

Today Exercise for Mr Hanis Class was Network Forensics.



Hint: it is from skr ctf(so sad, I spend so much time)

Shark Of Wire 2

20

I lose my network data again... Luckily I always got a backup pcap file! Please help me find my "flag" its important!

Flag format: SKR{flag}

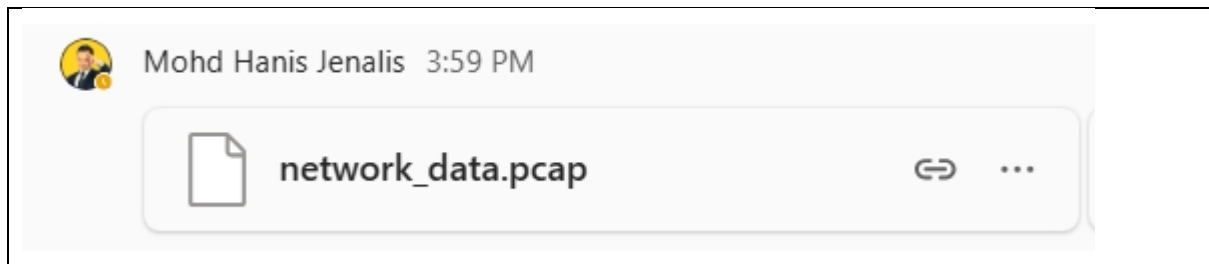
Note: There were some stego and crypto elements

Difficulty: Medium

Hint 1: Notice there were some image files?

Hint 2: I got login in a website, using godam as username. But sorry I forgot the password... It also used for a zip file that I kept it somewhere...

Prerequisite : Download pcap file provided by Mr Hanis



To make the following session interesting, Mr Hanis will Role Play as Doc Hudson(chief crew)



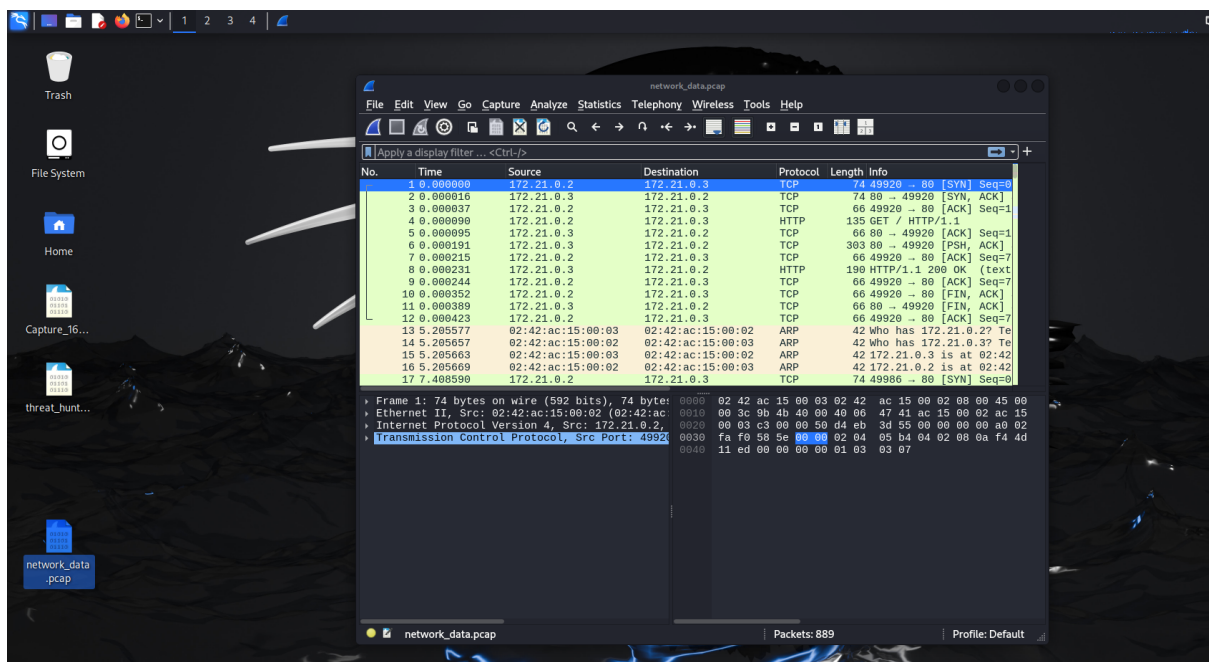
My Friend will roleplay as The King(former champion racer)



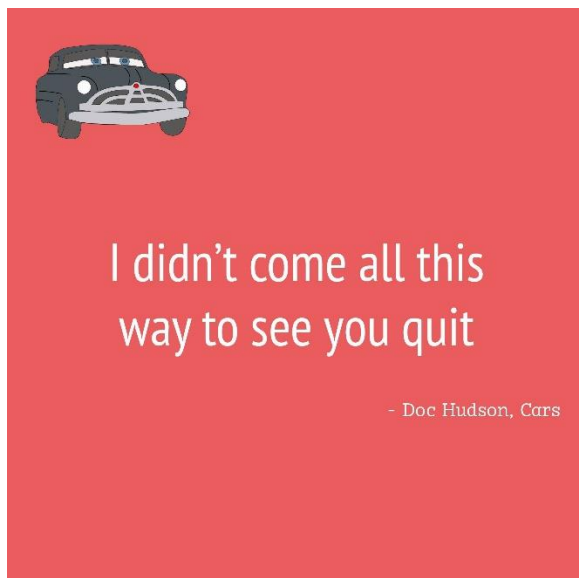
and I will roleplay as McQueen(champion racer)



First, Open kali linux, launch wireshark and drag the pcap file to wireshark



Damn, so many messy characters!





McQueen:

Hey Doc, what can I do? Like turning left to go right?



Doc Hudson:

Hey Kid, remember in network forensics protocol is the number one rule (ICMP,TCP/IP, HTTP,HTTPS). Here is some strategy for you.

1)analyze, follow, tcp or anything stream

2)statistics, protocol hierarchy

3) go to filter area, search ftp or http, if it is green, it is available

4) If it is images/data how you extract?

ans:Go to file, export object, http, save all



Mcqueen:

Kachow, time to prove I am speed.

Mcqueen:

Hey, doc how simple is this flag.

The image shows a Wireshark network capture of an HTTP transaction. The left pane displays a list of packets, with packet 8 selected. The middle pane shows the details of packet 8, which is an HTTP 200 OK response. The right pane shows the raw data of the selected packet, which is an HTML document.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.21.0.2	172.21.0.3	TCP	74	49920 → 80 [SYN] Seq=0 Win=0
2	0.000016	172.21.0.3	172.21.0.2	TCP	74	80 → 49920 [SYN, ACK] Seq=0
3	0.000037	172.21.0.2	172.21.0.3	TCP	66	49920 → 80 [ACK] Seq=1 Ack=
4	0.000090	172.21.0.2	172.21.0.3	HTTP	135	GET / HTTP/1.1
5	0.000095	172.21.0.3	172.21.0.2	TCP	66	80 → 49920 [ACK] Seq=1 Ack=
6	0.000191	172.21.0.3	172.21.0.2	TCP	383	80 → 49920 [PSH, ACK] Seq=1
7	0.000215	172.21.0.2	172.21.0.3	TCP	66	49920 → 80 [ACK] Seq=70 Ack=
8	0.000231	172.21.0.3	172.21.0.2	HTTP	190	HTTP/1.1 200 OK (text/html)
9	0.000244	172.21.0.2	172.21.0.3	TCP	66	49920 → 80 [ACK] Seq=70 Ack=
10	0.000352	172.21.0.2	172.21.0.3	TCP	66	49920 → 80 [FIN, ACK] Seq=7
11	0.000389	172.21.0.3	172.21.0.2	TCP	66	80 → 49920 [FIN, ACK] Seq=3
12	0.000423	172.21.0.2	172.21.0.3	TCP	66	49920 → 80 [ACK] Seq=71 Ack=

Packet 8 Details:

- Frame 8: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface 0
- Ethernet II, Src: 02:42:ac:15:00:03 (02:42:ac:15:00:03), Dst: 02:42:ac:15:00:03 (02:42:ac:15:00:03)
- Internet Protocol Version 4, Src: 172.21.0.3, Dst: 172.21.0.2
- Transmission Control Protocol, Src Port: 80, Dst Port: 49920
- [2] Reassembled TCP Segments (361 bytes): #0(2:255-255) [RST] Seq=1234567890 Win=0 Len=0
- Hypertext Transfer Protocol
- Line-based text data: text/html (10 Lines)

Raw Data:

```
0000 02 42 ac 15 00 02 02 42 ac 15 00 03 08 00 45 00
0010 00 b0 5a 70 40 00 40 06 87 a8 ac 15 00 03 ac 15
0020 00 02 00 50 c3 00 f9 c0 21 61 d4 eb 3d 9b 80 18
0030 01 fd 58 d2 00 00 01 01 08 0a 10 1d ea b9 f4 4d
0040 11 ed 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c
0050 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a
0060 09 3c 74 69 74 6c 65 3e 46 6c 61 67 3c 2f 74 69
0070 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f
0080 64 79 3e 0a 3c 68 31 3e 46 6c 61 67 3a 20 53 4b
0090 52 7b 4e 6f 74 5f 74 68 61 74 5f 65 61 70 79 5f
00a0 61 6e 79 64 6f 72 65 7d 3c 2f 68 31 3e 0a 3c
00b0 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e
```

HTTP Response Details:

```
GET / HTTP/1.1
Host: pcap2
User-Agent: curl/7.66.0
Accept: */*

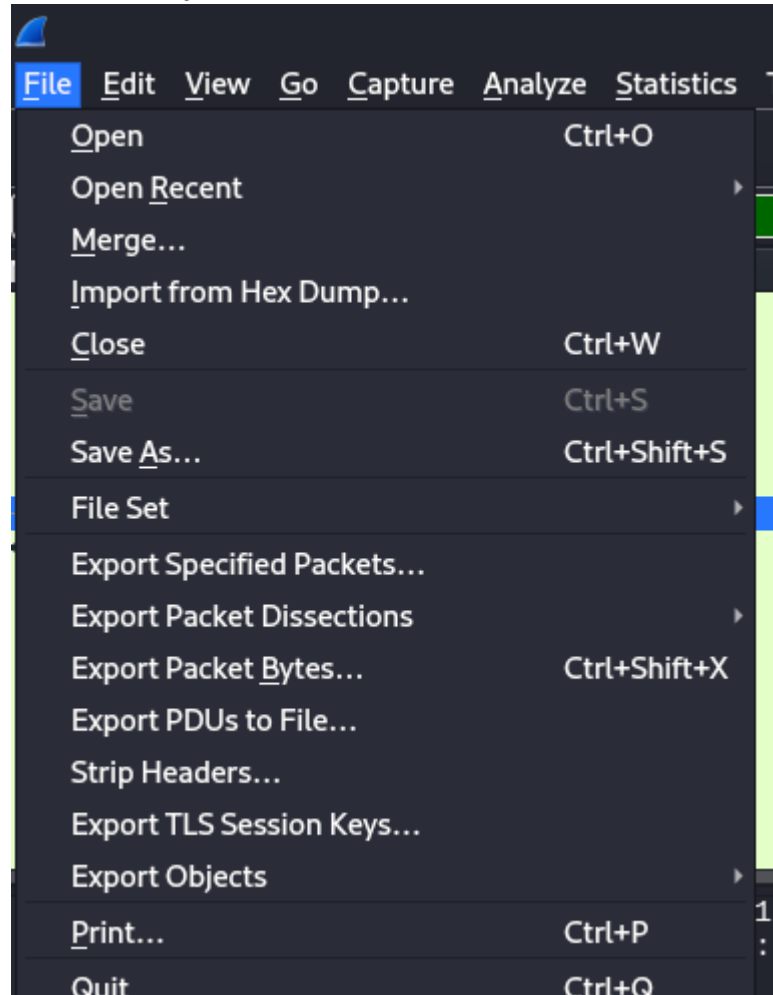
HTTP/1.1 200 OK
Server: nginx/1.17.3
Date: Wed, 08 Apr 2020 17:17:38 GMT
Content-Type: text/html
Content-Length: 124
Last-Modified: Wed, 08 Apr 2020 08:37:55 GMT
Connection: keep-alive
Etag: "5e8dbd63-7c"
Accept-Ranges: bytes

<!DOCTYPE html>
<html>
<head>
<title>Flag</title>
</head>
<body>
<h1>Flag: SKR(Not_that_easy_anymore)</h1>
</body>
</html>
```

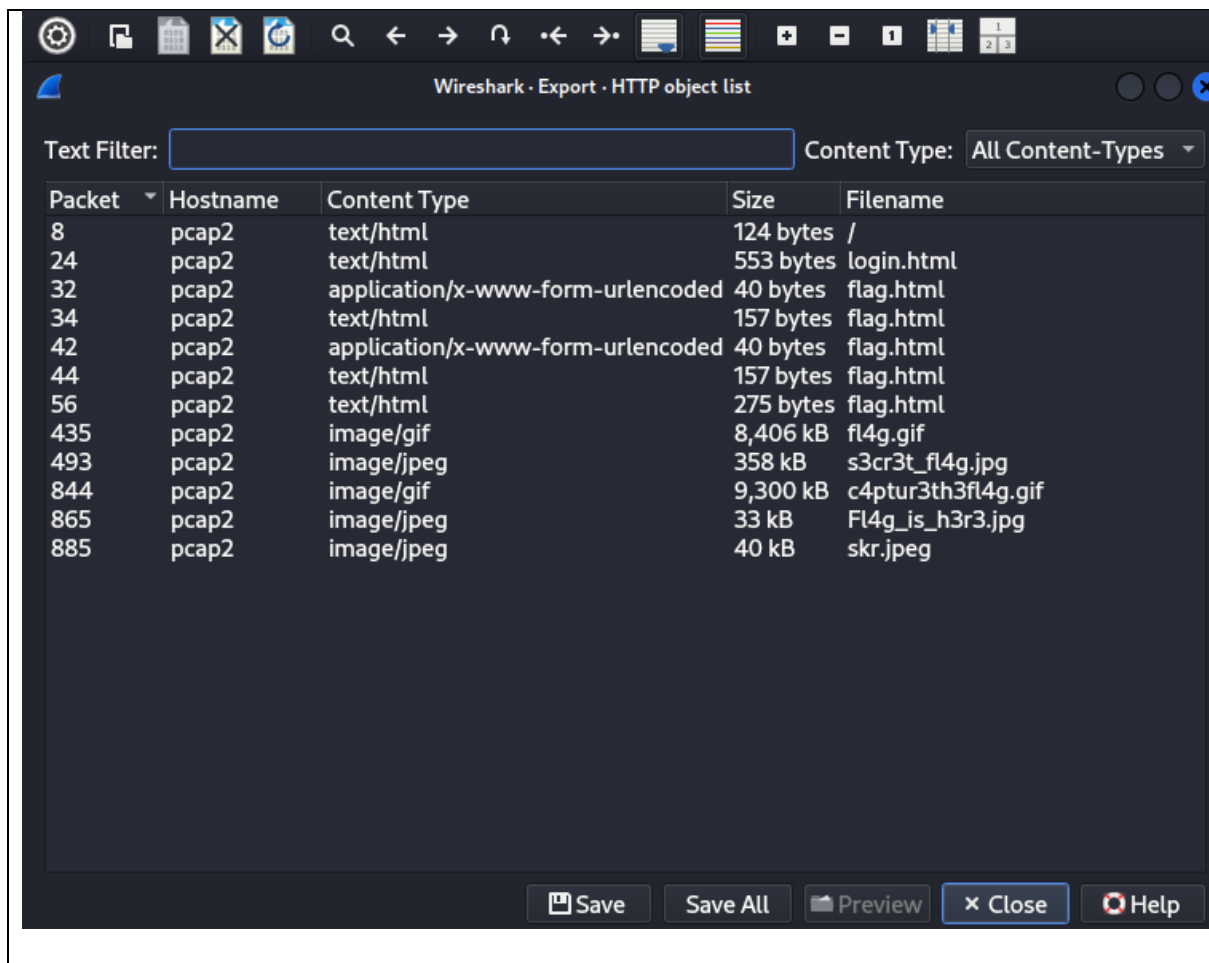


Doc:

Hahaha kid, you are still too naïve.



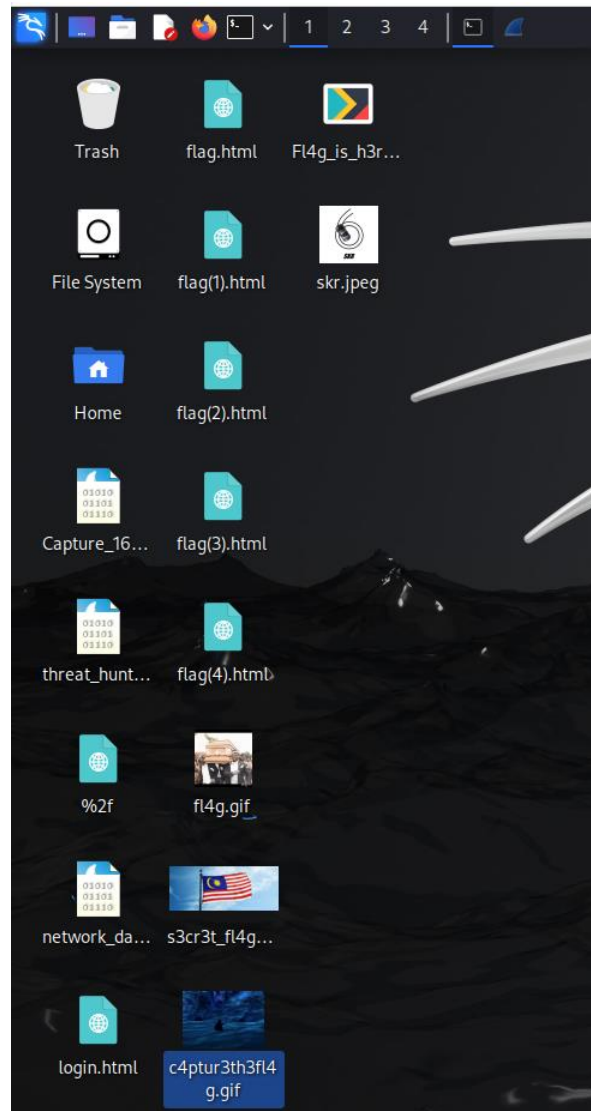
First, go to exports objects -> http -> save all





Mcqueen:

Then what? Which file I should start with?





The King(Strip Weathers):

Yo Kid, How about start with that Malaysia Flag jpg file? And try to binwalk it



Mcqueen:

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ binwalk s3cr3t_fl4g.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
10005	0x2715	Zip archive data, encrypted at least v2.0 to extract, compressed size: 348595, uncompressed size: 353020, name: mystery_letter.jpg
358780	0x5797C	End of Zip archive, footer length: 22

Ok, I saw a hidden zip file. How to extract it? After some reading from stack over flow. I got this!

```
s3cr3t_fl4g.jpg
358780 0x5797C End of Zip archive, footer length: 22
```

```
(kali@kali)-[~/Desktop]
$ binwalk -e s3cr3t_fl4g.jpg
```

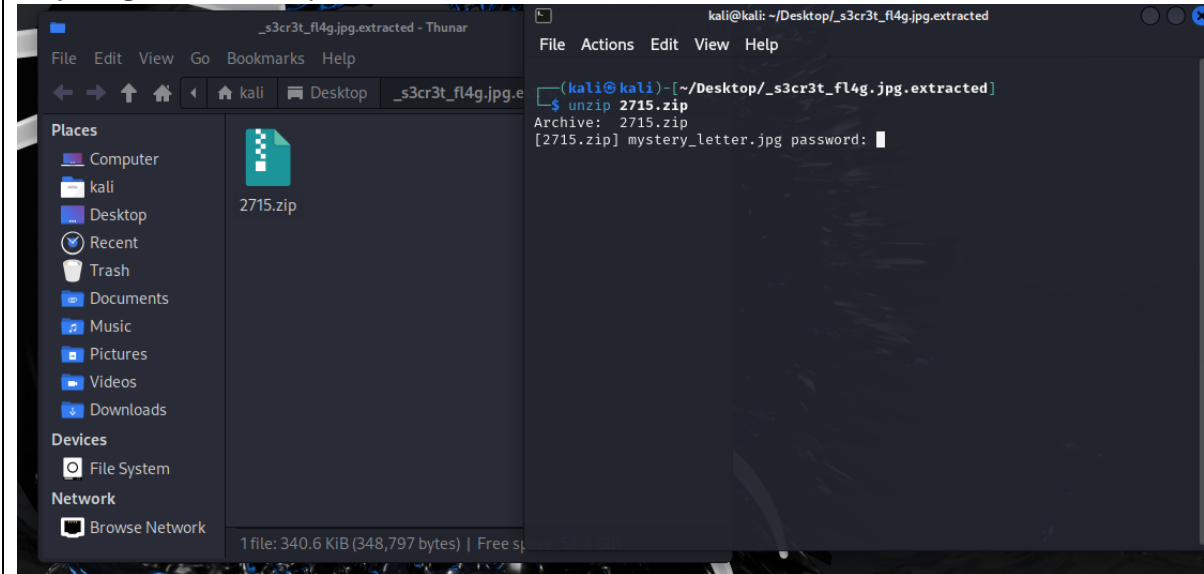
DECIMAL	HEXADECIMAL	DESCRIPTION
---------	-------------	-------------

Then, I unzip it



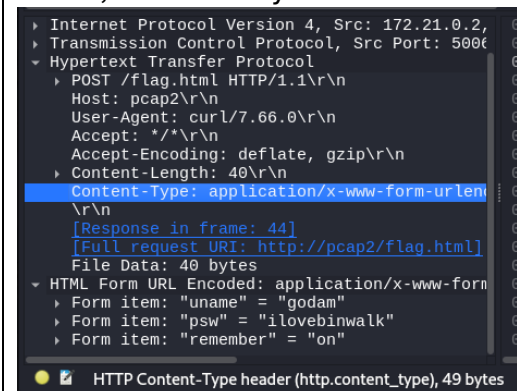
McQueen:

Hey King, what is the password.



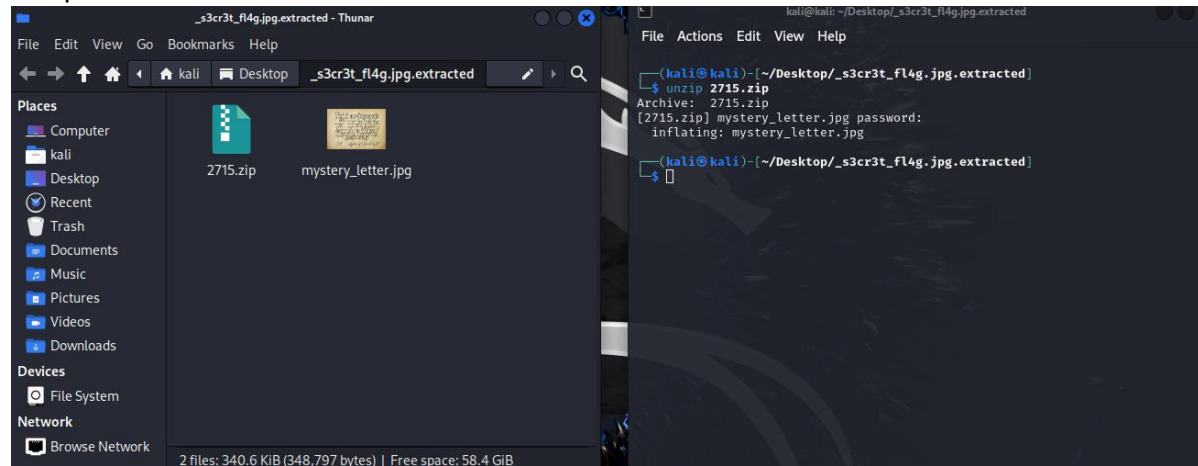
The King(Strip Weathers):

Yo Kid, Look closely at the hint 2.





Mcqueen:



Ok, I just got a mystery_letter.jpg now what?



Hey Son, have you ever tried the almighty all knowing 345 cubic inch V8 engine(Chatgpt)?
Try to ask.



Mcqueen:

Shark Of Wire 2

20

I lose my network data again... Luckily I always got a backup pcap file! Please help me find my "flag" its important!

Flag format: SKR{flag}

Note: There were some stego and crypto elements

Difficulty: Medium

Hint 1: Notice there were some image files?

Hint 2: I got login in a website, using godam as username. But sorry I forgot the password... It also used for a zip file that I kept it somewhere...

Steps I gone through:

- 1) Downloaded network_data.pcap file
- 2) Open and analyze with Wireshark
- 3) Extracted objects from Wireshark.
- 4) Found some files which include flag.html, s3cr3t_fl4g.jpg
- 5) Use binwalk s3cr3t_fl4g.jpg, found hidden zip file.
- 6) Extract the hidden zip file with binwalk -e s3cr3t_fl4g.jpg, then unzip the zip file with password found in flag.html which is password123
- 7) Saw a image which is mystery_letter.jpg, someone tell me it is about steganography
- 8) Got stucked, and ask ChatGPT



Use Steghide: You can try using steghide to extract hidden data from mystery_letter.jpg. Since you mentioned the passphrase was an issue earlier, here's how you can proceed:

bash

Copy code

```
steghide extract -sf mystery_letter.jpg -p password123
```



McQueen:

You liars, this does not work at all.



The King:

Open Your eyes and try to read from the mystery_letter, You will feel the power of rotary engine.



Steghide is a steganography program that is able to hide data in various kinds of image- and audio files. The color- respectively sample- frequencies are not changed thus making the embedding resistant against first-order statistical tests.
Note: Cuffbig of U4pr3c5g3t

Mcqueen:

The above message is about “steghide is a steganography program that is able to data in various kinds of”

Vroom, can't read the others!!!!

As I remember I won piston cup(first blood) and received the forbidden fuel



Hmm, It is time to use the forbidden fuel(OSINT) for extra power!

I am SPEED!!!



Mcqueen:

The words in the mystery_letter is actually from <https://library.mosse-institute.com/articles/2022/07/steghide-hiding-data-in-plain-sight/steghide-hiding-data-in-plain-sight.html>

Now I provide the full paragraph to 345 cubic inch hemi engine(chatgpt),
“Steghide is a steganography program that is able to hide data in various kinds of image and audio files. The color respectively sample-frequencies are not changed thus making the embedding resistant against first-order statistical tests. “

And ask the almighty engine to identify the below text and I get “Cuffjbeq vf U4px3e5g3t”

Which is “Phssword is H4ck3r5t3g”

Recipe	Input
ROT13 <input checked="" type="checkbox"/> Rotate lower case chars <input checked="" type="checkbox"/> Rotate upper case chars <input type="checkbox"/> Rotate numbers Amount: 13	Cuffjbeq vf U4px3e5g3t password Output Phssword is H4ck3r5t3g cnffjbeq



The King:

Hahaha Kid, One more step to go. Remember Steghide?



Mcqueen:

Yes, what was the passphrase?

```
kali@kali: ~/Desktop/_s3cr3t_fl4g.jpg.extracted
File Actions Edit View Help
(kali@kali)-[~/Desktop/_s3cr3t_fl4g.jpg.extracted]
$ steghide extract -sf mystery_letter.jpg
Enter passphrase:
```

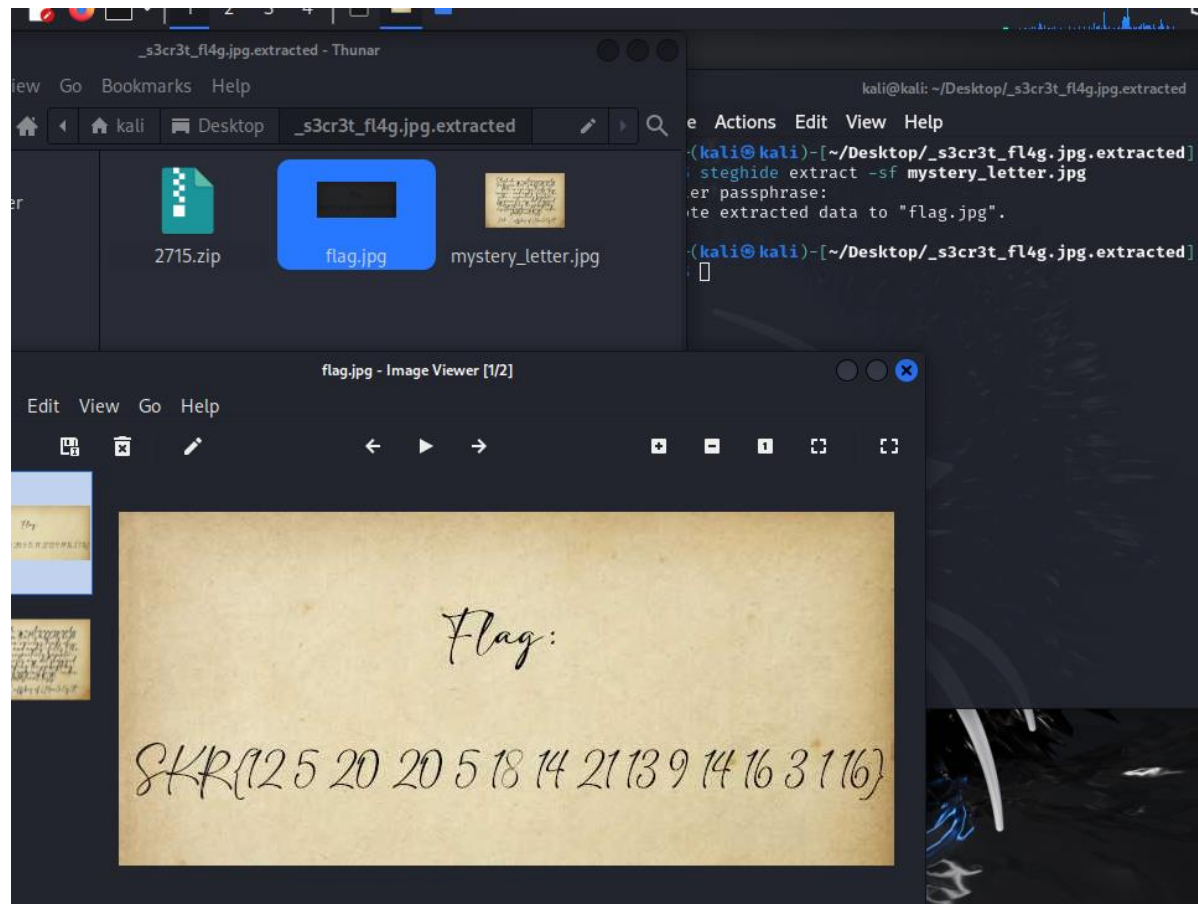



Jackson Storm:
Remember the password you found?



McQueen:

Yes, I saw a strings of numbers.





Jackson Storm:
Now try dcode.fr



McQueen:

Search for a tool

★ SEARCH A TOOL ON dCODE BY KEYWORDS:
e.g. type 'random'

★ BROWSE THE [FULL dCODE TOOLS' LIST](#)

Results

dcode's analyzer suggests to investigate:

⚠ Warning The text has a short length, this can affect the quantity and reliability of the results (see FAQ)

	11	11
Letter Number Code (A1Z26) A=1, B=2, C=3		■■■
ISBN Book Code		■

CIPHER IDENTIFIER

Cryptography > Cipher Identifier

ENCRYPTED MESSAGE IDENTIFIER

★ CIPHERTEXT TO RECOGNIZE (?)

125 20 20 5 18 14 21 13 9 14 16 3 1 16

★ CLUES/KEYWORDS (IF ANY)

▶ ANALYZE

See also: [Frequency Analysis](#) – [Index of Coincidence](#)

It looks like Letter number code

Mcqueen:

I got the flag

Search for a tool

★ SEARCH A TOOL ON dCode BY KEYWORDS:
e.g. type 'random'

★ BROWSE THE [FULL dCode TOOLS' LIST](#)

Results

	11	11
(A=1)	LETTERNUMINPCAP	
(A=1, A=27)	UTTERNUMINPCAP	
(A=01)	L5TT5RNUM9NP31P	
(A=26...01)	O5GG5IMFN9MK31K	
(A=0)	MFUUF5OVNJOQDBQ	
(A=0, A=26)	VUUF5OVNJOQDBQ	
(A=26...1)	OVGGVIMFNRMKXZK	

#7

Cryptography › Substitution Cipher
› Letter Number Code (A1Z26) A=1, B=2, C=3

NUMBER TO LETTER A1Z26 CONVERTER

★ LETTER TO ALPHABET NUMBER A1Z26 CIPHERTEXT (NUMBERS) ?
125 20 20 5 18 14 21 13 9 14 16 3 1 16

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

★ CODE FOR 'SPACE' CHARACTER 0

★ DECRYPTION ?
☒ AUTOMATIC (BASIC CASES) ?
☐ BRUTE-FORCE (W/O SEPARATOR) ?

▶ DECRYPT

See also: Word's Value – T9 (Text Message) – Cryptarithm Solver

Similar

- ★ Number to Letter Converter
- ★ Letter to Number Converter
- ★ Calculate
- ★ What is the (Definition)
- ★ How to encode
- ★ to-Number/A
- ★ low to de
- ★ er cipher
- ★ low to re
- ★ Number ciph
- ★ What are
- ★ Letter-to-Nu



Doc:

Congrats kid, you won your first piston cup with the correct flag.



Challenge

233 Solves

Writeups

♥ 6 ✕

Shark Of Wire 2 20

I lose my network data again... Luckily I always got a [backup pcap file](#)! Please help me find my "flag" its important!

Flag format: SKR{flag}

Note: *There were some stego and crypto elements*

Difficulty: **Medium**

View Hint

View Hint

SKR{LETTERNUMINPCAP}

Submit

You already solved this and the flag is correct