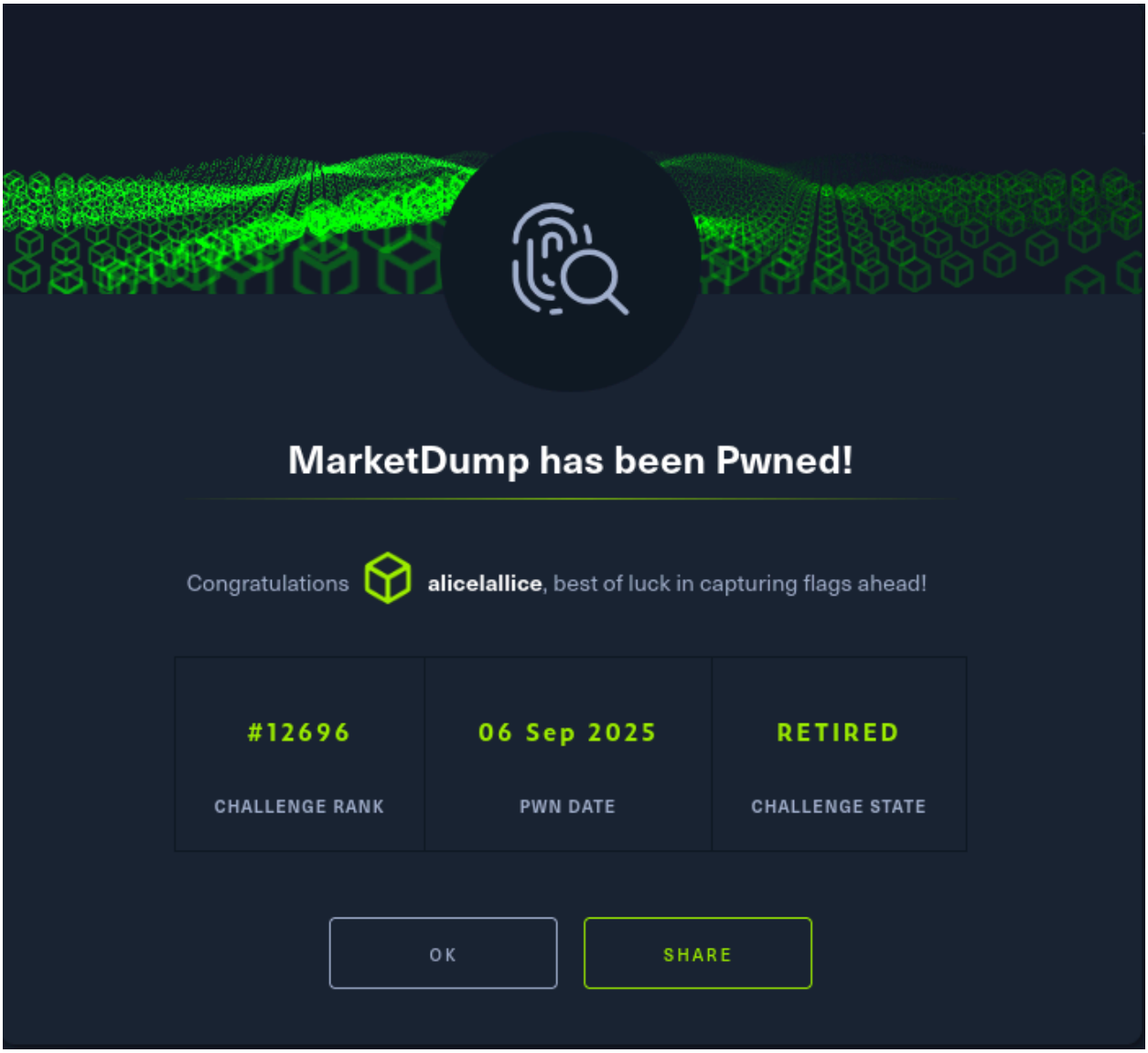
MarketDump

Types	forensic
CTF	HTB



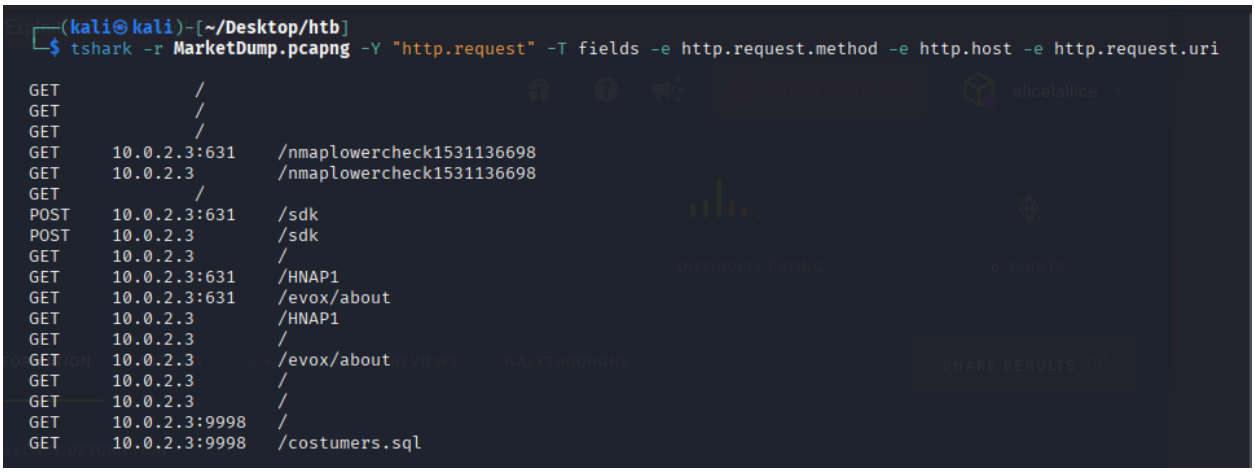
"In this challenge, we analyze a packet capture (`MarketDump.pcapng`) to identify how an attacker accessed and exfiltrated sensitive customer data. Our goal: find the targeted card number and reconstruct the attack path."

nitial Filtering

- **Command:**

  bash

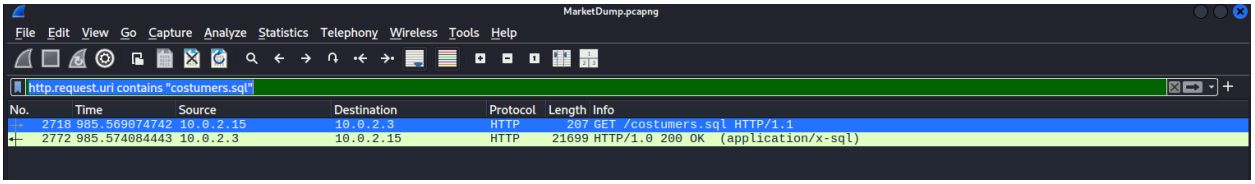
  ```
  tshark -r MarketDump.pcapng -Y "http.request" -T fields -e http.request.
  ```



Identifying the Sensitive File

`http.request.uri contains "costumers.sql"`

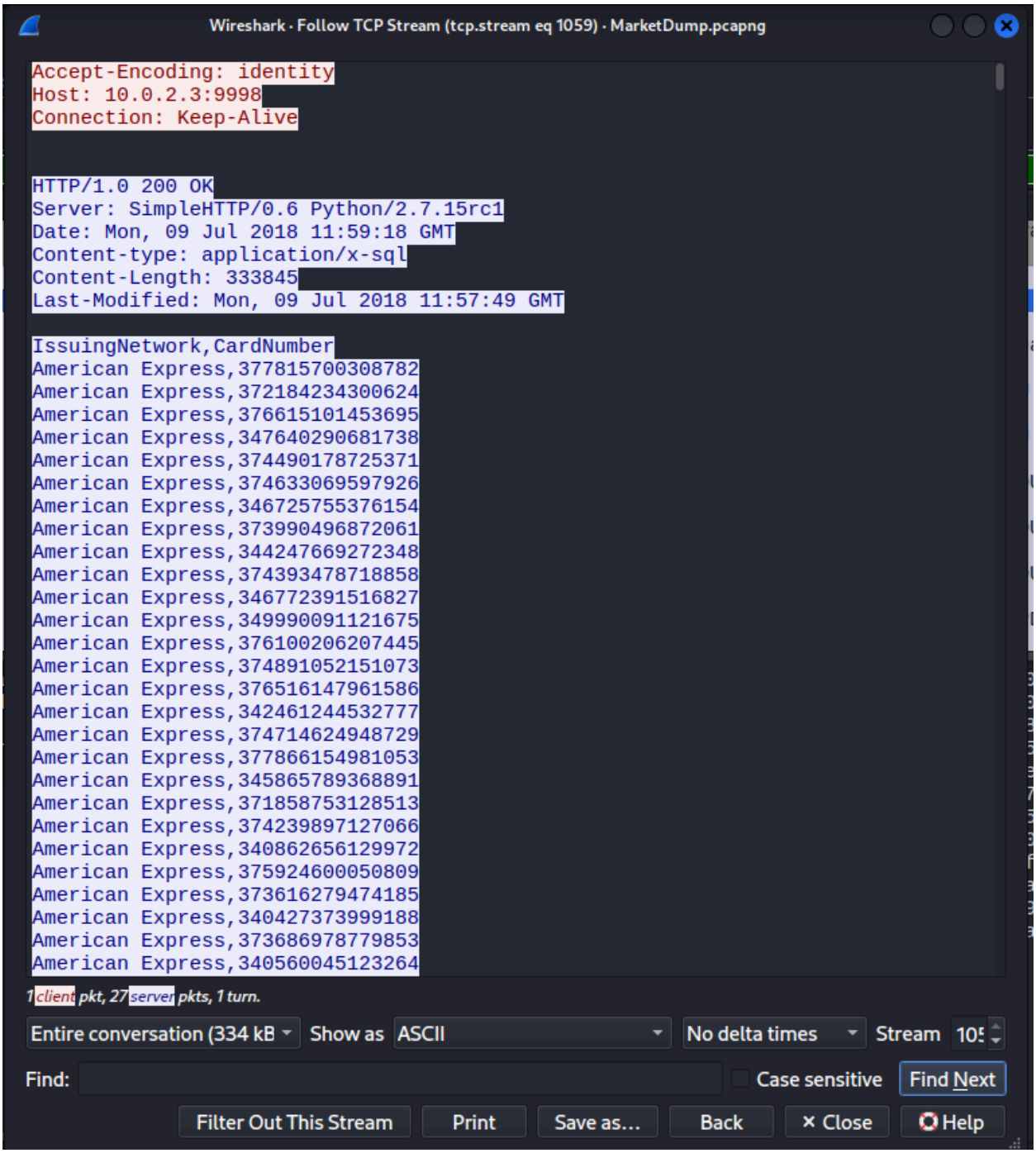
this command i use to filter in wireshark



and found our target at first line

To follow the full TCP stream:

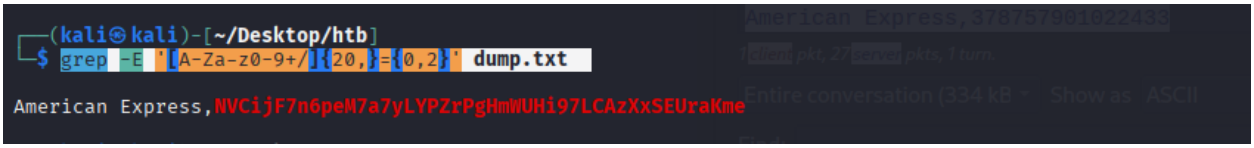
- Right-click the filtered packet → *Follow* → *TCP Stream*



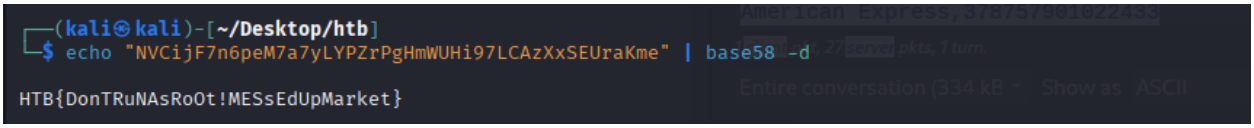
then i saved it as dump.txt

```
grep -E '[A-Za-z0-9+/]{20,}={0,2}' dump.txt
```

i use this command to grep any encryption



Decode it



HTB{DonTRuNAsRoOt!MESsEdUpMarket}

we found the flag!