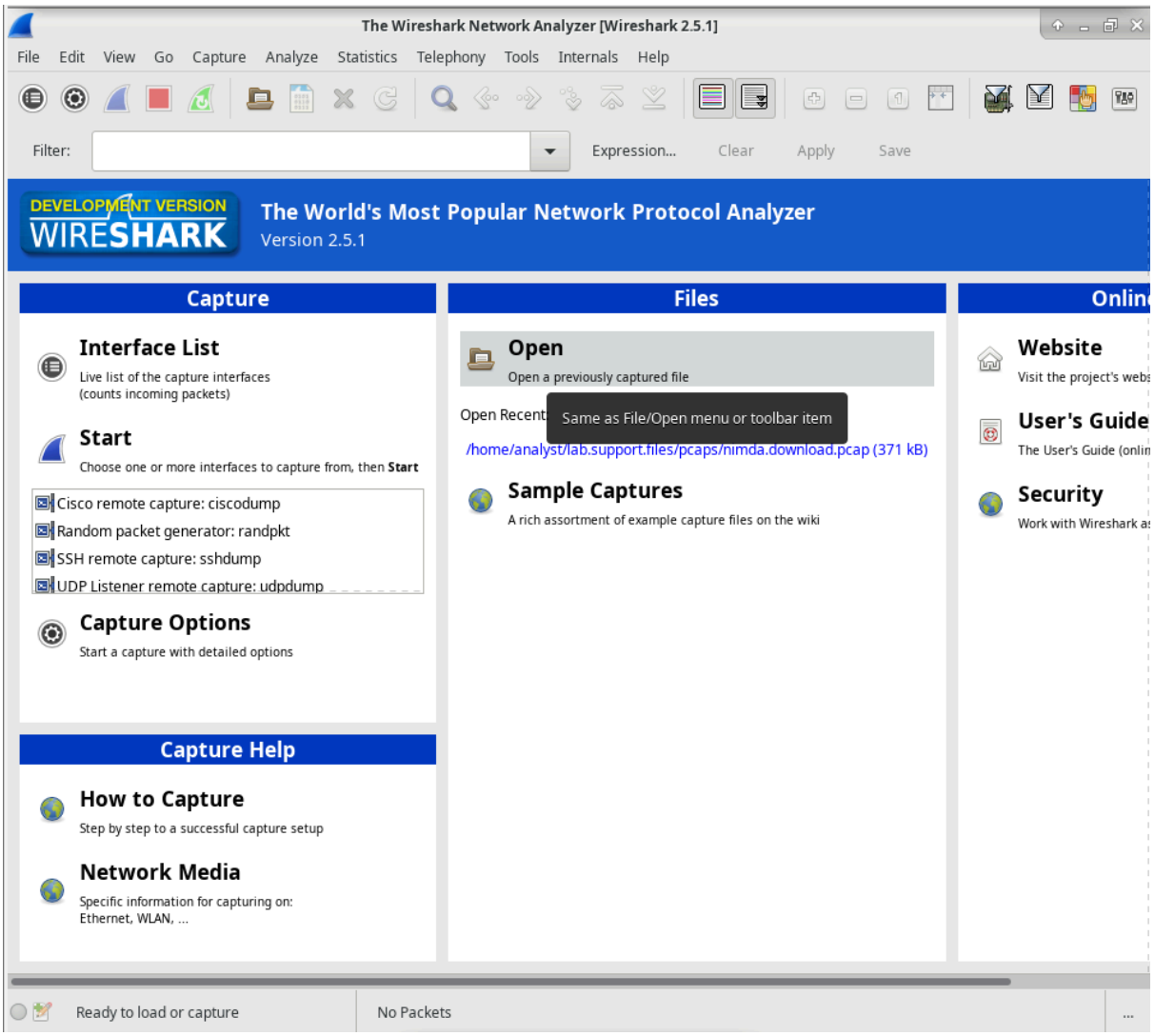
Guida per l'Analisi del Traffico di Rete e l'Estrazione di File Eseguibili da un File PCAP

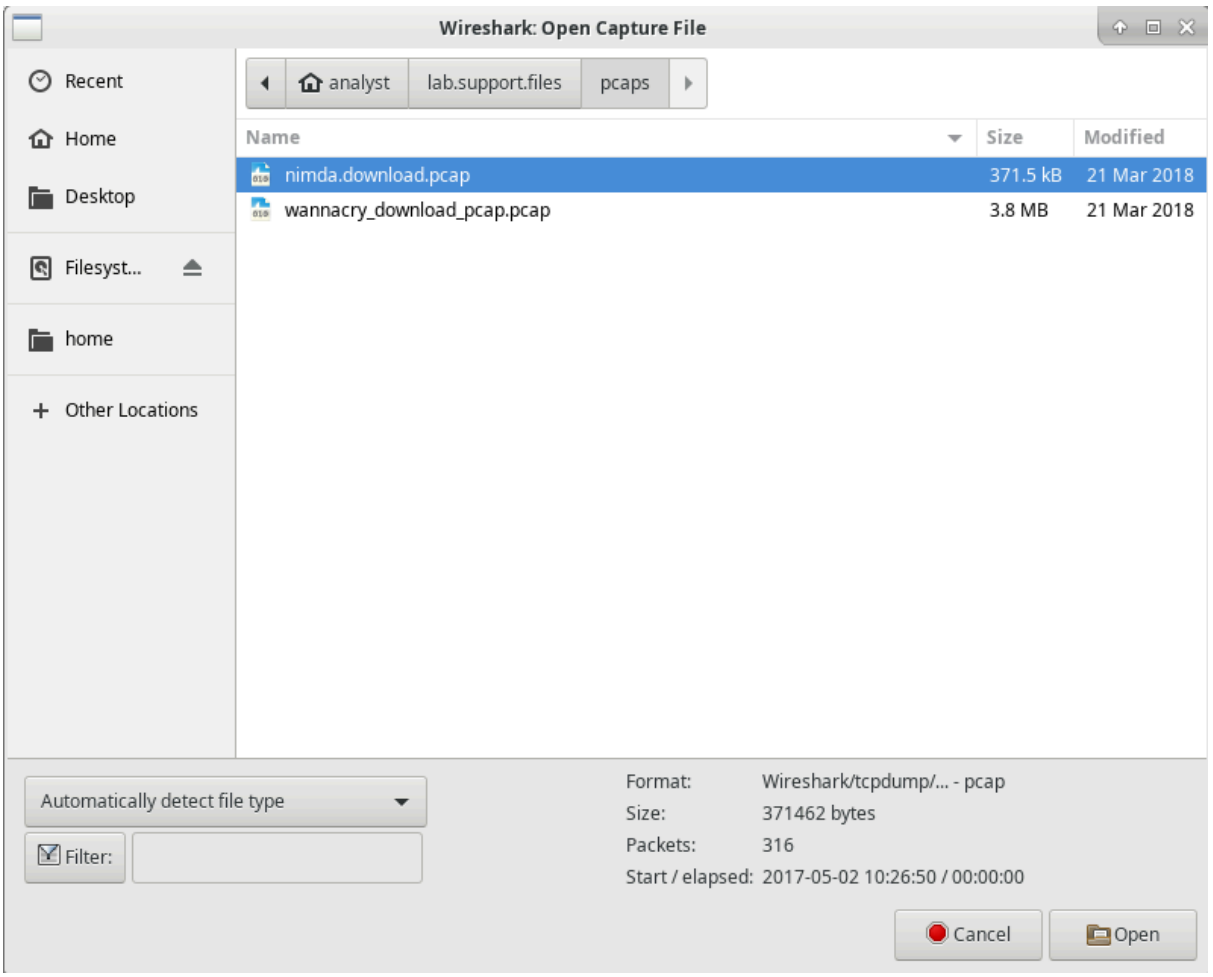
Parte 1: Analisi del Traffico di Rete con Wireshark

1. **Apertura del file PCAP**:
    - Avvia Wireshark

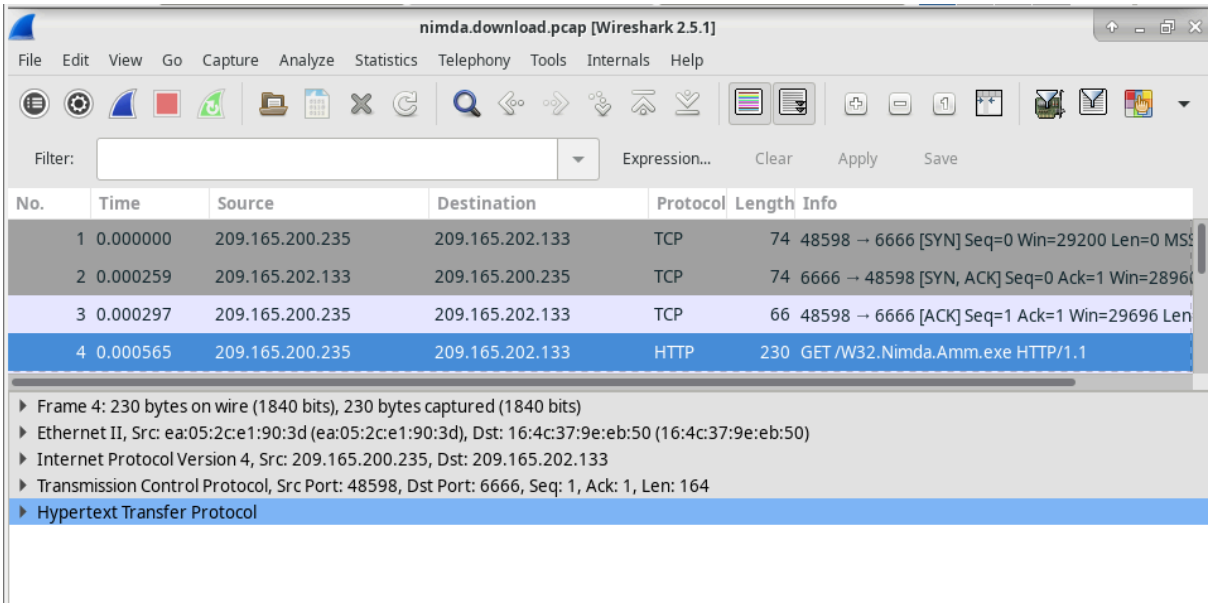
e carica il file `.pcap` contenente i dati di rete acquisiti in precedenza.



Selezioniamo dunque il file nimda.download.pcap



Questo file rappresenta una cattura di traffico di rete che dovrai analizzare.

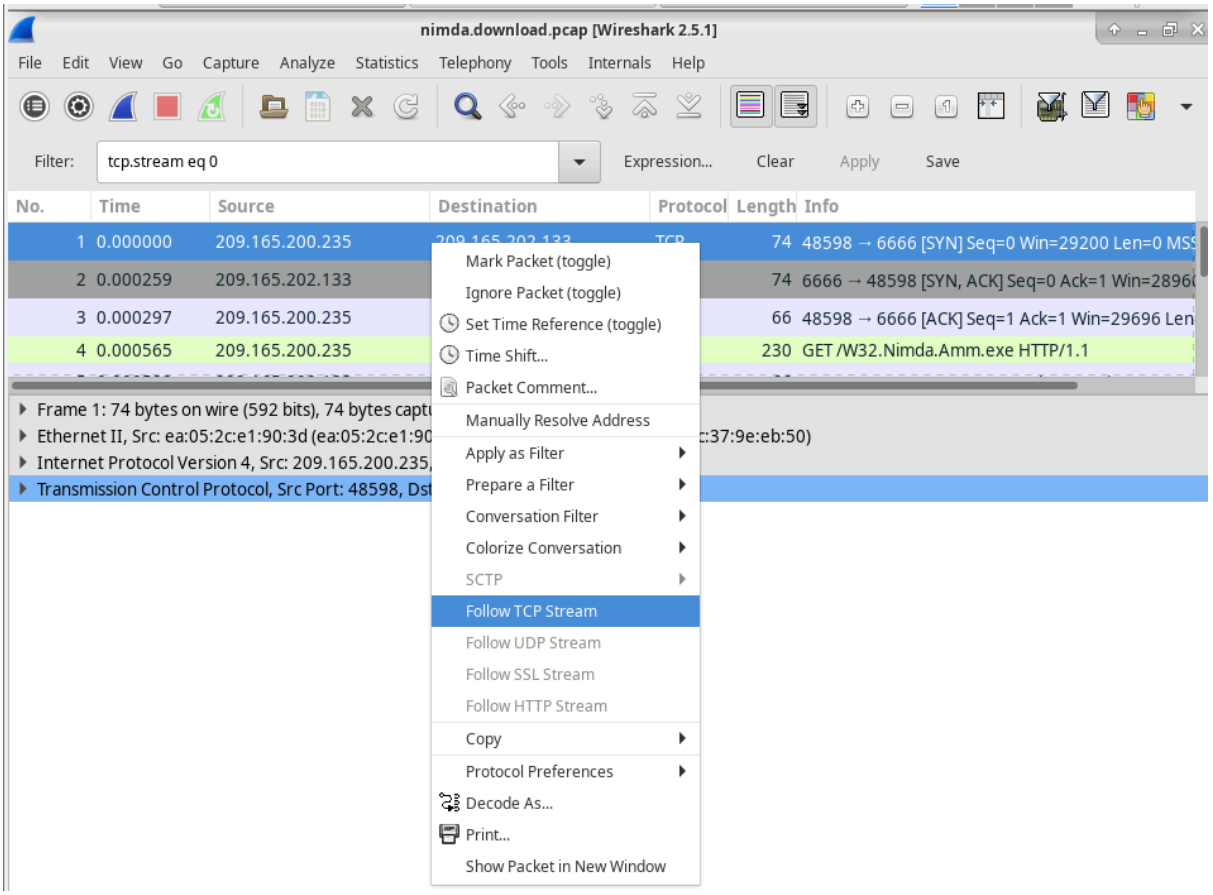


2. **Navigazione nel Traffico**:
    - Possiamo utilizzare i filtri per ridurre il traffico visualizzato, ad esempio applicando l'indirizzo IP della sorgente o della destinazione.
    - Filtra ulteriormente con `http` o altri protocolli per isolare pacchetti HTTP, come quelli relativi a richieste GET per file eseguibili. In questo caso, cerca pacchetti HTTP che possono includere file `.exe`.

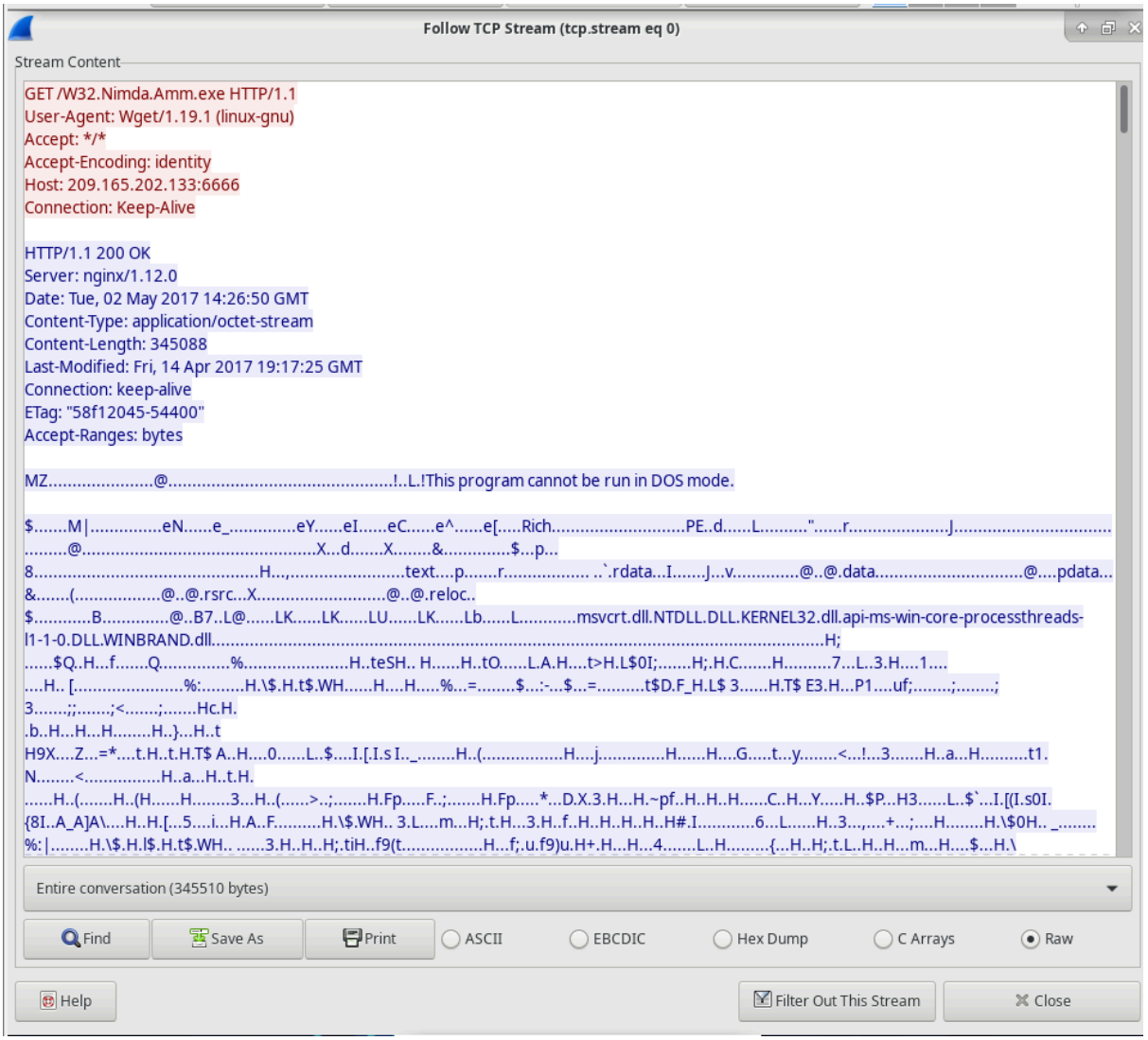
Parte 2: Estrazione del File dal PCAP

Seguire il Flusso TCP:

- Una volta individuato il pacchetto HTTP di interesse, fai clic destro su di esso e seleziona `Follow > TCP Stream`.

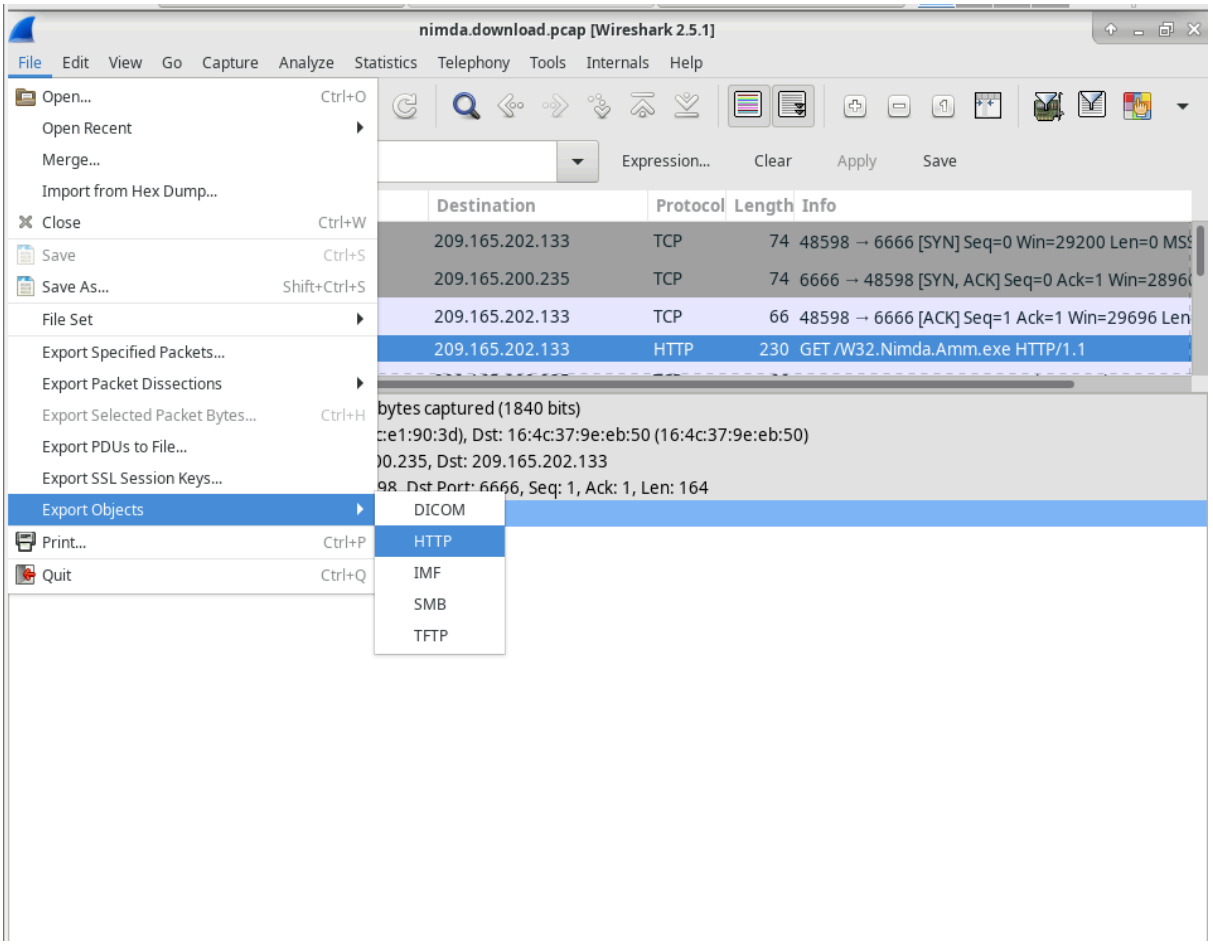


Questo ti permette di vedere l'intera conversazione tra client e server, incluso il trasferimento del file eseguibile.

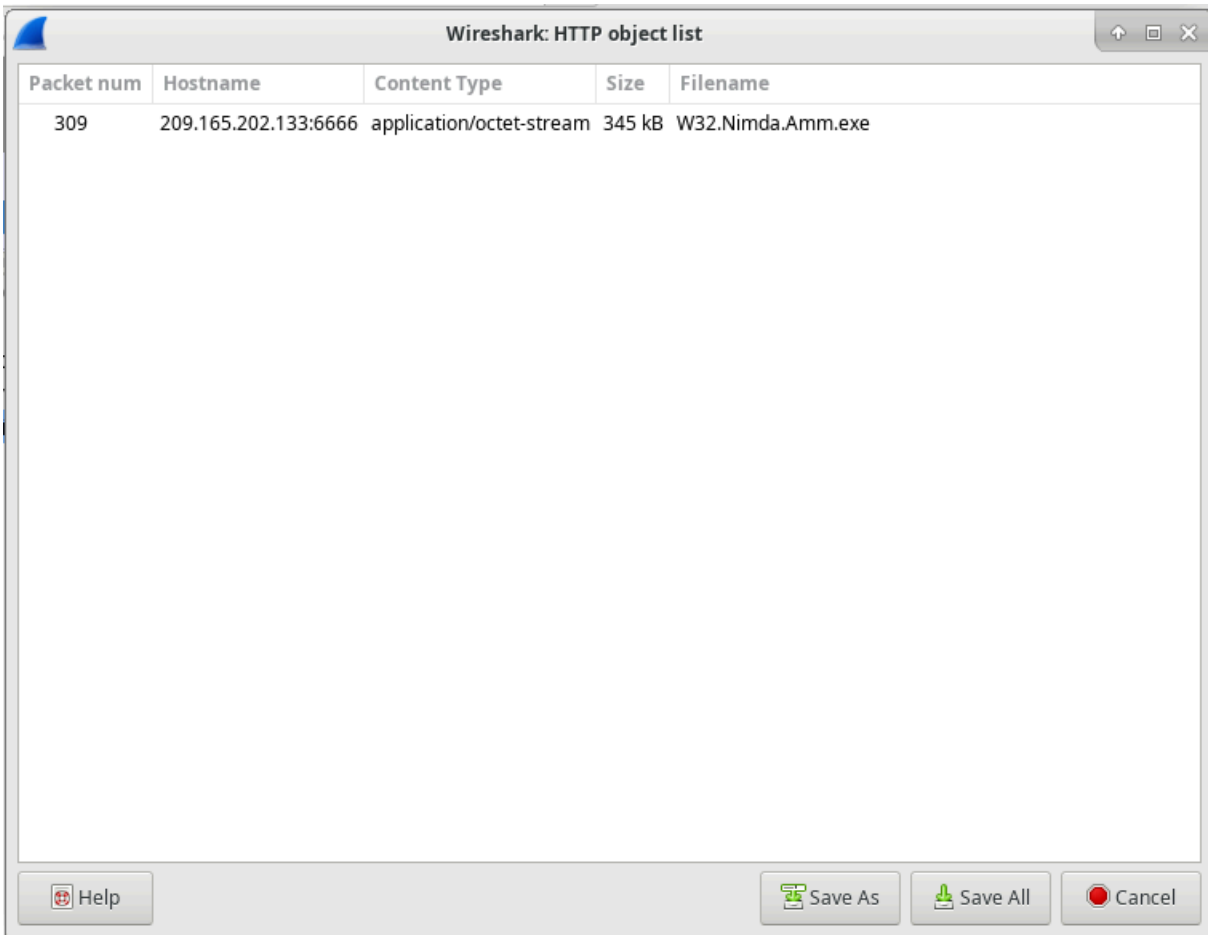


Esportazione dell'Oggetto HTTP:

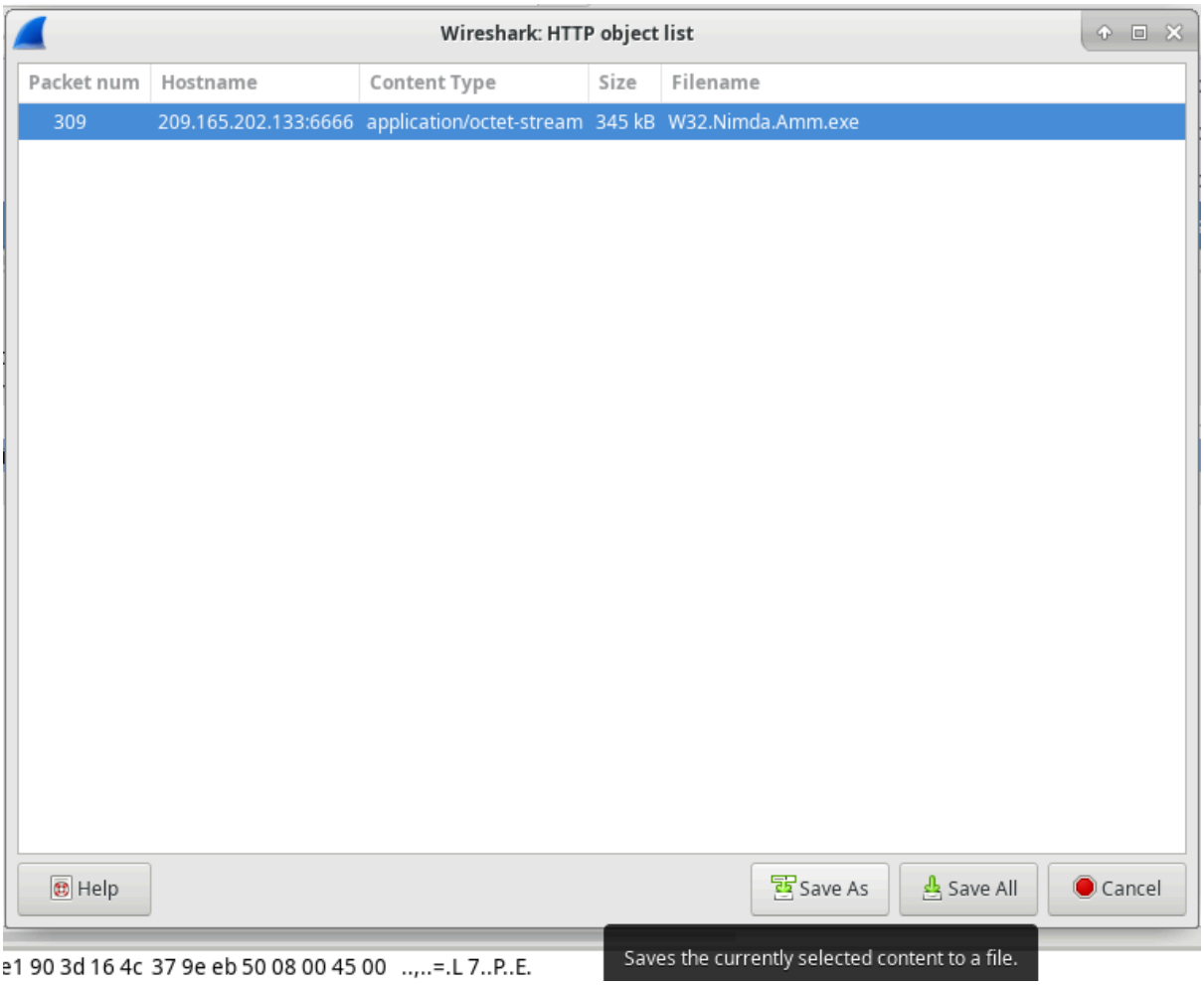
- Vai su `File > Export Objects > HTTP` per aprire l'elenco degli oggetti scaricabili presenti nel traffico HTTP. Questo passaggio permette di visualizzare i file disponibili per l'esportazione.



- Nell'elenco degli oggetti HTTP, cerca il file eseguibile `W32.Nimda.Amm.exe`.

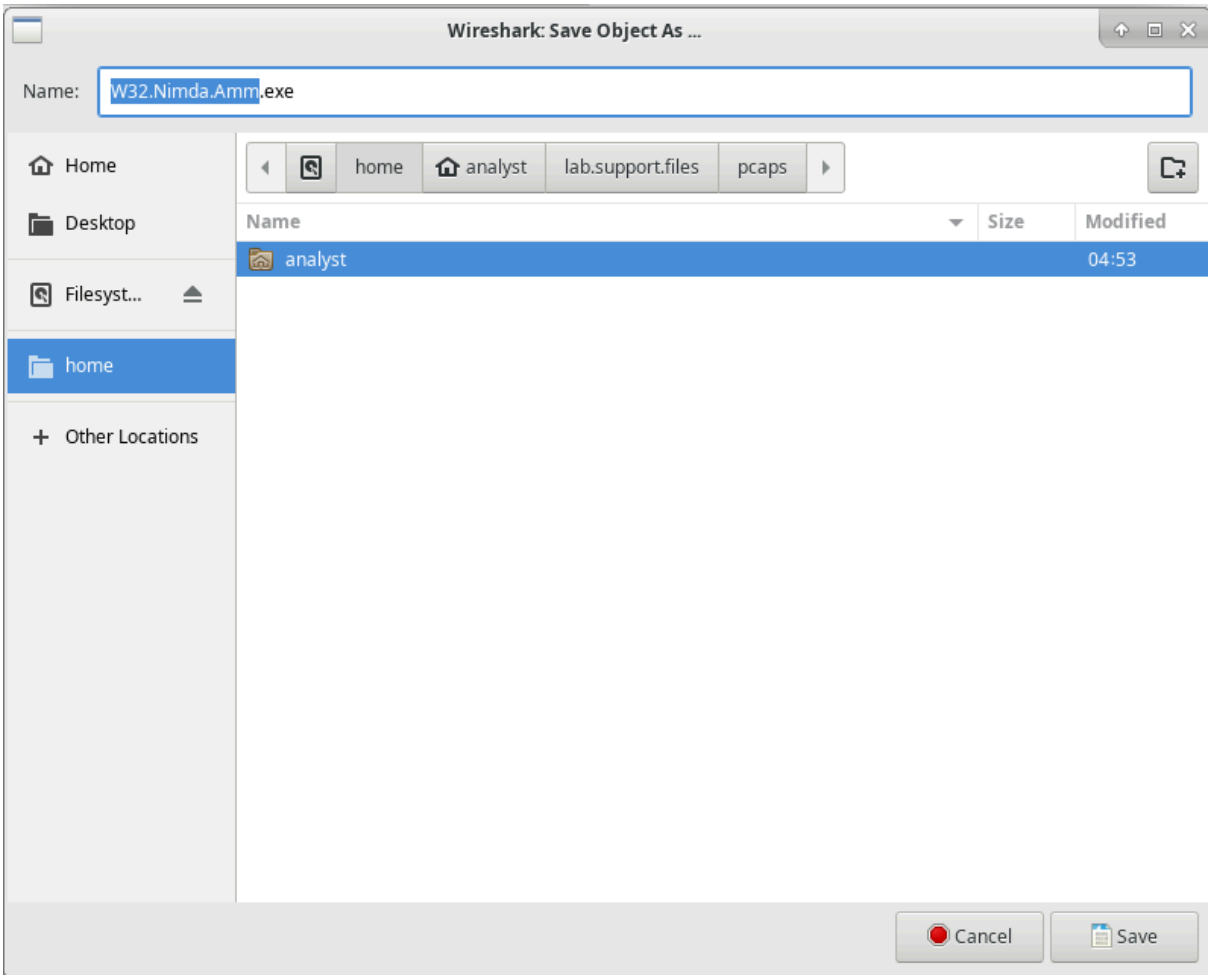

Wireshark: HTTP object list
Packet num
Hostname
Content Type
Size
Filename
309
209.165.202.133:6666
application/octet-stream
345 kB
W32.Nimda.Amm.exe
Help
Save As
Save All
Cancel

Seleziona questo file e fai clic su `Save As` per salvare il file localmente.

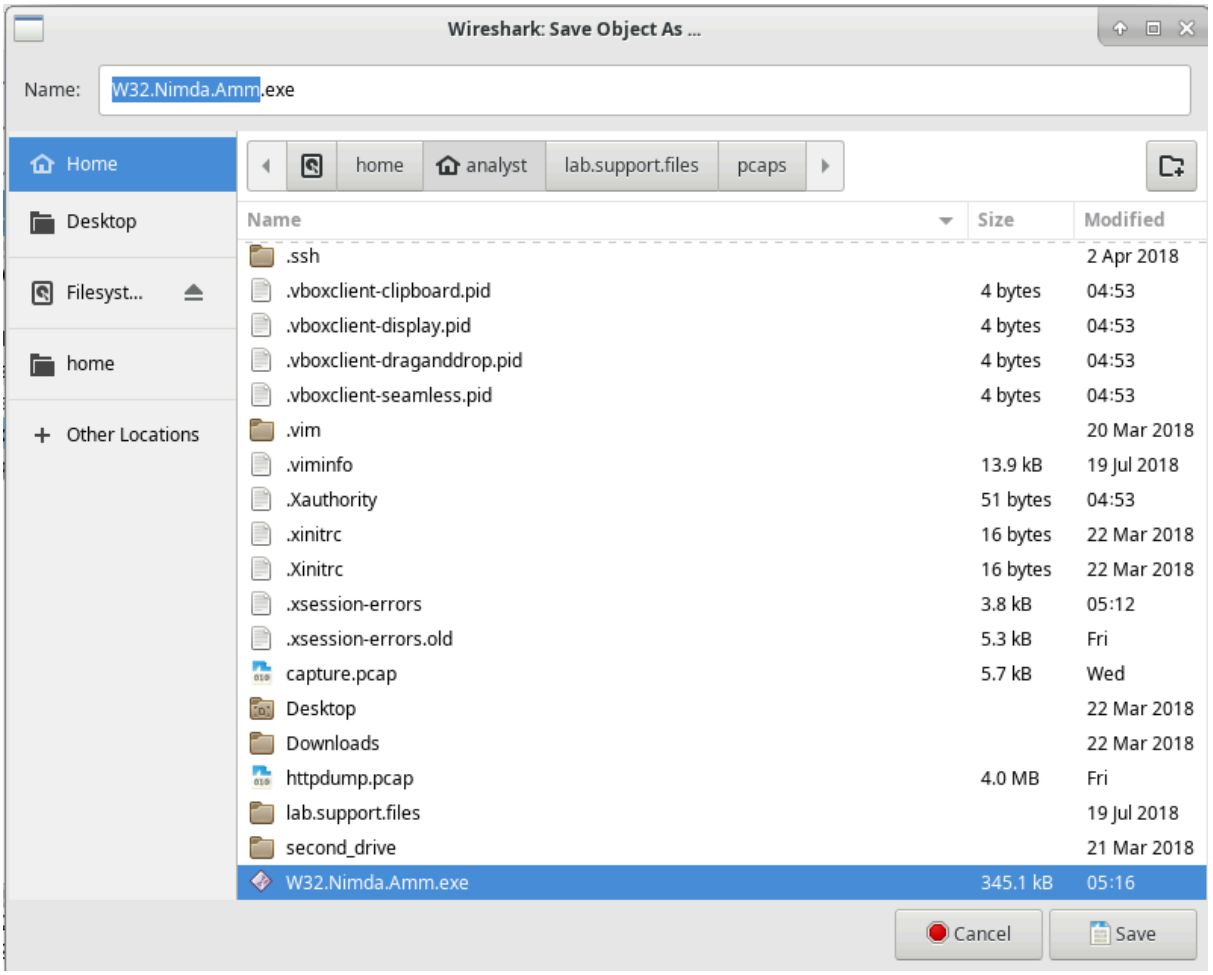


Selezione del Percorso di Salvataggio:

- Quando appare la finestra di dialogo per il salvataggio, naviga verso la directory di destinazione desiderata. Nel nostro caso, andremo a salvare il file all'interno della cartella `home/analyst` del sistema.



- Assicurati che il nome del file sia corretto (`W32.Nimda.Amm.exe`), poi conferma il salvataggio selezionando `Save`.



Verifica del File Estratto:

- Dopo aver salvato il file, apri una finestra del terminale per confermare che il file sia stato correttamente salvato e identificato.
- Cambia directory nella cartella **/home/analyst**

```
[analyst@secOps ~]$ cd /home/analyst
```

- Esegui il comando `ls -l` per visualizzare le proprietà del file e confermare le dimensioni e il percorso di salvataggio.

```
[analyst@secOps ~]$ ls -l
total 4260
-rw-r--r-- 1 root    root       5650 Oct 23 04:40 capture.pcap
drwxr-xr-x 2 analyst analyst    4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst    4096 Mar 22  2018 Downloads
-rw-r--r-- 1 root    root    3988205 Oct 25 12:46 httpdump.pcap
drwxr-xr-x 9 analyst analyst    4096 Jul 19  2018 lab.support.files
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst  345088 Oct 28 05:16 W32.Nimda.Amm.exe
```

- Usa il comando `file W32.Nimda.Amm.exe` per identificare il tipo di file e verificare che si tratti effettivamente di un eseguibile compatibile con Windows (PE32+ executable).

```
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
```