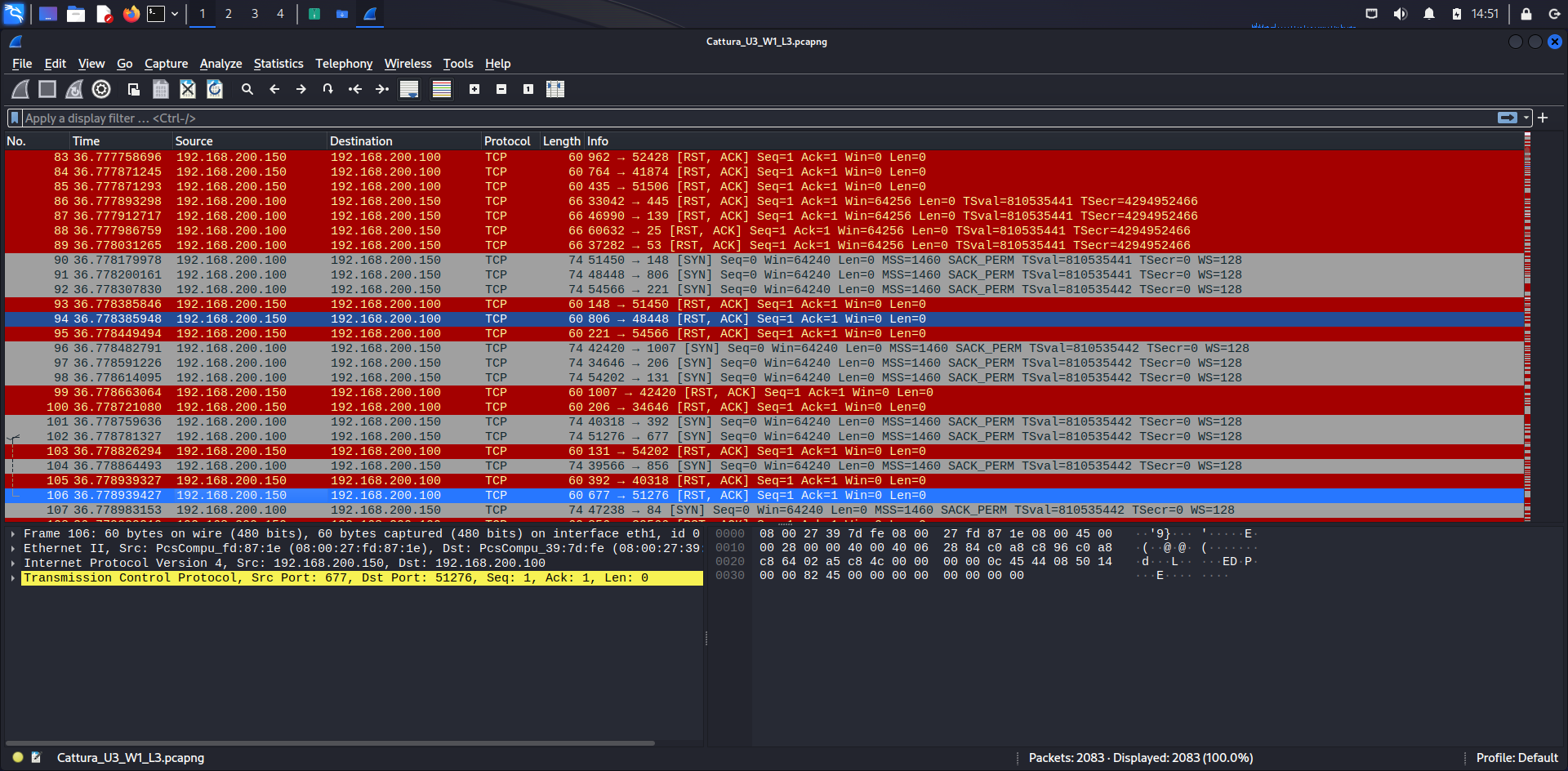
Nell’esercizio di oggi, dobbiamo analizzare una cattura di rete effettuata con Wireshark, cercando prove di possibili attacchi in corso (IOC). La schermata è la seguente:



Come mostrato dalla schermata, possiamo notare un numero elevato di segnali inviati da un singolo indirizzo IP (192.168.200.100) ad un altro indirizzo (192.168.200.150). Questo potrebbe significare che qualcuno sta provando ad effettuare un attacco DOS all’indirizzo di destinazione. Un attacco DOS è un tipo di attacco che prevede l’invio massiccio di “ping” alla vittima, con lo scopo di mandare in crash la macchina proprio perché la stessa non riesce a gestire tutti i segnali in entrata.

Per porre rimedio a questa situazione, quello che potremmo fare è andare a bloccare completamente i segnali in ingresso provenienti dall’indirizzo IP 192.168.200.100 oppure bloccare il segnale una volta superato un numero preciso di ping ( il numero dev’essere a scelta della security ma non elevato). Così facendo, tutto il traffico in eccesso non arriverà alla destinazione prefissata dall’attaccante.