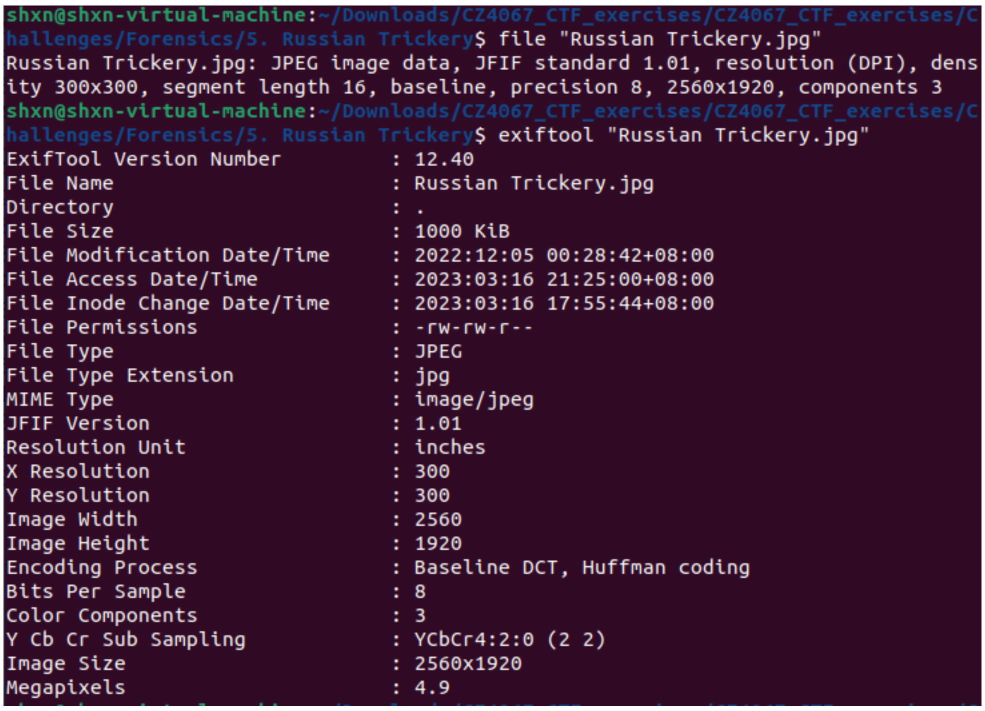
1. Regular checks to examine the contents of the JPG file and identify any irregularities. None identified

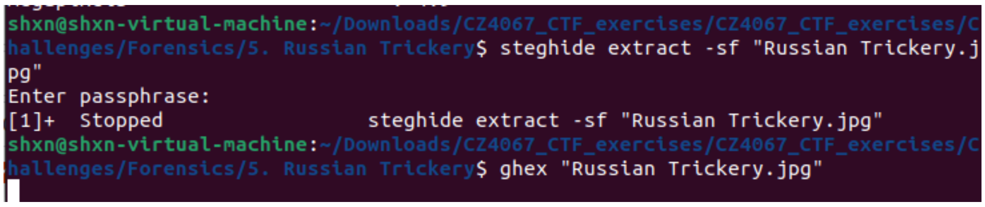


```
shxn@shxn-virtual-machine:~/Downloads/CZ4067_CTF_exercises/CZ4067_CTF_exercises/C
hallenges/Forensics/5. Russian Trickery$ file "Russian Trickery.jpg"
Russian Trickery.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), dens
ity 300x300, segment length 16, baseline, precision 8, 2560x1920, components 3
shxn@shxn-virtual-machine:~/Downloads/CZ4067_CTF_exercises/CZ4067_CTF_exercises/C
hallenges/Forensics/5. Russian Trickery$ exiftool "Russian Trickery.jpg"
ExifTool Version Number         : 12.40
File Name                       : Russian Trickery.jpg
Directory                       : .
File Size                       : 1000 KiB
File Modification Date/Time     : 2022:12:05 00:28:42+08:00
File Access Date/Time           : 2023:03:16 21:25:00+08:00
File Inode Change Date/Time     : 2023:03:16 17:55:44+08:00
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 300
Y Resolution                    : 300
Image Width                     : 2560
Image Height                    : 1920
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 2560x1920
Megapixels                      : 4.9
```

2. Next, I tried to use steghide to see if the file is actually hiding something.

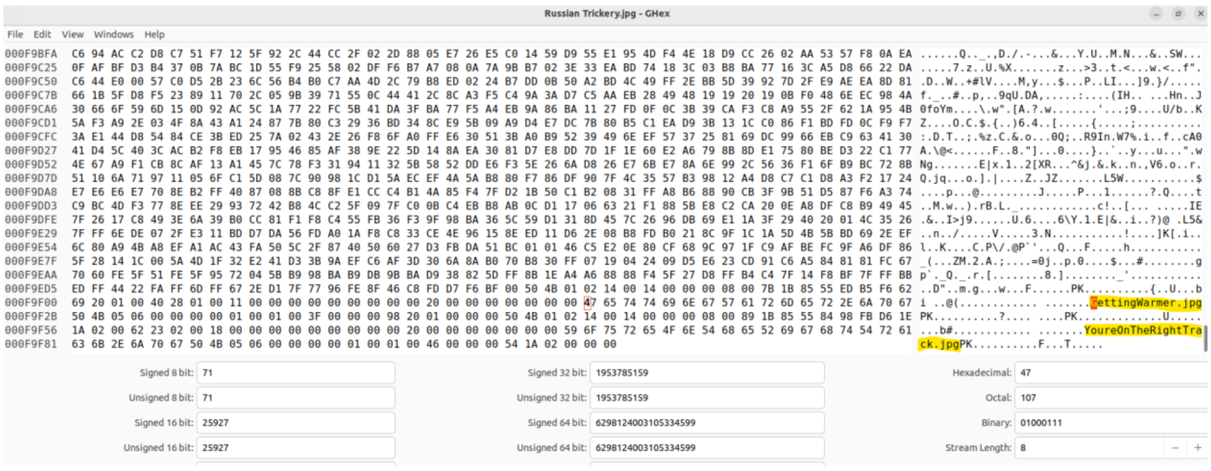
If the hidden information is encrypted, you will be prompted to enter the passphrase or password used to encrypt it.

Since we so not know the passphrase, examine the hex information of the jpg file using Ghex



```
shxn@shxn-virtual-machine:~/Downloads/CZ4067_CTF_exercises/CZ4067_CTF_exercises/C
hallenges/Forensics/5. Russian Trickery$ steghide extract -sf "Russian Trickery.j
pg"
Enter passphrase:
[1]+  Stopped                 steghide extract -sf "Russian Trickery.jpg"
shxn@shxn-virtual-machine:~/Downloads/CZ4067_CTF_exercises/CZ4067_CTF_exercises/C
hallenges/Forensics/5. Russian Trickery$ ghex "Russian Trickery.jpg"
```

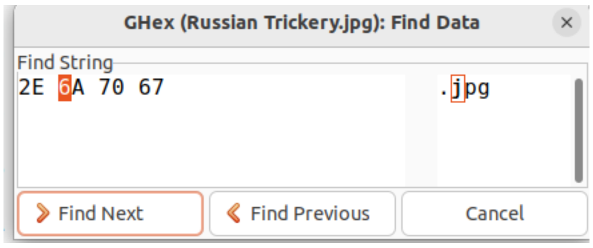
3. Upon examining the hex editor and you will find weird strings the seems to be file name such as GettingWarmer.jpg, etc.



```
000F9BFA  C6 94 AC C2 D8 C7 51 F7 12 5F 92 2C 44 CC 2F 02 2D 88 05 E7 26 E5 C0 14 59 D9 55 E1 95 4D F4 4E 18 D9 CC 26 02 AA 53 57 F8 0A EA  ......Q.._.,D./.-...&...Y.U..M.N...&..SW...
000F9C25  0F AF BF D3 B4 37 0B 7A BC 1D 55 F9 25 58 02 DF F6 B7 A7 08 0A 7A 9B B7 02 3E 33 EA BD 74 18 3C 03 B8 BA 77 16 3C A5 D8 66 22 DA  .....7.z..U.%X.......z...>3..t.<...w.<..f".
000F9C50  C6 44 E0 00 57 C0 D5 2B 23 6C 56 B4 B0 C7 AA 4D 2C 79 B8 ED 02 24 B7 DD 0B 50 A2 BD 4C 49 FF 2E BB 5D 39 92 7D 2F E9 AE EA 8D 81  .D..W..+#lV....M,y...$...P..LI...]9.}/.....
000F9C7B  66 1B 5F D8 F5 23 89 11 70 2C 05 9B 39 71 55 0C 44 41 2C 8C A3 F5 C4 9A 3A D7 C5 AA EB 28 49 48 19 19 20 19 0B F0 48 6E EC 98 4A  f._..#..p,..9qU.DA,.....:....(IH.. ...Hn..J
000F9CA6  30 66 6F 59 6D 15 0D 92 AC 5C 1A 77 22 FC 5B 41 DA 3F BA 77 F5 A4 EB 9A 86 BA 11 27 FD 0F 0C 3B 39 CA F3 C8 A9 55 2F 62 1A 95 4B  0foYm....\.w".[A.?.w.......'...;9....U/b..K
000F9CD1  5A F3 A9 2E 03 4F 8A 43 A1 24 87 7B 80 C3 29 36 BD 34 8C E9 5B 09 A9 D4 E7 DC 7B 80 B5 C1 EA D9 3B 13 1C C0 86 F1 BD FD 0C F9 F7  Z....O.C.$.{..)6.4..[.....{.....;.........
000F9CFC  3A E1 44 D8 54 84 CE 3B ED 25 7A 02 43 2E 26 F8 6F A0 FF E6 30 51 3B A0 B9 52 39 49 6E EF 57 37 25 81 69 DC 99 66 EB C9 63 41 30  :.D.T..;.%z.C.&.o...0Q;..R9In.W7%.i..f..cA0
000F9D27  41 D4 5C 40 3C AC B2 F8 EB 17 95 46 85 AF 38 9E 22 5D 14 8A EA 30 81 D7 E8 DD 7D 1F 1E 60 E2 A6 79 8B 8D E1 75 80 BE D3 22 C1 77  A.\@<......F..8."]...0....}..`..y...u...".w
000F9D52  4E 67 A9 F1 CB 8C AF 13 A1 45 7C 78 F3 31 94 11 32 5B 58 52 DD E6 F3 5E 26 6A D8 26 E7 6B E7 8A 6E 99 2C 56 36 F1 6F B9 BC 72 8B  Ng.......E|x.1..2[XR...^&j.&.k..n.,V6.o..r.
000F9D7D  51 10 6A 71 97 11 05 6F C1 5D 08 7C 90 98 1C D1 5A EC EF 4A 5A B8 80 F7 86 DF 90 7F 4C 35 57 B3 98 12 A4 D8 C7 C1 D8 A3 F2 17 24  Q.jq...o.].|....Z..JZ.......L5W...........$
000F9DA8  E7 E6 E6 E7 70 8E B2 FF 40 87 08 8B C8 8F E1 CC C4 B1 4A 85 F4 7F D2 1B 50 C1 B2 08 31 FF A8 B6 88 90 CB 3F 9B 51 D5 87 F6 A3 74  ....p...@.........J.....P...1......?.Q....t
000F9DD3  C9 BC 4D F3 77 8E EE 29 93 72 42 B8 4C C2 5F 09 7F C0 0B C4 EB B8 AB 0C D1 17 06 63 21 F1 88 5B E8 C2 CA 20 0E A8 DF C8 B9 49 45  ..M.w..).rB.L._...........c!..[... .....IE
000F9DFE  7F 26 17 C8 49 3E 6A 39 B0 CC 81 F1 F8 C4 55 FB 36 F3 9F 98 BA 36 5C 59 D1 31 8D 45 7C 26 96 DB 69 E1 1A 3F 29 40 20 01 4C 35 26  .&..I>j9......U.6....6\Y.1.E|&..i..?)@ .L5&
000F9E29  7F FF 6E DE 07 2F E3 11 BD D7 DA 56 FD A0 1A F8 C8 33 CE 4E 96 15 8E ED 11 D6 2E 08 B8 FD B0 21 8C 9F 1C 1A 5D 4B 5B BD 69 2E EF  ..n../.....V.....3.N...........!....]K[.i..
000F9E54  6C 80 A9 4B A8 EF A1 AC 43 FA 50 5C 2F 87 40 50 60 27 D3 FB DA 51 BC 01 01 46 C5 E2 0E 80 CF 68 9C 97 1F C9 AF BE FC 9F A6 DF 86  l..K....C.P\/.@P`'...Q...F.....h..........
000F9E7F  5F 28 14 1C 00 5A 4D 1F 32 E2 41 D3 3B 9A EF C6 AF 3D 30 6A 8A B0 70 B8 30 FF 07 19 04 24 09 D5 E6 23 CD 91 C6 A5 84 81 81 FC 67  _(...ZM.2.A.;....=0j..p.0....$...#........g
000F9EAA  70 60 FE 5F 51 FE 5F 95 72 04 5B B9 98 BA B9 DB 9B BA D9 38 82 5D FF 8B 1E A4 A6 88 88 F4 5F 27 D8 FF B4 C4 7F 14 F8 BF 7F FF BB  p`._Q._.r.[........8.]........_'..........
000F9ED5  ED FF 44 22 FA FF 6D FF 67 2E D1 7F 77 96 FE 8F 46 C8 FD D7 F6 BF 00 50 4B 01 02 14 00 14 00 00 00 08 00 7B 1B 85 55 ED B5 F6 62  ..D"..m.g...w...F......PK.........{..U...b
000F9F00  69 20 01 00 40 28 01 00 11 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 47 65 74 74 69 6E 67 57 61 72 6D 65 72 2E 6A 70 67  i ..@(............ .......GettingWarmer.jpg
000F9F2B  50 4B 05 06 00 00 00 00 01 00 01 00 3F 00 00 00 98 20 01 00 00 00 50 4B 01 02 14 00 14 00 00 00 08 00 89 1B 85 55 84 98 FB D6 1E  PK..........?.... ....PK.............U.....
000F9F56  1A 02 00 62 23 02 00 18 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 59 6F 75 72 65 4F 6E 54 68 65 52 69 67 68 74 54 72 61  ...b#............ .......YoureOnTheRightTra
000F9F81  63 6B 2E 6A 70 67 50 4B 05 06 00 00 00 00 01 00 01 00 46 00 00 00 54 1A 02 00 00 00                                             ck.jpgPK..........F...T.....
```

```
Signed 8 bit: 71              Signed 32 bit: 1953785159                 Hexadecimal: 47
Unsigned 8 bit: 71            Unsigned 32 bit: 1953785159               Octal: 107
Signed 16 bit: 25927          Signed 64 bit: 6298124003105334599        Binary: 01000111
Unsigned 16 bit: 25927        Unsigned 64 bit: 6298124003105334599      Stream Length: 8
```

Upon searching for .jpg in it’s hex form, we found 4 matches.


GHex (Russian Trickery.jpg): Find Data

Find String

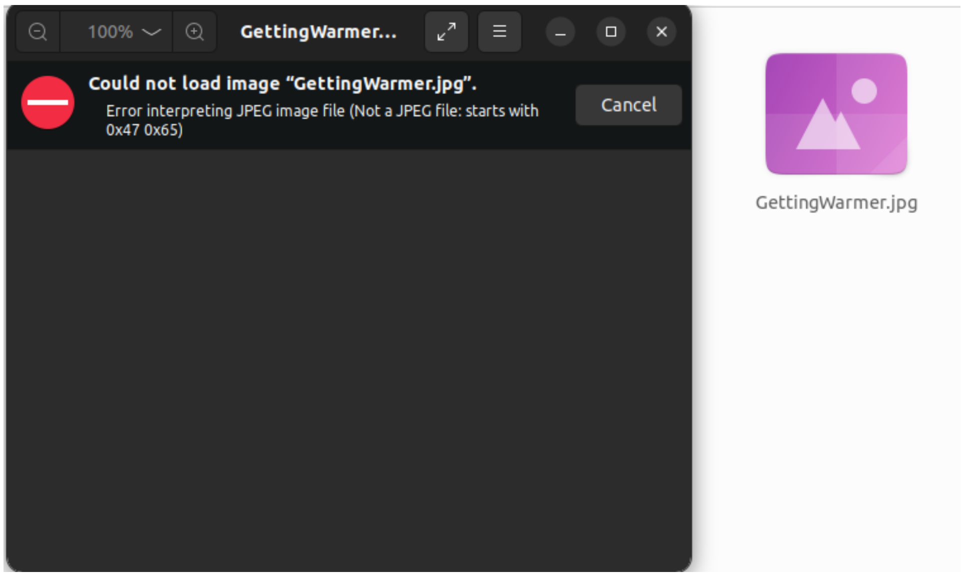
```
2E 6A 70 67        .jpg
```

4. Next I tried to extract the hidden files: Use the offset value to extract the hidden file from the image file.

You can use the dd command in Linux to extract the hidden file. For example, if the offset value is 1000 bytes, you can use the following command:

$dd if=”Russian Trickery.jpg” of=GettingWarmer.jpg bs=1 skip=(0xF9F1A).

However, when I tried to open the extracted jpgs, it seems that they are not images ($file image.jpg -> returns data)


Could not load image “GettingWarmer.jpg”.

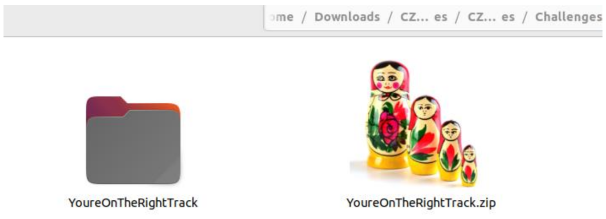
Error interpreting JPEG image file (Not a JPEG file: starts with 0x47 0x65)

5. Suspect that the “Russian Tickery.jpg” file is actually a zip file.

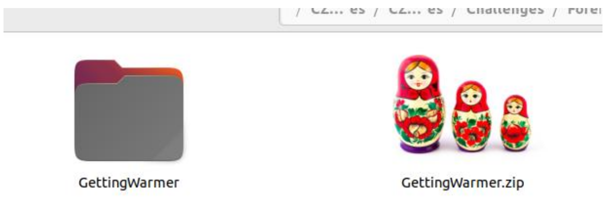
The presence of multiple JPEG (.jpg) files within the hexadecimal metadata of another file may indicate that the file is a compressed archive in the ZIP format.

This is because when multiple files are compressed together into a ZIP archive, each file is stored individually and sequentially within the archive, often with a specific file header that identifies its format. In the case of JPEG files, each file header typically begins with the hexadecimal sequence "FF D8 FF E0," which identifies it as a JPEG file.

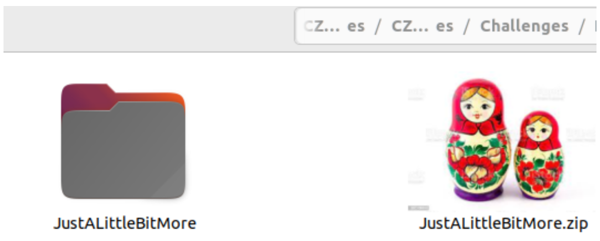
6. Repeatedly rename jpg to zip and extract contents



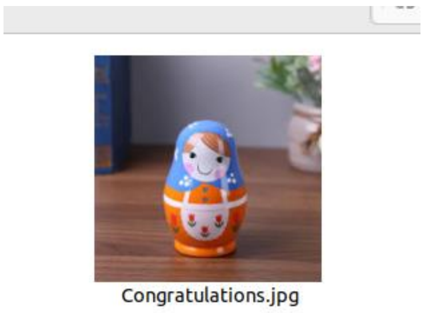
(Contents of Russian Trickery)



(Contents of YoureOnTheRightTrack)



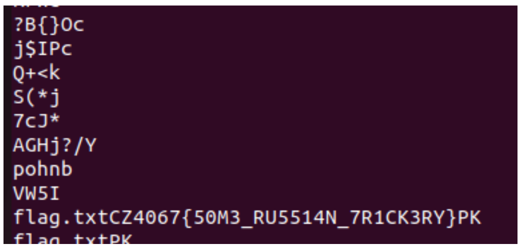
(Contents of GettingWarmer)



(Contents of JustALittleBitMore)

7. Look at the strings via $strings Congratulations.jpg

Notice the flag at the end of the string



```
?B{}Oc
j$IPc
Q+<k
S(*j
7cJ*
AGHj?/Y
pohnb
VW5I
flag.txtCZ4067{50M3_RU5514N_7R1CK3RY}PK
flag.txtPK
```