

WRITE UP PICOCTF FORENSICS

Mutiara Setya Rini

Daftar Isi

Challenge 1 : Scan Surprise	1
Challenge 2 : Secret of the Polyglot	3
Challenge 3 : Can You See	5
Challenge 4 : Information.....	7
Challenge 5 : Glory of the Garden	9

Challenge 1 : Scan Surprise

Scan Surprise

Bookmark this challenge

Easy Forensics picoCTF 2024 shell browser_webshell_solvable qr_code

AUTHOR: JEFFERY JOHN

Description

I've gotten bored of handing out flags as text. Wouldn't it be cool if they were an image instead?

You can download the challenge files here:

- [challenge.zip](#)

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.

Its current status is: **NOT_RUNNING**

Launch Instance

Hints ?

1 2 3

42,178 users solved

86% Liked

picoCTF{FLAG}

Submit Flag

Download file challenge.zip yang tersedia. Kemudian unzip file tersebut dan lihat isi di dalamnya.

```
(mutzy@kali)-[~/Downloads]
$ unzip challenge.zip
Archive:  challenge.zip
  creating: home/ctf-player/drop-in/
  extracting: home/ctf-player/drop-in/flag.png
```

```
(mutzy@kali)-[~/Downloads]
$ cd home

(mutzy@kali)-[~/Downloads/home]
$ ls
ctf-player

(mutzy@kali)-[~/Downloads/home]
$ cd ctf-player

(mutzy@kali)-[~/Downloads/home/ctf-player]
$ ls
drop-in

(mutzy@kali)-[~/Downloads/home/ctf-player]
$ cd drop-in

(mutzy@kali)-[~/Downloads/home/ctf-player/drop-in]
$ ls
flag.png

(mutzy@kali)-[~/Downloads/home/ctf-player/drop-in]
$ open flag.png

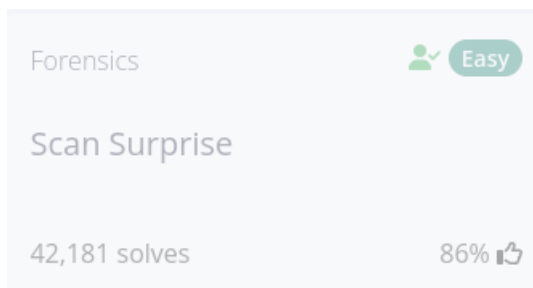
(mutzy@kali)-[~/Downloads/home/ctf-player/drop-in]
$
```



Terlihat bahwa file flag.png tersebut berisi QR code. Untuk membaca QR code ini, kita bisa menggunakan QR reader, seperti zbar tools.

```
(mutzy@kali)-[~/Downloads/home/ctf-player/drop-in]
$ zbarimg flag.png
QR-Code:picoCTF{p33k_@_b00_b5ce2572}
scanned 1 barcode symbols from 1 images in 0.01 seconds
```

Flag berhasil didapatkan.



Challenge 2 : Secret of the Polyglot

Secret of the Polyglot



Easy Forensics picoCTF 2024 file_format polyglot

AUTHOR: SYREAL

Description

The Network Operations Center (NOC) of your local institution picked up a suspicious file, they're getting conflicting information on what type of file it is. They've brought you in as an external expert to examine the file. Can you extract all the information from this strange file?
Download the suspicious file [here](#).

Hints 

1

23,255 users solved



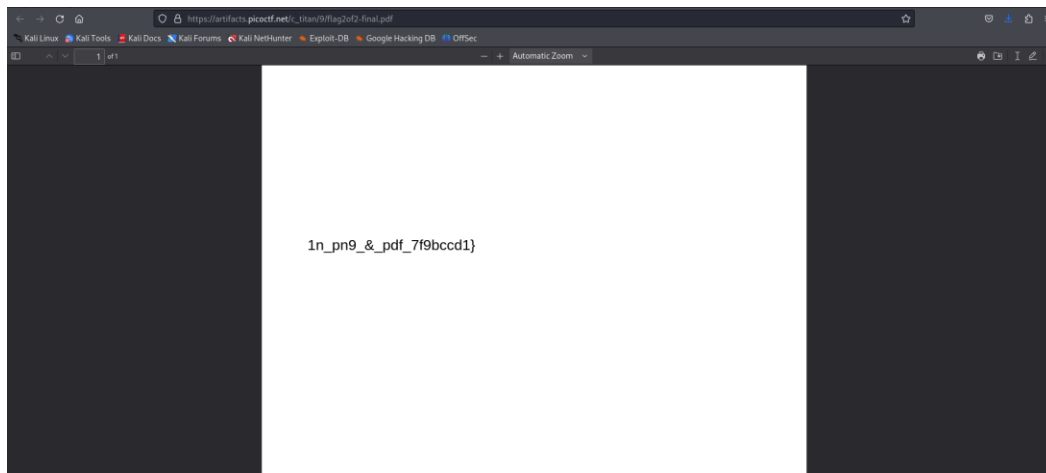
95% Liked



 picoCTF{FLAG}

Submit Flag

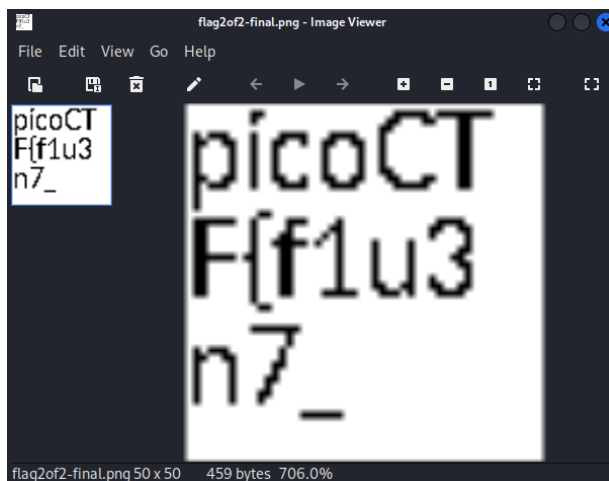
Pertama, download file yang ada di dalam attachment challenge. Kemudian coba lihat isi dari file tersebut.



Ternyata file tersebut merupakan file pdf yang berisi string yang suspicious. Dari hints yang diberikan pada challenge, yaitu *This problem can be solved by just opening the file in different ways*, kita bisa coba menggali informasi detail mengenai file tersebut dengan menggunakan command exiftool. Didapatkan hasil seperti ini :


```
(mutzy@kali)-[~/Downloads/CTFstuff]
$ exiftool flag2of2-final.pdf
ExifTool Version Number      : 12.76
File Name                    : flag2of2-final.pdf
Directory                   : .
File Size                    : 3.4 kB
File Modification Date/Time  : 2025:02:02 12:10:59+07:00
File Access Date/Time       : 2025:02:02 12:10:59+07:00
File Inode Change Date/Time  : 2025:02:02 12:10:59+07:00
File Permissions             : -rw-rw-r--
File Type                    : PNG
File Type Extension          : png
MIME Type                    : image/png
Image Width                  : 50
Image Height                 : 50
Bit Depth                    : 8
Color Type                   : RGB with Alpha
Compression                  : Deflate/Inflate
Filter                       : Adaptive
Interlace                    : Noninterlaced
Profile Name                  : ICC profile
Profile CMM Type              : Little CMS
Profile Version              : 4.3.0
Profile Class                 : Display Device Profile
Color Space Data              : RGB
Profile Connection Space     : XYZ
Profile Date Time             : 2023:11:02 17:42:31
Profile File Signature        : acsp
Primary Platform              : Apple Computer Inc.
CMM Flags                     : Not Embedded, Independent
Device Manufacturer          : 
Device Model                  : 
Device Attributes             : Reflective, Glossy, Positive, Color
Rendering Intent              : Perceptual
Connection Space Illuminant  : 0.9642 1 0.82491
Profile Creator               : Little CMS
Profile ID                    : 0
Profile Description           : GIMP built-in sRGB
```

Dari informasi tersebut, kita menjadi tahu bahwa sebenarnya file flag2of2-final tersebut berbentuk png. Dari hal tersebut, kemudian kita bisa convert file tersebut menjadi png dan coba membukanya.



Flag berhasil ditemukan. Flag ini merupakan part 1 dan lanjutan dari flag ini mungkin saja sebuah string yang ada di dalam file pdf tadi. Dan didapatkan flag fullnya adalah **picoCTF{f1u3n7_1n_pn9_&_pdf_53b741d6}**

Challenge 3 : Can You See


CanYouSee 

Easy Forensics picoCTF 2024 browser_webshell_solvable

AUTHOR: MUBARAK MIKAIL



Description


How about some hide and seek?
Download this file [here](#).

Hints 

1 2

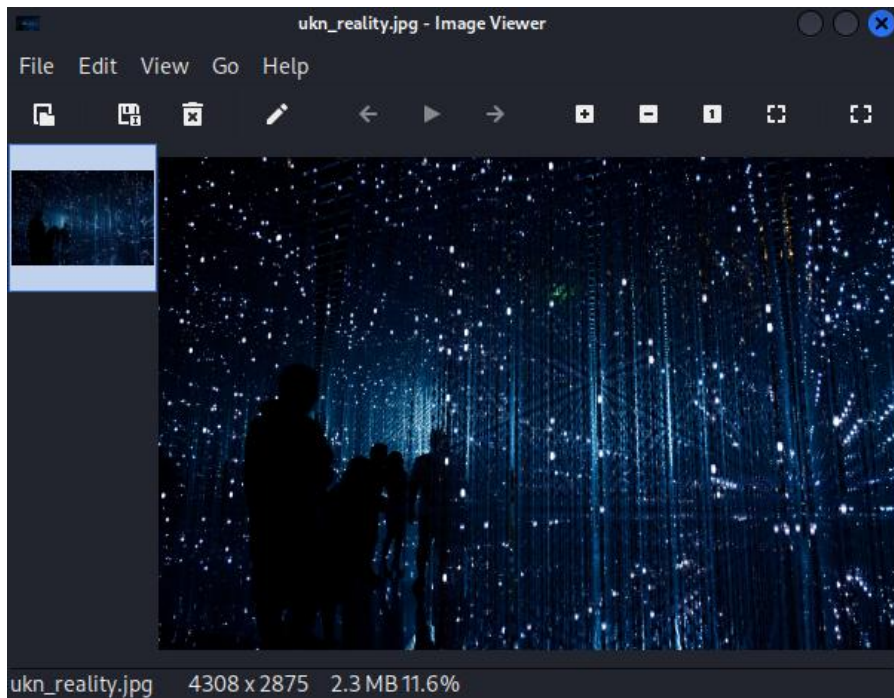
22,509 users solved

 93% Liked 

 picoCTF{FLAG}

Submit Flag

Pertama, download file yang ada di attachment challenge. Kemudian buka file tersebut. Didapatkan bahwa file jpg tersebut berisi gambar seperti ini :



Coba kita lihat informasi detail dari meta datanya menggunakan command exiftool. Didapatkan data sebagai berikut.

```

(mutzy@kali)-[~/Downloads]
$ exiftool ukn_reality.jpg
ExifTool Version Number      : 12.76
File Name                    : ukn_reality.jpg
Directory                    : .
File Size                     : 2.3 MB
File Modification Date/Time   : 2024:03:12 07:05:55+07:00
File Access Date/Time        : 2025:02:02 12:44:19+07:00
File Inode Change Date/Time   : 2025:02:02 12:44:19+07:00
File Permissions              : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : inches
X Resolution                  : 72
Y Resolution                  : 72
XMP Toolkit                  : Image::ExifTool 11.88
Attribution URL              : cGljb0NURntNRTc0RDQ3QV9ISUREM05fNmE5ZjVhYzR9Cg==
Image Width                  : 4308
Image Height                  : 2875
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                   : 4308x2875
Megapixels                   : 12.4

```

Ada satu komponen yang menarik, yaitu attribution URL, yang berbentuk seperti string base64 encoded. Kemudian, kita coba decode string tersebut menggunakan command seperti di bawah ini :

```

(mutzy@kali)-[~/Downloads]
$ echo "cGljb0NURntNRTc0RDQ3QV9ISUREM05fNmE5ZjVhYzR9Cg==" |base64 --decode
picoCTF{ME74D47A_HIDD3N_6a9f5ac4}

```

Dan flag berhasil didapatkan.

Forensics
✓ Easy

CanYouSee

22,510 solves
93%

Challenge 4 : Information

information 



Easy

Forensics

picoCTF 2021

AUTHOR: SUSIE

Description

Files can always be changed in a secret way. Can you find the flag? [cat.jpg](#)

Hints 

1 2

Look at the details of the file

123,802 users solved



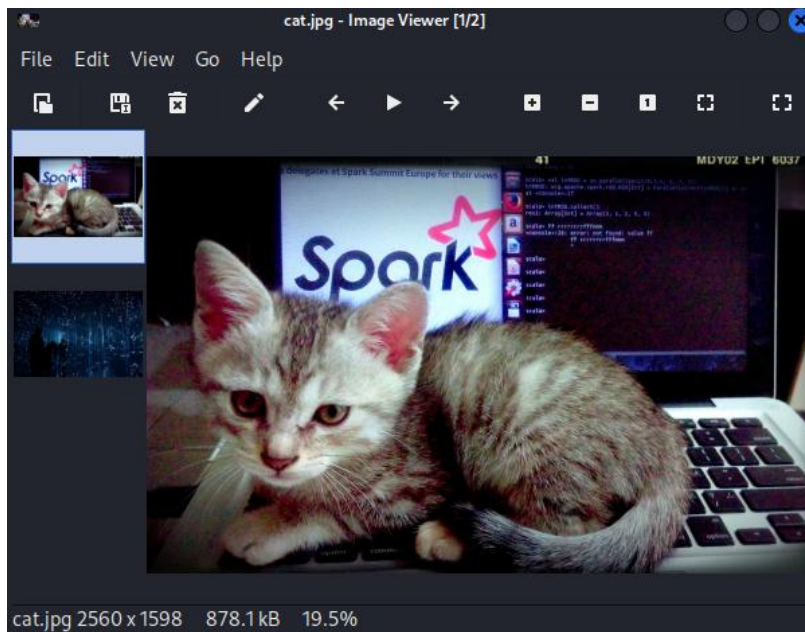
49% Liked



 picoCTF{FLAG}

Submit Flag

Download file yang ada di attachment dan coba membukanya. Didapatkan file berbentuk jpg dengan gambar seperti ini :



Coba kita lihat detail dari meta data file ini. Didapatkan data sebagai berikut.


```

(mutzy@kali)-[~/Downloads]
$ exiftool cat.jpg
ExifTool Version Number      : 12.76
File Name                    : cat.jpg
Directory                   : .
File Size                    : 878 kB
File Modification Date/Time  : 2025:02:02 13:17:31+07:00
File Access Date/Time       : 2025:02:02 13:17:31+07:00
File Inode Change Date/Time  : 2025:02:02 13:17:31+07:00
File Permissions             : -rw-rw-r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.02
Resolution Unit              : None
X Resolution                  : 1
Y Resolution                  : 1
Current IPTC Digest          : 7a78f3d9cfb1ce42ab5a3aa30573d617
Copyright Notice             : PicoCTF
Application Record Version   : 4
XMP Toolkit                  : Image::ExifTool 10.80
License                      : cGljb0NURnt0aGVfbTN0YWRhdGFfMXNfbW9kaWZpZW99
Rights                       : PicoCTF
Image Width                  : 2560
Image Height                  : 1598
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                   : 2560x1598
Megapixels                   : 4.1

```


Ada satu komponen yang suspicious, yaitu license. License tersebut seperti berbentuk string base64 encoded. Maka dari itu, kita bisa mencoba decode string tersebut dengan command berikut.

```


(mutzy@kali)-[~/Downloads]
$ echo "cGljb0NURnt0aGVfbTN0YWRhdGFfMXNfbW9kaWZpZW99" | base64 --decode
picoCTF{the_m3tadata_1s_modified}

```

Flag berhasil didapatkan.

Forensics


information

123,803 solves
49% 

Challenge 5 : Glory of the Garden

Glory of the Garden 



Easy Forensics picoCTF 2019

AUTHOR: JEDAVIS/DANNY

Description


This [garden](#) contains more than it seems.

Hints 

1

What is a hex editor?

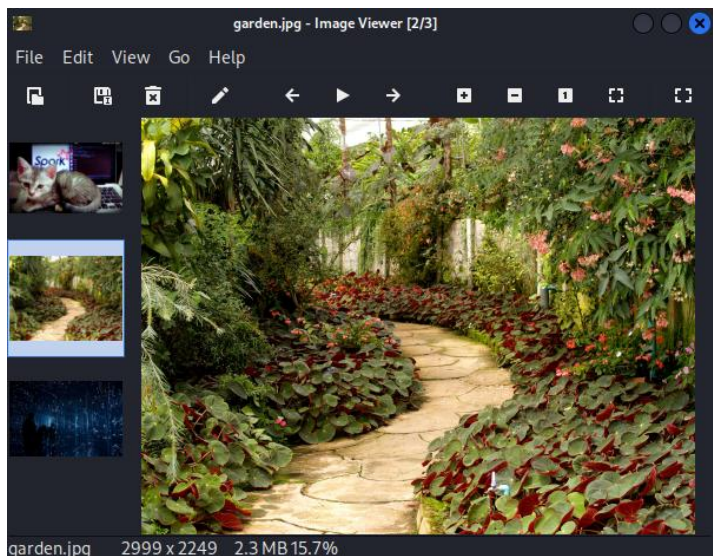
71,935 users solved

 89% Liked 

 picoCTF{FLAG}

Submit Flag

Pertama, coba download dan buka file garden. Didapatkan bahwa file garden berbentuk jpg dan berisi gambar seperti berikut.



Tidak ada sesuatu yang suspicious dalam gambar, sehingga kita bisa cari informasi lebih detail dari gambar ini, termasuk metadatanya.

```

(mutzy@kali)-[~/Downloads]
$ exiftool garden.jpg
ExifTool Version Number      : 12.76
File Name                    : garden.jpg
Directory                   : .
File Size                    : 2.3 MB
File Modification Date/Time  : 2025:02:02 13:24:53+07:00
File Access Date/Time       : 2025:02:02 13:24:53+07:00
File Inode Change Date/Time  : 2025:02:02 13:24:53+07:00
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                 : 72
Y Resolution                 : 72
Profile CMM Type             : Linotronic
Profile Version              : 2.1.0
Profile Class                : Display Device Profile
Color Space Data             : RGB
Profile Connection Space     : XYZ
Profile Date Time            : 1998:02:09 06:49:00
Profile File Signature       : acsp
Primary Platform             : Microsoft Corporation
CMM Flags                    : Not Embedded, Independent
Device Manufacturer         : Hewlett-Packard
Device Model                 : sRGB
Device Attributes            : Reflective, Glossy, Positive, Color
Rendering Intent             : Perceptual
Connection Space Illuminant  : 0.9642 1 0.82491
Profile Creator              : Hewlett-Packard
Profile ID                   : 0
Profile Copyright            : Copyright (c) 1998 Hewlett-Packard Company
Profile Description          : sRGB IEC61966-2.1
Media White Point            : 0.95045 1 1.08905
Media Black Point            : 0 0 0
Red Matrix Column            : 0.43607 0.22249 0.01392
Green Matrix Column         : 0.38515 0.71687 0.09708
Blue Matrix Column          : 0.14307 0.06061 0.7141
Device Mfg Desc              : IEC http://www.iec.ch
Device Model Desc           : IEC 61966-2.1 Default RGB colour space - sRGB
Viewing Cond Desc           : Reference Viewing Condition in IEC61966-2.1

```


Meta datanya adalah seperti ini. Namun tidak ada suatu hal yang suspicious, sehingga bisa kita abaikan sementara. Dari hint yang ada, terdapat mention mengenai hex editor, jadi kita coba masukkan file jpg tersebut ke dalam hex editor, seperti ghex.

The screenshot shows the Ghex hex editor with the file 'garden.jpg' loaded. The left pane shows a list of files. The main pane displays hex data in columns, with the first column showing the hex values and the second column showing the corresponding ASCII characters. The data starts with '20 AE 78 08 6A B8 0A 08 BA 6E A5 79 4A FC DD 7C CF AC 3C 5D 7A 56 26 96 3C 94 95 08 B1 BE 05 F3 48 BE B6 79 C8 29 82 0F A1 5F 42 EA' and continues with more hex and ASCII data.

Dari hex editor tersebut, kita dapat telusuri string yang memungkinkan menjadi flag, yaitu string yang mengandung picoCTF{...}. Dan string flag tersebut berhasil didapatkan di bagian akhir dari string.

picoCTF{more_than_m33ts_the_3y3657BaB2C}

Forensics

 Easy

Glory of the Garden

71,936 solves

89% 