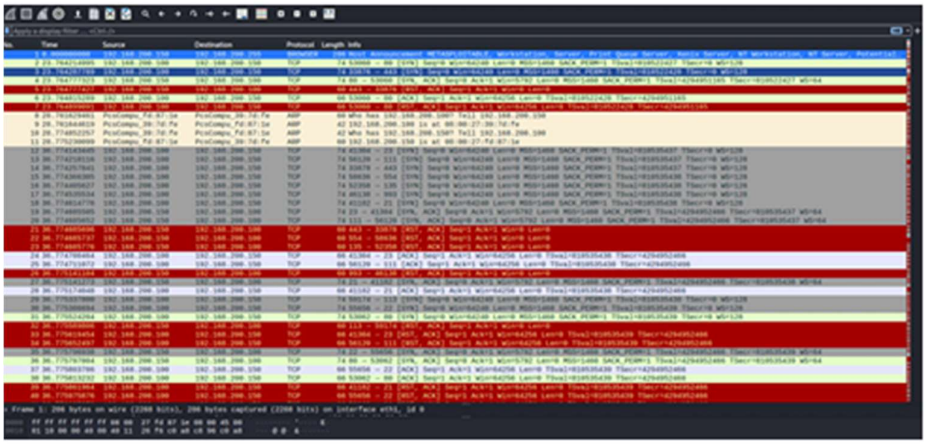
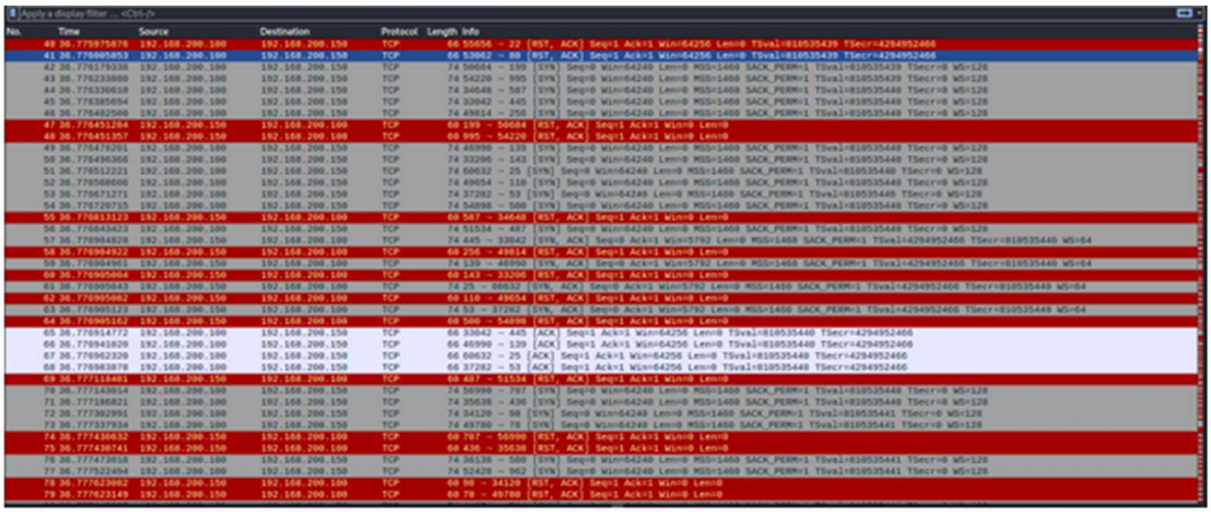
ESERCIZIO S9-L3

Lo scopo dell'esercizio di oggi è quella di analizzare il contenuto di una cattura su Wireshark e rispondere ai 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





Analizzando questa cattura deduco che l'evidenza dell'attacco in corso si vede dalle numerose richieste TCP ripetute su porte sempre diverse. Probabilmente si tratta di una scansione in corso dall'host 192.168.200.100 verso l'host target 192.168.200.150. Un consiglio per ridurre gli impatti dell'attacco può essere quello di configurare delle policy sul firewall per respingere le richieste da parte dell'attaccante.