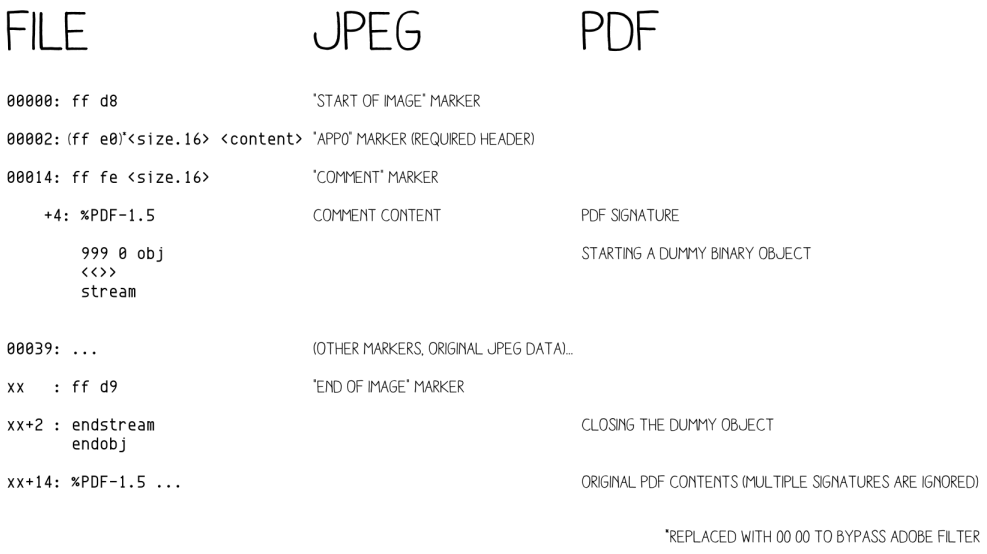
3 This PDF is a JPEG; or, This Proof of Concept is a Picture of Cats

by Ange Albertini

In this short little article, I'll teach you how to combine a PDF and a JPEG into a single polyglot file that is legal and meaningful in both languages.

The JPEG format requires its Start Of Image signature, `FF D8`, at offset `0x00`, exactly. The PDF format officially requires its `%PDF-1.x` signature to be at offset `0x00`, but in practice most interpreters only require its presence within the first 1,024 bytes of the files. Some readers, such as Sumatra, don't require the header at all.

In previous issues of this journal, you saw how a neighbor can combine a PDF document with a ZIP archive (PoC||GTFO 01:05) or a Master Boot Record (PoC||GTFO 02:08), so you should already know the conditions to make a dummy PDF object. The trick is to fit a fake `obj stream` in the first 1024 bytes containing whatever your second file demands, then to follow that `obj stream` with the contents of your real PDF.



To make these two formats play well together, we'll make our first `insert object stream` clause of the PDF contain a JPEG comment, which will usually start at offset `0x18`. Our PDF comment will cause the PDF interpreter ignore the remaining JPEG data, and the actual PDF content can continue afterward.

Unfortunately, since version 10.1.5, Adobe Reader rejects PDF files that start like a JPEG file ought to. It's not clear exactly why, but as all official segments' markers start with `FF`, this is what Adobe Reader checks to identify a JPEG file. Adobe PDF Reader will reject anything that begins with `FF D8 FF` as a JPEG.

However, a large number of JPEG files start with an APP0 segment containing a JFIF signature. This begins with an `FF E0` marker, so most JPEG viewers don't mind this in place of the expected APP0 marker. Just changing that `FF E0` marker at offset `0x02` to anything else will give will give us a supported JPEG and a PDF that our readers can enjoy with Adobe's software.

Some picky JPEG viewers, such as those from Apple, might still require the full sequence `FF D8 FF E0` to be patched manually at the top of `pocorgtfo03.pdf` to enjoy our cats, Calisson and Sarkozette.

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	ASCII
0000	ff	d8	00	00	00	10	4a	46	49	46	00	01	01	01	00	c7	......JFIF......
0010	00	c7	00	00	ff	fe	00	22	0a	25	50	44	46	2d	31	2e	.......".%PDF-1.
0020	35	0a	39	39	39	20	30	20	6f	62	6a	0a	3c	3c	3e	3e	5.999 0 obj.<<>>
0030	0a	73	74	72	65	61	6d	0a	ff	db	00	43	00	03	02	02	.stream....C....
0040	03	02	02	03	03	03	03	04	03	03	04	05	08	05	05	04	.....
0050	04	05	0a	07	07	06	08	0c	0a	0c	0c	0b	0a	0b	0b	0d	.....
0060	0e	12	10	0d	0e	11	0e	0b	0b	10	16	10	11	13	14	15	.....
0070	15	15	0c	0f	17	18	16	14	18	12	14	15	14	ff	db	00	.....
0080	43	01	03	04	04	05	04	05	09	05	05	09	14	0d	0b	0d	C.....
0090	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	.....
00a0	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	.....
00b0	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	.....
00c0	14	14	ff	c2	00	11	08	03	78	06	b3	03	01	11	00	02	........x.....
00d0	11	01	03	11	01	ff	c4	00	1c	00	00	03	01	00	03	01	.....
00e0	01	00	00	00	00	00	00	00	00	00	00	01	02	03	04	05	.....
00f0	06	07	08	ff	c4	00	1a	01	01	01	01	01	01	01	01	00	.....
0100	00	00	00	00	00	00	00	00	00	01	02	04	03	05	06	ff	.....