

# CSC-BZU

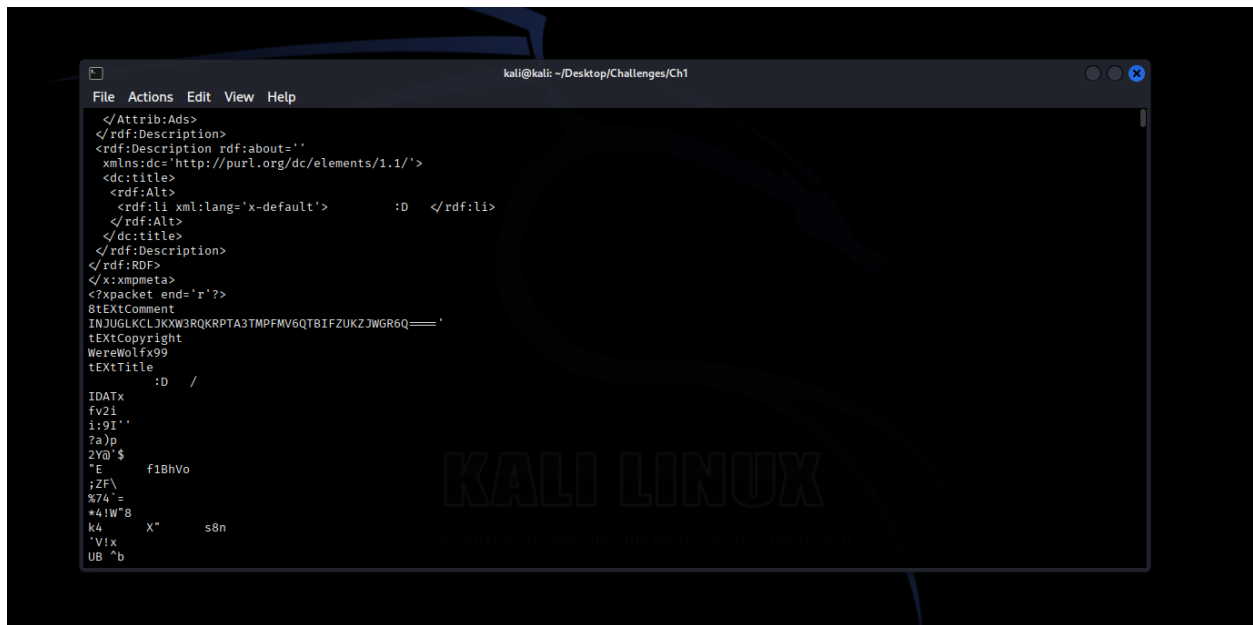
## Digital Forensics Writeup

### Challenge 1 :

( kid.png )

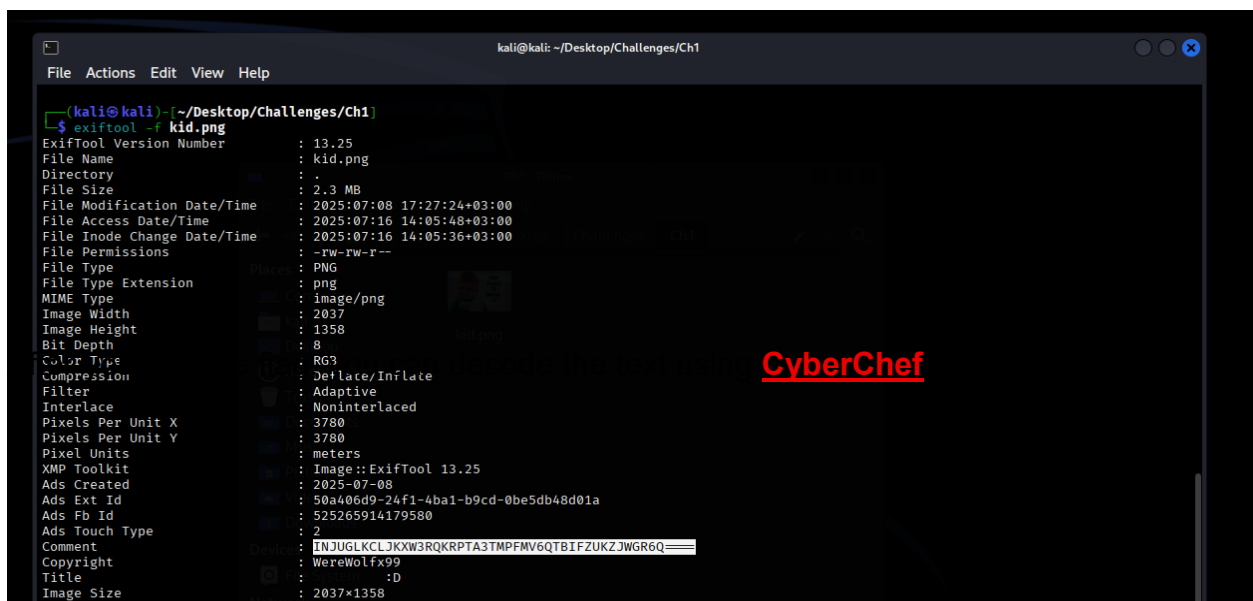
You can extract the metadata from a picture using:

1) using strings tool:



```
kali@kali: ~/Desktop/Challenges/Ch1
File Actions Edit View Help
</Attrib:Ads>
</rdf:Description>
<rdf:Description rdf:about=""
xmlns:dc="http://purl.org/dc/elements/1.1/">
<dc:title>
<rdf:Alt>
<rdf:li xml:lang="x-default"> :D </rdf:li>
</rdf:Alt>
</dc:title>
</rdf:Description>
</rdf:RDF>
</x:xmpmeta>
<?xpacket end="r"?'>
StEXtComment
INJUGLKCLJXKW3RQKRPTA3TMPFMV6QTBIFZUKZJWGR6Q====
tEXtCopyright
WereWolfx99
tEXtTitle
:D /
IDATx
fv2i
i:9I''
?a)p
2Y@ $
'E f1BhVo
iZF\
#74's
*4!W"8
k4 X" s8n
'Vix
UB ^b
```

2) using exiftool:



```
kali@kali: ~/Desktop/Challenges/Ch1
File Actions Edit View Help
(kali@kali)~/Desktop/Challenges/Ch1
$ exiftool -f kid.png
ExifTool Version Number : 13.25
File Name : kid.png
Directory : .
File Size : 2.3 MB
File Modification Date/Time : 2025:07:08 17:27:24+03:00
File Access Date/Time : 2025:07:16 14:05:48+03:00
File Inode Change Date/Time : 2025:07:16 14:05:36+03:00
File Permissions : -rw-rw-r--
File Type : PNG
File Type Extension : png
MIME Type : image/png
Image Width : 2037
Image Height : 1358
Bit Depth : 8
Color Type : RGB
Compression : Deflate/Inflate
Filter : Adaptive
Interlace : Noninterlaced
Pixels Per Unit X : 3780
Pixels Per Unit Y : 3780
Pixel Units : meters
XMP Toolkit : Image::ExifTool 13.25
Ads Created : 2025-07-08
Ads Ext Id : 50a406d9-24f1-4ba1-b9cd-0be5db48d01a
Ads Fb Id : 525265914179580
Ads Touch Type : 2
Comment : INJUGLKCLJXKW3RQKRPTA3TMPFMV6QTBIFZUKZJWGR6Q====
Copyright : WereWolfx99
Title : :D
Image Size : 2037x1358
```

Input

INJUGLKCLJKXW3RQKRPTA3TMPFMV6QTBIFZUKZJWGR6Q====

From Base32 will produce  
"CSC-  
BZU{n0T\_0nlyY\_BaAsEe64}"

REC 48 1 "

Output

INJUGLKCLJKXW3RQKRPTA3TMPFMV6QTBIFZUKZJWGR6Q====

Recipe

From Base32  
Alphabet  
A-Z2-7=  
☐ Remove non-alphabet chars

Input

INJUGLKCLJKXW3RQKRPTA3TMPFMV6QTBIFZUKZJWGR6Q====

REC 48 1

Output

CSC-BZU{n0T\_0nlyY\_BaAsEe64}

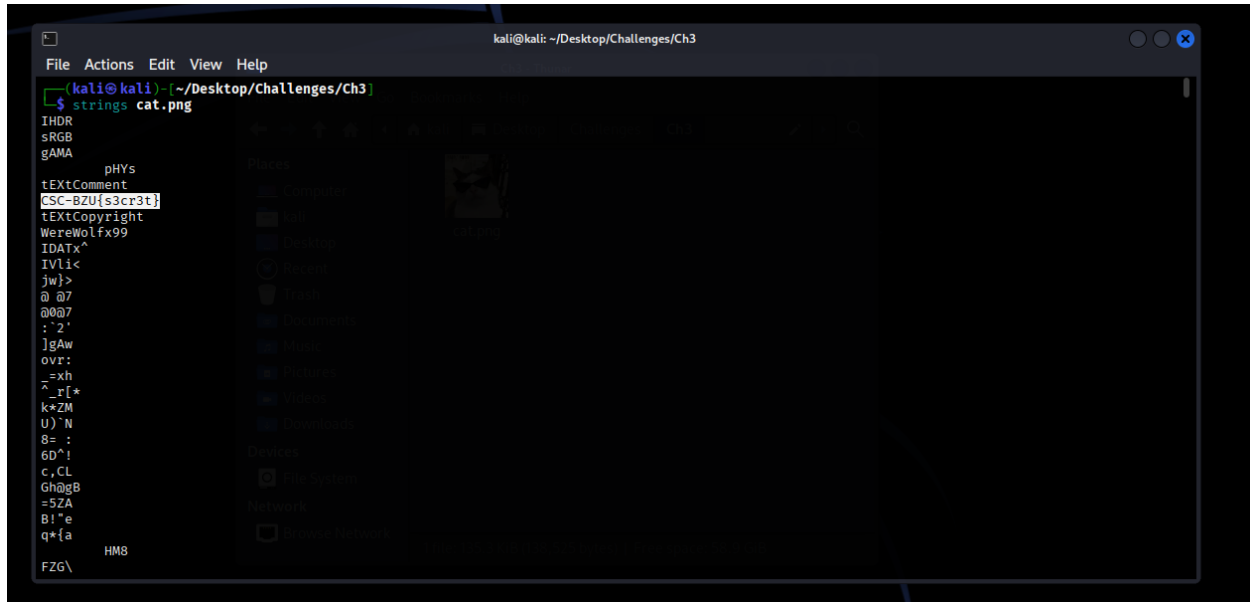
Flag : **CSC-BZU{n0T\_0nlyY\_BaAsEe64}**

Challenge 2:

( cat.png )

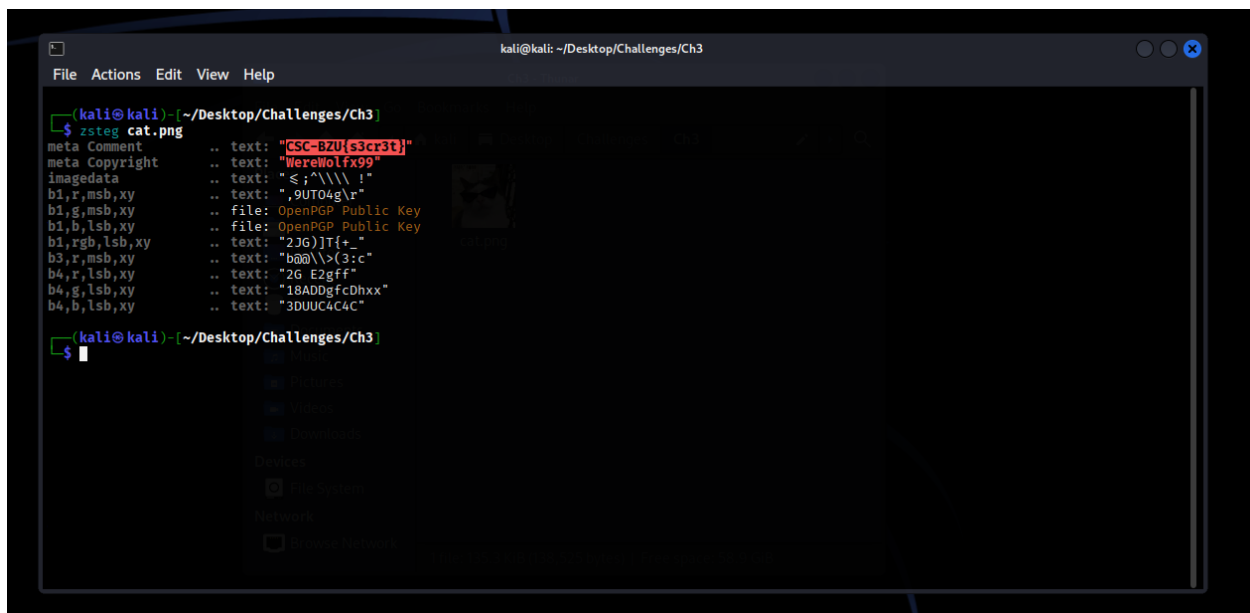
Here the flag is very easy to catch:

1) using **strings** tool:



```
kali@kali: ~/Desktop/Challenges/Ch3
$ strings cat.png
IHDR
sRGB
gAMA
pHYs
tEXtComment
CSC-BZU{s3cr3t}
tEXtCopyright
WereWolfx99
IDATx^
IVli<
jw}>
@ 07
@007
: 2'
]gAw
ovr:
^=xh
^_r[*
k*ZM
U) N
8= :
6D"!
c,CL
Gh@GB
=5ZA
B!`e
q*{a
HMB
FZG\
```

2) using **zsteg** tool:



```
kali@kali: ~/Desktop/Challenges/Ch3
$ zsteg cat.png
meta Comment .. text: "CSC-BZU{s3cr3t}"
meta Copyright .. text: "WereWolfx99"
imagedata .. text: "<^\\ \\ !"
b1,r,msb,xy .. text: ".9UT04g\r"
b1,g,msb,xy .. file: OpenPGP Public Key
b1,b,lsb,xy .. file: OpenPGP Public Key
b1,rgb,lsb,xy .. text: "23G)lT{+ "
b3,r,msb,xy .. text: "b@\\>(3:c"
b4,r,lsb,xy .. text: "26 E2gff"
b4,g,lsb,xy .. text: "18ADDgfcDhxx"
b4,b,lsb,xy .. text: "3DUUC4c4C"
```

You also can use **exiftool** to extract the metadata ☺ .

Flag: **CSC-BZU{s3cr3t}**