Inhaltsverzeichnis

NTFS Dateisystem

Boot Sektor

- Immer am Anfang der Partition (offset 0x0)

Offset	bis	Beschreibung
0x00	0x07	EB52 904E 5446 5320
0x0B	0x0C	Größe eines Blocks in Byte *Bsp: Dump: 00 02 = Hex: 02 00 Dec: 512*
0x0D		Größe eines Clusters in Blöcken
0x0E	0x0F	Reservierte Blöcke
0x15		Medien Typ: F8: HD; F0: HD Floppy
0x28	0x2F	Größe des Dateisystems in Blöcken
0x30	0x37	Clusteradresse des ersten Clusters der MFT
0x38	0x3F	Clusteradresse des ersten Clusters des MFT Mirror
0x40		Größe eines MFT-Eintrags (signed int !) in Blöcken
0x44		Größe der Index Einträge in Clustern
0x48	0x4F	Seriennummer des Volumes
0x1B8	0x1BB	Disk Signature

Master File Table (MFT)

- Ein MFT Eintrag hat eine feste Größe (typ. 1KB, Größe steht im Byte 44h im Bootsektor)
- …

Offset	bis	Beschreibung
0x00	0x03	4649 4C45 = „FILE“
0x04	0x05	Offset zur Update Sequenz
0x06	0x07	Anzahl der Einträge im fixup array
0x08	0x0F	$LogFile Sequenz Nummer (LSN) Wird bei jeder Veränderung des Eintrags verändert
0x10	0x11	Sequenz Nummer Anzahl wie oft der Eintrag benutzt wird 0, wenn Datei gelöscht ist
0x12	0x13	Anzahl der Hardlinks
0x14	0x15	Offset des ersten Attributes
0x16	0x17	0x01 ⇒ Eintrag benützt 0x02 ⇒ Eintrag ist Verzeichnis
0x18	0x1B	Belegte Größe des Eintrags
0x1C	0x1F	Reservierte Größe des Eintrags

Offset	bis	Beschreibung
0x20	0x27	Datei Referenz zum base FILE Eintrag ist 0 wenn selbst ein Basiseintrag 0x20 - 0x25: FILE Eintrag Nummer 0x26 - 0x27: Sequenz Nummer
0x28	0x29	Nächste Attribut ID
0x30	0x100	Attribute und fixup Werte

Links

http://www.reddragonfly.org/ntfs/concepts/file_record.html

Artikel Info	
Stand	Fertig