Introduzione

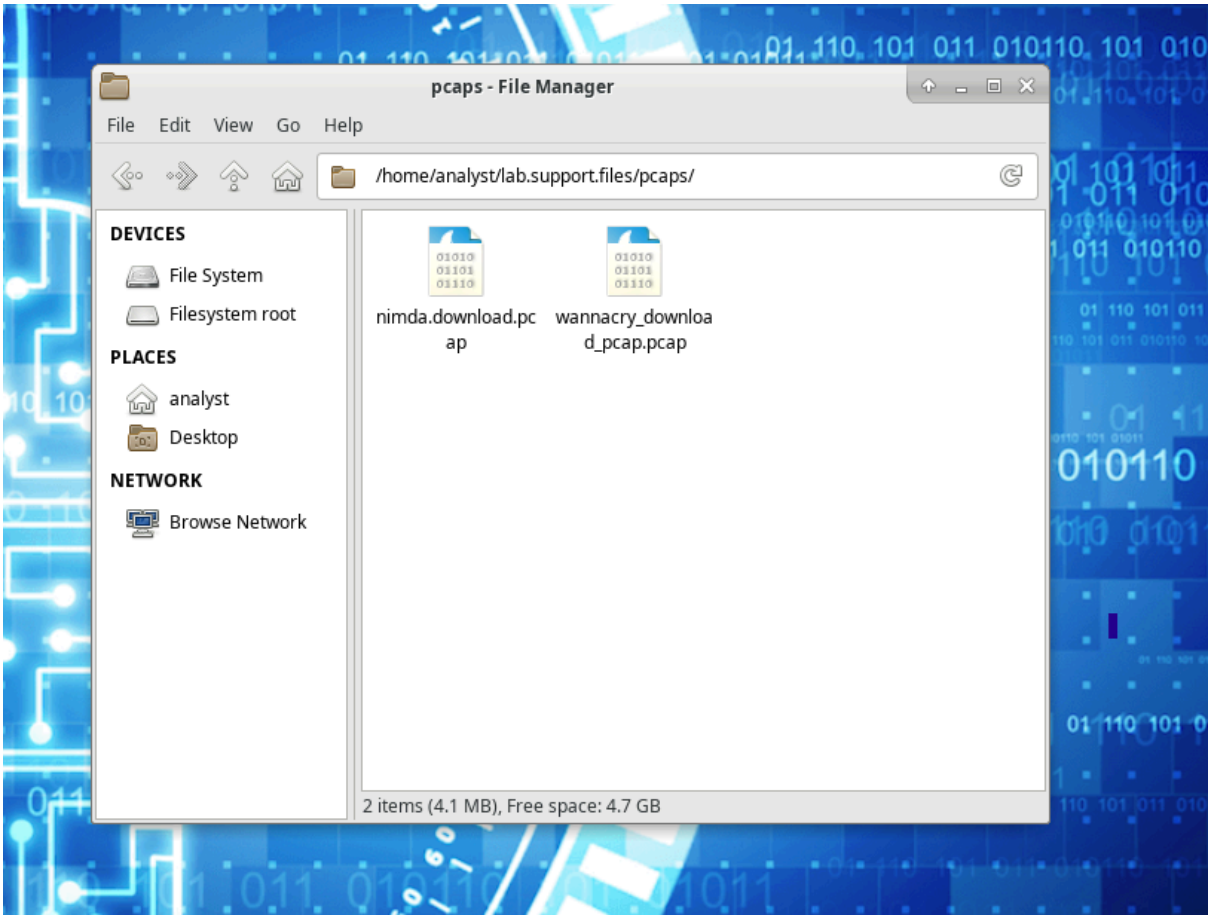
L’esercizio si svolge nel contesto di un’indagine simulata per conto della compagnia Theta, vittima di un possibile attacco informatico. La compagnia ha rilevato anomalie nei log di rete, che indicavano il download di un file eseguibile sospetto, **W32.Nimda.Amm.exe**. Lo scopo del test è analizzare un file PCAP catturato durante l’incidente per estrarre il file scaricato e raccogliere informazioni utili alla comprensione dell’attacco.

L’indagine si svolge su una macchina virtuale **Cisco Workstation** installata su **Oracle VirtualBox**, configurata appositamente per l’analisi di file di rete. Lo strumento principale utilizzato è **Wireshark**, noto per le sue capacità di catturare e analizzare pacchetti di dati trasmessi sulla rete. La simulazione ha l'obiettivo didattico di illustrare tecniche di analisi forense digitale, focalizzandosi sul recupero di file eseguibili da catture di rete.

Individuazione del file PCAP

L'analisi inizia con l'individuazione del file PCAP contenente i dati catturati durante l'attacco. Il file, denominato **nimda.download.pcap**, si trova nella directory `/home/analyst/lab.support.files/pcaps`. Questa cattura rappresenta uno snapshot del traffico di rete al momento del download del file sospetto.

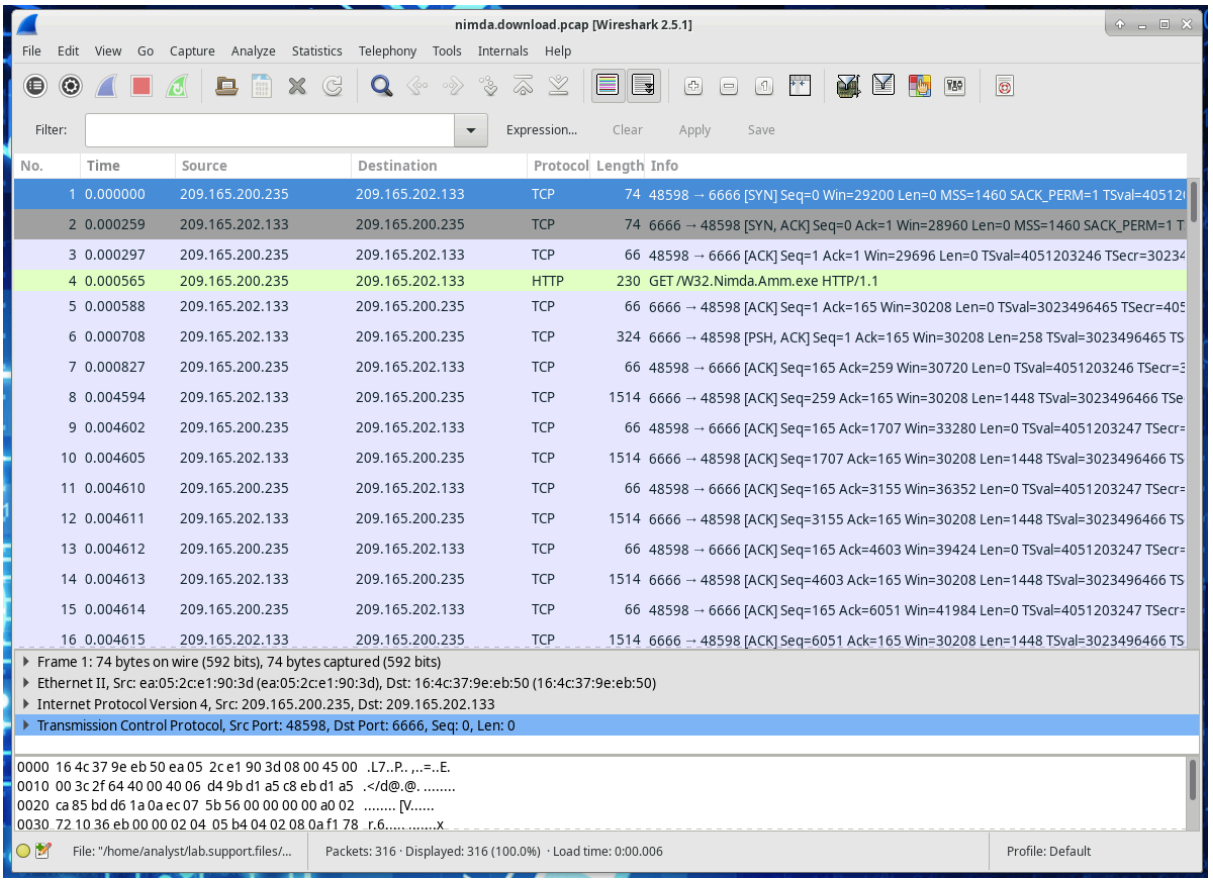
I file PCAP sono essenziali per le indagini forensi poiché contengono informazioni dettagliate su ogni pacchetto scambiato in rete, inclusi dati di livello applicativo come richieste HTTP o contenuti binari. Nel caso specifico, ci permette di ricostruire l'intera sequenza di eventi che ha portato al download del file. L'organizzazione e la corretta conservazione di questi file sono cruciali per garantire che le evidenze digitali siano integre e utilizzabili.



Apertura del file PCAP in Wireshark

Una volta identificato il file, viene aperto in **Wireshark**. Questo strumento consente di visualizzare ogni pacchetto trasmesso, con dettagli come il protocollo utilizzato, gli indirizzi IP di origine e destinazione, e i contenuti del payload.

Wireshark offre un'interfaccia che permette di filtrare i dati, semplificando l'analisi anche in presenza di migliaia di pacchetti. In questo caso, ci concentriamo sul traffico HTTP, poiché sappiamo che il file eseguibile è stato scaricato tramite una connessione web. L'uso di strumenti specializzati come Wireshark è indispensabile per gli analisti di rete, in quanto permette di tradurre il complesso linguaggio dei protocolli in informazioni comprensibili.

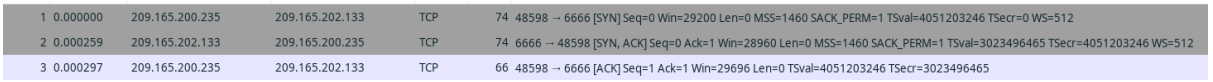


Identificazione della stretta di mano a tre vie

Nei primi tre pacchetti catturati, si osserva la **stretta di mano a tre vie** del protocollo TCP. Questo processo, fondamentale per stabilire connessioni affidabili, si compone di tre fasi:

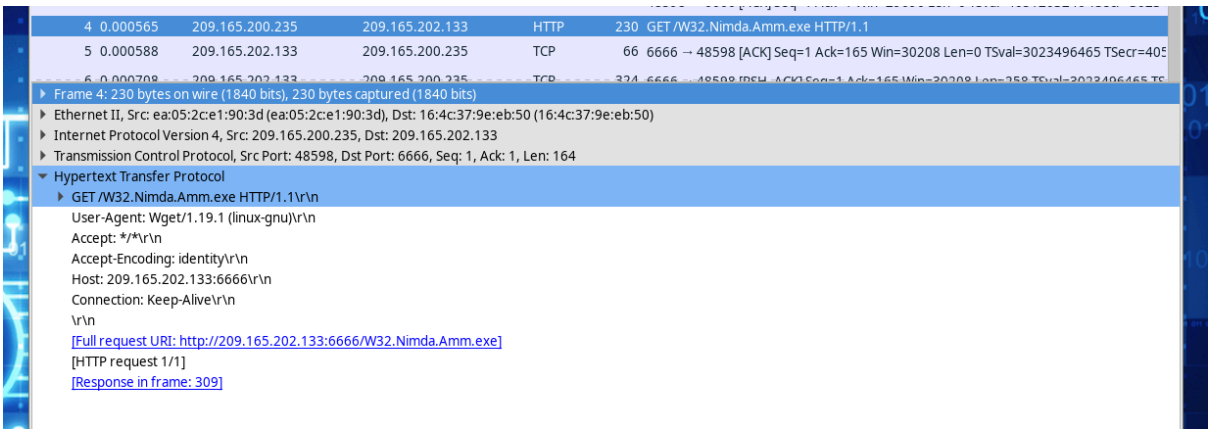
1. Il client invia un pacchetto **SYN** (Synchronize) al server per iniziare la connessione.
2. Il server risponde con un pacchetto **SYN/ACK** (Synchronize-Acknowledge), confermando la richiesta.
3. Il client completa il processo con un pacchetto **ACK** (Acknowledge), sancendo l'inizio dello scambio di dati.

La stretta di mano è un meccanismo progettato per garantire che entrambe le parti siano pronte a comunicare. È anche un indicatore importante per gli analisti, poiché segnala l'inizio di una connessione sospetta. Nel caso della compagnia Theta, questa connessione è il punto di partenza per l'attacco.



Nel **quarto pacchetto**, viene individuata una richiesta HTTP di tipo **GET**, utilizzata dal client per scaricare il file `W32.Nimda.Amm.exe`. Questa richiesta è un esempio di come gli attaccanti utilizzino protocolli standard come HTTP per trasferire file dannosi senza destare sospetti.

La richiesta GET è visibile nel payload del pacchetto e include dettagli come il nome del file richiesto e il percorso sul server remoto. Questa fase è cruciale per l'indagine, poiché ci conferma il momento esatto in cui il file sospetto è stato scaricato. Questo tipo di analisi permette alle organizzazioni come Theta di individuare vulnerabilità nei loro sistemi e implementare regole di blocco mirate nei firewall o nei sistemi di prevenzione delle intrusioni.

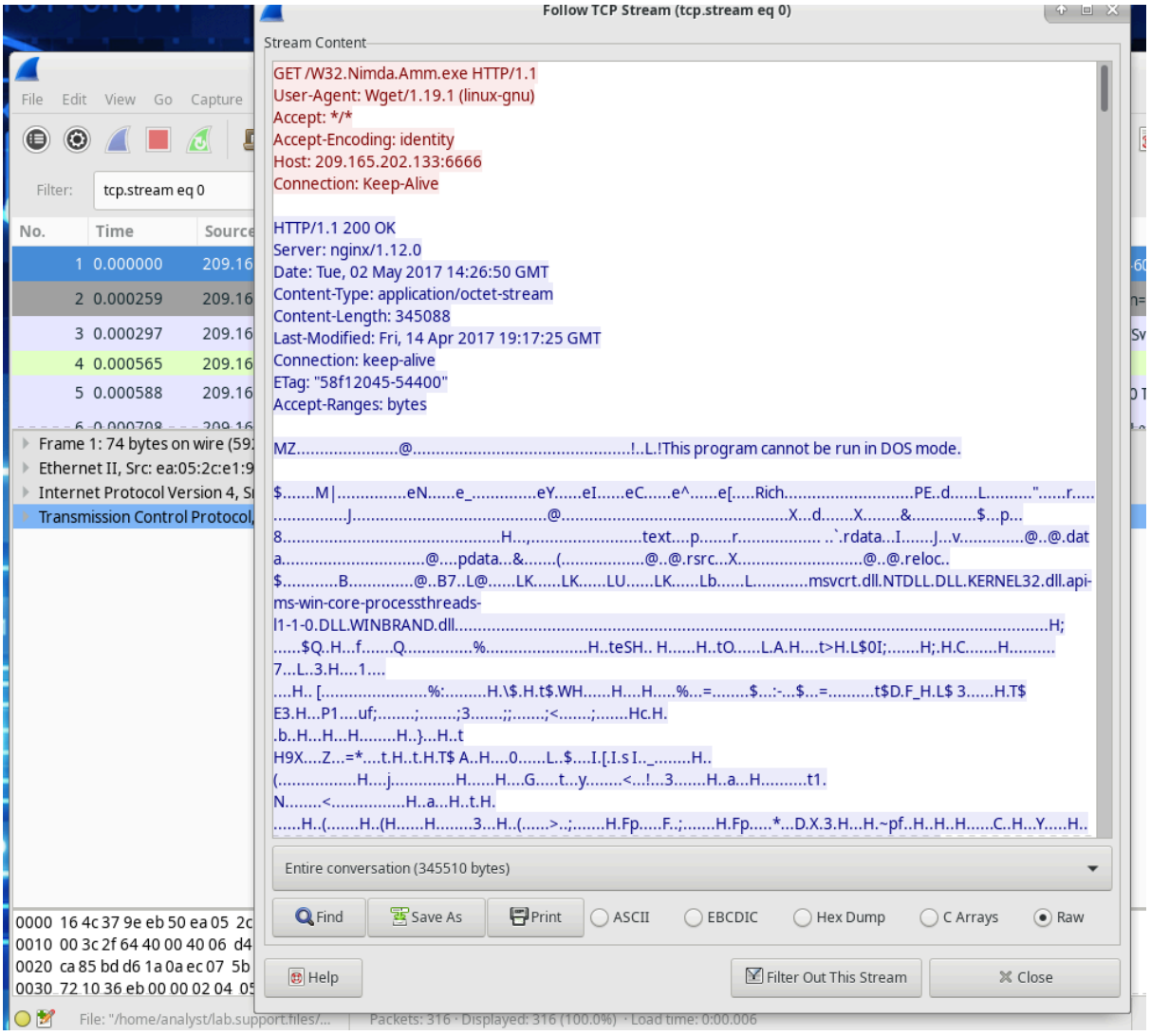


Esame del flusso TCP (Follow TCP Stream)

La funzione **Follow TCP Stream** di Wireshark consente di visualizzare l'intera comunicazione tra il client e il server come un flusso continuo. È particolarmente utile per analizzare il contenuto dei pacchetti, specialmente quando si sospetta il trasferimento di file o dati critici. In questo caso, l'analisi ha evidenziato due aspetti fondamentali:

Caratteri binari: il contenuto del file

Il primo elemento osservato nel flusso sono i **caratteri apparentemente senza senso**, che rappresentano il contenuto binario del file eseguibile scaricato. Questi caratteri sono la trascrizione diretta dei dati binari in formato leggibile per l'analista, ma non hanno un significato immediato senza strumenti adeguati. Essi costituiscono l'essenza del file `W32.Nimda.Amm.exe`, che viene ricostruito a partire da questi dati. Questa rappresentazione grezza è fondamentale per il recupero del file, poiché Wireshark traduce ogni pacchetto catturato in dati utili per l'estrazione. L'analisi del binario permette anche di rilevare anomalie o modifiche al file originale.



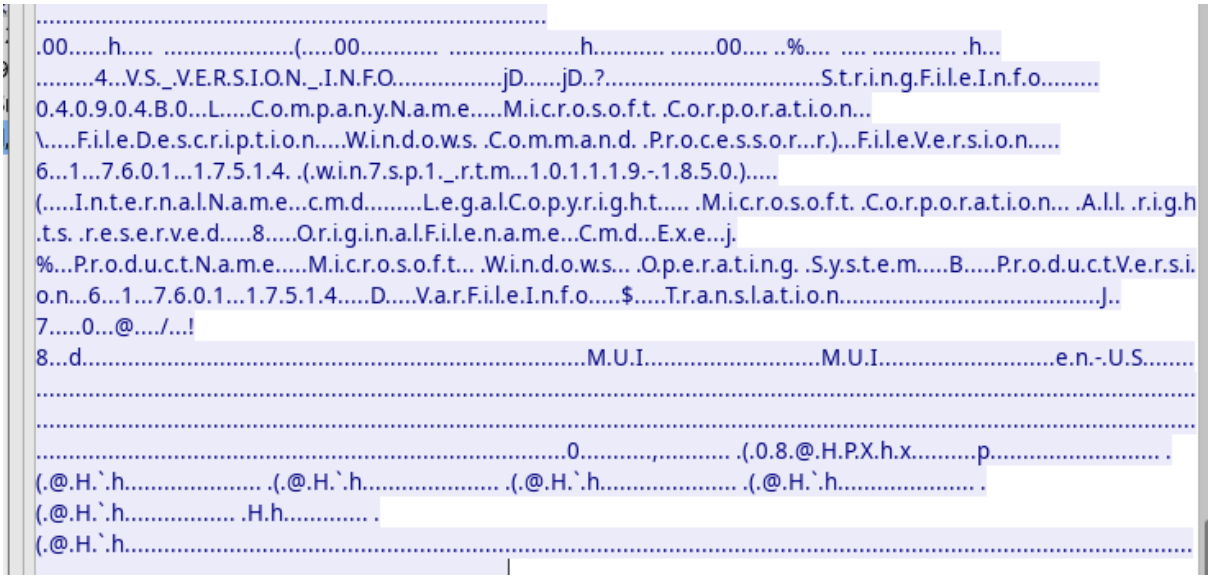
Stringhe leggibili: indizi sul comportamento del file

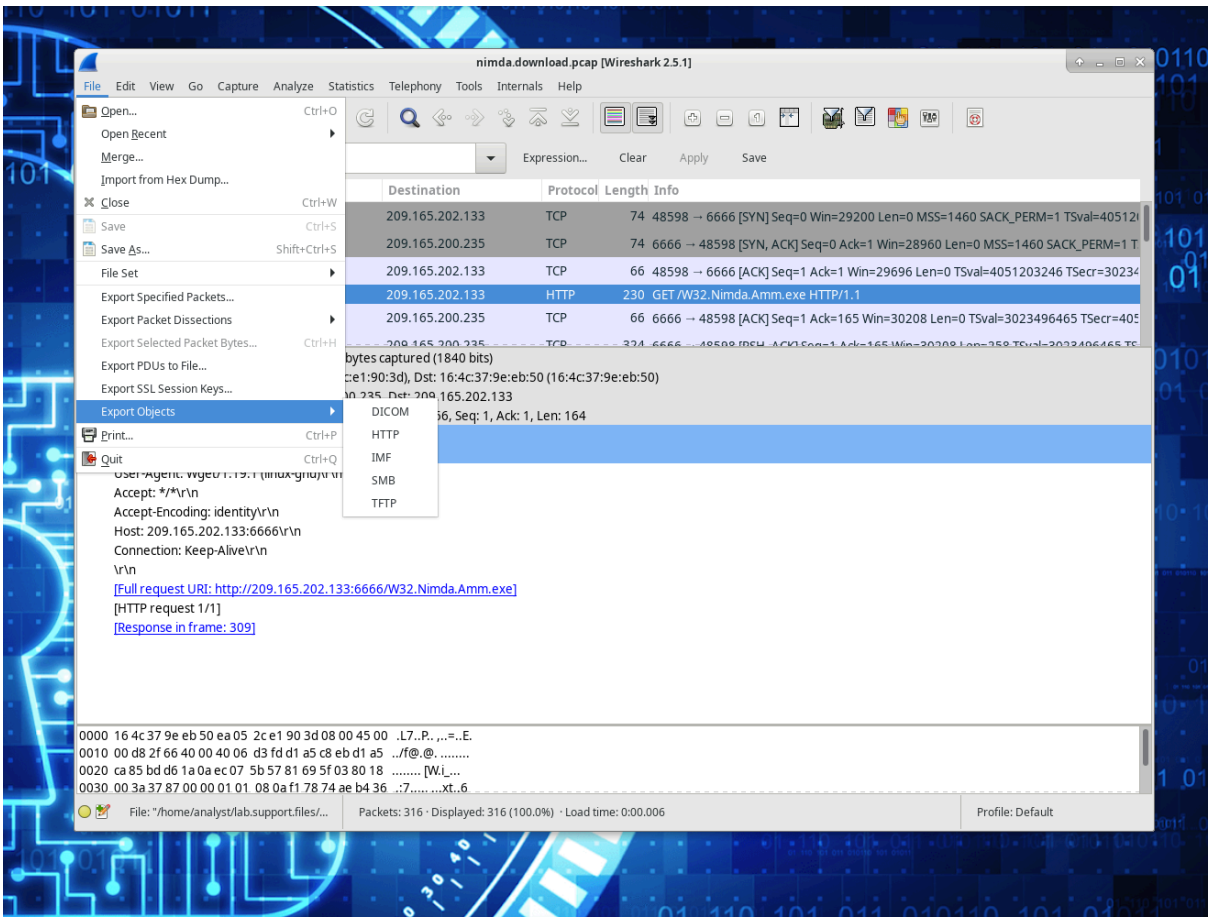
Oltre ai caratteri binari, il flusso TCP rivela anche alcune **stringhe di testo leggibili**. Queste stringhe sono frammenti di dati o comandi presenti nel file eseguibile, che possono fornire indizi preziosi sul suo scopo e funzionamento. Ad esempio, possono includere riferimenti a directory, chiamate di sistema, URL o altri dati significativi. Nel contesto di un'indagine forense, queste stringhe possono aiutare a determinare se il file è progettato per eseguire comandi dannosi, comunicare con server remoti o modificare il sistema operativo. L'interpretazione di queste stringhe, specie da parte di un analista esperto, è un passo chiave per comprendere il comportamento del file senza necessariamente eseguirlo, riducendo così il rischio di compromettere il sistema d'analisi.

Identificazione del file scaricato

Analizzando le stringhe presenti nel flusso TCP, emerge che il file `W32.Nimda.Amm.exe` è, in realtà, una copia del file di sistema **cmd.exe**, il prompt dei comandi di Windows. Questo è un dettaglio allarmante, poiché cmd.exe può essere utilizzato per eseguire una vasta gamma di comandi, inclusi script dannosi, apertura di backdoor o esecuzione di malware.

Questo passaggio evidenzia l'importanza di andare oltre il nome del file. Gli attaccanti spesso rinominano file dannosi con nomi innocui o ingannevoli per eludere il rilevamento.

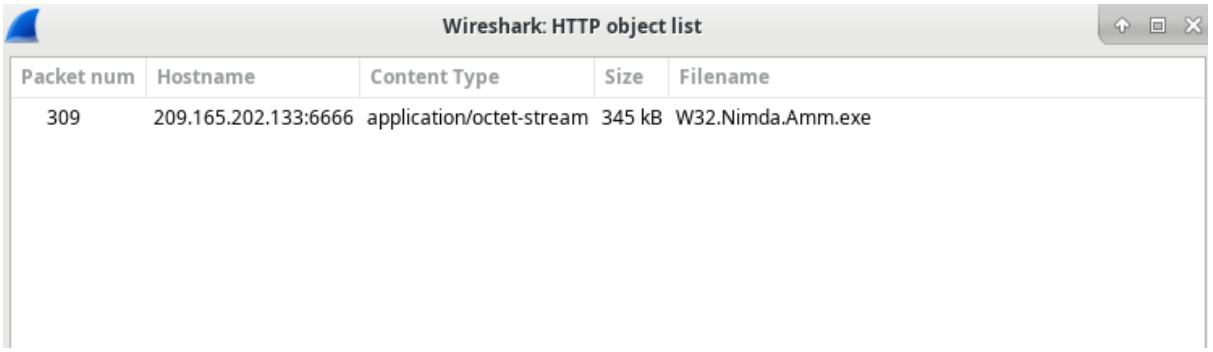




Esportazione dell'oggetto HTTP

Grazie alla funzione **Export Objects > HTTP** di Wireshark, il file eseguibile è stato isolato e salvato. Questa funzione ricostruisce il file originale dai dati binari catturati, permettendo agli analisti di esaminarlo direttamente.

Nell'elenco degli oggetti HTTP esportabili, il file `W32.Nimda.Amm.exe` è l'unico presente. Questo riflette il fatto che il file PCAP è stato catturato in un momento specifico, durante il download del file. Questo approccio dimostra come catture mirate possano fornire informazioni preziose con il minimo impatto sulle risorse di rete.

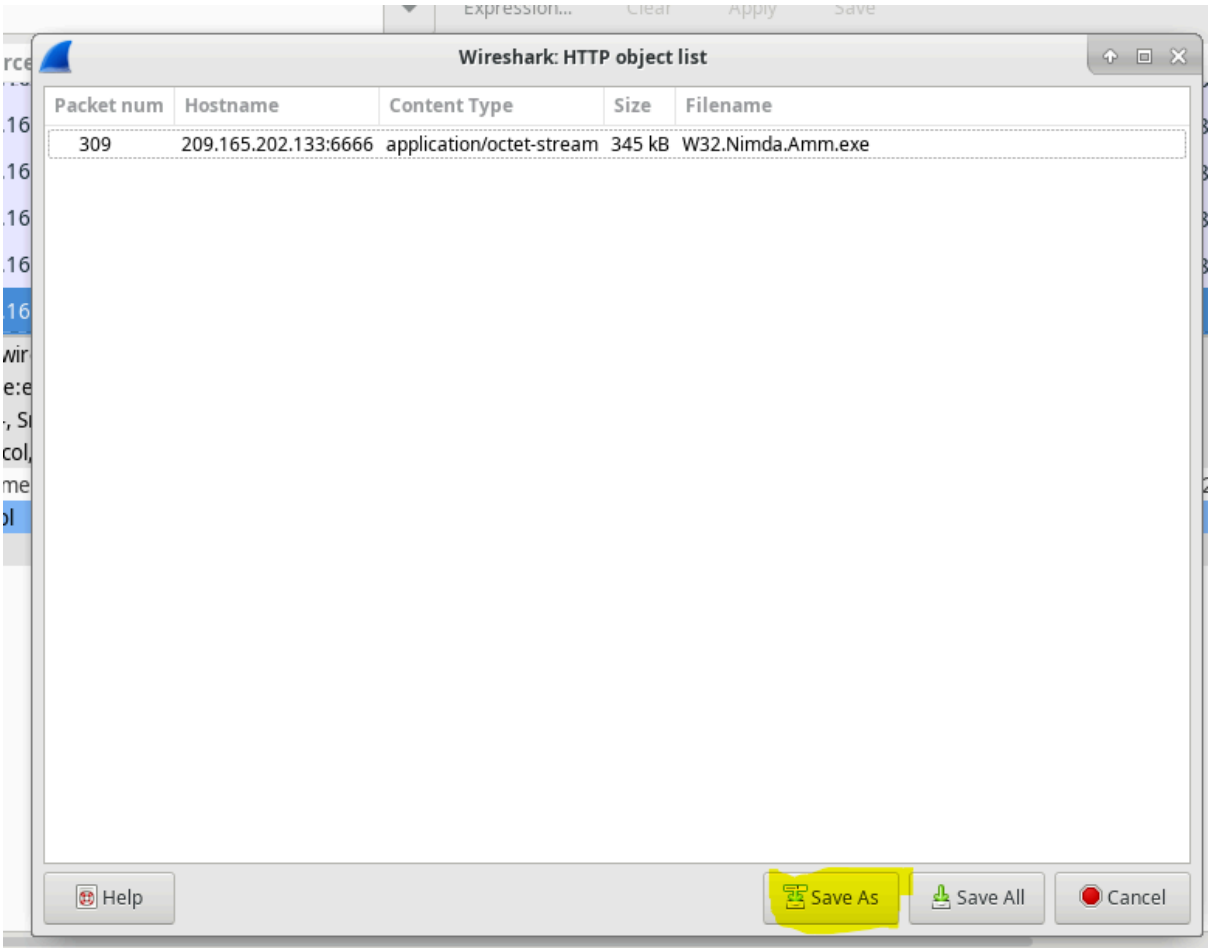


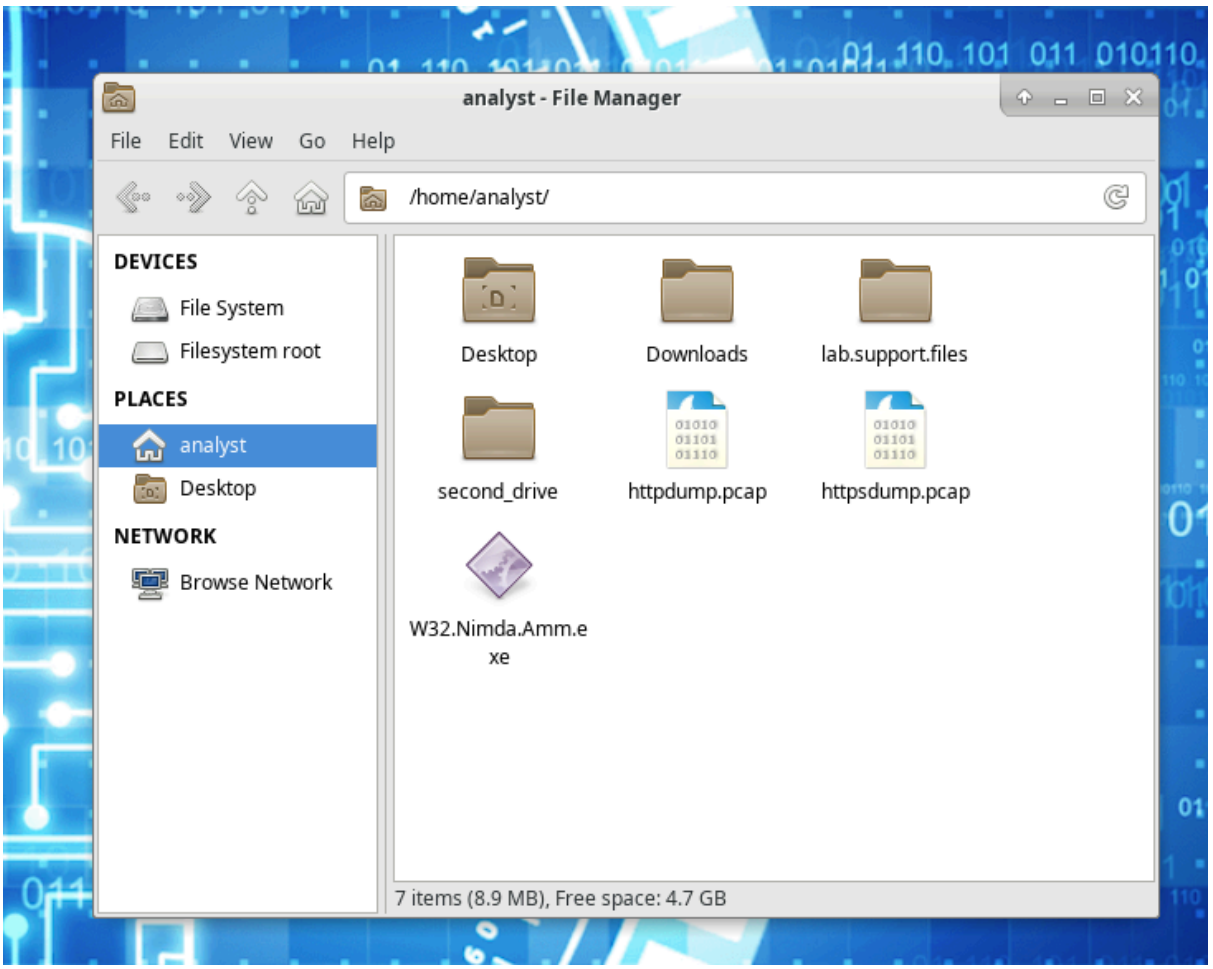
Salvataggio e verifica del file recuperato

Il file esportato è stato salvato nella directory `/home/analyst` e la sua presenza è stata confermata tramite comandi terminale:

- **`cd /home/analyst`** per accedere alla directory.
- **`ls -l`** per elencare i file e verificarne la correttezza.

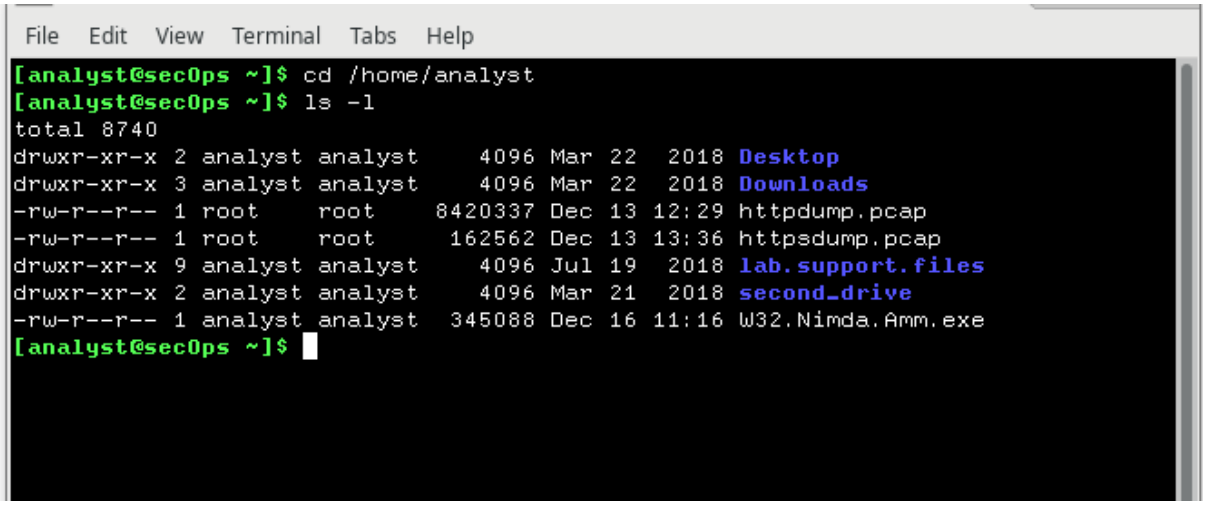
Questi passaggi sono fondamentali per garantire la catena di custodia del file, un aspetto critico in contesti forensi. La capacità di documentare ogni passaggio assicura che il file possa essere utilizzato come prova in un'indagine legale.

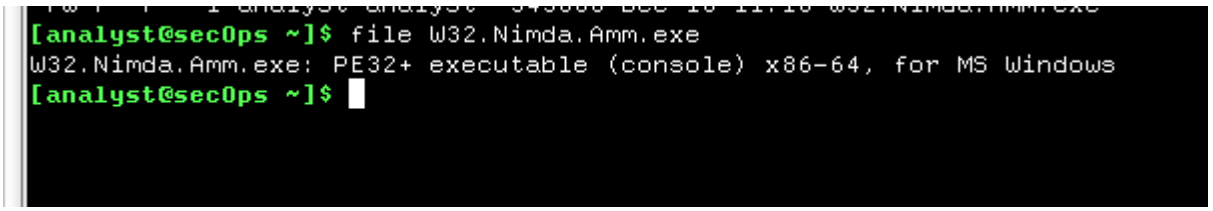




Analisi del file recuperato

Utilizzando il comando **`file`**, è stato confermato che `W32.Nimda.Amm.exe` è un eseguibile per Windows. Questa analisi preliminare fornisce una base per ulteriori indagini, come la decompilazione o l'analisi comportamentale, per determinare esattamente cosa fa il file e quale impatto potrebbe avere su un sistema compromesso.





Conclusione

L'esercizio ha dimostrato come il recupero e l'analisi di file eseguibili da catture di rete siano fondamentali per identificare e comprendere attacchi informatici. Per la compagnia Theta, questa capacità è risultata cruciale per determinare la natura dell'eseguibile sospetto, raccogliendo prove utili per implementare misure difensive e prevenire futuri incidenti.

Un concetto chiave che emerge è l'impatto sulla **Confidenzialità**, **Integrità** e **Accessibilità** (CIA) dei dati, i tre pilastri della sicurezza informatica:

> **Confidenzialità**: Il recupero di un file come `cmd.exe` evidenzia il rischio che attori malintenzionati possano accedere a informazioni sensibili o sfruttare la rete per ottenere privilegi non autorizzati. Preservare la confidenzialità significa limitare l'accesso solo a personale autorizzato, prevenendo fughe di dati.
>
> **Integrità**: La capacità di analizzare e verificare il contenuto del file recuperato consente di identificare eventuali alterazioni. La manipolazione di un file di sistema come `cmd.exe` compromette l'integrità dell'ambiente operativo, aprendo la strada a esecuzioni dannose che possono corrompere o modificare dati critici.
>
> **Accessibilità**: Se un attaccante utilizza un file come `cmd.exe` per eseguire attacchi di tipo denial-of-service o simili, l'accesso ai servizi aziendali potrebbe essere interrotto. Garantire la disponibilità significa prevenire che strumenti vitali o dati essenziali vengano bloccati o resi inutilizzabili.

Il recupero del file eseguibile non solo ha permesso di documentare l'attacco ma ha offerto spunti per migliorare le misure di sicurezza dell'azienda Theta. Questa analisi sottolinea l'importanza di una strategia di sicurezza integrata che protegga il sistema nel suo complesso, salvaguardando confidenzialità, integrità e accessibilità contro minacce esterne e interne.