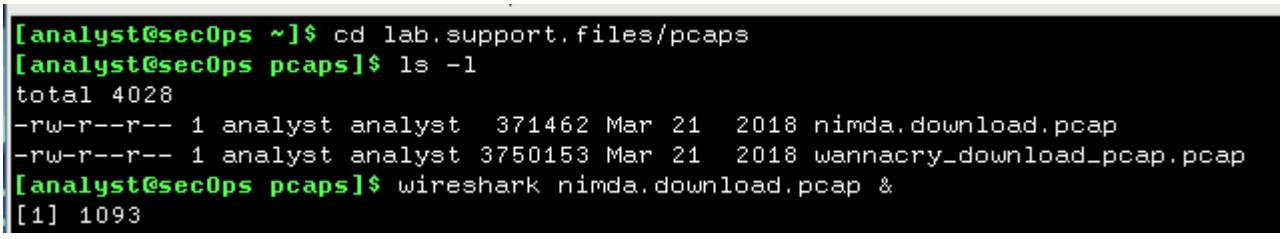
BW3 es.4 Analisi file pcap

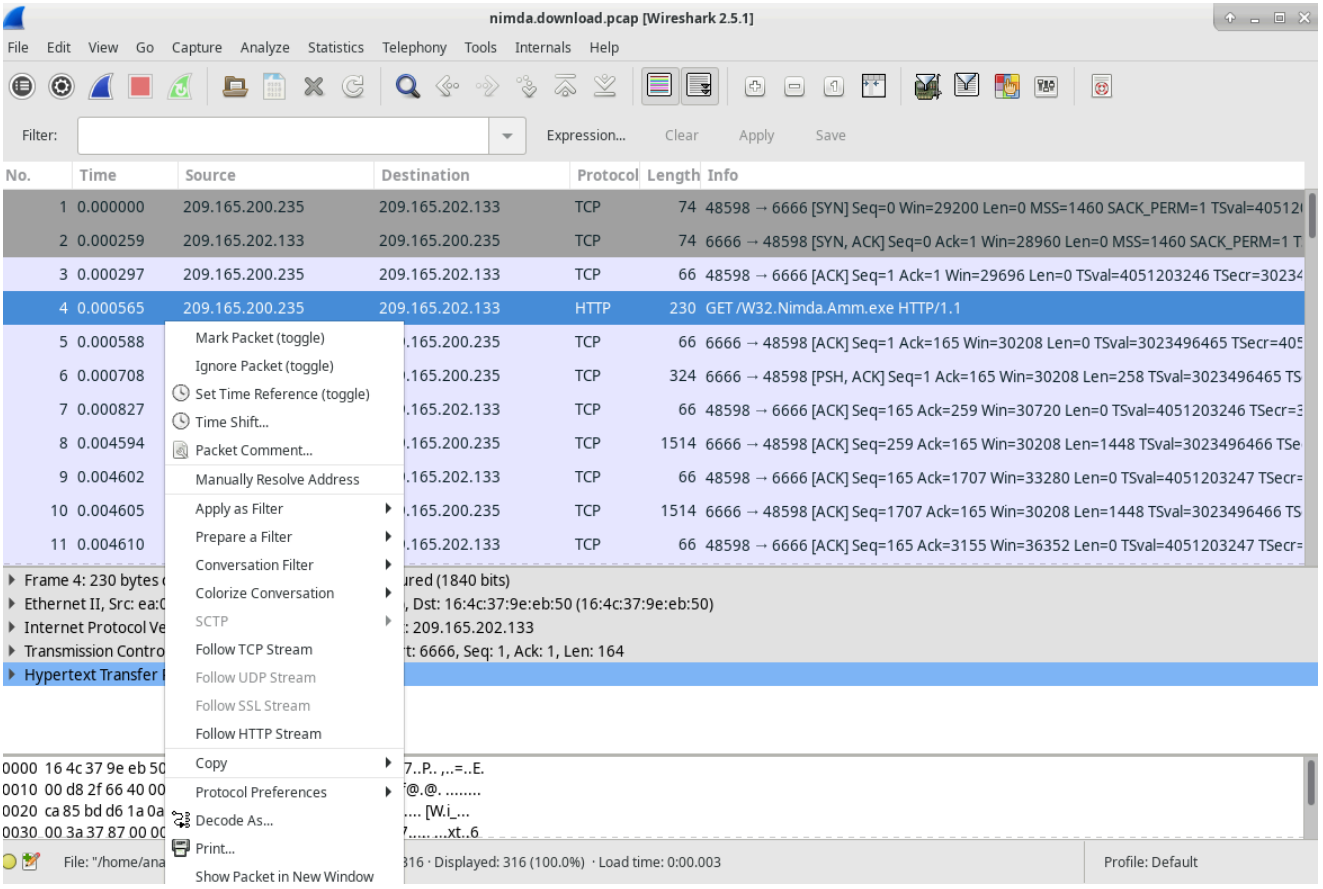
Parte 1: Analisi dei Log Pre-Catturati - Analyzing Pre-Captured Logs

⚜️ **Tag:** #wireshark #tcp #http #analisi_pacchetti

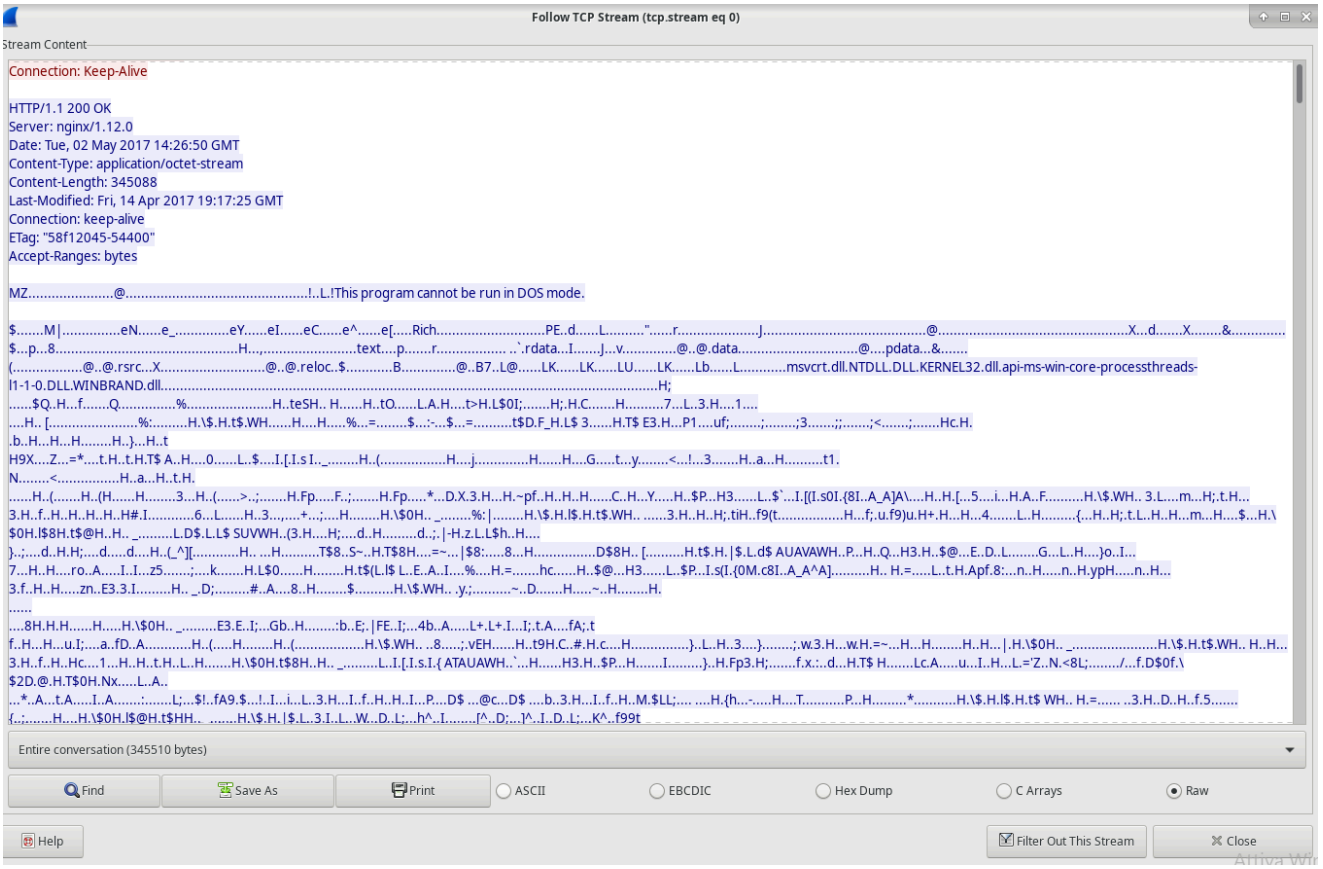
1. **Cambio Directory e Visualizzazione File**:
   - **Comando**: `ls -l` nella directory `support.files/pcaps` per elencare i file disponibili.
   - **Apertura File**: `download.pcap` viene aperto in Wireshark per l'analisi.



2. **Descrizione del File**:
   - Il file `download.pcap` contiene pacchetti relativi al download di un malware, catturati con `tcpdump` in una sessione precedente.
3. **Analisi dei Pacchetti**:
   - **Handshake TCP**: I pacchetti da uno a tre rappresentano il processo di handshake TCP.
   - **Quarto Pacchetto**: Mostra la richiesta GET HTTP per il download del malware.



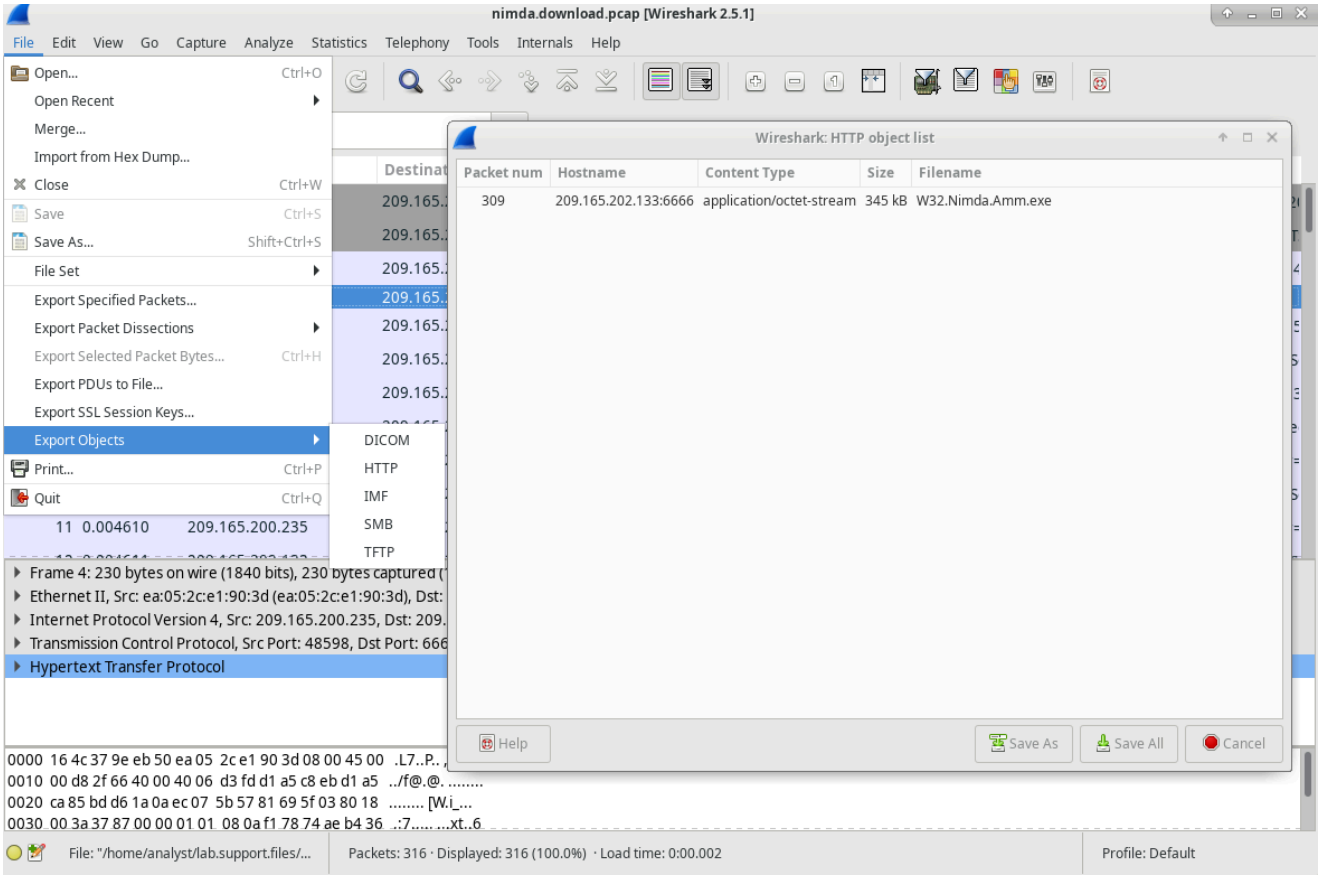
4. **Follow TCP Stream**:
    - Seleziono il primo pacchetto SYN e uso la funzione **Follow > TCP Stream** per ricostruire la transazione TCP completa.



Parte 2: Estrazione di File da PCAP - Extracting Files from PCAP

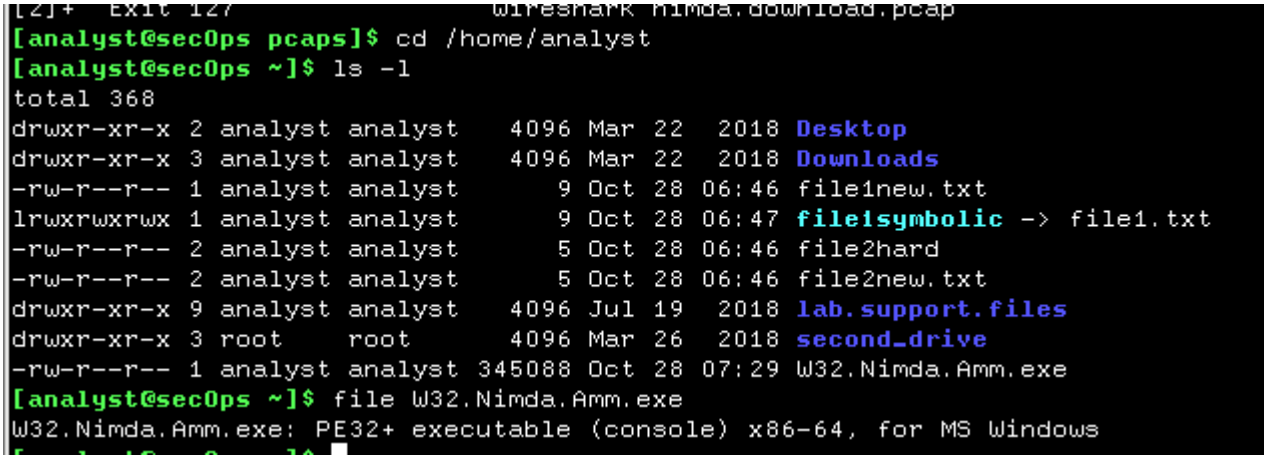
⚜️ **Tag:** #estrazione_file #wireshark #pcap #malware

1. **Estrazione del File HTTP**:
    - Con la richiesta GET selezionata, navigo in **File > Esporta oggetti > HTTP** per visualizzare gli oggetti HTTP nel flusso.
    - **File Identificato**: `Nimda.Amm.exe`, file sospetto, presente nel flusso TCP e selezionabile per il salvataggio.
2. **Salvataggio del File Estratto**:
    - Seleziono `Nimda.Amm.exe`, clicco su **Salva con nome**, e scelgo la cartella `analyst` come destinazione.



3. **Verifica e Identificazione del File**:
    - Dopo il salvataggio, cambio directory in `/home/analyst` e uso `ls -l` per confermare la presenza del file.

- **Comando**: `file W32.Nimda.Amm.exe` per verificare il tipo di file.
- **Risultato**: `W32.Nimda.Amm.exe` è identificato come eseguibile di Windows.



🔑 **Chiavi:**
[wireshark, pcap, tcp, http, estrazione file, malware, tcpdump, download.pcap]
