The MBR (master boot record) and the Partition Tables.

Summary:
This article describes the layout of the MBR. Partition tables are explained, and a byte-by-byte description is given of the partition table layout. Examples are used to explain a disk's partition layout. Several damage types and how they are repaired using **DiskPatch** are also explained.

The Master Boot Record ***(MBR)***:

In the IBM PC architecture the Master Boot Record (MBR), or partition sector, is the 512-byte (½ kilobyte) boot sector, i.e. the sector on the physical beginning of a hard disk that contains the sequence of commands necessary for booting the operating system(s) (OSes).

The bootstrapping firmware contained within the ROM BIOS loads and executes the master boot record. The MBR of a drive usually includes the drive's partition table, which the PC uses to load and run the boot record of the partition that is marked with the active flag. This design allows the BIOS to load any OS without knowing exactly where to start inside its partition. Because the MBR is read almost immediately when the computer is starts, many computer viruses made in the era before virus scanner software became widespread by changing the code within the MBR.

The Partition Table:

In computer engineering, hard disk drive partitioning is the creation of logical divisions on a hard disk that allows one to apply operating system-specific logical formatting.

The partition table is located in the master boot record on the disk. The master boot record is the first sector on a disk. The partition table consists of 64 bytes. There are 4 partition table entries. Each is 16 bytes in length.

The partition table starts at offset (Hexadecimal) 0x1BE. Each partition table entry is 16 bytes in length so:

```
Master Boot Record / Extended Partition Boot Record
(offset)
0x0000 to 0x01BD - First 446 bytes (boot loader code)
0x01BE to 0x01CD - Partition entry 1
0x01CE to 0x01DD - Partition entry 2
0x01DE to 0x01ED - Partition entry 3
0x01EE to 0x01FD - Partition entry 4
0x01FE to 0x01FF - Boot signature (55 AA)
```

Each partition table entry has the following arrangement:

Byte Count	Description of contents
1	Boot indicator (0x00 off, 0x80 on)
3	Starting head, cylinder and sector
1	File system descriptor
3	Ending head, cylinder and sector
4	Starting sector (offset to disk start
4	Number of sectors in partition

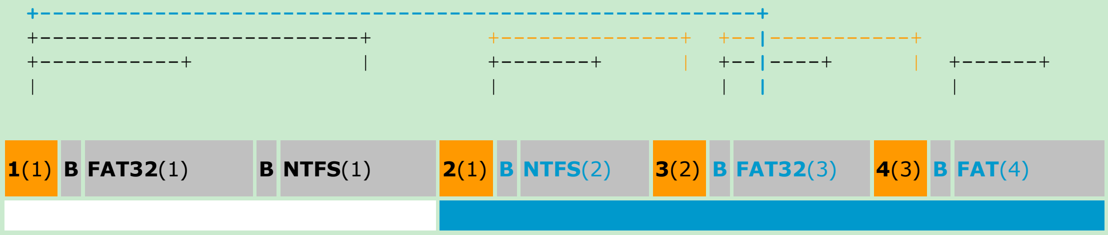
Sample partition table entry... (please also keep in mind that all bytes are in little endian):

```
offset: value                      explanation
======: =====                      ===========
0x01BE: 0x80                       bootable flag (0x00 for flag off,
0x80 for on)
0x01BF: 0x00 0x02 0x00             starting head, cylinder and sector
0x01C2: 0x07                       file system descriptor
0x01C3: 0x1A 0x5B 0x8C             ending head, cylinder and sector
0x01C6: 0x02 0x00 0x00 0x00        starting sector (relative to start of
disk)
0x01CA: 0x00 0x35 0x0C 0x00        number of sectors in partition
```

Active partition: The Bootable Flag determines the active partition. Only one partition can normally be active at a time. The active marker is used during boot: after the BIOS loads the MBR into memory and executes it, the MBR checks the partition table at its end, and locates the active partition. Then it proceeds to load the boot sector of that partition into memory and runs it.

Logical partitions: Logical partitions are a way to extend the Master Boot Record's limitation of four partitions. One partition can be designated as an extended partition. This can contain up to 24 logical partitions, whose details are listed in the extended partition's own partition table, the Extended Partition Boot Record or EPBR. Modern operating systems treat these the same as primary partitions.

Example disk partition layout:



Legend:
🟧 = Partition Table sector (the MBR or EPBR)
🟦 = the extended region that contains the logical partitions
B = Partition Boot Sector

The values that are between parenthesis point to the partition table sector (🟧) in which the partition table structures for that partition can be found.

Partition Table Sector **1** describes the:
FAT32 partition *(primary)*
NTFS partition *(primary)*
Extended partition *(primary)* ->---
|
|

The first sector of the extended partition **2** contains a *Partition Table Sector*. It defines: <---
NTFS partition *(logical)* + a pointer to **3** ->----
|
|

Partition Table Sector **3** describes: <---------------
FAT32 partition *(logical)* + a pointer to **4** ->----
|
|

Partition Table Sector **4** describes: <---------------
FAT partition *(logical)*

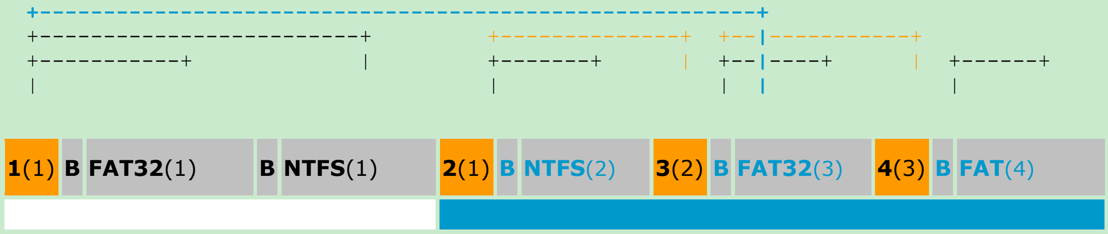
Common MBR, partition table damage/corruption patterns:

- Partition Table damage: MBR corrupt/damaged/empty
- CIH virus type damage
- Accidental partition deletion
- Partition table damage: EPBR corrupt/damaged/empty
- Partition boot sector corrupt/damaged/empty

MBR, EPBR and boot sector damages types

Partition Table damage: MBR corrupt/damaged/empty

Example disk partition layout:



Legend:
🟧 = Partition Table sector (the MBR or EPBR)
🟦 = the extended region that contains the logical partitions
B = Partition Boot Sector

The values that are between parenthesis point to the partition table sector (🟧) in which the partition table structures for that partition can be found.

Partition Table Sector **1** describes the:
FAT32 partition *(primary)*
NTFS partition *(primary)*
Extended partition *(primary)*

The first sector of the extended partition **2** contains a *Partition Table Sector*. It defines:
NTFS partition *(logical)*
+ a pointer to **3**

Partition Table Sector **3** describes:
FAT32 partition *(logical)*
+ a pointer to **4**

Partition Table Sector **4** describes:
FAT partition *(logical)*

Case: MBR damaged/corrupt/empty:

Legend:
🟥 = damaged structure / area requiring repair
⬜ = Area affected by damaged structure (data can not be accessed)
▨ = intact area (data can be accessed)

FAT32 = data inaccessible after repair
FAT32 = data accessible after repair

Description: MBR boot code and/or partition tables are corrupt/empty

Pre repair status: None of the partitions are detected by Fdisk or the operating system. None of the partitions can be accessed.

1(1)	**B**	**FAT32**(1)	**B**	**NTFS**(1)	**2**(1)	**B**	**NTFS**(2)	**3**(2)	**B**	**FAT32**(3)	**4**(3)	**B**	**FAT**(4)

Prognosis:

All data can be recovered by patching the MBR partition table (using the DiskPatch automatic partition repair). If the disk contained an operating system it is also likely that the system can be booted after the repair.

Procedure for recovering data by rebuilding the partition table:

Recovery of data by repairing corrupted disk structures with DiskPatch is an easy 4 step procedure:

- Start DiskPatch and select the physical disk; select **[Select Disk]** from the main menu and select the disk from the list that is displayed

- Scan the disk with DiskPatch. This is normally a process that takes a few minutes, less than 20 minutes for a 160 Gb SATA disk is common (if the scan process takes significantly longer this may be due to disk read errors). From the **[Perform repairs]** menu select **[Rebuild partition tables]**

- From the list of partitions select *all* partitions that you want to have present after the repair. Normally you will only see the partitions you expect to be found, however in some cases more partitions may be detected.

  For each partition additional information can be displayed, press <enter> and select **[Information]** from the menu.

  To select a partition for repair/recovery, press <enter> and select **[Select Partition]**

  When you have selected all partitions press <escape> and select **[Continue Repairs]**

- DiskPatch will now completely rebuild the partition table(s).

Verify that the recovered partitions can be accessed after the repair.

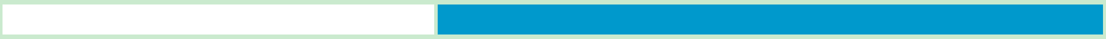
If so and when applicable, you can try to boot from the hard disk. You may need to set an active partition and/or refresh the MBR boot loader. Both tasks can be accomplished using DiskPatch.

CIH virus type damage

Example disk partition layout:

```
+--------------------------->-------------------------+
+----------->-------------+     +-------->------+  +--|----->-------+
+---->-----+              |     +--->----+      |  +--|-----+       | +--->--+
|                               |                  |  |               |
```

1(1)	**B**	**FAT32**(1)	**B**	**NTFS**(1)	**2**(1)	**B**	**NTFS**(2)	**3**(2)	**B**	**FAT32**(3)	**4**(3)	**B**	**FAT**(4)



Legend:
🟧 = Partition Table sector (the MBR or EPBR)
🟦 = the extended region that contains the logical partitions
B = Partition Boot Sector

The values that are between parenthesis point to the partition table sector (🟧) in which the partition table structures for that partition can be found.

Partition Table Sector **1** describes the:

FAT32 partition	*(primary)*
NTFS partition	*(primary)*
Extended partition	*(primary)*

The first sector of the extended partition **2** contains a *Partition Table Sector*. It defines:

NTFS partition	*(logical)*

+ a pointer to **3**

Partition Table Sector **3** describes:

FAT32 partition	*(logical)*

+ a pointer to **4**

Partition Table Sector **4** describes:

FAT partition	*(logical)*

Case: CIH virus type damage:

Legend:
🟥 = damaged structure / area requiring repair
⬜ = Area affected by damaged structure (data can not be accessed)
▨ = intact area (data can be accessed)

FAT32 = data inaccessible after repair
FAT32 = data accessible after repair

Description: The CIH virus dumps trash (random data) to the first 2048 sectors of a hard disk. MBR boot code and/or partition tables are corrupt/empty + boot sector of first primary partition is corrupt + FAT area of the primary partition is corrupt.

Pre repair status: None of the partitions are detected by Fdisk or the operating system. None of the partitions can be accessed.

Symptoms: Inability to boot from the disk ("No operating system found", "Operating system not found", "Invalid Partition Table", flashing cursor) - No partitions are detected in Fdisk or Windows Disk Management.

Pre repair:

1(1)	B	**FAT32**(1)	**B**	**NTFS**(1)	**2**(1)	**B**	**NTFS**(2)	**3**(2)	**B**	**FAT32**(3)	**4**(3)	**B**	**FAT**(4)

Post repair:

1(1)	B	**FAT32**(1)	**B**	**NTFS**(1)	**2**(1)	**B**	**NTFS**(2)	**3**(2)	**B**	**FAT32**(3)	**4**(3)	**B**	**FAT**(4)

(note that it's possible that better results may be achieved after manually performing additional repairs)

Prognosis:

In place repair of the primary partition requires expert advise. If the disk was divided into multiple partitions, all but the first can be recovered by running a DiskPatch repair.

Recovery procedure:

Recovery of data by repairing corrupted disk structures with DiskPatch is an easy 4 step procedure:

- Start DiskPatch and select the physical disk; select **[Select Disk]** from the main menu and select the disk from the list that is displayed
- Scan the disk with DiskPatch. This is normally a process that takes a few minutes, less than 20 minutes for a 160 Gb SATA disk is common (if the scan process takes significantly longer this may be due to disk read errors). From the **[Perform repairs]** menu select **[Rebuild partition tables]**
- From the list of partitions select *all* partitions that you want to have present after the repair. Normally you will only see the partitions you expect to be found, however in some cases more partitions may be detected.

  For each partition additional information can be displayed, press <enter> and select **[Information]** from the menu.

  To select a partition for repair/recovery, press <enter> and select **[Select Partition]**

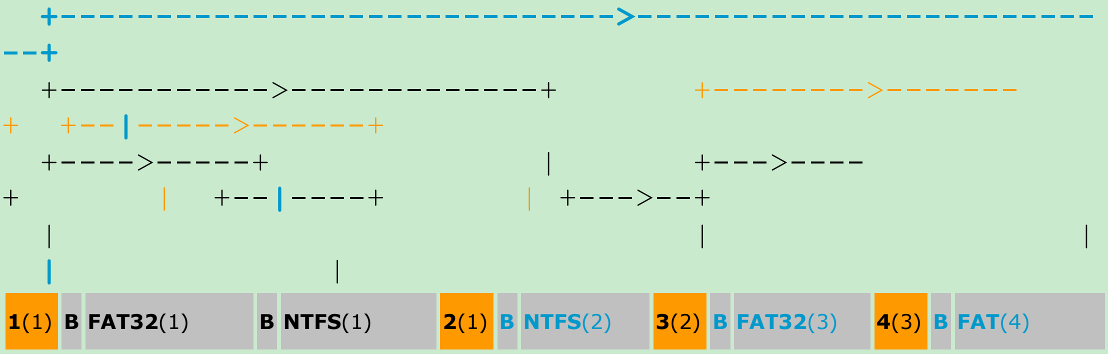
  When you have selected all partitions press <escape> and select **[Continue Repairs]**
- DiskPatch will now completely rebuild the partition table(s).

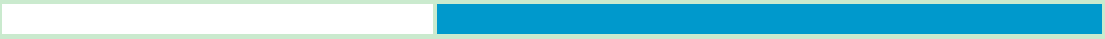
Verify that the recovered partitions can be accessed after the repair.

If so and when applicable, you can try to boot from the hard disk. You may need to set an active partition and/or refresh the MBR boot loader. Both tasks can be accomplished using DiskPatch.

Accidental partition deletion

Example disk partition layout:





Legend:
🟧 = Partition Table sector (the MBR or EPBR)
🟦 = the extended region that contains the logical partitions
B = Partition Boot Sector

The values that are between parenthesis point to the partition table sector (🟧) in which the partition table structures for that partition can be found.

Partition Table Sector **1** describes the:

FAT32 partition	*(primary)*
NTFS partition	*(primary)*
Extended partition	*(primary)*

The first sector of the extended partition **2** contains a *Partition Table Sector*. It defines:

NTFS partition	*(logical)*

+ a pointer to **3**

Partition Table Sector **3** describes:

FAT32 partition	*(logical)*

+ a pointer to **4**

Partition Table Sector **4** describes:

FAT partition	*(logical)*

Case: Accidental partition deletion:

Legend:
🟥 = damaged structure / area requiring repair
⬜ = Area affected by damaged structure (data can not be accessed)
▨ = intact area (data can be accessed)

FAT32 = data inaccessible after repair
FAT32 = data accessible after repair

Description: A partition was accidentally deleted, for example by (inappropriately) using Fdisk or the Windows Disk Administrator. The MBR and the partition table remain valid, but pointers to the partition are removed from the partition table.

Pre repair status: The deleted partition is not detected and is not assigned a drive letter.

Symptoms: The area previously occupied by the deleted partition shows up as unallocated or free space In Windows Disk Management or Fdisk.

1(1)	**B**	**FAT32**(1)	**B**	**NTFS**(1)	**2**(1)	**B**	**NTFS**(2)	**3**(2)	**B**	**FAT32**(3)	**4**(3)	**B**	**FAT**(4)

Prognosis:

All data can be recovered by adding an entry for the deleted partition to the partition table.

Procedure:

Recovery of data by repairing corrupted disk structures with DiskPatch is an easy 4 step procedure:

- Start DiskPatch and select the physical disk; select **[Select Disk]** from the main menu and select the disk from the list that is displayed

- Scan the disk with DiskPatch. This is normally a process that takes a few minutes, less than 20 minutes for a 160 Gb SATA disk is common (if the scan process takes significantly longer this may be due to disk read errors). From the **[Perform repairs]** menu select **[Rebuild partition tables]**

- From the list of partitions select *all* partitions that you want to have present after the repair. Normally you will only see the partitions you expect to be found, however in some cases more partitions may be detected.

  For each partition additional information can be displayed, press <enter> and select **[Information]** from the menu.

  To select a partition for repair/recovery, press <enter> and select **[Select Partition]**

  When you have selected all partitions press <escape> and select **[Continue Repairs]**

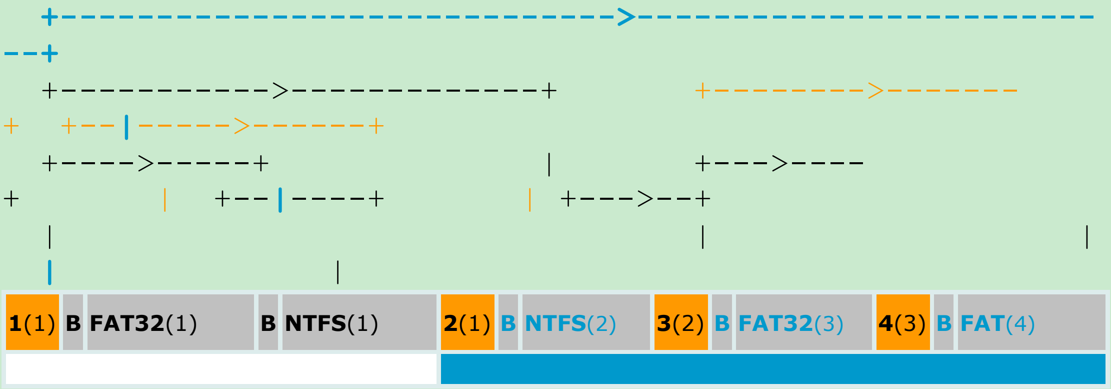
- DiskPatch will now completely rebuild the partition table(s).

Verify that the recovered partitions can be accessed after the repair.

If so and when applicable, you can try to boot from the hard disk. You may need to set an active partition and/or refresh the MBR boot loader. Both tasks can be accomplished using DiskPatch.

Partition table damage: EPBR corruption/damage/deleted

Example disk partition layout:



Legend:
🟧 = Partition Table sector (the MBR or EPBR)
🟦 = the extended region that contains the logical partitions
B = Partition Boot Sector

The values that are between parenthesis point to the partition table sector (🟧) in which the partition table structures for that partition can be found.

Partition Table Sector **1** describes the:
FAT32 partition *(primary)*

NTFS partition *(primary)*
Extended partition *(primary)*

The first sector of the extended partition **2** contains a *Partition Table Sector*. It defines:
NTFS partition *(logical)*
+ a pointer to **3**

Partition Table Sector **3** describes:
FAT32 partition *(logical)*
+ a pointer to **4**

Partition Table Sector **4** describes:
FAT partition *(logical)*

Case: EPBR damaged:

Legend:
🟥 = damaged structure / area requiring repair
⬜ = Area affected by damaged structure (data can not be accessed)
▨ = intact area (data can be accessed)

FAT32 = data inaccessible after repair
FAT32 = data accessible after repair

Description: EPBR partition tables are corrupt/empty

Pre repair status: None of the partitions described in the corrupt EPBR and following EPBRs can be accessed

1(1)	**B**	**FAT32**(1)	**B**	**NTFS**(1)	**2**(1)	**B**	**NTFS**(2)	**3**(2)	**B**	**FAT32**(3)	**4**(3)	**B**	**FAT**(4)

Prognosis:

All data can be recovered by rebuilding a valid logical partition chain using the Diskpatch automatic partition repair.

procedure:

Recovery of data by repairing corrupted disk structures with DiskPatch is an easy 4 step procedure:

- Start DiskPatch and select the physical disk; select **[Select Disk]** from the main menu and select the disk from the list that is displayed
- Scan the disk with DiskPatch. This is normally a process that takes a few minutes, less than 20 minutes for a 160 Gb SATA disk is common (if the scan process takes significantly longer this may be due to disk read errors). From the **[Perform repairs]** menu select **[Rebuild partition tables]**
- From the list of partitions select *all* partitions that you want to have present after the repair. Normally you will only see the partitions you expect to be found, however in some cases more partitions may be

detected.

For each partition additional information can be displayed, press <enter> and select **[Information]** from the menu.

To select a partition for repair/recovery, press <enter> and select **[Select Partition]**

When you have selected all partitions press <escape> and select **[Continue Repairs]**

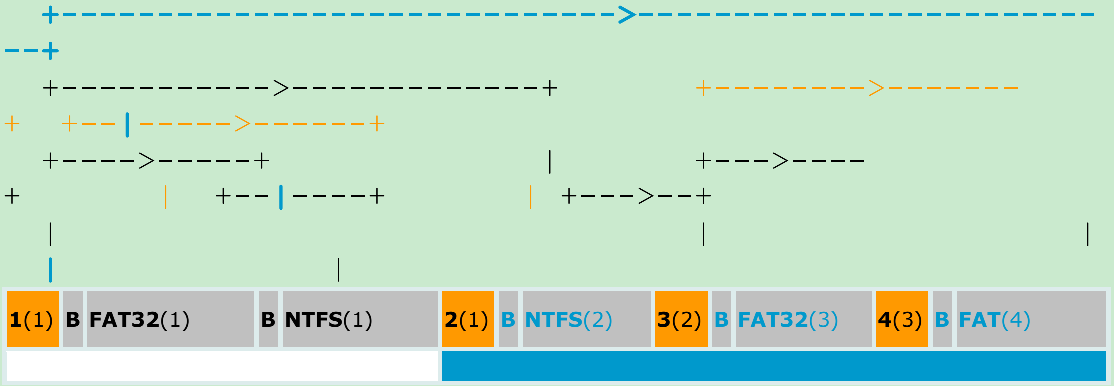
- DiskPatch will now completely rebuild the partition table(s).

Verify that the recovered partitions can be accessed after the repair.

If so and when applicable, you can try to boot from the hard disk. You may need to set an active partition and/or refresh the MBR boot loader. Both tasks can be accomplished using DiskPatch.

Partition boot sector corruption/damage/deleted

Example disk partition layout:



Legend:
🟧 = Partition Table sector (the MBR or EPBR)
🟦 = the extended region that contains the logical partitions
B = Partition Boot Sector

The values that are between parenthesis point to the partition table sector (🟧) in which the partition table structures for that partition can be found.

Partition Table Sector **1** describes the:
FAT32 partition *(primary)*
NTFS partition *(primary)*
Extended partition *(primary)*

The first sector of the extended partition **2** contains a *Partition Table Sector*. It defines:
NTFS partition *(logical)*
+ a pointer to **3**

Partition Table Sector **3** describes:
FAT32 partition *(logical)*
+ a pointer to **4**

Partition Table Sector **4** describes:
FAT partition *(logical)*

Common partition table and boot sector damage patterns:

Legend:
🟥 = damaged structure / area requiring repair
⬜ = Area affected by damaged structure (data can not be accessed)
▨ = intact area (data can be accessed)

FAT32 = data inaccessible after repair
FAT32 = data accessible after repair

Case: Partition Boot Sector damaged:

Description: Corrupt FAT32 boot sector (the boot sector contains data that is required for the OS to mount and access a partition).

Pre repair status: Primary FAT32 partition is assigned a drive letter but can not be accessed.

Symptoms: Windows displays partition as unformatted - "Do you want to format this partition?", "Sector not found" messages may be displayed, partition contents (file and folder structure) may look garbled.

1(1)	**B**	**FAT32**(1)	**B**	**NTFS**(1)	**2**(1)	**B**	**NTFS**(2)	**3**(2)	**B**	**FAT32**(3)	**4**(3)	**B**	**FAT**(4)

Prognosis:

It is likely that data can be recovered by repairing the partition boot sector (using the DiskPatch automatic partition repair).

Procedure:

Recovery of data by repairing corrupted disk structures with DiskPatch is an easy 4 step procedure:

- Start DiskPatch and select the physical disk; select **[Select Disk]** from the main menu and select the disk from the list that is displayed

- Scan the disk with DiskPatch. This is normally a process that takes a few minutes, less than 20 minutes for a 160 Gb SATA disk is common (if the scan process takes significantly longer this may be due to disk read errors). From the **[Perform repairs]** menu select **[Rebuild partition tables]**

- From the list of partitions select *all* partitions that you want to have present after the repair. Normally you will only see the partitions you expect to be found, however in some cases more partitions may be detected.

  For each partition additional information can be displayed, press <enter> and select **[Information]** from the menu.

  To select a partition for repair/recovery, press <enter> and select **[Select Partition]**

When you have selected all partitions press <escape> and select **[Continue Repairs]**

- DiskPatch will now completely rebuild the partition table(s).

Verify that the recovered partitions can be accessed after the repair.

If so and when applicable, you can try to boot from the hard disk. You may need to set an active partition and/or refresh the MBR boot loader. Both tasks can be accomplished using DiskPatch.

ATTENTION: if a backup boot sector is not present, the procedure as described above will not fix the problem. In that case the **[Rebuild boot sectors]** procedure is required. Please check the DiskPatch manual for details on how to perform this procedure.