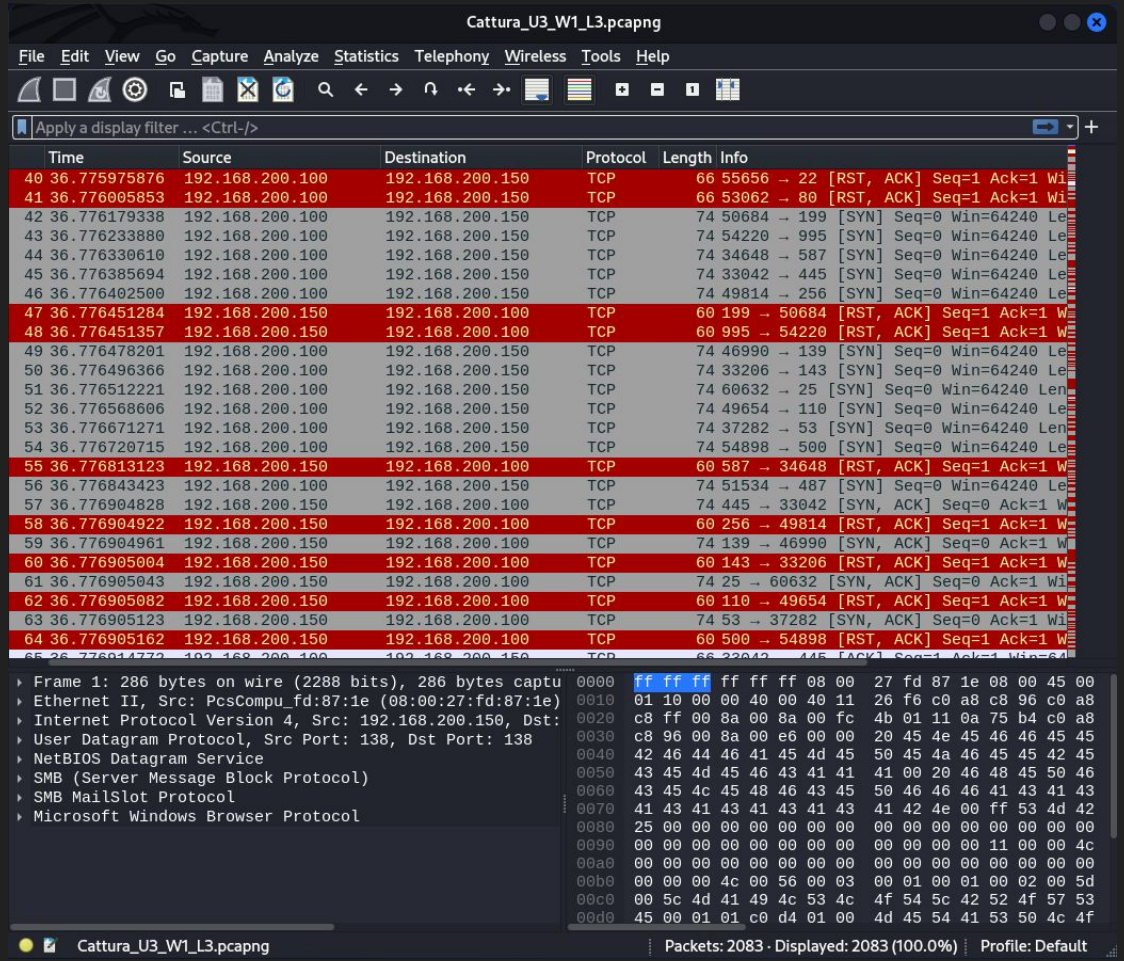
Analisi traffico Wireshark

Cattura traffico

Notiamo in grigio le molteplici richieste TCP inviate dall'host attaccante con IP 192.168.200.100, mentre in rosso notiamo le risposte dell'host vittima con IP 192.168.200.150



Vettore d’attacco

Multiple richieste TCP su ampi intervalli di porte

Azioni per ridurre l’impatto dell’attacco

Possiamo bandire tutte le future richieste provenienti dall’indirizzo IP malevolo e tramite firewall chiudere le porte vulnerabili