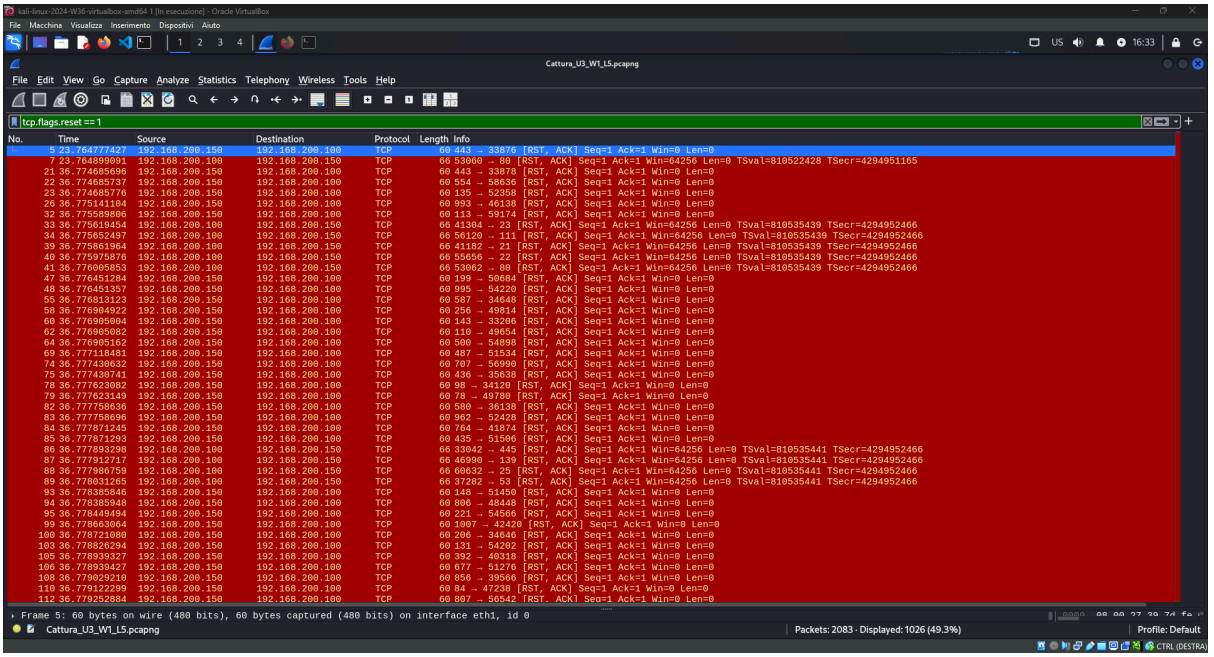
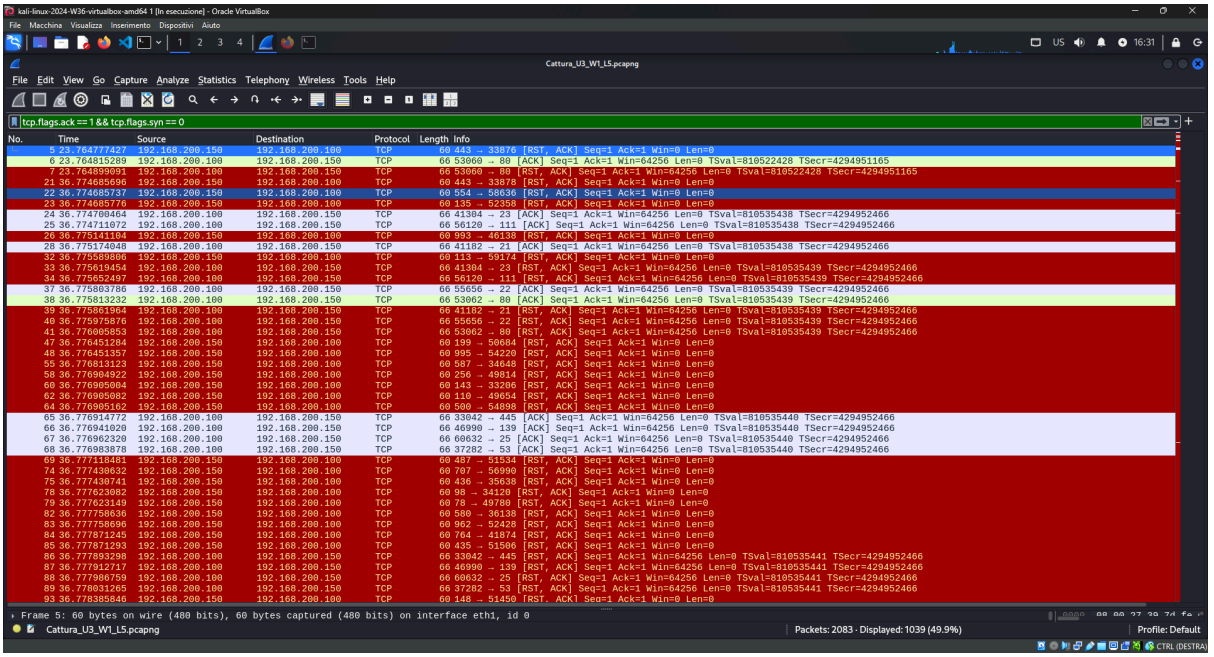
Threat Intelligence & IOC

In base all'analisi di Wireshark si possono notare due tipi di attacco principale:

- Reset Flood o RST Flood che tenta di interrompere le connessioni esistenti(1026 pacchetti)



- SYN Flood con spoofing delle porte si capisce perché ci sono molteplici pacchetti TCP con il flag SYN senza avere una risposta ACK(1039 pacchetti) , cambia anche le porte di origine per rendere più difficile filtrare il traffico malevolo.



Da qui si evince che molto sicuramente è un attacco DDos, probabilmente l'attacco è partito con l'utilizzo di un Botnet utilizzato per reclutare una rete di computer detti "zombie" ipotizzo questa soluzione perché utilizzano un RST Flood che vuole bloccare tutte le connessioni di rete o di un'applicazione.L'unico dubbio è che l'attacco proviene da un solo indirizzo IP.

Azioni per mitigare l’attacco attuale:

- Abilitare il Rate Limiting: configurando il Firewall o router per limitare il numero di richieste SYN e RST da una singola attività
- Filtraggio dei Pacchetti Anomali: inserendo delle regole nel Firewall per rifiutare pacchetti SYN e RST non richiesti o che provengono da indirizzi IP sconosciuti
- Attivare il SYN Cookie: per ridurre l'impatto degli attacchi SYN flood
- Utilizzare un Sistema di Prevenzione delle Intrusioni (IPS): per monitorare e bloccare traffico sospetto, compresi gli attacchi SYN e RST flood.
- Contattare il Fornitore di Servizi Internet (ISP): potrebbero essere in grado di bloccare il traffico malevolo prima che raggiunga la tua rete.

Azioni per prevenire attacchi futuri:

- Implementare un Servizio di Protezione DDoS: può rilevare e mitigare attacchi su larga scala in tempo reale
- Rafforzare la Sicurezza del Server: aggiornando costantemente il sistema operativo e le app
- Monitoraggio Continuo della Rete: implementando sistemi di monitoraggio che consentono di rivelare traffico o picchi sospetti ed anomali
- Pianificare e Testare un Piano di Risposta agli Incidenti: include azioni specifiche da intraprendere in caso di attacco DDoS e simula attacchi per testare l'efficacia del piano
- Bloccare le Reti di Botnet Note: aggiornando regolarmente le liste di indirizzi IP conosciuti per essere parte di botnet e bloccarle a livello di firewall.