

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}

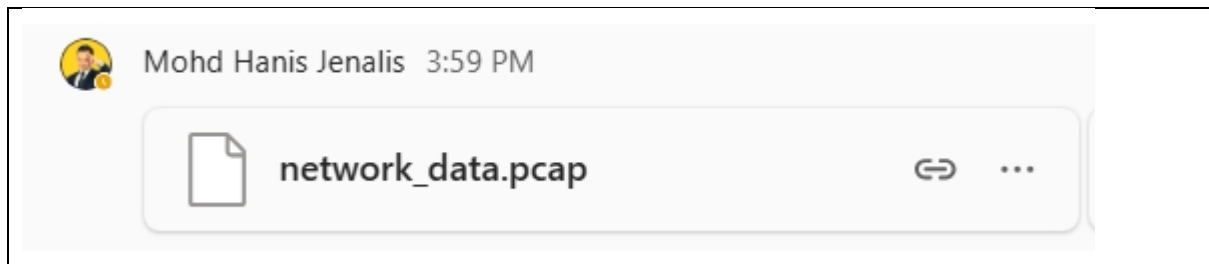
Note: There were some stego and crypto elements

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)



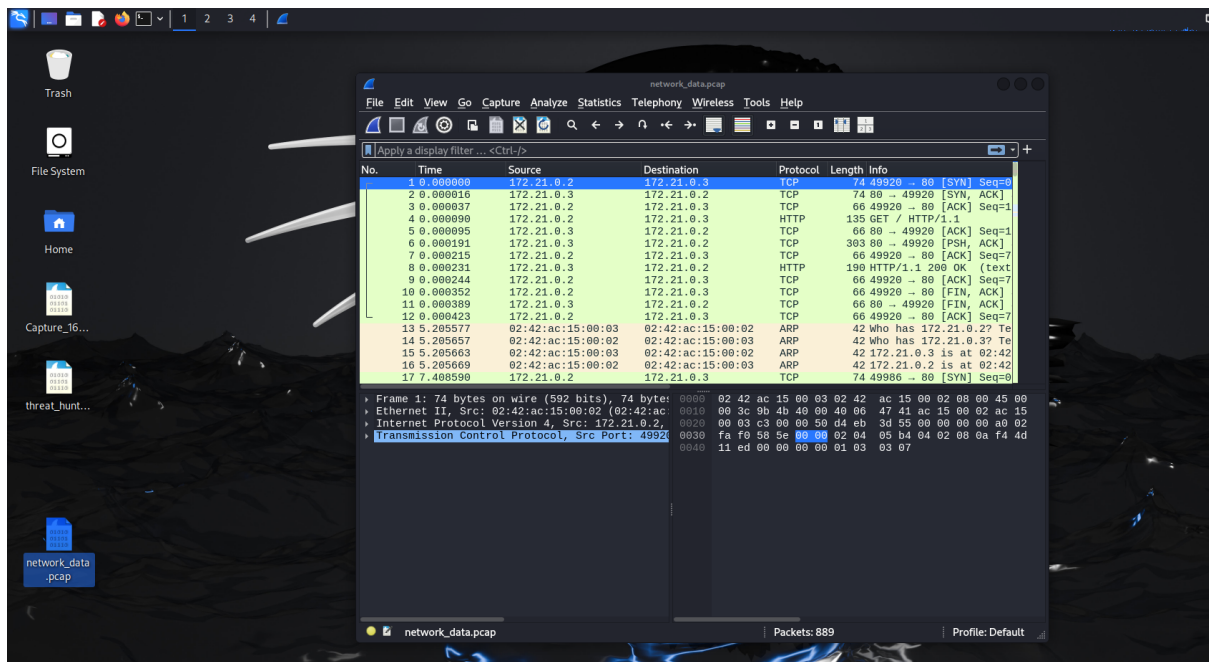
My Friend will roleplay as The King(former champion racer)



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 hierachy

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 displays two screenshots from the Wireshark network traffic analysis tool. The left screenshot shows a packet list for 'tcp.stream eq 0' with 12 packets. Packet 8 is highlighted, showing an HTTP 200 OK response from 172.21.0.3 to 172.21.0.2. The right screenshot shows the details of this packet, displaying the HTTP response structure including headers like 'Server: nginx/1.17.3', 'Date: Wed, 08 Apr 2020 17:17:38 GMT', and 'Content-Type: text/html'. The body of the response is an HTML document with a title 'Flag' and a body containing the text 'SKR(Not that easy anymore)'.

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=
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=

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

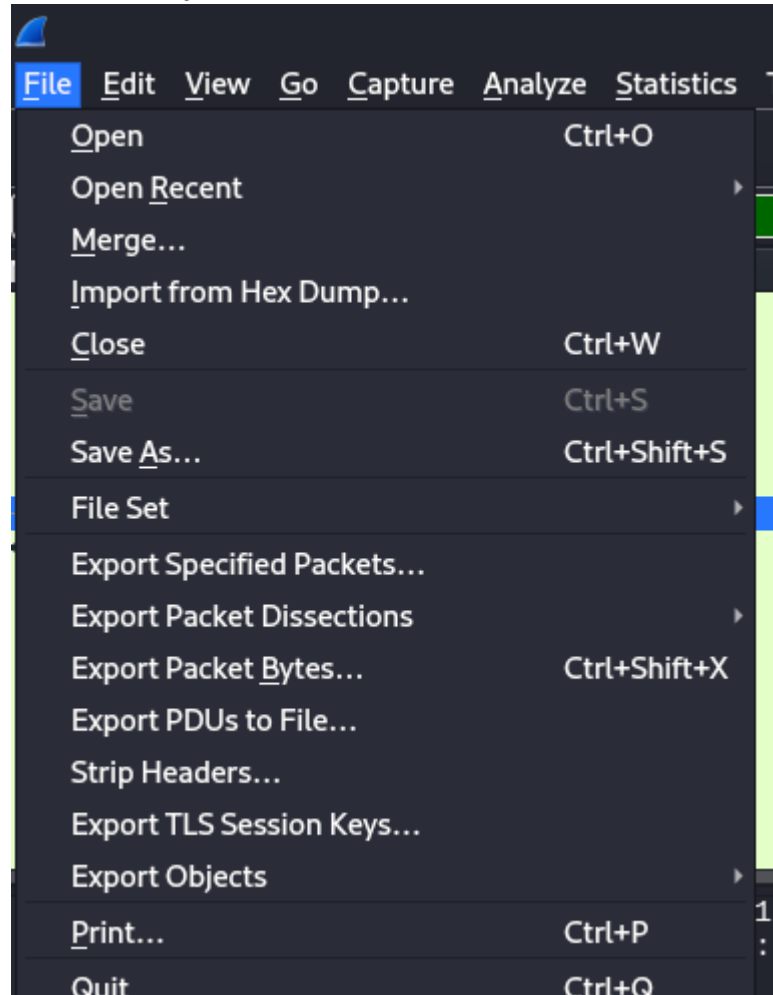
HTTP/1.1 200 OK
Server: nginx/1.17.3
Date: Wed, 08 Apr 2020 17:17:38 GMT
Content-Type: text/html
Content-Length: 124
Last-Modified: Wed, 08 Apr 2020 08:37:55 GMT
Connection: keep-alive
Etag: "5e8dbd63-7c"
Accept-Ranges: bytes

<!DOCTYPE html>
<html>
<head>
<title>Flag</title>
</head>
<body>
<h1>Flag: SKR(Not that easy anymore)</h1>
</body>
</html>
```

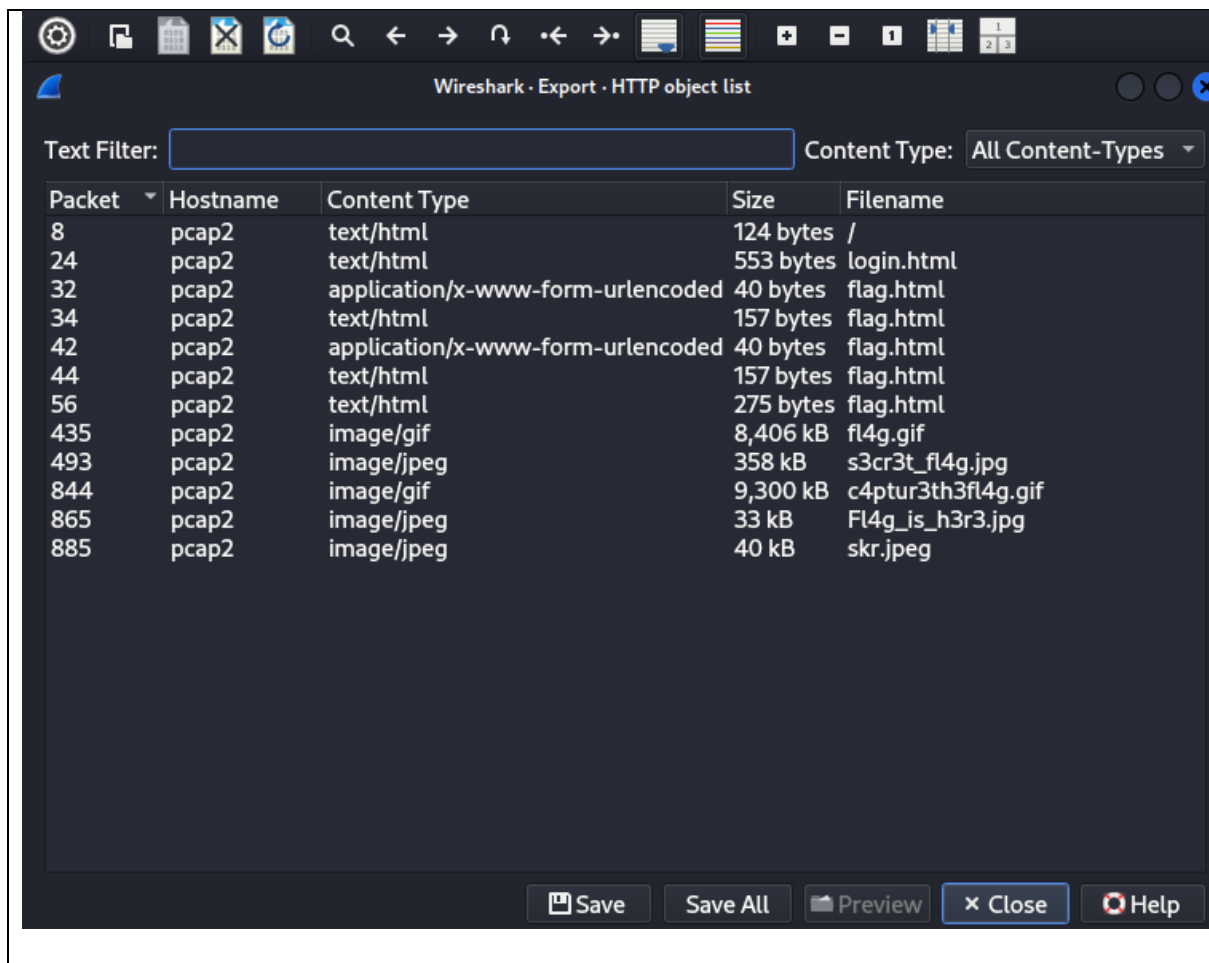


Doc:

Hahaha kid, you are still too naïve.



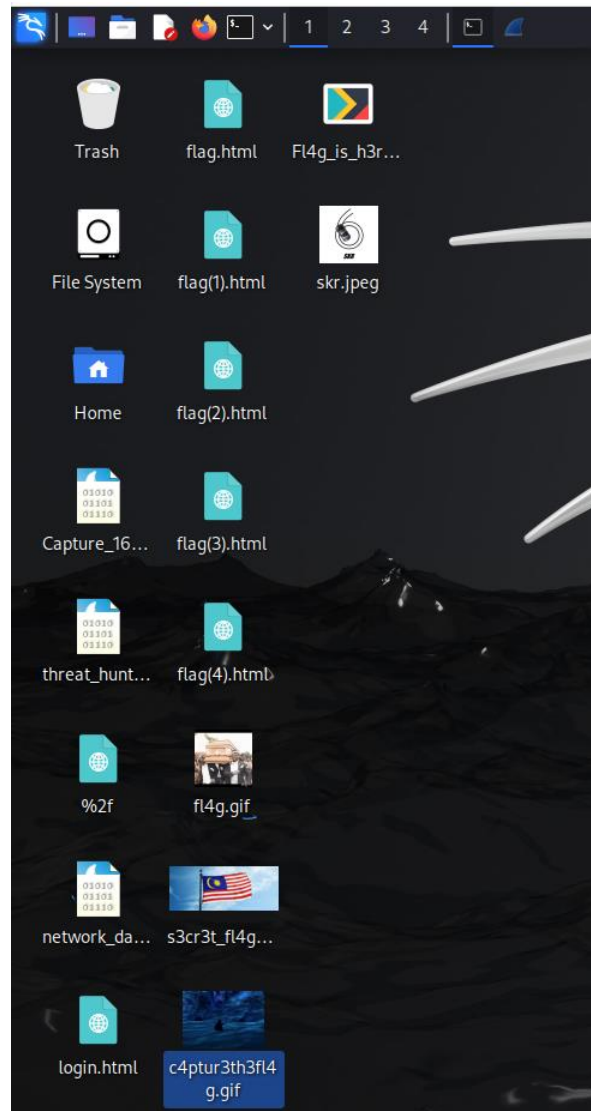
First, go to exports objects -> http -> save all





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_fl4...

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

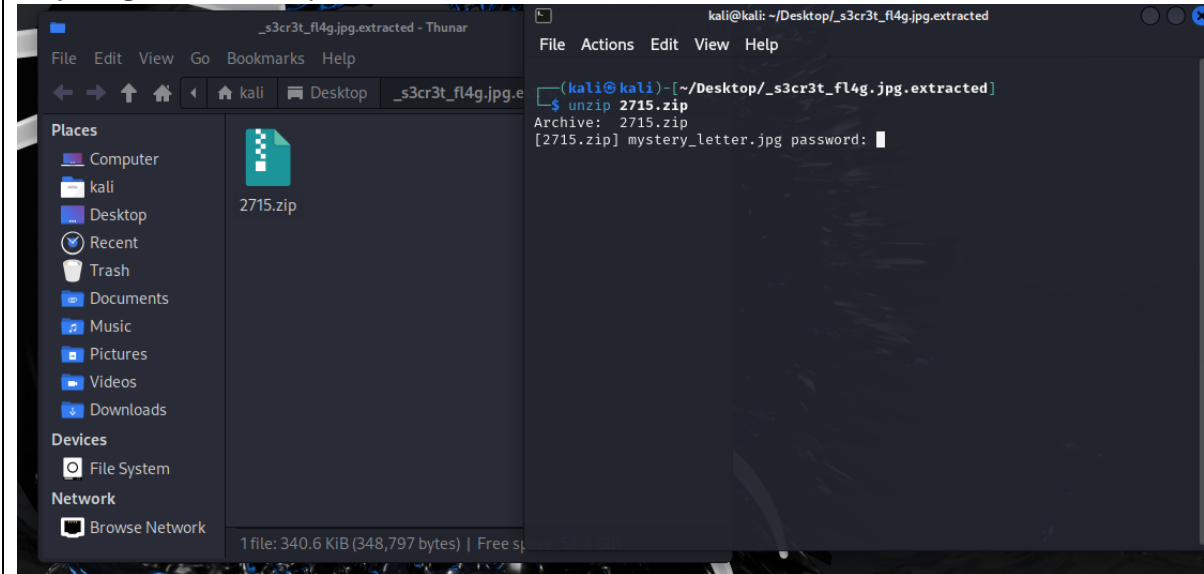
DECIMAL	HEXADECIMAL	DESCRIPTION
358780	0x5797C	End of Zip archive, footer length: 22

Then, I unzip it



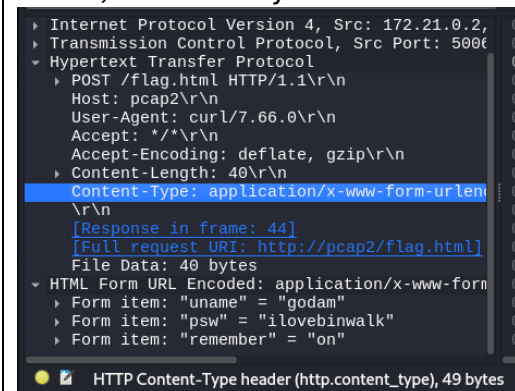
McQueen:

Hey King, what is the password.



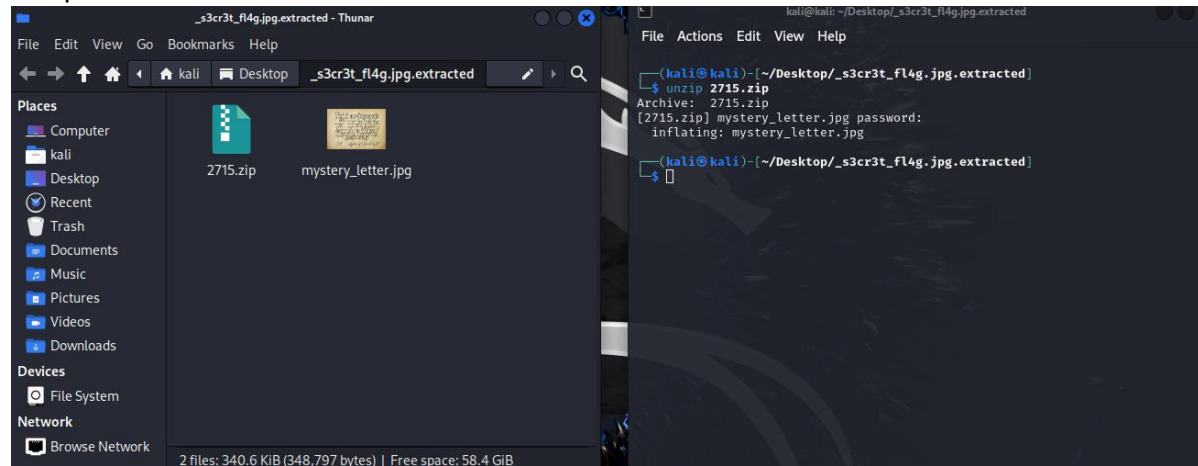
The King(Strip Weathers):

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 anlyze 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
```



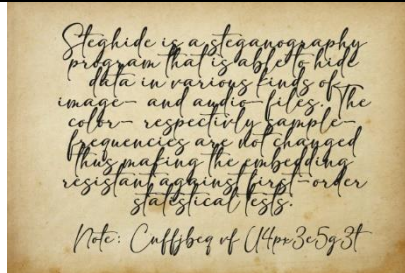
McQueen:

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.



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 Phssword is H4ck3r5t3g cnffjbeq

