Jpg ou mp4 ?
Pourquoi pas les deux

Un autre polyglotte

SSTIC 2014

Christophe GRENIER - grenier@cgsecurity.org

Jpg ou mp4 ?

Marker JPG :

- 0xFFD8 Start Of Image
- 0xFFFE Commentaire
- ...
- 0xFFDA Start Of Scan
- 0xFFD9 End Of Image

Fichier source.jpg

```
00000000  ff d8 ff e1 28 3e 45 78  69 66 00 00 49 49 2a 00  |....(>Exif..II*.|
00000010  08 00 00 00 0c 00 0e 01  02 00 14 00 00 00 9e 00  |................|
00000020  00 00 0f 01 02 00 14 00  00 00 b2 00 00 00 10 01  |................|
00000030  02 00 09 00 00 00 c6 00  00 00 12 01 03 00 01 00  |................|
00000040  00 00 01 00 00 00 1a 01  05 00 01 00 00 00 d0 00  |................|
00000050  00 00 1b 01 05 00 01 00  00 00 d8 00 00 00 28 01  |..............(.|
00000060  03 00 01 00 00 00 02 00  00 00 31 01 02 00 14 00  |..........1.....|
00000070  00 00 e0 00 00 00 32 01  02 00 14 00 00 00 f4 00  |......2.........|
00000080  00 00 13 02 03 00 01 00  00 00 01 00 00 00 69 87  |..............i.|
00000090  04 00 01 00 00 00 08 01  00 00 25 88 04 00 01 00  |..........%.....|
000000a0  00 00 ec 03 00 00 9c 04  00 00 53 41 4d 53 55 4e  |..........SAMSUN|
000000b0  47 20 20 20 20 20 20 20  20 20 20 20 20 00 53 41  |G            .SA|
000000c0  4d 53 55 4e 47 20 20 20  20 20 20 20 20 20 20 20  |MSUNG           |
000000d0  20 00 47 54 2d 49 39 30  30 30 00 00 48 00 00 00  | .GT-I9000..H...|
```

Fichier source.mp4

```
Atom MP4 :
 type ftyp
 type moov
  type mvhd
  type iods
  type trak
  type trak
  type udta
 type mdat
```

Jpg ou mp4 = fa6 ?

- Ben non, jpg ou mp4 = jpg et mp4
- La création d'un nouveau polyglotte

Demo Time !