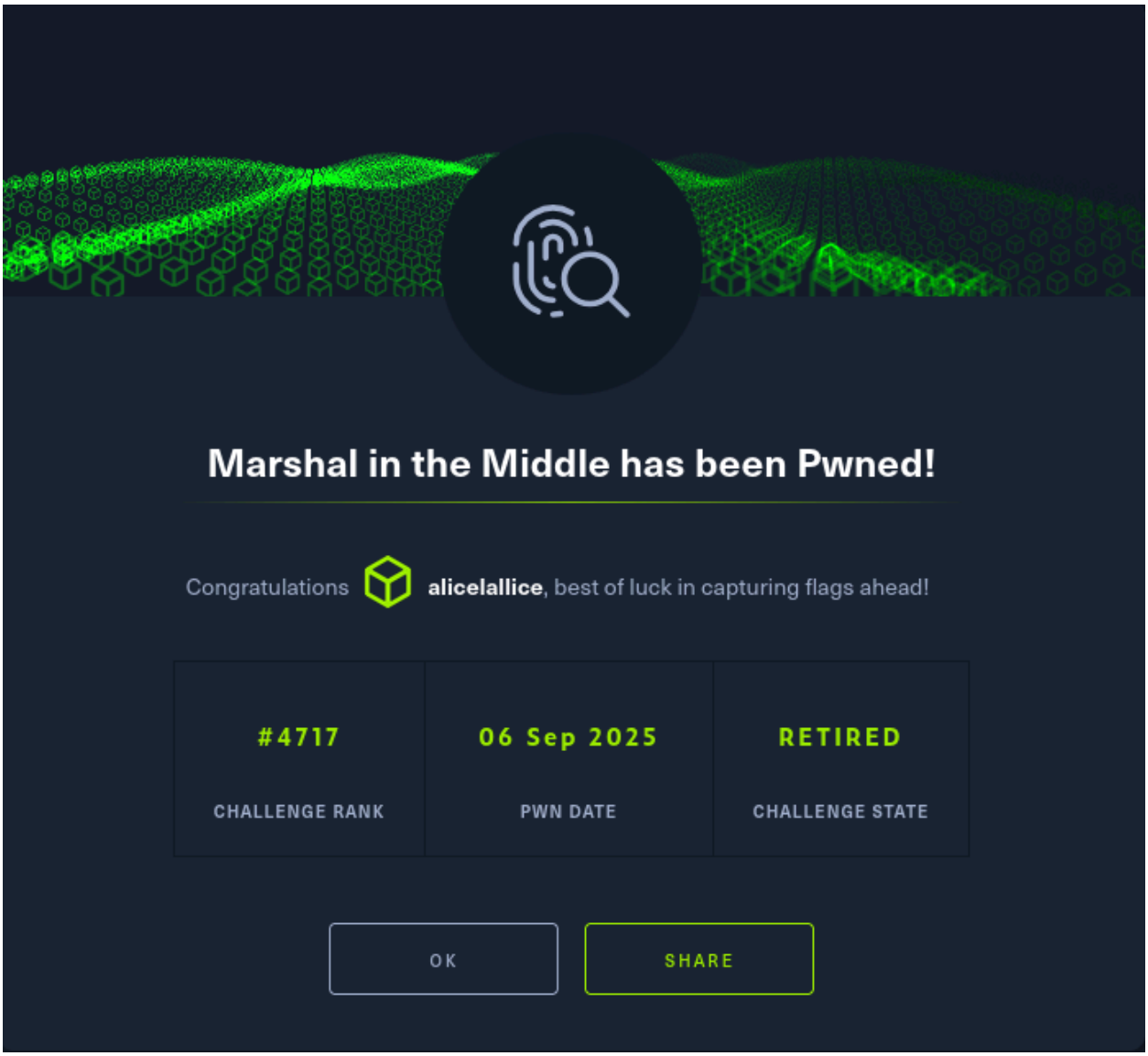
Marshal in the Middle

Types	forensic
CTF	HTB



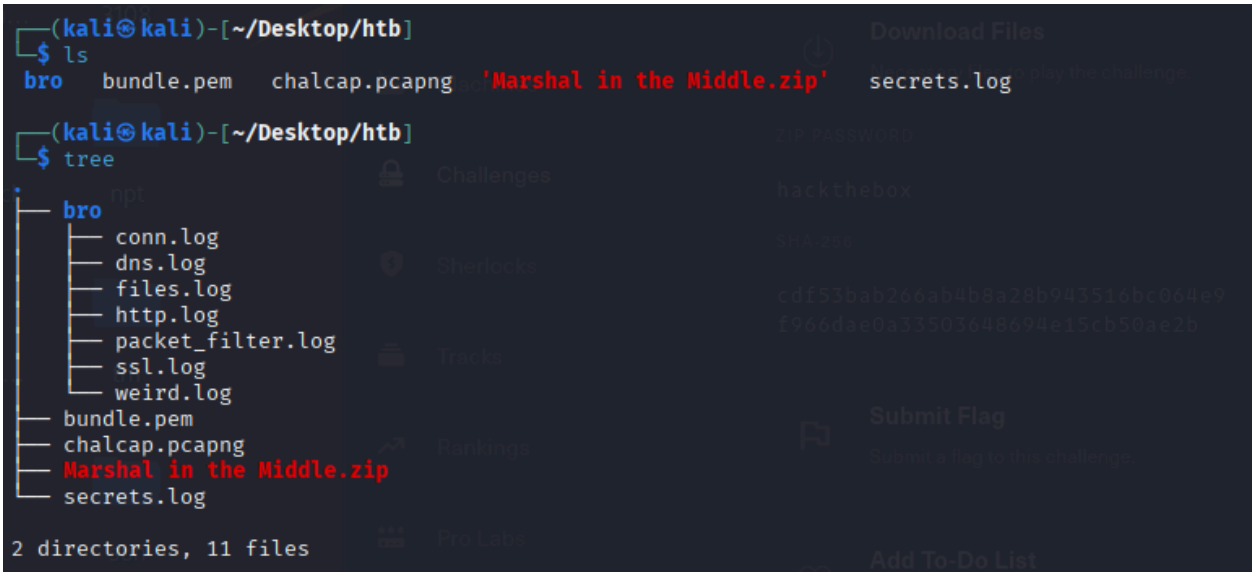
Challenge Description

The security team was alerted to suspicious network activity from a production web server. The task was to determine if any data was stolen and identify what it

was.

Given files:

- `chalcap.pcapng` → Network traffic capture
- `secrets.log` → TLS pre-master secrets log (for decrypting HTTPS traffic)
- Zeek logs (`bro/`) → Parsed traffic logs



Step 1 — Initial Analysis

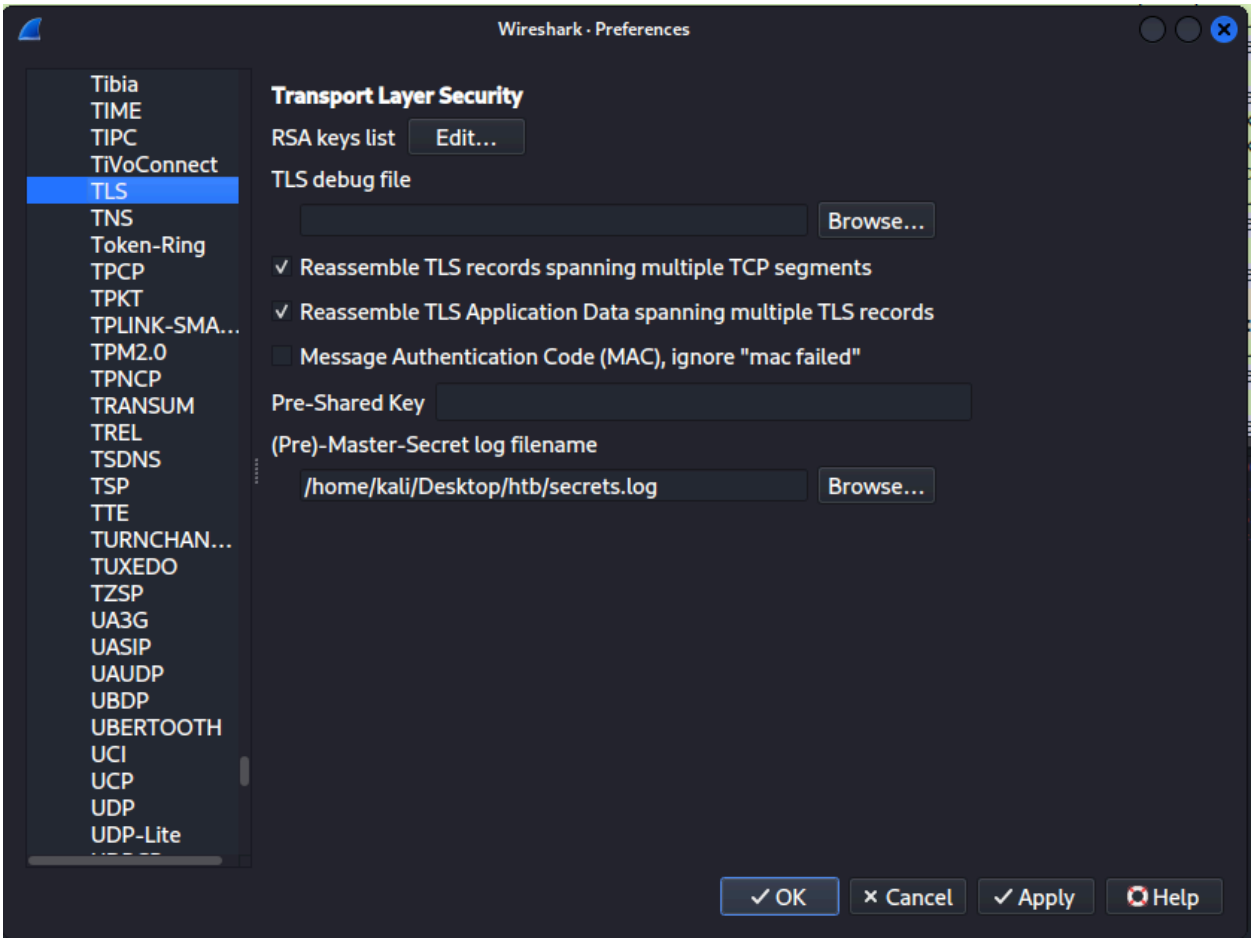
The provided packet capture (`chalcap.pcapng`) primarily contained encrypted TLS traffic. Since a **`secrets.log`** file was also given, this hinted that the HTTPS sessions could be decrypted to inspect the payload.

Step 2 — Decrypting TLS Traffic

To decrypt HTTPS:

1. Opened Wireshark → `Edit → Preferences → Protocols → TLS`.
2. Loaded `secrets.log` into **(Pre)-Master-Secret log filename**.

3. Reopened the `chalcap.pcapng`.

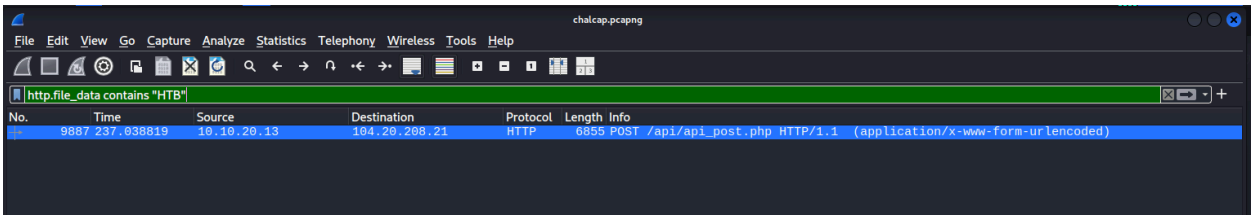


Step 3 — Filtering for Exfiltrated Data

To focus only on decrypted application data, I applied the following display filter in Wireshark:

```
http.file_data contains "HTB"
```

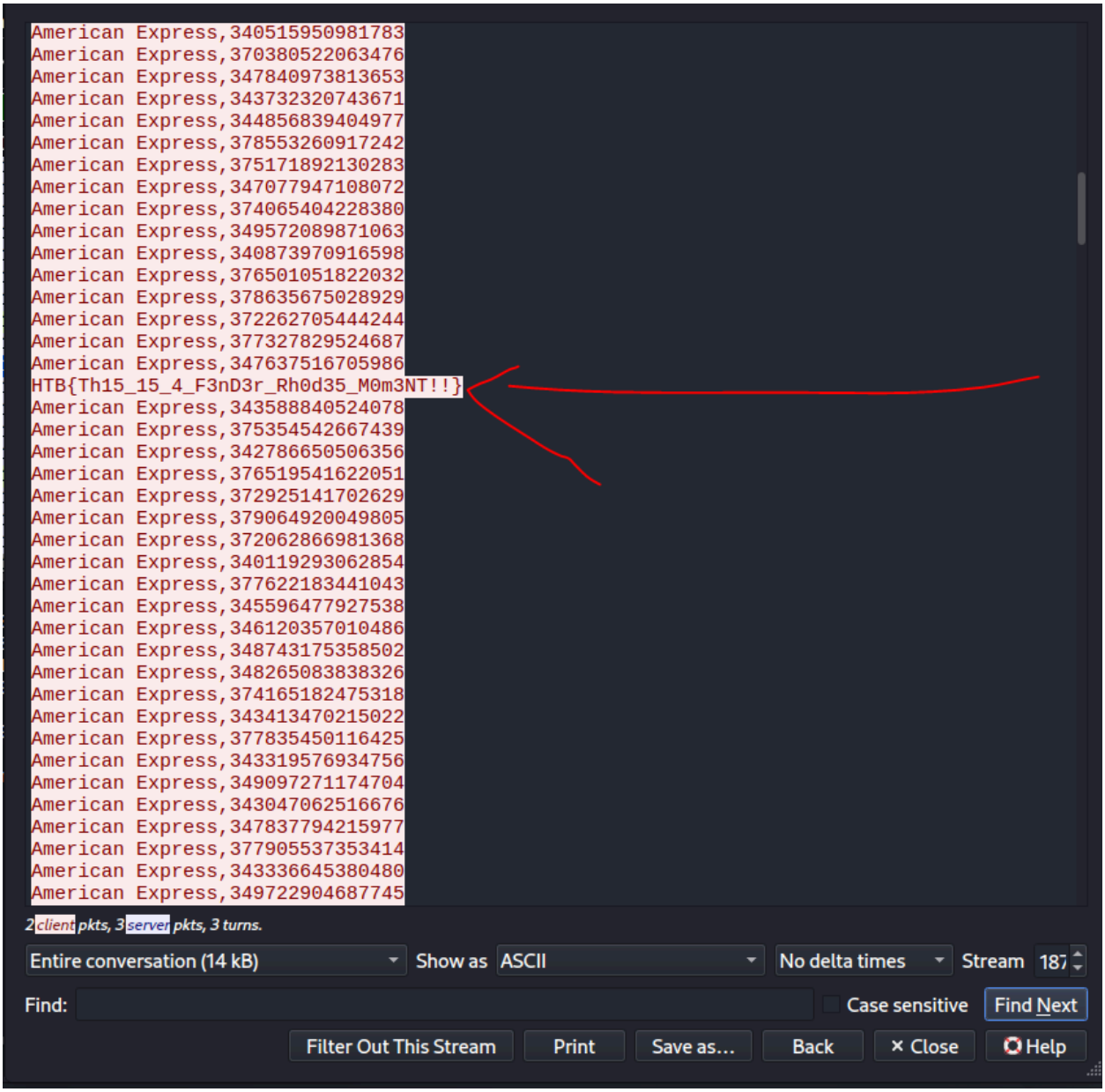
This directly searched HTTP payloads for the string `HTB`, which is a common flag format.



Step 4 — Identifying the Flag

After applying the filter, one packet contained suspicious outbound data with the flag string.

By inspecting the full decrypted HTTP payload (`Follow → TLS Stream`), the following flag was revealed:



HTB{Th15_15_4_F3nD3r_Rh0d35_M0m3NT!!}

boom thats our flag