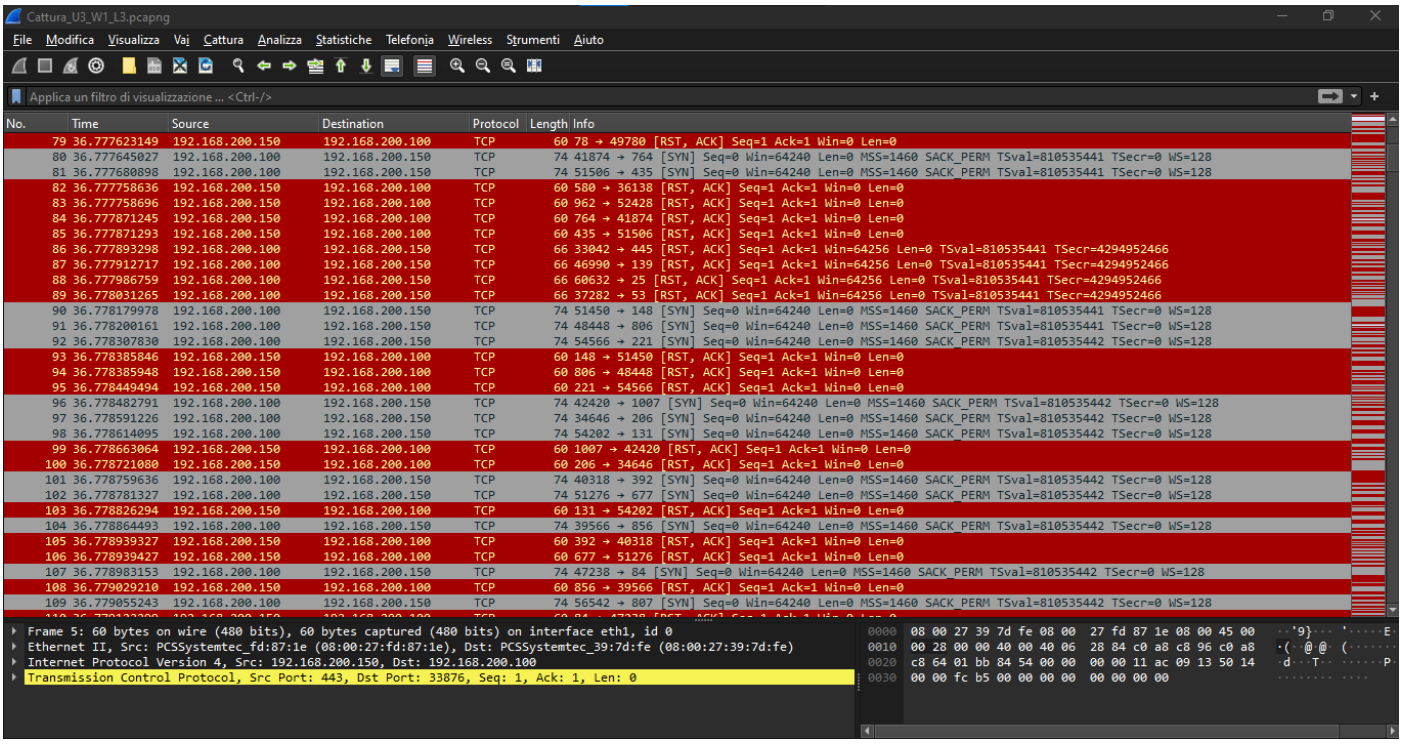
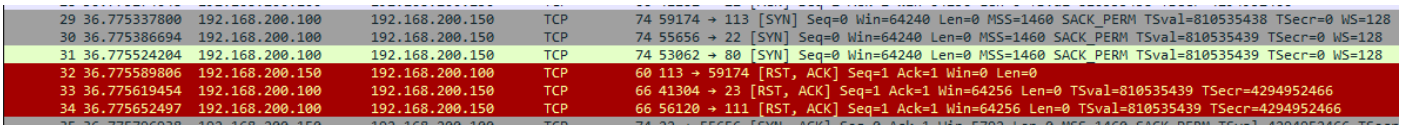
Analizzare la cattura di rete effettuata con Wireshark attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco



Analisi del file:

- Richieste eccessive TCP su porte differenti;
- Possibile controllo/scansione sul l'indirizzo IP 192.168.200.150 (target) da parte dell'indirizzo 192.168.200.100 (possibile attaccante);
- Applicare delle regole/policy sul Firewall per evitare che un malintenzionato possa utilizzarle a suo vantaggio.



Vediamo che ci sono molte richiesta a parte dell'IP 192.168.200.100 verso l'IP 192.168.200.150.
Infatti, vi sono delle righe dove le risposte sono positive (**SYN, ACK**) sulle porte aperte ed altre negative (**RST, ACK**) indicando le porte non risponde, pertanto chiusa.

Applicando delle regole sul Firewall possiamo impedire che l'Host 192.168.200.100 possa accedere.