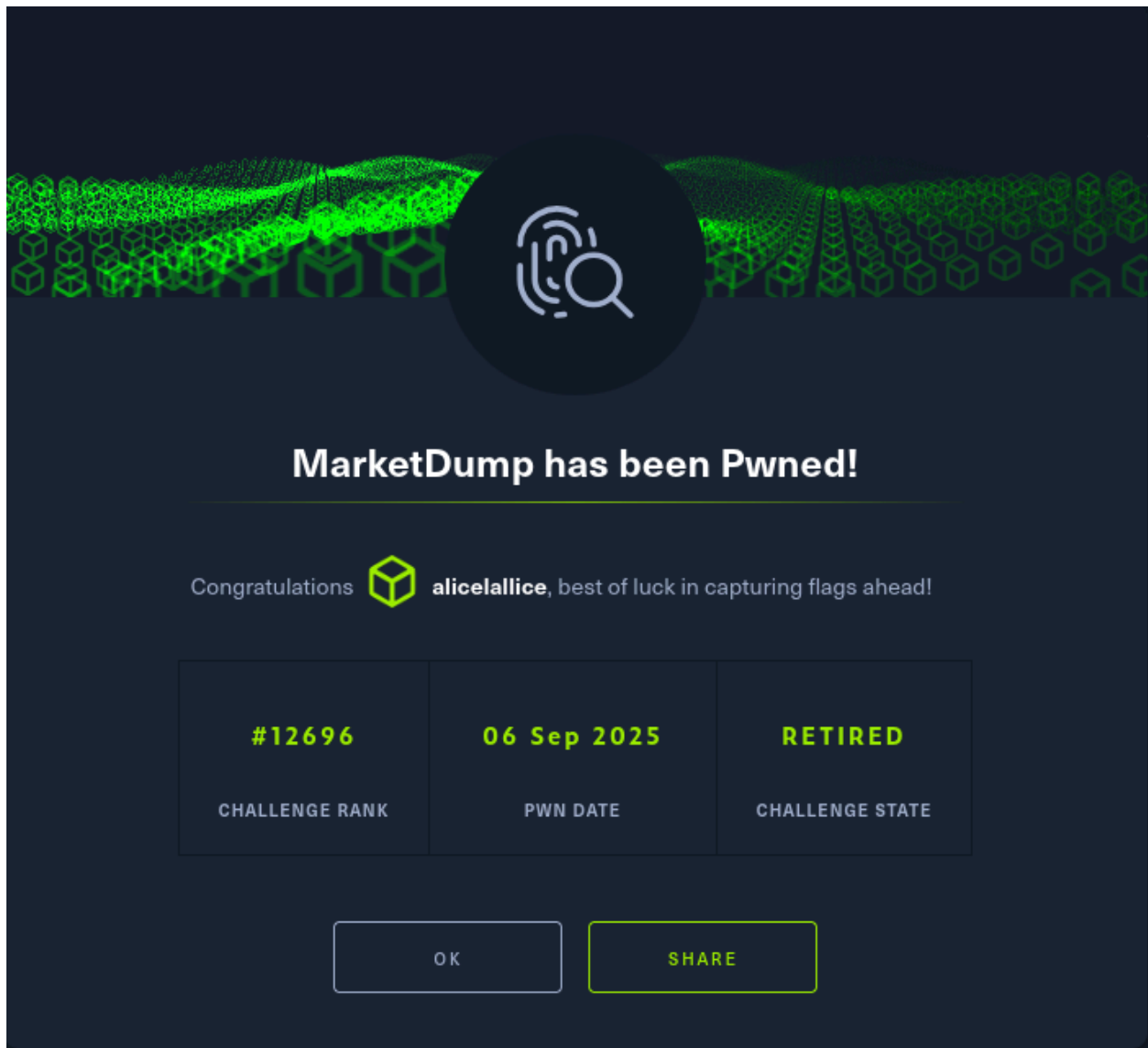


# MarketDump

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."*

## Initial Filtering

- **Command:**

bash

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

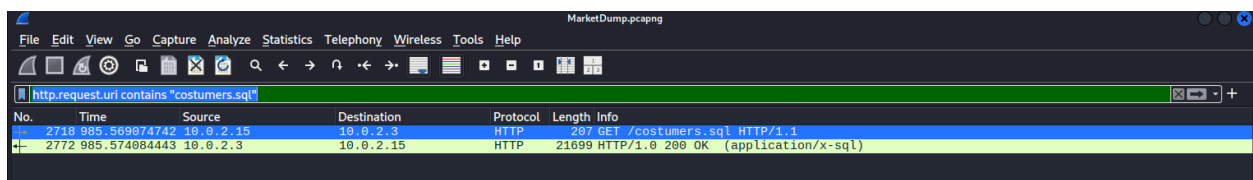
```
(kali@kali)-[~/Desktop/htb]
$ tshark -r MarketDump.pcapng -Y "http.request" -T fields -e http.request.method -e http.host -e http.request.uri

GET      /
GET      /
GET      /
GET      10.0.2.3:631 /nmaplowercheck1531136698
GET      10.0.2.3 /nmaplowercheck1531136698
GET      /
POST     10.0.2.3:631 /sdk
POST     10.0.2.3 /sdk
GET      10.0.2.3 /
GET      10.0.2.3:631 /HNAP1
GET      10.0.2.3:631 /evox/about
GET      10.0.2.3 /HNAP1
GET      10.0.2.3 /
GET      10.0.2.3 /evox/about
GET      10.0.2.3 /
GET      10.0.2.3 /
GET      10.0.2.3:9998 /
GET      10.0.2.3:9998 /costumers.sql
```

## Identifying the Sensitive File

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

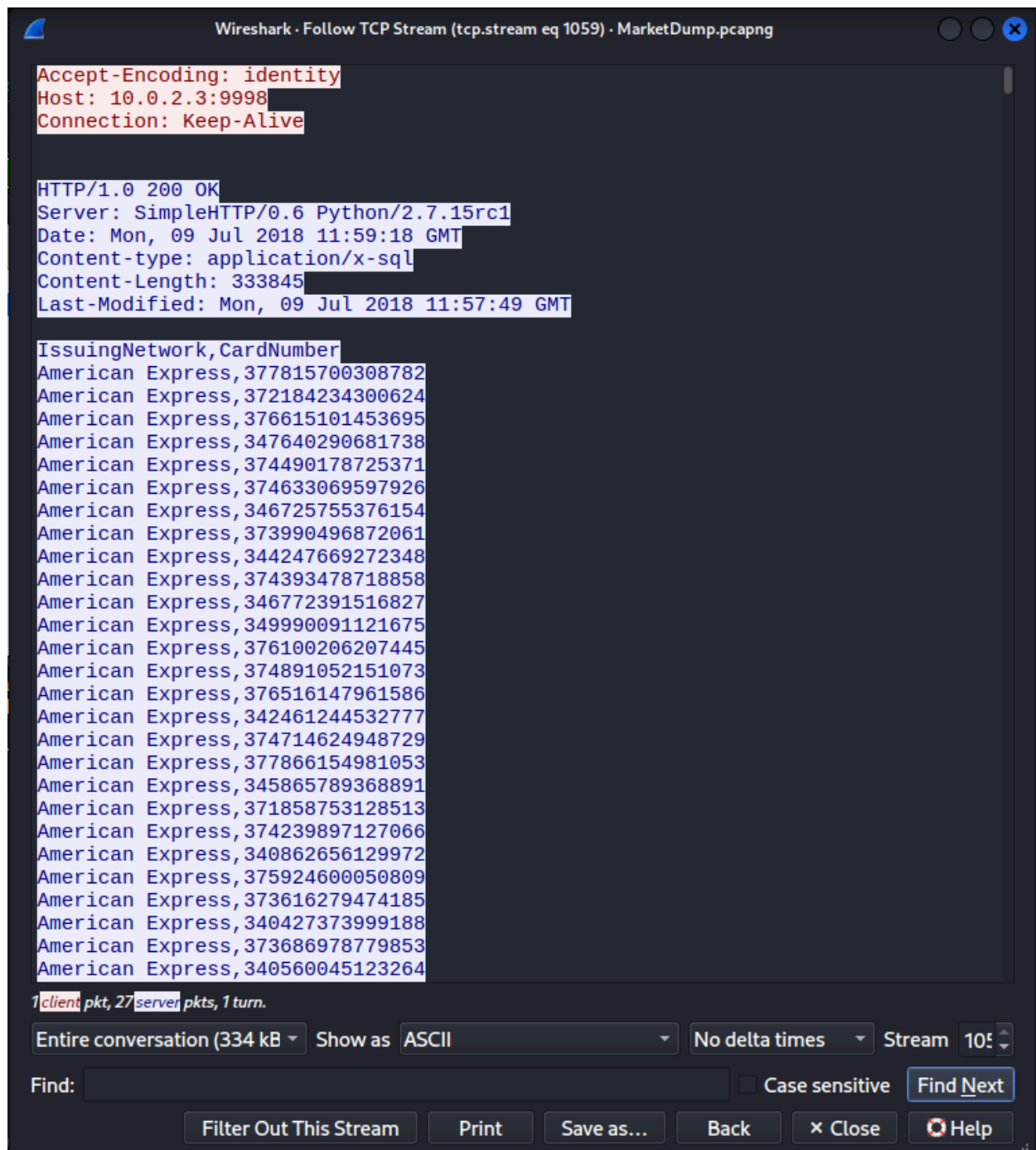
this command i use to filter in wireshark



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

```
(kali㉿kali)~[~/Desktop/htb]
$ grep -E '[A-Za-z0-9+/]{20,}={0,2}' dump.txt
American Express,NVCijF7n6peM7a7yLVPZrPgHmWUHi97LCAzXxSEUraKme
```

Decode it

```
(kali㉿kali)~[~/Desktop/htb]
$ echo "NVCijF7n6peM7a7yLVPZrPgHmWUHi97LCAzXxSEUraKme" | base58 --d
HTB{DonTRuNAsRoOt!MESsEdUpMarket}
```

HTB{DonTRuNAsRoOt!MESsEdUpMarket}

we found the flag!