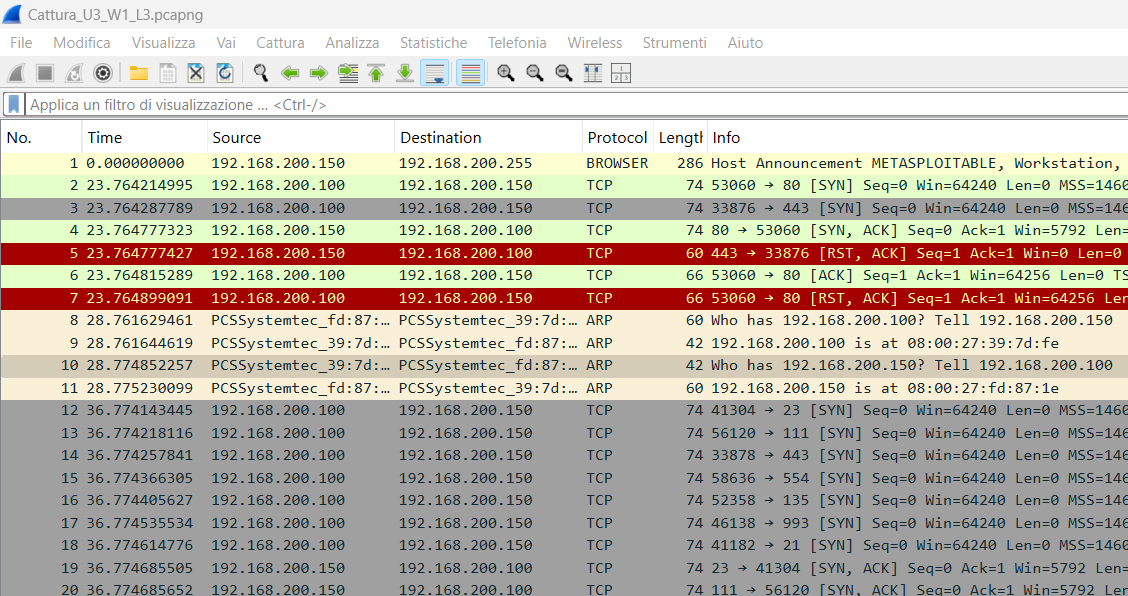
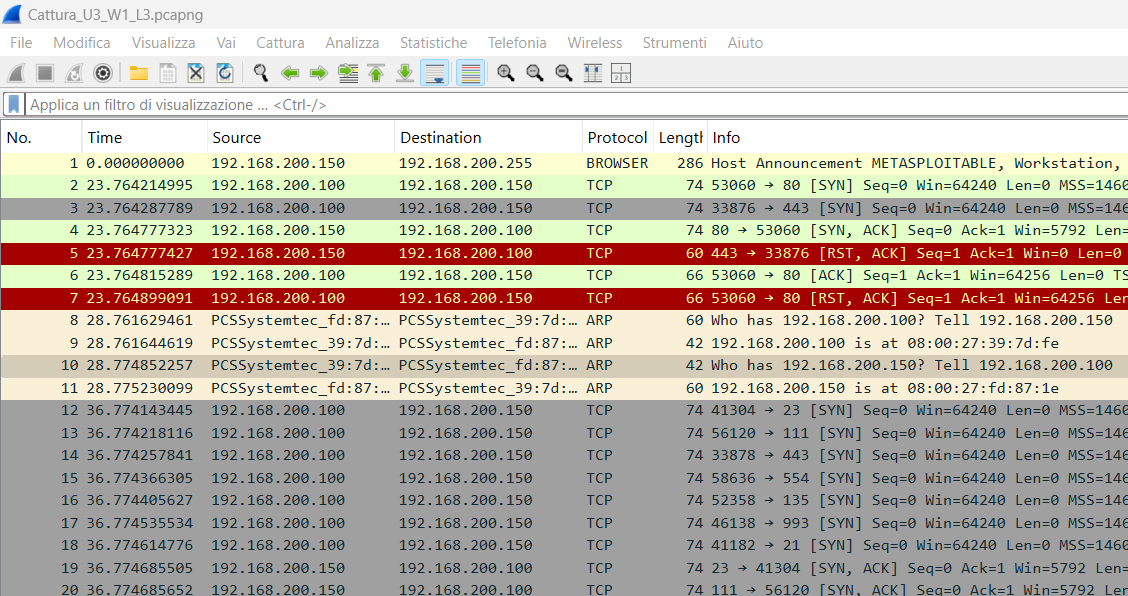
**PROGETTO S9E5**

Per il progetto di oggi la traccia richiedeva di mettere in pratica le nozioni viste durante la lezione, riguardanti la threat intelligence, e analizzare una cattura di rete effettuata con wireshark per:

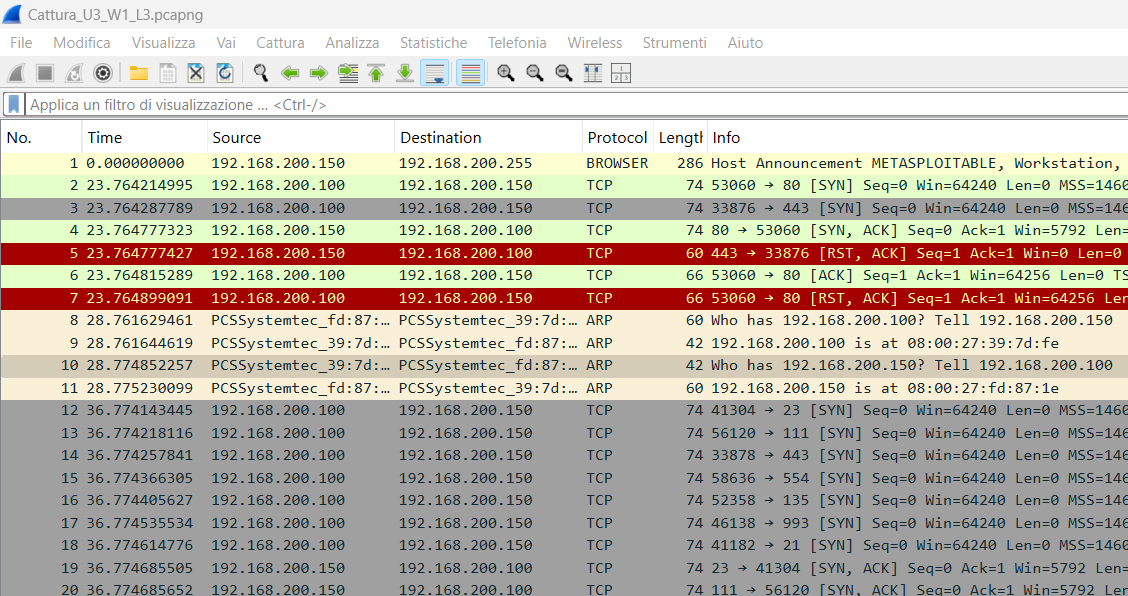
* Rilevarne i vari indicatori di compromissione
* Avanzare delle ipotesi su potenziali vettori di attacco utilizzati
* Consigliare un’azione per ridurre gli impatti dell’attacco attuale ed eventualmente di un simile attacco futuro.

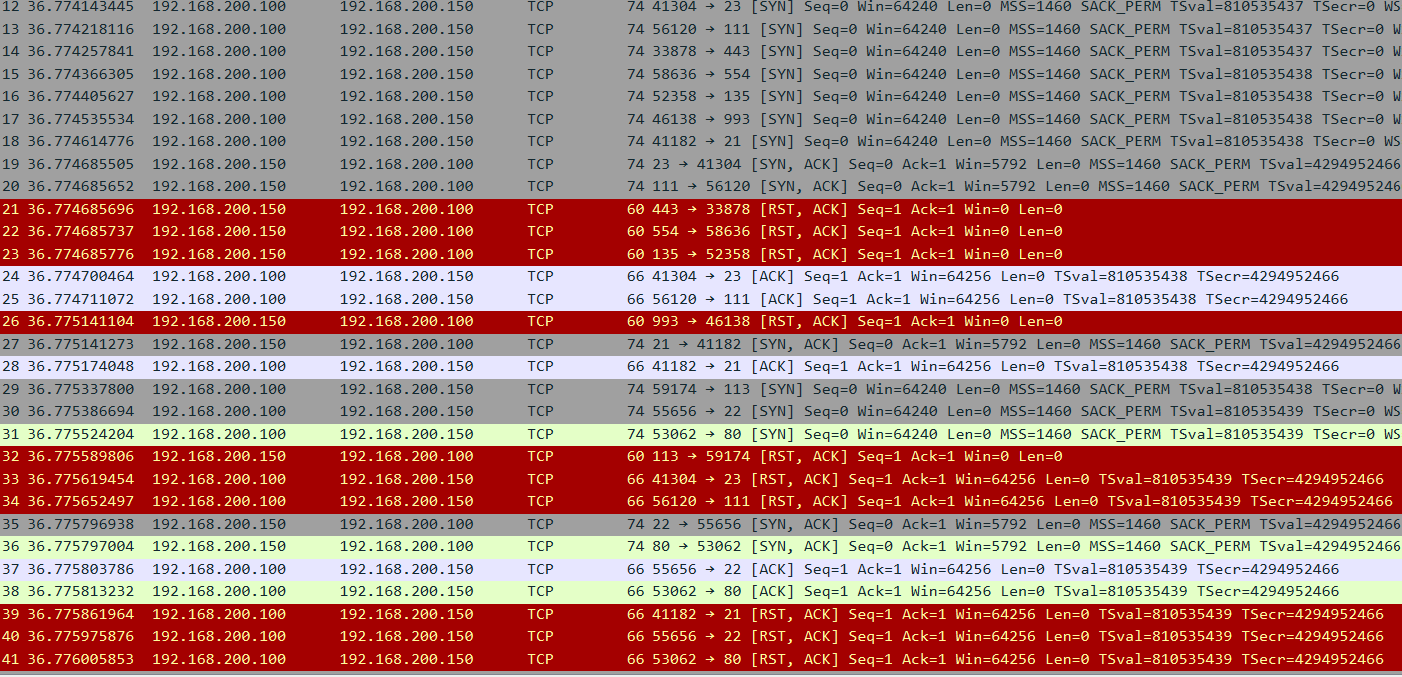


Da questa schermata iniziale la prima cosa che salta all’occhio sono le diverse richieste **SYN** mandate dall’indirizzo IP 192.168.200.100 su molteplici porte dell’indirizzo 192.168.200.150; il che risulta essere un primo IOC che ci allarma su un movimento anomalo che ci fa pensare ad una scannerizzazione di porte per capire se il dispositivo vittima ha delle porte aperte da poter sfruttare per creare un’eventuale connessione.



Notiamo poi che di tutte queste richieste **SYN** senza risposta da parte della vittima, c’è una prima stretta di mano a tre vie che va a buon fine.



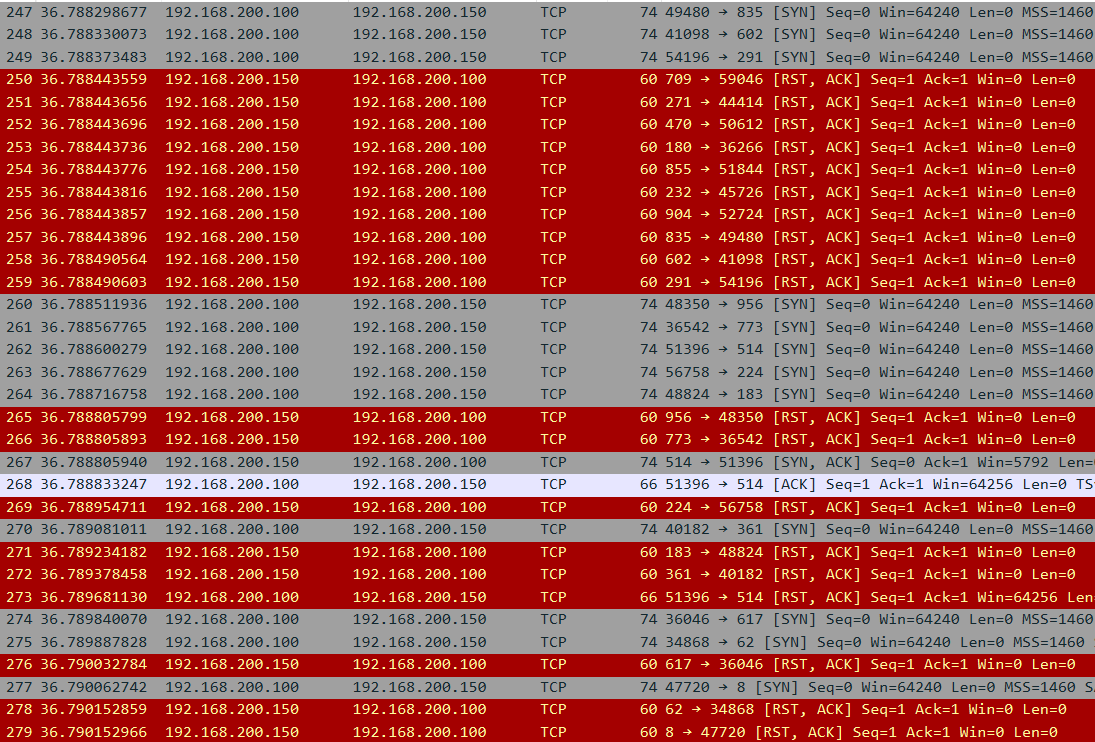


da questo screen possiamo notare come mentre l’attaccante continua a scannerizzare la rete, la vittima inizia a mandare delle risposte **RST** che ci indicano che tutte quelle porte a cui l’attaccante sta mandando richieste, sono in realtà chiuse, e quindi non concludono la stretta di mano a tre vie in maniera normale

Un altro IOC che ci fa sospettare di un comportamento anomalo da parte di questo indirizzo IP è la richiesta **ARP** che lui fa per associare l’indirizzo IP della vittima ad un indirizzo MAC, il che ci fa capire sia che l’attaccante si trova all’interno della nostra rete, sia che vuole sapere se quel determinato indirizzo IP sia effettivamente presente e attivo all’interno della rete.

Nella riga 2 si nota come l’attaccante manda un **SYN** sulla porta 80 della vittima; la vittima risponde con un **SYN-ACK** sulla riga 4 e sulla riga 6 l’attaccante conclude la stretta di mano a tre vie con un **ACK**, in maniera del tutto normale. La cosa anomala è la riga 7 dove l’attaccante, una volta conclusa la three way handshake, manda un **RST** che chiude la connessione in maniera volontaria, il che ci fa pensare che concludere la three way handshake sia servita all’attaccante solamente per delle informazioni da sfruttare, come identificare il s.o.

Andando avanti con la scansione notiamo come l’invio di richieste **SYN** e le risposte **RST** diventano sempre più massivi; il che ci fa dedurre che lo scopo dell’attaccante non è quello di concludere la stretta di mano a tre vie, ma quello di un attacco DOS per sovraccaricare il processore della macchina vittima che non avendo abbastanza risorse per rispondere a un così elevato numero di pacchetti va in down.



Un’azione consigliabile per evitare che questo tipo di attacco mandi la macchina vittima in down e che eviti che si ripeta in futuro, è quello di bloccare l’indirizzo IP in questione all’interno del firewall e creare una regola per limitare le connessioni TCP simultanee, in modo tale che un unico dispositivo possa mandare un massimo di pacchetti che quindi non permettono al dispositivo vittima di andare in down.

Inoltre implementare maggiori sistemi di sicurezza come IDS e IPS o utilizzare il bilanciamento del carico che quindi riduce il lavoro di un unico processore che lavorando meno andrà molto più difficilmente in down.