Information

Category: Forensics </br> AUTHOR: SUSIE

Description

```
Files can always be changed in a secret way. Can you find the flag? cat.jpg
```

The image

Here is our cute little cat: </br>

</br>

Whenever I get an image file, I go and run `file` (to make sure it's an image), `binwalk` (to see if there are hidden files), `strings` and usually I pair that with `grep` and lastly I check the image in a `hexeditor`, just to check the header and such.

```
root@kali:~/CTFs/Picoctf-2021/information-solved# file cat.jpg
cat.jpg: JPEG image data, JFIF standard 1.02, aspect ratio, density 1x1, segment
length 16, baseline, precision 8, 2560x1598, components 3
root@kali:~/CTFs/Picoctf-2021/information-solved# binwalk cat.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.02

root@kali:~/CTFs/Picoctf-2021/information-solved# strings cat.jpg | grep picoCTF{*
root@kali:~/CTFs/Picoctf-2021/information-solved#
```

Great, what about the hex?

```
......JFIF......
.......0Photosho
p 3.0.8BIM......
....t..PicoCTF..
.........http:/
/ns.adobe.com/xa
p/1.0/.<?xpacket
begin='...' id=
'W5M0MpCehiHzreS
zNTczkc9d'?>.<x:
xmpmeta xmlns:x=
'adobe:ns:meta/'
x:xmptk='Image:
```

```
:ExifTool 10.80'
>.<rdf:RDF xmlns
:rdf='http://www
.w3.org/1999/02/
22-rdf-syntax-ns
#'>.. <rdf:Descr
iption rdf:about
=''.  xmlns:cc='
http://creativec
ommons.org/ns#'>
.  <ccInformation
```

Category: Forensics </br> AUTHOR: SUSIE

Description

Files can always be changed in a secret way. Can you find the flag? cat.jpg

The image

Here is our cute little cat: </br>

cat

</br>

Whenever I get an image file, I go and run file (to make sure it's an image), binwalk (to see if there are hidden files), strings and usually I pair that with grep and lastly I check the image in a hexeditor, just to check the header and such.

```
root@kali:~/CTFs/Picoctf-2021/information-solved# file cat.jpg
cat.jpg: JPEG image data, JFIF standard 1.02, aspect ratio, density 1x1, segment
length 16, baseline, precision 8, 2560x1598, components 3
root@kali:~/CTFs/Picoctf-2021/information-solved# binwalk cat.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.02

root@kali:~/CTFs/Picoctf-2021/information-solved# strings cat.jpg | grep picoCTF{*
root@kali:~/CTFs/Picoctf-2021/information-solved#
```

Great, what about the hex?

```
......JFIF......
.......0Photosho
p 3.0.8BIM......
....t..PicoCTF..
..........http:/
/ns.adobe.com/xa
p/1.0/.<?xpacket
begin='...' id=
'W5M0MpCehiHzreS
zNTczkc9d'?>.<x:
xmpmeta xmlns:x=
'adobe:ns:meta/'
x:xmptk='Image:
:ExifTool 10.80'
>.<rdf:RDF xmlns
:rdf='http://www
```

```
.w3.org/1999/02/
22-rdf-syntax-ns
#'>.. <rdf:Descr
iption rdf:about
=''.  xmlns:cc='
http://creativec
ommons.org/ns#'>
.  <cc:license r
df:resource='cGl
jb0NURnt0aGVfbTN
0YWRhdGFfMXNfbW9
kaWZpZWR9'/>. </
rdf:Description>
.. <rdf:Descript
ion rdf:about=''
.  xmlns:dc='htt
p://purl.org/dc/
elements/1.1/'>.
 <dc:rights>.
<rdf:Alt>.    <
rdf:li xml:lang=
'x-default'>Pico
CTF</rdf:li>.
</rdf:Alt>.  </d
c:rights>. </rdf
:Description>.</
rdf:RDF>.</x:xmp
meta>.
```

Interesting... I can see some base64, maybe? W5M0MpCehiHzreSzNTczkc9d and cGljb0NURnt0aGVfbTN0YWRhdGFfMXNfbW9kaWZpZWR9

Decoding in the terminal

Linux

Just echo W5M0MpCehiHzreSzNTczkc9d | base64 -d and we get beautiful nonsense [�42���!��573��]r. So maybe try the next string:

```
echo cGljb0NURnt0aGVfbTN0YWRhdGFfMXNfbW9kaWZpZWR9 | base64 -d
```

```
picoCTF{the_m3tadata_1s_modified}
```

Great!!

Windows (PowerShell)

This looks a little bit more dawnting

```
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('cGljb0NURnt0aGVfbTN0YWRhdGFfMXNfbW9kaWZpZWR9'))
picoCTF{the_m3tadata_1s_modified}:license r
df:resource='cGl
jb0NURnt0aGVfbTN
0YWRhdGFfMXNfbW9
kaWZpZWR9'/>. </
rdf:Description>
.. <rdf:Descript
ion rdf:about=''
.  xmlns:dc='htt
```

```
p://purl.org/dc/
elements/1.1/'>.
 <dc:rights>.
<rdf:Alt>.    <
rdf:li xml:lang=
'x-default'>Pico
CTF</rdf:li>.
</rdf:Alt>.  </d
c:rights>. </rdf
:Description>.</
rdf:RDF>.</x:xmp
meta>.
```

Interesting... I can see some base64, maybe? `W5M0MpCehiHzreSzNTczkc9d` and `cGljb0NURnt0aGVfbTN0YWRhdGFfMXNfbW9kaWZpZWR9`

Decoding in the terminal

Linux

Just `echo W5M0MpCehiHzreSzNTczkc9d | base64 -d` and we get beautiful nonsense `[�42���!��573��]r`. So maybe try the next string:

```
echo cGljb0NURnt0aGVfbTN0YWRhdGFfMXNfbW9kaWZpZWR9 | base64 -d
```

```
picoCTF{the_m3tadata_1s_modified}
```

Great!!

Windows (PowerShell)

This looks a little bit more dawnting

```
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('cGljb0NURnt
0aGVfbTN0YWRhdGFfMXNfbW9kaWZpZWR9'))
picoCTF{the_m3tadata_1s_modified}
```