### **TRACCIA 4**

### **Report di Analisi – Estrazione di un Eseguibile da un PCAP**

**OS:**

**Strumento utilizzato:** **Wireshark  
File analizzato:** nimda.download.pcap  
**Obiettivo:** **Identificare ed estrarre un file eseguibile da un file di cattura del traffico di rete (PCAP).**

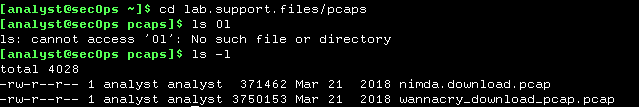
### **1. Obiettivo del Laboratorio**

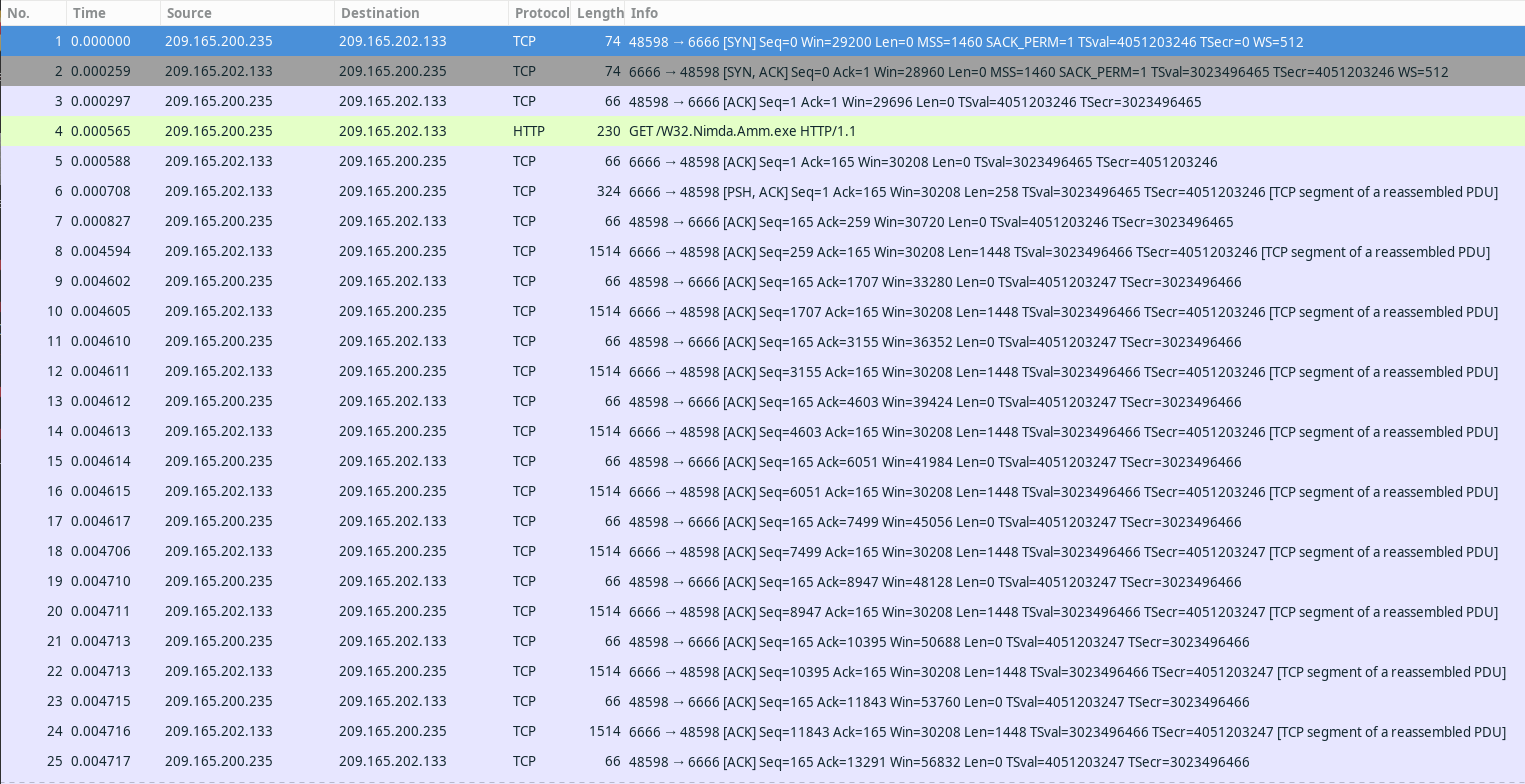
L'analisi del traffico di rete è fondamentale per individuare transazioni sospette e attacchi informatici. In questo laboratorio, si è analizzato un file di cattura per identificare ed estrarre un eseguibile scaricato attraverso il protocollo HTTP.

### **2. Procedura**

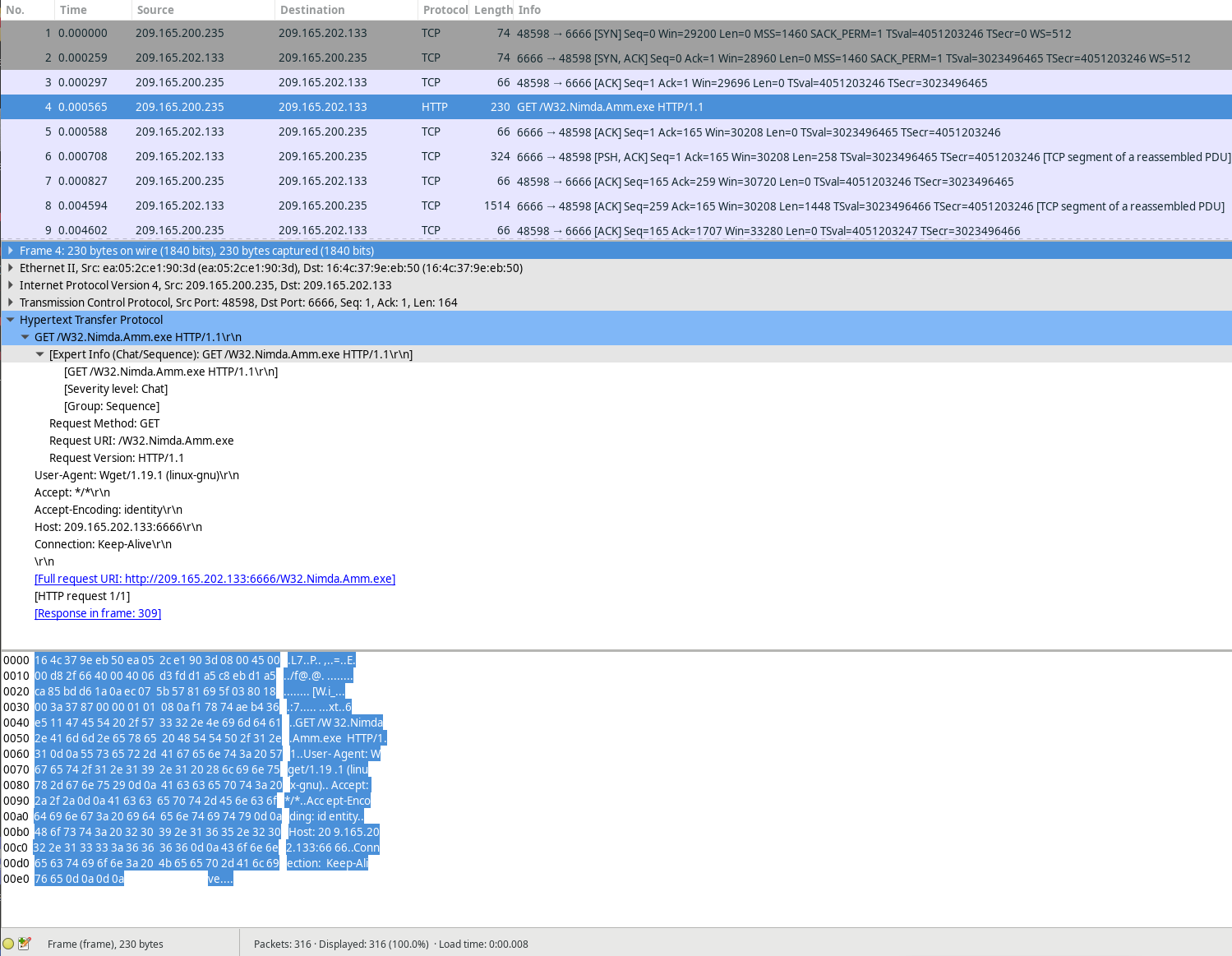
#### **Parte 1: Analisi del traffico catturato**

1. **Accesso ai file PCAP**

Il file nimda.download.pcap è stato localizzato nella directory:  
 /home/analyst/lab.support.files/pcaps

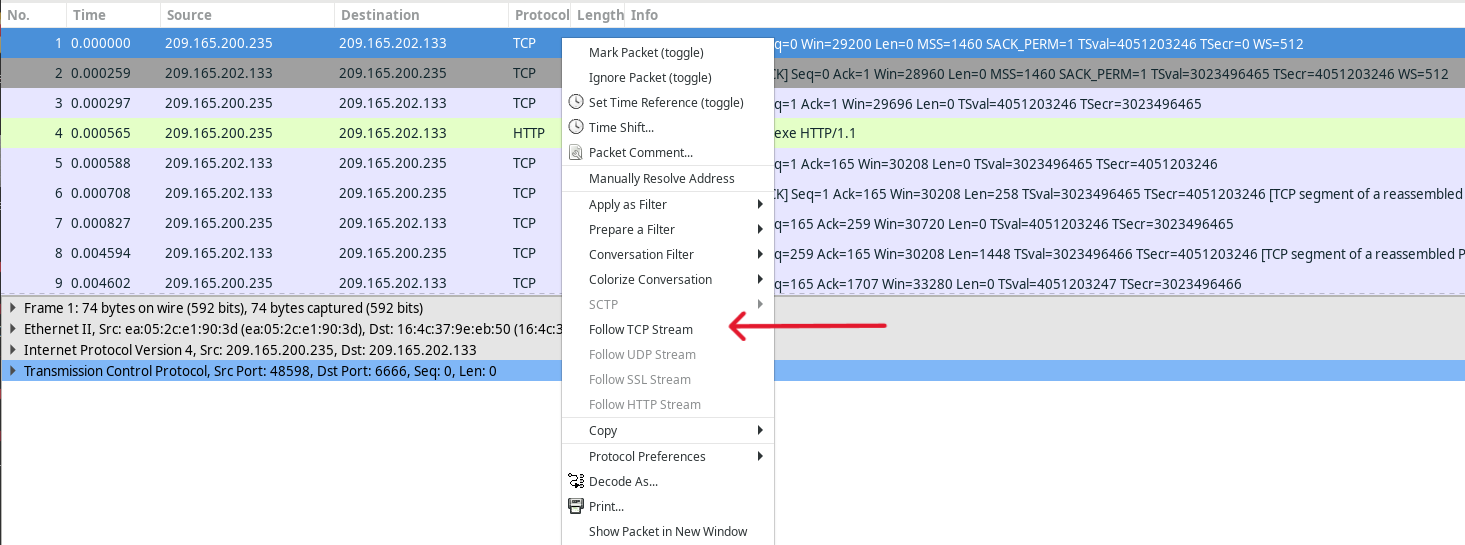
1. **Apertura del file con Wireshark per l’analisi dei pacchetti**

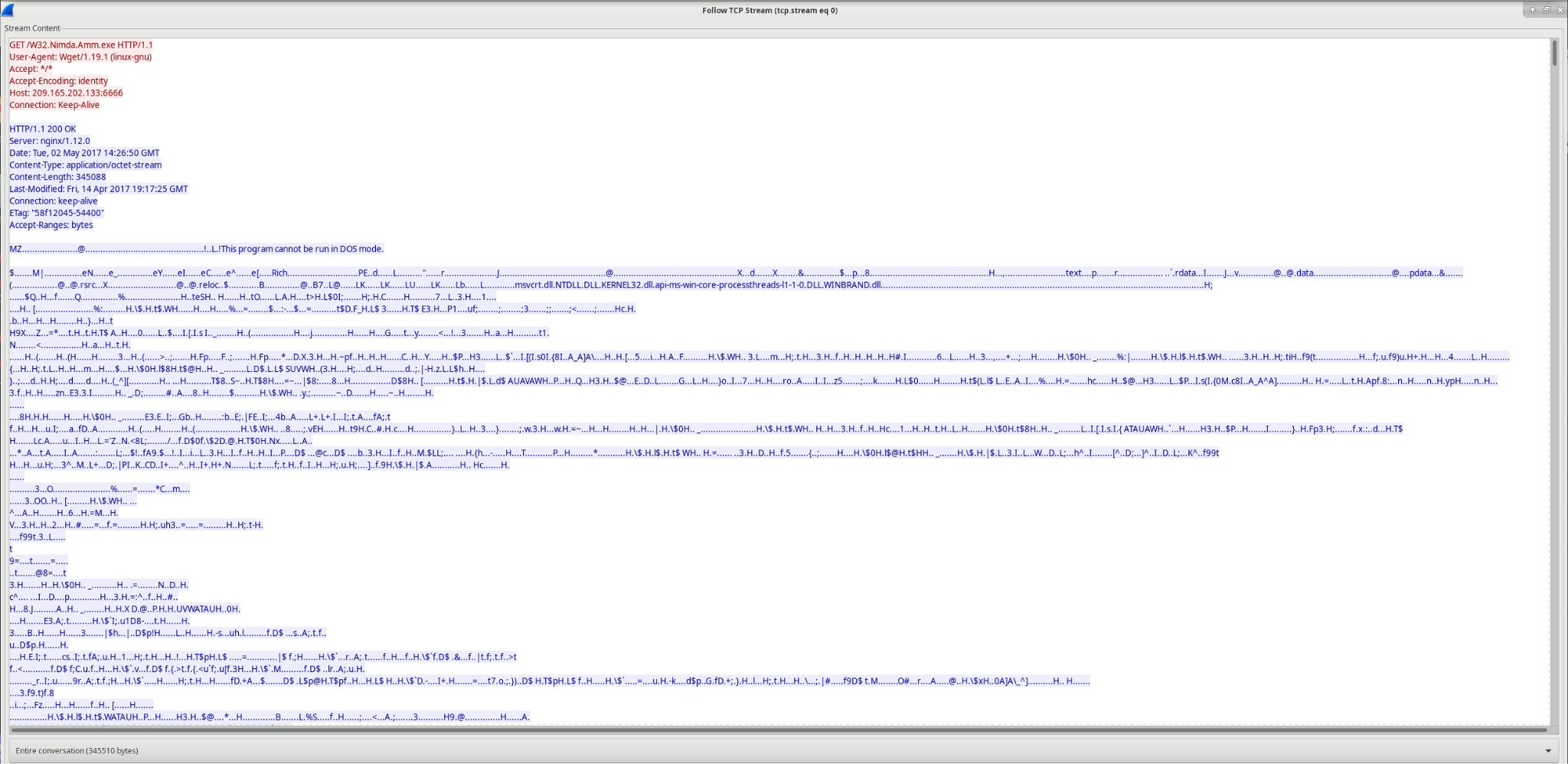
Si analizza il flusso di traffico registrato.

1. **Identificazione del traffico sospetto**I primi **tre pacchetti** del PCAP rappresentano la **stretta di mano TCP** (SYN, SYN-ACK, ACK).

Il **quarto pacchetto** rappresenta una **richiesta GET HTTP** per il download di un file sospetto.

1. **Analisi del contenuto della richiesta HTTP**Selezionato il **quarto pacchetto**, è stata espansa la sezione **Hypertext Transfer Protocol (HTTP)** per visualizzare il contenuto della richiesta.

Si è confermato che il download del file avveniva tramite HTTP, utilizzando una richiesta **GET**.

1. **Ispezione del traffico binario**È stato utilizzato **Follow TCP Stream** su Wireshark per ricostruire il traffico.

Il contenuto visualizzato presentava **caratteri binari e stringhe leggibili**, suggerendo la presenza di un file eseguibile.



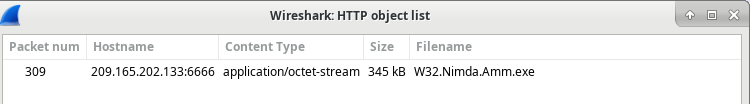
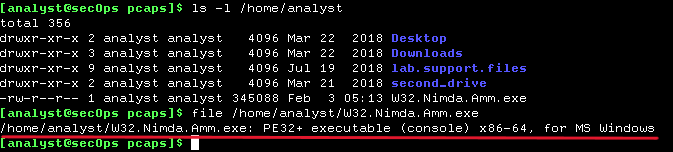
#### 

#### 

#### **Parte 2: Estrazione dell'eseguibile**

1. **Individuazione del file scaricato**

Si è identificato che la richiesta GET proveniva da:  
 209.165.200.235 → 209.165.202.133

1. **Esportazione dell'oggetto HTTP**
   * Selezionato il pacchetto contenente la richiesta GET.
   * Navigato su **File > Export Objects > HTTP** in Wireshark.
   * L’elenco degli oggetti HTTP conteneva un solo file: **W32.Nimda.Amm.exe.**
   * Il file è stato salvato nella directory /home/analyst.
2. **Identificazione del tipo di file**Con il tool  **file** (da cli) si identifica la tipologia del file estratto; ovvero un file **eseguibile Windows** per architetture **x86-64.**

### **3. Risultati e Conclusioni**

* Il **malware Nimda** è stato identificato all'interno della cattura PCAP.
* Il file è stato estratto con successo utilizzando Wireshark.
* Il file **W32.Nimda.Amm.exe** è stato confermato come un eseguibile Windows.
* L'analisi del flusso TCP ha mostrato **stringhe leggibili**, possibili indicatori delle funzioni del malware.

### **4. Mitigazione e Contromisure ana**

**Isolare il file in un ambiente controllato**

* Spostare il file in una sandbox (es. Cuckoo, Any.Run) per ulteriori analisi.

**Eseguire un'analisi statica e dinamica**

* Analisi statica con strumenti come **strings, PEStudio, die (Detect It Easy)**.
* Analisi dinamica con strumenti come **Process Monitor**, **Wireshark**, e **Regshot**.

**Verificare Indicatori di Compromissione (IoC)**

* Controllare hash del file con **VirusTotal**.
* Identificare eventuali IP/Domini sospetti collegati al file.

**Aggiornare firewall e antivirus**

* Bloccare eventuali comunicazioni malevole.
* Aggiornare il database delle firme malware.