MOV Signature format

MOV Signature Format: Documentation & Recovery Example

MOV file type, a video container, is a common multimedia format often used in Apple's Quicktime for saving movies and other video files, using a proprietary compression algorithm developed by Apple Computer, compatible with both Macintosh and Windows platforms.MOV container (QuickTime Container File Type) can store different videos data formats, like MPEG-4 and OGG.

MOV files consist of consecutive chunks. Each chunk has 8 byte header: 4-byte chunk size (big-endian, high byte first) and 4-byte chunk type - one of pre-defined signatures: "ftyp", "mdat", "moov", "pnot", "udta", "uuid", "moof", "free", "skip", "jP2 ", "wide", "load", "ctab", "imap", "matt", "kmat", "clip", "crgn", "sync", "chap", "tmcd", "scpt", "ssrc", "PICT".

First chunk must be of type "ftype" and has a sub-type at offset 8. MOV defined by sub-type which must be "qt ".

To compose MOV file, iterating chunks is needed until unknown type is detected.

Let's examine the sample

When inspecting sample.mov file's binary data using any Hex Viewer, like Active@ Disk Editor we can see it starts with a signature **ftyp** (hex: 66 74 79 70) at offset 4, which defines QuickTime Container File Type.

File sub-type is **qt__** (hex: 71 74 20 20) which points to MOV file type. First block size is 32 (hex: 00 00 00 20, big-endian, high byte first), size located at offset 0.

At offset 32 (hex: 20) is located the second chunk, which has a size of 8 and type **mdat** (hex: 6D 64 61 74).

The next chunk is located at offset 32+8=40 (hex: 28) and has a size 3,263,028 (hex: 00 31 CA 34) and type **mdat** (hex: 6D 64 61 74) at offset 44 (hex: 2C).

The next chunk is located at offset 40 + 3,263,028=3,263,068 (hex: 00 31 CA 5C) and has a size 21,189 (hex: 00 00 52 C5) and type **moov** (hex: 6D 6F 6F 76) at offset 1,836,019,574 (hex: 00 31 CA 60). This is the last chunk, so total file size is 3,263,068+21,189=3,284,257 bytes.

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	ASCII
00000000	00	00	00	20	66	74	79	70	71	74	20	20	20	05	03	00	... ftypqt ...
00000010	71	74	20	20	00	00	00	00	00	00	00	00	00	00	00	00	qt ....
00000020	00	00	00	08	77	69	64	65	00	31	CA	34	6D	64	61	74	....wide.1·4mdat
00000030	00	00	01	B0	01	00	00	01	B5	89	13	00	00	01	00	00	...°....µ‰......
00000040	01	20	00	0	...	...	...	C	E1	8A	02	1E	0A	3	...	00	.. .Д€Р...¶.a'ѓ
00000050	...	32	3	69	76	78	40	A7	00	00	01	B6	...	36	...	83	.I3ivx@§...¶.a'ѓ
00000060	·х	...	6F	E3	6D	B	...	...	...	36	...	...	...	6F	·хЫогмїЌ¶ю6ышЫо
00000070	E3	6D	BF	8D	B6	FE	36	D	...	E3	6D	BF	8D	B6			гмїЌ¶ю6ышЫогмїЌ¶
00000080	FE	36	DB	F8	DB	6F	E3	6D	BF	8D	B6	FE	36	DB	F8	DB	ю6ышЫогмїЌ¶ю6ышы

Block size: 32

Block size: 8

Type: ftyp

Block size: 3,263,028

Type: mdat

Sub-type: qt