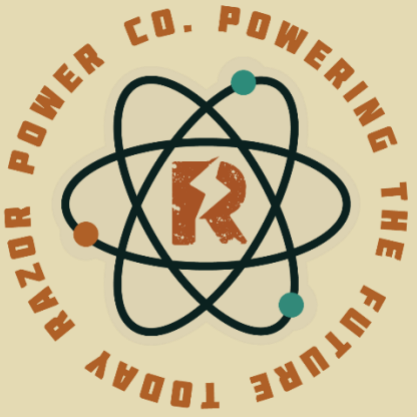
RazorHack 2024 Writeup

“Homer's Reminders 1”



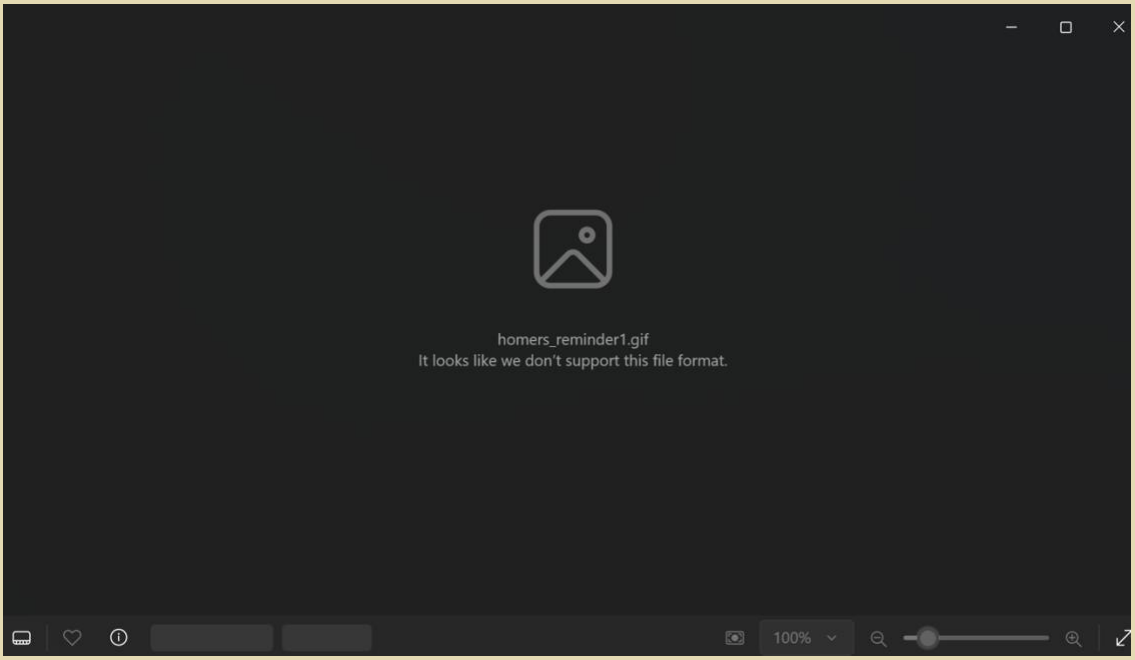
Homer, one of RazorPower's nuclear technicians, is known to be quite forgetful. So, he likes to leave himself reminders of important things in files. Can you find the reminder Homer left himself? The flag's format should be flag{insert reminder here}.

Author: Kate

In this challenge, participants will work with a file named homers_reminder1.gif, which they need to download. Attempting to open the file normally will result in an error.

Here's the error message a Mac user might see:

Here's the error message a Window's user might see:



Opening the image in a hex editor reveals some interesting details. Typically, the first few hex bytes indicate the file type, providing a signature unique to each format.

-Untitled- × homers_reminder1.gif ×

```
00000000  47 94 64 83 39 61 F4 01 77 01 F7 00 00 04 01 00  Gödâ9a⌠.w.≈.....
00000010  0C 06 07 17 0A 04 10 0B 14 1C 14 18 22 0F 03 2C  ............"..,
00000020  15 04 26 14 09 2C 19 0C 35 1B 05 34 1C 0B 39 1E  ..&..,..5..4..9.
00000030  0B 2C 1B 12 28 1B 19 32 1E 13 31 1F 19 3B 21 06  .,..(..2..1..;!.
00000040  35 21 0D 3B 22 0C 2E 20 17 34 22 13 3C 24 12 36  5!.;".. .4".<$.6
00000050  29 14 3D 29 14 34 22 1B 3B 25 19 3D 29 1A 0D 10  ).=).4".;%.=)...
00000060  30 17 19 38 26 1D 27 1C 21 3C 38 28 27 2E 28 34  0..8&.'.!<8('.(4
00000070  36 2C 34 47 2B 0D 51 2F 08 4E 30 0D 5C 33 06 53  6,4G+.Q/.N0.\3.S
00000080  32 0B 5C 35 0C 41 25 12 42 29 13 49 2E 17 44 2D  2.\5.A%.B).I..D-
00000090  1B 4D 31 19 53 33 13 5C 36 12 53 36 1D 57 38 1C  .M1.S3.\6.S6.W8.
000000A0  5B 3A 1D 61 37 0C 64 38 0B 61 36 14 63 39 13 69  [:.a7.d8.a6.c9.i
000000B0  3D 12 63 3A 19 42 2D 22 40 2D 29 4A 32 23 58 3A  =.c:.B-"@-)J2#X:
000000C0  20 44 36 39 60 3F 21 69 40 17 64 41 1D 69 42 1B   D69`?!i@.dA.iB.
000000D0  5F 40 22 63 42 22 6B 44 23 05 0F 4D 09 16 48 16  _@"cB"kD#..M..H.
000000E0  1C 46 06 18 57 21 1E 44 1A 24 49 0F 24 5A 18 27  .F..W!.D.$I.$Z.'
```

Referring to the provided hint, we see it suggests examining GIF file signatures. According to Wikipedia, a valid GIF file begins with one of these hex signatures:

47 49 46 38 37 61

47 49 46 38 39 61

en.wikipedia.org/wiki/List_of_file_signatures

hide	47 49 46 38 37 61 47 49 46 38 39 61	GIF87a GIF89a	0	gif	Image file encoded in the Graphics Interchange Format (GIF)[9]

To illustrate, let's open a working GIF file displaying a "thank you" message (thanks for reading this write-up!).

In the hex editor, we see:

```
00000000  47 49 46 38 39 61 C8 00 A6 00 F7 F0 00 0A 02 02  GIF89a╚.ª.≈≡....
00000010  0A 03 02 0B 03 02 0B 04 02 0C 05 02 0E 07 03 11  ................
00000020  0A 03 16 10 05 1A 0E 04 1B 15 08 1F 19 0B 24 20  ..............$
00000030  0E 25 0F 04 2A 1C 0C 2A 26 13 2B 14 05 30 24 11  .%..*..*&.+..0$.
00000040  30 2B 1A 32 19 07 33 2A 12 35 30 1D 36 20 0C 39  0+.2..3*.50.6 .9
00000050  26 16 39 35 1D 3B 2E 12 3C 25 0B 3C 2B 1B 3C 33  &.95.;..<%.<+.<3
00000060  22 3C 38 1E 3D 3A 1F 3E 3B 24 3F 32 16 3F 3C 20  "<8.=:.>;$?2.?<
00000070  40 2A 10 41 31 21 41 39 26 42 3D 26 42 3E 23 43  @*.A1!A9&B=&B>#C
00000080  41 26 44 40 29 45 30 15 45 38 1F 46 43 2A 47 36  A&D@)E0.E8.FC*G6
00000090  27 47 43 2D 48 46 2D 49 3B 2C 49 46 2E 49 46 33  'GC-HF-I;,IF.IF3
000000A0  4B 48 33 4B 49 32 4C 3D 2F 4C 4A 34 4C 4B 35 4D  KH3KI2L=/LJ4LK5M
000000B0  34 19 4D 3B 23 4D 4A 35 4D 4C 38 4E 42 34 4E 4B  4.M;#MJ5ML8NB4NK
000000C0  37 4F 4F 3A 50 4C 37 51 46 38 51 4D 39 51 51 3C  7OO:PL7QF8QM9QQ<
000000D0  52 40 33 52 53 3D 53 4B 3B 53 51 3D 54 3F 28 54  R@3RS=SK;SQ=T?(T
000000E0  55 42 55 38 1C 55 43 38 56 47 33 56 56 45 57 4B  UBU8.UC8VG3VVEWK
000000F0  3D 58 3D 26 58 47 3B 5B 45 32 5B 4D 41 5C 4A 3E  =X=&XG;[E2[MA\J>
```

This working GIF matches the expected signature! Now, let's look back at the original homers_reminder1.gif file. Notice that some of its hex bytes are reversed:

-Untitled- × homers_reminder1.gif ×

```
00000000  47 94 64 83 39 61 F4 01 77 01 F7 00 00 04 01 00  Gödâ9a⌠.w.
00000010  0C 06 07 17 0A 04 10 0B 14 1C 14 18 22 0F 03 2C  ..........
```

Instead of 47 49 46 38 39 61, we see 47 94 64 39 61.

By correcting these values to match a valid GIF signature, saving the file, and reopening it, we reveal the hidden message:

homers_reminder1.gif ×

```
47 49 46 38 39 61 F4 01 77 01 F7 00 00 04 01 00  GIF89a⌠.w.≈.....
0C 06 07 17 0A 04 10 0B 14 1C 14 18 22 0F 03 2C  ............",,
15 04 26 14 09 2C 19 0C 35 1B 05 34 1C 0B 39 1E  ..&..,..5..4..9.
```

flag{Reminder: Do NOT leave your badge in the donut box.}