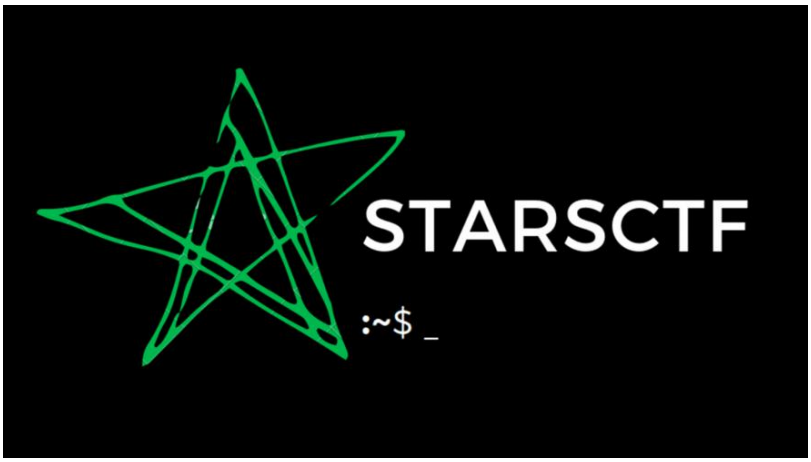

Name: Ajude o admin!
Category: Network
File: 1d7fdcab411184f372d9ee54ecf955de
Message:

A senha do admin foi vazada. Ajude-nos a encontrar!

Resolução:

Neste desafio estamos procurando por uma senha;
Temos um arquivo sem extensão.

Baixamos e usamos nosso conhecido comando *file* para descobrir a extensão:

```
shell3r@lhost:~/Downloads$ file 1d7fdcab411184f372d9ee54ecf955de
1d7fdcab411184f372d9ee54ecf955de: tcpdump capture file (little-endian) - version 2.4
(Ethernet, capture length 262144)
```

Image 1 - Comando file em arquivo

Se trata de um arquivo TCPDump, podemos ler com a ferramenta *WireShark* usando o comando:

```
wireshark -r 1d7fdcab411184f372d9ee54ecf955de
```

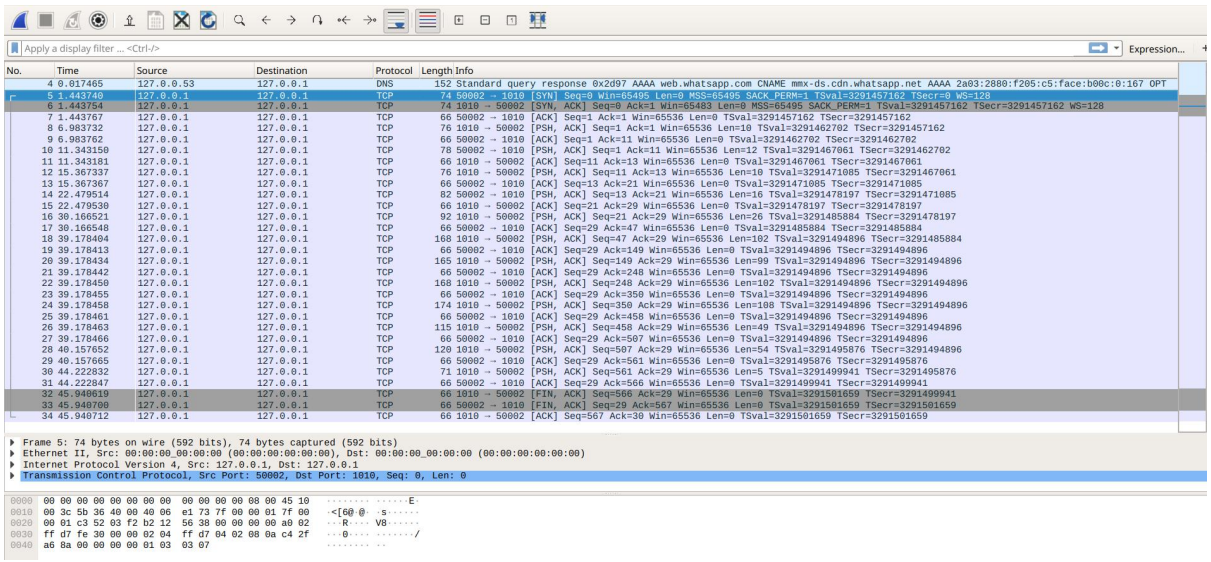

Image 2 - Arquivo TCPDump pelo Wireshark

Nessa captura de pacotes de rede, temos apenas uma requisição TCP. Para visualisarmos melhor usamos a opção *TCP Stream*:

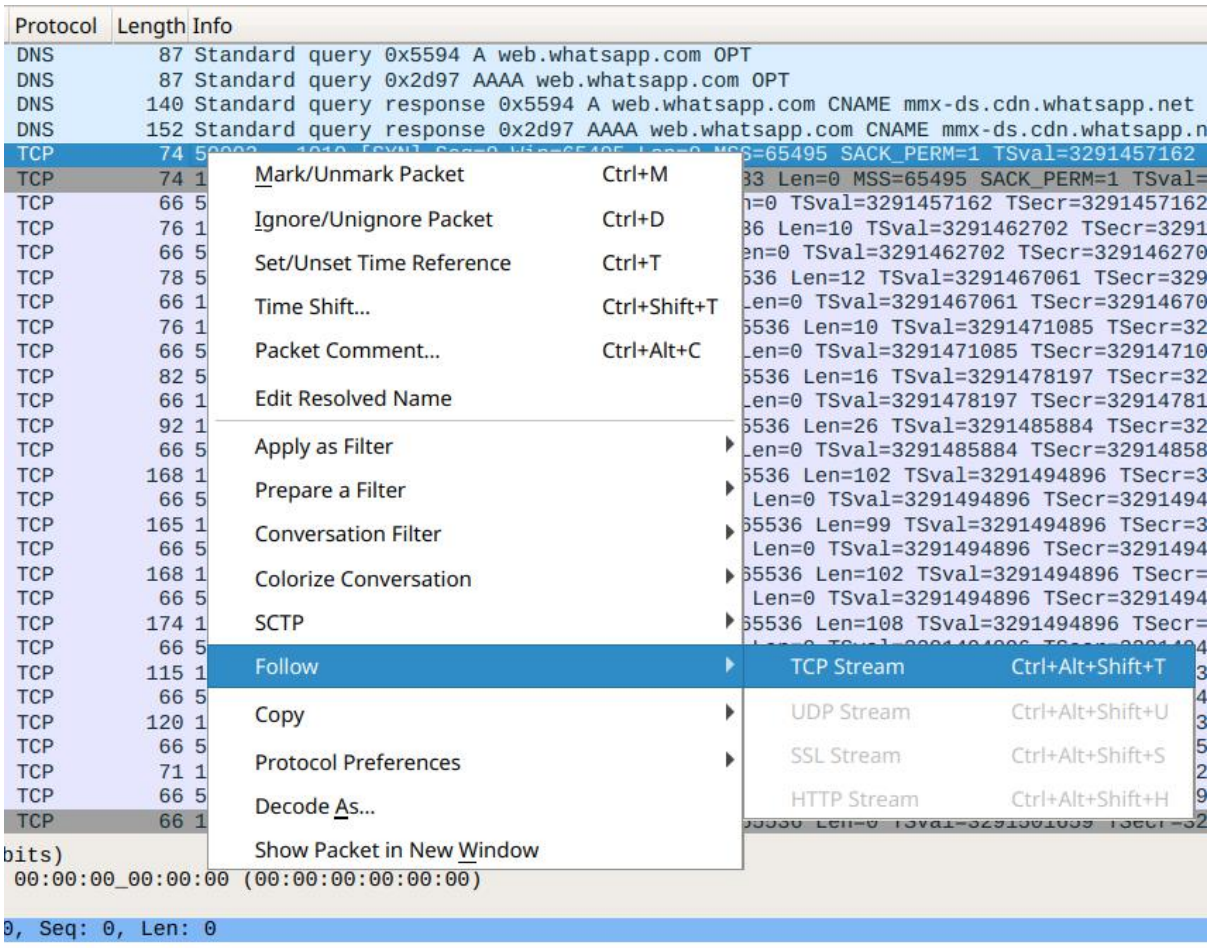

Image 3 - TCP Stream no Wireshark

```
Username:
myusername
Password:
MyP@ss!aoba!01
Logged in! Listing files:
-rwsr-xr-x 1 root root   67816 mar  5 14:23 su
-rwxr-xr-x 1 root root   18664 mar  5 14:23 mountpoint
-rwsr-xr-x 1 root root   55528 mar  5 14:23 mount
-rwxr-xr-x 1 root root   43160 mar  5 14:23 more
-rwxr-xr-x 1 root root  133352 mar  5 14:23 lsblk
-rwxr-xr-x 1 root root   73128 mar  5 14:23 findmnt
-rwxr-xr-x 1 root root   84440 mar  5 14:23 dmesg
lrwxrwxrwx 1 root root       4 mar 11 16:32 lsmod -> kmod
-rwxr-xr-x 1 root root  166232 mar 11 16:32 kmod
-rwxr-xr-x 1 root root  196792 mar 23 09:25 hciconfig
Bye!
```

Image 4 - TCP Stream no Wireshark 2

Achamos então, o *username* e *password* do usuário.

E aqui está nossa flag;

Flag(*MyP@ss!aoba!01***)**

Pesquisas:
encurtador.com.br/ipEOY