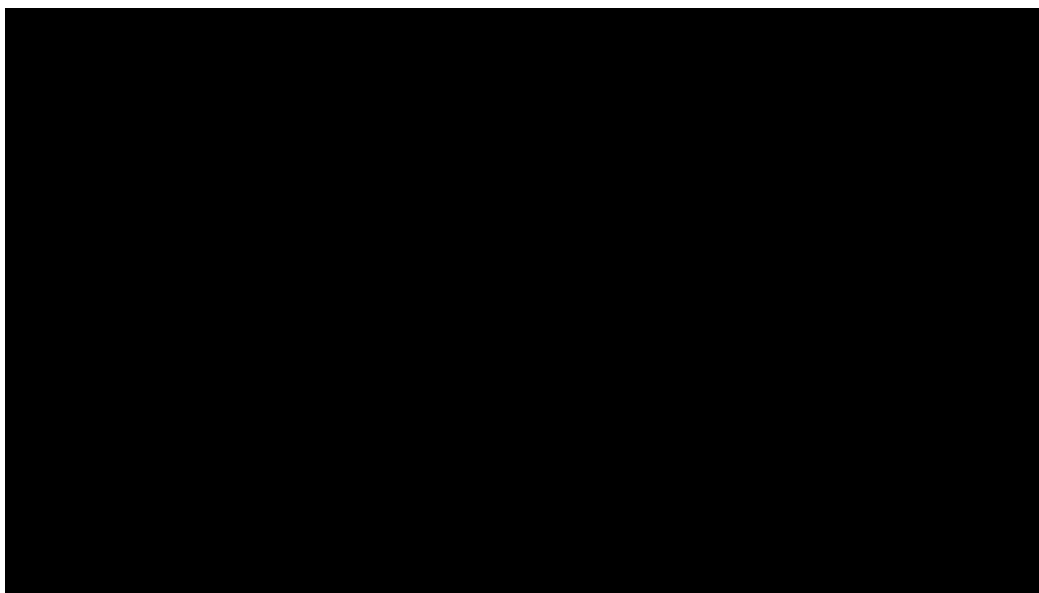


Event	Oooverflow Defcon Quals 2019
Challenge	redacted-puzzle
Writeup	l4cr0ss
Date	2019-05-12

The challenge is to extract a flag from this .gif:



The header of the .gif appears well-formed, but you can see that the global color table has three of its four colors set to black. Rewriting the GCT with some color produces a more sensible gif, numbering 35 frames in total.


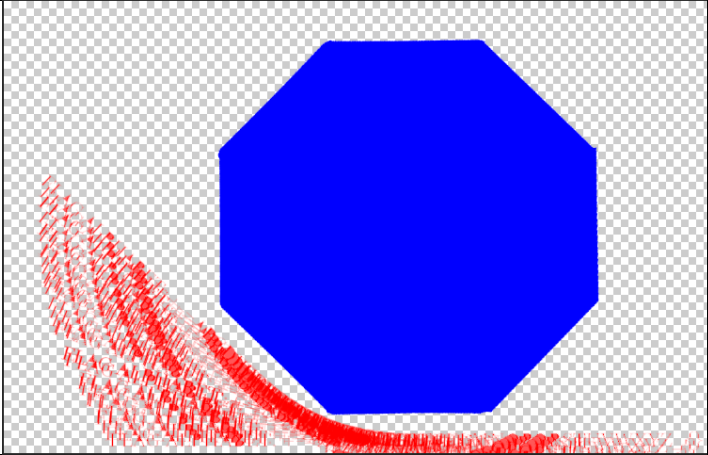
Original color table; first three colors == rgb(0,0,0)	Modified table; rgb(255,0,0), rgb(0,255,0), rgb(0,0,255)
<p>redacted-puzzle4.gif (Hex)</p> <pre> 00000000 47 49 46 38 39 61 00 05 GIF89a... 00000008 d0 02 a1 03 00 00 00 00 ..... 00000010 00 00 00 00 00 00 ff ff ..... 00000018 ff 21 ff 0b 4e 45 54 53 !..NETS 00000020 43 41 50 45 32 2e 30 03 CAPE2.0. 00000028 01 00 00 00 21 f9 04 00 ....!... 00000030 19 00 ff 00 2c 00 00 00 ....,... 00000038 00 00 05 d0 02 40 02 fe .....@.. 00000040 84 8f a9 cb ed 0f a3 9c ..... 00000048 b4 da 8b b3 de bc fb 0f ..... 00000050 86 e2 48 96 e6 89 a6 ea ..H.... 00000058 ca b6 ee 0b c7 f2 4c d7 .....L. 00000060 f6 8d e7 fa ce f7 fe 0f ..... 00000068 0c 0a 87 c4 a2 f1 88 4c .....L 00000070 2a 97 cc a6 f3 09 8d 4a *......J 00000078 a7 d4 aa f5 8a cd 6a b7 .....j. 00000080 dc ae f7 0b 0e 8b c7 e4 ..... 00000088 b2 f9 8c 4e ab d7 ec b6 ...N.... 00000090 fb 0d 8f cb e7 f4 ba fd ..... 00000098 8e cf eb f7 fc be ff 0f ..... 000000a0 18 28 38 48 58 68 78 88 .(8HXhx. 000000a8 98 a8 b8 c8 d8 e8 f8 08 ..... </pre>	<p>redacted-puzzle5.gif (Hex)</p> <pre> 00000000 47 49 46 38 39 61 00 05 GIF89a... 00000008 d0 02 a1 03 00 ff 00 00 ..... 00000010 00 ff 00 00 00 ff ff ff ..... 00000018 ff 21 ff 0b 4e 45 54 53 !..NETS 00000020 43 41 50 45 32 2e 30 03 CAPE2.0. 00000028 01 00 00 00 21 f9 04 00 ....!... 00000030 19 00 ff 00 2c 00 00 00 ....,... 00000038 00 00 05 d0 02 40 02 fe .....@.. 00000040 84 8f a9 cb ed 0f a3 9c ..... 00000048 b4 da 8b b3 de bc fb 0f ..... 00000050 86 e2 48 96 e6 89 a6 ea ..H.... 00000058 ca b6 ee 0b c7 f2 4c d7 .....L. 00000060 f6 8d e7 fa ce f7 fe 0f ..... 00000068 0c 0a 87 c4 a2 f1 88 4c .....L 00000070 2a 97 cc a6 f3 09 8d 4a *......J 00000078 a7 d4 aa f5 8a cd 6a b7 .....j. 00000080 dc ae f7 0b 0e 8b c7 e4 ..... 00000088 b2 f9 8c 4e ab d7 ec b6 ...N.... 00000090 fb 0d 8f cb e7 f4 ba fd ..... 00000098 8e cf eb f7 fc be ff 0f ..... 000000a0 18 28 38 48 58 68 78 88 .(8HXhx. 000000a8 98 a8 b8 c8 d8 e8 f8 08 ..... </pre>

Event	Oooverflow Defcon Quals 2019
Challenge	redacted-puzzle
Writeup	l4cr0ss
Date	2019-05-12

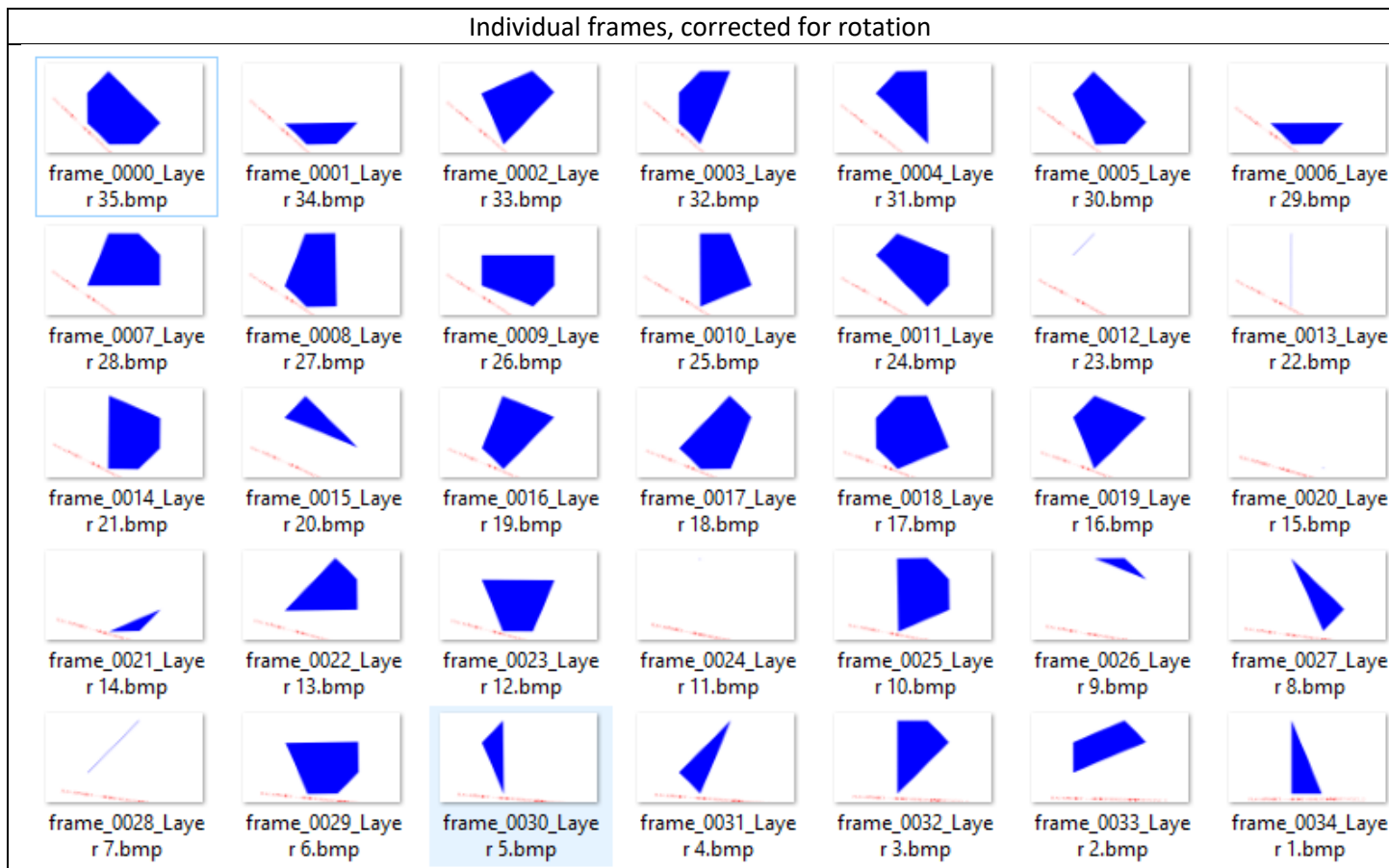
`convert -coalesce redacted-puzzle5.gif frame_%d.gif` will split the gif into frames, one per file:



We continue by making the background of each frame transparent by setting the transparent color flag and selecting the appropriate transparent color index in the graphic control extension for each embedded frame. From the resulting animation we can see that each subsequent frame is offset from the previous by an arbitrary degree of rotation. Correcting for this rotation by hand and merging the frames together reveals 8 unique vertices from which each figure is composed.

Animation with transparency enabled	Frames overlaid revealing octagon
 <p>FLAG ALPHABET: +=ABCDEFGHIJKLMNOPQRSTUVWXYZ_{} </p>	

Event	Oooverflow Defcon Quals 2019
Challenge	redacted-puzzle
Writeup	l4cr0ss
Date	2019-05-12



From here the key observation to make is that the custom flag alphabet embedded in the frames is an appropriate base32 encoding, and that treating each of the frames as representing eight bits (one for each possible vertex) gives an even number of base32-decoded characters.

Starting at the topmost vertex of the first frame and proceeding clockwise to the last frame\*, we generate a bit-string by returning 1 when the point is present and 0 when the point is absent, where present/absent means the vertex is included in the figure shown in a given frame.

This string, base32 encoded and used as an index into the flag alphabet, gives the flag.

OOO { FORCES-GOVERN+TUBE+FRUIT \_GROUP=FALLREMEMBER \_WEATHER }

\*it was known beforehand that the flag must begin with the sequence OOO{... and starting at any other point resulted in an invalid flag