Windows Forensics

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

Certifications:
http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

The Volume Boot Record

Volume Boot Record

- Used to describe the filesystem
- First 28 bytes same for all versions of FAT
- One sector for FAT12/16
- Multiple sectors (32?) for FAT32
  - Backup boot sector
  - More boot code
  - Extra information

FAT12/16/32 First Parts

Offset	Length	Item
0 (0x00)	3 (0x3)	Jump to bootstrap
3 (0x03)	8 (0x08)	OEM name (who made this filesystem?)
11(0x0B)	2 (0x02)	Bytes/sector (probably 512)
13 (0x0D)	1 (0x01)	Sectors/cluster (usually power of 2)
14 (0x0E)	2 (0x02)	Reserved sectors before filesystem (1 or 32)
16(0x10)	1 (0x01)	Copies of FAT (probably 2)

FAT12/16/32 Second Parts

Offset	Length	Item
17 (0x11)	2 (0x2)	Root directory entries (0 for FAT32)
19 (0x13)	2 (0x02)	Filesystem sectors if under 32MB (64k sectors)
21(0x15)	1 (0x01)	Media descriptor (F0=floppy, F8=everything else)
22 (0x16)	2 (0x02)	Sectors/FAT (will show 0 for FAT32)
24 (0x18)	2 (0x02)	Sectors/track
26 (0x1A)	2 (0x02)	Number of heads

FAT12/16 Third Parts

Offset	Length	Item
28 (0x1C)	4 (0x4)	Hidden sectors (preceding this partition)
32 (0x20)	4 (0x04)	Filesystem sectors if over 32MB (64k sectors)
36 (0x24)	1 (0x01)	Logical drive number (0x80, 0x81...)
38 (0x26)	24 (0x18)	Extended boot signature if 1st byte 0x29
62 (0x18)	448 (0x1C0)	Bootstrap code (16-bit assembly)
510 (0x1FE)	2 (0x02)	Signature (0x55 0xAA)

FAT12/16 Extended Signatures

Offset	Length	Item
38 (0x26)	1 (0x1)	0x29 indicates an extended signature follows
39 (0x27)	4 (0x04)	Partition serial number
43 (0x2B)	11 (0x0B)	Volume label or “NO NAME”
54 (0x36)	8 (0x08)	Human readable filesystem type

FAT32 Third Parts

Offset	Length	Item
28 (0x1C)	4 (0x4)	Hidden sectors (preceding this partition)
32 (0x20)	4 (0x04)	Filesystem sectors if over 32MB (64k sectors)
36 (0x24)	4 (0x04)	Sectors/FAT
40 (0x28)	2 (0x02)	Mirror Flag (b7=1 single FAT then b0-3 tell which)
42 (0x2A)	2	Filesystem version
44 (0x2C)	4 (0x04)	First cluster of root directory (probably 2)

FAT32 Fourth Parts

Offset	Length	Item
48 (0x30)	2 (0x2)	FSINFO sector # in reserved area (probably 1)
50 (0x32)	2 (0x02)	Backup boot sector # in reserved are (usually 6)
64 (0x40)	1 (0x01)	Logical Drive (0x80, 0x81...)
66 (0x42)	24 (0x18)	Extended boot signature (same as FAT12/16)
90 (0x5A)	420 (0x1A4)	Bootstrap code
510 (0x1FE)	2 (0x02)	Signature (0x55 0xAA)

FAT32 FSINFO Block

Offset	Length	Item
0 (0x00)	4 (0x4)	Signature RRaA
484 (0x1E4)	4 (0x04)	Start marker rrAa
488 (0x1E8)	4 (0x04)	Free clusters (0xFFFFFFFF = unknown)
492 (0x1EC)	4 (0x04)	Last allocated cluster (0xFFFFFFFF = unknown)
508 (0x1FC)	4 (0x04)	Signature (0x00 0x00 0x55 0xAA)