

LinkedIn: [Kelvin Kimotho](#)

GitHub: [Kelvin Kimotho](#)

Wireshark doo dooo do doo...



Medium

Forensics

picoCTF 2021

AUTHOR: DYLAN

Hints ?

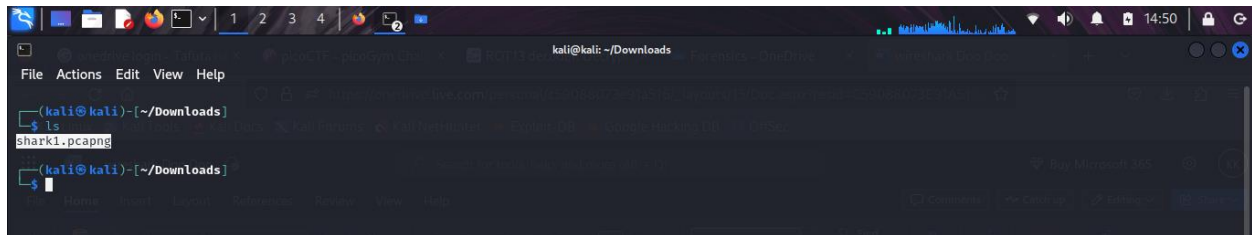
Description

(None)

Can you find the flag? [shark1.pcapng](#).

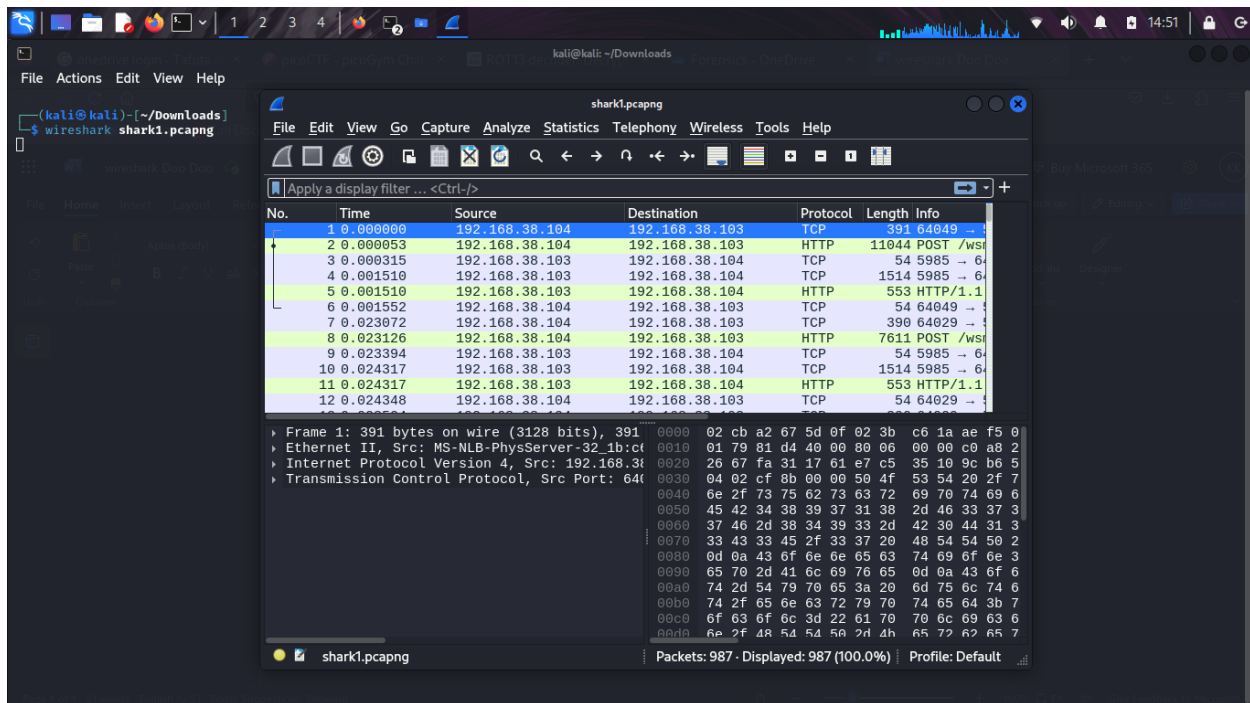
Solution

I began by downloading the **pcap** file.

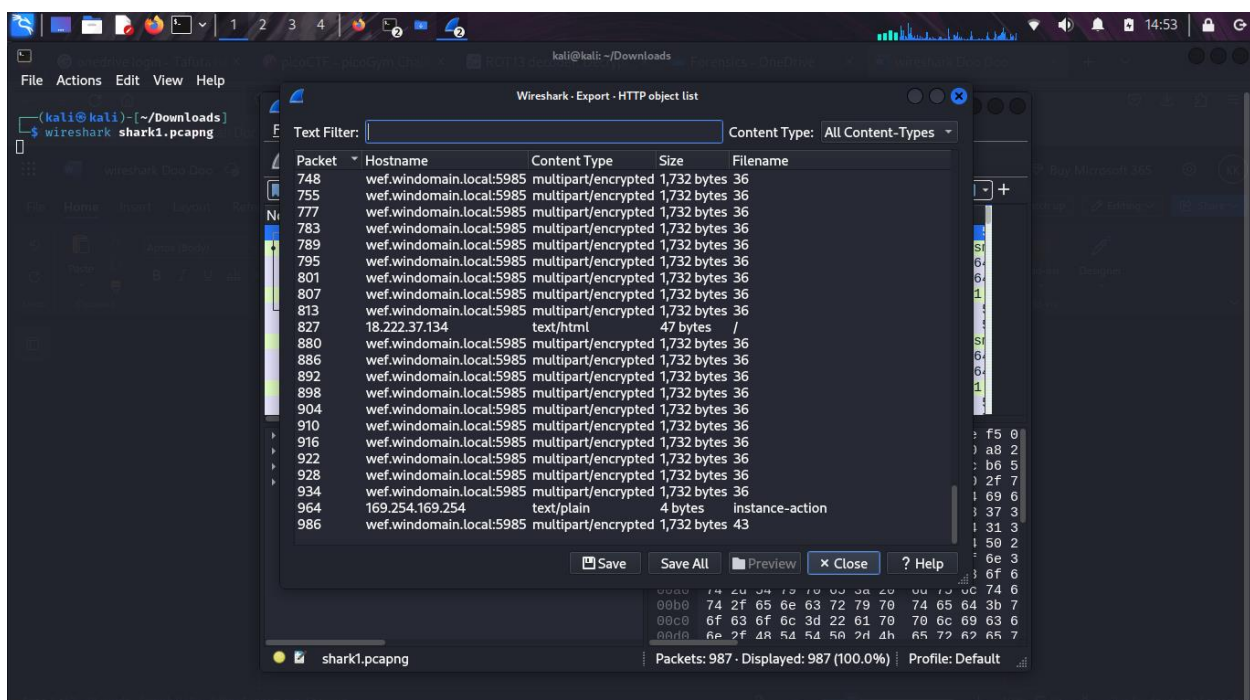


```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~/Downloads]
$ ls
shark1.pcapng
(kali@kali)-[~/Downloads]
$
```

I then opened the capture file using **wireshark**.

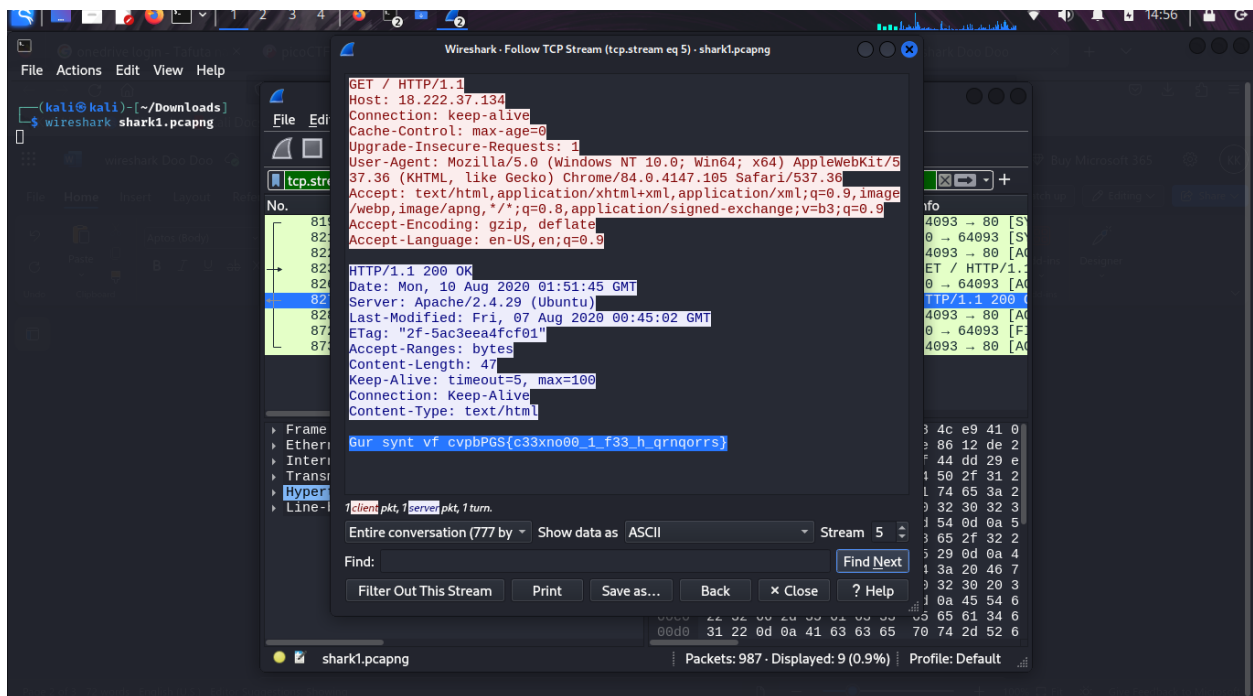


The capture had 987 packets. I went ahead looking for files that might have been shared over the network involving all the Ip addresses in the capture. I found nothing Interesting.



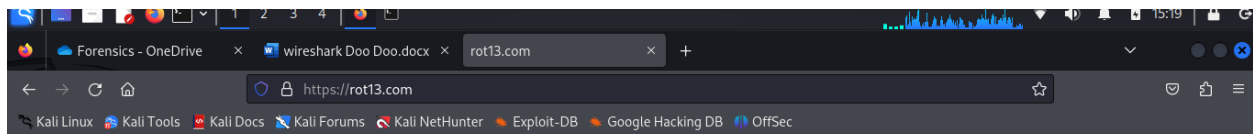
I went ahead analyzing each and every packet where I came across some text that resembled the picoCTF{...} flag format. I followed the analyze tab on Wireshark then followed the available

stream "tcp stream" and after navigating through several streams I came across one that contained something interesting.



This string "Gur synt vf cvpbPGS{c33xno00_1_f33_h_qrnqorrs}"

Appeared to be a rotational encoding. I tried using online tools to decode the encoding.



rot13.com

[About ROT13](#)

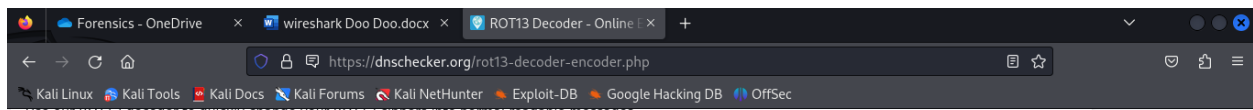
```
Gur synt vf cvpbPGS{c33xno00_1_f33_h_qrnqorr}
```



ROT13 ▾



The flag is `picoCTF{p33kab00_1_s33_u_deadbeef}`



Use our ROT13 decoder to quickly change your ROT13 ciphers into normal readable messages.



Choose Your Plan Now

Open

ROT-13 ▾

Input Text

```
Gur synt vf cvpbPGS{c33xno00_1_f33_h_qrnqorr}
```

Result

The flag is `picoCTF{p33kab00_1_s33_u_deadbeef}`



And that's how i found the flag `picoCTF{p33kab00_1_s33_u_deadbeef}`.