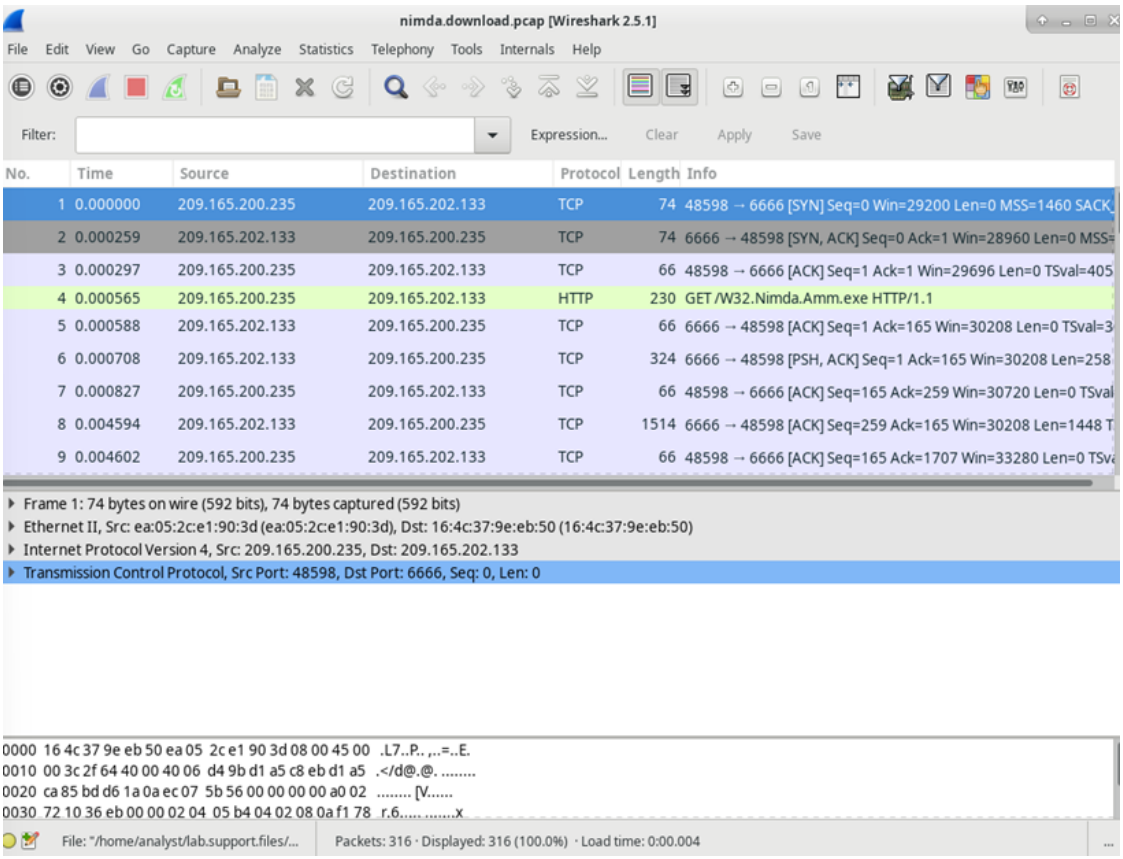
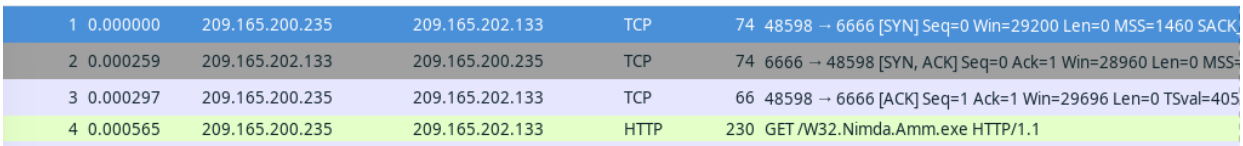
Extract an Executable from a PCAP

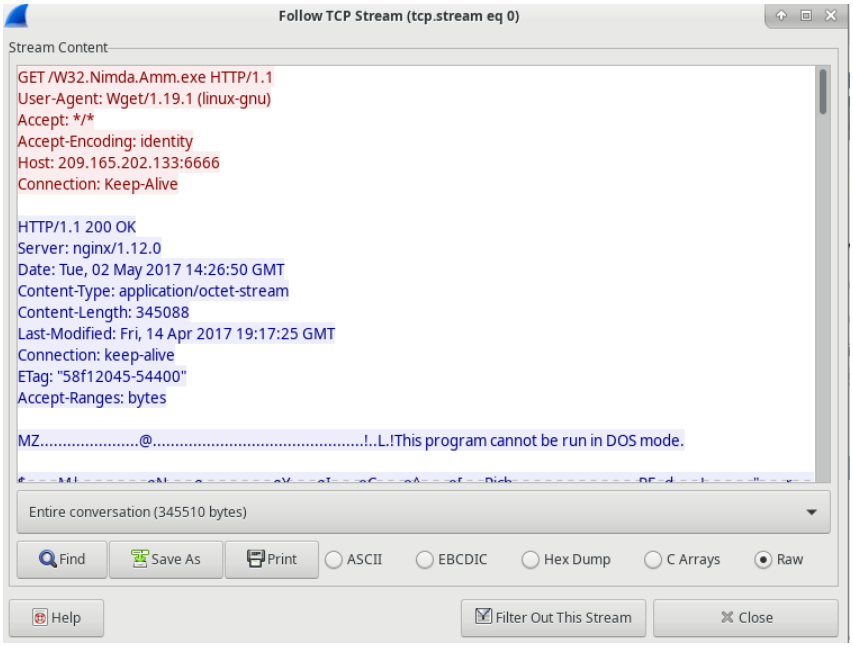
Utilizziamo il file **download.pcap** contenente la cattura dei pacchetti relativa al download del malware eseguito in un precedente laboratorio e lo avviamo con Wireshark. Il **pcap** contiene tutti i pacchetti inviati e ricevuti mentre **tcpdump** era in esecuzione.



I pacchetti da uno a tre rappresentano l'handshake TCP mentre il quarto pacchetto mostra la richiesta del file malware. La richiesta è stata effettuata tramite HTTP, inviata come richiesta GET.



Poiché HTTP funziona su TCP, è possibile usare la funzionalità **Follow TCP Stream** di Wireshark per ricostruire la transazione TCP. Selezioniamo il primo pacchetto TCP nella cattura, un pacchetto SYN. Facciamo clic con il pulsante destro del mouse e scegliamo **Follow** > **TCP Stream**.



I simboli sono il contenuto effettivo del file scaricato e, poiché si tratta di un file binario, Wireshark non sa come rappresentarlo. I simboli visualizzati sono la migliore ipotesi di Wireshark per dare un senso ai dati binari mentre li decodifica come testo.

Estrarre i file scaricati da PCAP

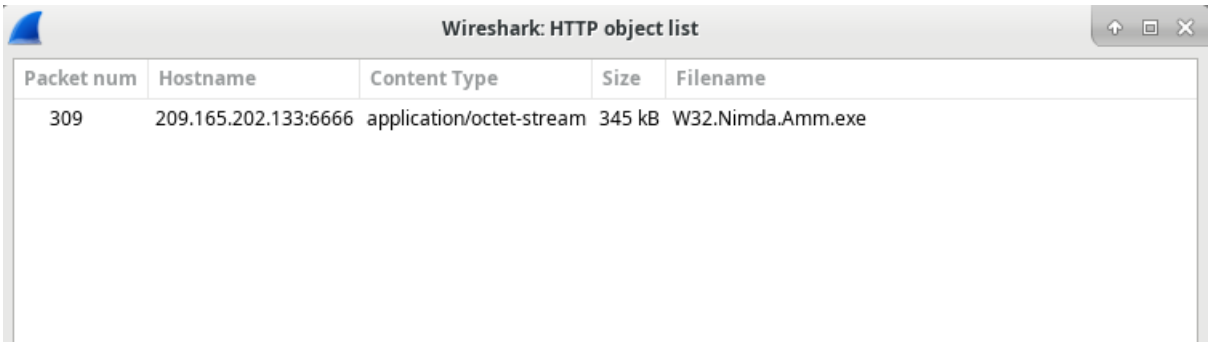
Poiché i file di cattura contengono tutti i pacchetti correlati al traffico, un PCAP può essere utilizzato per recuperare un file scaricato in precedenza.

Nel quarto pacchetto abbiamo modo di notare che la richiesta HTTP GET è stata generata da **209.165.200.235** a **209.165.202.133** .

1	0.000000	209.165.200.235	209.165.202.133	TCP	74 48598 → 6666 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_
2	0.000259	209.165.202.133	209.165.200.235	TCP	74 6666 → 48598 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=
3	0.000297	209.165.200.235	209.165.202.133	TCP	66 48598 → 6666 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=405
4	0.000565	209.165.200.235	209.165.202.133	HTTP	230 GET /W32.Nimda.Amm.exe HTTP/1.1

Con il pacchetto di richiesta GET selezionato andiamo su **File > Esporta oggetti > HTTP** dal menu di Wireshark **.**

Wireshark visualizzerà tutti gli oggetti HTTP presenti nel flusso TCP che contiene la richiesta GET. In questo caso, solo il file **Nimda.Amm.exe** è presente nella cattura.



Poiché la cattura è stata avviata subito prima del download e interrotta subito dopo nessun altro traffico è stato intercettato mentre la cattura era attiva.

Nella finestra dell'elenco degli oggetti HTTP andiamo a selezionare il file **Nimda.Amm.exe.**

Salviamo il file nella cartella Analyst.

Andiamo ora sul terminale e cambiando directory nella cartella **/home/analyst** ed elenchiamo i file della stessa usando *ls -l*.

```
[analyst@secOps pcaps]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 1056
-rw-r--r-- 1 root    root      5563 Oct 23 05:06 capture.pcap
drwxr-xr-x 2 analyst analyst   4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst   4096 Mar 22  2018 Downloads
lrwxrwxrwx 1 analyst analyst      9 Oct 28 05:35 fileisymbolic -> file1.txt
-rw-r--r-- 1 analyst analyst      9 Oct 28 05:32 file1.txt
lrwxrwxrwx 1 analyst analyst      9 Oct 28 05:35 file2har -> file2.txt
-rw-r--r-- 1 analyst analyst      4 Oct 28 05:32 file2.txt
-rw-r--r-- 1 root    root    581279 Oct 25 04:57 httpdump.pcap
-rw-r--r-- 1 root    root    118206 Oct 25 05:16 httspdump.pcap
drwxr-xr-x 9 analyst analyst   4096 Jul 19  2018 lab.support.files
drwxr-xr-x 3 root    root      4096 Mar 26  2018 second_drive
-rw-r--r-- 1 analyst analyst 345088 Oct 28 05:51 W32.Nimda.Amm.exe
```

Utilizziamo il comando file per saperne di più sul malware, come mostrato di seguito:

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

W32.Nimda.Amm.exe è effettivamente un file eseguibile di Windows.