UNIVERSIDAD TECNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

"CONTROL TECNOLÓGICO DEL TRÁFICO DE RED DE LA EMPRESA ELECTROCONSTRU S.A UTILIZANDO HERRAMIENTAS OPEN SOURCE"

Estudiante: Roberto Yance Alcívar

Tutor: Ing. Wellington Maliza Cruz

Babahoyo – Los Ríos

2024

Certificación de Responsabilidad

Yo, Ing. Wellington Maliza Cruz certifico que el presente trabajo fue desarrollado por el Sr. Roberto Yance Alcivar. titulado "CONTROL TECNOLOGICO DE LA RED EMPRESARIAL "ELECTCONSTRU S.A" UTILIZANDO LA HERRAMIENTA OPEN SOURCE" ha sido revisado en su totalidad quedando autorizada su presentación según acuerdo de la dirección de nuestro centro y el mismo cumple los requisitos que debe tener un trabajo de esta envergadura.

_____

Ing. Wellington Maliza Cruz.

Acta de Cesión de Derechos

Yo, ROBERTO AARON YANCE ALCIVAR, estudiante de la Universidad Técnica de Babahoyo mención en INGENIERÍA EN SISTEMAS DE INFORMACIÓN declaro conocer y aceptar las disposiciones y autorizo a la Universidad Técnica de Babahoyo, para que hagan el uso que estimen pertinente con el presente trabajo.

_____

Sr. Roberto Aarón Yance Alcívar.

Certificación de Autoría

Yo, ROBERTO AARON YANCE ALCIVAR, declaro que soy el único autor del trabajo para la obtención del título de ingeniería en sistemas de información titulado: “CONTROL TECNOLOGICO DE LA RED EMPRESARIAL “ELECTCONSTRU S.A” UTILIZANDO LA HERRAMIENTA OPEN SOURCE

”, El presente Plan de Trabajo de Grado, en cuanto a las ideas, conceptos, procedimientos, resultados patentizados aquí, son de exclusiva responsabilidad del autor.

_____

Sr. Roberto Aaron Yance Alcivar.

AGRADECIMIENTO

El autor de este trabajo desea agradecer a:

Dios, por permitirme terminar este camino, por darme el valor, coraje necesario, perseverancia y fuerza para afrontarlo todo en cada momentode mi vida y la capacidad para disfrutarlo en losmomentos felices.

A mi querida familia, porque en sus momentos, buscaron lo mejor para mí y me hicieron una persona con valores y principios para toda la vida.

También quiero agradecer a todas esas personas que han aportado con su ayuda paracumplir mi meta: amigos, profesores y autoridades de este prestigioso establecimiento educativo.

Dedicatoria

Dedico este trabajo a mi señor Jesucristo, quien me ha dado fortaleza, sabiduría y su inmensa ayuda en cada paso de mi vida, quienme ha levantado de los momentos más difíciles.

A mi dulce madre y mi querida familia que creyeron en mí y me dieron la oportunidad de estudiar, con gran esfuerzo e inmenso amor y paciencia.

A todos mis hermanos que hemos pasado en los buenos y malos momentos, espero que lessirva de ejemplo para seguir adelante, todo esalcanzable en la vida mientras se proponen, suerte mis hermanos

A todas aquellas personas que, durante este largo camino de mi carrera profesional, han creído en mí y me han ayudado a formar las bases de mi vida.

Roberto Aaron Yance Alcivar.

Tabla de Contenidos

Lista de Cuadros Y Gráficos

Resumen

Las redes informáticas, se vuelven cada vez más complejas y la exigencia en cuanto a la operación de las mismas es cada vez más grande. Las redes soportan más aplicaciones y servicios estratégicos. Por lo cual el análisis y monitoreo de redes se ha convertido en una labor más importante y de carácter proactivo para evitar problemas y mejorar la calidad del servicio que se brinda a los usuarios de las redes.

Se ha seleccionado el software de monitoreo de red la elección del mismose la ha hecho en base a las grandes capacidades que posee y a que es de licencia libre, compatible con multiplataforma y soporta varios protocolos entre otras cualidades que se describirán más adelante. Wireshark es un analizador de protocolos utilizado para realizar elanálisis, captura de paquetes de datos y solucionar problemas en redes de comunicaciones cuenta con todas las características estándares de un analizador de protocolos

Análisis comparativo

- CACTI, LibreNMS y OpenNMS están más orientados al monitoreo de redes, con CACTI enfocado en la visualización de rendimiento, LibreNMS en la facilidad de uso y OpenNMS en la escalabilidad y detección proactiva.
- Wireshark, en cambio, es una herramienta para el análisis profundo de tráfico en tiempo real, útil para la resolución de problemas específicos, pero no para el monitoreo continuo.
- OpenNMS es más robusto para grandes infraestructuras, mientras que LibreNMS ofrece una configuración más simple. CACTI sobresale en la visualización de métricas históricas, y Wireshark en el diagnóstico detallado de paquetes.

Una vez que estas herramientas han identificado las vulnerabilidades en la red, es importante aplicar controles para mitigar los riesgos.

Tráfico no cifrado

- **Problema**: La detección de tráfico no cifrado puede exponer datos sensibles.
- **Control**: Implementar cifrado en todas las comunicaciones usando HTTPS, FTPS o SSH. También se recomienda usar VPN para proteger el tráfico en redes inseguras.

CAPITULO I – INTRODUCCIÓN

1.1. Tema

1.2. Análisis y recopilación de paquetes de datos en la red utilizando herramientas Open Source.

1.3. Planteamiento del Problema

1.3.1. Antecedentes

La pérdida del rendimiento de la red es algo que todos los administradores de redes han tenido que enfrentar en algún momento. En ese caso, sabrá que tener claro por qué está sucediendo el problema puede ser difícil debido a la falta de tiempo y recursos o al desconocimiento de las herramientas adecuadas.

Los analizadores de redes siempre han sido dispositivos de hardware costosos y difíciles de usar. Sin embargo, con los nuevos avances tecnológicos, se han desarrollado analizadores de red basados en software que permiten a los administradores solucionar problemas de red de manera más fácil y económica.

El análisis de la red se realiza para facilitar el almacenamiento y el procesamiento.

Información porque nos permitirá compartir datos, de la misma manera nos permitiría configurar

Recursos a los que se puede acceder en línea. Desde 2006, Ethereal se conoce como Wireshark, una herramienta gráfica

Es utilizado por expertos, administradores o usuarios de la red para identificar y analizar la información entrante.

Capture todo tipo de tráfico en cualquier momento.

1.2.2. Diagnosticar o tratar el problema general.

1.2.2.1. Las Causa y los efectos

- No realizar análisis de red.
- Recursos tecnológicos de la red no utilizados en su totalidad
- El uso inadecuado de protocolos en el tráfico de paquetes de datos
- captura de paquetes
- Sobrecarga de tráfico de red
- Vulnerabilidades de la red, pérdida de información de la red.

La falta de conocimientos o herramientas de seguridad, mecanismos de seguridad inapropiados para la información en paquetes de datos y la falta de recursos o herramientas tecnológicos para solucionar problemas de seguridad en las redes

1.3.1.1. Pronóstico y control del pronóstico

La falta de mecanismos de seguridad en las redes aumenta la vulnerabilidad a los ataques de rastreador significa que se pierden datos importantes de la empresa. Las posibles causas de los problemas de red incluyen la falta de comprensión de los puertos, protocolos y mecanismos de seguridad, direcciones IP, tráfico que circula en la red, congestionamiento, pérdida de paquetes y tiempos de respuesta más largos.

Control del pronóstico

Para controlar estos efectos, se utilizan análisis de redes, observación del tráfico y captura de paquetes de datos, uso de protocolos seguros y puertos.

1.4. Formulación de un problema específico.

1.4.1. Problema principal.

La herramienta de supervisión de código abierto permite a los usuarios rastrear y supervisar sus sistemas, redes e infraestructuras para detectar problemas de rendimiento y seguridad en tiempo real.

Ofrecen información y visualización de datos en tiempo real para ayudar a los usuarios a optimizar el rendimiento y solucionar problemas, minimizar el tiempo de inactividad y garantizar la fiabilidad de la infraestructura informática.

1.4.2. Problemas Secundarios

- Problema de usabilidad
- Actualizaciones y migraciones
- Problemas legales
- Adaptación y formación
- Problemas de rendimiento

Estos problemas secundarios tambien son importantes de considerar al evaluar las herramientas Open Source para el uso en diversos análisis

1.5. Objetivos

1.5.1. Objetivo general

Generar Controles al tráfico de la red de la empresa ELECTCONSTRU S.A. a través del escaneo de la red con herramientas open source.

1.5.2. Objetivos Específicos

- Analizar las herramientas Open Source para escaneo de redes de la empresa ELECTCONSTRU S.A.
- Examinar la red de la empresa ELECTCONSTRU S.A., para determinar la vulnerabilidad a la cual está expuesta
- Determinar los controles para mejorar la seguridad del trafico de la red de la empresa ELECTCONSTRU S.A.

Justificación

1.5.3. Justificación Teórica

El análisis de redes, también conocido como análisis de paquetes, análisis de protocolos o análisis de tráfico, es el proceso de capturar tráfico en la red e inspeccionarlo de cerca para determinar lo que está sucediendo en la red.

Un analizador de paquetes decodifica datos de protocolos comunes y muestra el tráfico de red en un formato legible por humanos. Los programas llamados rastreadores monitorean los datos enviados a través de las redes y los analizadores de redes pueden ser dispositivos de hardware separados que contienen software o software especializado instalado en computadoras portátiles o de escritorio. Las características del analizador de red incluyen interfaz de usuario, gráficos, capacidades estadísticas y cantidad de protocolos admitidos.

Justificación Metodológica

El Capítulo 3 de Metodologías detalla las técnicas necesarias para plantear, Analizar y recopilar paquetes de datos en la red.

Gracias a una investigación que utiliza métodos y técnicas informáticas que se pueden usar en una red, utilizando herramientas de licencia pública que vamos a usar en nuestro análisis y captura de datos.

1.5.4. Justificación Práctica.

La herramienta Open Source que se utilizara para analizar y capturar paquete de datos se puede usar, implementar e instalar en cualquier máquina, y porque está disponible bajo la licencia pública GPL, los administradores de redes y los usuarios de varias redes pueden usarlo.

Todos los procesos de envío, recepción y seguimiento de la información que circula en la red podrán ser ayudados por el estudio de este análisis y captura de paquetes de datos.

1.6. Cronograma

Cronograma de Actividades

Nombre de la Tarea	Junio 2024	Julio 2024	Agosto 2024
Presentación y Aprobación			
Presentación del tema de tesis de graduación.	x		
Aprobación del tema de tesis de graduación.	x		
Designación de Tutor	x		
Unidad 1: Diseño del Anteproyecto		x	
Redacción del Diseño del Anteproyecto		x	
Revisión y Ajustes del Anteproyecto		x	
Unidad 2: Marco de Referencia		x	
Desarrollo del Marco Teórico		x	
Elaboración del Marco Conceptual		x	
Redacción del Marco Legal		x	
Unidad 3: Metodología		x	
Selección y Justificación de Metodologías		x	
Definición de Técnicas de Investigación		x	
Unidad 4: Desarrollo del Proyecto			x
Desarrollo del Objetivo 1			x
Desarrollo del Objetivo 2			x
Desarrollo del Objetivo 3			x
Desarrollo del Objetivo 4			x
Desarrollo del Objetivo 5			x
Finalización y Presentación			x
Revisión y Presentación del Proyecto			x
Elaboración de la versión en borrador			x
Unidad 5: Conclusiones y Cierre			x
Redacción de Conclusiones y Recomendaciones			x
Compilación de Anexos			x

Elaborado por: Roberto Yance

CAPITULO II - MARCO DE REFERENCIA

1.7. Marco Teórico

1.7.1. Análisis de Paquetes de Datos

Para poder estudiar su contenido, un análisis es dividir un todo en partes más pequeñas. Los paquetes de datos contienen datos que se pueden analizar y capturar. Con una herramienta que pueda capturar y analizar paquetes de datos en una red.

Los paquetes de datos con la información pueden cifrarse con una clave de acceso para que no toda la información pueda interpretarse o registrarse.

1.7.2. ¿Quién utiliza Analizadores de Red?

Los analizadores de red son una herramienta muy útil para el diagnóstico y resolución de problemas de red, problemas de configuración del sistema y problemas de aplicación, que son utilizados por el administrador de sistemas, ingeniero de redes, ingeniero de seguridad, operador de sistemas y programadores.

El arte del análisis de redes tiene muchas facetas. Los intrusos utilizan el análisis de la red para propósitos dañinos, mientras que los profesionales de la seguridad lo utilizan para la solución de problemas y el control de la red. Un analizador de redes es una herramienta y, como cualquier herramienta, puede utilizarse tanto para el bien como para el mal. (Orebau et al., 2007)

1.7.3. Los analizadores de red se utilizan para:

• Solucionar problemas de red

• Analizar el rendimiento de la red para encontrar cuellos de botella.

• Detección de intrusiones en la red

• Registrar el tráfico de la red para debates y pruebas.

• Analizar el rendimiento de las aplicaciones.

1.7.3. ¿Por qué los atacantes utilizan interceptores?

Los rastreadores pueden representar una grave amenaza para la seguridad de la red. cuando son utilizados por personas malintencionadas. Los piratas de la red utilizan sniffers para recopilar datos confidenciales.

Los términos "sniffing" y "análisis de red" se están convirtiendo cada vez más en un término no negativo.

Dado que los sniffers no se conectan directamente con otros sistemas de la red, su uso ilegítimo se considera un ataque pasivo. Mediante un ataque activo, un rastreador puede instalarse como partV

Los atacantes utilizan analizadores de red para:

- Guardar contraseñas y nombres de usuario en texto sin formato.
- Detectar patrones de uso de los usuarios en la web
- Recopilar información confidencial, capturar y reproducir voz en conversaciones telefónicas IP (VoIP) y mapear la distribución de la red, y realizar pruebas de huellas de sistema operativo pasiva.

1.7.4. Evaluación de un analizador de paquetes

Al seleccionar un rastreador de paquetes para evaluar un analizador de paquetes, se deben considerar varios factores, incluidos los siguientes:

Cada uno de los protocolos que se soportan para capturar paquetes de datos puede interpretar un protocolo diferente.

La mayoría de las personas pueden comprender los protocolos de red comunes (como IPv4 e ICMP), los protocolos de la capa de transporte (como TCP y UDP) y los protocolos de la capa de aplicación (como DNS y HTTP). Sin embargo, no se pueden utilizar con protocolos más antiguos o más nuevos, como IPv6, SMBv2 y SIP. Al elegir un rastreador, asegúrese de que sea compatible con los protocolos que desea utilizar.

Considere el diseño del programa, la instalación fácil y el flujo normal de operaciones. El programa que seleccione debe ser compatible con su nivel de experiencia. Es posible que desee evitar sniffers de línea de comandos más avanzados como tcpdump si no tiene experiencia en análisis de paquetes.

Si tiene una gran riqueza de experiencia, puede encontrar un programa avanzado más atractivo. A diferencia del análisis de paquete, Incluso puede resultar útil combinar varios programas de rastreo en determinados casos. Existen muchos programas gratuitos de detección de paquetes que compiten con los productos comerciales. La diferencia más notable entre los productos comerciales y las alternativas gratuitas es la función de informes. Los productos comerciales suelen incluir un módulo de informes. Que las aplicaciones libres normalmente no tienen.

Soporte para aplicaciones Incluso después de aprender los fundamentos de un programa de soplado, Es posible que necesite ayuda para resolver nuevos problemas, encontrar documentación para desarrolladores, foros públicos y listas de correo.

Las comunidades que utilizan estas aplicaciones incluyen foros de discusión, wikis y blogs que ayudan a los usuarios a utilizar la herramienta. Desafortunadamente, no todos los rastreadores de paquetes son compatibles con todos los sistemas operativos.

Elija uno que funcione en todos los sistemas operativos que necesite. (Sanders, 2011)

1.8. Describa el proceso de implementación de Wireshark para su uso en una red.

Todos los lineamientos necesarios para implementar y utilizar Wireshark seexplicarán en detalle a continuación.:

1.8.1. Paso 1 - Cumple con los requisitos específicos para su instalación.

Requisitos del sistema para instalar Wireshark

Para instalar Wireshark, su sistema debe cumplir con los siguientes requisitos mínimos:

- Procesador con frecuencia de 400 MHz o superior.
- RAM 512 MB o más.

- 80 MB de espacio libre en disco
- Para almacenar capturas de paquetes de información se requiere una mayor cantidad de espacio en disco duro.
- La tarjeta de red NIC está aceptada de forma amistosa.
- Se utiliza WinPcap como controlador de captura.
- Programación de software Wireshark.

1.8.2. Paso 2 - Tienen una conexión de red para su implementación.

Requisitos de red necesarios para la implementación de Wireshark

Es necesaria una conexión a la red para utilizar la herramienta de wireshark en una red.
La red puede estar compuesta físicamente por equipos reales o virtualmente por equipos virtuales que operan dentro de un mismo equipo.
Con todas las topologías de red conocidas

Se compone de un equipo o más, aunque se puede examinar en un sistema. El cableado estructurado e inalámbrico es una forma de conectar la red. La captura remota de paquetes de datos es posible con Wireshark.

1.8.3. Paso 3 - Sistema operativo compatible con la versión Wireshark.

Protocolos soportados

Cuando un analista de red lee los datos de la red, debe tener una comprensión de lo que observay luego presentar los resultados en un formato que sea fácil de leer. El término para esto es el protocolo de decodificación. El número de protocolos que un sniffer puede leer y mostrar con frecuencia determina su fuerza; por esta razón, la mayoría de los sniffers comerciales pueden operar con cientos de protocolos. Con su actual soporte de más de 750 protocolos, Wireshark es muy competitivo en este campo. Varios colaboradores del proyecto Wireshark están incorporando constantemente nuevos protocolos.

El protocolo, también conocido como disectores, se puede incluir como complementoso directamente en el código.

1.8.4. Paso 4 - Sistema operativo compatible con la versión Wireshark.

Sistemas Operativos con sus plataformas Compatibles:

- Microsoft Windows
- Mac OS X
- FreeBSD
- Linux
- NetBSD
- OpenBSD
- Android
- Solaris
- Unix

1.8.5. Paso 5 - Descargue o instale la biblioteca Wireshark.

- **WinPcap**

WinPcap se encuentra compuesto por un controlador, el cual extiende el sistema operativo con el fin de Proporcionar acceso a la red de bajo nivel y se utilizan bibliotecas para acceder de manera sencilla a las capturas de red de bajo nivel, y tiene otras características útiles, como un capturador de paquetes y las herramientas de filtrado de código abierto incluyen el filtrado. Soporte para paquetes a nivel de kernel, herramienta de estadísticas de red y captura remota de paquetes.

Información descargada del sitio web oficial de WinPcap http://www. winpcap.org/

La Aplicación de programación de captura de paquetes pcap. y de interfaz (API) es implementado por Windows. En resumen, este conductor trabaja con el sistema operativo para recopilar los datos sin procesar del paquete, utilizar filtros y modificar de manera promiscua la tarjeta de entrada y salida.

1.9. El proceso de capturar paquetes de datos a través de un filtro de búsqueda usando Wireshark

1.9.1. ¿Dónde Realizar la Captura de Datos?

Definir dónde analizar el tráfico es el primer paso para conocer la red. Además, Wireshark brinda la capacidad de capturar y analizar el tráfico de forma remota. Dónde ponerlo es la pregunta que surge.

Para analizar el tráfico que circula por ese segmento de red, aunque parece razonable instalar Wireshark en el propio servidor de ficheros, nos encontraremos con situaciones en las que, por razones de seguridad, no podremos acceder físicamente al servidor.

Las técnicas que permiten realizar una captura de tráfico sin tener que cargar Wireshark en el propio servidor son alternativas.

1.9.2. Modo Promiscuo

Una tarjeta de interfaz de red (NIC), que admite un controlador en modo promiscuo, es necesaria para capturar paquetes en una red. En el modo promiscuo, una tarjeta puede ver todos los paquetes que pasan por la red.

Podemos garantizar que la NIC captura todo el tráfico de manera promiscua. Independientemente de la dirección, la tarjeta pasa a cada paquete que se ve en el procesador principal cuando funciona en modo promiscuo. Una aplicación de recolección de paquetes puede capturarlo y analizarlo una vez que el paquete llega a la CPU.

La interfaz gráfica de Wireshark incluye los controladores de libpcap / WinPcap, que le permiten transferir su tarjeta de red en modo promiscuo directamente. Además, los NIC más actuales soportan el modo promiscuo.

Es necesario disponer de un sistema operativo que permita el uso promiscuo. Si no existen privilegios de usuario en un sistema, no se debe realizar ninguna captura de paquetes en la red. La mayoría de sistemas operativos no permiten el uso indiscriminado de la tarjeta de red.

Para los oyentes que solo desean ver el tráfico enviado directamente a la red, el modo mixto de NIC no es necesario. (Sanders, 2011).

1.9.3. Cuadro comparativo de herramientas Open Source.

Característica	Cacti	OpenNMS	LibreNMS	Wireshark
Propósito Principal	Recolección de datos y generación de gráficos de red	Monitorización empresarial de redes y sistemas	Monitorización de redes y sistemas mediante SNMP	Análisis de tráfico de red
Arquitectura	Basado en PHP/MySQL, SNMP para recolección de datos	Arquitectura modular, basada en Java	Basado en PHP/MySQL, SNMP para recolección de datos	Basado en captura de paquetes, análisis en tiempo real
Licencia	Open Source (GPL)	Open Source (AGPL)	Open Source (GPL)	Open Source (GPL)
Interfaz de Usuario	Interfaz web con gráficos detallados	Interfaz web avanzada con mapas de red y alertas	Interfaz web intuitiva y personalizable	Interfaz gráfica de usuario (GUI)
Alertas y Notificaciones	Limitado, requiere plugins adicionales	Soporte completo para alertas, notificaciones y escalado	Soporte para alertas basadas en SNMP	No disponible, se centra en captura y análisis
Capacidad de Escalabilidad	Escalabilidad limitada, ideal para pequeñas redes	Altamente escalable, apto para grandes entornos	Moderadamente escalable, mejor para redes medianas	No aplica, diseñado para análisis en tiempo real de un solo punto de captura
Compatibilidad	Windows, Linux, macOS	Linux, Windows, macOS	Windows, Linux, macOS	Windows, Linux, macOS
Recolección de Datos	Basado en SNMP, plantillas personalizables	Recolección automática de datos mediante SNMP, ICMP, WMI	Recolección automática de datos mediante SNMP	Captura de paquetes en tiempo real, análisis de datos pasivos

Integraciones	Limitadas, pero soporta plugins externos	Integración con múltiples herramientas y APIs	Soporte para integraciones externas y plugins	Se integra con herramientas de análisis de red
Comunidad y Soporte	Comunidad activa, buena documentación	Amplia comunidad, soporte comercial disponible	Comunidad activa, soporte a través de foros	Amplia comunidad, soporte extensivo en análisis de redes
Ventajas	Fácil de configurar y usar, gráficos detallados	Solución completa, escalabilidad, automatización avanzada	Fácil de configurar, buena detección automática	Análisis profundo de tráfico de red, decodificación de protocolos
Desventajas	Limitado en cuanto a escalabilidad y notificaciones	Curva de aprendizaje más pronunciada, requiere más recursos	Menos robusto que OpenNMS en grandes redes	No es una herramienta de monitorización, se limita al análisis post-captura

Resumen:

- **Cacti** es ideal para pequeñas redes que necesitan monitorear y visualizar el rendimiento de la red mediante gráficos detallados.
- **OpenNMS** es una solución más robusta y escalable, adecuada para entornos empresariales con necesidades de monitorización avanzada.
- **LibreNMS** se enfoca en la simplicidad y es una buena opción para redes medianas, ofreciendo detección automática y facilidad de uso.
- **Wireshark** se diferencia de las otras herramientas al centrarse en el análisis profundo del tráfico de red, sin capacidades de monitoreo continuo.

Cada herramienta es adecuada para diferentes casos de uso, dependiendo del tamaño de la red, la necesidad de escalabilidad, y el tipo de monitoreo o análisis que se requiere.

Para el Control Tecnológico del tráfico de red, que implica una supervisión detallada del flujo de datos, identificación de patrones anómalos, análisis en tiempo real, y control del comportamiento de la red, Wireshark es la mejor herramienta entre las opciones mencionadas.

Razones:

1. **Análisis Detallado del Tráfico**:
    - **Wireshark** es específicamente diseñado para capturar y analizar paquetes de datos en la red. Te permite inspeccionar el tráfico en tiempo real y ofrece un análisis profundo de cada paquete, mostrando información como la fuente, el destino, el protocolo utilizado, y el contenido de los datos.
2. **Decodificación de Protocolos**:
    - Wireshark soporta la decodificación de cientos de protocolos, lo que es esencial para entender exactamente qué está sucediendo en la red en un nivel granular.
3. **Detección de Anomalías y Problemas**:
    - Al ser capaz de capturar el tráfico en tiempo real, Wireshark permite identificar inmediatamente cualquier comportamiento anómalo o malicioso en la red, lo que es crucial para el control tecnológico.
4. **Compatibilidad y Usabilidad**:
    - Es compatible con Windows, Linux y macOS, y aunque tiene una curva de aprendizaje, es muy poderosa para usuarios que necesitan un análisis detallado y control total sobre lo que sucede en la red.

Limitaciones:

- **Wireshark** no es una herramienta de monitoreo continuo ni de gestión de la red. Está más enfocada en la captura y análisis en tiempo real o posterior. Por lo tanto, para un monitoreo de red a largo plazo, puede ser complementada con otras herramientas como **Cacti**, **OpenNMS** o **LibreNMS**.

1.9.4. ¿Por qué Wireshark?

Wireshark es una herramienta muy popular en el mundo de la seguridad informática y las redes por varias razones:

1. **Captura de Paquetes en Tiempo Real**: Wireshark permite capturar y analizar el tráfico de red en tiempo real, lo que es crucial para diagnosticar problemas de red, detectar intrusiones, o analizar el rendimiento de una red.
2. **Análisis Detallado**: Ofrece un análisis profundo de cada paquete de datos que pasa por la red. Puedes ver desde los encabezados de protocolo hasta el contenido de los paquetes, lo que ayuda a comprender exactamente qué está sucediendo en la red.
3. **Soporte de Múltiples Protocolos**: Wireshark soporta una amplia gama de protocolos de red, lo que lo hace útil en casi cualquier entorno de red, independientemente de los protocolos que se utilicen.
4. **Interfaz Gráfica Intuitiva**: A pesar de ser una herramienta poderosa, Wireshark cuenta con una interfaz gráfica que facilita su uso, incluso para aquellos que no son expertos en la línea de comandos.
5. **Gratuito y de Código Abierto**: Wireshark es un software libre y de código abierto, lo que significa que cualquiera puede usarlo, modificarlo y contribuir a su desarrollo sin costo alguno.
6. **Comunidad Activa**: Al ser una herramienta tan ampliamente utilizada, Wireshark tiene una comunidad activa que contribuye a su mejora continua, lo que incluye la actualización regular de la base de datos de protocolos y el soporte técnico.
7. **Compatibilidad Multiplataforma**: Wireshark está disponible para varios sistemas operativos, incluidos Windows, macOS, y Linux, lo que lo hace accesible para una amplia variedad de usuarios.

Por estas razones, Wireshark es la elección preferida para administradores de redes, profesionales de la seguridad, y cualquier persona que necesite analizar y entender el tráfico de red en profundidad.

1.9.5. ¿Cómo Trabajan los Analizadores de paquetes?

El proceso de limpieza de paquetes requiere la colaboración del hardware y del software. Esto se puede dividir en tres fases:

El rastreador de paquetes primero recopila datos binarios del cable de red. Por lo general, esto se logra cambiando la interfaz de red promiscua. De esta manera, la tarjeta de red puede escuchar todo el tráfico del segmento de red, no sólo el tráfico dirigido a él.

Tambien los datos binarios recopilados que se convierten a un formato legible en este paso de conversión. Los paquetes son capturados por la línea de comandos más avanzada. En este momento, los datos de la red pueden interpretarse solo en un nivel. El análisis es el tercer y último paso, que implica el análisis real de la recopilación y transformación de datos. El analizador de red captura paquetes de datos. (Sanders, 2011)

1.10. Marco Conceptual

1.10.1. Wireshark

Wireshark funciona como analizador de paquetes de red. Los analizadores de paquetes de red registran paquetes de datos e intentan mostrarlos con el mayor detalle posible. El analizador de paquetes de red es un dispositivo de medición que examina lo que está sucediendo dentro de un cable de red.

1.10.2. Paquete de Datos

En todas las redes de computadoras modernas, un paquete de datos es un componente esencial para transmitir información.

Tres componentes suelen componer un paquete: una cabecera, que normalmente contiene la información necesaria para enviar el paquete desde el emisor al receptor, un área de datos, que contiene los datos que se desean enviar, y una cola, que generalmente contiene

un código de detección de errores.

1.10.3. Red

Una red informática, también conocida como red de información o red de computadora, es un conjunto de dispositivos informáticos conectados entre sí mediante dispositivos físicos o inalámbricos para enviar y recibir impulsos eléctricos, ondas electromagnéticas u otros medios de transmisión de datos con fines de participación. información y recursos. El objetivo principal de la creación de una red informática es permitir el intercambio remoto de recursos e información, garantizar la confiabilidad y disponibilidad de la información, aumentar la velocidad de transferencia de datos y reducir los costos generales de estos esfuerzos.

1.10.4. Protocolo

Las redes modernas constan de múltiples sistemas que se ejecutan en múltiples plataformas. Se utilizan protocolos para facilitar la comunicación. El Protocolo de control de transmisión (TCP), el Protocolo de Internet (IP), el Protocolo de resolución de direcciones (ARP) y el Protocolo de configuración dinámica de host (DHCP) son algunos de los protocolos disponibles.

Una pila de protocolos es un conjunto lógico de protocolos que funcionan juntos.

Los protocolos funcionan de manera similar, lo que nos permite determinar cuántos paquetes ordenar, cómo iniciar la conexión y cómo garantizar que se reciban los datos.

Dependiendo de la función, el protocolo puede ser muy sencillo o muy complejo.

1.10.5. Programas Empaquetados con Wireshark

La versión de línea de comandos de Wireshark, tshark, y otros cinco programas de apoyo se instalan con Wireshark para ayudarlo a manipular, evaluar y crear archivos de captura.

1. Tshark
2. El editcap

Estos programas auxiliares se pueden utilizar juntos para proporcionar capacidades de administración de archivos de captura muy avanzadas. Estos archivos se pueden capturar con tshark, editar con editcap y fusionar en un archivo de captura de paquetes separado con

mergecap. (Orebau et al., 2007)

2.1. Tshark

La versión de línea de comandos de Wireshark se llama Tshark. Los paquetes en vivo se pueden capturar, decodificar e imprimir desde el cable para guardar o leer archivos de captura.

Dado que utiliza la misma biblioteca de ganchos libpcap y la mayoría del mismo código, tshark y Wireshark tienen algunas de las mismas características.

Tshark puede leer formatos de captura de paquetes similares a los de Wireshark y puede identificar automáticamente el tipo. Las secuencias de comandos son una ventaja de usar tshark. (Orebaugh, y otros, 2007).

2.1.1.1. Editcap

El programa Editcap se puede usar para eliminar o seleccionar paquetes de un archivo y Convierta el formato del archivo capturado. Simplemente lee datos de un archivo de captura guardado y luego escribe algunos o todos los paquetes en un nuevo archivo de captura. No registre datos directamente. Editcap puede leer y escribir todos los archivos del mismo tipo desde Wireshark y, por defecto, usar el formato libpcap. Editcap puede identificar el tipo de archivo que está leyendo y puede leer archivos comprimidos con gzip. Editcap escribe todos los paquetes del archivo de captura al archivo de salida por defecto. (Orebaugh, y otros, 2007)

2.1.1.2. Mergecap

El método mergecap combina varios archivos de captura salvados en un solo archivo de salida. Mergecap puede leer todos los archivos del mismo tipo desde Wireshark y guardarlos en formato libpcap de forma predeterminada. Los lotes de archivos de entrada se combinan en el orden correcto y cronológico basado en la fecha y hora de cada paquete de manera predeterminada. (Orebaugh, y otros, 2007)

2.1.1.3. Text2pcap

Text2pcap crea archivos de captura leyendo códigos hexadecimales ASCII y luego escribiendo los datos en el archivo de salida libpcap. Puede leer la salida hexadecimal de un paquete o más y crear archivos de captura con él.

Además, text2pcap solo puede leer hexdumps de datos de nivel de aplicación creando cabeceras ficticias de Ethernet, IP y UDP o TCP para Wireshark. (Orebaugh, y otros, 2007).

2.1.1.4. Capinfos.

Capinfos - nueva herramienta de línea de comando que puede usar con Wireshark para examinar sus archivos de captura guardados y analizar estadísticas de informes sobre el recuento de paquetes, el tamaño de los paquetes e información específica. En cambio, Capinfos proporciona una breve descripción del contenido del archivo de captura. proporciona información sobre el tráfico, a diferencia de otras herramientas de informes estadísticos proporcionadas por las herramientas Wireshark.

2.1.1.5. Dumpcap

El tráfico de una interfaz vivo se captura y guarda con la utilidad dumpcap en un archivo libpcap. La biblioteca de decodificadores de protocolo no está incluida en esta utilidad, pero sí un subconjunto de las funciones que están disponibles en tshark. Esto reduce el tamaño del dumpcap, lo que puede ser beneficioso para la captura de tráfico con múltiples procesos en sistemas de baja memoria. (Orebaugh, y otros, 2007).

2.1.1.6. Marco Temporal

En la ciudad de Babahoyo, Ecuador, se trabajará en el análisis y recopilación de paquetes de datos en la red de la Empresa ELETCONSTRUC S.A. utilizando Wireshark. En el ámbito de las redes, puede ser bastante amplio, dependiendo de dónde planee analizar y recopilar paquetes de datos, así como la estructura física, tecnológica y los recursos que manejan o disponen en la red.

Con el director del proyecto estableceremos el tiempo de desarrollo para analizar y recopilar paquetes de datos de la red con Wireshark, que se ajustará al cronograma de actividades que se presenta al final de este capítulo.

2.1.1.7. Marco Legal - Base jurídica

Antes de abrir el analizador de protocolos de red, por ejemplo: Wireshark, que instalo para cualquier uso, lea atentamente las políticas de la empresa. La ejecución de los analizadores de red está prohibida si las políticas de red no están escritas y utilizadas correctamente.

En el análisis de redes de las empresas que ofrecen consultoría de seguridad a sus clientes, confirmar el uso de un sniffer está incluido en su reglamento. Especifica cómo, dónde y cuándo se usará la herramienta. Indicar cláusulas de no divulgación que lo eximen de la responsabilidad de aprender información confidencial.

3. CAPITULO III – METODOLOGÍAS

3.1. Metodología

La metodología implementada se basó mediante un enfoque cualitativo obteniendo la respectiva información mediante textos informativos, realizando investigaciones de diferentes sitios web y tambien en algunos casos de estudios llegando así al final en una observación directa para poder realizar una comparación entre diferentes herramientas Open Source, para obtener un resultado final y así saber cuál herramienta es la más adecuada para realizar este trabajo.

3.2.Técnicas

3.2.1 Investigación.

- Análisis documental. (implico la revisión, interpretación y análisis de documentos existentes para obtener información relevante sobre un tema).
- Observación. (incluyo a observar de manera directa el comportamiento de las herramientas).
- Estudio correlacional. (este método fue utilizado para analizar la relación y obtener un cuadro comparativo de las herramientas).

4. CAPITULO IV - DESARROLLO

4.1.Importancia de implementar medidas de seguridad para proteger los paquetes deataques.

Considere la situación en la que un ladrón de bancos intenta robar el banco más grande de la ciudad, ubicado en la dirección A. Pasan una semana planeando un elaborado robo, pero cuando llegan a la dirección allí, descubren que el banco se había trasladado a la dirección B. Aún peor. Considere una situación en la que un ladrón planea irrumpir en un banco durante el horario comercial para robar de la bóveda, pero descubre que el banco está cerrado ese día. ¿Qué pasa si un ladrón entra a un banco sin saber lo que está pasando? diseño de edificios? Como no conoce las vulnerabilidades de seguridad física, no sabrá cómo acceder al edificio.

En estos tres escenarios distintos, los ladrones de bancos comparan a un atacante de red con un programa de rastreo para hacer más comprensible cómo un atacante planea realizar su objetivo en la red o la información. En esta sección demostraremos la importancia de implementar medidas de seguridad para evitar ataques a paquetes de datos.

4.1.2. Técnicas Avanzadas de Sniffing

Para el uso en redes, hay numerosas alternativas a Wireshark. Lamentablemente, los atacantes pueden utilizar estas técnicas para robar contraseñas u otros datos de la red.

4.1.3. Reconocimiento - Footprinting

Un atacante necesita primero realizar una investigación en profundidad sobre el sistema de destino. Este paso, conocido como footprinting, se puede realizar con frecuencia con una variedad de recursos o herramientas de software, como Wireshark.El atacante generalmente comenzará a examinar la dirección IP o el nombre DNS después de completar esta investigación con el fin de abrir puertos o servicios que se ejecutan.

El primer paso, también conocido como fase 1 o fase de reconocimiento, es el paso más importante para que los hackers obtengan toda la información necesaria antes de lanzar un ataque. El primer obstáculo que debe superar un atacante es asegurarse de que el objetivo esté vivo y sea accesible. El escaneo también le dice al atacante que los puertos de destino están escuchando.

El atacante logra, reúne y organiza toda la información necesaria acerca de su objetivo o víctima en esta parte del footprinting. Cuanta más información obtiene con mayor precisión, puede lanzar un ataque, obteniendo información como:

Contramedidas:

La realización de fotografías en una organización puede aportar a los responsables de la organización de red a saber qué tipo de información reside fuera de la empresa y las amenazas que contiene. Se deben tomar medidas preventivas para evitar que la información presentada se utilice para "explotar" el sistema.

4.1.3.1.1. Fingerprinting Pasivo

Algunos campos se verifican en los paquetes enviados desde el destino mediante impresión de huellas pasiva para determinar el sistema operativo en uso. Dado que la técnica solo escucha a los paquetes de envió de la máquina objetivo y no envía activamente paquetes al mismo host, se considera pasiva. Debido a que les permite ser cautelosos, el reconocimiento de huellas es el tipo ideal para los atacantes. La toma de huellas dactilares pasiva examina campos específicos en los paquetes enviados desde el objetivo para identificar el sistema

operativo utilizado. La técnica se considera pasiva, ya que solo escucha los paquetes de envío de la máquina objetivo y no puede enviar paquetes al mismo host. Este es el tipo de Fingerprinting más adecuado para los atacantes, ya que les permite ser cautelosos.

4.1.3.1.2. Fingerprinting Activo

Si el monitoreo pasivo del tráfico no da los resultados esperados, puede ser necesario un método más directo.

Este método se conoce como impresión de dedos activa. Se trata de que el atacante esté enviando paquetes que han sido especialmente diseñados para obtener las respuestas revelan el sistema operativo utilizado en la computadora de la víctima, que revela el sistema operativo utilizado en la computadora de la víctima. Gracias a este enfoque, emprende una comunicación directa con la víctima, no es nada reservado, pero puede ser muy eficaces.

4.1.3.2.Escaneo SYN

Un escaneo TCP SYN, también conocido como escaneo de sigilo o análisis de medio abierto, es el tipo de análisis que se realiza con frecuencia en contra de un sistema. Por varias razones, un escaneo SYN es el tipo más común:

• Es confiable y rápido.

• Es menos ruidoso que otras técnicas de escaneo y es preciso en todas las plataformas, independientemente de la aplicación

El proceso de negociación de tres vías sirve como base para el escaneo SYN TCP para Establecer qué puertos están disponibles en un host de destino. Al recibir este paquete SYNTCP, el atacante envía un paquete SYNTCP a diversos puertos de la víctima, como si deseara establecer un canal de comunicaciónnormal en los puertos. Una de las pocas situaciones que pueden surgir son como se muestra en la figura,los posibles resultados de un escaneo TCP SYN.

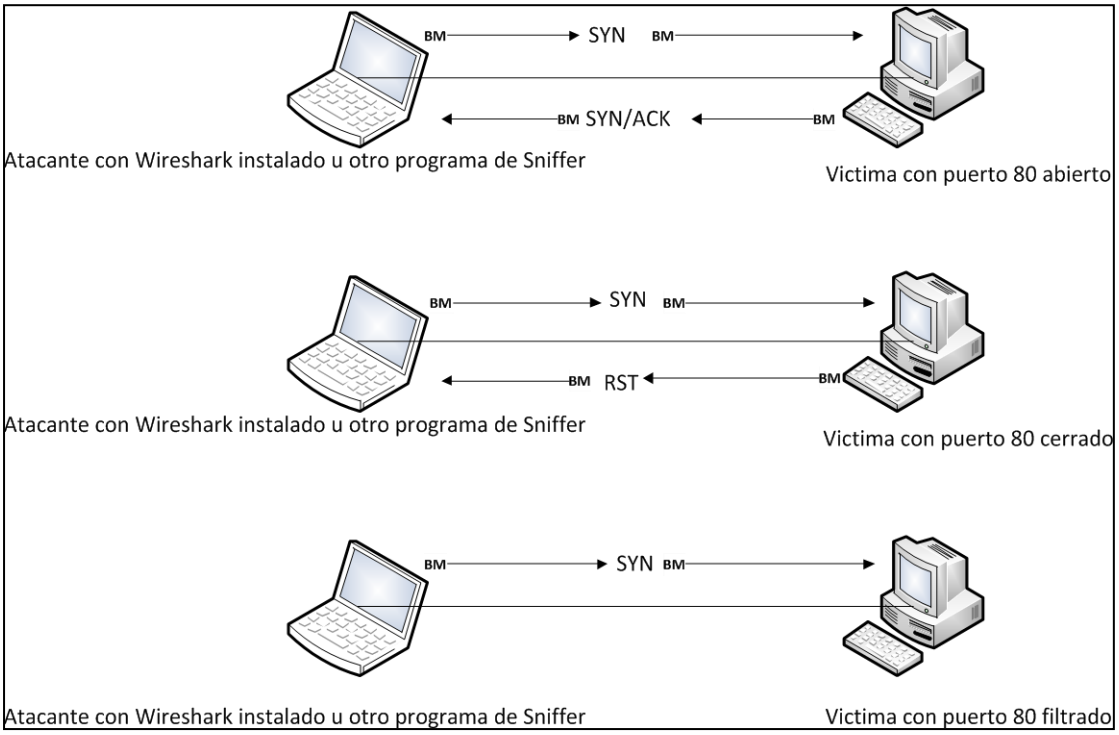


Figura 1 Posibles resultados del escaneo SYN

Si el servicio está ubicado en la computadora de la víctima escucha un paquete SYN en un puerto que lo recibe, el atacante responde con un paquete TCP SYN/ACK, la segunda parte de la conexión TCP. El atacante sabe entonces que el puerto se encuentra abierto y que un servicio está a su disposición. En este caso, el atacante no quiere que eso suceda porque no se comunica con el host más, pero normalmente se envía un TCP ACK final para completar el protocolo de enlace de conexión. Como resultado, el atacante no intenta completar la conexión TCP.

El atacante no recibirá un paquete si el servicio no escucha en el puerto de la computadora, Además, el atacante no puede recibir respuesta alguna. Esto podría indicar que un dispositivo intermedio, como un firewall o el propio anfitrión, está filtrando el puerto. Por otro lado, es posible que simplemente se haya perdido la respuesta en el tránsito. Aunque este resultado general indica que el puerto está cerrado, no es definitivo.

4.1.3.3.Ataques MITM Man-in-the-middle – Intermediarios

Los protocolos de cifrado como SSL y SSH son los más efectivos para protegerse contra el espionaje. Sin embargo, los paquetes dsniff y Ettercap más recientes incluyen técnicas para engañar el cifrado, conocidas como ataques MITM Man-in-the-middle.

El atacante crea un servidor que responde a la solicitud de los clientes, por ejemplo, un servidor que responde a una solicitud de https://www.servidor.com, se puede utilizar la misma técnica. Un usuario se conecta a esta máquina con la intención de iniciar una sesión encriptada con Amazon.com. Al mismo tiempo, el ciberdelincuente se conecta a www.servidor.com real y se presenta como el usuario. El atacante participa en teoría, Los protocolos de cifrado otorgan protección contra este. Un usuario que afirma ser Ejemplo.com debe demostrar que es Ejemplo.com. En el ámbito práctico, la mayoría de los usuarios son ignorantes. Los ataques MITM han demostrado ser de gran utilidad cuando se utiliza en el ámbito laboral.

4.1.3.4. Cracking

Herramientas como dsniff y Ettercap capturan contraseñas no cifradas y contraseñas encriptados.

La captura de contraseñas encriptadas no tiene sentido en teoría. Sin embargo, cuando alguien elige contraseñas débiles, como palabras del diccionario, un atacante puede usar un diccionario de 100.000 palabras y comparar la forma encriptada de cada palabra del diccionario con la contraseña cifrada en unos segundos. El atacante ha descubierto la contraseña si hay una coincidencia.

Estos programas pueden descifrar contraseñas que ya han sido descubiertas. Las herramientas como dsniff y Ettercap simplemente sacan contraseñas encriptadas de tal forma que puedan leerlas.

4.1.3.5. ARP Spoofing

El interruptor limita la velocidad que se encuentra por encima de su trayectoria, lo que es un problema importante para el control del tráfico en una red conmutada. Los interruptores guardan en su interior una lista de las direcciones MAC de los hosts presentes en cada puerto. Solo se envía tráfico a un puerto si el host de destino está registrado como presente en ese puerto.

Muchos sistemas operativos tienen la capacidad de sobrescribir la memoria caché de ARP, lo que permite la asociación de la dirección MAC con la dirección IP por defecto a través del escaneo como puerta de enlace. Esto significa que todo el tráfico saliente del host de destino será filtrado.

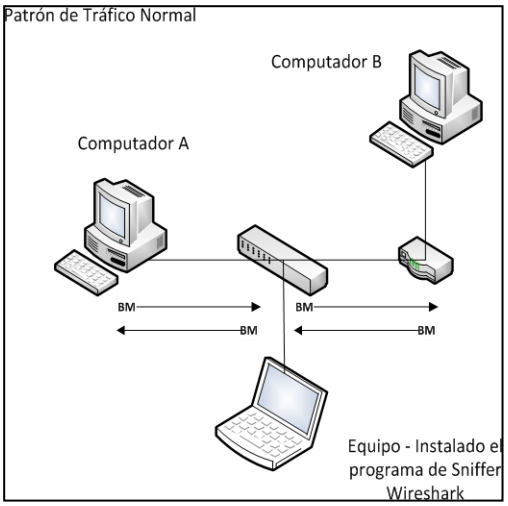
Agregue manualmente una entrada a la tabla ARP para la puerta predeterminada real pueda asegurarse de que el tráfico se envíe al destino real y para asegurarse de que se haya habilitado el reenvío IP.

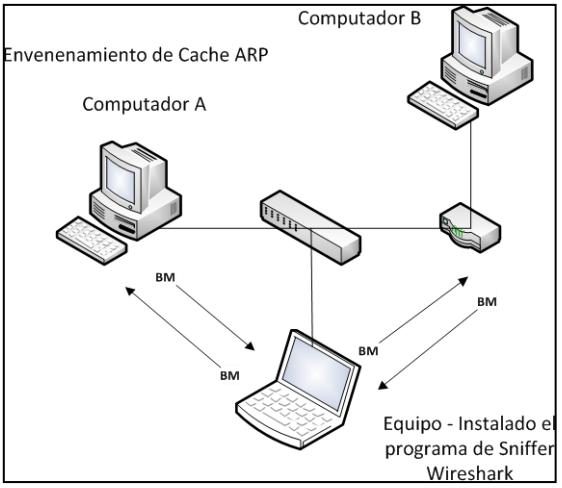
Debido a que las redes de cable módem son esencialmente redes Ethernet con cable módems que actúan como puentes, muchas son susceptibles a este tipo de ataques.

¿Cómo funciona ARP Spoofing?

El proceso de enviar los mensajes ARP a conmutadores o enrutadores Ethernet han falsificado direcciones MAC de capa 2 para bloquear el tráfico de otro equipo se conoce como envenenamiento de caché ARP. Este proceso también se conoce como ARP spoofing.

Envenenamiento por caché El método avanzado de aprovechar el cable en una red conmutada se conoce como ARP. Los atacantes suelen usarlo para envíos de paquetes señuelo a los sistemas cliente para bloquear el tráfico o provocar ataques de denegación de servicio (DoS) en los objetivos. Sin embargo, capturar paquetes de máquinas en una red conmutada también puede ser un método eficaz.





4.1.4. Proteja los paquetes de datos en la red de los rastreadores

Existen muchas alternativas y funciones más económicas para proteger los paquetes de datos de la red de atacantes específicos.

4.1.4.1.Utilizar el cifrado

La encriptación es el arma de metal que impulsará a un rastreador de paquetes sea inútil, por suerte para la seguridad de la red, cuando se usa correctamente.

Si se considera que la encriptación es confiable, su implementación frustrará a cualquier atacante que intente monitorear pasivamente la red.

Muchos protocolos de red actuales tienen su contraparte que se basa en el cifrado fuerte y todos los mecanismos que abarcan, como IPSec y OpenVPN. Lamentablemente, la seguridad IP (IPSec) es poco utilizada en Internet.

4.1.4.2.Protocolo de Seguridad en línea (IPSec)

IPSec es un protocolo de capa de red que extiende el encabezado del paquete IP para integrar la seguridad en los protocolos IPv4 e IPv6 directamente a nivel de paquete. De esta manera, se puede codificar cualquier protocolo de capa superior. Se ha integrado en cortafuegos, clientes y dispositivos de enrutamiento para garantizar que las redes sean confiables entre sí. El cifrado y la autenticación de llaves públicas y el cifrado de claves simétrico están disponibles con IPSec. Puede funcionar en modo de túnel para proporcionar

Una nueva cabecera IP que incluye las máscaras de la fuente original y de destino, así como datos transmitidos. La aplicación denominada OpenVPN emplea un único puerto TCP o UDP, lo cual resulta más

sencillo de utilizar en situaciones de dificultad con NAT y arquitecturas de cortafuegos. Asimismo, puededesempeñarse como un puente de red virtual en una capa de nivel.

4.1.5. Expresar la relevancia y el empleo de la herramienta Wireshark.

La importancia de implementar y utilizar la herramienta Wireshark para solucionar una variedad de necesidades y problemas que pueden surgir en una red y que los administradores de redes o los usuarios puedan resolver diversos problemas se demuestra por los múltiples usos que tiene.

4.1.6. La utilización de Wireshark para resolver problemas de red.

El conocimiento de cómo funciona la red en condiciones normales le permitirá detectar de manera rápida las operaciones inusuales y anormales que puedan surgir al utilizar Wireshark para resolver problemas de red.

Usar un programa de sniffer en distintos puntos de la red es una forma común de conocer cómo funciona su red. Esto permitirá comprender los protocolos que se implementan en

la red, los dispositivos presentes en cada sección y los computadores que transmiten y reciben los datos con mayor frecuencia.

Una vez que se tiene claro cómo funciona una red, puede desarrollar una estrategia para solucionar los problemas de la red.

Esto puede abordar metódicamente el problema y resolverlo con una interrupción mínima para los usuarios o clientes. Algunos minutos dedicados a la evaluación de los síntomas pueden minimizar horas de tiempo perdidas en el seguimiento del problema cuando se abordan los problemas. Un enfoque adecuado para solucionar problemas de red se basa en los siguientes procedimientos:

1. Identificar los signos que pueden desencadenar la problemática.
2. Lamentar el problema.
3. El problema se puede analizar.
4. Establecer la problemática.
5. Identificar y determinar la causa del problema.
6. Resolver la problemática.
7. Verifique la resolución del asunto.

4.1.7. Uso de Wireshark en arquitectura de red

Explore algunas arquitecturas y puntos de red cruciales de Wireshark. Para solucionar problemas y realizar un análisis adecuado, es esencial ubicar la red. Es fundamental asegurarse de que se encuentren en el segmento de red adecuado.

4.1.8. Uso de Wireshark para la administración del sistema

Se sabe que los administradores del sistema preguntan si hay un problema con la red y los administradores de red son conocidos por decir que el problema está dentro del sistema.

La verdad espera ser descubierta por Wireshark en medio de este juego de culpas.

4.1.9. Utilice Wireshark para la gestión de seguridad

¿Este protocolo es seguro? Wireshark es la herramienta perfecta para su uso, ya que es una de las tareas más comunes de los administradores de seguridad.

El reensamblaje de paquetes, esto le permite ver el contenido de los datos que se intercambian y es una de las funciones más populares y útiles de Wireshark.

Para protocolos como Telnet y FTP, Wireshark muestra sin ningún montaje el nombre de usuario y la contraseña para la conexión.

Se puede utilizar el montaje para capturar el tráfico con Wireshark o cualquier otra herramienta, Luego, utilice el botón derecho del ratón para cargar el archivo de captura en Wireshark y cargarlo en cualquier paquete de conexión para protocolos desconocidos.

La ventana con todas las comunicaciones que se realizaron durante ese período de sesiones si selecciona la opción TCP Stream. Puede ayudarlo al seleccionar la opción ASCII; además, si el protocolo es ruidoso, puede seleccionar una conversación de toda la pantalla, de emisor o receptor.

4.1.10. Implementar Wireshark como IDS en su red

Aunque existe herramientas de código abierto especializadas para detectar intrusos en redes. Wireshark podría alertar sobre cualquier otro criterio, a menos que se utilice como un sistema IDS. Las reglas para detectar intrusos de Wireshark son las siguientes:

Conexiones entre su base de datos y otros sistemas, como sus servidores Web, se realizan.

Los intentos de enviar un correo electrónico a fuentes de correo electrónico externas desde otros servidores de correo electrónico en el puerto TCP 25.

El uso de Wireshark como escuchador de conexiones a una dirección IP no utilizada o el intento de uso de una conexión remota hacia su escritorio (RDC) desde el exterior de la red.

4.1.11. Utilice Wireshark como escucha de transmisiones de información privilegiada

No hay razón por la cual Wireshark no pueda ser utilizado para detectar la transmisión de información, ya que toda empresa tiene datos confidenciales y patentados.

Para capturar todo el tráfico que sale de un puerto en un momento específico, puede utilizar Wireshark con captura de paquetes. Sin embargo, esto puede provocar graves atascos.

Para eliminar el tráfico en el que no se espera que la información de propiedad sea derivada a través del informe de DNS y el tráfico de red interna, puede utilizar la captura de filtros.

Para eliminar el tráfico en el que no se espera que la información de propiedad se pueden utilizar filtros para capturar consultas de DNS y tráfico de red interna.

Detección de Contraseñas sin Cifrar

- **Hallazgo en Wireshark**: Wireshark puede capturar y mostrar contraseñas que se transmiten en texto plano a través de protocolos inseguros como HTTP, FTP o Telnet.
- **Vulnerabilidad**: Transmitir credenciales sin cifrar expone información sensible a posibles atacantes que intercepten el tráfico de red.
- **Contramedida**: Implementar cifrado mediante el uso de protocolos seguros como HTTPS, FTPS o SSH. También se puede usar VPN para asegurar las comunicaciones a través de redes inseguras.

Captura de Tráfico DNS Inseguro

- **Hallazgo en Wireshark**: Se detecta que las consultas DNS se están realizando a través de UDP sin cifrado, lo que deja expuesta la información de navegación a posibles ataques como "DNS spoofing" o "DNS hijacking".
- **Vulnerabilidad**: Un atacante puede interceptar y modificar respuestas DNS, redirigiendo a los usuarios a sitios maliciosos.
- **Contramedida**: Implementar DNS sobre HTTPS (DoH) o DNS sobre TLS (DoT) para asegurar que las consultas DNS estén cifradas. Además, se puede utilizar DNSSEC para garantizar la autenticidad de las respuestas DNS.

4.1.12. Capturar paquetes de datos.

Para recopilar paquetes de datos, primero debe capturarlos utilizando Wireshark. Para hacer esto, capture los primeros paquetes usando el siguiente procedimiento:

1. Establecer Wireshark. Para comenzar a familiarizarse con Wireshark después de haberlo instalado exitosamente en su sistema. Finalmente, puede abrir por completo el sniffer de paquetes y observar cómo funciona. La primera vez que Wireshark se ejecuta, no resulta muy atractivo.

2. Elija Capturar y luego Interfaces del menú desplegable del menú principal. Un diálogo muestra las diferentes interfaces que se pueden emplear para capturar los paquetes de datos, así como sus respectivas direcciones IP.

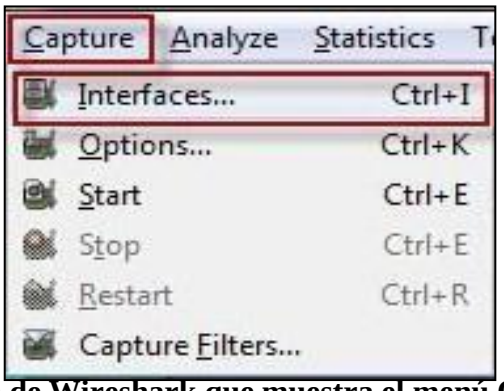


Figura 2 Imagen obtenida de Wireshark que muestra el menú Captura/Interfaz

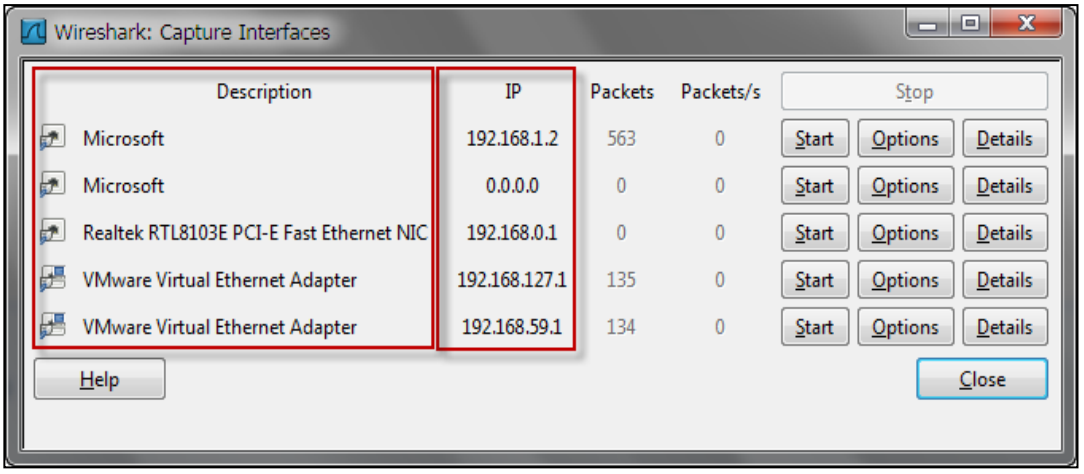


Figura 3 La imagen obtenida de Wireshark muestra las interfaces de captura junto con sus direcciones IP en pantalla

3. Como se muestra en la Figura, seleccione la interfaz que desea usar y haga clic en Inicio; alternativamente, Haga clic en un tema en la sección Lista de temas de la página de bienvenida. La ventana comenzará a llenarse de datos.

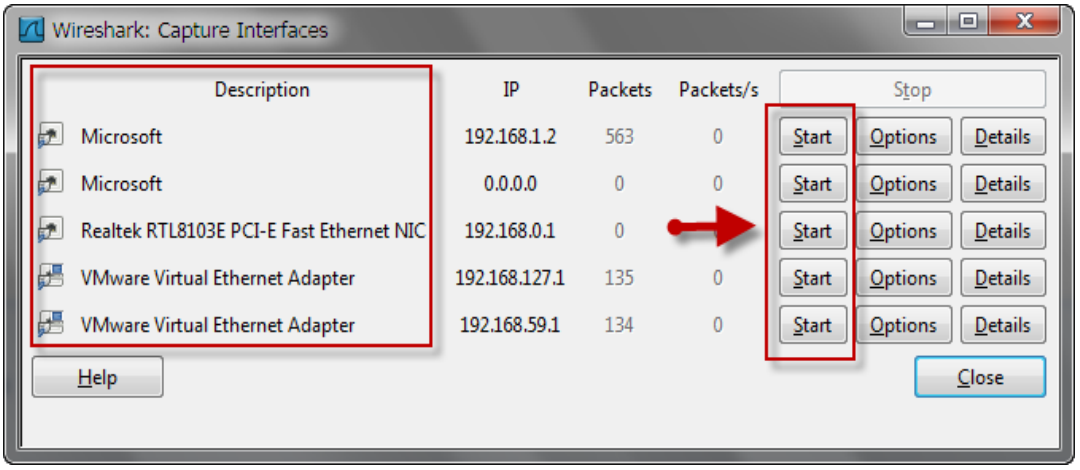


Figura 4 Imagen obtenida de Wireshark. Le permite elegir la interfaz para capturar paquetes de datos

4. Después de iniciar la captura, esperar el tiempo necesario; luego, para ver los datos, haga clic en el botón Detener captura en el menú desplegable.

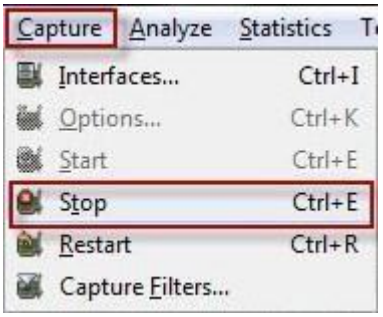


Figura 5 Imagen obtenida de Wireshark que muestra el menú Capturar/Detener captura.

La captura habrá concluido después de completar estos pasos; la ventana principal de Wireshark debería mostrar una gran cantidad de datos capturados.

4.1.13. Ventana principal de Wireshark

Figura 6 Ventana de visualización de la interfaz de red de donde se va a capturar datos

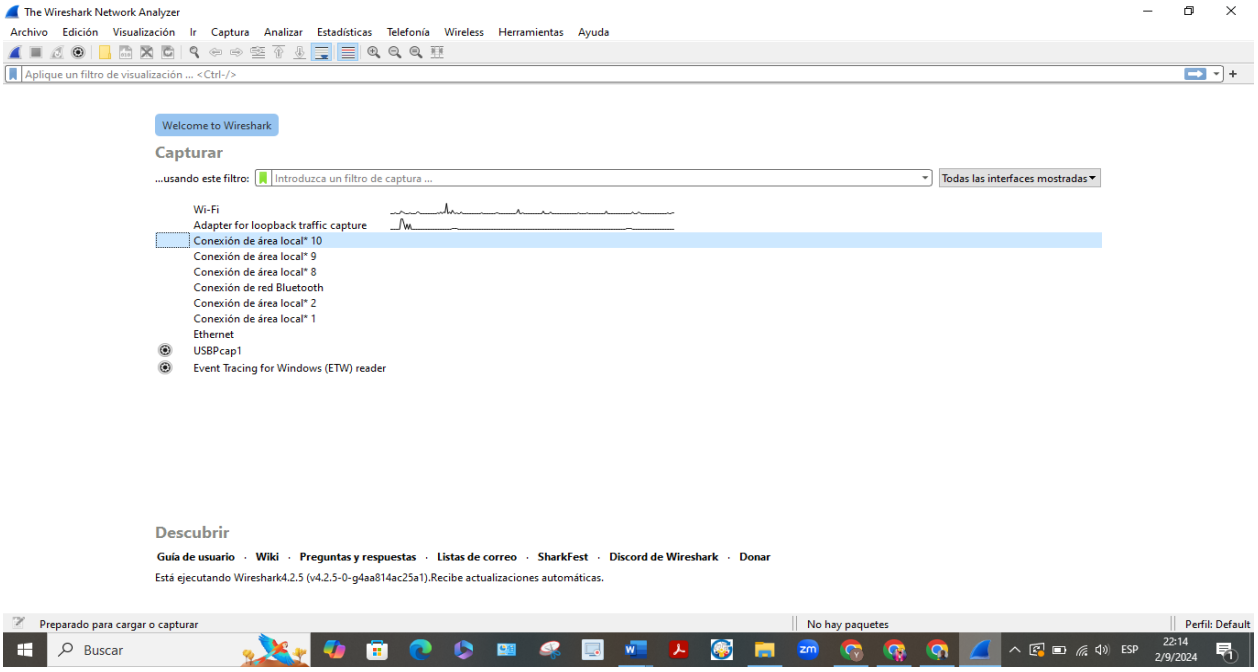
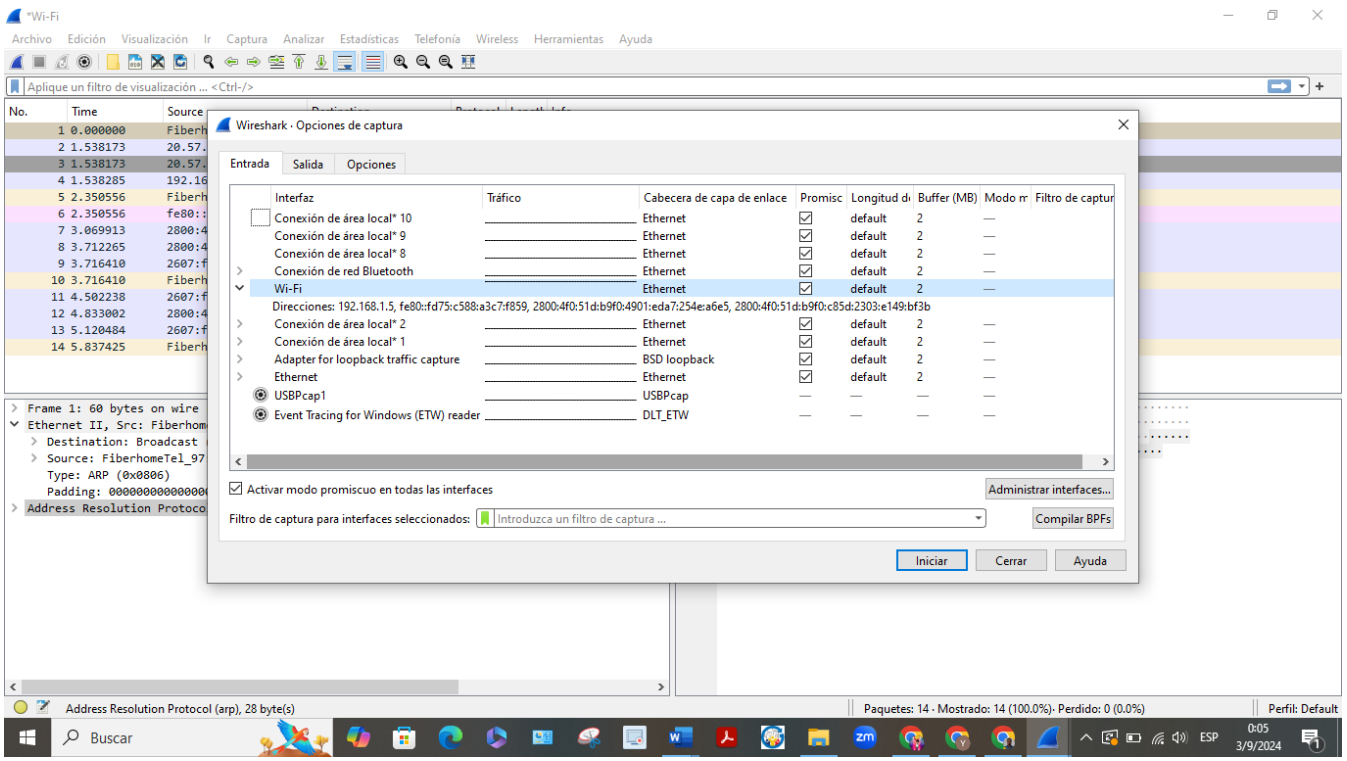


Figura 7 Ventana de captura de la interfaz de red de donde se va a capturar datos



La ventana de Wireshark. Todos los paquetes capturados se muestran aquí y sedividen en un formato más fácil de entender. Los protocolos no se separan visualmente en capas; todos los paquetes se muestran tal y como son aceptados en la red.

Figura 8 La imagen muestra la ventana principal de Wireshark en formato de tres paneles.

La ventana principal de Wireshark tiene tres paneles que dependen entre sí. Para ver los detalles de un solo paquete por separado.

4.1.13.1. Lista de paquetes Capturados

Una tabla con una lista de todos los paquetes de captura actual se encuentra en el panel superior. Son columnas que incluyen:

4.1.13.2. Número de paquete: enumera cada paquete capturado por turno.
4.1.13.3. Tiempo: tiempo aproximado para capturar el paquete,
4.1.13.4. Fuente: de qué dirección se recibió el paquete
4.1.13.5. Destino: la dirección a la que se envía el envío,
4.1.13.6. Protocolo utilizado por el paquete. Longitud del embalaje
4.1.13.7. Alguna información general se puede encontrar en el embalaje.

4.1.13.8. Detalles del paquete Seleccionado

La información sobre un paquete se presenta jerárquicamente en el panel central. Se puede ampliar y reducir esta pantalla para mostrar toda la información recopilada sobre un paquete específico.

4.1.13.9. Bytes del paquete

El más confuso panel inferior muestra un paquete en su forma cruda, sin procesar; es decir, muestra cómo aparece a medida que viaja a través de la red. Una zona de visualización que muestra la cantidad de paquetes presentes en la captura actual.

4.1.14. Configuración de Wireshark para capturar paquetes de Datos

1. La interfaz de captura se puede seleccionar en la lista desplegable; también se puede elegir la interfaz de red para configurar. Es posible determinar si la interfaz es local o remota en la lista desplegable de la izquierda.

2.- La dirección IP de la interfaz que se ha elegido se muestra en la parte inferior de esta lista desplegable de la derecha, que muestra todas las interfaces de captura disponibles.

3.- Los botones en el lado derecho de la captura brindan acceso a las configuraciones inalámbricas y remotas. La opción de tamaño del búfer, que solo está disponible en sistemas que utilizan Microsoft Windows, se encuentra debajo de ellos.

4.- La cantidad de datos puede definir la captura de paquetes para que se almacene en el búfer antes de escribir en el disco.

5.- El modo mixto, siempre habilitado de forma predeterminada, captura paquetes de forma probado en formato pcap-ng y limitado el tamaño de cada paquete de captura por byte, son posibles mediante las tres casillas de verificación situadas en el lado izquierdo

del cuadro de diálogo.

6.- Puede establecer un filtro de captura para capturar solo lo que se ha especificado en el filtro de búsqueda de paquetes mediante la opción Filtro de captura.

7.- En lugar de capturar los paquetes y luego guardarlos, la sección de captura de archivos permite almacenar automáticamente los paquetes en un archivo. El manejo de la cantidad de paquetes que se guardan es mucho más flexible.

Para controlar la cantidad de archivos que crea, puede incluso guardar un solo archivo o un conjunto de archivos. Para habilitar esta opción, ingrese el nombre del archivo y la ruta completa en el cuadro de texto del archivo. La agregación de archivos puede resultar útil al grabar largos períodos de tiempo o al grabar mucho tráfico.

8.- Puede controlar la cantidad de paquetes que se muestran cómo están siendo capturados en la sección Opciones de visualización. Las actualizaciones de la lista de

Se explican por sí mismos los paquetes en la opción de tiempo real y se pueden combinar con función de desplazamiento automático en modo de disparo en vivo. La pantalla muestra todos los paquetes capturados, con las capturas más recientes, cuando ambas opciones están activadas.

9.- Mediante el cumplimiento de determinados factores desencadenantes, Wireshark puede automáticamente detener las capturas. El tamaño de los paquetes, el número de paquetes y los intervalos de tiempo, como segundos, minutos o días, pueden desencadenarlos.

10.- Se puede activar automáticamente la resolución de nombres de MAC capa 2, red nivel 3 y transporte nivel 4 para su captura en la sección opciones de resolución de nombres.

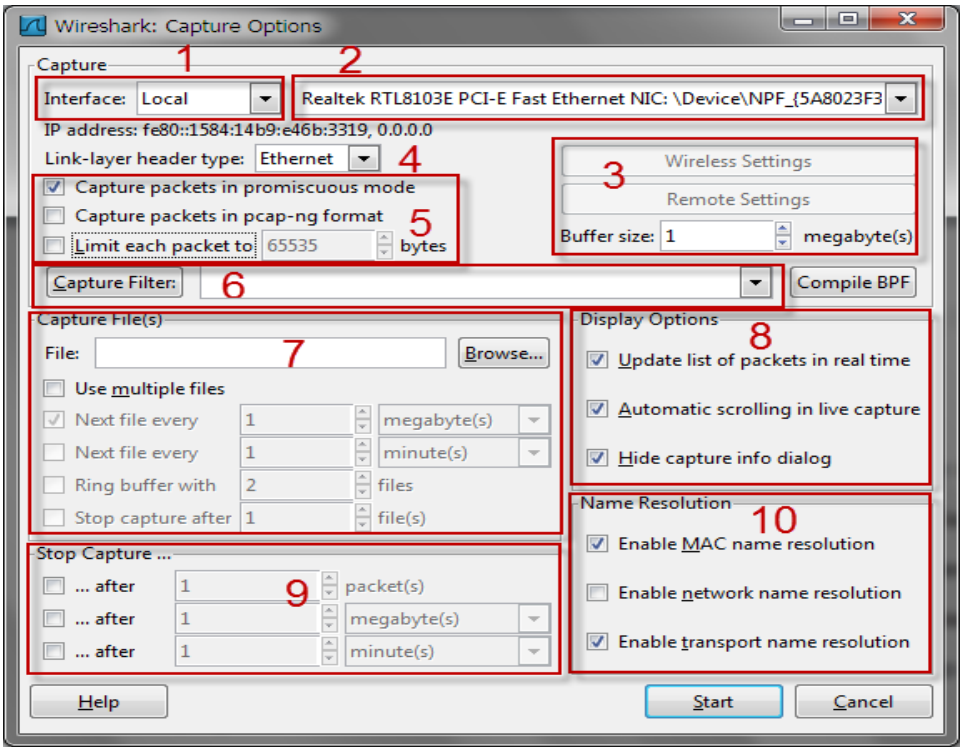


Figura 9 de configuración de Wireshark para capturar paquetes de datos.

4.1.15. Usando colores en paquetes de datos con Wireshark

Cada paquete tiene un color específico por una razón. La paleta de colores representa el protocolo del paquete. Por ejemplo, todo el tráfico HTTP es verde y todo el tráfico UDP es azul. El código de colores facilita la diferenciación rápida entre los distintos protocolos, por lo que no es necesario leer el campo de protocolo en la tabla de lista de paquetes para cada paquete específico.

La navegación a través de los archivos de captura de gran tamaño se acelera significativamente de esta manera hay una razón por la cual cada paquete se muestra en un color específico. Estos colores indica el protocolo del paquete. Por ejemplo, todo el tráfico UDP es azul y todo el tráfico HTTP es verde.

La ventana de coloración de reglas de Wireshark facilita ver los colores asignados a cada protocolo. Para abrir esta ventana, haga clic en "Reglas de coloreado" y seleccione "Ver" en el menú desplegable principal.

Figura 10 Imagen captada de Wireshark que muestra el menú Ver/Reglas de color.

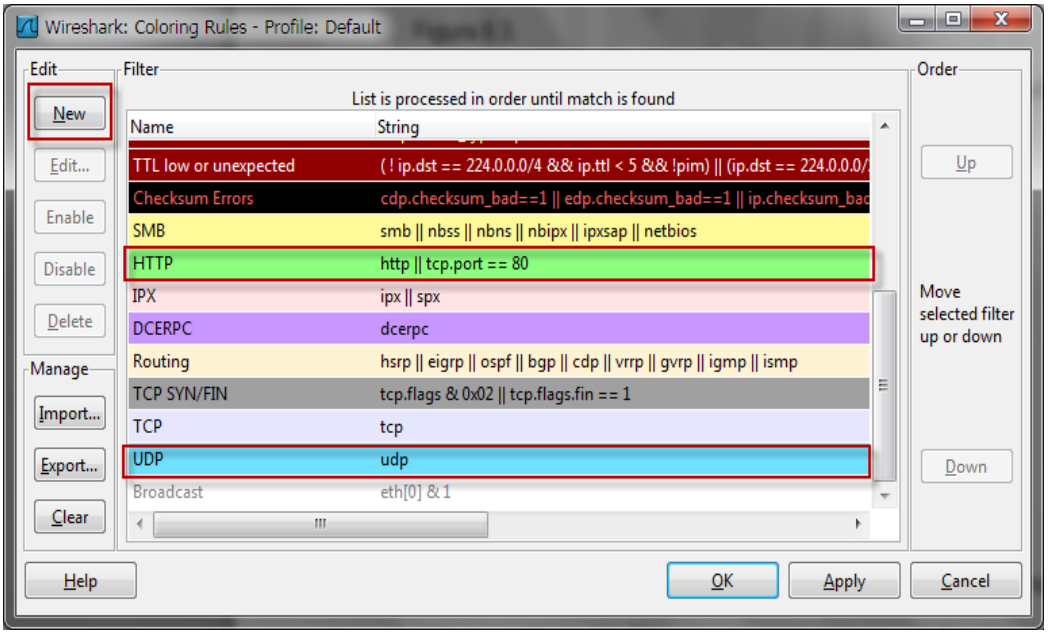


Figura 11 La ventana Rule Coloring en Wireshark le permite ver, cambiar y crear nuevos colores de paquetes.

4.1.16. Filtrado de Paquetes de Datos

Para su análisis, los filtros le permiten especificar qué paquetes tenemos disponibles. Los criterios para la inclusión o exclusión de paquetes se definen mediante una expresión conocida como filtro.

El proceso de captura de paquetes actualmente emplea filtros de captura. El rendimiento es una de las principales razones para utilizar un filtro de captura.

4.1.16.1. Filtrado durante la captura

Se usa cuando se muestran los paquetes y se usa en la captura de paquetes.

Cuando los paquetes se capturan, se utilizan los filtros de captura; solo se capturan los paquetes que están especificados para la inclusión/exclusión en la expresión dada.

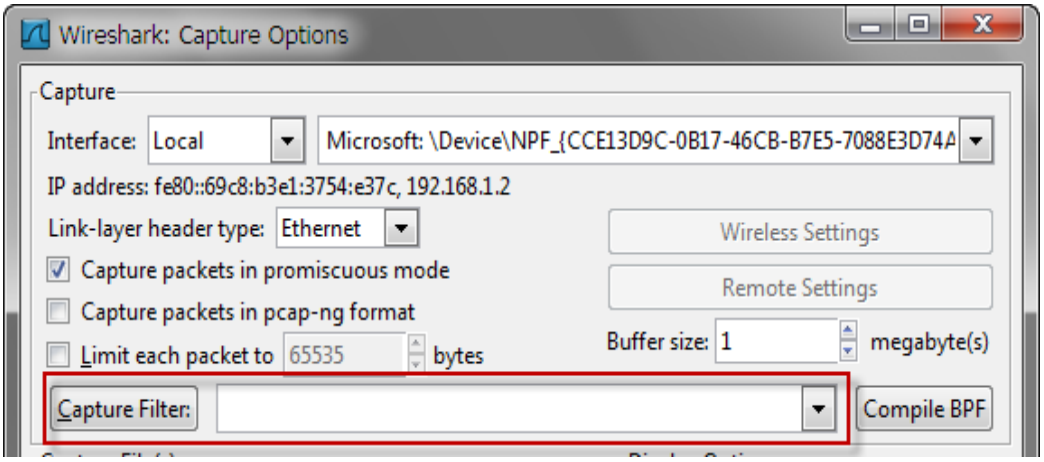


Figura 12 Ventana de Wireshark para configurar los filtros de captura de paquetes

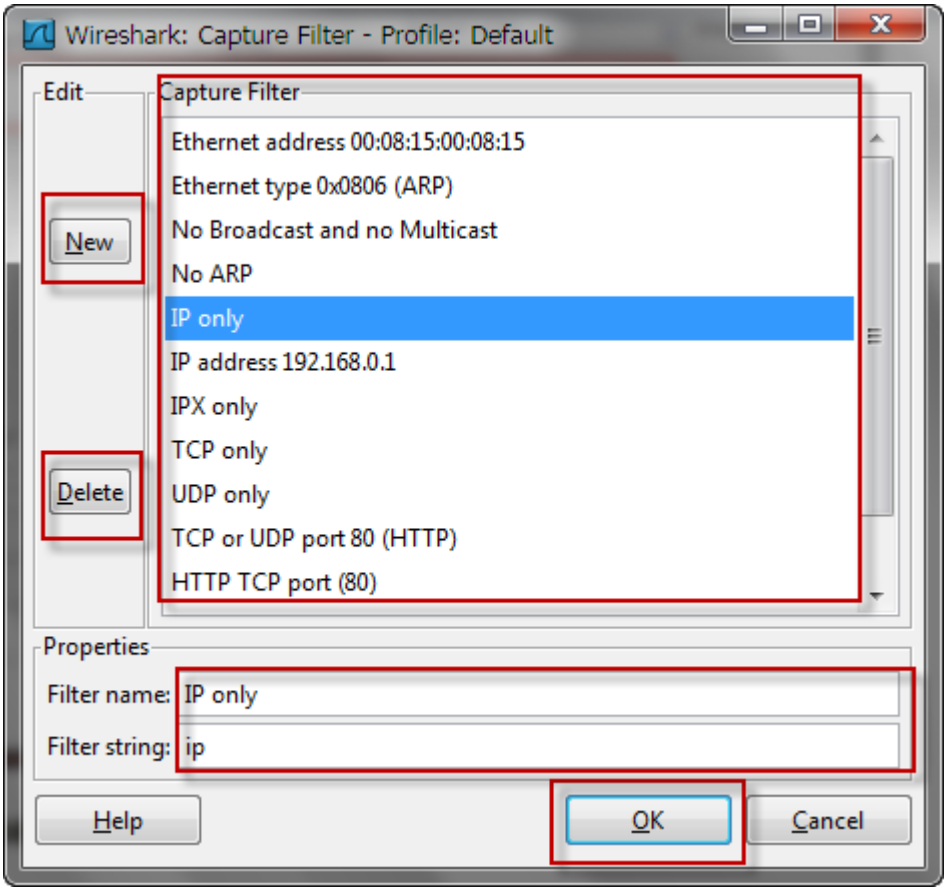


Figura 13 Ventana de Wireshark que permite crear o borrar nuevos filtros para captura de paquetes

4.1.16.2. Filtrar paquetes mientras navega

El conjunto utiliza un filtro de pantalla actual de paquetes capturados para mostrar los paquetes que desea u ocultar los paquetes no deseados según la expresión especificada.

Los filtros de pantalla le permiten enfocarse en los paquetes que tiene interés en ocultar y en los que no tiene interés en este momento. Le permiten elegir los paquetes según:

4.1.16.2.1. Protocolo

4.1.16.2.2. La disposición de un campo

4.1.16.2.3. valores de campos

4.1.16.2.4. Un balance entre los campos

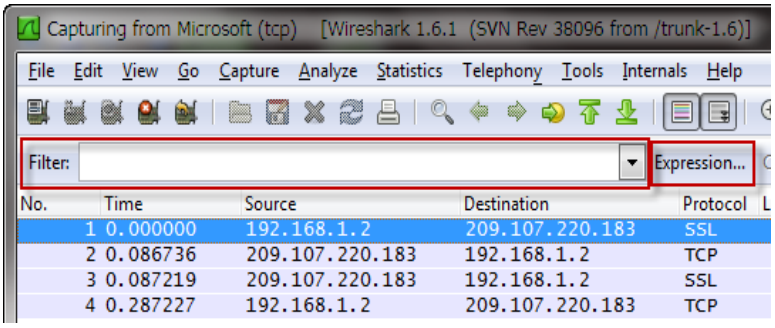


Figura 14 La imagen descargada de Wireshark muestra filtros de captura de paquetes mientras navega.

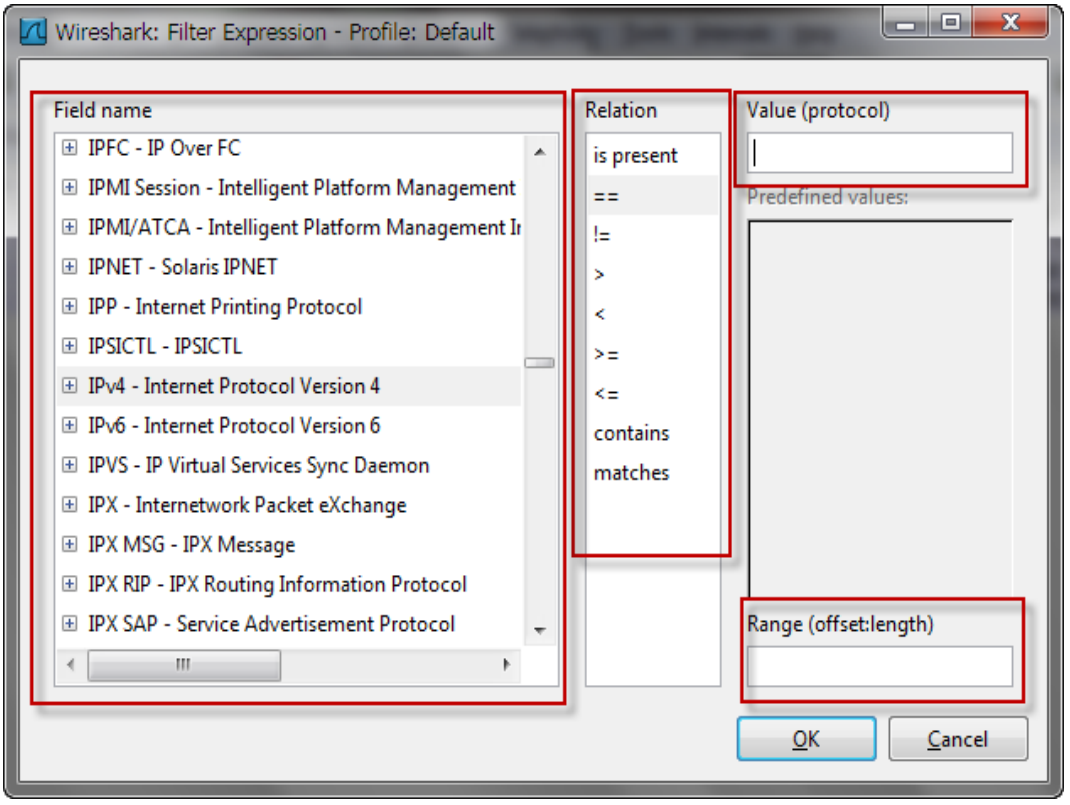


Figura 15 Imagen descargada de Wireshark que muestra la ventana de configuración del filtro con factor de captura.

4.1.17. Guardar Paquete de Datos

Para que otras herramientas puedan leer los datos de captura, Wireshark puede almacenar el paquete de datos en el formato de archivo de algún otro analizador de protocolos, así como en su formato nativo de archivo libpcap.

Los formatos de archivo tienen distintas precisiones en cuanto a fecha y hora. Wireshark puede almacenar los siguientes formatos de archivo tienen extensiones:

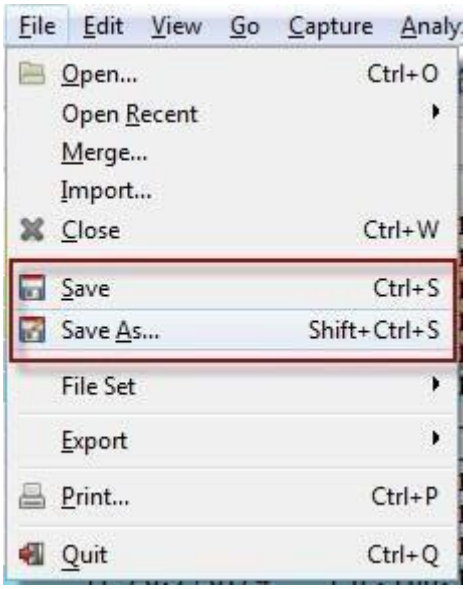


Figura 16. Imagen descargada de Wireshark que muestra los menús Archivo/Guardar y Guardar como para paquetes de datos capturados.

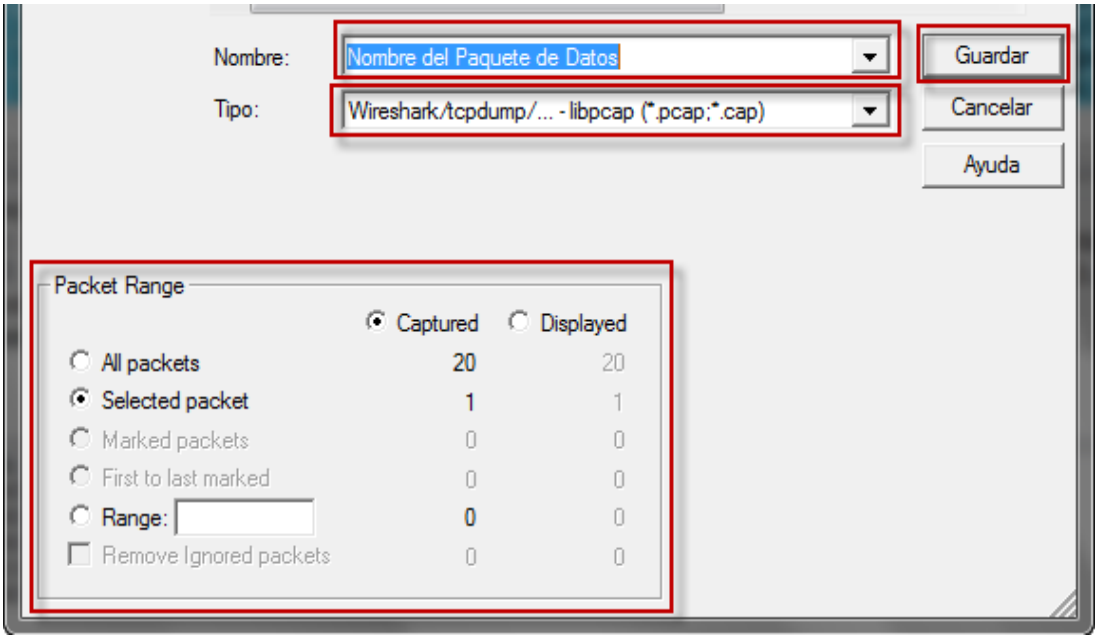


Figura 17 La imagen descargada de Wireshark muestra una ventana que guarda paquetes de datos convarios parámetros.

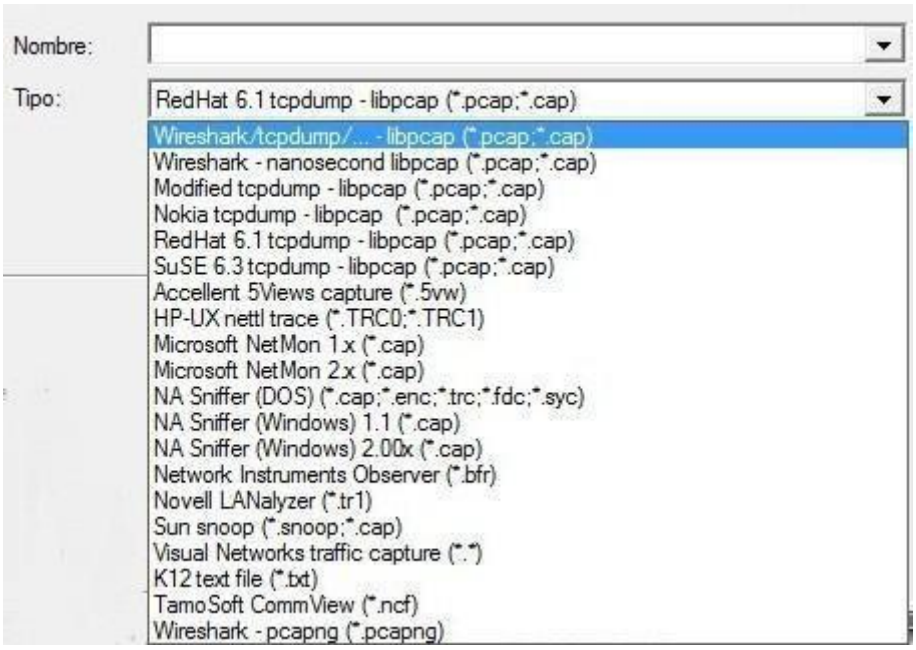


Figura 18. La imagen descargada de Wireshark muestra todas las extensiones disponibles paraguardar archivos de captura.

4.1.18. Exportando a otros Formatos los Paquetes de Datos

Para que puedan ser visualizados en otros medios de comunicación o importados a otras herramientas de análisis de paquetes, Wireshark permite exportar los paquetes de datos capturados en una variedad de formatos.

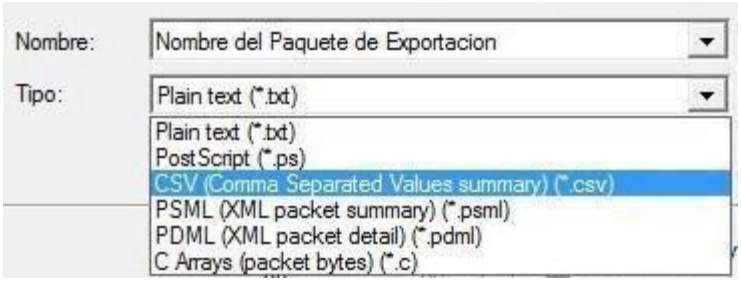


Figura 19. Imagen descargada de Wireshark que muestra todas las extensiones disponibles para el archivo de salida.

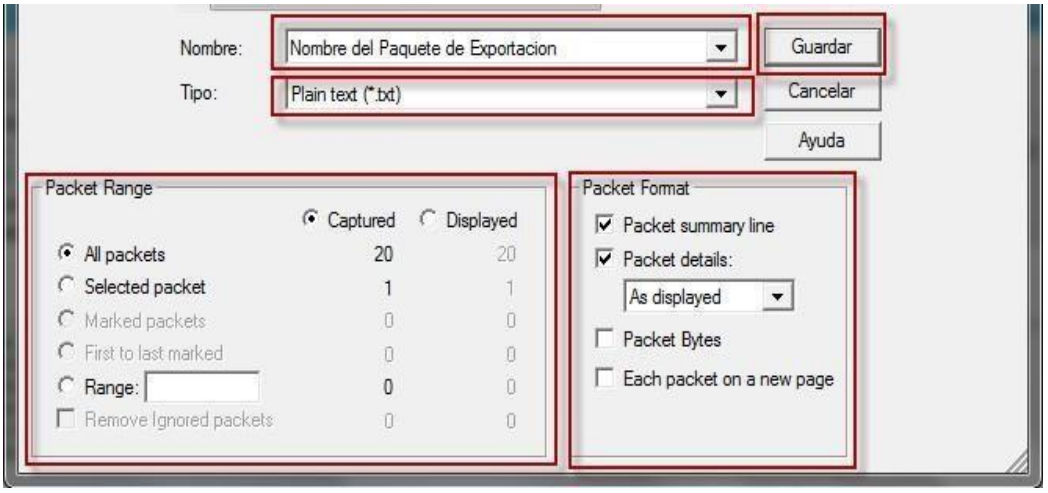


Figura 20. Imagen obtenida de Wireshark que muestra las extensiones disponibles para el archivo de exportación que seexportar a otro formato.

Para exportar la captura de paquetes, haga clic en el archivo de exportación y luego en elformato del archivo exportado. Un cuadro de diálogo Guardar se mostraría, que contienelas opciones asociadas con ese formato particular.

4.2. Analizar los paquetes de datos recibidos de la red para su argumentación yregistro.

Normalmente, se realizan varias capturas en diferentes momentos y los paquetes se almacenan y examinan simultáneamente.

Por lo tanto, Wireshark permite guardar archivos de captura para su posterior análisis.

Se pueden combinar varios archivos de captura.

4.2.2. Análisis de Paquetes

El análisis de paquetes, también conocido como detección de paquetes o análisis de protocolo, es el proceso de interpretación y captura de datos en tiempo real que fluyen a través de una red con el fin de comprender mejor lo que está sucediendo en la red.

Un analizador de paquetes se usa con frecuencia para realizar el análisis de paquetes; en este caso, Wireshark es una herramienta que captura datos en bruto de la red que atraviesa el cable.

La siguiente puede ser una ayuda para el análisis de paquetes:

El rastreo de paquetes puede ayudar en los siguientes casos:

- Conozca las características de la red.
- Formación en línea
- Identifique quién o qué está utilizando su ancho de banda disponible
- Determinar el uso de la red durante las horas pico
- Identificar posibles ataques o actividades maliciosas

Para comprender mejor los problemas de la red, todos los problemas de la red se muestran en un nivel de paquete. Solo los datos encriptados son verdaderos secretos en este nivel de paquetes. Cuanto más podamos llevar a cabo el análisis a nivel de paquetes, más podemos dirigir la red y solucionar sus problemas.

Porque capturar los paquetes de datos cuando la red no contiene ninguna amenaza. Para realizar el análisis de paquetes, no hay ningún problema. La mayoría de los analistas de paquetes, en realidad, dedican más tiempo a analizar el tráfico sin problemas que al tráfico con un problema.

Para detectar anomalías en la actividad diaria de la red, es necesario comprender la actividad normal.

Todos los problemas de la red se identifican a nivel de paquete para comprender mejor los problemas de la red. No hay verdaderos secretos a este nivel de paquete, sólo datos cifrados. Cuanto más podamos analizar a nivel de paquete, mejor podremos monitorear y solucionar problemas de la red.

4.2.3. Fusionar Archivos de Captura

La habilidad de combinar múltiples archivos de captura es necesaria para ciertos tipos de análisis. Este es un método común al comparar dos flujos de datos o combinar flujos del mismo tráfico registrado por separado. Para fusionar archivos de captura, abra uno de los archivos de captura. que desea combinar. Para abrir el cuadro de diálogo de fusión con la captura de archivos, seleccione Archivo - Combinar. Seleccione el archivo que desea fusionar en el archivo que ya está abierto y luego elija el método para fusionar los archivos.

Figura 21. Imagen obtenida de Wireshark muestra el menú desplegable Archivo/Combinar archivos capturados.

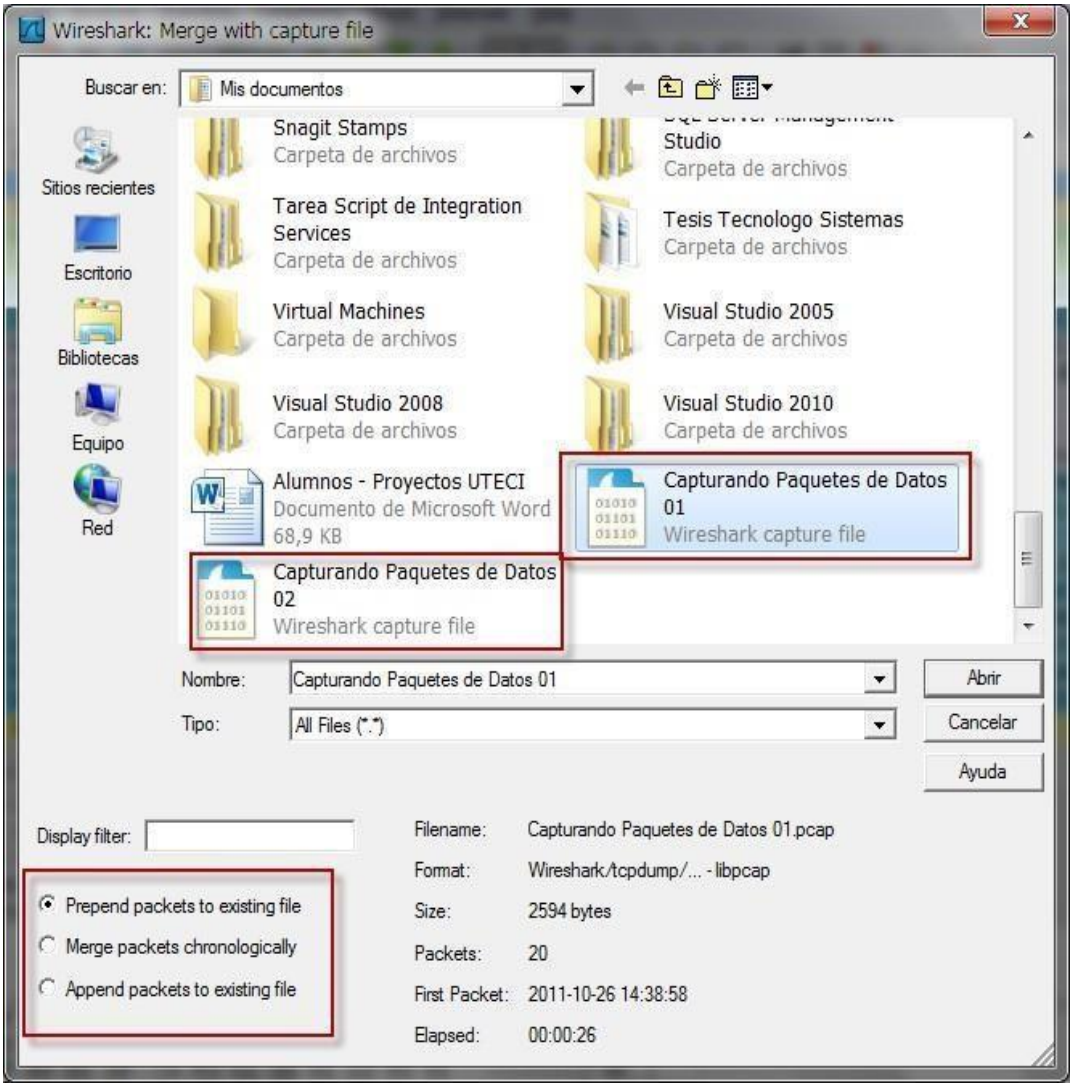


Figura 22. El cuadro de diálogo Fusionar archivos de captura le permite combinar dos archivos de captura.

4.2.4. Imprimir Paquetes Capturados

Es posible que se requiera imprimir los datos capturados, a pesar de que la mayor parte del análisis se realizará en la pantalla del ordenador. Se puede hacer referencia

rápidamente a su contenido mientras se analizan otros paquetes al imprimirlos.

Además, Wireshark le permite imprimir paquetes capturados en archivos PDF; Esto es especialmente útil para generar informes.

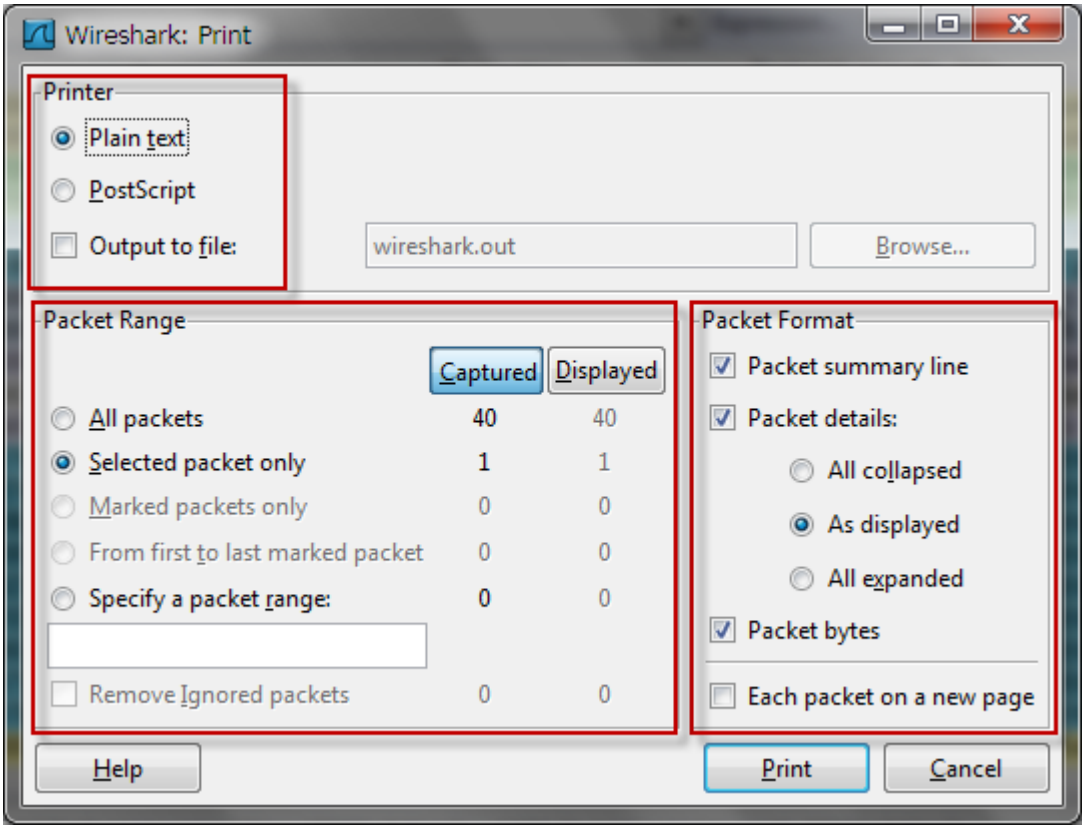


Figura 23. La imagen capturada de Wireshark muestra la ventana de configuración de impresión de archivos.

Para imprimir paquetes capturados, seleccione el menú principal "Imprimir archivo" en el cuadro de diálogo de impresión.

Aparece el cuadro de diálogo de impresión.

4.2.5. Búsqueda de Paquetes de Datos Capturados

Situaciones en las que se han capturado muchos paquetes. Para explorar a través de paquetes de manera más efectiva, el número de estos paquetes se eleva a miles y hasta millones. Por medio de Wireshark, es posible localizar y marcar los paquetes que cumplan con ciertos requisitos. Además, puede imprimir los paquetes para una referencia sencilla.

El cuadro de diálogo Búsqueda de paquetes de Wireshark le permite buscar paquetes que coincidan con ciertos criterios. Para hacer esto, presione CTRL-F para abrirlo.

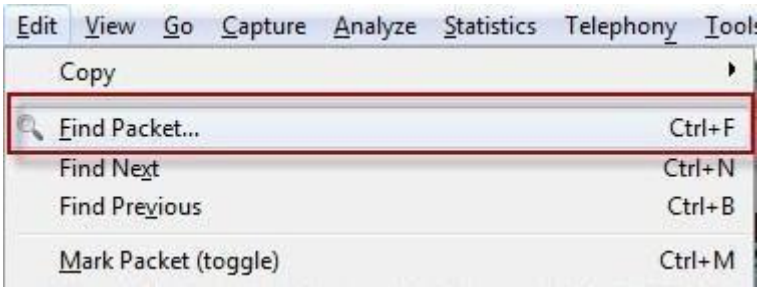


Figura 24. Obtenido de Wireshark: menú Archivo/Buscar paquetes capturados

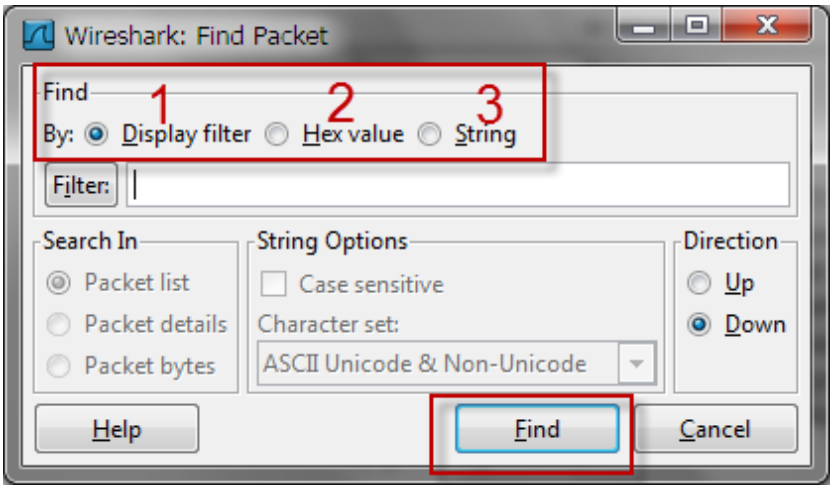
Tres opciones para localizar los paquetes están disponibles en este cuadro de diálogo de búsqueda:

1. Se puede utilizar la opción de filtro de pantalla para crear un filtro que busca únicamente los paquetes que cumplen con esa expresión.

2. La opción de búsqueda hexadecimal busca paquetes con valores hexadecimales que contengan bytes separados por dos puntos del valor especificado

3.- Para buscar cadenas de paquetes, debe especificarse el texto que contiene una cadena.

Figura 25. Busque paquetes en Wireshark según criterios específicos



4.2.6. Marcado de paquetes

Se pueden marcar solamente los paquetes que cumplan con los criterios de búsqueda una vez que se hayan encontrado. Es posible que desee marcar los paquetes, por ejemplo, para poder guardarlos por separado o para encontrarlos rápidamente en función de la coloración.

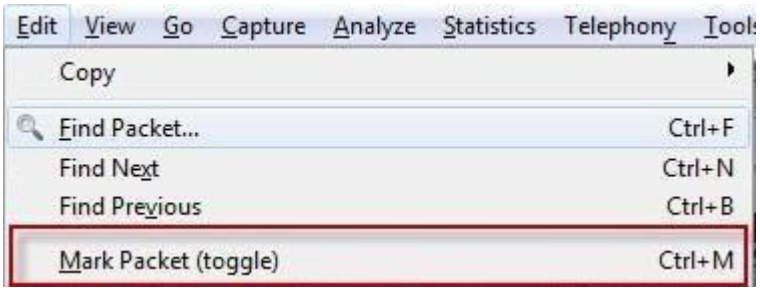


Figura 26. Obtenido de Wireshark: Muestra el menú Editar/Seleccionar paquete.

Es posible resolver solo los paquetes marcados guardando las capturas de los paquetes; los paquetes marcados se distinguen por un fondo negro y un texto blanco.

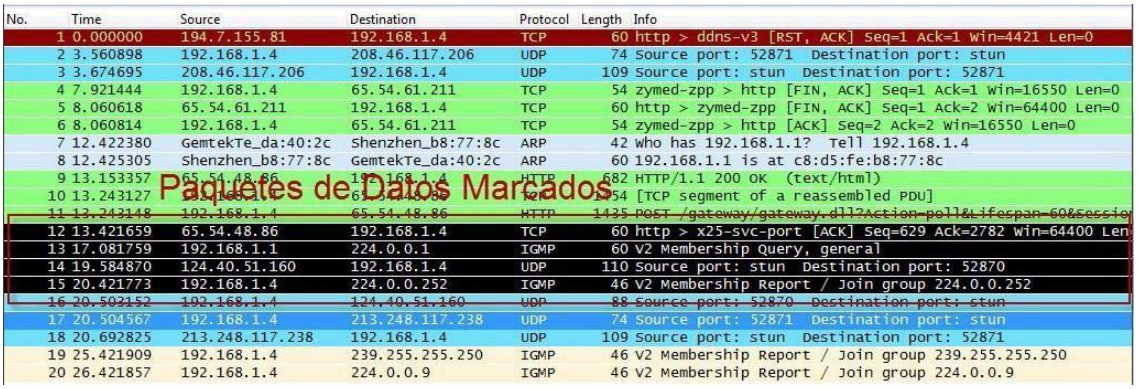


Figura 27. Imagen descargada de Wireshark que muestra una lista de paquetes seleccionados.

Ejecute clic derecho en el panel Lista de paquetes y seleccione Inspeccionar en el menú emergente; también puede hacer clic en un paquete en el panel Lista de paquetes y presionar CTRL-M para marcar un paquete. Salir con CTRL-M de nuevo para desmarcar un paquete y cambiar esto. Puede etiquetar tantos paquetes como quiera.

Que quiera en una captura. Entre los paquetes marcados, pulse SHIFT-CTRL-N y SHIFT-CTRL-B para saltar hacia delante y hacia atrás, respectivamente.

4.2.7. Gráficos

En el análisis, los gráficos son cruciales y son una de las mejores formas de obtener una comprensión general de un conjunto de datos. Para facilitar la comprensión de la captura de datos, Wireshark ofrece una variedad de características gráficas distintas.

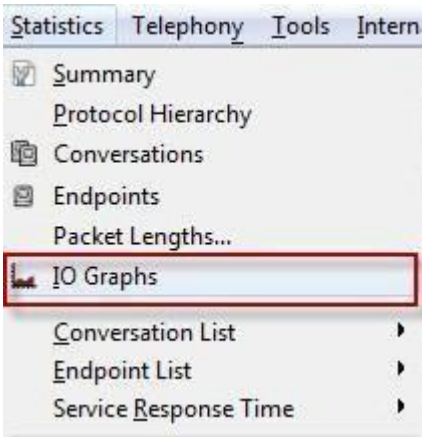


Figura 28. Obtenido de Wireshark: Mostrar menú gráfico/estadísticas de E/S.

Puede visualizar el rendimiento de la red en la ventana del gráfico de Wireshark. Mediante gráficos, puede encontrar picos y caídas en el rendimiento de datos, encontrar latencias en protocolos de inicio individuales y comparar flujos de datos simultáneos.

El flujo de datos a lo largo del archivo de captura se muestra en la ventana de gráficos.

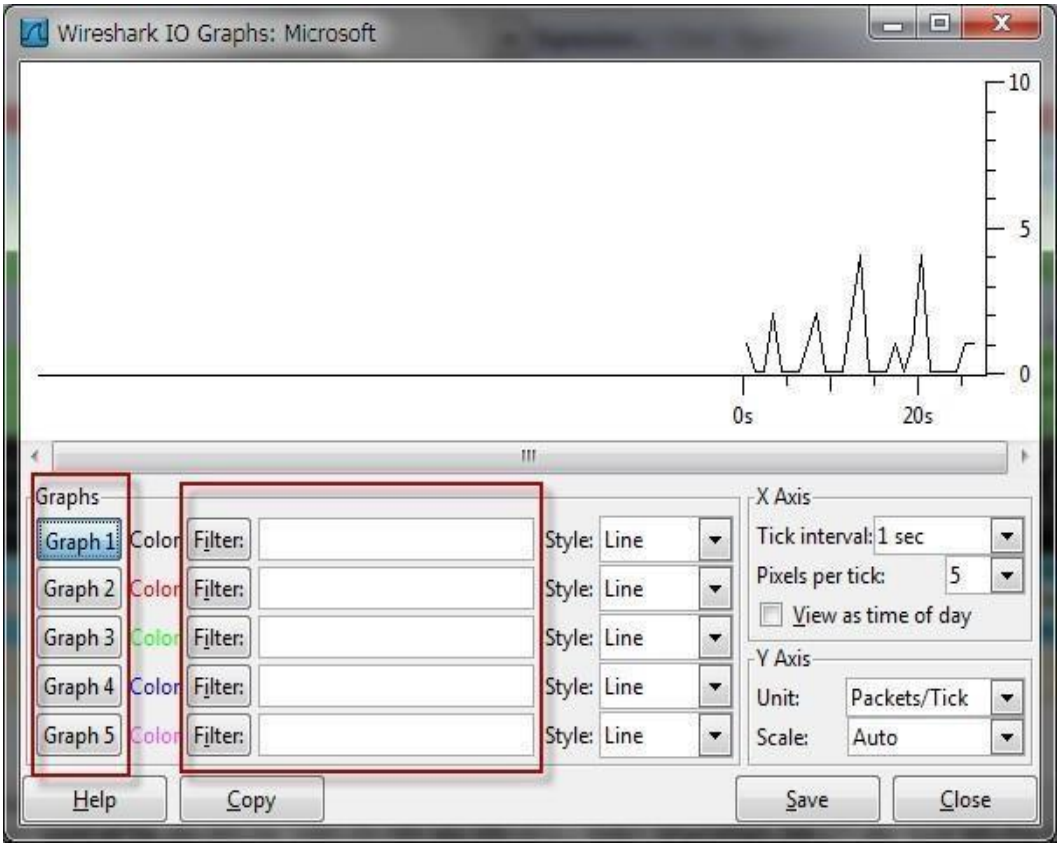


Figura 29: tomada de Wireshark, muestra los gráficos de E/S.

En la parte inferior de esta ventana se encuentran las opciones configurables. Utilizando la misma sintaxis como una pantalla de filtro de captura y El filtro de color de la pantalla facilita distinguir las tendencias de rendimiento entre los distintos tipos de protocolos, hasta cinco gráficos con sus filtros distintos.

4.2.8. Estadísticas de jerarquía de protocolos

Para una mejor comprensión desde este escenario, podemos ver los protocolos de capa de aplicación utilizados en las conexiones TCP y UDP. en la ventana de estadísticas de jerarquía de protocolos. Para acceder a la ventana de jerarquía de protocolos, haga clic en el menú estadísticas; se muestran los porcentajes de completado y tamaño del paquete en bytes.

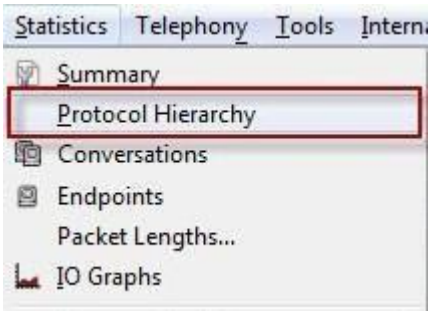


Figura 30. obtenida de Wireshark que muestra el menú estadísticas/Jerarquías de protocolos

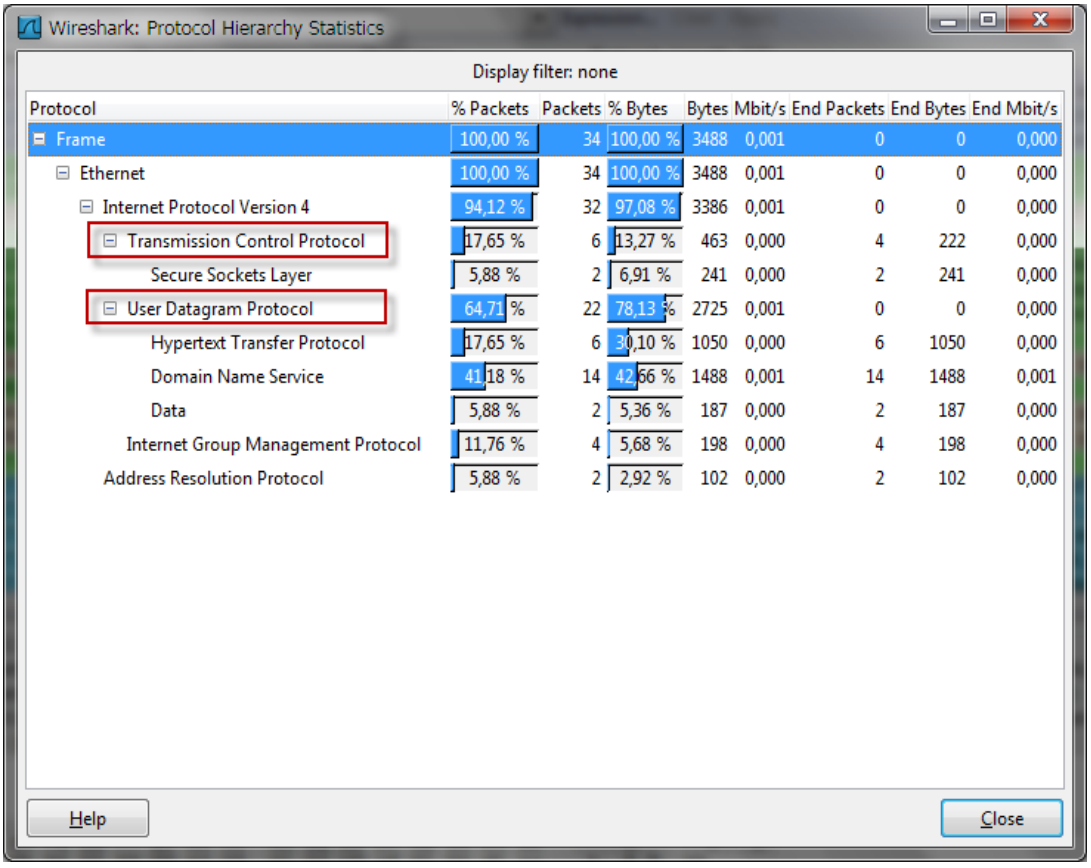


Figura 31: la imagen de Estadísticas de jerarquía de protocolos muestra la distribución de los protocolos de captura depaquetes.

5. CAPITULO V - CONCLUSION Y RECOMENDACION

5.1.Conclusión

Wireshark es la herramienta más adecuada para el control tecnológico detallado del tráfico de red debido a su capacidad para realizar análisis profundos y en tiempo real. Sin embargo, en un entorno de red empresarial, suele utilizarse junto a otras herramientas de monitoreo continuo para obtener una visión completa de la red.

También es importante señalar que la funcionalidad utilizada en este informe es solo una pequeña parte del potencial total que nos ofrece Wireshark, el objetivo principal de esta funcionalidad es servir de guía a cualquier administrador para detectar, analizar o resolver una necesidad. problema de red. anomalía. Finaliza este artículo sobre el análisis y captura de paquetes de datos en la red utilizando Wireshark, la importancia de esta herramienta de software, algunas de sus características más funcionales, usabilidad y compatibilidad de sistemas operativos y protocolos probados. que Wireshark funciona. Los administradoreso usuarios de red pueden utilizar este modelo para realizar análisis de red siguiendo el proceso de instalación e implementación. Todos los problemas de la red son causados por paquetes de datos, por lo que es importante analizar y capturar paquetes de datos utilizando herramientas de software que se adapten a las necesidades de los administradores de red, así como a su conocimiento de la estructura general que conforma la red. toda la parte lógica es software y la parte física es hardware.

5.1.2. Falla encontrada en la red de la empresa ELECTROCONSTRU S.A.

- **Encuentro en Wireshark**: Se detecto que las consultas DNS se están realizando a través de UDP sin cifrado, lo que deja expuesta la información de navegación a posibles ataques como "DNS spoofing" o "DNS hijacking".

Solución Propuesta:

1. **Habilitar DNS sobre HTTPS (DoH) o DNS sobre TLS (DoT)**:
    - **DNS sobre HTTPS (DoH)** cifra las consultas DNS utilizando el protocolo HTTPS, asegurando que las solicitudes de DNS no puedan ser interceptadas ni manipuladas.
    - **DNS sobre TLS (DoT)** cifra las consultas DNS utilizando el protocolo TLS,

proporcionando una capa de seguridad adicional para el tráfico DNS.

2. **Configurar el Cliente DNS**:

Actualiza la configuración del servidor DNS en los dispositivos y servidores para que utilicen un proveedor que soporte DoH o DoT. Ejemplos de servicios DNS seguros son:

- **Google Public DNS**: 8.8.8.8 (IPv4) y 2001:4860:4860::8888 (IPv6) con soporte para DoH/DoT.
- **Cloudflare DNS**: 1.1.1.1 (IPv4) y 2606:4700:4700::1111 (IPv6), que soporta DoH y DoT.

3. **Configurar Navegadores y Sistemas Operativos**:

- Muchos navegadores modernos como Firefox y Chrome soportan DoH. Habilita esta opción desde las configuraciones avanzadas del navegador.
- Configura tu sistema operativo o red local para forzar el uso de DoT si es más apropiado.

Pasos para Configurar DoH en Firefox:

1. Abre Firefox y ve a Opciones > General > Configuración de Red.
2. Activa la opción "Enable DNS over HTTPS".
3. Elige un proveedor (puedes usar Cloudflare u otro).

Beneficios:

- Las consultas DNS estarán cifradas, protegiendo la información de navegación.
- Evitarás ataques como DNS Spoofing o DNS Hijacking, ya que los atacantes no podrán interceptar ni modificar las respuestas DNS.
- Es una solución relativamente simple de implementar y no requiere cambios drásticos en la infraestructura.

Esta solución proporciona una capa de seguridad adicional sin necesidad de realizar cambios profundos en la red, y mejora considerablemente la privacidad y seguridad de las consultas DNS.

5.2.Recomendación

Le recomendamos que realice un análisis de tráfico, también conocido como análisis de paquetes, de forma continua en lugar de esperar a que ocurra un problema antes de tomar medidas. Esto requerirá mucho tiempo para detectar errores, así como costes económicos que provocarán pérdidas a la empresa. Entonces, es recomendable tener información básica de la red para saber cómo se comporta la red en circunstancias normales, para poder compararla con futuros análisis de la red, lo que ayudará a detectar rápidamente anomalías y poder contrarrestar esta amenaza. Aunque la herramienta Wireshark se utiliza principalmente para analizar y recopilar paquetes de datos en una red, existen muchas herramientas adicionales que funcionan en combinación y serán muy útiles para realizar análisis de paquetes, ya sea para solucionar problemas o depurar problemas generales, de red lenta o de seguridad. problemas de red inalámbrica. Recomiendo algunas herramientas útiles para detectar paquetes y otros recursos de capacitación para detectar paquetes. Recomiendo usar Wireshark, aunque existen varias herramientas que no son de Wireshark y que son muy útiles para analizar y capturar paquetes. A continuación, se muestran algunos nombres de herramientas que resultan útiles. Considerado por muchos como una herramienta de análisis y captura de paquetes, tcpdump está completamente basado en texto.

Windump es simplemente una distribución tcpdum preconstruida para Windows.

http://www.tcpdump.org/.http://www.winpcap.org/windump/.CloudSharkCloudShark, desarrollado por QA Café, es un recurso que permite compartir paquetes capturados con otros usuarios. CloudShark es una web que muestra archivos de captura web en su navegador. Puede capturar, descargar archivos y enviar enlaces a sus colegas para realizar análisis colaborativos.

Bibliografía Y Web grafía

Bibliografía

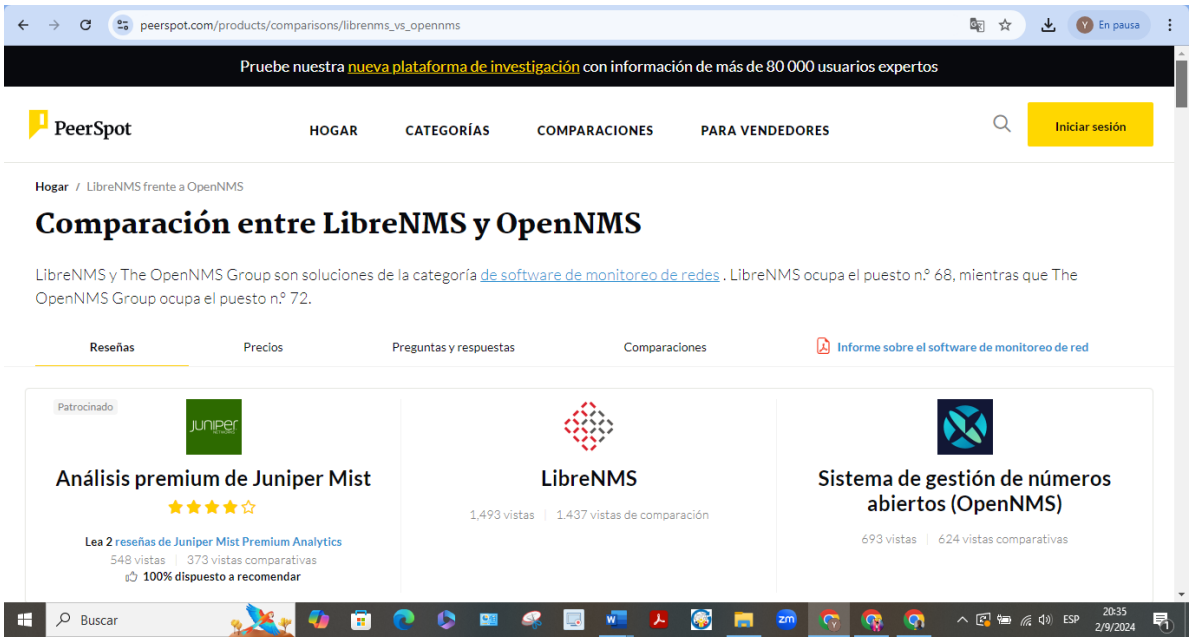
Problema principal: https://geekflare.com/es/best-o pen-source-monitoring-software/

https://www.peerspot.com/landing/category-report-network-monitoring-software

https://itsoftware.com.co/content/cacti-sistema-recoleccion-datos-graficas/

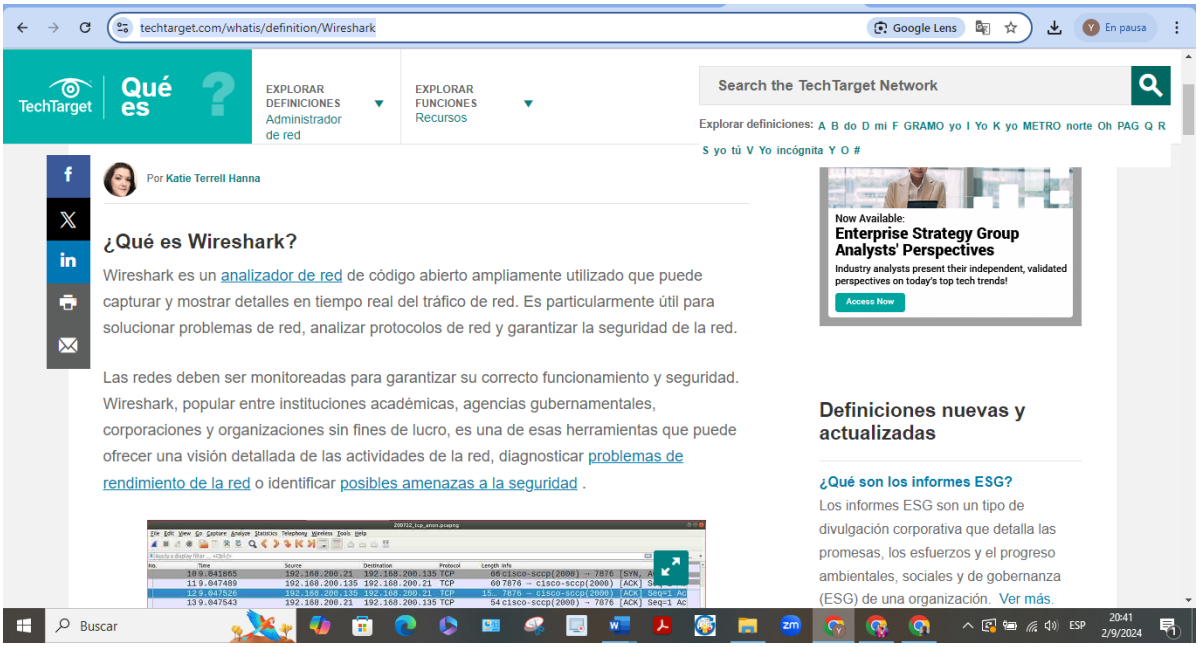
https://www.techtarget.com/whatis/definition/Wireshark

Web grafía



https://www.peerspot.com/landing/category-report-network-monitoring-software

https://itsoftware.com.co/content/cacti-sistema-recoleccion-datos-graficas/

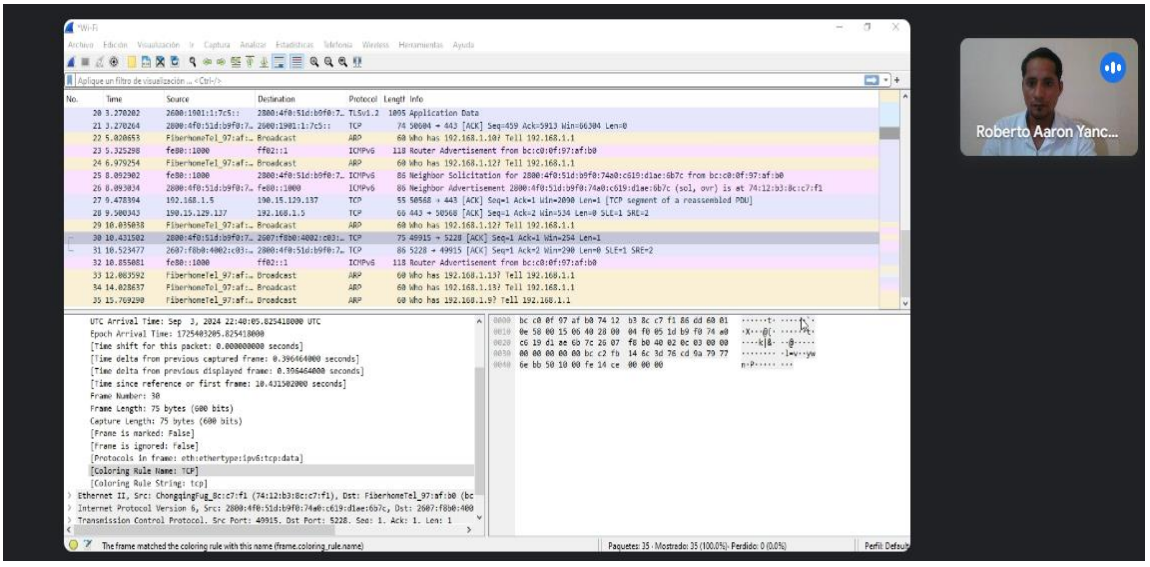


https://www.techtarget.com/whatis/definition/Wireshark

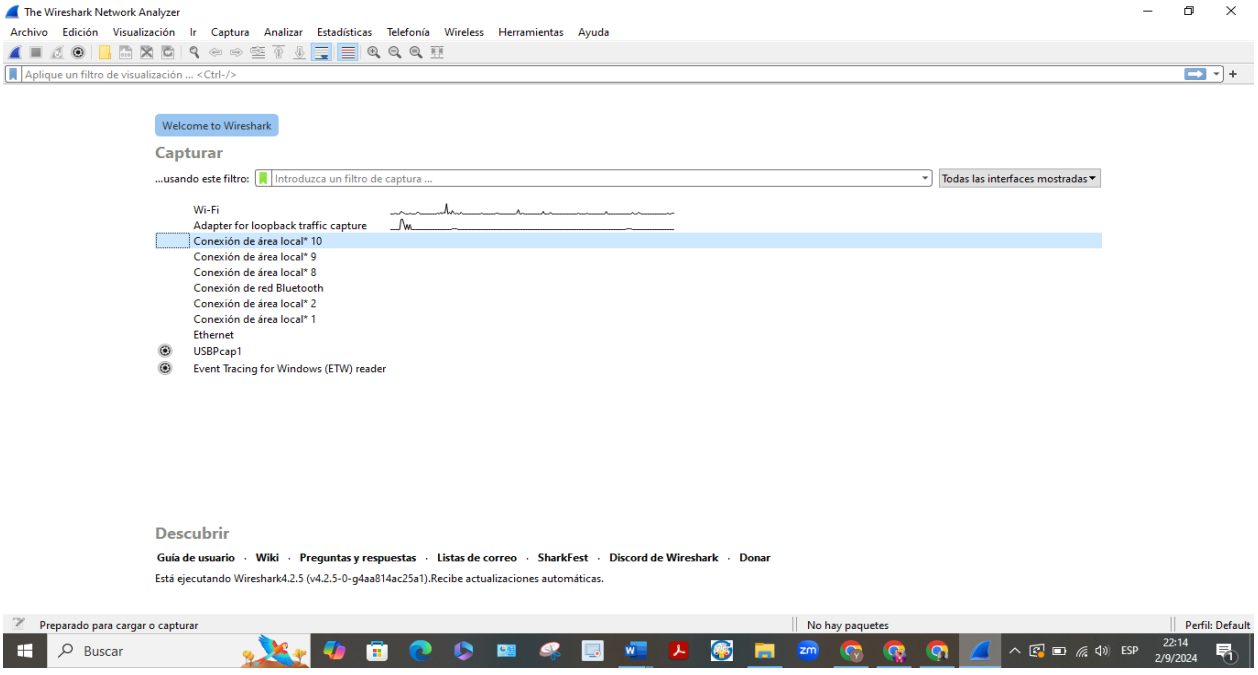
LISTA DE ANEXOS

Anexo 1. Ejecutación de wireshark

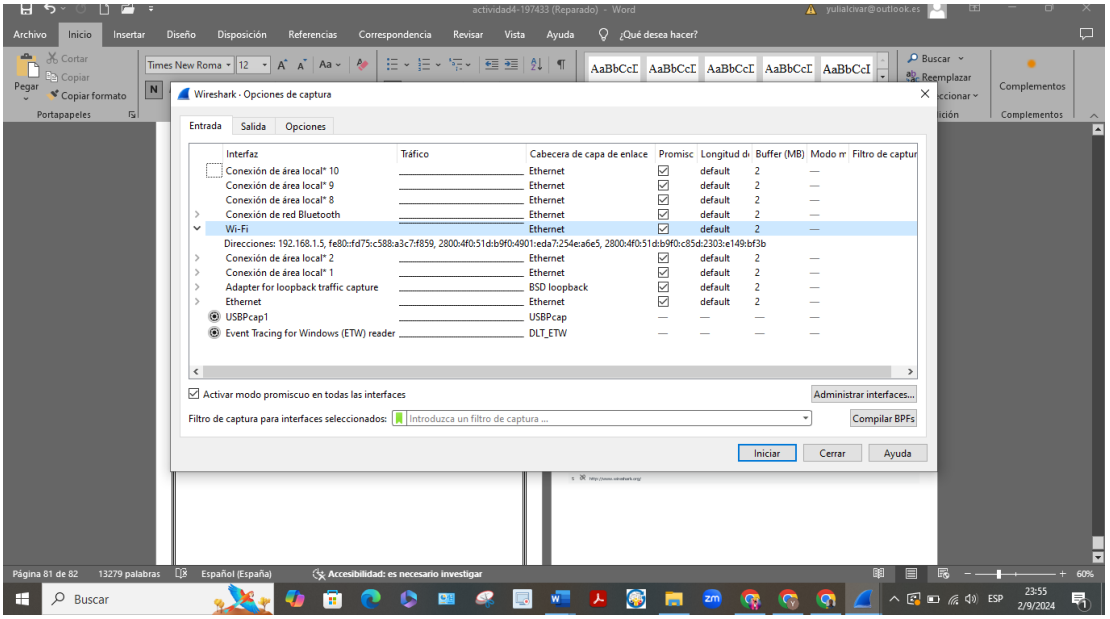
Análisis de red con wireshark



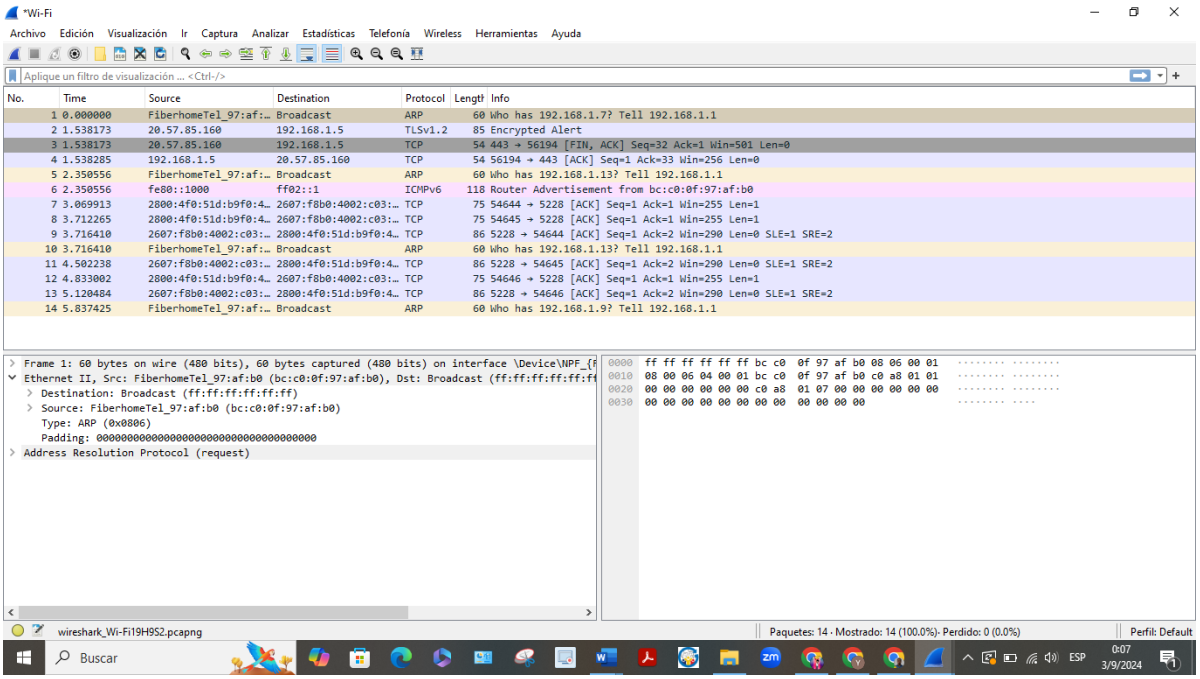
ventana de visualización de la interfaz de red de donde se va a capturar datos



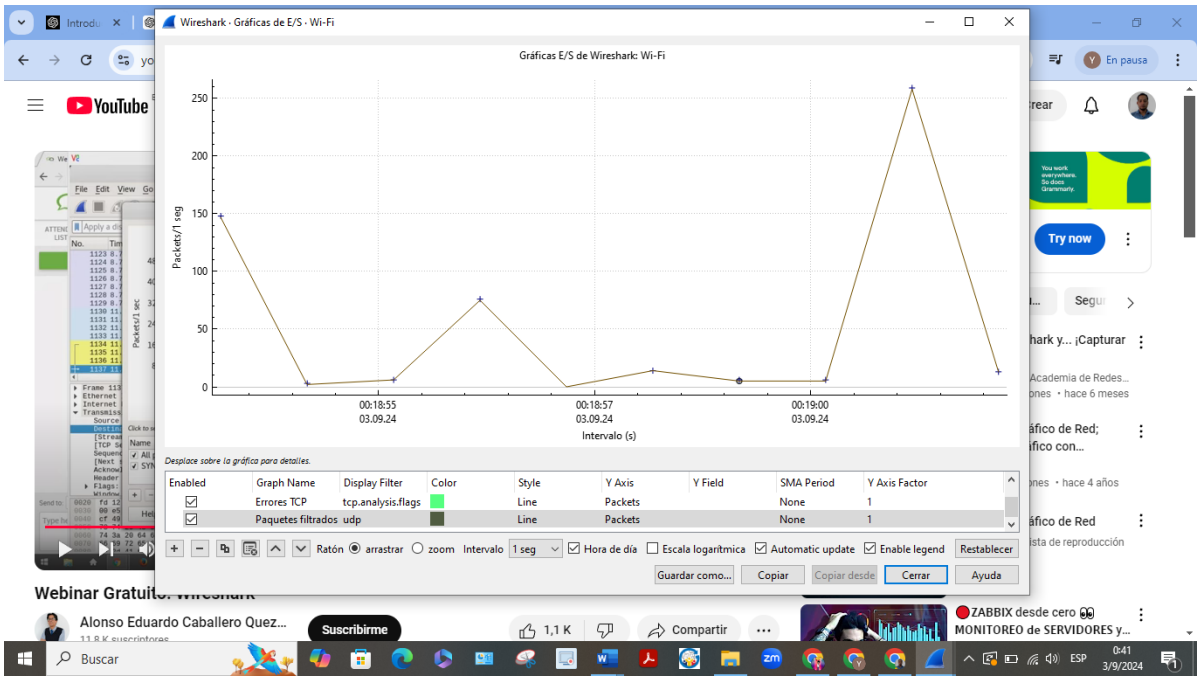
ventana de captura de interfaces



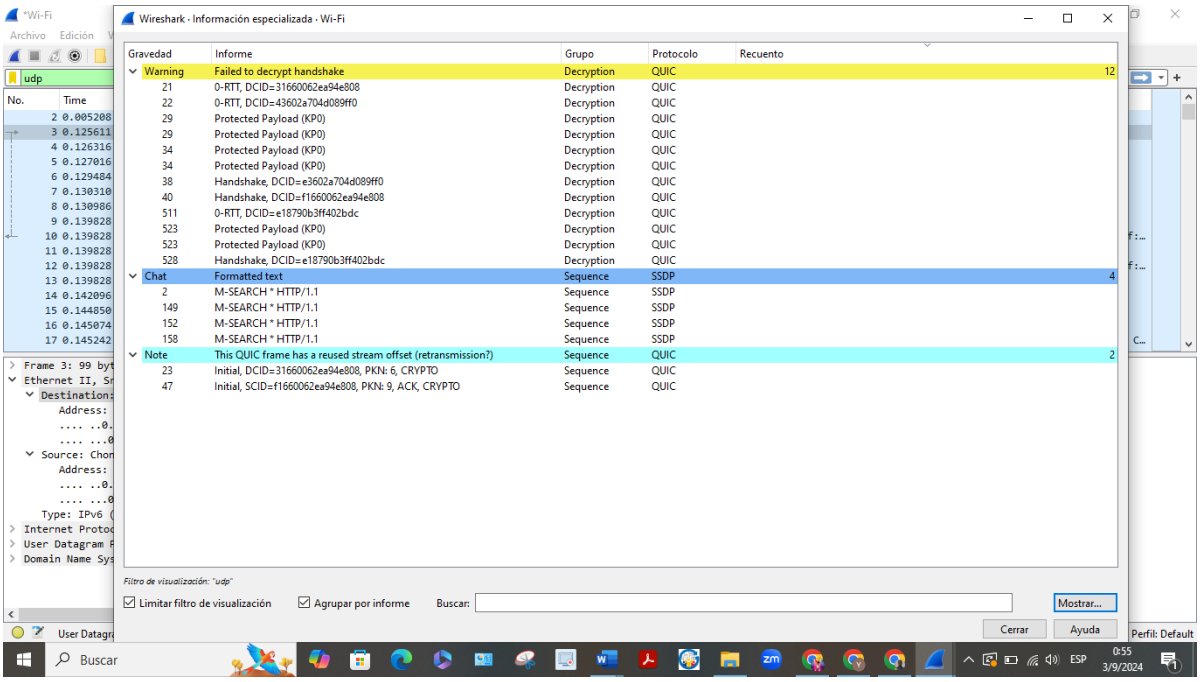
ventana de paquetes de red capturados.



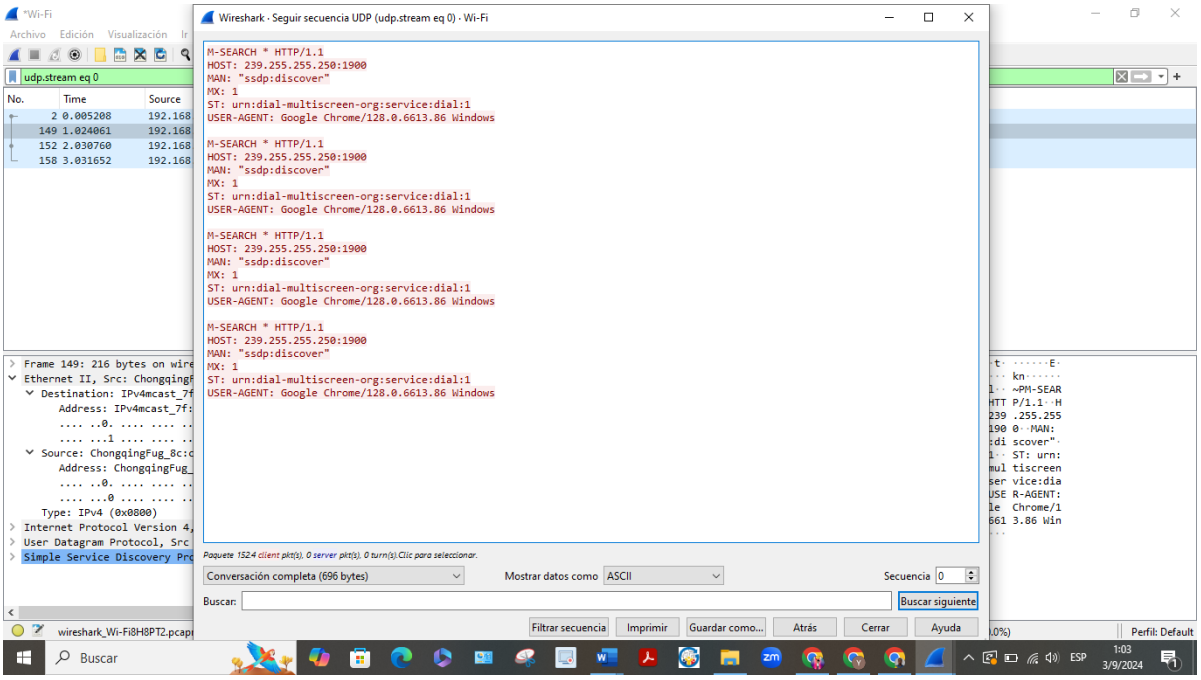
ventana grafica de los paquetes capturados y sus longitudes.



Ventana de análisis



Ventana de flujo



Anexo 2. Certificado de análisis anti plagio

CERTIFICADO DE ANÁLISIS
magister

1.2. Análisis y recopilación de paquetes de datos en la red utilizando Wireshark.

documento corregido

Nombre del documento: roberto yance .pdf
ID del documento: f2ea6cfa00540a56c294278b49037dbf5a1795bc
Tamaño del documento original: 3,07 MB
Autor: Roberto Yance

Depositante: Roberto Yance
Fecha de depósito: 13/8/2024
Tipo de carga: url_submission
fecha de fin de análisis: 13/8/2024

Número de palabras: 13.781
Número de caracteres: 88.933

Ubicación de las similitudes en el documento:

Fuente principal detectada

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.uisrael.edu.ec http://repositorio.uisrael.edu.ec/bitstream/47000/168/1/UISRAEL-EC-SIS-378.242-404.pdf 1 fuente similar	< 1%		Palabras idénticas: < 1% (78 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	examenredes.com | 8.2.8 Práctica de laboratorio: Uso de Wireshark para examinar... https://examenredes.com/8-2-8-practica-de-laboratorio-uso-de-wireshark-para-examinar-las-trama...	< 1%		Palabras idénticas: < 1% (11 palabras)
2	repository.unad.edu.co http://repository.unad.edu.co/bitstream/10596/21426/1/13872463.pdf	< 1%		Palabras idénticas: < 1% (10 palabras)

Fuentes mencionadas (sin similitudes detectadas)

Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://www.servidor.com
2 http://www.servidor.com/
3 http://www.openssh.com/
4 http://www
5 http://www.wireshark.org/