Report Threat Intelligence & IOC

Traccia

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:

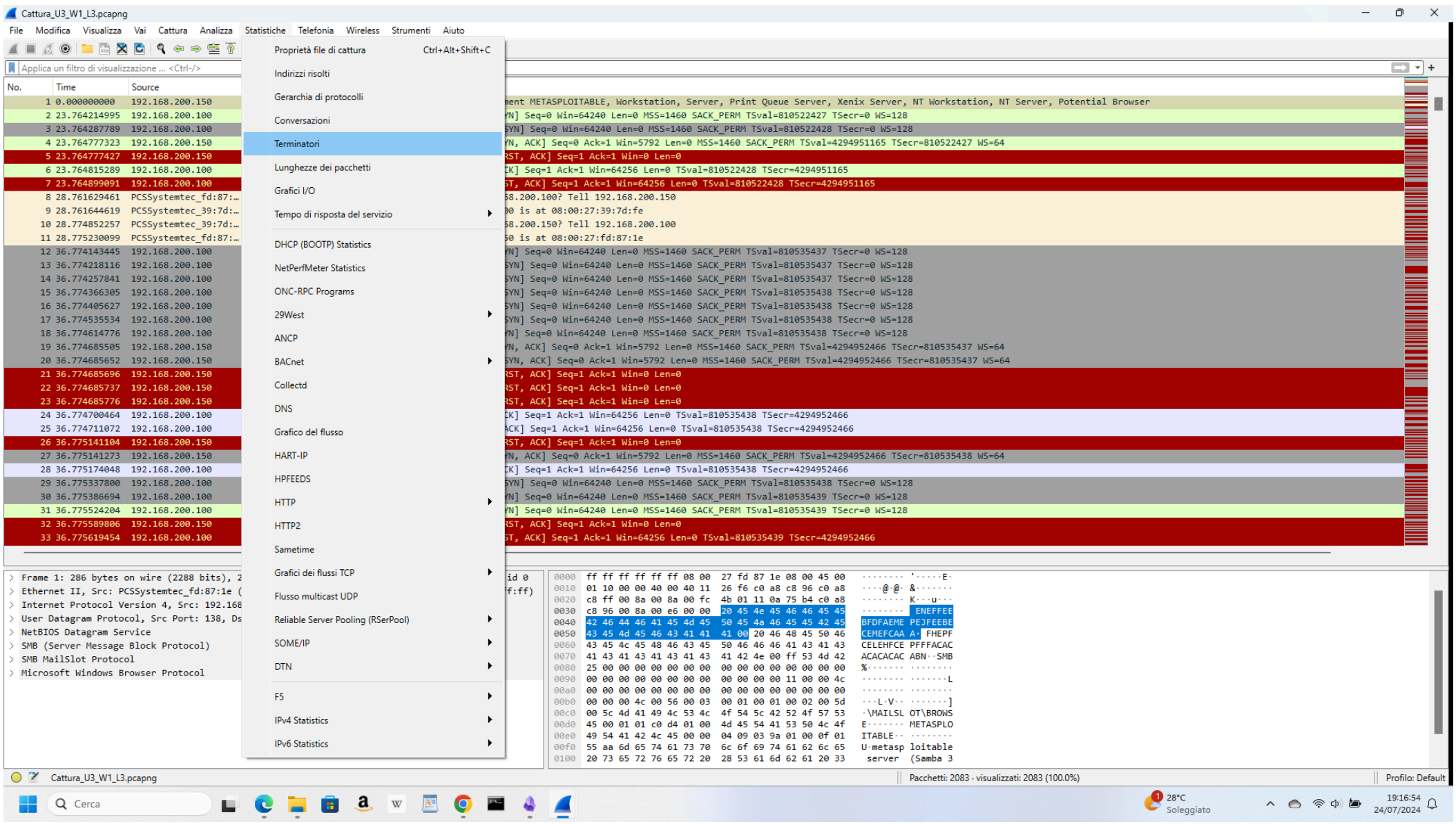
- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

Che cos'è WireShark e come può essere utile per individuare IOC nel traffico di rete

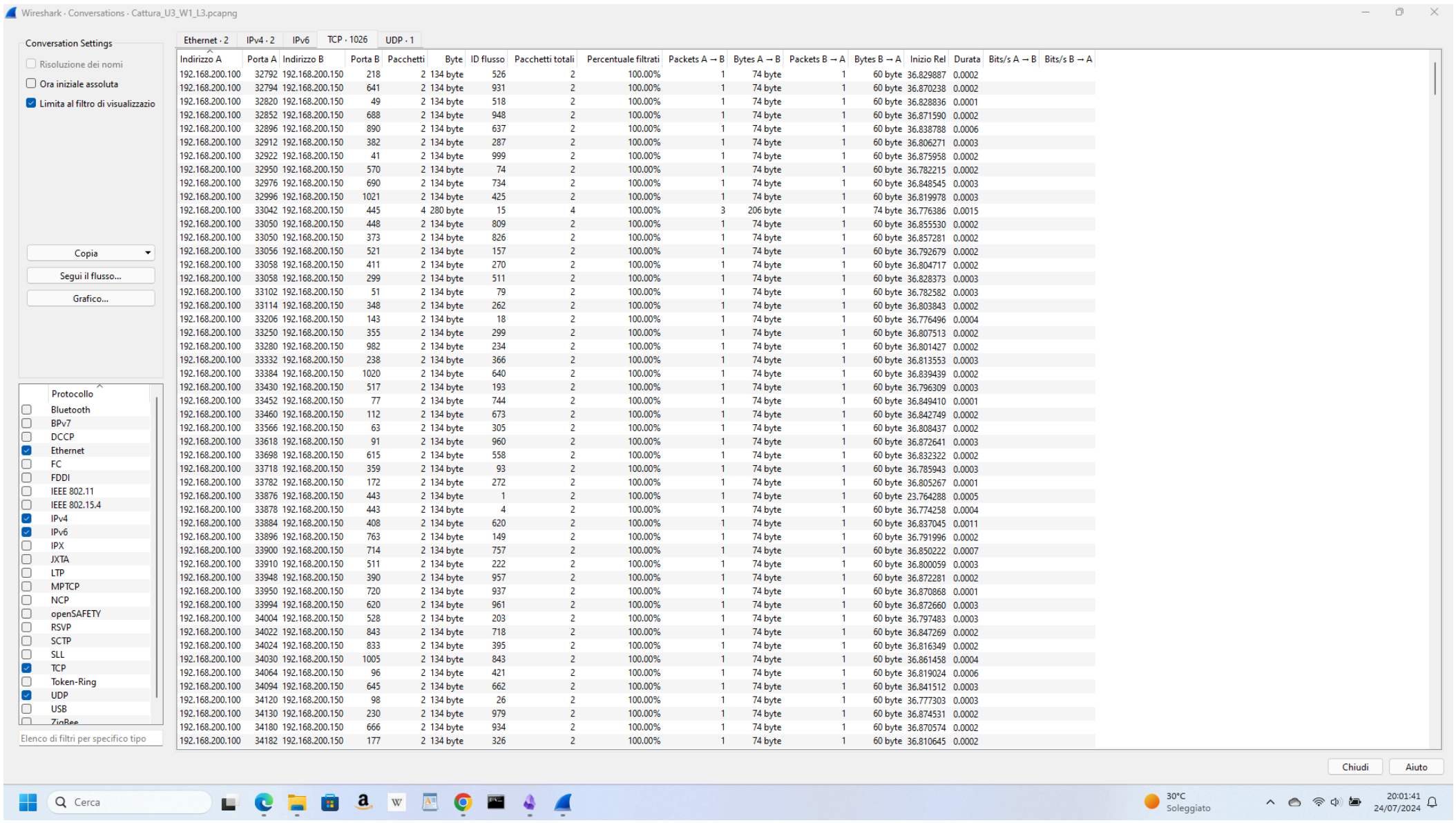
Wireshark è un analizzatore di protocollo di rete open-source che consente di catturare e analizzare il traffico di rete in tempo reale ed è un potente strumento per individuare **Indicatori di Compromissione (IOC)** nel traffico di rete. Infatti, analizzando i pacchetti di dati scambiati, Wireshark permette di identificare modelli di comportamento anomalo, individuare attività sospette come attacchi di rete o comunicazioni con server di comando e controllo associati a malware. La sua capacità di esaminare dettagliatamente il traffico aiuta a rilevare eventuali pattern che indicano compromissioni o attività malevole. Gli analisti possono utilizzare Wireshark per monitorare e rispondere tempestivamente a minacce, migliorando la sicurezza informatica complessiva dell'ambiente di rete.

Identificazione di IOC e potenziali vettori di attacco utilizzati

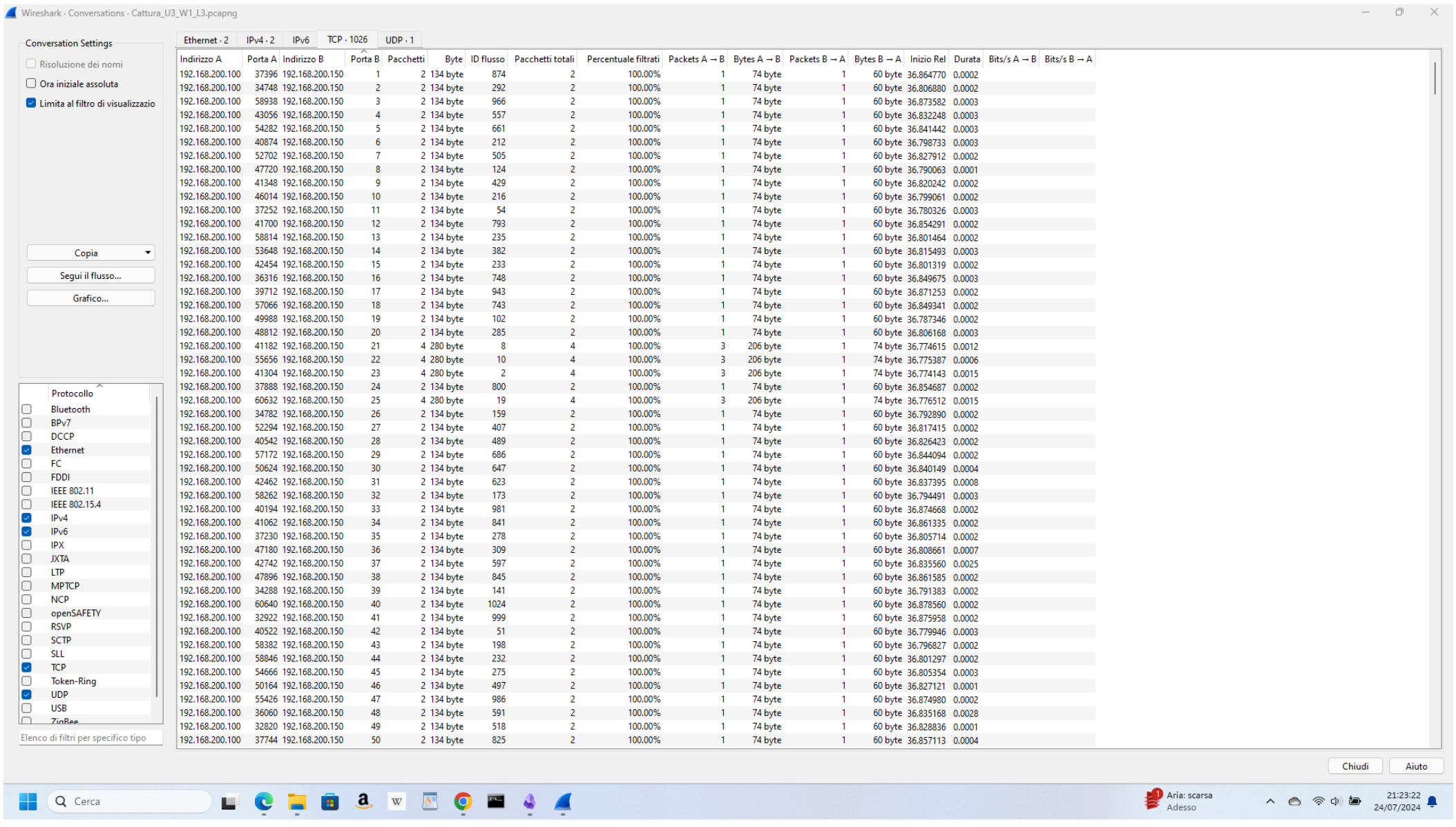
All'interno di Wireshark, nel menù in cima all'applicazione selezioniamo **Statistiche** e poi **Terminatori** e come si può ben notare vi sono tre endpoint. Visionando attentamente gli indirizzi IP presenti, ci accorgiamo subito che sono sulla stessa rete dove troviamo un indirizzo che termina in 255 e dunque è l'indirizzo di broadcast e gli altri terminano rispettivamente in 100 e 150, quindi possiamo supporre appartengano a due macchine comunicanti fra loro.

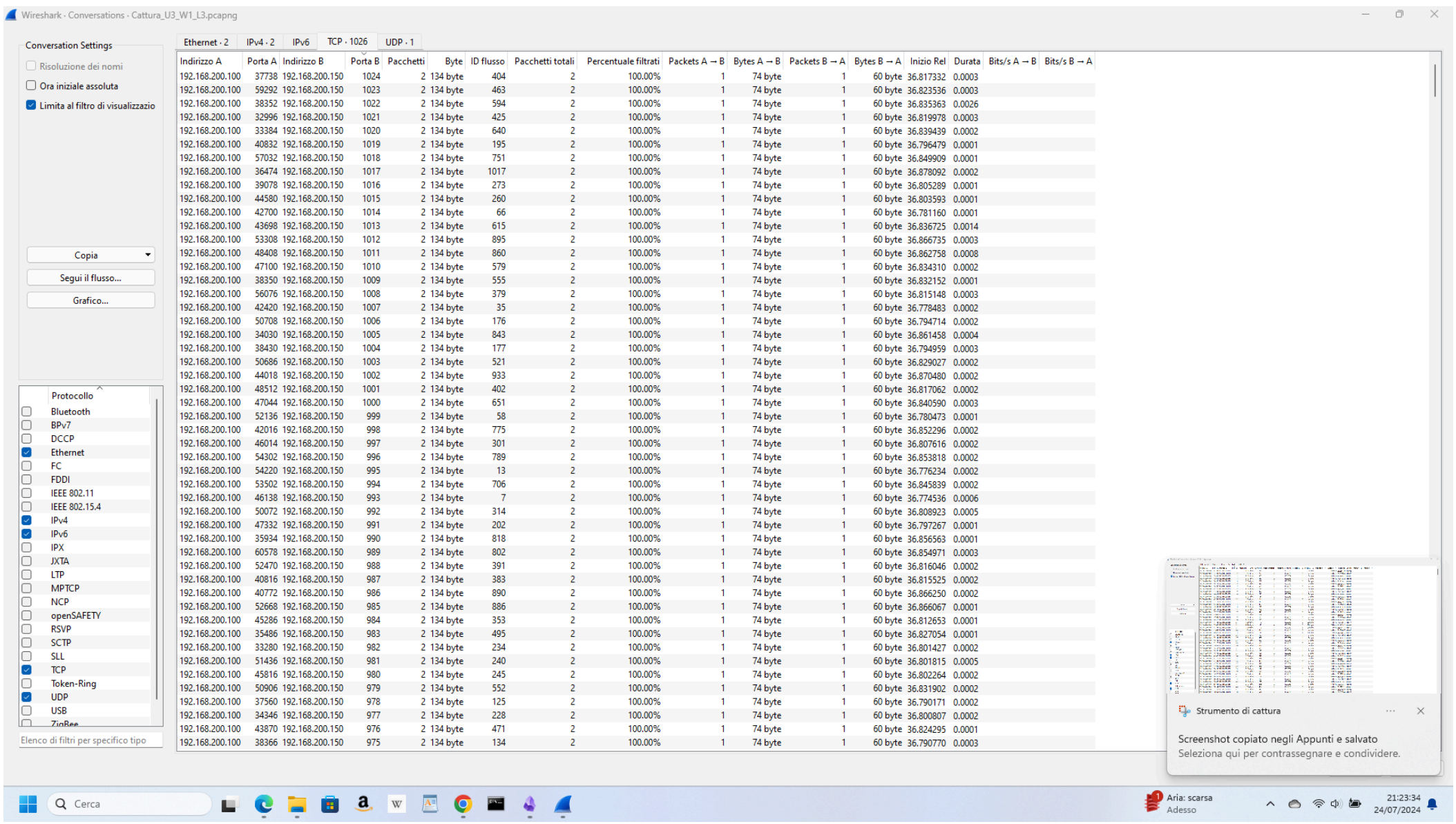


Spostandoci successivamente su Statistiche e selezionando conversazioni è possibile notare che la tab TCP è quella con più entries e di conseguenza ci spostiamo lì

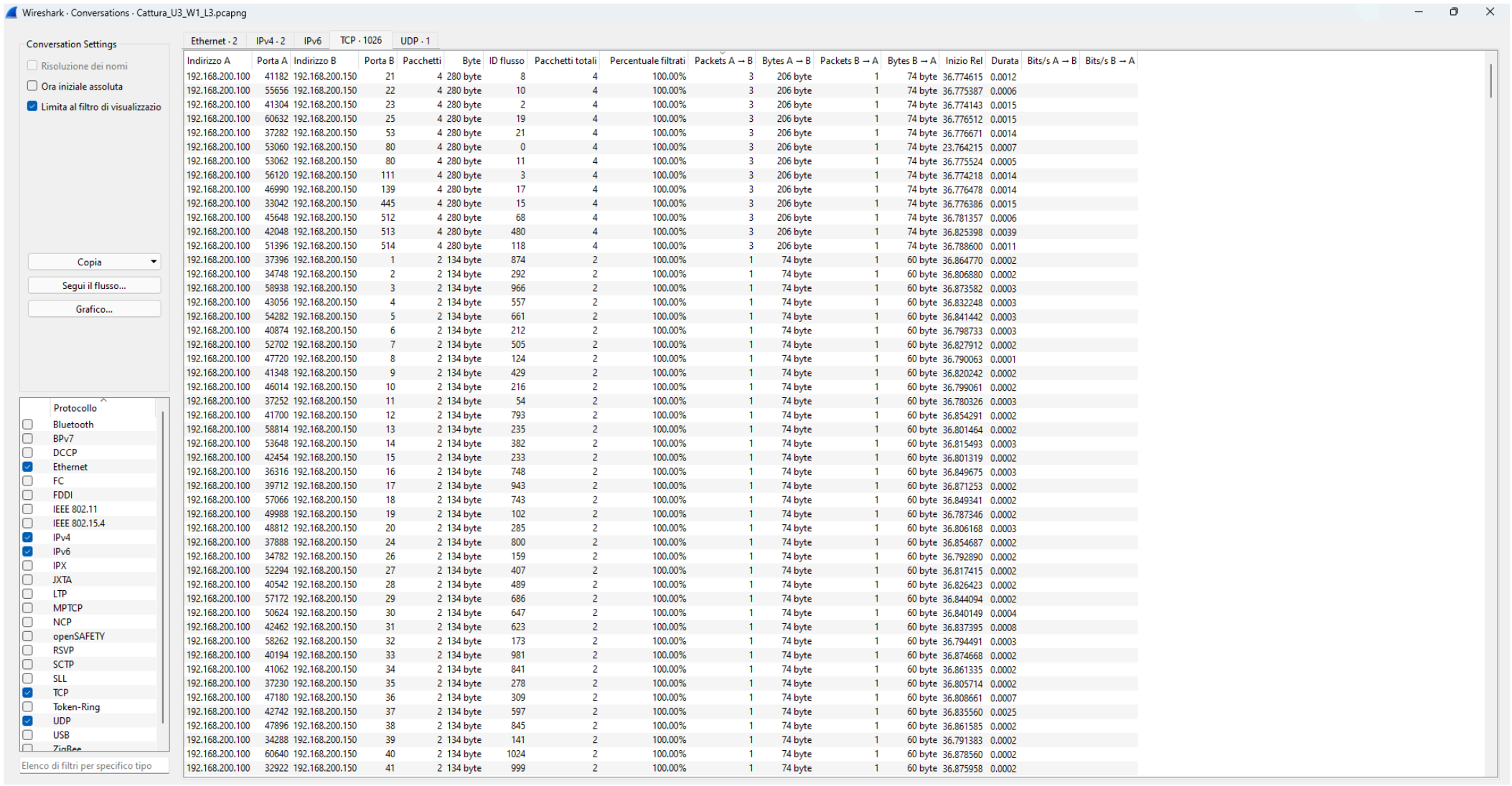


Soffermandoci in particolar modo sulla colonna “**Porta B**” e cliccando su di essa per ordinare le porte, è possibile notare come siano indicate tutte le porte dalla 1 alla 1024 che sappiamo essere il numero di porte “ben note”, ovvero su cui solitamente stanno in ascolto i servizi noti e ben definiti. Questo è indice di una scansione effettuata molto probabilmente tramite “**Nmap**”, un tool comunemente usato per identificare le porte aperte e i servizi attivi su un computer in una rete. In particolar modo, analizzando il caso specifico, si rileva che le richieste TCP provengono dalla macchina con IP 192.168.200.100 e sono dirette verso diverse porte dell'host con IP 192.168.200.150





A questo punto, spostandoci sulla colonna **Packets A -> B** e ordinando la colonna dal più grande al più piccolo, possiamo notare come vi siano alcune entrate dove il valore della colonna è 3 e altre dove il valore della colonna è 1. Questo ci ricorda il **three way handshake**, da cui è possibile supporre che la scansione specifica utilizzata sia stata un TCP Connect Scan, indicato dall'opzione -sT in Nmap. Questo tipo di scansione, come dicevamo in precedenza, si avvale del completo three-way handshake, un processo fondamentale nel protocollo TCP, per stabilire una connessione. Il three-way handshake consiste in tre fasi: **SYN** (synchronize), **SYN-ACK** (synchronizeacknowledge), e **ACK** (acknowledge). Quando una porta è aperta, il target risponde con un SYN-ACK dopo aver ricevuto un SYN, e la scansione completa il processo inviando un ACK. Questo è diverso dal SYN Scan (opzione -sS in nmap), che non completa il three-way handshake e si limita a inviare un pacchetto RST (reset) dopo aver ricevuto il SYN-ACK, riducendo così la visibilità della scansione. Di conseguenza, è possibile ipotizzare che le porte con 3 pacchetti fossero aperte e quelle con 1 pacchetto chiuse.

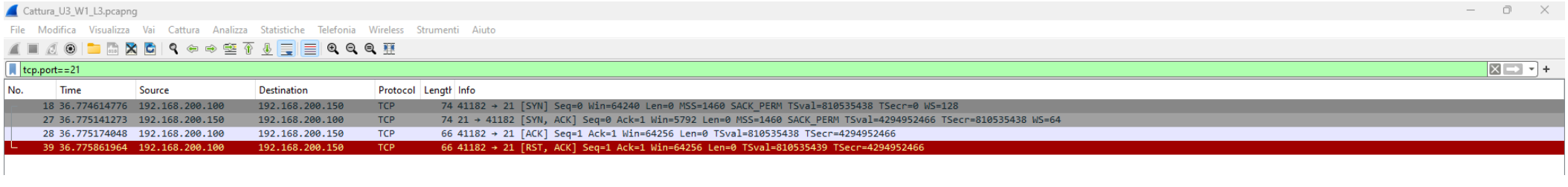


In effetti, le possibili porte aperte identificate nella terza colonna, sono le porte tipicamente associate ai servizi più comuni. Volendo fare alcuni esempi, possiamo vedere la porta 21 che è associata al protocollo FTP (File Transfer Protocol) che è utilizzato per il trasferimento di file; La porta 80 che è riservata al protocollo HTTP (Hypertext Transfer Protocol), comunemente utilizzato per il traffico Web non crittografato e la porta 445 che è comunemente associata al protocollo SMB (Server Message Block) usato per la condivisione di file e risorse in reti Microsoft Windows. A questo punto, appuntiamoci i numeri delle porte identificate, torniamo alla schermata principale di Wireshark e applichiamo dei filtri che ci permettano di selezionare solamente i pacchetti scambiati tramite le porte TCP scelte.

Il comando da digitare nel campo del filtro per fare questo è il seguente:

tcp.port==[numero porta]

Nel nostro caso, andremo a ispezionare la porta 21 e quindi a digitare: **tcp.port==21** dove è possibile vedere la sequenza SYN, SYN ACK, ACK, RST ACK, tipica di una scansione TCP con Nmap, ovvero una scansione che completa la connessione.



Consigli per ridurre gli impatti dell’attacco

Alla luce delle vulnerabilità esposte da una scansione delle porte, è fondamentale adottare misure preventive e di mitigazione per ridurre il rischio di attacchi. Ecco alcune raccomandazioni:

- **Chiudere le porte critiche:** nel nostro caso, le porte come ftp (21), ssh (22), telnet (23), SMTP (25), DNS (53), http (80), portmapper RPC (111), netbios (139), smb (445) e quelle per il remote login, se non sono essenziali, devono essere chiuse. Questo riduce la superficie di attacco disponibile. È importante notare che alcune di queste porte potrebbero essere utilizzate da servizi legittimi all'interno dell'organizzazione, pertanto, una valutazione approfondita è necessaria prima di chiuderle.

- **Firewall e accesso limitato:** configurare policy di sicurezza sui firewall per limitare l'accesso ai servizi esposti è cruciale. Questo può includere l'abilitazione di regole che consentono l'accesso solo a specifici indirizzi IP autorizzati. È anche consigliabile impiegare tecniche come il filtraggio degli indirizzi MAC, quando possibile, per un ulteriore livello di sicurezza.

- **Autenticazione forte e controllo accessi:** dove i servizi sono necessari e devono rimanere aperti, assicurarsi che vi siano misure di autenticazione forte e controllo degli accessi. L'uso di password complesse, l'autenticazione a più fattori (MFA) e certificati digitali può notevolmente aumentare la sicurezza.

- **Aggiornamenti e patch di sicurezza:** mantenere aggiornati i sistemi e le applicazioni è fondamentale. Gli aggiornamenti spesso includono patch per vulnerabilità di sicurezza note che potrebbero essere sfruttate da un attaccante.

- **Monitoraggio e analisi del traffico di rete:** implementare soluzioni di monitoraggio del traffico di rete per identificare modelli di traffico insoliti o sospetti. Gli strumenti di rilevamento delle intrusioni (IDS) e i sistemi di prevenzione delle intrusioni (IPS) possono aiutare a identificare e bloccare attività potenzialmente dannose.

- **Sicurezza a livelli multipli (Defense in Depth):** applicare un approccio di sicurezza a più livelli, dove diversi strati di sicurezza lavorano insieme per proteggere gli asset. Questo può includere, oltre ai firewall e al controllo degli accessi, la segregazione della rete, la cifratura dei dati e la formazione degli utenti sulla sicurezza informatica.

- **Valutazioni periodiche di sicurezza:** effettuare regolari valutazioni di sicurezza e penetration test per identificare e mitigare le vulnerabilità prima che possano essere sfruttate.