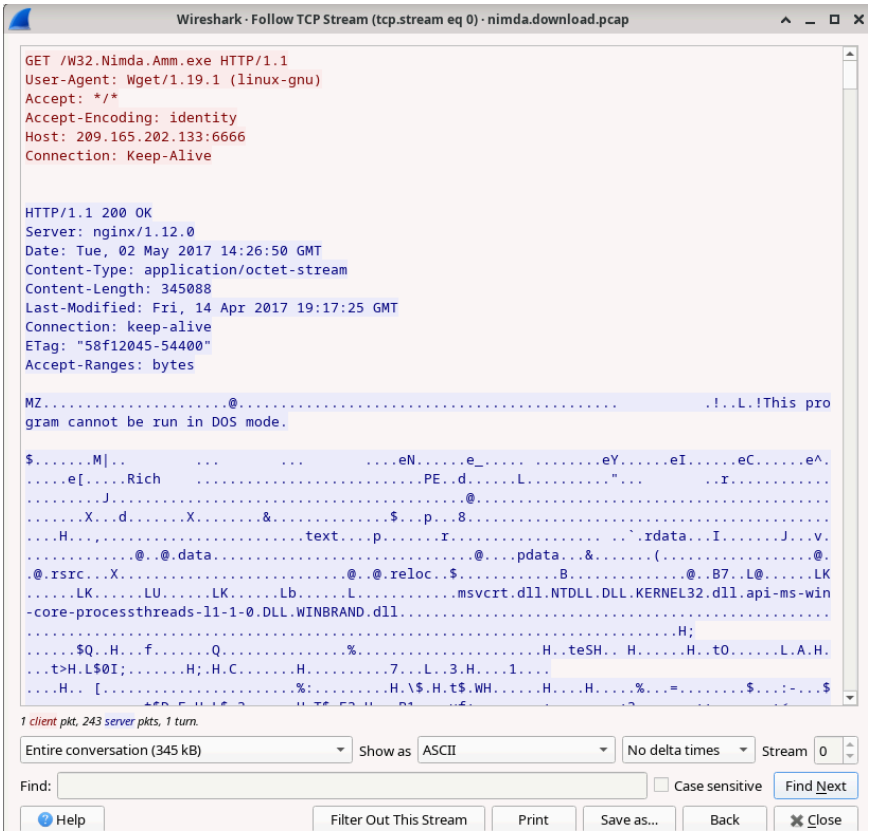
# Esercizio 6: Estrarre un Eseguibile da un PCAP

## 1.Cosa sono tutti quei simboli mostrati nella finestra Follow TCP Stream? Sono rumore di connessione? Dati? Spiega. Ci sono alcune parole leggibili sparse tra i simboli. Perché sono lì?

Non sono rumori ma byte binari del file trasmessi via rete. I caratteri leggibili (MZ, DOS mode, DLL, ecc.) fanno parte dell'header e delle stringhe interne di un file PE di Windows, confermando che si tratta di un .exe.




## 2.Domanda Sfida: Nonostante il nome W32.Nimda.Amm.exe, questo eseguibile non è il famoso worm. Per motivi di sicurezza, questo è un altro file eseguibile che è stato rinominato come W32.Nimda.Amm.exe. Usando i frammenti di parole visualizzati dalla finestra Follow TCP Stream di Wireshark, puoi dire quale eseguibile sia realmente?

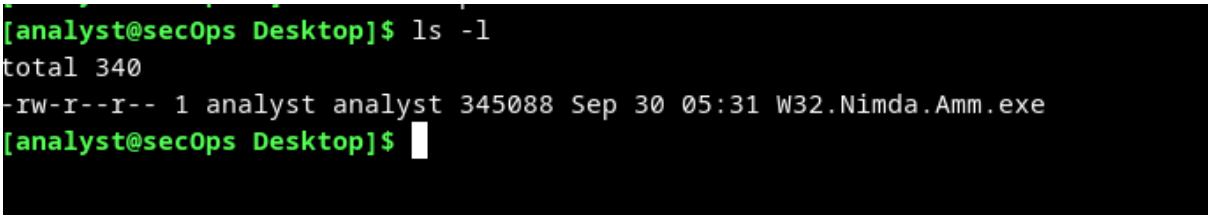
L'eseguibile è un branding che mostra la versione di windows, ce ne siamo accorti dalla libreria "WINBRAND.dll

## 3.Perché W32.Nimda.Amm.exe è l'unico file nella cattura?

La cattura ha rilevato solo questo .exe, se ci fossero stati altri file cifrati, l’export object di wireshark non li avrebbe considerati

## 4.Il file è stato salvato?

Si, il file è stato salvato con successo.




## 5.Nel processo di analisi del malware, quale sarebbe un probabile passo successivo per un analista di sicurezza?

In un’analisi di sicurezza il primo passo sarebbe un’analisi statica del malware, confermando che sia un malware vero e proprio,controllare hash, ecc .
Senza eseguire il file sull’host: spostare il file in una VM isolata “FLAREVM” con snapshot e rete controllata per procedere come passo successivo ad un’analisi statica dinamica base.