3,293,388
```

Girdi #6 bir Genişletilmiş DOS partition türüdür. Bu nedenle başlangıç sektörü, geçerli bölüm olan birincil genişletilmiş bölümün başlangıcına göre değişir.

3,293,325 + 4,096,575 = 7,389,900

Figure 5.7. Disk layout after processing the second partition table (not to scale).

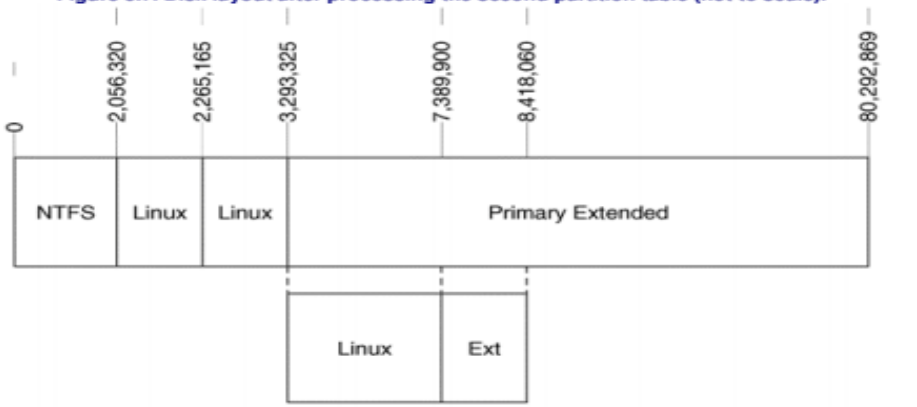
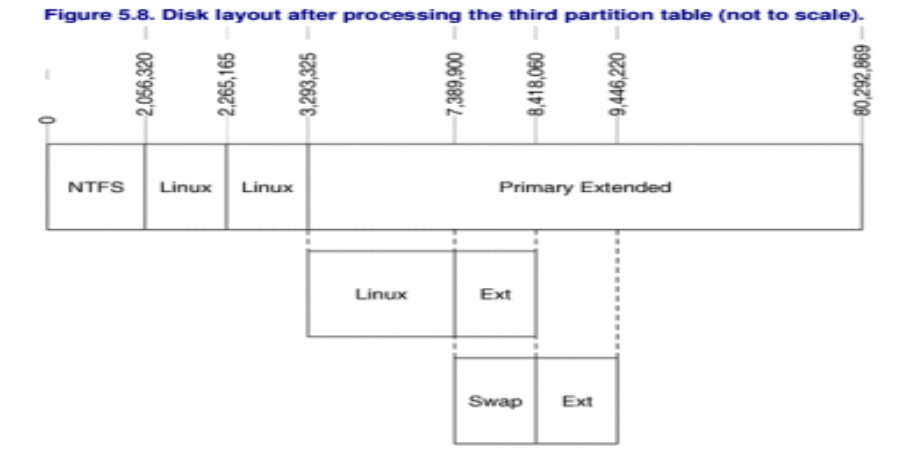


Table 5.6. The contents of the first secondary extended partition table in the example disk image.

#	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)

Figure 5.8. Disk layout after processing the third partition table (not to scale).



Örnek İmaj Çıktısı -fdisk

- Fdisk komutu Linux ile birlikte gelir ve Windows ile birlikte gelen aynı ada sahip araçtan farklıdır.
- Fdisk, Linux aygıtında veya dd tarafından üretilen bir disk imaj dosyasında çalıştırılabilir.
- -l bayrağı, partitionlarında düzenlenebileceği interaktif moda girerek bölümleri listelemeye zorlar.
- -u bayrağı çıktıyı silindir yerine sektörlere zorlar.
- Elle ayrıştırdığımız DOS Bölmeli disk çıktısı şöyledir:

```
# fdisk -lu disk3.dd
Disk disk3.dd: 255 heads, 63 sectors, 0 cylinders
Units = sectors of 1 * 512 bytes

   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
```

Örnek Çıktı –mmls,dd

- Bu çıktıdan birçok şeyi gözlemleyebiliriz.
- Çıktıda yalnızca birincil genişletilmiş bölüm (disk3.dd4) listelenmiştir.
- Linux swap bölümünün bulunduğu ikincil genişletilmiş bölüm görüntülenmiyor.
- Çoğu durumda bu kabul edilebilir, çünkü yalnızca birincil ve ikincil dosya sistemi bölümleri bir soruşturma için gereklidir, ancak tüm bölüm tablosu girdilerini görmediğiniz unutulmamalıdır.
- Seluth Kitindeki mmls aracı biraz daha farklı bilgiler sağlar. Bir partition tarafından kullanılmayan sektörler, bölüm tablolarının konumu işaretlenir ve genişletilmiş bölüm konumları kaydedilir.
- İlk fdisk örneği için kullandığımız aynı diski kullanarak, aşağıdakiler görülür:

```
# mmls -t dos disk3.dd
Units are in 512-byte sectors
     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)
22:  -----   0017639370   0017639370   0000000001   Table #5
23:  -----   0017639371   0017639432   0000000062   Unallocated
24:  05:00   0017639433   0048371714   0030732282   Linux (0x83)
```

Çıktı Yapısı

- Unallocated girdiler, bölümler arasındaki boşluk ve bölüm tablosunun sonu ile ilk bölümün başlangıcı arasındaki boşluk içindir.
- Mmls çıktısı hem bitiş adresini hem de boyutunu verir, bu nedenle dd bölümleri görmek için kolayca kullanılabilir.
- Mmls çıktısı bölümün başlangıç sektörüne göre sıralanır, bu nedenle ilk sütun her bir giriş için bir sayaçtır.
- Bölüm tablosu girdisi ile hiçbir korelasyona sahip değildir.
- İkinci sütun, bölüm tablosunun bulunduğu bölümü ve hangi tabloda yer aldığını gösterir.
- İlk sayı, tabloyu gösterir, 0 ilk tablo başlangıcını 1 ilk uzatılmış tablo başlangıcıdır.
- Sıralanmış çıktı, bölümlenmemiş sektörleri tanımlamaya yardımcı olur. Örneğin, şu çıktıyı düşünün

```
# mmls -t dos disk1.dd
Units are in 512-byte sectors
     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Table #0
01:  -----   0000000001   0000000062   0000000062   Unallocated
02:  00:00   0000000063   0001028159   0001028097   Win95 FAT32 (0x0B)
03:  -----   0001028160   0002570399   0001542240   Unallocated
04:  00:03   0002570400   0004209029   0001638630   OpenBSD (0xA6)
05:  00:01   0004209030   0006265349   0002056320   NTFS (0x07)
```

Bu çıktıda, NTFS bölümünün OpenBSD bölümünden önceki bir slotta olduğunu, ancak NTFS partitionı OpenBSD partitionundan sonra başladığını görüyoruz. Ayrıca '00:02 'girişi olmadığını ve FAT ile OpenBSD bölümleri arasındaki 1.542.240 sektörün ayrılmamış olarak algılandığını görebiliriz.

Analiz Kuralları

- Genişletilmiş bölümler için 63 sektör ayrılır. Bu nedenle, genişletilmiş bölüm veya MBR'nin sektör 0 kod ve bölüm tablosu için kullanılır, ancak 1-62 arasındaki kesimler kullanılamaz. Kullanılmayan alan, ek önyükleme kodu ile kullanılabilir, ancak aynı zamanda önceki bir kurulumdan, sıfırlar veya gizli verilerden gelen verileri de içerebilir.
- Windows XP, bir diski bölümlendirirken kullanılmayan sektörlerdeki verileri silmez.
- Teorik olarak, genişletilmiş bölümlerin yalnızca iki girdisi olmalıdır: bir ikincil dosya sistem bölümü ve bir başka ikincil uzatılmış bölümdür.
- Çoğu partition aracı bu teoriyi takip eder, ancak elle üçüncü bir girdi oluşturmak mümkündür. Microsoft Windows XP ve Red Hat 8.0 ekstra partitionlar gösterir.
- Bir "geçersiz" yapılandırma mevcut olduğunda tüm bölümleri gösterdiklerinden emin olmak için analiz aracınızı test edin.
- Bir kullanıcı dizüstü bilgisayarın hazırda bekleme modu için olan bir bölüme bir FAT dosya sistemi koyabilir. Windows'da bu alanları mount yapamazlar, ancak Linux'ta yapabilirler.

Analiz Kuralları

- Bir partition tablosunun yapısı bozulduysa, genişletilmiş parition tablolarını aramak gerekebilir.
- Genişletilmiş bölümleri bulmak için, bir sektörün son 2 baytında **0xAA55** araması yapılabilir. Bu imza değerinin bir NTFS ve FAT dosya sisteminin ilk kesiminde aynı yerde olduğunu ve bir bölüm tablosu veya bir dosya sistemi önyükleme kesimi olup olmadığını belirlemek için sektörün geri kalanının incelenmesi gerektiğini unutmayın.
- Bir dosya sistemi bir önyükleme sektörü olarak bulunursa, bir partition tablosu ondan önce 63 sektör içerebilir.

Apple Partitionları

Giriş

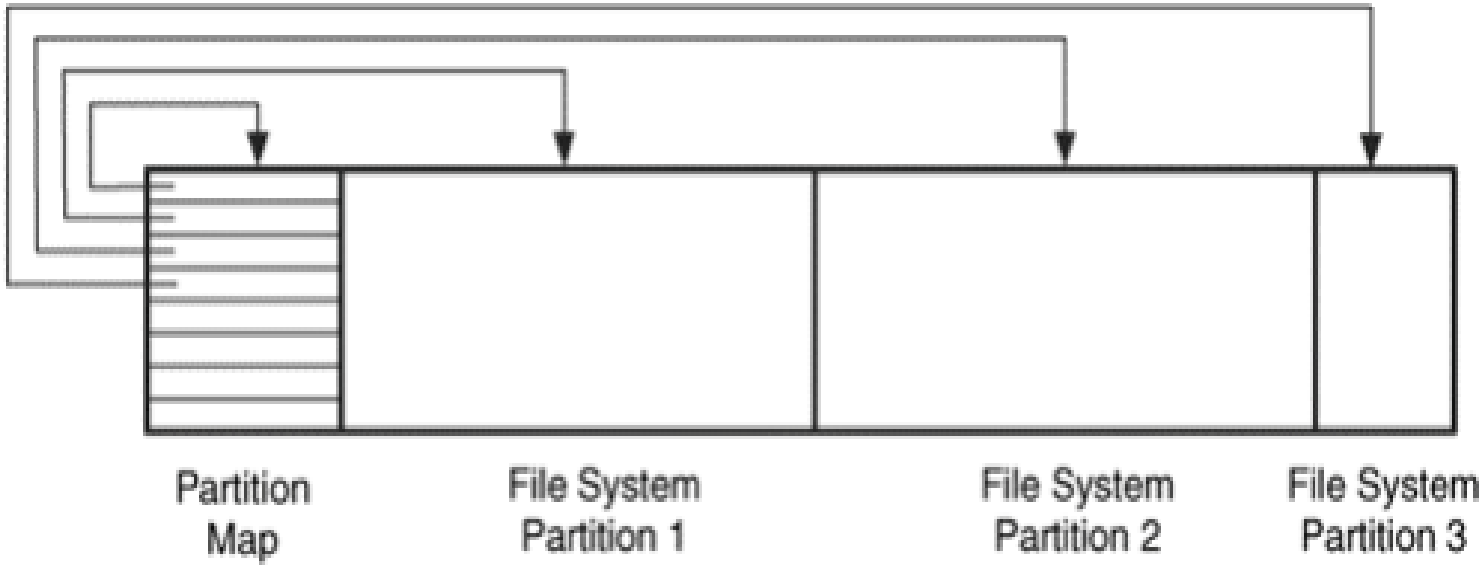
- Apple Macintosh işletim sistemini çalıştıran sistemler, Microsoft Windows'un çalışanları kadar yaygın değildir.
- Burada açıklayacağımız bölümler, OS X çalıştıran en yeni Apple dizüstü bilgisayarları ve masaüstlerinde, Macintosh 9 çalıştıran daha eski sistemlerde ve hatta MP3 ses çalabilen taşınabilir iPod cihazlarında bulunabilir.
- Partition haritası, bir Macintosh sisteminin dosyalarının disk imaj dosyasını almak içinde kullanılabilir. Disk imaj dosyası, Windows'daki bir zip dosyasına veya Unix'te bir tar dosyasına benzer. Disk imajındaki dosyalar bir dosya sisteminde saklanır ve dosya sistemi bir partitiondadır.
- Apple sistemlerdeki partition sisteminin tasarımı, DOS tabanlı partitionların karmaşıklığı ile sınırlı bölüm sayısı arasında güzel bir denge oluşturur. Apple bölümü herhangi bir sayıda bölümü tanımlayabilir ve veri yapıları diskin ardışık sektörlerindedir

Genel Bakış

- Apple partitionları, diskin başında bulunan partition harita yapısında tanımlanır. Bu yapı firmware kodu içerir, bu nedenle DOS bölüm tablosunda gördüğümüz gibi harita önyükleme kodunu içermez.
- Partition haritasındaki her kayıt, partitionun başlangıç sektörünü, boyutunu, türünü ve birim adını tanımlar. Veri yapısı ayrıca, veri alanının konumu ve herhangi bir önyükleme kodunun konumu gibi partition içindeki verilerle ilgili değerler de içerir.
- Partition haritasındaki ilk girdi genellikle kendisi için bir giriştir ve partition haritasında olabilecek en fazla boyutu gösterir.
- Apple, donanım sürücülerini depolamak için partitionlar oluşturur, bu nedenle bir Apple sistemi ana diskinde sürücüleri ve dosya olmayan diğer içeriği içeren birçok bölüm bulunur.

Partition Yapısı

Figure 5.9. An Apple disk with one partition map partition and three file system partitions.



Mac OS X bir BSD çekirdeği üzerine kurulu olmasına rağmen, bir Apple parition haritası kullanır, bir disk etiketi kullanmaz.

Veri Yapıları

- Partition kayıt türü ASCII olarak verilir ve diğer bölüm şemaları kullandığı gibi bir tamsayı kullanılmaz.
- Her bölüm için durum değerleri hem eski A/UX sistemleri hem de modern Macintosh sistemleri için geçerlidir.
- A/UX Apple'ın eski bir işletim sistemidir. Durum değeri, Tablo 5.8'de gösterilen değerlerden birine sahip olabilir

Table 5.7. Data structure for Apple partition entries.

Byte Range	Description	Essential
0–1	Signature value (0x504D)	No
2–3	Reserved	No
4–7	Total Number of partitions	Yes
8–11	Starting sector of partition	Yes
12–15	Size of partition in sectors	Yes
16–47	Name of partition in ASCII	No
48–79	Type of partition in ASCII	No
80–83	Starting sector of data area in partition	No
84–87	Size of data area in sectors	No
88–91	Status of partition (see table 5-8)	No
92–95	Starting sector of boot code	No
96–99	Size of boot code in sectors	No
100–103	Address of boot loader code	No
104–107	Reserved	No
108–111	Boot code entry point	No
112–115	Reserved	No
116–119	Boot code checksum	No
120–135	Processor type	No
136–511	Reserved	No

Table 5.8. Status value for Apple partitions.

Type	Description
0x00000001	Entry is valid (A/UX only)
0x00000002	Entry is allocated (A/UX only)
0x00000004	Entry in use (A/UX only)
0x00000008	Entry contains boot information (A/UX only)
0x00000010	Partition is readable (A/UX only)
0x00000020	Partition is writable (Macintosh & A/UX)
0x00000040	Boot code is position independent (A/UX only)
0x00000100	Partition contains chain-compatible driver (Macintosh only)
0x00000200	Partition contains a real driver (Macintosh only)
0x00000400	Partition contains a chain driver (Macintosh only)
0x40000000	Automatically mount at startup (Macintosh only)
0x80000000	The startup partition (Macintosh only)

Disk Partitionlarını Okumak

- Bir Apple diskteki bölümleri tanımlamak için, bir araç (veya kişi) ikinci sektördeki veri yapısını okur.
- Toplam partition sayısını öğrenmek için işlenir ve daha sonra diğer partition bilgileri toplanır.
- İlk girdi genellikle partition haritasının kendisidir. Sonra bir sonraki sektör okunur ve süreç tüm bölümler okunana kadar devam eder. Bölüm haritasındaki ilk girdinin içeriği aşağıdaki gibidir.

```
# dd if=mac-disk.dd bs=512 skip=1 | xxd
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  ................
[REMOVED]
```

Disk Partitionlarını Okumak

- Apple bilgisayarları 2006 yılına kadar Motorola Power PC ve 2006 yılından sonra İntel işlemcilerini kullanır ve bu nedenle motorola işlemcileri verileri big-endian intel işlemcileri little endian sıralamada saklarlar.
- Sonuç olarak, DOS bölümleriyle yaptığımız gibi sayıların sırasını tersine 2006 yılından sonra üretilen mac bilgisayarlarında çevirmemize diğerlerinde gerek kalmayacaktır.

```
# dd if=mac-disk.dd bs=512 skip=1 | xxd
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  ................
[REMOVED]
```

Disk Partitionlarını Okumak

- 0 ile 1 bayt arasında 0x504d imza değeri ve bayt 4 ile 7 arasında bölme sayısı 10 (0x0000000a) görünmektedir.
- Bayt 8-11 bize diskin ilk sektörünün bu bölüm için başlangıç sektörü olduğunu ve boyutunun 63 sektör (0x3f) olduğunu gösteriyor.
- Bölümün adı "Apple" ve bölüm "Apple_partition_map" şeklindedir.
- 88'den 91'e kadar olan baytlar, bu bölüm için hiçbir bayrak ayarlanmadığını gösterir. Bölüm haritasında kendisine ait olmayan diğer girişler statü değerlerine sahiptir.

```
# dd if=mac-disk.dd bs=512 skip=1 | xxd
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  ................
[REMOVED]
```

Örnek Çıktı

- Bu çıktıda, sonuçlar başlangıç sektörüne göre sıralanır ve ikinci sütundaki değer partition haritasındaki hangi bölüme eşlendiğini gösterir.
- Bu durumda, girişler zaten sıralanmış yapıdadır. Apple'ın şimdilik yapılandırmadığı allocated sektörleri bildirdiğini 12 girişinde görebiliyoruz.
- Bölüm haritasında hangi alan ve sektörlerin kullanıldığını göstermek için girdiler 0, 2 ve 3 mmls aracı tarafından eklenmiştir. Burada listelenen sürücüler, önyükleme yaparken sistem tarafından kullanılır.

```
# mmls -t mac mac-disk.dd
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
```

Örnek Çıktı

- pdisk aracı çıktısı yanda verilmiştir.
- Disk imaj dosyası, dosya sistemi içeren tek bir partition içerebilir veya yalnızca bir dosya sistemi içerebilir ve hiçbir bölüm içermeyebilir.
- Bir test disk imaj dosyasının düzeni (.dmg uzantılı dosyalar) aşağıdaki düzene sahiptir

```
# mmls -t mac test.dmg
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 0000000003 0000000003 Table
03: ----- 0000000004 0000000063 0000000060 Unallocated
04: 01    0000000064 0000020467 0000020404 Apple_HFS
05: 02    0000020468 0000020479 0000000012 Apple_Free
```

```
# pdisk mac-disk.dd -dump
mac-disk.dd map block size=512

   #:                type name             length   base ( size )
   1: Apple_partition_map Apple                63 @ 1
   2:       Apple_Driver43*Macintosh           54 @ 64
   3:       Apple_Driver43*Macintosh           74 @ 118
   4:     Apple_Driver_ATA*Macintosh           54 @ 192
   5:     Apple_Driver_ATA*Macintosh           74 @ 246
   6:       Apple_FWDriver Macintosh          200 @ 320
   7:   Apple_Driver_IOKit Macintosh          512 @ 520
   8:        Apple_Patches Patch Partition     512 @ 1032
   9:            Apple_HFS untitled        39068516  @ 1544 ( 18.6G)
  10:          Apple_Free                       0+@  39070060

Device block size=512, Number of Blocks=10053
DeviceType=0x0, DeviceId=0x0
Drivers-
1: @ 64 for 23, type=0x1
2: @ 118 for 36, type=0xffff
3: @ 192 for 21, type=0x701
4: @ 246 for 34, type=0xf8ff
```

Analiz Kısıtları

- Apple bölümlerinin tek karakteristik özelliği, az miktarda veriyi gizlemek için kullanılabilecek, veri yapısında kullanılmayan birkaç alan olmasıdır.
- Ayrıca veri yapısı gereği son sektör ile bölüm haritasına ayrılan alanın sonu arasındaki sektörlerde veriler gizli olabilir.
- Herhangi bir partition haritasında olduğu gibi, standart bir isime veya belirli bir türe sahip olan bölümlerde herhangi bir şey olabilir.

Çıkarılabilir Medyalar

Disket/Flash/Usb Bellek

- Çoğu çıkarılabilir ortamın partiton yapısı vardır, ancak sabit disklerin kullandığı yapıları bazıları kullanır.
- Bu kuralın istisnası, bir Windows veya UNIX sisteminde FAT12 ile biçimlendirilmiş disketlerdir. Bölüm tablolarına sahip değildirler ve tüm disklerin tamamı tek bir bölüm gibi ele alınmaktadır.
- Bir disket imajı incelenirken, bir dosya sistemi olarak doğrudan analiz edilebilir. Küçük USB depolama aygıtlarının bazıları (bazen "thumb drivers" olarak adlandırılır) partition yapısı kullanmaz. Sadece bir dosya sistemi içerir, Bazılarında ise partition yapıları mevcuttur.
- Çoğu flash belleğin bir FAT dosya sistemi vardır ve normal inceleme araçları kullanılarak analiz edilebilir.

Flash Bellek İçeriği

```
# mmls -t dos camera.dd
DOS Partition Table
Units are in 512-byte sectors
     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000031   0000000031   Unallocated
02:  00:00   0000000032   0000251647   0000251616   DOS FAT16 (0x06)
```

CD / DVD Yapısı

- CD-ROM'lar daha karmaşıktır çünkü birçok olası türü mevcuttur.
- Çoğu CD ISO 9660 (CDFS) formatını kullanır, böylece birden fazla işletim sistemi CD içeriğini okuyabilir. ISO 9660 isimlendirme gereksinimleri sıkıdır ve Joliet ve Rock Ridge gibi daha esnek ISO 9660 uzantıları vardır.
- CD'leri açıklamak çok karmaşıktır, çünkü bir CD'de temel ISO 9660 formatında ve Joliet formatında veriler olabilir. CD bir Apple hibrid diskse, veriler aynı zamanda bir Apple HFS + formatında olabilir. Dosyaların gerçek içeriği yalnızca bir kez kaydedilir, ancak veriler çeşitli yerlere yönlendirilir.

CD/DVD - RW

- Kaydedilebilir CD, DVD 'ler veya CD, DVD R'ler, bir oturum kavramına sahiptir.
- Bir CD-R üzerinde bir veya daha fazla oturum olabilir ve oturumların amacı, CD-R'ye birden fazla kez veri eklemeye devam edebilmenizdir.
- Veriler CD-R'ye her yazılışında yeni bir oturum açılır. CD'nin kullanıldığı işletim sistemine bağlı olarak, her oturum bir bölüm gibi görünüyor olabilir.
- Örneğin, üç oturumla bir CD oluşturmak için bir Apple OS X uygulaması kullanalım. CD bir OS X sisteminde kullanıldığında, oturumların üçü de dosya sistemleri olarak mount edilir.
- CD bir Linux sisteminde kullanıldığında, son oturum mount için varsayılan oturumdur fakat diğer ikisi mount komutları kullanılarak mount edilebilir.
- CD'de oturum sayısını belirlemek çeşitli araçlar kullanılabilir. (readcd gibi)

Boot Edilebilir CD/DVD

- Birçok Boot edilebilir CD'nin de yerel bir partition sistemi vardır. Sparc Solaris bootable CD'lerinde ISO içeriğinde Volüm Tablosu yapısı bulunur
- Intel bootable CD'leri, CD'nin başında bir DOS tabanlı partition tablosuna sahip olabilir.
- Bu yapılar, işletim sisteminin CD'den önyüklenmesinden sonra ve sistemi önyüklemek için gereken kod ISO biçiminde olduğunda kullanılır.