Category: Miscellaneous
Challenge: Mission: "Sabanci"

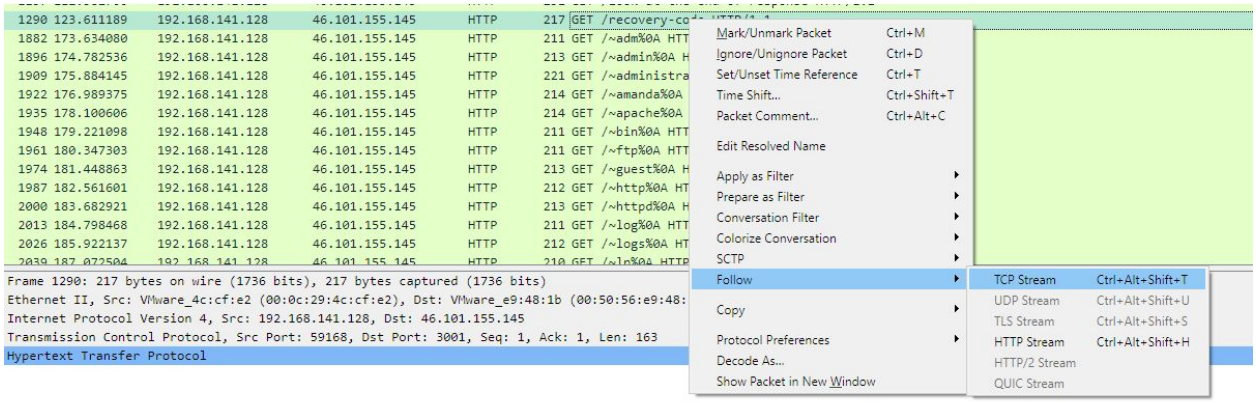
Write-up:

We need to connect with Netcat to start the challenge.

After making some choices that are not requiring any cyber-security knowledge, we encounter a network forensics challenge.

```
1856 171.420293    192.168.141.128    46.101.155.145    HTTP    215 GET /_vti_txt%0A HTTP/1.1
1869 172.530047    192.168.141.128    46.101.155.145    HTTP    211 GET /_www%0A HTTP/1.1
 897 90.346490     192.168.141.128    46.101.155.145    HTTP    228 GET /long-urls-are-suspicious HTTP/1.1
1157 112.582700    192.168.141.128    46.101.155.145    HTTP    231 GET /look-at-the-end-of-response HTTP/1.1
1290 123.611189    192.168.141.128    46.101.155.145    HTTP    217 GET /recovery-code HTTP/1.1
1882 173.634080    192.168.141.128    46.101.155.145    HTTP    211 GET /~adm%0A HTTP/1.1
1896 174.782536    192.168.141.128    46.101.155.145    HTTP    213 GET /~admin%0A HTTP/1.1
1909 175.884145    192.168.141.128    46.101.155.145    HTTP    221 GET /~administrator%0A HTTP/1.1
```

One can easily see the /recovery-code page. After following the TCP stream, we can see a base64 encoded string.



Encoded: "UmVjb3ZlcnkgY29kZSBpczogMTIzcmVjb3ZlcnkxMjM="
Decoded: **"Recovery code is: 123recovery123"**

When we enter this recovery code, the game continues. After making some choices, we are encountering some puzzle.
The code is: **"3024"**
After entering the code, we are given encoded data.

Encoded: **"HFXGU{I3hK3xg+}".** After some research, one can understand that it is a monoalphabetic cypher called Atbash. With decoding it with the Atbash Cipher scheme; **Flag is: SUCTF{R3sP3ct+}**