

RED

kami mendapat sebuah file gambar lagi dengan format png, kami melakukan forensic dengan menggunakan exiftool dan zsteg untuk mengetahui bagaimana file disembunyikan (<https://cybersectools.com/tools/zsteg>)

zsteg adalah alat baris perintah yang dirancang untuk mendeteksi dan mengekstrak data tersembunyi dalam berkas gambar PNG dan BMP menggunakan teknik steganografi.

Alat ini khusus dalam mengidentifikasi data yang disembunyikan melalui steganografi Least Significant Bit (LSB), aliran yang dikompresi zlib, dan metode yang digunakan oleh alat seperti OpenStego dan Camouflage 1.2.1.

```
cyberjunkie@shadow:~/ctf/pico$ exiftool red.png
ExifTool Version Number      : 12.76
File Name                    : red.png
Directory                    : .
File Size                    : 796 bytes
File Modification Date/Time  : 2026:01:15 00:00:28+07:00
File Access Date/Time       : 2026:01:15 00:02:19+07:00
File Inode Change Date/Time  : 2026:01:15 00:00:34+07:00
File Permissions             : -rw-rw-r--
File Type                    : PNG
File Type Extension          : png
MIME Type                    : image/png
Image Width                  : 128
Image Height                 : 128
Bit Depth                    : 8
Color Type                   : RGB with Alpha
Compression                  : Deflate/Inflate
Filter                       : Adaptive
Interlace                    : Noninterlaced
Poem                         : Crimson heart, vibrant and bold,.Hearts flutter at your si
ght..Evenings glow softly red,.Cherries burst with sweet life..Kisses linger with your warmth..Love deep as merlot..Scarlet leaves falling softly,.Bold in every stroke.
Image Size                   : 128x128
Megapixels                   : 0.016
```

poetry

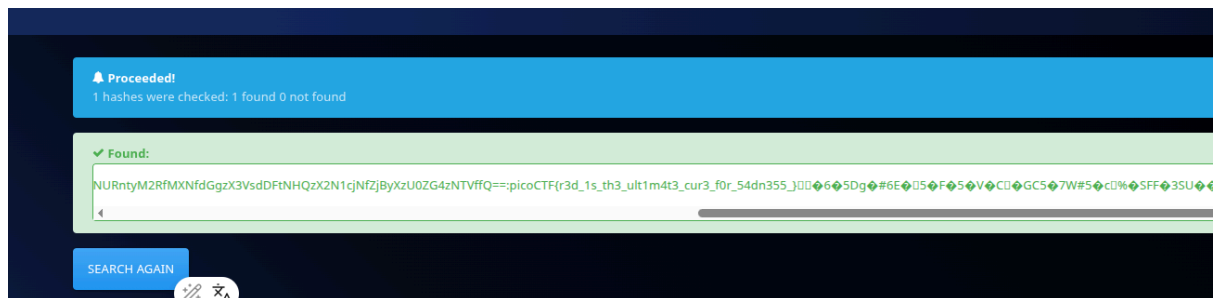
Crimson heart, vibrant and bold,.Hearts flutter at your sight..Evenings glow softly red,.Cherries burst with sweet life..Kisses linger with your warmth..Love deep as merlot..Scarlet leaves falling softly,.Bold in every stroke.

CHECK LSB

-> using zsteg

```
cyberjunkie@shadow:~/ctf/pico$ zsteg red.png
meta Poem      .. text: "Crimson heart, vibrant and bold,\nHearts flutter at your sight
.\nEvenings glow softly red,\nCherries burst with sweet life.\nKisses linger with your warmth
h.\nlove deep as merlot.\nScarlet leaves falling softly,\nBold in every stroke."
b1,rgba,lsb,xy .. text: "cGljb0NURntyM2RfMXNfdGgzX3VsdDFtNHQzX2N1cjNfZjByXzU0ZG4zNTVffQ
==cGljb0NURntyM2RfMXNfdGgzX3VsdDFtNHQzX2N1cjNfZjByXzU0ZG4zNTVffQ==cGljb0NURntyM2RfMXNfdGgzX3
VsdDFtNHQzX2N1cjNfZjByXzU0ZG4zNTVffQ==cGljb0NURntyM2RfMXNfdGgzX3VsdDFtNHQzX2N1cjNfZjByXzU0ZG
4zNTVffQ=="
b1,rgba,msb,xy .. file: OpenPGP Public Key
b2,g,lsb,xy     .. text: "ET@UETPETUUT@TUUTD@PDUDDDDPE"
b2,rgb,lsb,xy   .. file: OpenPGP Secret Key
b2,bgr,msb,xy   .. file: OpenPGP Public Key
b2,rgba,lsb,xy  .. file: OpenPGP Secret Key
b2,rgba,msb,xy  .. text: "CIkiiiI"
b2,abgr,lsb,xy  .. file: OpenPGP Secret Key
b2,abgr,msb,xy  .. text: "iiaakikk"
b3,rgba,msb,xy  .. text: "#wb#wp#7p"
b3,abgr,msb,xy  .. text: "7r'wb#7p"
b4,b,lsb,xy     .. file: 0421 Alliant compact executable not stripped
```

cGljb0NURntyM2RfMXNfdGgzX3VsdDFtNHQzX2N1cjNfZjByXzU0ZG4zNTVffQ==cGljb0NURntyM2RfMXNfdGgzX3VsdDFtNHQzX2N1cjNfZjByXzU0ZG4zNTVffQ==cGljb0NURntyM2RfMXNfdGgzX3VsdDFtNHQzX2N1cjNfZjByXzU0ZG4zNTVffQ==cGljb0NURntyM2RfMXNfdGgzX3VsdDFtNHQzX2N1cjNfZjByXzU0ZG4zNTVffQ==



picoCTF{r3d_1s_th3_ult1m4t3_cur3_f0r_54dn355_}