

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.

```
[analyst@sec0ps ~]$ cd lab.support.files/pcaps
[analyst@sec0ps pcaps]$ ls -l
total 4028
-rw-r--r-- 1 analyst analyst 371462 Mar 21 2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21 2018 wannacry_download_pcap.pcap
[analyst@sec0ps pcaps]$ wireshark nimda.download.pcap &
[1] 1093
```

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.

Wireshark 2.5.1 interface showing a packet capture of nimda.download.pcap. The packet list shows a SYN packet (No. 1) and an ACK packet (No. 2). The packet details pane shows the selected packet (No. 2) with its structure: Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the selected packet.

4. Follow TCP Stream:

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

Wireshark 2.5.1 interface showing the 'Follow TCP Stream' window. The window displays the raw data of the selected packet (No. 2) in ASCII, EBCDIC, Hex Dump, C Arrays, and Raw formats. The raw data shows the connection details and the raw bytes of the packet.

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

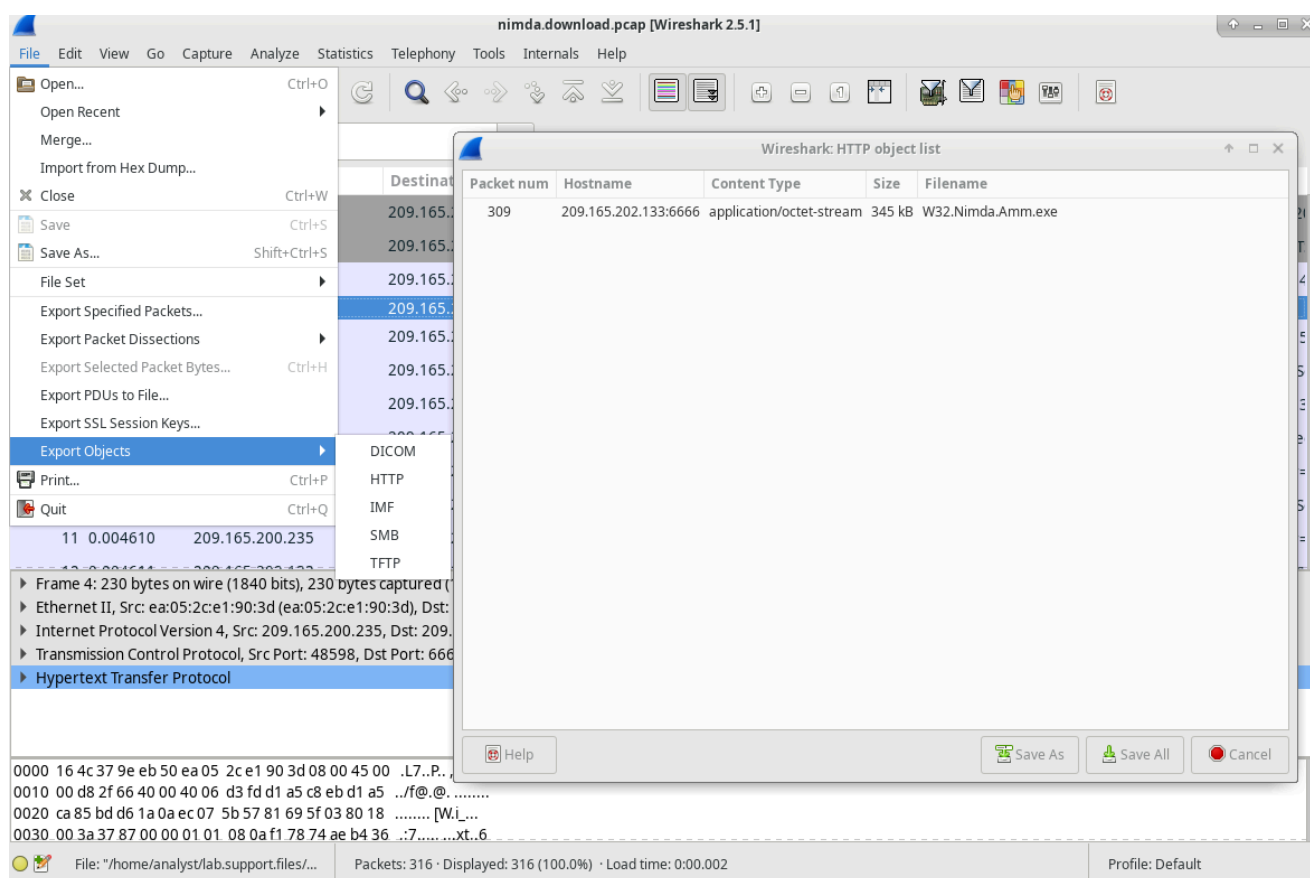
🌸 Tag: #estrazione_file #wireshark #pcap #malware

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:

- Selezione `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.

```
[2]+  Exit 127                  Wireshark: Nimda.download.pcap
[analyst@sec0ps pcaps]$ cd /home/analyst
[analyst@sec0ps ~]$ ls -l
total 368
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 analyst analyst   9 Oct 28 06:46 file1new.txt
lrwxrwxrwx 1 analyst analyst   9 Oct 28 06:47 file1symbolic -> file1.txt
-rw-r--r-- 2 analyst analyst   5 Oct 28 06:46 file2hard
-rw-r--r-- 2 analyst analyst   5 Oct 28 06:46 file2new.txt
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 07:29 W32.Nimda.Amm.exe
[analyst@sec0ps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
```

Chiavi:

[wireshark, pcap, tcp, http, estrazione file, malware, tcpdump, download.pcap]
