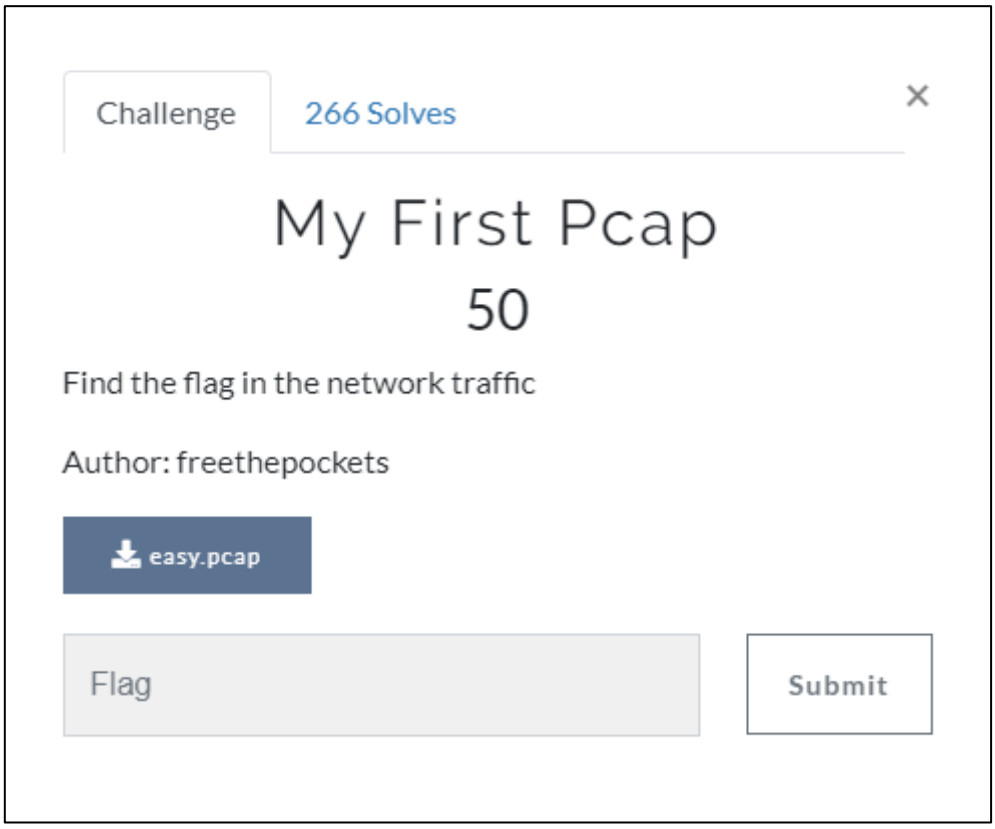
Forensics : My First Pcap 50

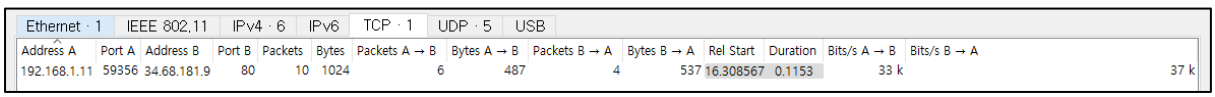
Description : Find the flag in the network traffic

Attachment : easy.pcap

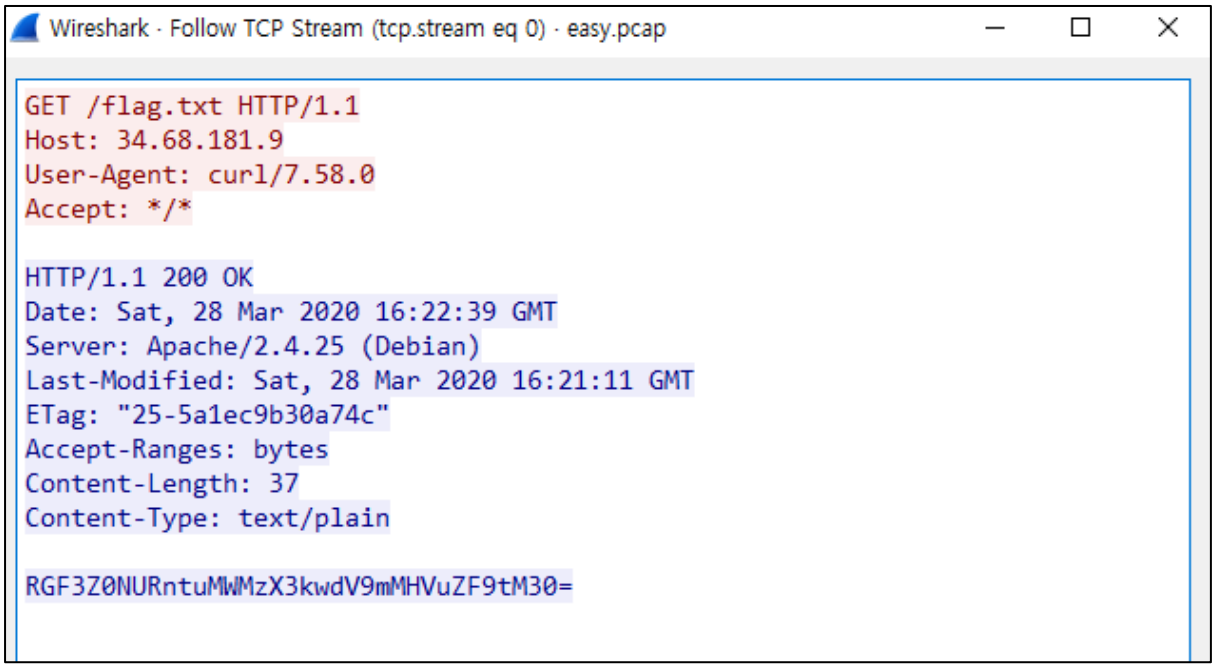


Solutions :

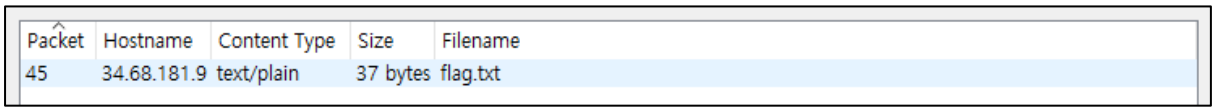
1. Opening Attachment file in WireShark.
2. Check the packet in conversation.



3. See the packet movement in TCP and follow stream.



4. Extract flag.txt file.

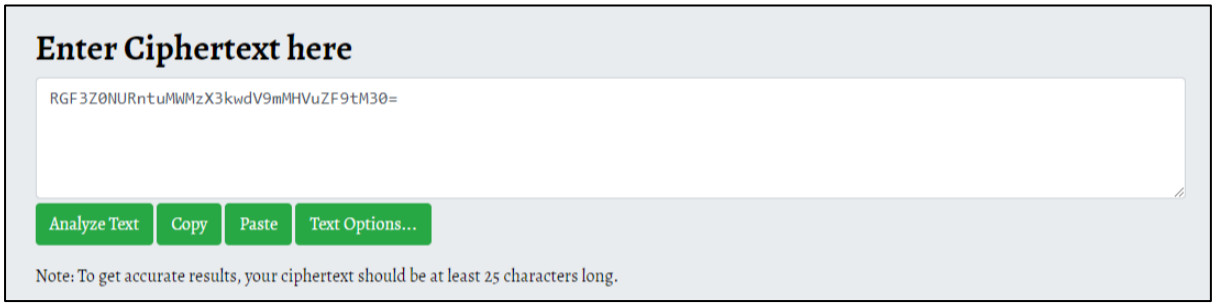


Packet	Hostname	Content Type	Size	Filename
45	34.68.181.9	text/plain	37 bytes	flag.txt

5. The contents of the file are the same as those found in the packet.

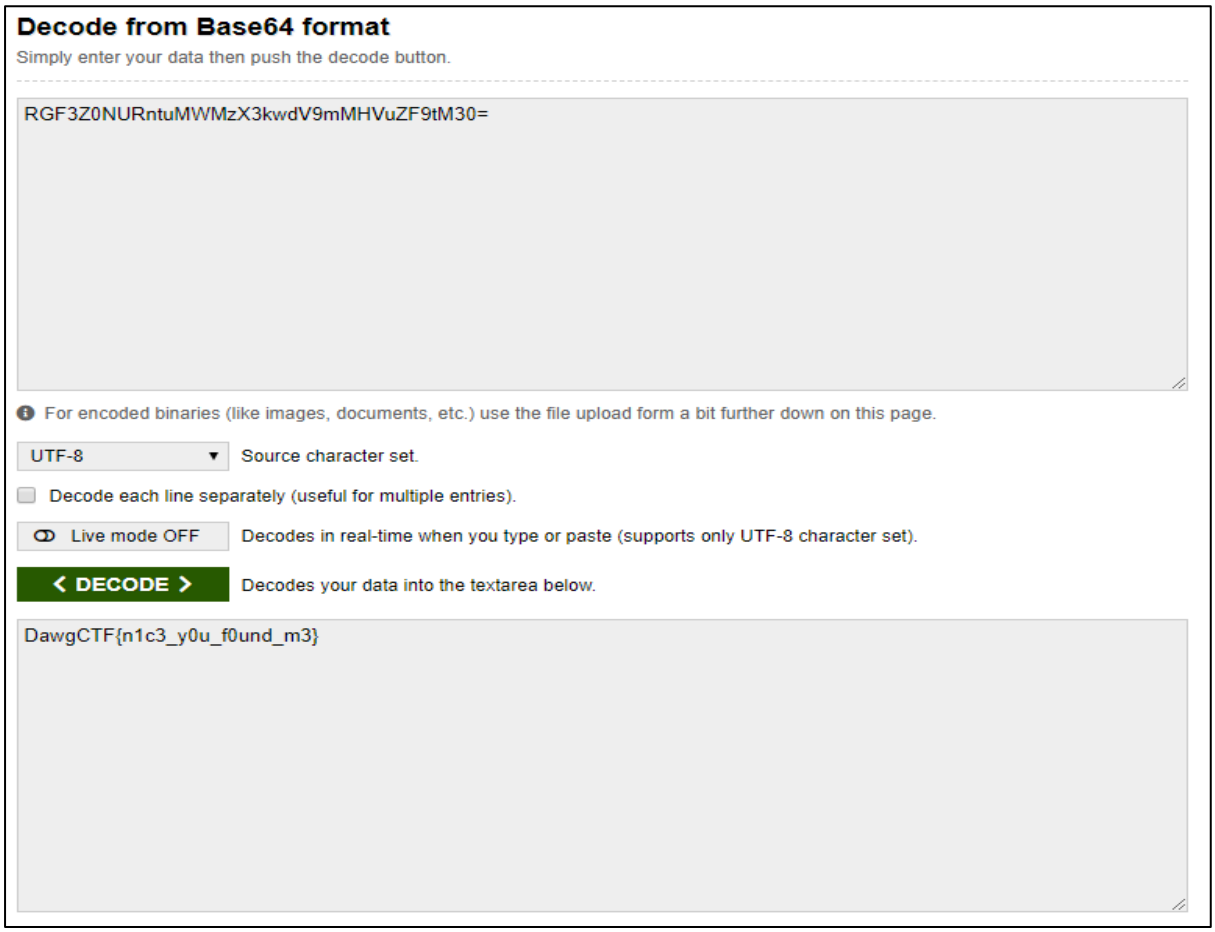
```
RGF3Z0NURntuMWMzX3kwdV9mMHVuZF9tM30=
```

6. However, since the flag is encrypted, the encryption type is detected and decrypted.



7. Encryption type is Base64.

8. Thus, when decrypting this ciphertext, the flag is appeared.



9. Flag is DawgCTF{n1c3_y0u_f0und_m3}

Flag : DawgCTF{n1c3_y0u_f0und_m3}