2024

Laboratorio 2

UNIVERSIDAD RAFAEL LANDÍVAR

CURSO DE REDES Y TELECOMUNICACIONES

Contenido

Objetivo

- Efectuar el análisis de una captura “PCAP” mediante el uso de la herramienta Wireshark.

Capturas de Paquete (PCAP)

Las capturas de paquetes (Paquet CAPture) son un método para poder obtener, almacenar y analizar el tráfico de red. La información se almacena en archivos con extensión “pcap” donde quedan grabados los registros de paquetes de red interceptados o capturados, los cuales contienen información básica del paquete como: direcciones de origen y destino, marca de tiempo, protocolo y carga útil.

Los archivos PCAP pueden ser generados por aplicaciones rastreadoras de paquetes de red como Wireshark y tcpdump. Aunque los fabricantes de equipos proporcionan métodos propios para sus equipos para realizar también dichas facturas.

Los administradores de red y los ingenieros de seguridad utilizan la captura de paquetes para las siguientes tareas en general:

- Supervisar el tráfico de red y analizar sus patrones.
- Identificar y solucionar problemas de red.
- Detectar brechas de seguridad en la red, como intrusiones no autorizadas, actividad de spyware o análisis de ping.
- Analizar comunicación entre empleados o personas que han hecho uso de la red para efectuar análisis forenses.

Materiales

Instalador de Wireshark

En la carpeta compartida del curso busque la subcarpeta “Wireshark” que contiene el instalador de dicha aplicación “Wireshark-4.2.6-x64.exe”.

Protocolo SMTP

En la carpeta compartida del curso busque la subcarpeta “Laboratorio 2” en la misma encontrará el archivo “RFC 821 - Protocolo SMTP.pdf”. Este archivo contiene la definición del protocolo SMTP, el cual le será de utilidad para responder las preguntas del laboratorio.

Archivo de Captura

En la carpeta compartida del curso busque la subcarpeta “Laboratorio 2” en la misma encontrará el archivo “Captura_investigación_archivo_evidencia_01.pcap”.

Ejercicio de Análisis de Captura

Consiste una simulación de investigación forense, en el cual usted determinará información acerca de 2 personas sospechosas de intentar robar propiedad intelectual de una empresa. Una de ellas recibe el nombre Anita y se ha mantenido en comunicación a través de correo electrónico con el otro sospechoso a quien se le denomina simplemente “Amigo de Anita”. El archivo de captura fue obtenido gracias a que los administradores de red apreciaron que Anita había intentado acceder a recursos de información sensibles en la empresa, por lo que iniciaron un monitoreo e intercepción de sus comunicaciones.

Ahora es su turno de analizar el archivo de captura para responder varias preguntas. Pero para ello primero debe comprender un poco el Protocolo SMTP, por lo que debe abrir el documento del protocolo y leer las siguientes secciones:

- Vaya a la página 6 sección “The SMTP Model” lea el texto y entienda su relación con la figura 1.
- Vaya a la página 8 sección “The SMTP Procedures” y lea hasta el final de la página 10.

➢ Una vez terminada la lectura, proceda a abrir el archivo de captura con la herramienta Wireshark.

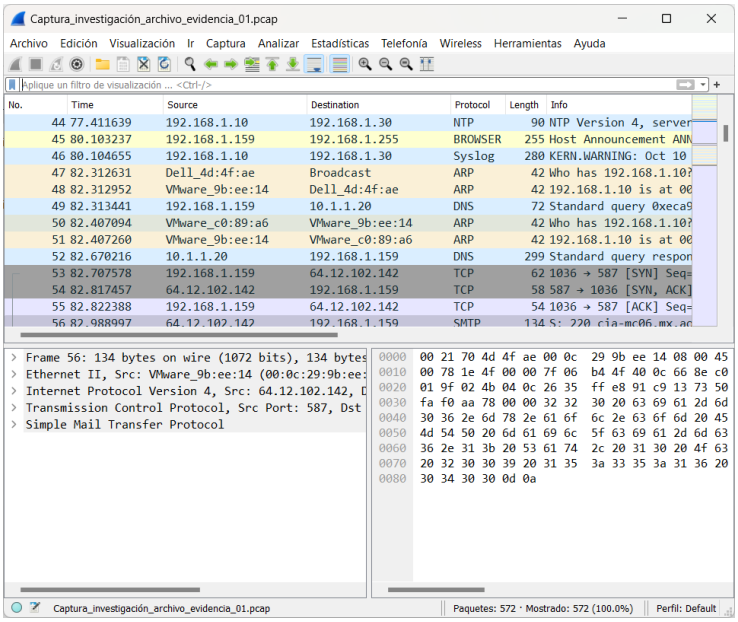

Figura 1 Vista inicial de un archivo de captura abierto

Las capturas de tráfico en general colectan muchos tipos de protocolo por lo que es necesario emplear filtros para analizar de mejor manera la información que contienen. En este caso el trafico que se requiere analizar es SMTP, por lo que puede se puede filtrar ese protocolo escribiendo “smtp” en el cuadro de texto “Aplique un filtro de visualización” y vea como cambia la información presentada.

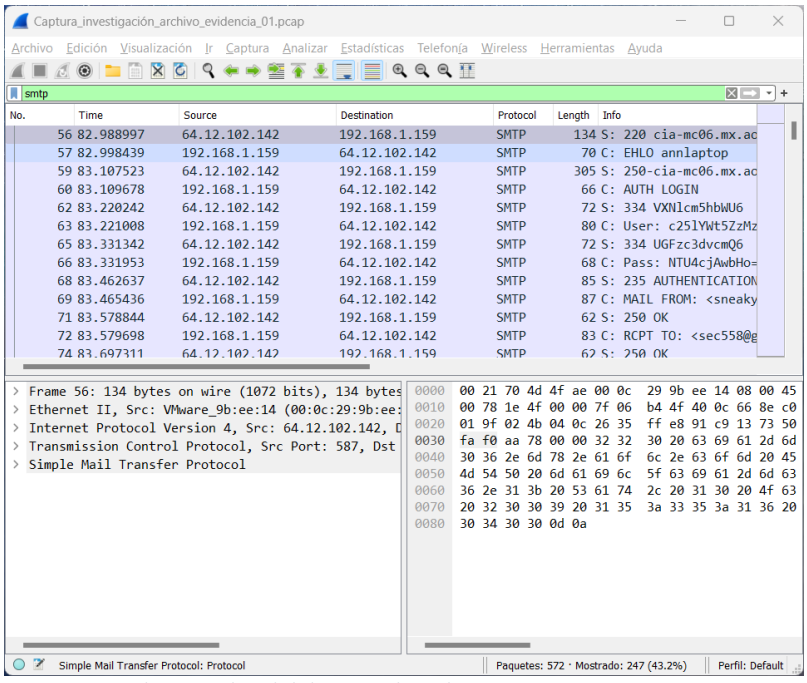

Figura 2 Vista inicial al aplicar filtro de protocolo smtp

Ahora trabaje en responder las siguientes preguntas:

1. ¿Cuál es la dirección de correo electrónico de Anita?
2. ¿Cuál es el correo electrónico del amigo de ella?
3. ¿Cuál es la clave del correo de Anita?
4. ¿Cuáles fueron las 2 cosas que le dijo Anita a su amigo que debe llevar con él?
5. ¿Cuál es el nombre del archivo adjunto que le envió Anita a su amigo? Para resolver esta pregunta vaya a la línea 140 haga clic derecho sobre ella y luego vaya a la opción Seguir y por último elija Secuencia TCP.

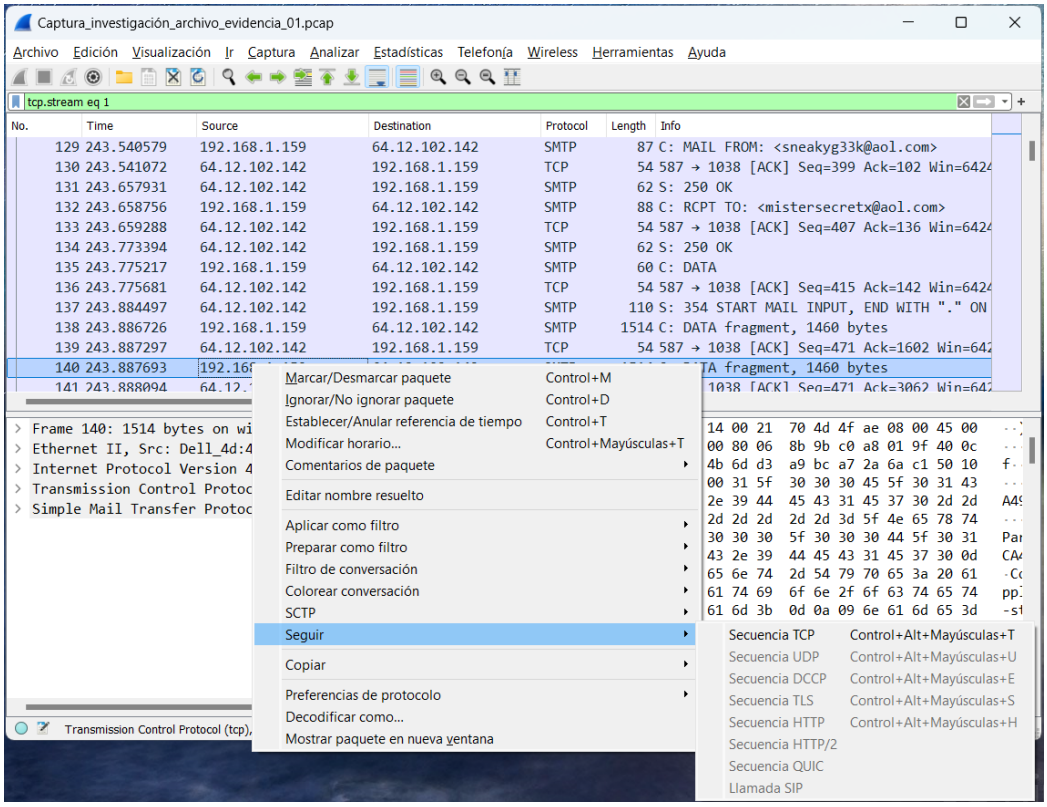

Figura 3 Seguir una "conversación"