

# File System Analysis and Comprehension

BELLEC Vincent

PetroleVB

May 22, 2013

# Contents

<b>1</b>	<b>FAT</b>	<b>2</b>
1.1	Boot Sector . . . . .	2
1.1.1	FAT12/FAT16 . . . . .	2
1.1.2	FAT32 . . . . .	4
1.2	FAT 12 . . . . .	6
1.3	FAT 16 . . . . .	6
1.4	FAT 32 . . . . .	6
<b>2</b>	<b>NTS</b>	<b>7</b>
<b>3</b>	<b>EXT</b>	<b>8</b>
3.1	EXT 2 . . . . .	8
3.2	EXT 3 . . . . .	8
3.3	EXT 4 . . . . .	8

# Chapter 1

## FAT

### 1.1 Boot Sector

Le secteur de boot est un secteur (donc de 512 octets) qui va contenir des informations essentielles sur les fat et qui fini normalement par 55 AA.

Les Nombres sont tous écrits en BIG Endian dans la mémoire, ainsi, 0x0002 par exemple doit s'inverser en 0x0200, soit 512.

#### 1.1.1 FAT12/FAT16

```
00000000 | eb 3c 90 6d 6b 64 6f 73 | 66 73 00 00 02 01 01 00 | |.<.mkdosfs.....|
00000010 | 02 e0 00 40 0b f0 09 00 | 12 00 02 00 00 00 00 00 | |...@.....|
00000020 | 00 00 00 00 00 00 29 a5 | 0e ae eb 20 20 20 20 20 | |.....)....|
00000030 | 20 20 20 20 20 20 46 41 | 54 31 32 20 20 20 0e 1f | |      FAT12  ..|
00000040 | be 5b 7c ac 22 c0 74 0b | 56 b4 0e bb 07 00 cd 10 | |.[|."t.V.....|
00000050 | 5e eb f0 32 e4 cd 16 cd | 19 eb fe 54 68 69 73 20 | |^..2.....This |
00000060 | 69 73 20 6e 6f 74 20 61 | 20 62 6f 6f 74 61 62 6c | |is not a bootabl|
00000070 | 65 20 64 69 73 6b 2e 20 | 20 50 6c 65 61 73 65 20 | |e disk. Please |
00000080 | 69 6e 73 65 72 74 20 61 | 20 62 6f 6f 74 61 62 6c | |insert a bootabl|
00000090 | 65 20 66 6c 6f 70 70 79 | 20 61 6e 64 0d 0a 70 72 | |e floppy and..pr|
000000a0 | 65 73 73 20 61 6e 79 20 | 6b 65 79 20 74 6f 20 74 | |less any key to t|
000000b0 | 72 79 20 61 67 61 69 6e | 20 2e 2e 2e 20 0d 0a 00 | |ry again ... ...|
000000c0 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |.....|
*
000001f0 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 55 aa | |.....U.|
```

16 premiers octets :

- 3 Octets : eb 3c 90 : Saut vers un programme qui va charger le système d'exploitation
- 8 Octets : mkdosfs : Nom du programme qui a formaté le disque
- 2 Octets : 00 02 : Nombre d'octets par secteur (512, 1 024, 2 048 ou 4 096).
- 1 Octet : 01 : Nombre de secteurs par cluster (1, 2, 4, 8, 16, 32, 64 ou 128).
- 2 Octets : 01 00 : Nombre de secteurs réservés en comptant le secteur de boot (32 par défaut pour FAT32, 1 par défaut pour FAT12/16).

00000000 | eb 3c 90 6d 6b 64 6f 73 | 66 73 00 00 02 01 01 00 | .<.mkdosfs.....|

16 seconds octets :

- 1 Octet : 02 : Nombre de FATs sur le disque
- 2 Octets : e0 00 : Taille du répertoire racine en nombre d'entrées.
- 2 Octets : 40 0b : Nombre total de secteurs 16-bit.
- 1 Octet : f0 : Type de disque (0xF8 pour les disques durs, 0xF0 pour les disquettes).
- 2 Octets : 09 00 : Taille d'une FAT en secteurs.
- 2 Octets : 12 00 : Nombre de secteurs par piste.
- 2 Octets : 02 00 : Nombre de têtes.
- 4 Octets : 00 00 00 00 : Secteurs cachés (0 par défaut si le disque n'est pas partitionné).

00000010 | 02 e0 00 40 0b f0 09 00 | 12 00 02 00 00 00 00 00 | ...@.....|

Spécifiques aux FAT12 - FAT16 :

- 4 Octets : 00 00 00 00 : Nombre total de secteurs 32-bit.
- 1 Octet : 00 : Identifiant du disque (à partir de 0x00 pour les disques amovibles et à partir de 0x80 pour les disques fixes).
- 1 Octet : 00 : Réserve pour usage ultérieur.
- 1 Octet : 29 : Signature (0x29 par défaut).
- 4 Octets : a5 0e ae eb : Numéro de série du disque.
- 11 Octets : 20 20 20 20 20 20 20 20 20 20 20 : Nom du disque sur 11 caractères.
- 8 Octets : 46 41 54 31 32 20 20 20 : Type de système de fichiers (FAT, FAT12, FAT16).

00000020 | 00 00 00 00 00 00 29 a5 | 0e ae eb 20 20 20 20 20 | .....). .... |  
00000030 | 20 20 20 20 20 20 46 41 | 54 31 32 20 20 20 0e 1f | FAT12 ..|

### 1.1.2 FAT32

```

00000000 | eb 58 90 6d 6b 64 6f 73 | 66 73 00 00 02 01 20 00 | .X.mkdosfs.... .|
00000010 | 02 00 00 00 00 f8 00 00 | 20 00 40 00 00 00 00 00 | ..... .@.....|
00000020 | 00 00 02 00 f1 03 00 00 | 00 00 00 00 02 00 00 00 | .....|
00000030 | 01 00 06 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | .....|
00000040 | 00 00 29 be 55 74 03 20 | 20 20 20 20 20 20 20 20 | ..).Ut.      |
00000050 | 20 20 46 41 54 33 32 20 | 20 20 0e 1f be 77 7c ac |  FAT32   ...w|.|
00000060 | 22 c0 74 0b 56 b4 0e bb | 07 00 cd 10 5e eb f0 32 | ".t.V.....^..2|
00000070 | e4 cd 16 cd 19 eb fe 54 | 68 69 73 20 69 73 20 6e | .....This is n|
00000080 | 6f 74 20 61 20 62 6f 6f | 74 61 62 6c 65 20 64 69 | ot a bootable di|
00000090 | 73 6b 2e 20 20 50 6c 65 | 61 73 65 20 69 6e 73 65 | sk. Please inse|
000000a0 | 72 74 20 61 20 62 6f 6f | 74 61 62 6c 65 20 66 6c | rt a bootable fl|
000000b0 | 6f 70 70 79 20 61 6e 64 | 0d 0a 70 72 65 73 73 20 | oppy and..press |
000000c0 | 61 6e 79 20 6b 65 79 20 | 74 6f 20 74 72 79 20 61 | any key to try a|
000000d0 | 67 61 69 6e 20 2e 2e 2e | 20 0d 0a 00 00 00 00 00 | gain ... .....|
000000e0 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | .....|
*
000001f0 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 55 aa | .....U.|

```

16 premiers octets :

- 3 Octets : eb 58 90 : Saut vers un programme qui va charger le système d'exploitation
- 8 Octets : mkdosfs : Nom du programme qui a formaté le disque
- 2 Octets : 00 02 : Nombre d'octets par secteur (512, 1 024, 2 048 ou 4 096).
- 1 Octet : 01 : Nombre de secteurs par cluster (1, 2, 4, 8, 16, 32, 64 ou 128).
- 2 Octets : 02 00 : Nombre de secteurs réservés en comptant le secteur de boot (32 par défaut pour FAT32, 1 par défaut pour FAT12/16).

```
00000000  eb 58 90 6d 6b 64 6f 73  66 73 00 00 02 01 20 00  |.X.mkdosfs.... .|
```

16 seconds octets :

- 1 Octet : 02 : Nombre de FATs sur le disque (2 par défaut)
- 2 Octets : 00 00 : Taille du répertoire racine en nombre d'entrées.
- 2 Octets : 00 00 : Nombre total de secteurs 16-bit.
- 1 Octet : f8 : Type de disque (0xF8 pour les disques durs, 0xF0 pour les disquettes).
- 2 Octets : 00 00 : Taille d'une FAT en secteurs.
- 2 Octets : 20 00 : Nombre de secteurs par piste.
- 2 Octets : 40 00 : Nombre de têtes.
- 4 Octets : 00 00 00 00 : Secteurs cachés (0 par défaut si le disque n'est pas partitionné).

```
00000010  02 00 00 00 00 00 f8 00  20 00 40 00 00 00 00 00  |..... .@.....|
```

### Spécifiques aux FAT32 :

- 4 Octets : 00 00 02 00 : Nombre total de secteurs 32-bit.
- 4 Octets : f1 03 00 00 : Taille d'une FAT en secteurs (remplace l'équivalent cité au-dessus)
- 2 Octets : 00 00 : Attributs du disque.
- 1 Octet : 00 : Version majeure du système de fichiers.
- 1 Octet : 00 : Version mineure du système de fichiers.
- 4 Octets : 02 00 00 00 : Numéro du premier cluster du répertoire racine.

00000020 | 00 00 02 00 f1 03 00 00 | 00 00 00 00 02 00 00 00 | .....|

- 2 Octets : 01 00 : Informations supplémentaires sur le système de fichiers (1 par défaut).
- 2 Octets : 06 00 : Numéro de secteur de la copie du secteur de boot.
- 12 Octets : 00 00 00 00 00 00 00 00 00 00 00 00 : Réserve pour des ajouts ultérieurs

00000030 | 01 00 06 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | .....|

- 1 Octet : 00 : Identifiant du disque  
(à partir de 0x00 pour les disques amovibles et à partir de 0x80 pour les disques fixes).
- 1 Octet : 00 : Réserve pour usage ultérieur.
- 1 Octet : 29 : Signature (0x29 par défaut).
- 4 Octets : be 55 74 03: Numéro de série du disque.
- 11 Octets : 20 20 20 20 20 20 20 20 20 20 20 : Nom du disque sur 11 caractères.
- 8 Octets : 46 41 54 33 32 20 20 20 : Type de système de fichiers (FAT32).

00000040 | 00 00 29 be 55 74 03 20 | 20 20 20 20 20 20 20 20 | ...).Ut. |  
 00000050 | 20 20 46 41 54 33 32 20 | 20 20 0e 1f be 77 7c ac | FAT32 ...w|. |

## 1.2 FAT 12

La File Allocation Table va indiquer quels sont les clusters utilisés par les fichiers, et de quel façon le fichier a été découpé s'il est plus gros qu'un cluster

Comme indiqué dans le nom, la FAT12 utilise des entrées de 12 bits. Les valeurs prises dans la FAT peuvent prendre différentes valeurs, indiquant :

0x000 : Le cluster est vide.

0x001 : Le cluster est réservé.

0x002 - 0xFEFF : Le cluster contient un fichier, continue dans le cluster indiqué par ce numéro.

0xFF0 - 0xFF6 : valeurs réservées.

0xFF7 : Mauvais cluster.

0xFF8 - 0xFFFF : Le cluster contient la fin d'un fichier.

## 1.3 FAT 16

La File Allocation Table va indiquer quels sont les clusters utilisés par les fichiers, et de quel façon le fichier a été découpé s'il est plus gros qu'un cluster

Comme indiqué dans le nom, la FAT16 utilise des entrées de 16 bits. Les valeurs prises dans la FAT peuvent prendre différentes valeurs, indiquant :

0x0000 : Le cluster est vide.

0x0001 : Le cluster est réservé.

0x0002 - 0xFFEF : Le cluster contient un fichier, continue dans le cluster indiqué par ce numéro.

0xFFF0 - 0xFFF6 : valeurs réservées.

0xFFF7 : Mauvais cluster.

0xFFF8 - 0xFFFF : Le cluster contient la fin d'un fichier.

## 1.4 FAT 32

La File Allocation Table va indiquer quels sont les clusters utilisés par les fichiers, et de quel façon le fichier a été découpé s'il est plus gros qu'un cluster

Comme indiqué dans le nom, la FAT32 utilise des entrées de 32 bits. Les valeurs prises dans la FAT peuvent prendre différentes valeurs, indiquant :

0x00000 : Le cluster est vide.

0x00001 : Le cluster est réservé.

0x00002 - 0xFFFFEF : Le cluster contient un fichier, continue dans le cluster indiqué par ce numéro.

0xFFFF0 - 0xFFFF6 : valeurs réservées.

0xFFFF7 : Mauvais cluster.

0xFFFF8 - 0xFFFFF : Le cluster contient la fin d'un fichier.



## Chapter 2

### NTS

## Chapter 3

# EXT

**3.1** EXT 2

**3.2** EXT 3

**3.3** EXT 4