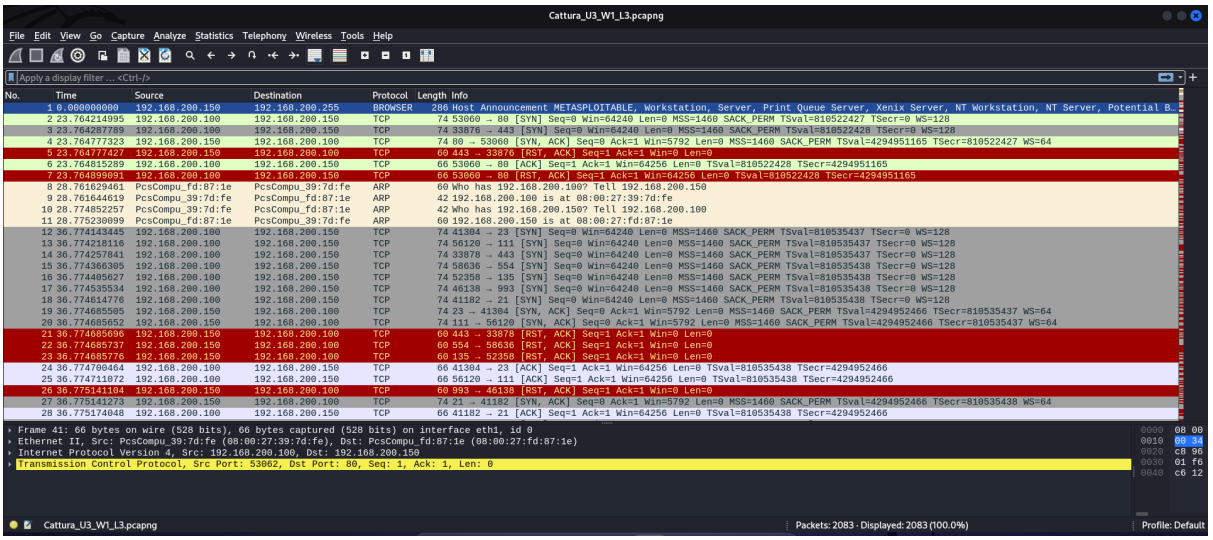
CONSEGNA S9/L3

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

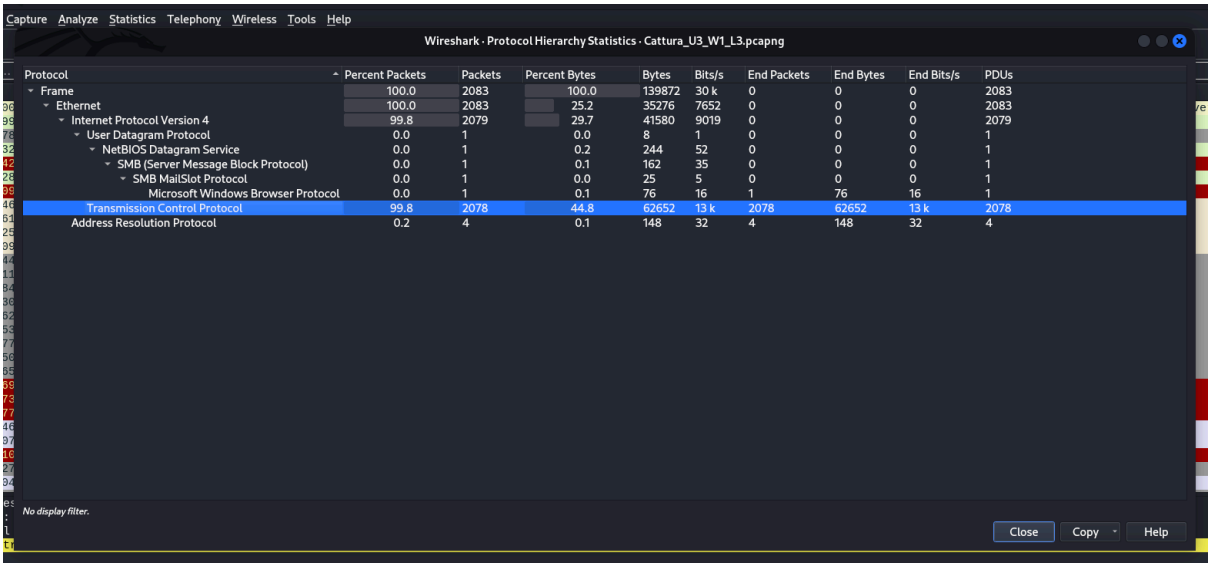
Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- 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

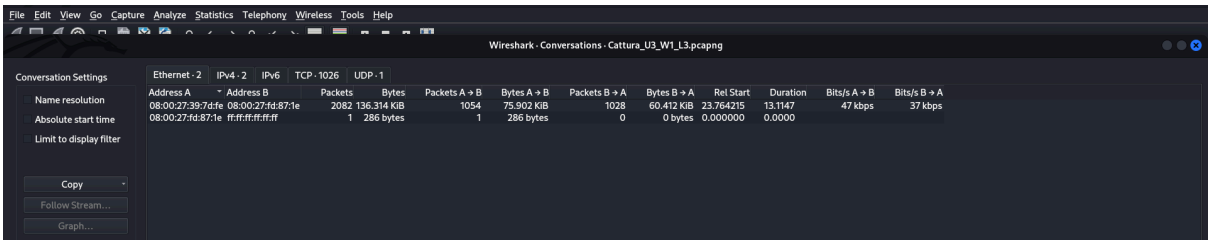
Si inizia l'esercizio spostando su Kali il **file** della scansione **Wireshark**.
Una volta fatto lo si può aprire con Wireshark e si può iniziare ad **osservare** la **situazione** che ci troviamo davanti.



Ad una rapida occhiata vediamo tantissimi **protocolli TCP**, ma andiamo ad indagare più a fondo.
Andando su **Statistics>Protocol Hierarchy** possiamo vedere la gerarchia di tutti i protocolli presenti nella cattura.
Fondamentalmente questa sezione ci mostra i **protocolli catturati** con la relativa **quantità** a fianco.
In questo caso per quanto riguarda il protocollo TCP (*Transmission Control Process*) sono stati trovati ben **2078 pacchetti**, esattamente il **99,8%** di tutti i pacchetti catturati.

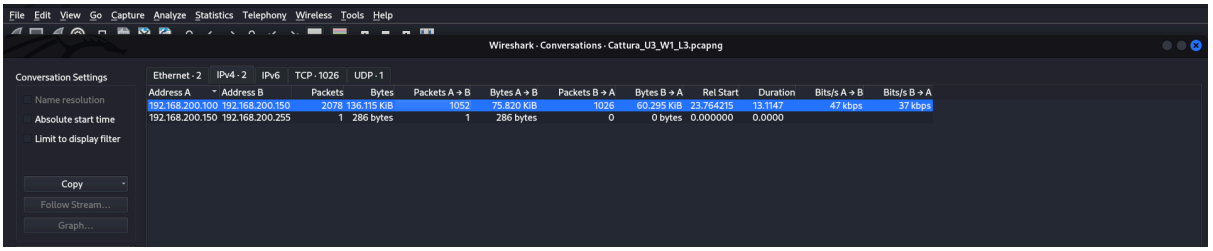


Andando su **Statistics>Conversations** possiamo ottenere più il **MAC Address** sia dell'**host attaccante** che dell'**host attaccato**, rispettivamente *Address A* e *Address B*, come in figura.

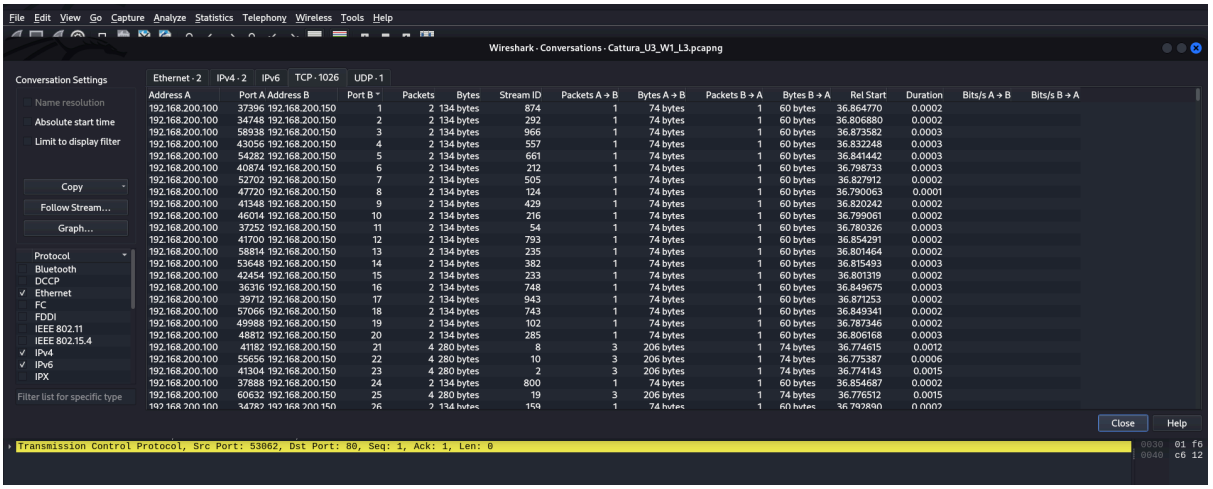


Rimanendo sempre in questa voce e recandoci nella sezione **IPv4** possiamo ottenere gli **indirizzi IP** sia dell'**host attaccante** che dell'**host attaccato**, rispettivamente *Address A* e *Address B*, come in figura.
In questo caso:

- **192.168.200.150 è l'attaccante**
- **192.168.200.100 è la macchina host**

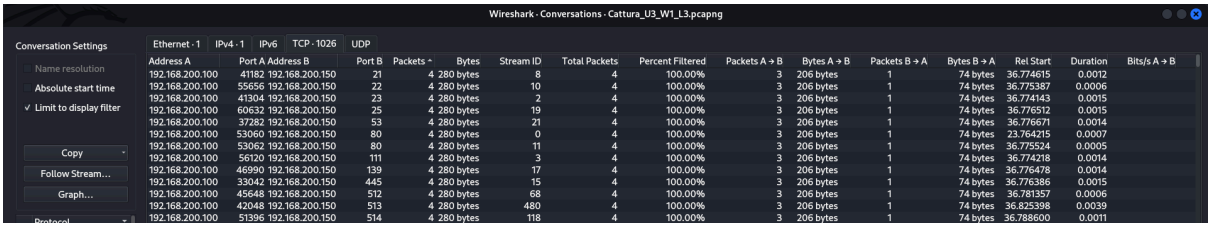


Rechiamoci anche nella sezione **TCP** per visionare tutti i pacchetti TCP che sono stati catturati.
Se clicchiamo una volta sulla voce "**Port B**" possiamo **ordinare** tutti i pacchetti inviati dalla macchina attaccante, come in figura sotto.

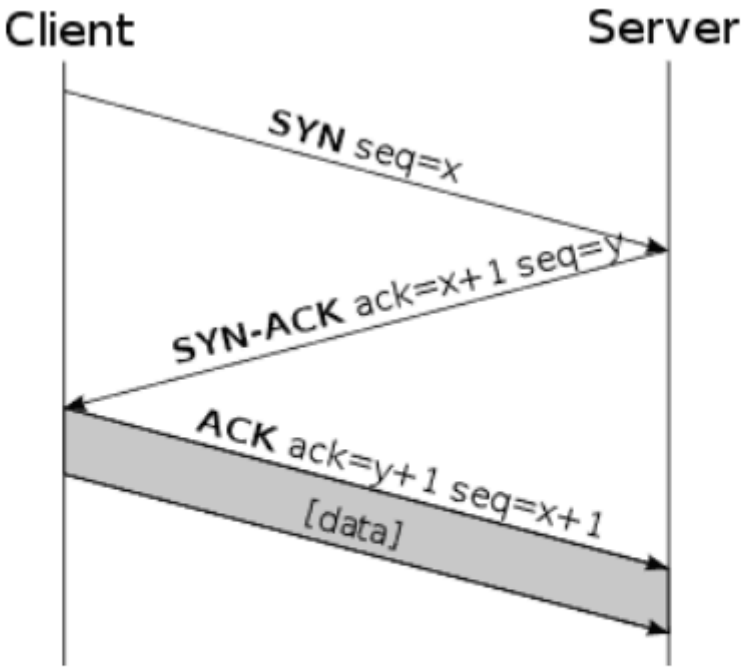


Possiamo ottenere anche l'elenco delle **porte aperte** cliccando una volta su "**Packets**".
Il programma ci ordinerà i pacchetti per **grandezza** e quelli più grandi (da **4 pacchetti**) sono le nostre *porte aperte*, perché completano il **Three-Way-Handshake**, un metodo utilizzato in una rete **TCP/IP** per creare una connessione tra un host/client locale e un server scambiando i pacchetti **SYN** e **ACK**.

- Le **porte aperte** che sono state individuate sono: **21**, **22**, **23**, **25**, **53**, **80**, **111**, **139**, **445**, **512**, **513**, **514**.



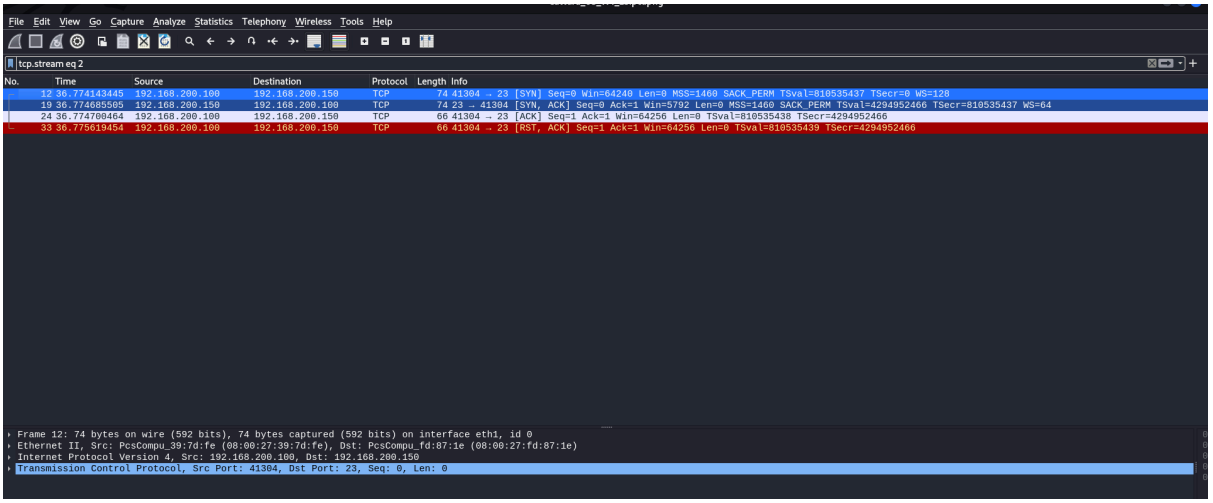
Il *Three-Way-Handshake* è raffigurato nella figura sotto.



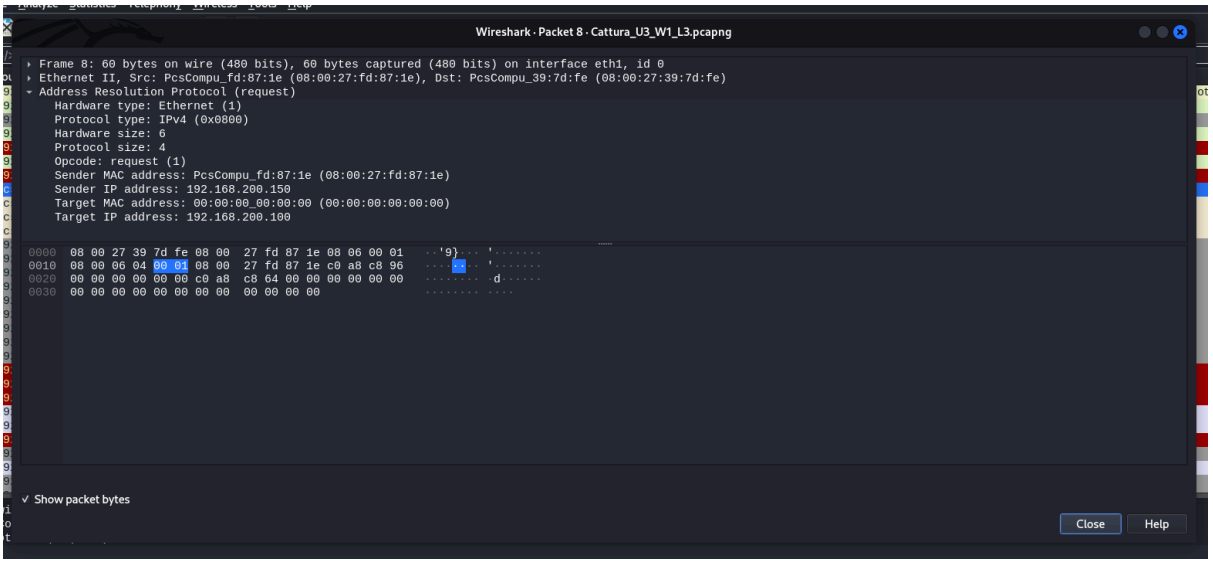
Tcp-handshake : Client = A : Server = B

Three-way handshake

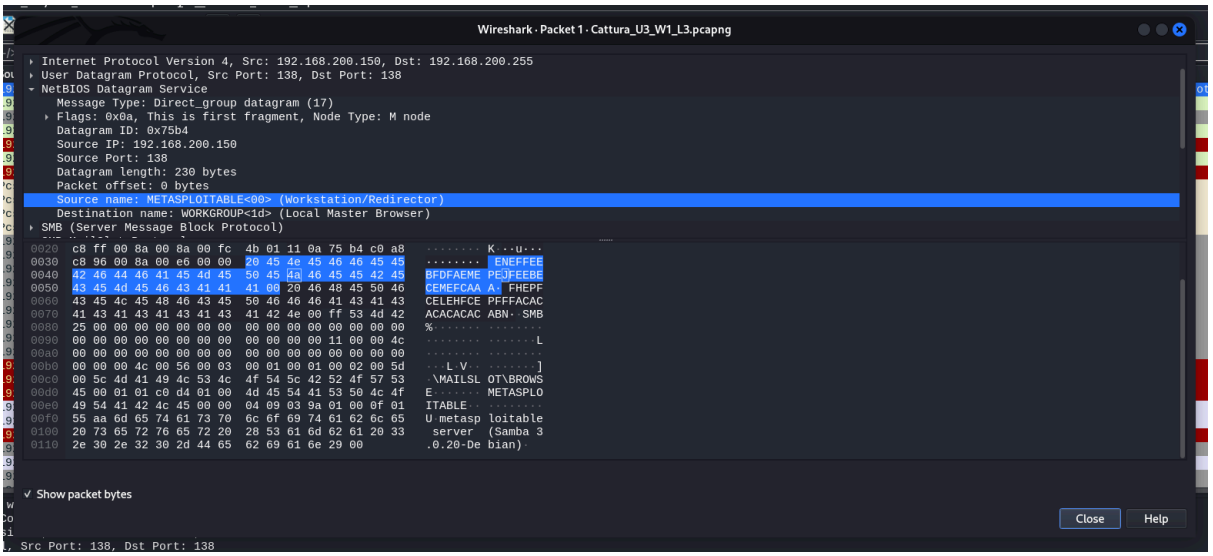
Con il filtro “**tcp.stream eq 2**” da applicare nella **barra dei filtri** in alto (oppure semplicemente facendo **tasto destro** su un pacchetto **TCP**, “**Follow**” e poi “**TCP Stream**”) si può ottenere nel dettaglio il flusso del pacchetto TCP.
Nella figura sotto il pacchetto TCP selezionato completa il *Three-Way-Handshake*.

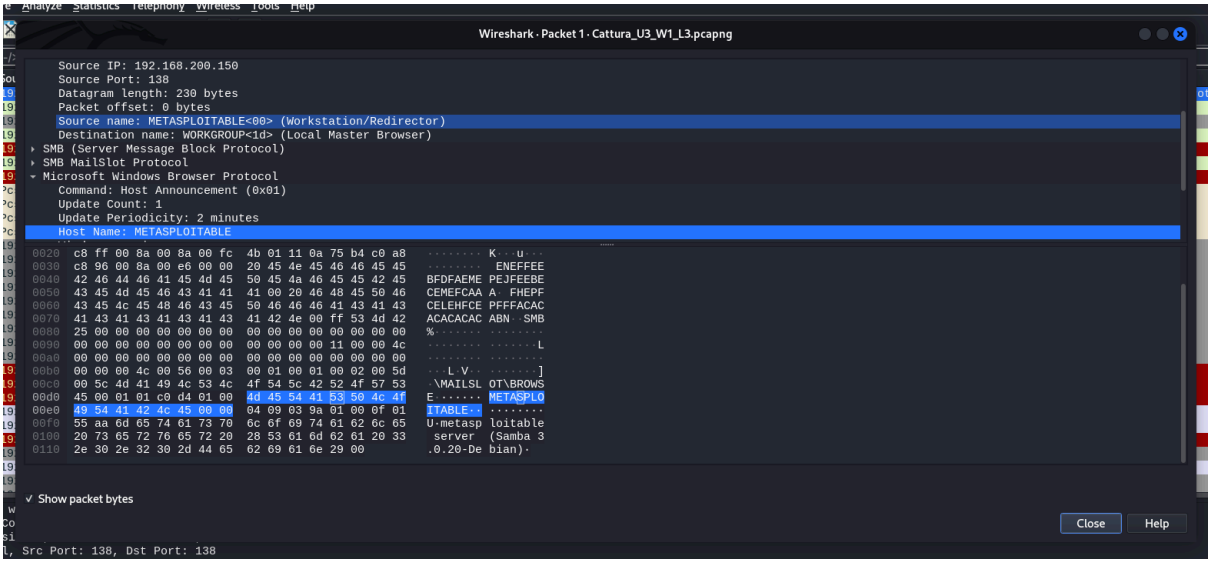


Nel dettaglio in figura sotto il **protocollo ARP** dell'attaccante.



Possiamo notare anche la presenza del **pacchetto BROWSER**, il primo che troviamo nella scansione.
Se facciamo doppio click su tale pacchetto possiamo scoprire che la macchina attaccante è **Metasploitable**.ed è presente sia nella dicitura "**Source name**" che in "**Host**", come da figure.





Possiamo fare anche la controprova seguendo il traffico del pacchetto, facendo **tasto destro** sul pacchetto **BROWSER**, “**Follow**” e poi “**UDP Stream**”.
Così facendo possiamo vedere molto meglio le informazioni che ci servono: abbiamo trovato un attaccante che usa una macchina **Metasploitable basata su Samba 3.0.20-Debian**.

- Giunti a questo punto si può tranquillamente affermare che l’attaccante stava eseguendo un **port scanning** sul nostro host.
  Come **azione** per **ridurre** gli **impatti dell’attacco** si può (e si deve) utilizzare un **firewall**.