Forensics: Eat_pcap

Description

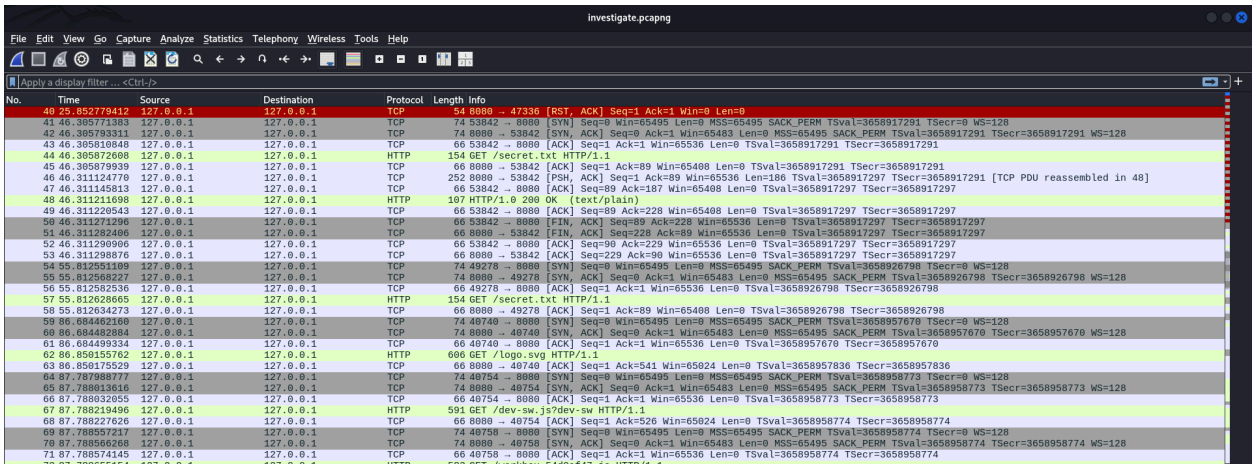
My Teacher told me https is more secure than http traffic. Thank you sir!!!

Approach

This is the pcap file investigation challenge

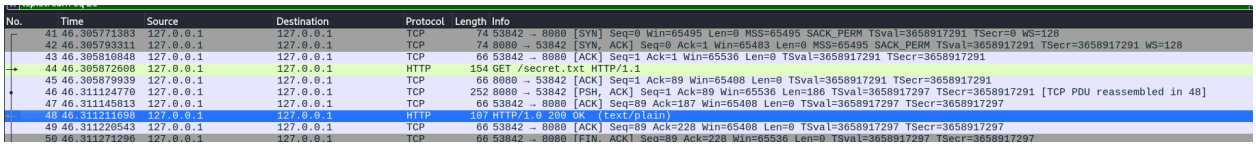
Step 1:

Open the given Pcap file in wireshark



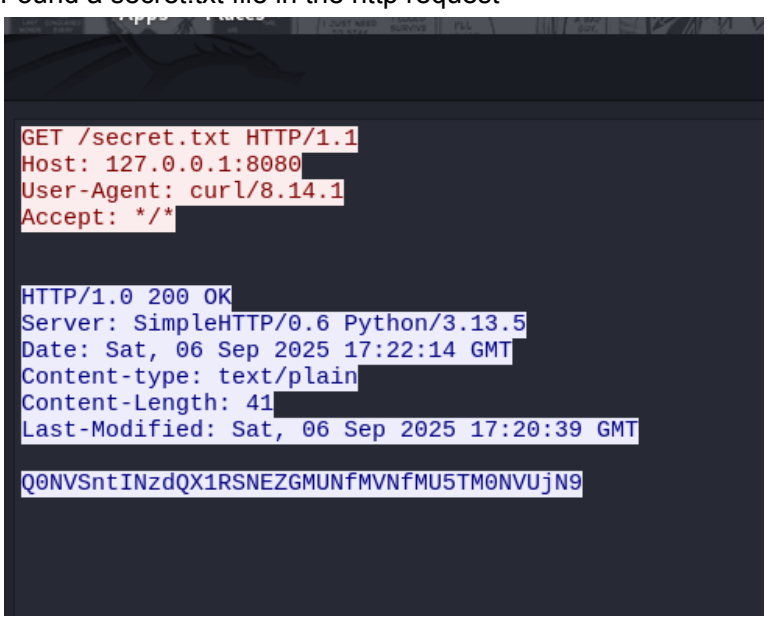
Step2

Search for any http or FTP traffic



Step 3:

Found a secret.txt file in the http request



Step 4:
the file contain a string value most probably base64 So, encode it

```
└─$ echo -n 'Q0NVSntINzdQX1RSNEZGMUNfMVNfMU5TM0NVUjN9' | base64 -d
CCUJ{H77P_TR4FF1C_1S_1NS3CUR3}
```

Flag: CCUJ{H77P_TR4FF1C_1S_1NS3CUR3}