

# Interpretar imagem como texto

Como foi explicado na seção de **dados e códigos**, qualquer arquivo no computador pode ser interpretado como uma sequência binária, e dessa forma, tem sua representação em texto. Assim, esse recurso pode ser usado para esconder informação numa imagem.

Um recurso comum em CTFs é colocar um trecho de texto puro em alguma região arbitrária da imagem. Por exemplo, se queremos esconder a palavra `such cake` na imagem `doge.jpg`, podemos usar o comando Linux:

```
echo "such cake" >> doge.jpg
```

Com isso, `"such cake"` ficará no final dos dados da imagem.

## Solucionando

Para extrair a informação escondida por esse método, várias ferramentas podem ser usadas. As duas principais são os comandos de Linux `strings` e `hexdump`.

O comando `strings` imprime basicamente todas as sequências de dados *imprimíveis* de um arquivo. Por exemplo, o comando aplicado a imagem `doge.jpg`

```
strings doge.jpg
```

Com isso, o final da saída do comando será algo da forma:

```
~/D/I/I/c/g/stegano
File Edit View Search Terminal Help
kqZ&Y
30be
u,4L
Qb%7J
fcs0
/; T
4j\k
BYW,e
`Op
:CdD
Q8/P
]s0.
q8s4
      LIwq
1KoMA0
f*%Y[
a70WpAE
){cD]
u|Lv
)w)C5
3P}a(
  l?R
such cake
~/D/I/I/ctf-starter-pack > +... guides/stegano
```

Já o comando `hexdump` permite que a imagem seja analisada de forma mais minuciosa, onde o formato de leitura e impressão pode ser especificado pelo usuário. Por exemplo, um uso do comando com a imagem `doge.jpg`, onde a flag `-C` representa a forma canônica de impressão hex+ASCII:

```
hexdump -C doge.jpg
```

O final da saída desse comando é algo da forma:

```
~/D/I/I/c/g/stegano
File Edit View Search Terminal Help
0000bee0 e2 64 ac f2 e6 55 b5 03 ec 96 06 8f 54 10 29 e0 |.d...U.....T.)|
0000bef0 41 08 69 b2 56 2a 3d ac a0 a1 a8 51 7e 93 72 ac |A.i.V*=....Q~.r.|
0000bf00 a5 43 55 1a b5 4f 05 42 d8 06 9a 04 60 6a 8e c6 |.CU..O.B....`j..|
0000bf10 60 13 18 ad 51 1e 01 27 bb 80 18 df 36 43 27 03 |`...Q..'....6C'.|
0000bf20 a2 70 ec f5 09 c9 84 06 01 25 5e 0f 22 e0 06 29 |.p.....%^."..)|
0000bf30 ee 0d b0 20 fb 4a 01 fb 80 85 97 0f a0 fb 8f a3 |... .J.....|
0000bf40 48 f0 46 ad af c9 1a 05 5e 61 57 8e 25 78 96 0a |H.F.....^aW.%x..|
0000bf50 08 75 7c 4c 76 b8 b0 21 de e2 d0 18 b9 5e 77 00 |.u|Lv..!.....^w.|
0000bf60 c9 2c b2 c2 ec 8b 96 a0 2b 12 ae 25 b0 29 77 29 |.,.....+..%.)w|
0000bf70 43 35 05 d0 35 b6 58 de ce 25 37 51 0e 31 9c c7 |C5..5.X..%7Q.1..|
0000bf80 50 d3 d3 36 fa 84 36 9a ce 5f 8d 23 b7 d4 d2 72 |P..6..6.._#...r|
0000bf90 8e a6 c7 b8 6f e0 6d 18 4d 0f ff 00 80 eb e1 4f |...o.m.M.....0|
0000bfa0 f2 2c 1f 36 b3 97 c1 46 b0 46 48 70 06 26 ad e6 |.,.6...F.FHp.&..|
0000bfb0 e6 37 50 d8 65 fd 9a 3e a6 a8 6d f1 a4 01 42 f5 |.7P.e...>..m...B.|
0000bfc0 09 c3 e1 23 b2 e6 90 dd f0 33 b3 33 50 7d 61 28 |...#.....3.3P}a(|
0000bfd0 1f 49 a7 d4 30 b3 71 ab b5 9f e5 30 5e d1 ad b6 |.I..0.q....0^...|
0000bfe0 ef 77 10 28 a3 d8 c2 ff 00 07 73 2b a5 cd 37 d4 |.w.(.....s+.7.|
0000bff0 21 a0 3e a1 38 10 ad 82 20 6c 3f 52 ff 00 fc a0 |!.>.8... l?R....|
0000c000 d9 0f c8 4c 94 51 f0 07 18 42 c0 5f 71 25 0d 7a |...L.Q...B._q%.z|
0000c010 99 15 eb e0 6d f8 3f f2 3b 8c 75 f5 f1 7f cc 78 |...m.?.;.u....x|
0000c020 9c 7c 68 fb 9c a7 2f 8e 8f ff 00 c0 2e 75 18 ff |.|h.../.....u..|
0000c030 d9 73 75 63 68 20 63 61 6b 65 0a |.such cake.|
0000c03b
~/D/I/I/ctf-starter-pack > guides/stegano
```

# Exercícios

WeChall: Stegano I

picoCTF-2018: hex-editor

# Referências

HowtoForge

Sanfoudry

Revision #2

Created Sat, Oct 6, 2018 7:06 PM by Andrew

Updated Sat, Oct 6, 2018 7:10 PM by Andrew