Wireshark doo dooo do doo…

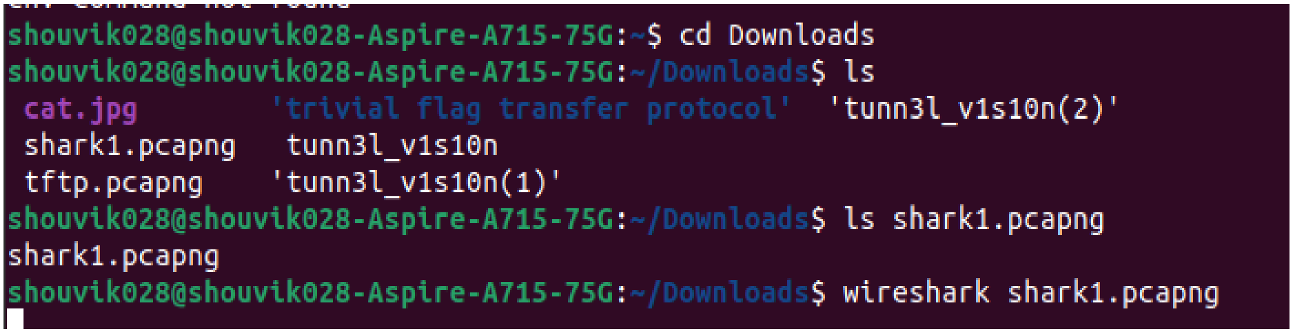
Forensics

Description

Can you find the flag? Shark1.pcapng.

Solution:

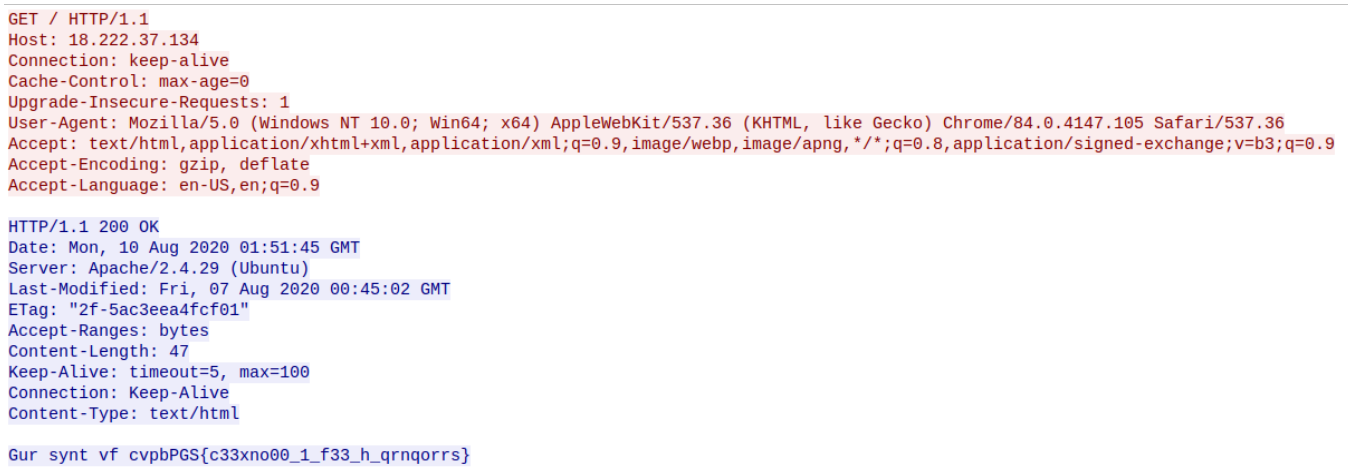
1) Open the file in wireshark.



```
shouvik028@shouvik028-Aspire-A715-75G:~$ cd Downloads
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads$ ls
 cat.jpg        'trivial flag transfer protocol'   'tunn3l_v1s10n(2)'
 shark1.pcapng   tunn3l_v1s10n
 tftp.pcapng    'tunn3l_v1s10n(1)'
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads$ ls shark1.pcapng
shark1.pcapng
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads$ wireshark shark1.pcapng
```

2) Click on TCP Stream.

3) The encoded flag will be shown as
   Gur synt vf cvpbPGS{c33xno00_1_f33_h_qrnqorrs}

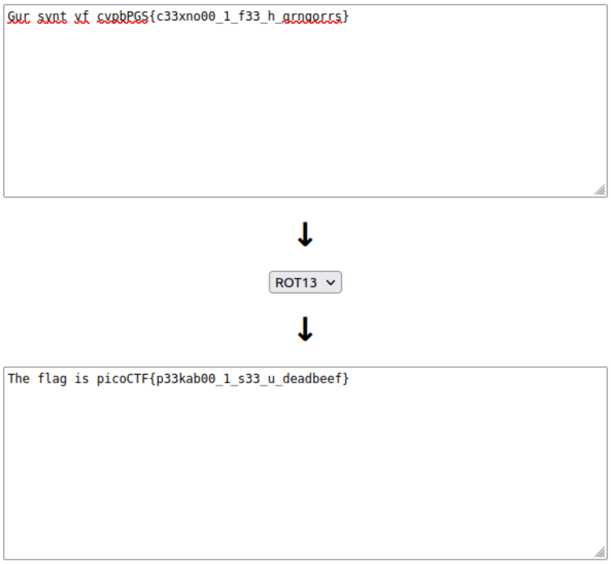


```
GET / HTTP/1.1
Host: 18.222.37.134
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Date: Mon, 10 Aug 2020 01:51:45 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Fri, 07 Aug 2020 00:45:02 GMT
ETag: "2f-5ac3eea4fcf01"
Accept-Ranges: bytes
Content-Length: 47
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Gur synt vf cvpbPGS{c33xno00_1_f33_h_qrnqorrs}
```

4) Use ROT13 to find the final flag.



```
Gur synt vf cvpbPGS{c33xno00_1_f33_h_qrnqorrs}
```

```
The flag is picoCTF{p33kab00_1_s33_u_deadbeef}
```

Flag: picoCTF{p33kab00_1_s33_u_deadbeef}