Relazione sull'Analisi del Malware attraverso il File PCAP: W32.Nimda.Amm.exe

Obiettivo: Questa attività di laboratorio si concentra sull'analisi e l'estrazione di un file eseguibile contenente malware dal file `nimda.download.pcap`, usando strumenti come Wireshark per ispezionare il traffico catturato e identificare i pacchetti relativi a un download di malware.

Fase 1: Configurazione Iniziale e Apertura del File

1. **Individuazione del File di Interesse**:
    - L'utente ha cambiato directory nella cartella `/home/analyst/lab.support.files/pcaps` e ha elencato i file per verificare la presenza del file `nimda.download.pcap`, che contiene i pacchetti del download del malware Nimda.
2. **Apertura in Wireshark**:
    - Utilizzando Wireshark, è stato caricato il file `nimda.download.pcap`. L'interfaccia grafica di Wireshark facilita l'analisi del contenuto catturato, in particolare dei pacchetti che compongono il download.
3. **Analisi del Protocollo e del Flusso TCP**:
    - Il quarto pacchetto è stato selezionato e l'espansione del protocollo HTTP ha rivelato che il download del malware è stato effettuato tramite una richiesta HTTP di tipo GET.
4. **Ricostruzione del Flusso TCP**:
    - È stata utilizzata la funzionalità "Follow TCP Stream" di Wireshark per ricostruire il flusso completo della transazione TCP, visualizzando i contenuti effettivi del file scaricato.

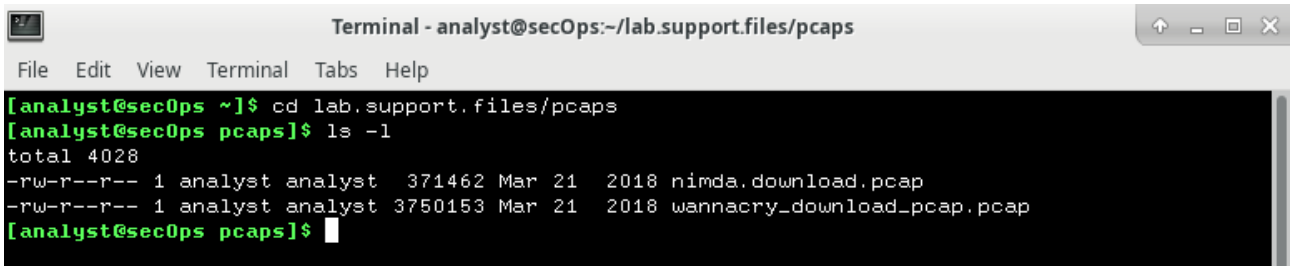
Fase 2: Estrazione del File Eseguibile

1. **Selezione e Salvataggio del File HTTP**:
    - Il pacchetto con la richiesta HTTP GET è stato selezionato, e tramite Wireshark, è stata esportata l'oggetto HTTP, ovvero il file `W32.Nimda.Amm.exe`. Il file è stato salvato nella cartella `/home/analyst`.
2. **Verifica del Salvataggio e Tipologia del File**:
    - Utilizzando il comando `file`, è stato confermato che `W32.Nimda.Amm.exe` è un eseguibile per Windows a 64 bit, in formato PE32+.

L'attività ha permesso di comprendere e applicare tecniche di analisi forense per il recupero di file da traffico di rete, l'identificazione dei pacchetti critici e l'estrazione di oggetti da un flusso TCP. Questo processo fornisce una base solida per la gestione del malware, la sua identificazione e l'analisi per la sicurezza in contesti operativi.

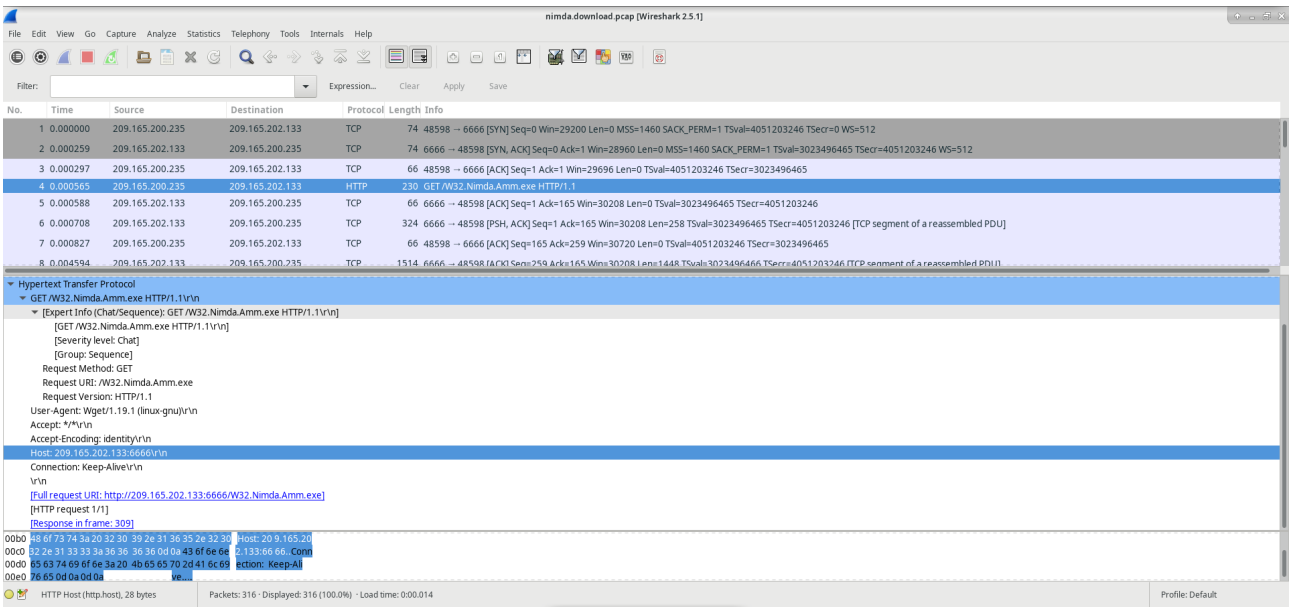
27.2.10 Lab – Estrazione di un file eseguibile da un file PCAP

Prima di tutto, apriamo un terminale, ci spostiamo nella directory contenente i files .pcap con il comando **cd lab.support.files/pcaps** e utilizziamo il comando **ls -l** per ottenere una lista dei files presenti nella directory:

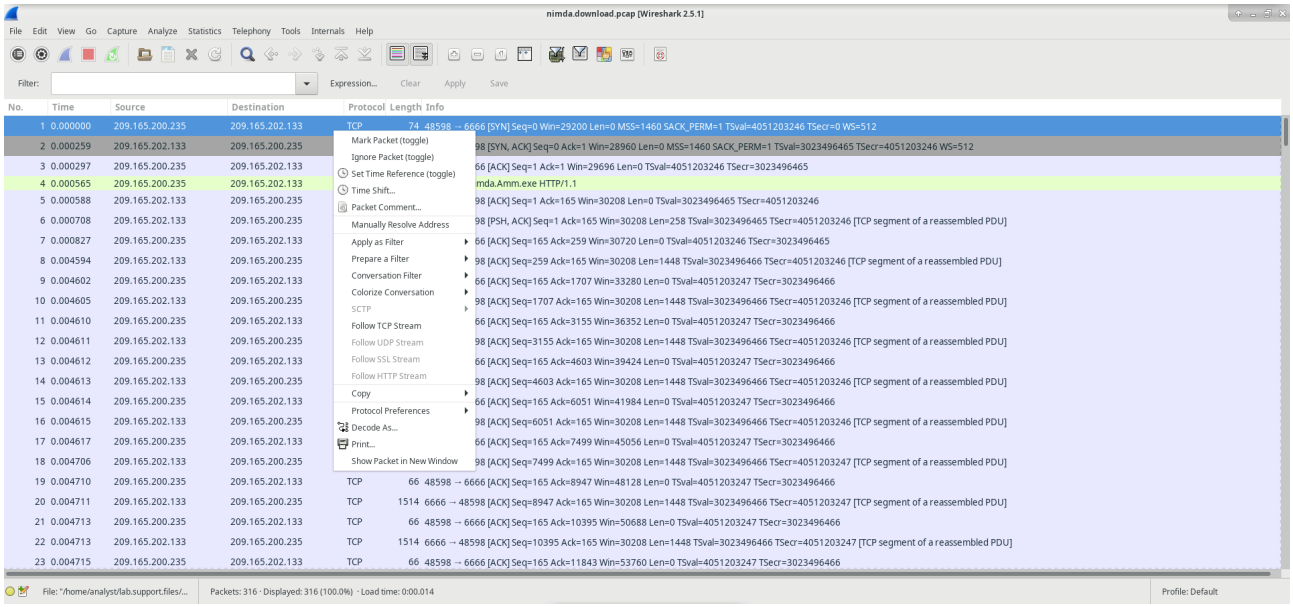


Dopo aver individuato il file **nimda.download.pcap,** utilizziamo il comando **wireshark nimda.download.pcap &** per aprire il file con Wireshark:

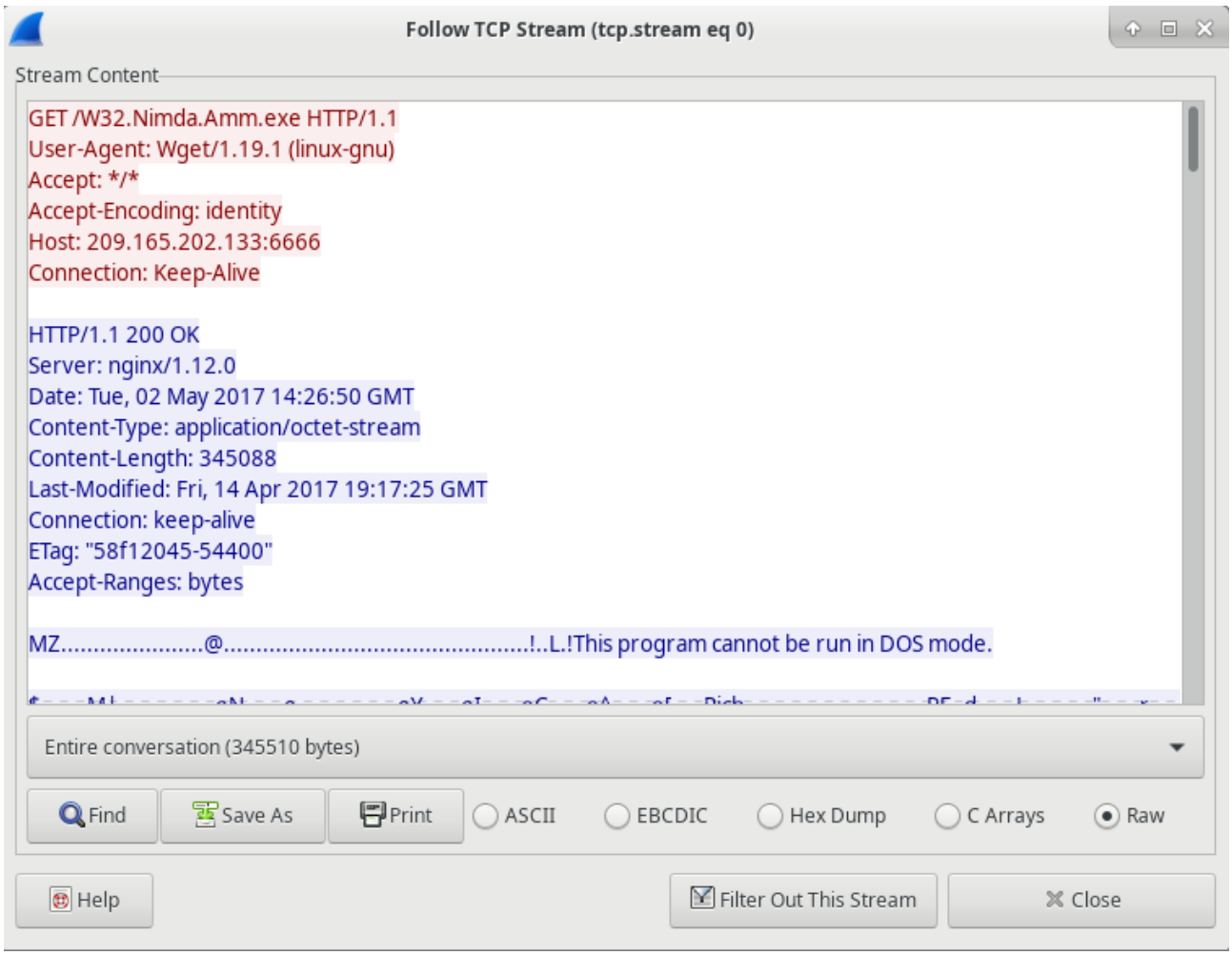
Di fronte a questa schermata, che ci mostra tutti i pacchetti inviati e ricevuti mentre tcpdump era in esecuzione, andiamo a selezionare il quarto pacchetto, che mostra la richiesta per il file contenente il malware:



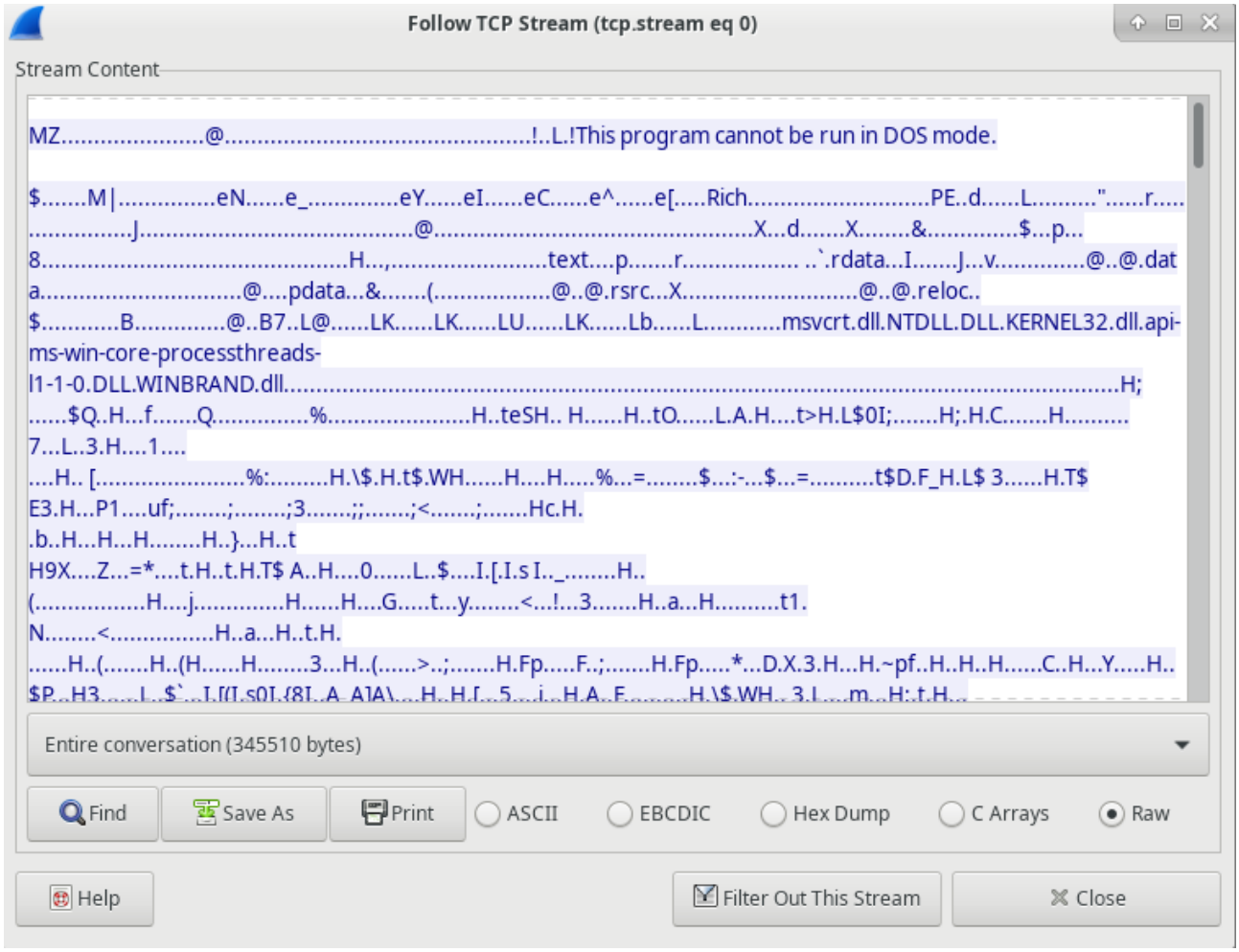
Successivamente, clicchiamo col tasto destro sul primo pacchetto, ovvero l'inizio del **TCP handshake** e selezioniamo la voce **Follow TCP Stream**. In questo modo, possiamo ricostruire ciò che è avvenuto durante lo scambio di pacchetti:



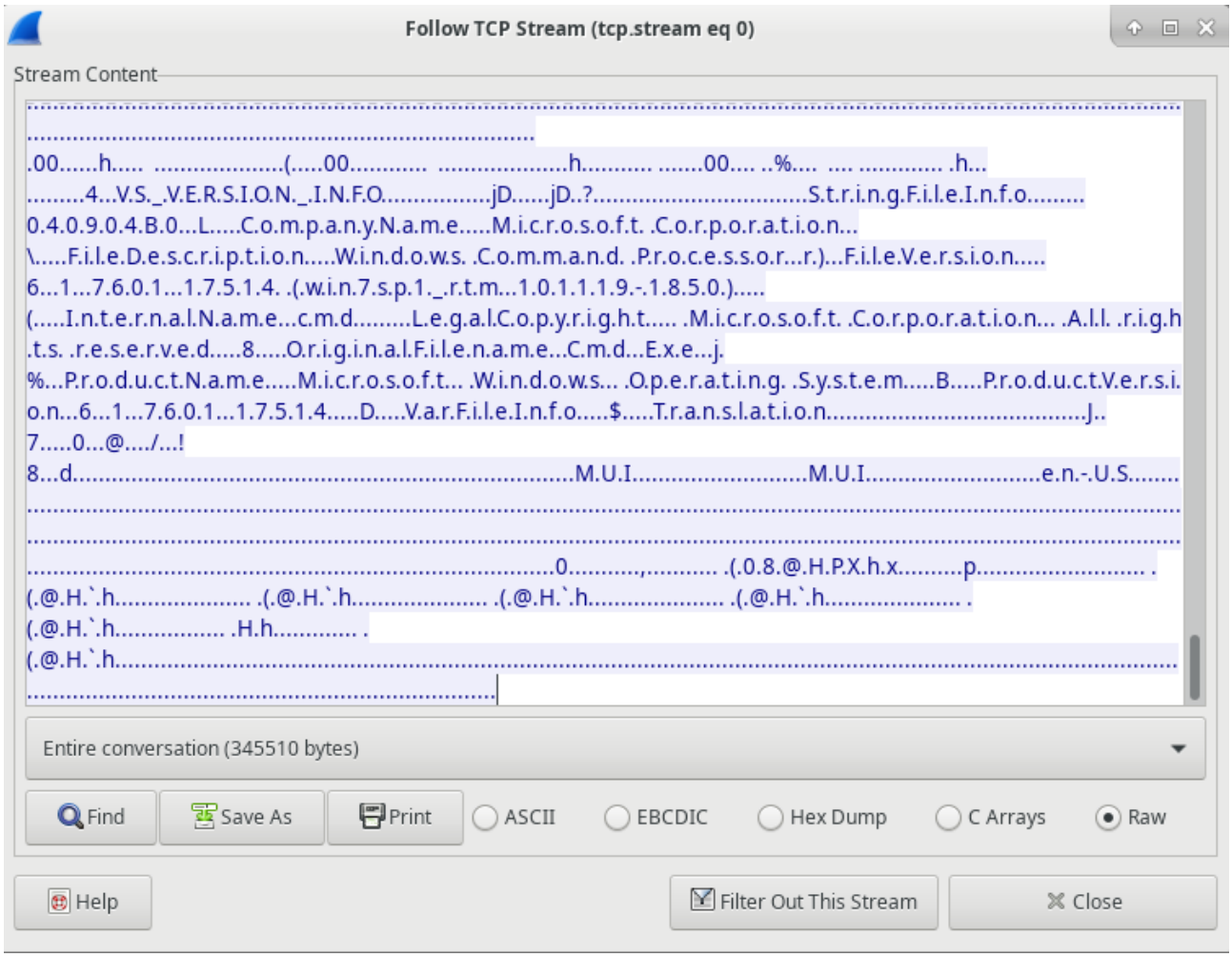
Si aprirà la seguente finestra, contentente tutti i dettagli relativi al flusso TCP:



Navigando all'interno della finestra, ci imbattiamo in simboli, che non sono altro che il contenuto del file scaricato. Poiché si tratta di un file binario, Wireshark non sa come rappresentarlo. I simboli visualizzati rappresentano la migliore ipotesi di Wireshark per dare un senso ai dati binari decodificandoli come testo. Inoltre, possiamo notare la presenza di alcune parole leggibili tra i vari simoboli. Di solito, queste parole fanno parte dei messaggi forniti dal programma all'utente durante l'esecuzione:

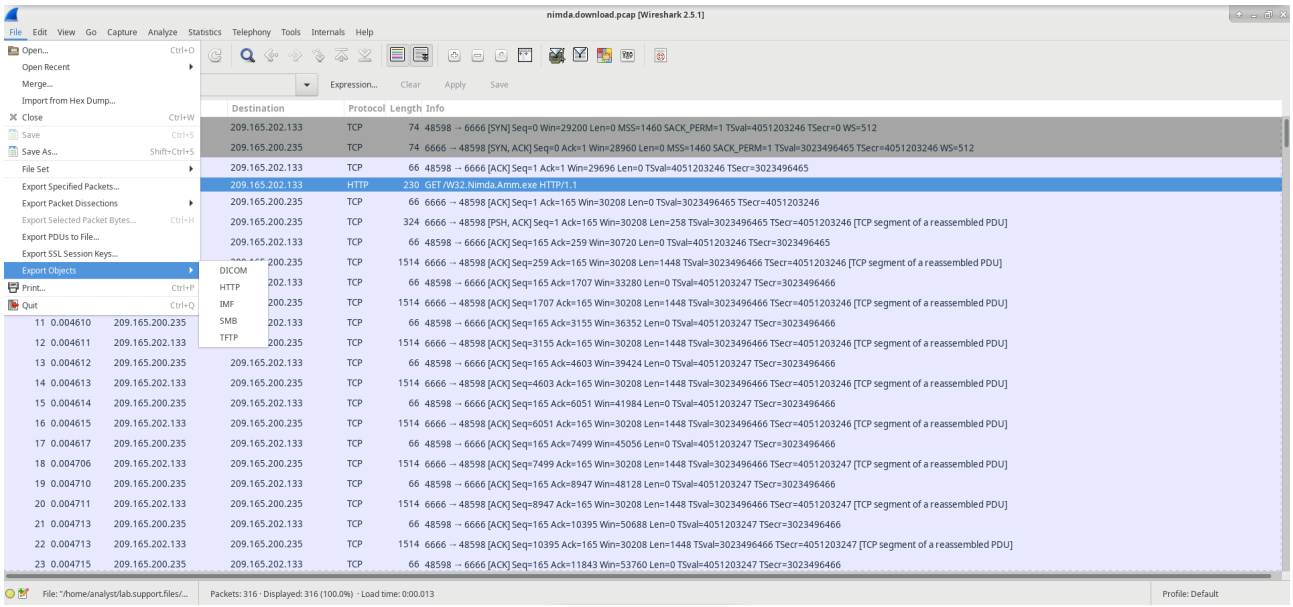


Nonostante il nome **W32.Nimda.Amm.exe**, questo eseguibile non è il famoso worm. Per motivi di sicurezza, questo è un altro file eseguibile che è stato rinominato **W32.Nimda.Amm.exe**. Usando i frammenti di parole visualizzati dalla finestra **Follow TCP Stream** di Wireshark, possiamo risalire alla vera identità dell'eseguibile. Scorrendo fino in fondo a quella finestra, scopriamo che si tratta del file **cmd.exe** di **Microsoft Windows**:

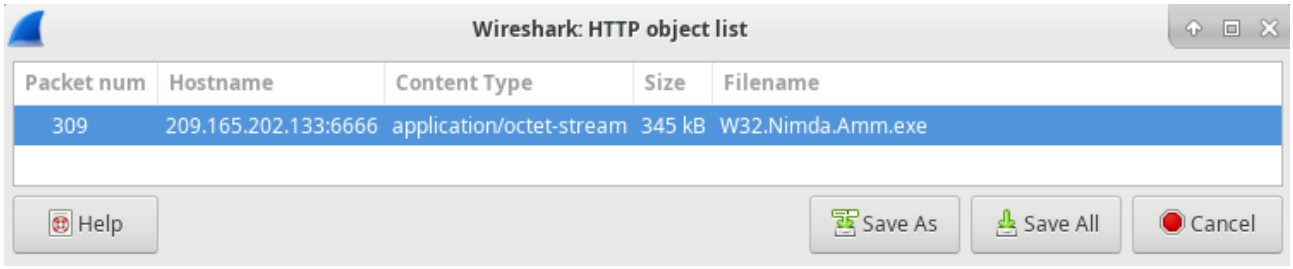


Poiché i file di acquisizione, contengono tutti i pacchetti relativi al traffico, è possibile utilizzare un PCAP di un download per recuperare un file scaricato in precedenza.

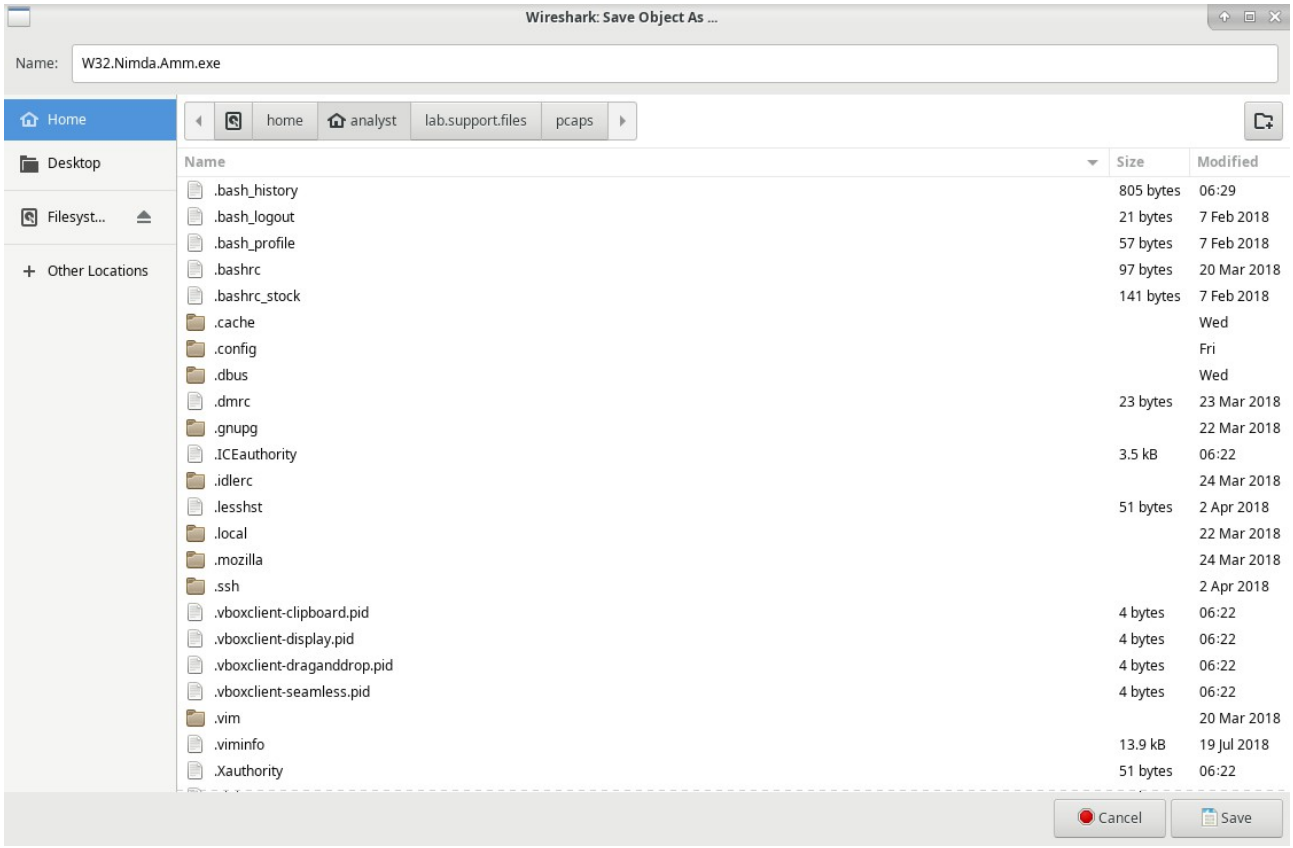
Nel quarto pacchetto nel file download.pcap, notiamo che la richiesta **HTTP GET** è stata generata da **209.165.200.235** a **209.165.202.133**. La colonna **Info** mostra anche che questa è in effetti la richiesta **GET** per il file. Mentre il quarto pacchetto è selezionato, andiamo su **File**, clicchiamo su **Export Objects** e infine su **HTTP**:



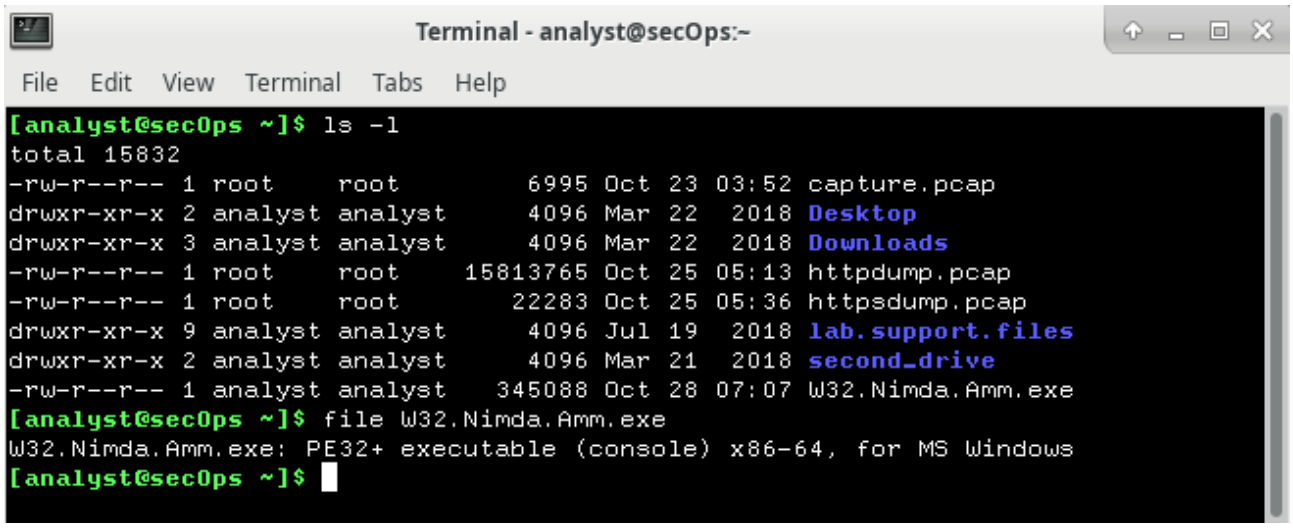
Wireshark visualizzerà tutti gli **oggetti HTTP** presenti nel **flusso TCP** che contiene la **richiesta GET**. In questo caso, nella cattura è presente solo il file **Nimda.Amm.exe**. Questo perché l'acquisizione è stata avviata subito prima del download e interrotta subito dopo. Nessun altro traffico è stato catturato mentre l'acquisizione era attiva:



Dopo aver cliccato su **Save as** nella parte inferiore della finestra precedente, ci si apre questa nuova finestra e non dobbiamo fare altro che salvare il file nella directory **analyst** che è presente in **home**:



Dopo aver salvato il file, non ci resta che verificare di averlo salvato dove volevamo. Assicuriamoci di ciò tramite l'esecuzione del comando del comando **ls -l**. Una volta accertata la presenza del file, possiamo utilizzare il comando **file** seguito dal **nome del file** che abbiamo scaricato per visualizzarne le informazioni:



Come possiamo notare, il file **W32.Nimda.Amm.exe** è effettivamente un file eseguibile di Windows.