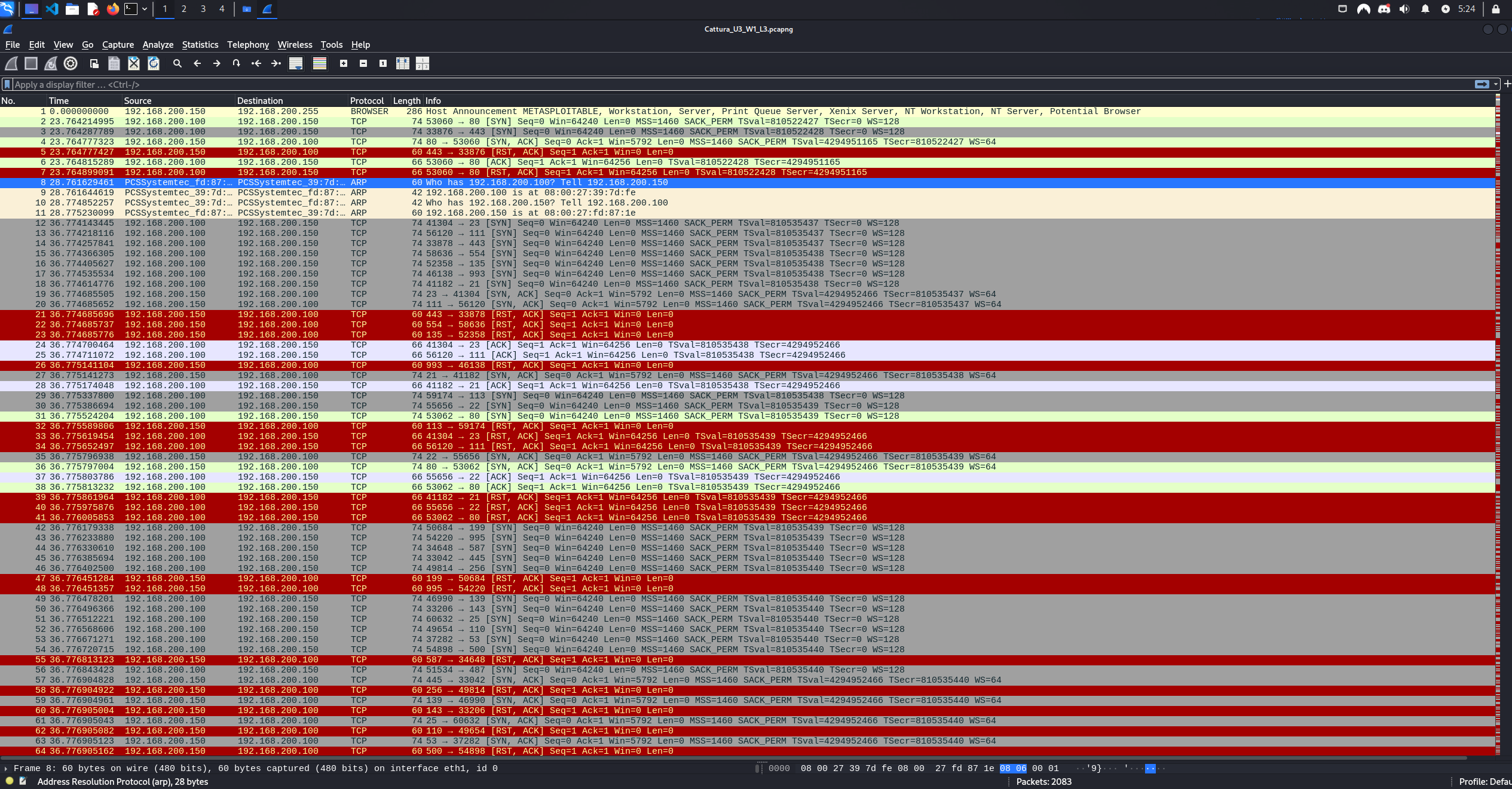
Esercizio S9/L5

**Wireshark**



Dalla rilevazione di wireshark si evince che è stato effettuato un attacco DoS sulla macchina 192.168.200.150.

Un attacco DoS (Denial of Service) è un tipo di attacco informatico che mira a rendere un servizio, una rete o una risorsa informatica non disponibile agli utenti legittimi, saturando le risorse del sistema o sovraccaricandolo.

Nello specifico si usa Syn Flood, un tipo di attacco che sfrutta il TCP. L’attaccante manda un flusso continuo di pacchetti Syn senza mai completare l’handshake a tre vie (SYN, SYN-ACK, ACK) necessario per stabilire una connessione TCP.

**Prevenzione e Mitigazione degli attacchi DoS**

La prevenzione e la mitigazione degli attacchi DoS e DDoS richiedono una combinazione di tecnologie, strumenti di sicurezza e strategie di gestione del traffico.

* **Firewall**: i firewall possono essere configurati per bloccare specifici tipi di traffico (es. pacchetti SYN flood o UDP flood) basati su regole definite. Possono anche limitare le connessioni da determinati IP o regioni geografiche sospette.
* **Load Balancer** **(Bilanciatori di Carico)**: distribuiscono il traffico tra più server per prevenire il sovraccarico di una singola macchina. In caso di un attacco DoS, un load balancer può ridurre l'impatto dividendo il carico tra diversi server, rendendo più difficile per un singolo attacco saturare l'intera rete.
* **Rate Limiting** **(Limitazione della velocità):** limita il numero di richieste che un singolo IP o una specifica risorsa può inviare in un determinato intervallo di tempo. Se un attaccante cerca di inondare il server con richieste, il rate limiting riduce il numero di richieste che vengono effettivamente gestite.
* **Content Delivery Network (CDN):** una CDN è una rete distribuita di server che memorizzano copie dei contenuti di un sito web e li distribuiscono agli utenti da posizioni geografiche più vicine. Questo non solo migliora le prestazioni per gli utenti legittimi, ma può anche distribuire il carico di un attacco DoS, rendendo più difficile per l'attaccante saturare una singola destinazione.