UNIVERSIDAD TECNOLÓGICA ISRAEL

Facultad de Ingeniería en Sistemas Informáticos

ANÁLISIS Y CAPTURA DE PAQUETES DE DATOS EN UNA RED MEDIANTE LA HERRAMIENTA WIRESHARK

Estudiante: Roberto Carlos Zeas Martínez

Tutor: Msc. Marco Lituma Orellana Ing.

Quito – Ecuador

2011

Certificación de Responsabilidad

Yo, Ing. Marco Lituma certifico que el presente trabajo fue desarrollado por el Sr. Roberto Zeas M. titulado “Análisis Y Captura de Paquetes de Datos en una red mediante Wireshark” 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. Marco Lituma Orellana.

Acta de Cesión de Derechos

Yo, ROBERTO CARLOS ZEAS MARTÍNEZ, estudiante de la Universidad Tecnológica Israel mención en INGENIERÍA EN SISTEMAS INFORMÁTICOS declaro conocer y aceptar las disposiciones y autorizo a la Universidad Tecnológica Israel, para que hagan el uso que estimen pertinente con el presente trabajo.

_____ __

Sr. Roberto Carlos Zeas Martínez

Certificación de Autoría

Yo, Roberto Carlos Zeas Martínez, declaro que soy el único autor del trabajo para la obtención del título de ingeniería en sistemas informáticos titulado: “Análisis Y Captura de Paquetes de Datos en una Red mediante Wireshark”, 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 Carlos Zeas Martínez.

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 los momentos más difíciles de mi vida y la capacidad para disfrutarlo en los momentos felices.

A mi querida madre, María Zeas, porque en su momento, buscó lo mejor para mí y me hizo una persona con valores y principios para toda la vida.

También quiero agradecer a todas esas personas que han aportado con su ayuda para cumplir 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, quien me ha levantado de los momentos más difíciles.

A mi dulce madre que creyó en mí y me dio 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 les sirva de ejemplo para seguir adelante, todo es alcanzable 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 Carlos Zeas Martínez

Tabla de Contenidos

1. CAPITULO I – INTRODUCCIÓN ..... - 1 -

1.1. Tema ..... - 1 -

1.2. Planteamiento del Problema ..... - 1 -

1.2.1. Antecedentes ..... - 1 -

1.2.2. Diagnóstico o planteamiento de la problemática general ..... - 2 -

1.2.2.1. Causas y Efectos ..... - 2 -

1.2.2.2. Pronóstico y control del pronóstico ..... - 3 -

1.3. Formulación de la problemática especifica ..... - 3 -

1.3.1. Problema Principal ..... - 3 -

1.3.2. Problemas Secundarios ..... - 4 -

1.4. Objetivos ..... - 4 -

1.4.1. Objetivo general ..... - 4 -

1.4.2. Objetivos Específicos ..... - 4 -

1.5. Justificación ..... - 5 -

1.5.1. Justificación Teórica ..... - 5 -

1.5.2. Justificación Metodológica ..... - 5 -

1.5.3. Justificación Práctica ..... - 6 -

1.6. Cronograma ..... - 7 -

2. CAPITULO II - MARCO DE REFERENCIA ..... - 8 -

2.1. Marco Teórico ..... - 8 -

2.1.1. Análisis de Paquetes de Datos ..... - 8 -

2.1.2. ¿Quiénes utilizan un Analizador de Redes? ..... - 8 -

2.1.3. Un analizador de red se utiliza para: ..... - 9 -

2.1.4. ¿Para que usan los intrusos un programa de Sniffer? ..... - 9 -
2.1.5. Evaluación de un analizador de paquetes..... - 10 -
2.1.6. ¿Por qué Wireshark?..... - 11 -
2.1.7. ¿Cómo Trabajan los Analizadores de paquetes?..... - 12 -
2.2. Marco Conceptual ..... - 13 -
2.2.1. Wireshark ..... - 13 -
2.2.2. Paquete de Datos..... - 13 -
2.2.3. Red..... - 14 -
2.2.4. Protocolos ..... - 14 -
2.2.5. Programas Empaquetados con Wireshark..... - 15 -
2.2.5.1. Tshark..... - 15 -
2.2.5.2. Editcap ..... - 16 -
2.2.5.3. Mergecap ..... - 16 -
2.2.5.4. text2pcap..... - 16 -
2.2.5.5. Capinfos..... - 17 -
2.2.5.6. dumpcap ..... - 17 -
2.3. Marco Temporal ..... - 18 -
2.4. Marco Legal..... - 18 -
3. CAPITULO III – METODOLOGÍAS ..... - 20 -
3.1. Metodología..... - 20 -
3.2. Técnicas..... - 21 -
3.2.1. Encuesta ..... - 21 -
3.2.2. Formato de la Encuesta ..... - 21 -

3.2.3. Análisis & Resultados de la Encuesta ..... - 23 -
3.2.3.1. Pregunta número 1 de la encuesta ..... - 23 -
3.2.3.2. Pregunta número 2 de la encuesta ..... - 24 -
3.2.3.3. Pregunta número 3 de la encuesta ..... - 26 -
3.2.3.4. Pregunta número 4 de la encuesta ..... - 27 -
3.2.3.5. Pregunta número 5 de la encuesta ..... - 28 -
3.2.3.6. Pregunta número 6 de la encuesta ..... - 29 -
3.2.3.7. Pregunta número 7 de la encuesta ..... - 31 -
3.2.3.8. Pregunta número 8 de la encuesta ..... - 32 -
4. CAPITULO IV - DESARROLLO ..... - 34 -
4.1.Importancia de la implementación de medidas de seguridad para evitar ataques en los paquetes de datos. ..... - 34 -
4.1.1. Técnicas Avanzadas de Sniffing..... - 34 -
4.1.1.1. Reconocimiento – Footprinting..... - 35 -
4.1.1.2. Escaneo SYN..... - 37 -
4.1.1.3. Ataques MITM Man-in-the-middle – Intermediarios ..... - 39 -
4.1.1.4. Cracking..... - 40 -
4.1.1.5. ARP Spoofing..... - 40 -
4.1.2. Asegurar los paquetes de datos en una Red de los Sniffers..... - 42 -
4.1.2.1. Utilizar el cifrado ..... - 42 -
4.1.2.2. Encriptación ..... - 43 -
4.1.2.3. Sistemas de encriptación ..... - 43 -

4.1.2.4. Clave simétrica..... - 44 -

4.1.2.5. Cifrado Asimétrico..... - 45 -

4.1.2.6. SSL Secure Sockets Layer ..... - 47 -

4.1.2.7. Algoritmos de encriptación usando Funciones Hash ..... - 48 -

4.1.2.8. SSH ..... - 49 -

4.1.2.9. Seguridad IP (IPSec) ..... - 50 -

4.1.2.10. OpenVPN..... - 51 -

4.2. Manifestar la importancia y el uso de la herramienta Wireshark ..... - 51 -

4.2.1. Uso de Wireshark para Solucionar problemas de red ..... - 51 -

4.2.2. Uso de Wireshark en una arquitectura de red ..... - 52 -

4.2.3. Uso de Wireshark para Administración de Sistemas..... - 53 -

4.2.4. Uso de Wireshark para la Administración de Seguridad ..... - 53 -

4.2.5. Uso de Wireshark como un IDS en una red ..... - 54 -

4.2.6. Uso de Wireshark como un detector para la transmisión de información privilegiada ..... - 54 -

4.3. Describir el procedimiento para la implementación de la herramienta Wireshark para su utilización en redes. ..... - 55 -

4.3.1. Paso 1 - Cumplir con los requisitos especificados para su instalación- 55 -

4.3.2. Paso 2 - Disponer de una conexión de Red para su implementación - 56 -

4.3.3. Paso 3 - Protocolos utilizados en la red sean soportados por Wireshark.. - 56 -

4.3.4. Paso 4 - Sistemas Operativos sean compatibles con la versión de Wireshark ..... - 57 -
4.3.5. Paso 5 - Descargar o disponer el software de Wireshark + librerías .. - 58 -
4.3.5.1. WinPcap ..... - 58 -
4.3.5.2. ¿Cómo Obtener la librería WinPcap para Wireshark? ..... - 59 -
4.3.5.3. Cómo Obtener Wireshark Para Sistemas Windows ..... - 60 -
4.3.5.4. Obtener Wireshark para Sistemas Linux ..... - 61 -
4.3.6. Paso 6 - Obtener permisos de Usuario en el sistema ..... - 65 -
4.3.7. Paso 7 - Instalación de Wireshark en equipos Host ..... - 66 -
4.3.8. Paso 8 - Seleccionar la interfaz de red que utilizaremos ..... - 66 -
4.3.9. Paso 9 - Seleccionar la ubicación en la red en donde se va a trabajar- 67 -
4.3.9.1. Sniffing alrededor de Hubs ..... - 67 -
4.3.9.2. Sniffing en un entorno de Switch ..... - 68 -
4.3.9.3. Sniffing en un Entorno Router ..... - 69 -
4.4. Proceso de captura de los paquetes de datos mediante filtros de búsqueda utilizando Wireshark. ..... - 70 -
4.4.1. ¿Dónde Realizar la Captura de Datos? ..... - 70 -
4.4.2. Modo Promiscuo ..... - 70 -
4.4.3. Capturar los paquetes de datos ..... - 71 -
4.4.4. Ventana principal de Wireshark ..... - 74 -
4.4.4.1. Lista de paquetes Capturados ..... - 74 -
4.4.4.2. Detalles del paquete Seleccionado ..... - 75 -

4.4.4.3. Bytes del paquete ..... - 75 -

4.4.5. Configuración de Wireshark para capturar paquetes de Datos ..... - 75 -

4.4.6. Utilización de Colores en los Paquetes de datos con Wireshark..... - 78 -

4.4.7. Filtrado de Paquetes de Datos..... - 79 -

4.4.7.1. Filtrado durante la captura ..... - 79 -

4.4.7.2. El filtrado de paquetes durante la visualización ..... - 81 -

4.4.8. Guardar Paquete de Datos..... - 82 -

4.4.9. Exportando a otros Formatos los Paquetes de Datos ..... - 84 -

4.5. Realizar el análisis de los paquetes de datos capturados de la red para su argumentación y registro..... - 86 -

4.5.1. Análisis de Paquetes..... - 86 -

4.5.2. Fusionar Archivos de Captura..... - 87 -

4.5.3. Imprimir Paquetes Capturados..... - 88 -

4.5.4. Búsqueda de Paquetes de Datos Capturados ..... - 89 -

4.5.5. Marcado de paquetes..... - 91 -

4.5.6. Gráficos..... - 92 -

4.5.7. Estadísticas de jerarquía de protocolos..... - 93 -

5. CAPITULO V - CONCLUSIONES Y RECOMENDACIONES..... - 95 -

5.1. Conclusiones..... - 95 -

5.2. Recomendaciones..... - 96 -

Bibliografía Y Web grafía ..... - 98 -

Bibliografía..... - 98 -

Web grafía..... - 99 -

Glosario de Términos..... - 101 -

Lista de Cuadros Y Gráficos

Figura 1 Posibles resultados de un escaneo SYN ..... - 38 -

Figura 2 Imagen que explica cómo funciona la encriptación..... - 43 -

Figura 3 Cifrado Simétrico..... - 44 -

Figura 4 Cifrado Asimétrico..... - 46 -

Figura 5 Utilización de Llaves Públicas Y Privadas..... - 47 -

Figura 6 SSH Secure Shell ..... - 49 -

Figura 7 OpenSSH..... - 50 -

Figura 8 WinPcap..... - 59 -

Figura 9 Descargar WinPcap para Windows..... - 59 -

Figura 10 Wireshark ..... - 60 -

Figura 11 Descargar Wireshark para Windows..... - 60 -

Figura 12 Descargar Wireshark para Linux..... - 61 -

Figura 13 Imagen tomada fedoraproject. ..... - 62 -

Figura 14 Listado de Paquetes de Wireshark para Fedora..... - 63 -

Figura 15 Información del Paquete de Wireshark ..... - 64 -

Figura 16 Ventana para abrir o guardar paquetes RPM ..... - 65 -

Figura 17 listado de dispositivos de interfaces de red disponibles..... - 66 -

Figura 18 lista de interfaces disponibles ..... - 67 -

Figura 19 Sniffing con Wireshark en un concentrador de red ..... - 68 -

Figura 20 La visibilidad en una red conmutada..... - 69 -

Figura 21 Menú Captura/Interfaces..... - 72 -

Figura 22 pantalla de interfaces de captura con su IP ..... - 72 -

Figura 23 Seleccionar una interfaz para la captura de paquetes de datos .. - 73 -

Figura 24 Menú Captura/Parar capturas ..... - 73 -

Figura 25 ventana principal de Wireshark con un diseño de tres paneles. .. - 74 -

Figura 26 Ventana de configuración de Wireshark ..... - 77 -

Figura 27 Menú Ver/Reglas para Colorear. ..... - 78 -

Figura 28 Ventana colorear reglas de Wireshark ..... - 79 -

Figura 29 Ventana de Wireshark para configurar los filtros de captura..... - 80 -

Figura 30 Ventana de Wireshark permite crear nuevos o borrar los filtros .. - 80 -

Figura 31 Filtros de captura de paquetes durante la visualización..... - 81 -

Figura 32 Ventana para configurar los filtros durante la visualización ..... - 82 -

Figura 33 Menú Archivo/Guardar y Guardar ..... - 83 -

Figura 34 ventana para Guardar los paquetes de datos ..... - 83 -

Figura 35 Extensiones disponible para guardar un archivo de captura..... - 84 -

Figura 36 Extensiones disponibles para el archivo de exportación..... - 84 -

Figura 37 Ventana para seleccionar los paquetes de datos para exportar . - 85 -

Figura 38 Menú de plegable Archivo/Fusionar archivos capturados..... - 87 -

Figura 39 El cuadro de dialogo de fusión de archivos de captura..... - 88 -

Figura 40 Ventana de configuración de impresión de archivos capturados. - 89 -

Figura 41 Menú Archivo/ Encontrar Paquetes Capturados ..... - 90 -

Figura 42 Búsqueda de paquetes en Wireshark ..... - 90 -

Figura 43 Menú Editar/ Marcar Paquetes ..... - 91 -

Figura 44 Lista de Marcar Paquetes ..... - 91 -

Figura 45 Menú Estadísticas/Gráficos IO..... - 92 -

Figura 46 Tomada de Wireshark muestra los gráficos de IO ..... - 93 -

Figura 47 Menú estadísticas/Jerarquías de protocolos..... - 94 -

Figura 48 La ventana de estadísticas de jerarquía de protocolos ..... - 94 -

Figura 49 Imagen obtenida desde http://www.cloudshark.org/ ..... - 97 -

Figura 50 Instalación de Wireshark en Microsoft Windows Paso N°1..... - 106 -

Figura 51 Instalación de Wireshark en Microsoft Windows Paso N°2..... - 106 -

Figura 52 Instalación de Wireshark en Microsoft Windows Paso N°3..... - 107 -

Figura 53 Instalación de Wireshark en Microsoft Windows Paso N°4..... - 108 -

Figura 54 Instalación de Wireshark en Microsoft Windows Paso N°5..... - 108 -

Figura 55 Instalación de Wireshark en Microsoft Windows Paso N°6..... - 109 -

Figura 56 Instalación de Wireshark en Microsoft Windows Paso N°7..... - 109 -

Figura 57 Instalación de Wireshark en Microsoft Windows Paso N°8..... - 110 -

Figura 58 Instalación de Wireshark en Microsoft Windows Paso N°9..... - 110 -

Figura 59 Instalación de Wireshark en Microsoft Windows Paso N°10..... - 111 -

Figura 60 Instalación de Wireshark en Microsoft Windows Paso N°11..... - 111 -

Figura 61 Instalación de Wireshark en Microsoft Windows Paso N°12..... - 112 -

Figura 62 Instalación de Wireshark en Microsoft Windows Paso N°13..... - 112 -

Figura 63 Instalación de Wireshark en Microsoft Windows Paso N°14..... - 113 -

Figura 64 Instalación de Wireshark en sistemas Linux Paso N°01 ..... - 114 -

Figura 65 Instalación de Wireshark en sistemas Linux Paso N°02 ..... - 114 -

Figura 66 Instalación de Wireshark en sistemas Linux Paso N°03 ..... - 115 -

Figura 67 Instalación de Wireshark en sistemas Linux Paso N°04 ..... - 116 -

Figura 68 Instalación de Wireshark en sistemas Linux Paso N°05 ..... - 117 -

Lista de Cuadros

1 Grafico de Resultados de la pregunta número 1 de la encuesta..... - 24 -

2 Grafico de Resultados de la pregunta número 2 de la encuesta..... - 25 -

3 Grafico de Resultados de la pregunta número 1 de la encuesta..... - 27 -

4 Grafico de Resultados de la pregunta número 4 de la encuesta..... - 28 -

5 Gráfico de Resultados de la pregunta número 5 de la encuesta..... - 29 -

6 Gráfico de Resultados de la pregunta número 6 de la encuesta..... - 30 -

7 Gráfico de Resultados de la pregunta número 7 de la encuesta..... - 32 -

8 Gráfico de Resultados de la pregunta número 8 de la encuesta..... - 33 -

Lista de Tablas

Tabla 1 Resultados de la pregunta número 1 de la encuesta ..... - 23 -

Tabla 2 Resultados de la pregunta número 2 de la encuesta ..... - 25 -

Tabla 3 Resultados de la pregunta número 3 de la encuesta ..... - 26 -

Tabla 4 Resultados de la pregunta número 4 de la encuesta ..... - 27 -

Tabla 5 Resultados de la pregunta número 5 de la encuesta ..... - 28 -

Tabla 6 Resultados de la pregunta número 6 de la encuesta ..... - 30 -

Tabla 7 Resultados de la pregunta número 7 de la encuesta ..... - 31 -

Tabla 8 Resultados de la pregunta número 8 de la encuesta ..... - 32 -

Lista de Anexos

Anexo 1 Manual de Instalación de Wireshark en sistemas Windows……...-92-

Anexo 2 Manual de Instalación de Wireshark en sistemas Linux……-99-

Anexo 3 Formato de la Encuesta……...-119-

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 pro-activo 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 Wireshark la elección del mismo se 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 el análisis, captura de paquetes de datos y solucionar problemas en redes de comunicaciones cuenta con todas las características estándares de un analizador de protocolos

En el presente trabajo se pretende dar a conocer las funcionalidades básicas de Wireshark a los administradores o usuarios de redes, como el análisis y captura de paquetes de datos en una red, pero primeramente se bebe tener en cuenta, un procedimiento básico para la implementación y su utilización de Wireshark antes de realizar los objetivos mencionados.

Summary

Computer networks are becoming increasingly complex and demanding as to the operation of them is getting bigger. The networks support more applications and strategic services. Therefore the analysis and network monitoring has become more important work and proactive basis to avoid problems and improve the quality of service provided to network users.

You select the network monitoring software Wireshark's choice of it has been made based on the broad capabilities that already has a free license that is compatible with multi-platform and supports multiple protocols and other qualities that will be described later. Wireshark is a protocol analyzer used to perform the analysis, packet capture and troubleshoot data communications networks has all the standard features of a protocol analyzer

In this paper seeks to highlight the basic features of Wireshark for network administrators or users, such as analysis and packet capture data on a network, but first drink taken into account, a basic procedure for implementing and use of Wireshark prior to the stated objectives.

1. CAPITULO I – INTRODUCCIÓN

1.1. Tema

Análisis y Captura de paquetes de datos en una red mediante Wireshark.

1.2. Planteamiento del Problema

1.2.1. Antecedentes

Todo administrador de redes ha tenido que enfrentarse alguna vez a una pérdida del rendimiento de la red. En ese caso sabrá que no siempre es sencillo, por falta de tiempo y recursos, o por desconocimiento de las herramientas apropiadas, para tener claro los motivos o causas por lo que está sucediendo el problema.

Históricamente, los analizadores de red se dedicaban en dispositivos de hardware que eran caros y difícil de usar. Sin embargo, nuevos avances en tecnología han permitido el desarrollo de analizadores de redes basadas en software, lo que hace que sea más conveniente y asequible para los administradores para solucionar con eficacia los problemas de una red.

Los análisis en las redes se realizan con el fin facilitar el almacenamiento y procesamiento de la información ya que nos permitirá compartir datos, de igual manera nos permiten establecer los recursos a los que se puedan acceder en la red.

A partir del año 2006 Ethereal es conocido como Wireshark, una herramienta gráfica utilizada por los profesionales, administradores o usuarios de la red para identificar, analizar hasta capturar todo tipo de tráfico en un momento determinado.

1.2.2. Diagnóstico o planteamiento de la problemática general

1.2.2.1. Causas y Efectos

No realizar análisis en las redes

- Recursos tecnológicos de redes no utilizados en su totalidad
- Desconocimiento de la cantidad de tráfico que circula en la red con relación al ancho de banda
- Mala utilización de los protocolos en el tráfico de los paquetes de datos.

Captura de paquetes

- Congestionamiento en el trafico de la red
- Redes vulneradas
- Redes con perdida de la informacion
- Penetracion en las redes
- Descubrimiento de puertos abiertos y servicios en ejecución

Desconocimiento de normas de seguridad o herramientas

- Mecanismos inapropiados de seguridad para la información en los paquetes de datos
- La no utilización de recursos tecnológicos o herramientas para solventar la seguridad en las redes
- No emplear puertos seguros para él envió y recepción de los paquetes de datos

1.2.2.2. Pronóstico y control del pronóstico

Pronóstico

La falta de mecanismos de seguridad en redes hace que sean más vulnerables a ataques de programas de sniffer, lo que implica pérdida de la información que es valiosa para las empresas.

El desconocimiento de puertos, protocolos, mecanismos de seguridad, direcciones IP, la cantidad de tráfico que circula por la red, ocasiona congestionamiento, perdida de paquetes, tiempos de respuesta más largos, diversas causas que pueden ocasionar diferentes problemas en las redes.

Control del pronóstico

Para lograr un control de estos efectos, se emplean análisis de las redes, realizando observación del tráfico y captura de los paquetes de datos, utilización de protocolos seguros, puertos, para buscar soluciones para hacer frente a los diversos problemas que se pueden presentar en las redes.

1.3. Formulación de la problemática especifica

1.3.1. Problema Principal

¿Permitirá el análisis y captura de paquetes de datos en una red mediante Wireshark dar a conocer la herramienta de software, para ayudar en el análisis de las redes a observar, capturar, analizar el tráfico de paquetes de datos, para resolver las necesidades y dificultades que se presentan al momento de realizar todo el proceso de envío y recepción de los paquetes de datos?

1.3.2. Problemas Secundarios

- Desconocimiento de la cantidad de tráfico en la red
- Mecanismos de seguridad inapropiados en la red
- Recursos tecnológicos de redes no utilizados en su totalidad
- Descubrimiento de puertos abiertos y servicios en ejecución
- Penetracion en las redes
- Mala utilización de los protocolos en el tráfico de los paquetes de datos.
- No emplear puertos seguros para él envió y recepción de los paquetes de datos.

1.4. Objetivos

1.4.1. Objetivo general

Fundamentar teóricamente el análisis y como capturar los paquetes de datos en una red mediante la herramienta de software de distribución pública Wireshark.

1.4.2. Objetivos Específicos

- Demostrar la importancia de la implementación de medidas de seguridad para evitar ataques en los paquetes de datos.
- Manifestar la importancia y el uso de la herramienta Wireshark
- Describir el procedimiento para la implementación de la herramienta Wireshark para su utilización en redes.
- Explicar el proceso de captura de los paquetes de datos mediante filtros de búsqueda utilizando Wireshark.
- Realizar el análisis de los paquetes de datos capturados de la red para su argumentación y registro.

1.5. Justificación

1.5.1. Justificación Teórica

El análisis de redes también conocido como análisis de tráfico, análisis de protocolos, o el análisis de paquetes, y así sucesivamente es el proceso de captura de tráfico de red e inspeccionar de cerca para determinar lo que está sucediendo en la red.

Un analizador de paquetes decodifica los datos de los protocolos comunes y muestra el tráfico de red en un formato legible. Un sniffer es un programa que monitorea los datos que viajan en una red.

Un analizador de red puede ser un dispositivo de hardware independiente con software especializado, o software que se instala en un ordenador de sobremesa o portátil. Entre los analizadores de red dependen las características tales como el número de protocolos soportados que se pueden descifrar, la interfaz de usuario, gráficos y las capacidades estadísticas.

1.5.2. Justificación Metodológica

La metodología necesaria para el planteamiento del análisis y captura de paquetes de datos en una red mediante Wireshark, son las siguientes que detallamos a continuación ver Capítulo 3 – Metodologías.

La herramienta de licencia publica Wireshark que va destinada para el uso en nuestro análisis y captura de datos, gracias a una investigación haciendo uso de métodos y técnicas informáticas que se puedan emplear en una red.

1.5.3. Justificación Práctica

La herramienta Wireshark utilizada en este análisis y captura de paquetes de datos puede ser utilizada, implementada e instalada en cualesquier máquina, como es de dominio GPL licencia pública podrá ser empleada por administradores de redes o usuarios en diferentes redes.

El estudio de este análisis y la captura de paquetes de datos podrán ser utilizados como guías para ayudar en todos los procesos de envió, recepción y control de la información que circula en una red.

1.6. Cronograma

Cronograma de Actividades

Nombre de la Tarea	Septiembre				Octubre				Noviembre			
Semana	01	02	03	04	01	02	03	04	01	02	03	04
Presentación del Tema de Tesis												
Aprobación del Tema de Tesis												
Designación de Tutor												
Unida 1												
Diseño del Anteproyecto												
Diseño del Anteproyecto												
Diseño del Anteproyecto												
Unidad 2												
Marco de Referencia												
Marco Teórico												
Marco Conceptual												
Marco Legal												
Unidad 3												
Metodologías												
Técnicas												
Unidad 4												
Desarrollo												
Objetivo 1												
Objetivo 2												
Objetivo 3												
Objetivo 4												
Objetivo 5												
Presentación del proyecto												
Versión de Borrador												
Capítulo 5												
Conclusiones y Recomendaciones, Anexos												

2. CAPITULO II - MARCO DE REFERENCIA

2.1. Marco Teórico

2.1.1. Análisis de Paquetes de Datos

Un análisis es una descomposición de un todo en partes pequeñas para poder estudiar su contenido. Los paquetes de datos contienen información que puede ser analizada y capturada.

Wireshark es una herramienta que permite el análisis y captura de paquetes de datos que circulan en una red.

No todos los paquetes de datos pueden ser interpretados o capturados debido a la implementación adicional de seguridad que tienen, los paquetes de datos que contienen información pueden estar encriptados con claves de acceso.

2.1.2. ¿Quiénes utilizan un Analizador de Redes?

Los administradores de sistemas, ingenieros de redes, ingenieros de seguridad, operadores de sistemas y los programadores todos usan los analizadores de red, que son herramientas muy valiosas para el diagnóstico y resolver problemas de red, problemas de configuración del sistema y las dificultades de aplicación.

El arte del análisis de redes es un arma de doble filo. Mientras que los profesionales de la seguridad hacen uso para la solución de problemas y el control de la red, intrusos utilizan el análisis de la red para propósitos dañinos. Un analizador de red es una herramienta, y como todas las herramientas, puede ser utilizado para fines tanto buenos como malos. (Orebaugh, y otros, 2007)

2.1.3. Un analizador de red se utiliza para:

- La conversión de los paquetes datos binarios a un formato legible
- Resolución de problemas en la red
- Analizar el rendimiento de una red para descubrir cuellos de botella
- Detección de intrusos en una red
- Registro de tráfico de red para la argumentación y las pruebas
- El análisis de las operaciones de las aplicaciones
- El descubrimiento de tarjetas de red defectuosas
- Descubrir el origen de los brotes de virus o de denegación de servicio (DoS)
- Validar el cumplimiento de las políticas de seguridad de la empresa
- Como un recurso educativo en el aprendizaje acerca de los protocolos

2.1.4. ¿Para que usan los intrusos un programa de Sniffer?

Cuando es utilizado por personas malintencionadas, sniffers pueden representar una amenaza significativa para la seguridad de una red. Los intrusos de la red utilizan sniffers para capturar información confidencial.

Los programas de sniffing se están convirtiendo en un término no negativo, la mayoría utiliza los términos sniffing y análisis de la red de manera intercambiable.

El uso de un sniffer de forma ilegítima se considera un ataque pasivo, ya que no se conectan directamente con otros sistemas en la red. Un sniffer puede también ser instalado como parte del compromiso de un equipo en una red mediante un ataque activo. El ataque pasivo es lo que hace difícil su detección. (Orebaugh, y otros, 2007)

Los intrusos utilizan los analizadores de redes para:

- La captura de nombres de usuario y contraseñas de texto plano
- El descubrimiento de los patrones de uso de los usuarios en una red
- Comprometer información confidencial
- Captura y reproducción de voz sobre **IP** conversaciones telefónicas (**VoIP**)
- Mapeo de la distribución de la red
- Pasiva OS fingerprinting.

2.1.5. Evaluación de un analizador de paquetes

Para evaluar un analizador de paquetes se debe tener en cuenta una serie de factores al seleccionar un sniffer de paquetes, incluyendo los siguientes:

Todos los protocolos soportados para capturar paquetes de datos pueden interpretar los distintos protocolos.

La mayoría puede interpretar protocolos de red comunes como por ejemplo, IPv4 e ICMP, la capa de transporte protocolos como TCP y UDP, y protocolos de la capa de aplicación como DNS y HTTP. Sin embargo, no pueden soportar protocolos tradicionales o nuevos como el IPv6, SMBv2 y SIP. Al elegir un sniffer, asegúrese de que es compatible con los protocolos que se utilizaran.

Tener en cuenta la facilidad de uso del analizador de paquetes, el diseño del programa, la facilidad de instalación, y el flujo general de operaciones estándar.

El programa que elija debe ajustarse a su nivel de experiencia. Si se tiene muy poca experiencia, en análisis de paquetes es posible que desee evitar, línea de comandos sniffers más avanzados como tcpdump.

Por otro lado, si se posee una gran riqueza de experiencia, se puede encontrar con un programa avanzado más atractivo. Como el análisis de paquetes,

incluso puede ser útil para combinar múltiples programas de sniffing para adaptarse a situaciones particulares.

El costo acerca de programas para captura de paquetes existen muchos gratuitos, los que compiten con los productos comerciales. La diferencia más notable entre los productos comerciales y sus alternativas libres es la presentación de informes. Los productos comerciales suelen incluir algún módulo de generación de informes, esto por lo general no existen en las aplicaciones libres.

Soporte para programas incluso después de haber dominado los fundamentos de un programa de sniffing, Se puede necesitar ayuda para resolver nuevos problemas, buscar documentación para desarrolladores, foros públicos y listas de correo.

Wireshark, tienen comunidades que usan estas aplicaciones, estas comunidades de usuarios y colaboradores ofrecen foros de discusión, wikis, y los blogs diseñado para ayudar a emplear la herramienta.

Desafortunadamente, no todos los programas analizadores de paquetes soportan todos los sistemas operativos. Elija uno que funcione en todos los sistemas operativos que se necesiten. (Sanders, 2011)

2.1.6. ¿Por qué Wireshark?

Wireshark es un analizador de protocolos ***open-source*** diseñado por Gerald Combs y que actualmente está disponible para múltiple plataformas. Conocido originalmente como **Ethereal**, su principal objetivo es el análisis de tráfico además de ser una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red.

Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para más de 1100 protocolos soportados actualmente; y una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados. Gracias a que Wireshark “entiende” la estructura de los protocolos, podemos visualizar los campos de cada una de las cabeceras y capas que componen los paquetes monitorizados, proporcionando un gran abanico de posibilidades al administrador de redes a la hora de abordar ciertas tareas en el análisis de tráfico.

2.1.7. ¿Cómo Trabajan los Analizadores de paquetes?

El proceso de sniffing de paquetes implica un esfuerzo de cooperación entre el software y el hardware. Este proceso se puede dividir en tres pasos:

Colección En el primer paso, el rastreador de paquetes recoge datos binarios del cable de red. Por lo general, esto se hace cambiando la interfaz de red seleccionada en modo promiscuo. En este modo, la tarjeta de red puede escuchar todo el tráfico en un segmento de red, no solamente el tráfico que se dirigida a este.

En este paso de conversión, los datos binarios capturados se convierten en una forma legible. La línea de comandos más avanzada captura paquetes. En este punto, los datos de la red está en una forma que puede ser interpretado sólo en un nivel muy básico, dejando a la mayoría de los análisis para el usuario final.

El análisis es el tercer y último paso consiste en el análisis real de la captura y se convierten los datos. El rastreador de red captura paquetes de datos,

verifica su protocolo basado en la información extraída y comienza su análisis de las características del protocolo. (Sanders, 2011)

2.2. Marco Conceptual

2.2.1. Wireshark

Wireshark es un analizador de paquetes de red. Un analizador de paquetes de red captura los paquetes de datos y tratara de mostrar los paquetes lo más detallado posible. Un analizador de paquetes de red es como un dispositivo de medición utilizado para examinar lo que está pasando en el interior de un cable de red.

Se distribuye bajo **GNU** Licencia Pública General Y **GPL** licencia de código abierto.

2.2.2. Paquete de Datos

Un paquete de datos es una unidad fundamental de transporte de información en todas las redes de computadoras modernas.

Un paquete está generalmente compuesto de tres elementos: una cabecera contiene generalmente la información necesaria para trasladar el paquete desde el emisor hasta el receptor, el área de datos que contiene los datos que se desean trasladar, y la cola, que comúnmente incluye código de detección de errores.

http://es.wikipedia.org/wiki/Paquete_de_datos

2.2.3. Red

Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos con la finalidad de compartir información y recursos.

La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el coste general de estas acciones.

http://es.wikipedia.org/wiki/Red_de_computadoras

2.2.4. Protocolos

Las redes modernas se componen de una variedad de sistemas que se ejecutan en diferentes plataformas. Para facilitar esta comunicación, se utiliza un conjunto de lenguajes comunes llamados protocolos.

- Protocolo de Control de Transmisión (TCP),
- Protocol de Internet (IP),
- Address Resolution Protocol (ARP),
- Dynamic Host Configuration Protocol (DHCP).

Una pila de protocolos es una agrupación lógica de los protocolos que trabajan juntos. Los protocolos trabajan en gran parte del mismo modo, lo que nos permite definir el número de paquetes deben ser colocados, como iniciar una conexión y la forma de asegurar el recibimiento de los datos. Un protocolo puede ser muy simple o muy complejo, dependiendo de su función.

2.2.5. Programas Empaquetados con Wireshark

Wireshark viene con una interfaz gráfica de usuario (GUI). Cuando está instalado Wireshark, también incluye otros programas de apoyo: la versión de línea de comandos de Wireshark, llamado tshark, y otros cinco programas para ayudarle en la manipulación, la evaluación y la creación de archivos de captura.

- Tshark
- editcap,
- mergecap,
- text2pcap,
- capinfos,
- Dumpcap.

Estos programas de apoyo se pueden utilizar juntos para proporcionar una manipulación muy potente de los archivos de captura. Estos archivos pueden ser capturados con tshark, editado con editcap y se combinan en un archivo de captura de paquetes individuales con mergecap. (Orebaugh, y otros, 2007)

2.2.5.1. Tshark

Tshark es la versión de línea de comandos de Wireshark. Se puede utilizar para capturar, decodificar e imprimir la pantalla de paquetes en vivo desde el cable para guardar o leer archivos de captura.

Algunas de las mismas características que se aplican tanto a tshark y Wireshark, ya que utilizan la misma biblioteca de captura libpcap y la mayor parte del mismo código.

Tshark puede leer todos los mismos formatos de captura de paquetes como Wireshark y determinará automáticamente el tipo. La ventaja de utilizar tshark es las secuencias de comandos. (Orebaugh, y otros, 2007)

2.2.5.2. Editcap

editcap es un programa usado para eliminar o seleccionar los paquetes desde un archivo y para convertir el formato de los archivos capturados. No captura el tráfico en vivo, sino que solamente lee los datos de un archivo de captura salvado y salva a algunos o todos los paquetes en un archivo de captura nueva. editcap puede leer todos los archivos del mismo tipo de Wireshark y por defecto, escribe en formato libpcap.

editcap puede determinar el tipo de archivo que está leyendo, y es capaz de leer archivos comprimidos con gzip. Por defecto, editcap escribe todos los paquetes en el archivo de captura para el archivo de salida. (Orebaugh, y otros, 2007)

2.2.5.3. Mergecap

mergecap se utiliza para combinar múltiples archivos de captura salvado en un único archivo de salida. mergecap puede leer todos los archivos del mismo tipo de Wireshark y por defecto, escribe en formato libpcap. De manera predeterminada, los paquetes de los archivos de entrada se fusionan en orden cronológico basado en fecha y hora de cada paquete. (Orebaugh, y otros, 2007)

2.2.5.4. text2pcap

text2pcap genera archivos de captura mediante la lectura de captura ASCII hexadecimal y escribe los datos en un archivo de

salida libpcap. Es capaz de leer un volcado hexadecimal de los paquetes individuales o múltiples, y la creación de archivos de captura de la misma.

text2pcap también puede leer hexdumps de datos de nivel de aplicación únicamente, mediante la creación ficticia de Ethernet, IP y UDP o las cabeceras de TCP para Wireshark. (Orebaugh, y otros, 2007)

2.2.5.5. Capinfos

Capinfos es una nueva herramienta de línea de comandos incluido en Wireshark que examina un archivo de captura almacenado y las estadísticas de los informes relacionados con el número de paquetes, tamaño de los paquetes, y una información puntual.

A diferencia de otras estadísticas de los mecanismos de información en que las herramientas de Wireshark, capinfos no informa sobre el contenido del tráfico, en lugar de dar un breve resumen de los contenidos de archivo de captura. (Orebaugh, y otros, 2007)

2.2.5.6. dumpcap

La utilidad dumpcap se utiliza para capturar el tráfico de una interfaz vivo y guardar en un archivo libpcap. Esta utilidad incluye un subconjunto de las funciones disponibles en tshark, pero no incluye la biblioteca de decodificadores de protocolo. Esto le da dumpcap un tamaño mucho menor, que puede ser beneficioso en sistemas de baja memoria para la captura de tráfico con múltiples procesos. (Orebaugh, y otros, 2007)

2.3. Marco Temporal

El planteamiento, desarrollo del análisis y captura de paquetes de datos en una red mediante Wireshark se desarrollara en la ciudad de Cuenca – Ecuador. En el ámbito de redes puede ser bastante amplio dependiendo en qué lugar se planea hacer el análisis y la captura de paquetes de datos y que estructura física, tecnológica, que recursos manejan o disponen en esa red.

El análisis y captura de paquetes de datos de una red mediante Wireshark tendrá su tiempo de desarrollo establecido por el director de carrera de la universidad que ira de acuerdo al cronograma de actividades que se presenta en la última parte de este capítulo.

2.4. Marco Legal

Antes de abrir un analizador de protocolos de red como Wireshark que instalo para cualesquier uso, lea detalladamente las políticas de la empresa. Un escrito correctamente y completo uso adecuado de políticas de red prohíben la ejecución de los analizadores de red.

En el análisis de redes de las empresas, en donde se proporcionan servicios de consultoría de seguridad para clientes, confirmar el uso de un sniffer es incluido en su reglamento. Especificar sobre cómo, dónde y cuándo va a ser utilizado la herramienta. Indicar cláusulas como acuerdos de no divulgación que le exime de la responsabilidad del aprendizaje de información confidencial.

Un administrador permite ejecutar legítimamente un sniffer, para hacer cumplir la política de seguridad de su empresa. Las políticas sobre el uso de Wireshark o cualquier otra herramienta de sniffers relacionada con la seguridad no están claras o definidas en su organización, primero obtener el permiso por escrito de los departamentos correspondientes antes de usarlos.

3. CAPITULO III – METODOLOGÍAS

3.1. Metodología

Utilizaremos la metodología inductiva porque es una herramienta de investigación, que nos permitirá obtener resultados específicos a partir de hechos generales, comenzando con una parte de la investigación a una totalidad de la misma.

La metodología deductiva es una herramienta de investigación que considera que los hechos generales definen la investigación específica. La investigación deductiva es válida cuando los hechos son verdaderos.

La observación del tráfico en redes

El registro de todos los Paquetes de Datos Capturados

La clasificación de los Paquetes de Datos

Procesos informáticos:

Escaneo Y Enumeración de puertos en la red

Captura de paquetes de datos en una red

Guardar paquetes de datos

Exportar a otros formatos los paquetes de datos capturados

Imprimir los Paquetes de datos

Análisis, gráficos y estadísticas de los paquetes de datos

Búsquedas de paquetes de datos x Filtros

3.2. Técnicas

3.2.1. Encuesta

Una encuesta es un estudio observacional, los datos se obtienen a partir de realizar un conjunto de preguntas normalizadas dirigidas a una muestra o totalidad de la población estadística que es el objeto de nuestro estudio, con el fin de conocer resultados.

Realizaremos un formato de encuesta de la cual podremos sacar conclusiones específicas, para evaluar el conocimiento y utilización de la herramienta de software Wireshark en las redes informáticas de la localidad.

Diseñando este modelo de encuesta por medio de las cual comprobaremos más de cerca el conocimiento de herramientas de software analizadores de redes como Wireshark en gran parte la efectividad de este herramienta en las redes de la ciudad. La encuesta está dirigida a la siguiente población:

- Administradores de Redes
- Usuarios de redes
- Personas que están relacionadas con las redes informáticas

La muestra necesaria para nuestra encuesta está establecida en un número total de 10 encuestas.

3.2.2. Formato de la Encuesta

Formato del cuestionario realizado a los administradores de redes.

Para el trabajo de graduación “Análisis Y Captura de paquetes de datos en una red Mediante Wireshark” para la Universidad Tecnológica Israel se está realizando una encuesta para el conocimiento sobre la utilización de herramientas de software en las redes informáticas de la ciudad de Cuenca.

Para cumplir con lo propuesto, requerimos amablemente a UD. Que nos proporcione información real, agradeciéndole por la atención prestada a la encuesta.

1.-.Sabe que es un software analizador de Red

[ ] Si [ ] No

2.- Conoce Herramientas de Software para el análisis de Redes.

[ ] Si [ ] No

Cuales

_____

_____

3.- ¿Ha trabajado antes con alguna herramienta de software para el análisis de Redes?

[ ] Si [ ] No

4.- ¿Seleccione con qué frecuencia se debería realiza un análisis en la red?

[ ] Continuamente

[ ] Parcialmente

[ ] Solamente cuando se presenta un problema en la red

5.- ¿Conoce que es Wireshark?

[ ] Si [ ] No

6.- Ha empleado Wireshark en una Red

[ ] Si [ ] No

7.- Con la utilización de un analizador de red cree UD. que ayudarían a solucionar los problemas dentro de una red.

[ ] Si [ ] No

¿Por qué?

_____

_____

8.- Estaría de acuerdo que en una red se implemente un software informático para el análisis de redes.

[ ] Si [ ] No

¿Por qué?

_____

_____

3.2.3. Análisis & Resultados de la Encuesta

3.2.3.1. Pregunta número 1 de la encuesta

1.-.Sabe que es un software analizador de Red

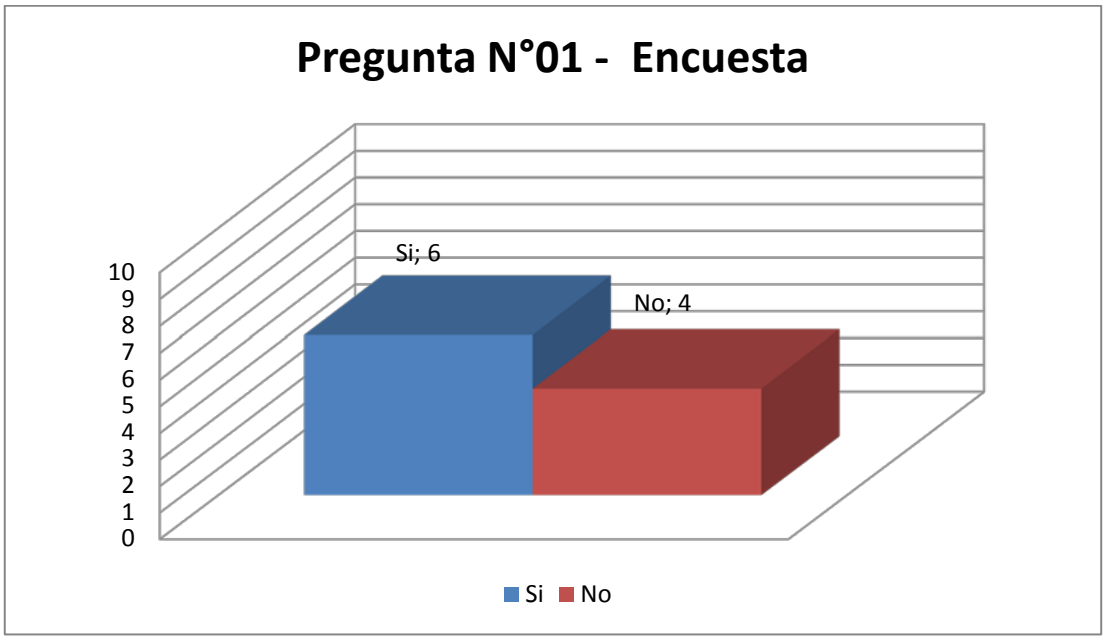
[ ] Si [ ] No

Opciones	Seleccionadas	Porcentaje
Si	**6**	**60%**
No	**4**	**40%**
Blanco		
Totales	**10**	**100%**

Tabla 1 Resultados de la pregunta número 1 de la encuesta

En la pregunta número uno de la encuesta dirigida a nuestra muestra, podemos observar cómo nos presenta visualmente el grafico, las 6 personas que afirman saber que es un software analizador de red, tal vez se deba porque la muestra fue tomada a personas relacionadas directamente con redes, pero existe un 40% restante que señala no conocer, entonces el presente trabajo de análisis y captura de paquetes de datos mediante Wireshark servirá para dar a conocer que es un analizador de red.

Grafico



1 **Grafico de Resultados de la pregunta número 1 de la encuesta**

3.2.3.2. Pregunta número 2 de la encuesta

2.- Conoce Herramientas de Software para el análisis de Redes.

[ ] Si [ ] No

Cuales

_____

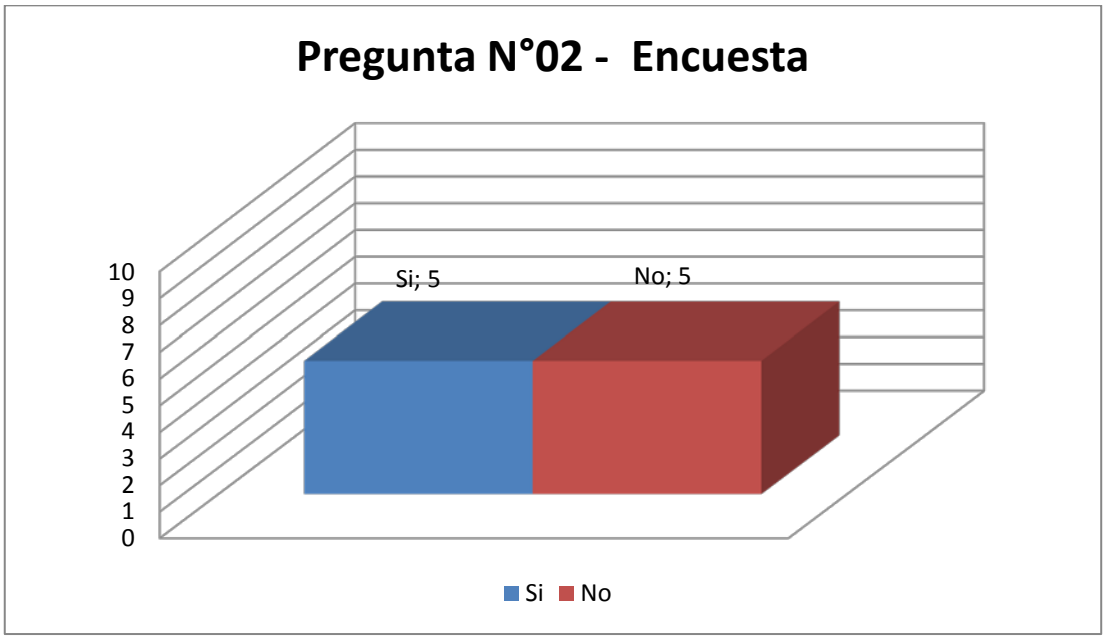
_____

Opciones	Seleccionadas	Porcentaje
Si	**5**	**50%**
No	**5**	**50%**
Blanco		
Totales	**10**	**100%**

Tabla 2 Resultados de la pregunta número 2 de la encuesta

En la pregunta número dos de la encuesta dirigida a nuestra muestra, podemos observar cómo nos presenta visualmente el grafico, 5 afirman conocer algunas herramientas de analizador de red esto representa un 50% del total mientras que los 5 restantes no conocen ninguna herramienta de red representado la otra mitad el 50%, posiblemente las personas que mencionaron saber que es un analizador de red posiblemente conozcan algunas herramientas de software.

Grafico



2 Grafico de Resultados de la pregunta número 2 de la encuesta

3.2.3.3. Pregunta número 3 de la encuesta

3.- ¿Ha trabajado antes con alguna herramienta de software para el análisis de Redes?

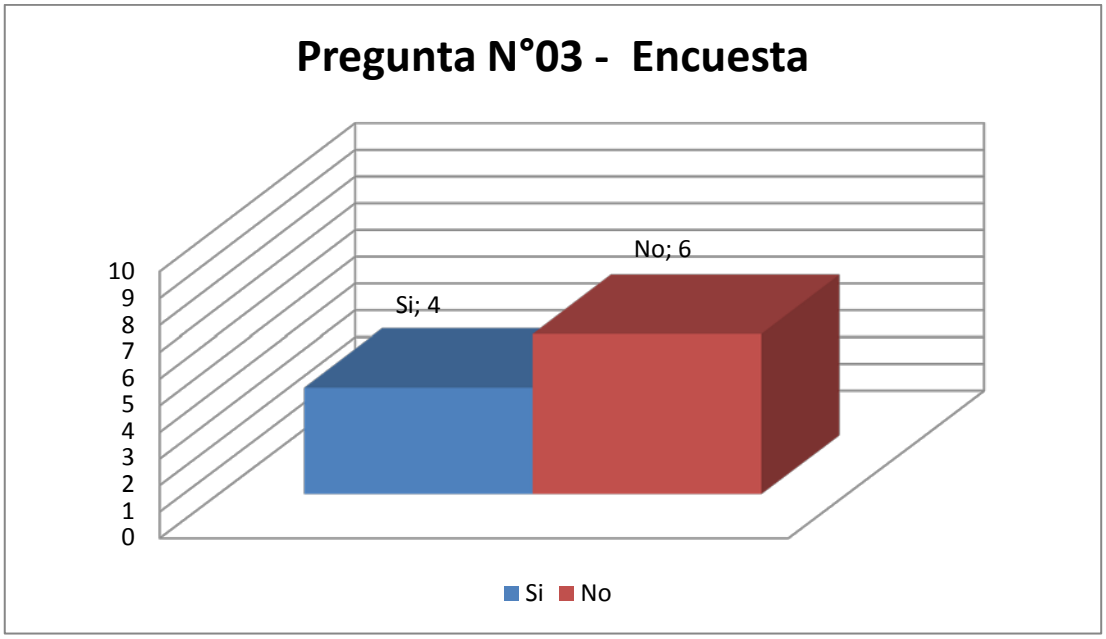
[ ] Si [ ] No

Opciones	Seleccionadas	Porcentaje
Si	**4**	**40%**
No	**6**	**60%**
Blanco		
Totales	**10**	**100%**

Tabla 3 Resultados de la pregunta número 3 de la encuesta

En la pregunta número tres de la encuesta dirigida a nuestra muestra, podemos observar cómo nos presenta visualmente el grafico, 4 afirman haber trabajado con alguna herramienta analizador de red esto representa un 40% del total mientras que los 6 restantes señalaron no haber trabajado, las personas que afirmaron saber que es un analizador de red, y que conocían algunas herramientas entonces por múltiples factores se deban que no han utilizado estas herramientas, lo que se pretende en este trabajo es dar a conocer las funcionalidades de la herramienta Wireshark que sirva como guía orientativa.

Grafico



3 Grafico de **Resultados de la pregunta número 3 de la encuesta**

3.2.3.4. Pregunta número 4 de la encuesta

4.- ¿Seleccione con qué frecuencia se debería realizar un análisis en la red?

[ ] Continuamente

[ ] Parcialmente

[ ] Solamente cuando se presenta un problema en la red

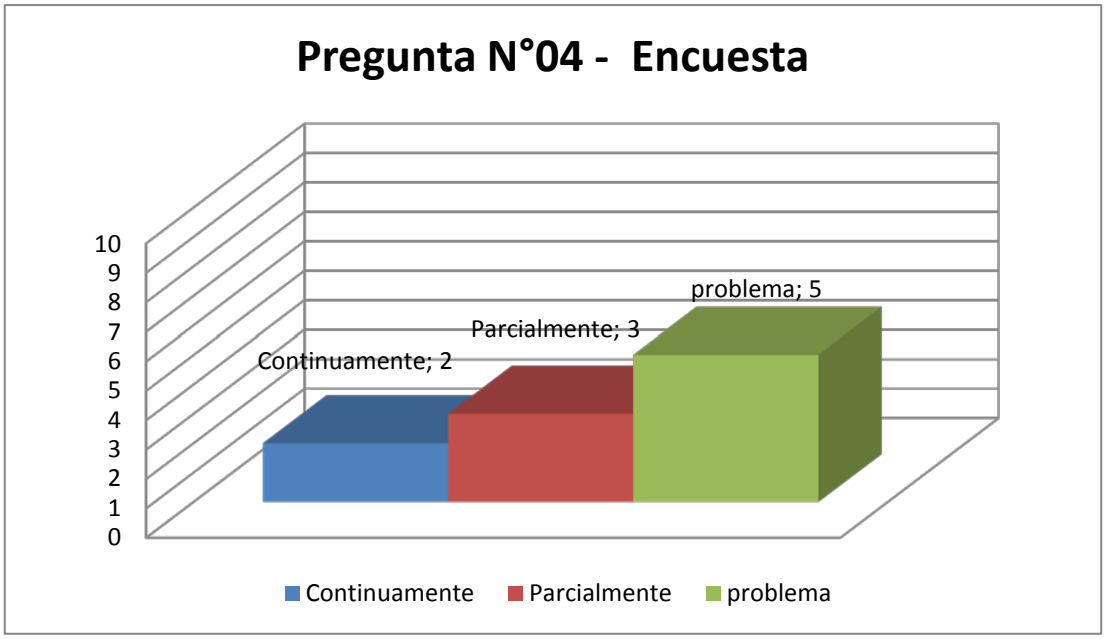
Opciones	Seleccionadas	Porcentaje
Continuamente	**2**	**20%**
Parcialmente	**3**	**30%**
Presenta un problema	**5**	**50%**
Totales	**10**	**100%**

Tabla 4 Resultados de la pregunta número 4 de la encuesta

En la pregunta número cuatro de la encuesta dirigida a nuestra muestra, podemos observar cómo nos presenta visualmente el grafico, cabe recalcar que esta pregunta era de selección múltiple, obteniendo 2 personas aseguran que se debe realizar continuamente, en lo personal estoy de acuerdo, mientras

que 3 señalaron parcialmente, esto depende de la red y 5 afirmaron solamente cuando se presente un problema.

Grafico



4 Grafico de Resultados de la pregunta número 4 de la encuesta

3.2.3.5. Pregunta número 5 de la encuesta

5.- ¿Conoce que es Wireshark?

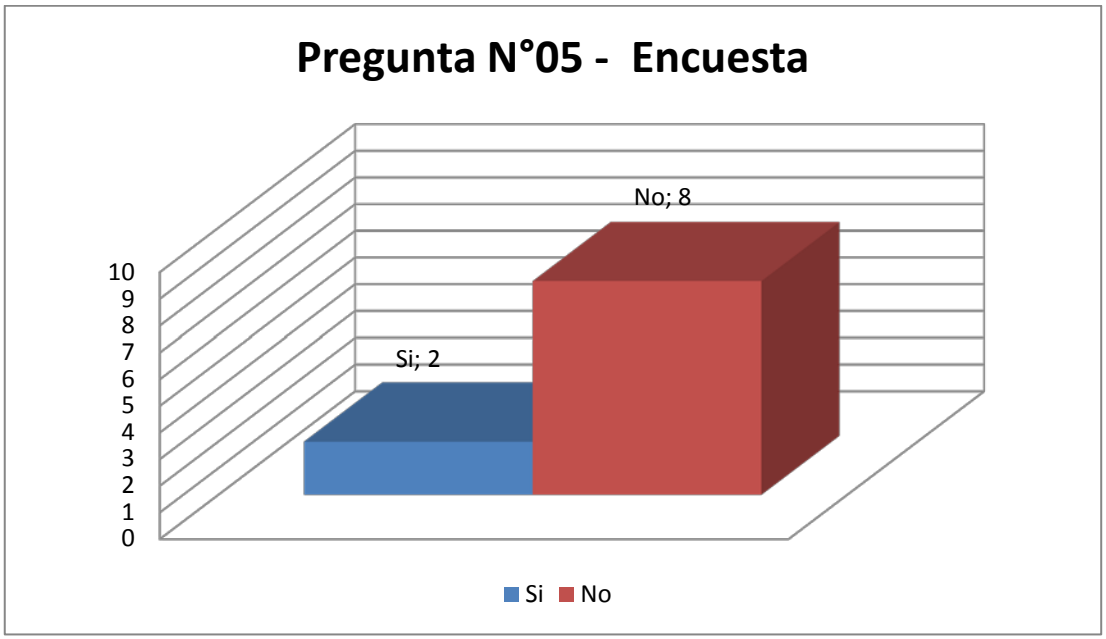
[ ] Si [ ] No

Opciones	Seleccionadas	Porcentaje
Si	**2**	**20%**
No	**8**	**80%**
Blanco		
Totales	**10**	**100%**

Tabla 5 Resultados de la pregunta número 5 de la encuesta

En la pregunta número cinco de la encuesta dirigida a nuestra muestra, podemos observar cómo nos presenta visualmente el grafico, solamente 2 afirman conocer la herramienta Wireshark representa un bajo porcentaje de un 20% mientras que los 8 restantes no conocen que es Wireshark, cabe mencionar que algunas personas mencionaron conocer herramientas analizadores de redes.

Grafico



5 Gráfico de **Resultados de la pregunta número 5 de la encuesta**

3.2.3.6. Pregunta número 6 de la encuesta

6.- Ha empleado Wireshark en una Red

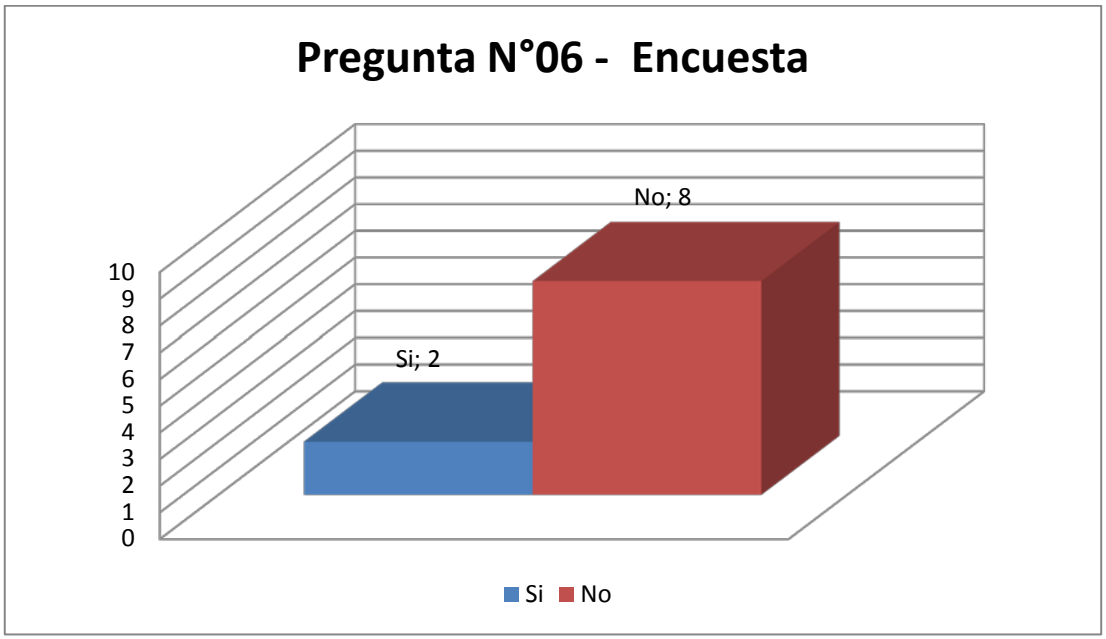
[ ] Si [ ] No

Opciones	Seleccionadas	Porcentaje
Si	**2**	**20%**
No	**8**	**80%**
Blanco		
Totales	**10**	**100%**

Tabla 6 Resultados de la pregunta número 6 de la encuesta

En la pregunta número seis de la encuesta dirigida a nuestra muestra, podemos observar cómo nos presenta visualmente el grafico, que las mismas 2 que afirmaron conocer que es Wireshark, también lo han utilizado, mientras que los 8 restantes no han empleado Wireshark, pese a ser una herramienta importante y utilizada bastante a nivel mundial en el ámbito de redes.

Grafico



6 Gráfico de Resultados de la pregunta número 6 de la encuesta

3.2.3.7. Pregunta número 7 de la encuesta

7.- Con la utilización de un analizador de red cree UD. que ayudarían a solucionar los problemas dentro de una red.

[ ] Si [ ] No

¿Por qué?

_____

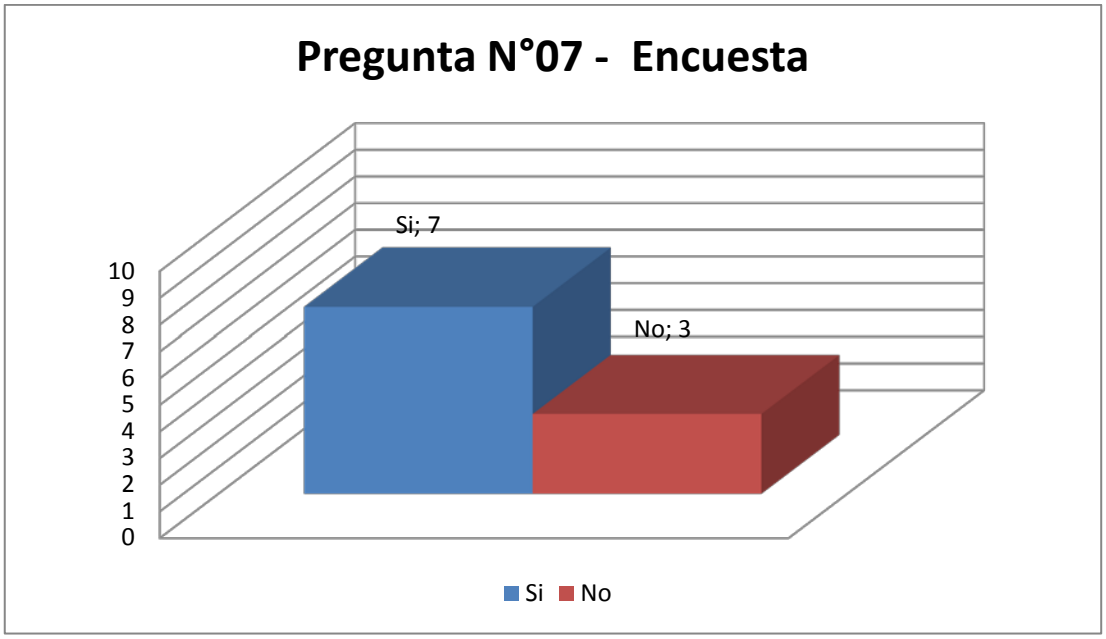
_____

Opciones	Seleccionadas	Porcentaje
Si	**7**	**70%**
No	**3**	**30%**
Blanco		
Totales	**10**	**100%**

Tabla 7 Resultados de la pregunta número 7 de la encuesta

En la pregunta número siete de la encuesta dirigida a nuestra muestra, podemos observar cómo nos presenta visualmente el grafico, la mayoría está de acuerdo 7 afirman que si ayudarían a resolver problemas en una red, mientras que los 3 restantes señalaron que no, esto se deba por desconocimiento de los analizadores de red o simplemente disponen de otros mecanismos en la red.

Grafico



7 Gráfico de Resultados de la pregunta número 7 de la encuesta

3.2.3.8. Pregunta número 8 de la encuesta

8.- Estaría de acuerdo que en una red se implemente un software informático para el análisis de redes.

[ ] Si [ ] No

¿Por qué?

_____

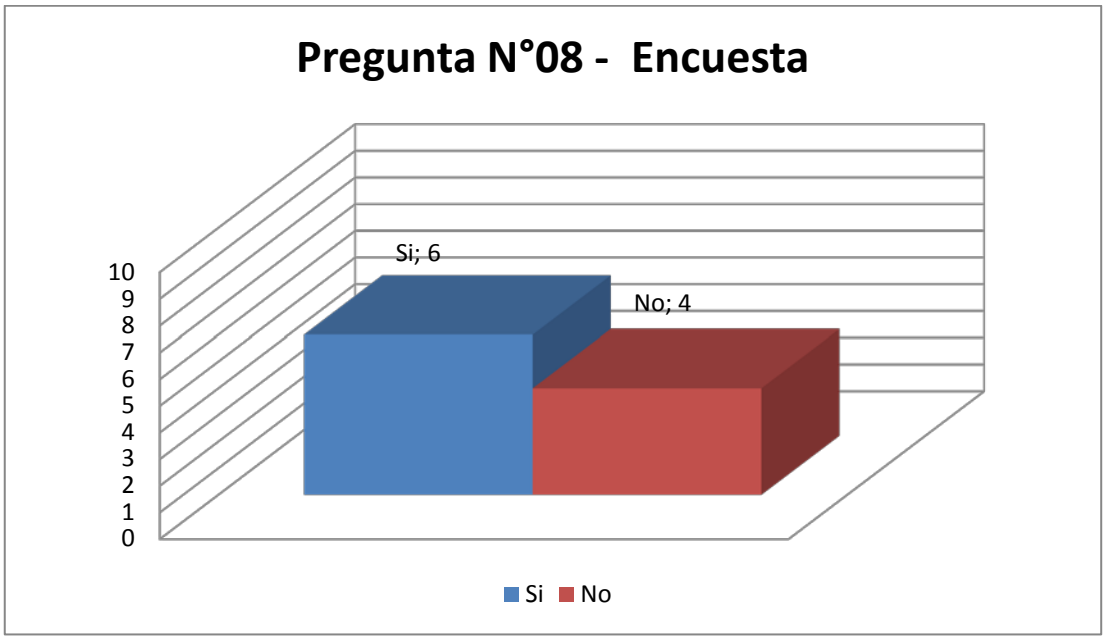
_____

Opciones	Seleccionadas	Porcentaje
Si	**6**	**60%**
No	**4**	**40%**
Blanco		
Totales	**10**	**100%**

Tabla 8 Resultados de la pregunta número 8 de la encuesta

En la pregunta número ocho de la encuesta dirigida a nuestra muestra, podemos observar cómo nos presenta visualmente el grafico, 6 afirman conocer que si estarían de acuerdo en la implementación de un analizador de red mientras que los 4 restantes no aceptarían tal vez porque cuentan con políticas de la empresa que prohíben el uso de este tipo de software en sus redes.

Grafico



8 Gráfico de **Resultados de la pregunta número 8 de la encuesta**

4. CAPITULO IV - DESARROLLO

4.1. Importancia de la implementación de medidas de seguridad para evitar ataques en los paquetes de datos.

Considerando un escenario, en el que un ladrón de bancos planifica robar el banco más grande de la ciudad, ubicado en la dirección A. Pasa la semana planeando un atraco elaborado, sólo para descubrir que a su llegada a la dirección objetivo, de que el banco se ha trasladado a la dirección B.

Peor aún, imaginar un escenario en el que el ladrón planea entrar en el banco durante el funcionamiento normal en horas de trabajo, con la intención de robar de la bóveda, sólo para ir al banco y descubrir que se cierra ese día.

Qué pasaría si el ladrón se presentó en el banco sin ningún tipo de conocimiento de la estructura física del edificio. Él no tendría idea de cómo acceder al edificio, porque él no sabe los puntos débiles de la seguridad física.

En estos tres diferentes escenarios del ladrón de bancos son comparaciones con un atacante de red con un programa de sniffer, es para hacerlo más entendible como un atacante planea antes de realizar su objetivo en la red, o la información.

En esta sección demostraremos la importancia de la implementación de medidas de seguridad para evitar ataques en los paquetes de datos**.**

4.1.1. Técnicas Avanzadas de Sniffing

Existen muchas alternativas a la utilización de Wireshark, para el uso en las redes. Desafortunadamente, los atacantes pueden utilizar estas técnicas para robar contraseñas u otros datos de la red.

4.1.1.1. Reconocimiento - Footprinting

El primer paso que un atacante necesita, es llevar a cabo una investigación en profundidad sobre el sistema de destino. Este paso, comúnmente conocida como **footprinting**, a menudo se logra utilizando diferentes recursos, o herramientas de software como Wireshark.

Una vez que esta investigación se ha completado, el atacante normalmente empezará a escanear la dirección IP o nombre DNS, de este objetivo para abrir puertos o servicios que se ejecutan. Este análisis permite al atacante determinar si el objetivo está vivo y accesible.

El Footprinting es el primer paso y el paso más importante que toman los Hacker para obtener toda la información que necesitan antes de lanzar un ataque, a este paso se le conoce también como la fase 1 o fase de Reconocimiento.

Asegurar el objetivo está vivo y accesible es el primer obstáculo que deben cruzar los atacantes. Otro resultado importante del escaneo, es que le dice al atacante que los puertos del destino se encuentran escuchando.

En esta parte del Footprinting es donde el atacante obtiene, reúne y organiza toda la información posible sobre su objetivo o su víctima, mientras más información obtiene con mayor precisión puede lanzar un ataque, obteniendo información como:

- Rango de Red y sub-red
- Acertar maquinas o computadoras activas
- Puertos abiertos y las aplicaciones que están corriendo en ellos
- Detectar versiones de Sistemas Operativos

- Nombres de Dominios
- Bloques de Red
- Direcciones IP específicas
- Ubicación donde se encuentran los Servidores
- Información de Contacto (números telefónicos, emails, etc.).
- DNS records

Contramedidas:

Hacer **Footprinting** en una empresa puede ayudar a los administradores de red saber qué tipo de información reside fuera de la compañía y las potenciales amenazas que esa información posee. Se deben usar medidas preventivas para asegurarse de que la información expuesta no pueda ser usada para "explotar" el sistema.

4.1.1.1.1. Fingerprinting Pasivo

Utilizando Fingerprinting pasivo, se examinan algunos campos dentro de los paquetes enviados desde el blanco con el fin de determinar el sistema operativo en uso. La técnica es considerada pasiva, ya que sólo escucha a los paquetes de envió de la máquina objetivo y no activamente envía paquetes al mismo host. Este es el tipo más ideal Fingerprinting para los atacantes, ya que les permite ser cautelosos.

4.1.1.1.2. Fingerprinting Activo

Cuando pasivamente se monitorea el tráfico no produce los resultados deseados, un enfoque más directo puede ser requerido.

Este enfoque se denomina Fingerprinting activo. Se trata de que el atacante esté enviando paquetes especialmente diseñados con el fin de obtener

respuestas que revelan el sistema operativo en uso en el equipo víctima. Desde este enfoque implica la comunicación directa con la víctima, no es sigiloso lo más mínimo, pero puede ser muy eficaz.

4.1.1.2. Escaneo SYN

El tipo de análisis a menudo se hace primero en contra de un sistema, es un escaneo TCP SYN, también conocido como un escaneo de sigilo o un análisis de medio abierto. Un escaneo SYN es el tipo más común por varias razones:

- Es muy rápido y fiable.
- Es preciso en todas las plataformas, independientemente de la aplicación sobre TCP.
- Es menos ruidoso que otras técnicas de escaneo.

El escaneo TCP SYN se basa en el proceso de negociación de tres vías para determinar qué puertos están abiertos en un host de destino. El atacante envía un paquete SYN TCP paquete a un rango de puertos en la víctima, como si tratara de establecer un canal para la comunicación normal en los puertos.

Una vez que este paquete es recibido por la víctima, una de las pocas cosas que pueden suceder es como se muestra en la Figura posibles resultados de un escaneo TCP SYN.

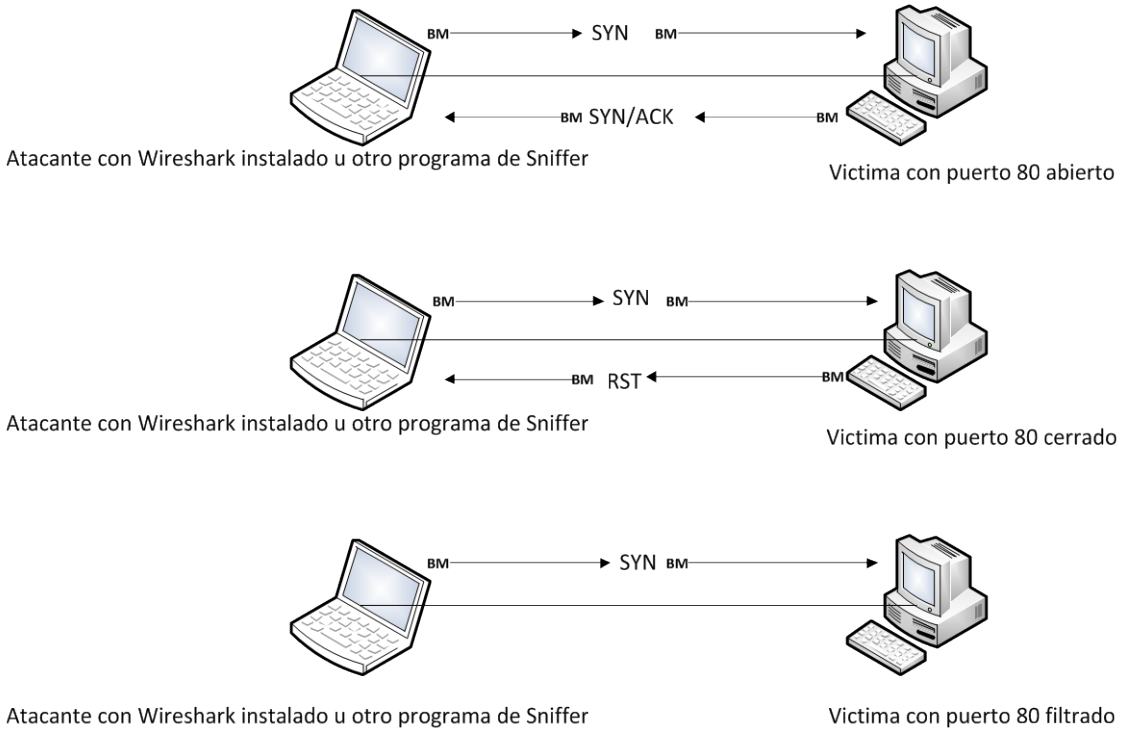


Figura 1 Posibles resultados de un escaneo SYN

Si un servicio en la máquina de la víctima está escuchando en un puerto que recibe el paquete SYN, es la respuesta al atacante con un paquete TCP SYN / ACK, la segunda parte de la conexión TCP. Entonces, el atacante sabe que el puerto está abierto y un servicio está escuchando en él. En circunstancias normales, un TCP ACK final se enviará a fin de completar el protocolo de enlace de conexión, pero en este caso, el atacante no quiere que eso suceda, ya que no se comunica con el host más en este punto. Por lo tanto, el atacante no intenta para completar la conexión TCP.

Si el servicio no está escuchando en un puerto de la máquina, el atacante no recibirá un paquete SYN / ACK. Dependiendo de la configuración del sistema operativo de la víctima, el atacante podría recibir un paquete RST, a cambio, lo que indica que el puerto está cerrado.

Asimismo, el atacante puede recibir ninguna respuesta en absoluto. Eso podría significar que el puerto está filtrado por un dispositivo intermedio, como un firewall o el propio anfitrión. Por otro lado, podría ser simplemente que la respuesta se ha perdido en el tránsito. Este resultado general indica que el puerto está cerrado, pero en esta última instancia, no son concluyentes.

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

La defensa más eficaz contra los sniffing es a través de protocolos de cifrado como **SSL** y **SSH**. Sin embargo, los últimos paquetes **dsniff** y **Ettercap** contienen técnicas para engañar el cifrado, esto se le conoce como un ataque MITM Man-in-the-middle.

La misma técnica se puede aplicar a los protocolos de cifrado, cuando un atacante crea un servidor que responde a las peticiones de los clientes por ejemplo, el servidor responde a una solicitud de https://www.servidor.com. Un usuario se pone en contacto con esta máquina falsamente creyendo que han establecido una sesión encriptado con Amazon.com. Al mismo tiempo, el atacante en contacto con el www.servidor.com real y se hace pasar por el usuario. El atacante juega dos papeles, descifrar los datos de entrada del usuario y volver a cifrar para la transmisión a su destino original.

En teoría, los protocolos de cifrado tienen defensas contra este. Un servidor que dice ser Ejemplo.com tiene que demostrar que sí es Ejemplo.com. En la práctica, la mayoría de los usuarios ignoran esto. Los ataques MITM han demostrado ser muy efectivo cuando se usa en el campo.

4.1.1.4. Cracking

Herramientas tales como **dsniff** y **Ettercap** capturan contraseñas sin cifrar y contraseñas encriptados.

En teoría, la captura de contraseñas encriptados no sirve para nada. Sin embargo, a veces las personas eligen contraseñas débiles por ejemplo, palabras del diccionario y sólo toma unos segundos para que un atacante pueda ir a través de un diccionario de 100.000 palabras, la comparación de la forma encriptado de cada palabra del diccionario contra la contraseña cifrada. Si se encuentra una coincidencia, el atacante ha descubierto la contraseña.

Estos programas descifran contraseñas ya existentes. Herramientas como dsniff y Ettercap simplemente sacan las contraseñas encriptados de tal forma que estas herramientas pueden leer.

4.1.1.5. ARP Spoofing

Cuando se trata de controlar el tráfico en una red conmutada, es un grave problema:

El interruptor se limita el tráfico que pasa por encima de su tramo de la red. Interruptores mantienen una lista interna de las direcciones MAC de los hosts que están en cada puerto. El tráfico sólo se envía a un puerto si el host de destino se registra como estar presente en ese puerto.

Es posible sobrescribir la memoria caché de ARP en muchos sistemas operativos, que permiten asociar la dirección MAC con la dirección IP por defecto sniffing como puerta de enlace. Esto haría que todo el tráfico saliente desde el host de destino se entregará a un sniffing.

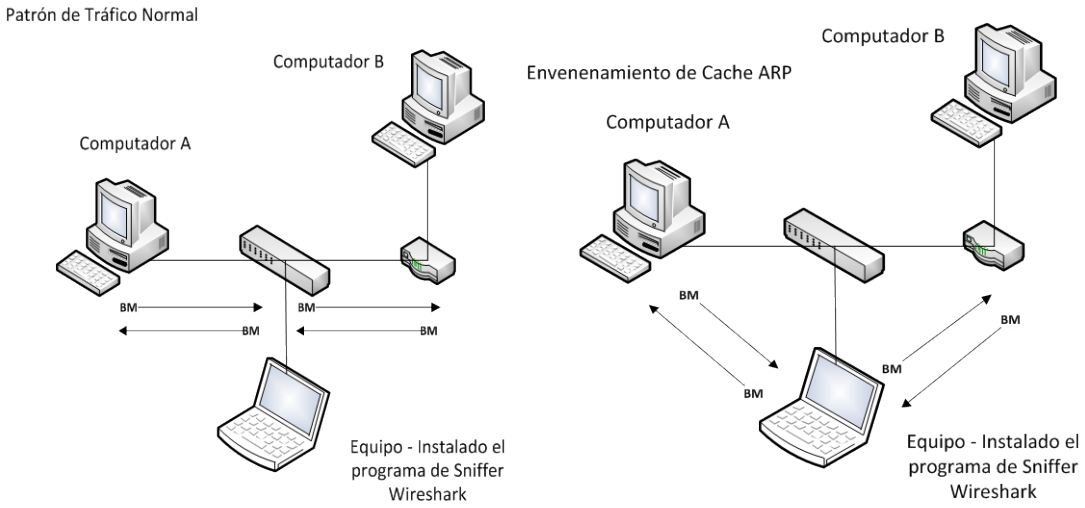
Añadir manualmente una entrada de tabla ARP para que la puerta de enlace predeterminada real, pueda asegurar que el tráfico que se envían al destino real y para asegurarse de que tienen el reenvío IP habilitado.

Muchas redes de cable módem son vulnerables a este tipo de ataques, debido a que la red de cable módem es esencialmente una red Ethernet con cable módems que actúan como puentes.

¿Cómo funciona ARP Spoofing?

Envenenamiento de la caché ARP, a veces llamado ARP spoofing, es el proceso de envío de mensajes ARP a un conmutador Ethernet o un router con falsas direcciones MAC en la capa 2, con el fin de interceptar el tráfico de otro equipo.

Envenenamiento de la caché ARP es una forma avanzada de aprovechar el cable en una red conmutada. Es comúnmente usado por los atacantes para enviar paquetes falsos dirigidos a los sistemas clientes con el fin de interceptar el tráfico o causar la denegación de servicios ataques (DoS) sobre un objetivo. Sin embargo, también puede ser una forma legítima para capturar los paquetes de una máquina en una red conmutada.



4.1.2. Asegurar los paquetes de datos en una Red de los Sniffers

Existen diferentes maneras, funciones más amigables para ayudar a proteger los paquetes de datos de la red de un intruso determinado.

4.1.2.1. Utilizar el cifrado

Afortunadamente para el estado de seguridad de red, cuando se utiliza correctamente, la encriptación es la bala de plata que hará que un sniffer de paquetes sea inútil.

El uso de encriptación suponiendo que su mecanismo es válido es frustrar cualquier atacante de intentar monitorear pasivamente la red.

Muchos protocolos de red existentes tienen su contraparte que se basan en el cifrado fuerte y que todos los mecanismos que abarca por ejemplo, IPSec y OpenVPN proporcionan esta para todos los protocolos. Desafortunadamente, Seguridad IP (IPSec) no se usa ampliamente en el Internet.

4.1.2.2. Encriptación

La encriptación sería la codificación la información de archivos o de un paquete de datos para protegerla para que no pueda ser descifrado en caso de ser interceptado por terceros mientras esta información viaja por la red.

La encriptación es el proceso que utilizan complejas fórmulas matemáticas para volver ilegible la información considerada importante, una vez encriptado los datos sólo puede leerse aplicándole una clave.

La encriptación de los datos se hace cada vez más necesaria debido al aumento de los robos o capturas de la información que circula por la red.

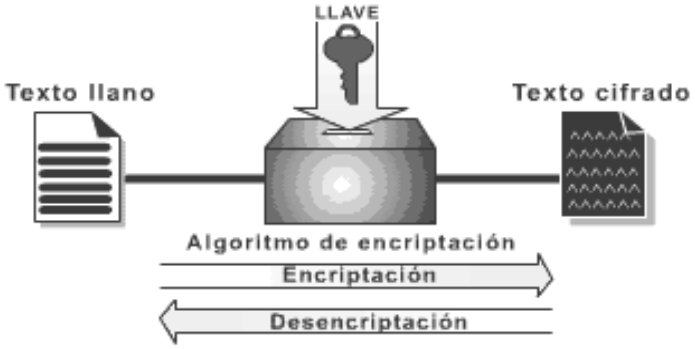


Figura 2 Imagen que explica cómo funciona la encriptación

4.1.2.3. Sistemas de encriptación

La encriptación de la información, está basada en la ciencia de la criptología, que ha sido usada a través de la historia con frecuencia. Antes de la era digital, hacían uso de la criptología, con mensajes codificados eran los gobiernos, particularmente para propósitos militares.

En la actualidad la mayoría de los sistemas de criptografía son aplicables a la información en los ordenadores, simplemente porque los algoritmos son demasiados complejos para ser calculados por los seres humanos.

Muchos de los sistemas de encriptación pertenecen a dos categorías:

- Encriptación de clave simétrica.
- Encriptación de clave pública.

4.1.2.4. Clave simétrica

En este tipo de encriptación, cada ordenador tiene una clave secreta como si fuera una llave que puede utilizar para encriptar un paquete de información, antes de ser enviada sobre la red a otro ordenador. Las claves simétricas requieren que sepan los ordenadores que van a estar comunicando entre sí para poder instalar la clave en cada uno de ellos.

Podemos entender una clave simétrica, como un código secreto que deben saber los ordenadores que se están comunicando para poder decodificar la información a su llegada.

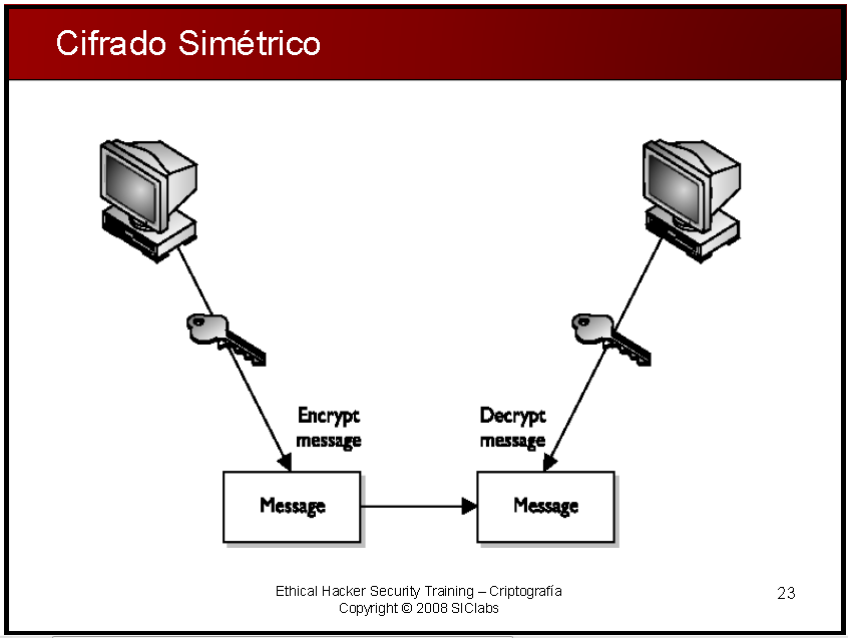


Figura 3 Cifrado Simétrico - Imagen tomada de Ethical Hacker Security Training

4.1.2.4.1. Debilidades del Cifrado Simétrico

- Crece el número de claves secretas en una proporción igual a n2 para un valor n grande de usuarios lo que imposibilita usarlo

- Mala gestión, distribución de claves
- No existe posibilidad de enviar de forma segura una clave a través de un medio inseguro
- No tiene firma digital
- Es posible autenticar el mensaje mediante una marca, pero no es posible firmar digitalmente el mensaje

4.1.2.4.2. ¿Entonces por qué se utiliza?

- La velocidad de cifrado es muy alta
- Con claves pequeñas obtendremos una alta seguridad
- La no linealidad del algoritmo hace que el único ataque factible sea fuerza bruta

4.1.2.4.3. Algoritmos de cifrado Simétrico.

- **DES** (Data Encryption Standard)
- **3DES** cifra el mensaje original 3 veces, mejora del DES
- **IDEA** International Data Encryption Algorithm
- **RC2** Cifrador en bloque de clave variable
- **RC5** es una unidad de cifrado por bloques notable por su simplicidad
- **Blowfish** – 5 veces más rápido que DES Cifrador tipo Feistel de clave variable

4.1.2.5. Cifrado Asimétrico

La operación característica del cifrado asimétrico es la exponenciación. Cifrado con clave pública de destino para intercambio de clave de sesión. Cifrado con clave privada de origen para firma digital

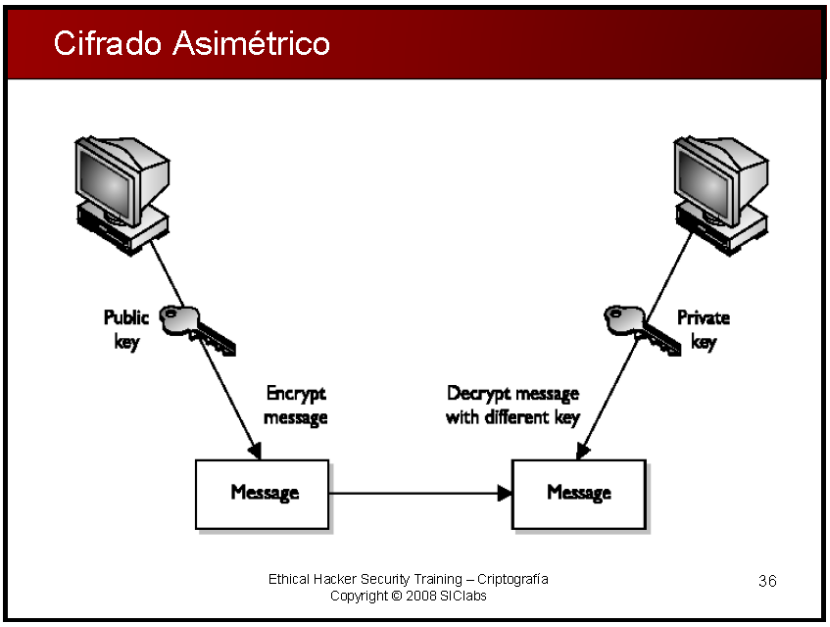


Figura 4 Cifrado Asimétrico - Imagen tomada de Ethical Hacker Security Training

4.1.2.5.1. Clave pública

Este método usa una combinación de una clave privada y una clave pública. La clave privada solo la sabe un ordenador, mientras que la clave pública es entregada por el ordenador a cualquier otro ordenador que quiere realizar una comunicación. Para decodificar un mensaje encriptado, un ordenador debe hacer uso de la clave pública, entregada por el ordenador original, y su propia clave privada.

Una clave pública de encriptación es muy popular **PGP** (*Pretty good Privacy*) que permite encriptar casi todo

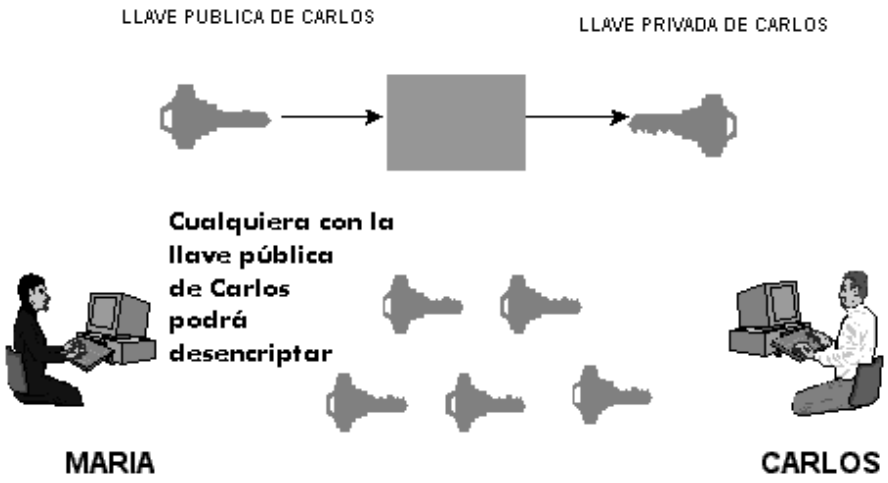


Figura 5 Utilización de Llaves Públicas Y Privadas

4.1.2.5.2. Combinación de Clave Simétrica Y Clave Pública

Muchos sistemas usan una combinación de clave pública y simetría. Cuando dos ordenadores inician una sesión segura, un ordenador crea una clave simétrica y la envía al otro ordenador usando encriptación de clave pública.

Los dos ordenadores pueden entonces comunicarse entre ellos usando una encriptación de clave simétrica. Una vez que la sesión ha finalizado, cada ordenador descarta la clave simétrica usada para esa sesión. Cualquier sesión adicional requiere que una nueva clave simétrica sea creada, y el proceso es repetido.

4.1.2.6. SSL Secure Sockets Layer

Una implementación de la encriptación de clave pública es **SSL** (*Secure Sockets Layer*). Originalmente desarrollada por Netscape, SSL es un protocolo de seguridad para Internet usado por navegadores y servidores Web para transmitir información sensitiva. SSL se ha convertido en parte de un protocolo de seguridad general llamado **TLS** (*Transport Layer Security*).

SSL proporciona servicios de autenticación y cifrado, y también se puede utilizar como una red privada virtual (VPN). Este proxy transparente se puede

configurar para descifrar la conexión SSL, de la aspiración y luego se vuelve a cifrar. Cuando esto sucede, se solicita al usuario con un cuadro de diálogo que indica que el certificado SSL no fue emitido por una autoridad de confianza.

El problema es que la mayoría de los usuarios ignoran las advertencias y continuar de todos modos.

4.1.2.7. Algoritmos de encriptación usando Funciones Hash

Una de las aplicaciones más interesantes de la criptografía es la posibilidad de añadir una firma digital: autenticación completa. Es un modelo de cifrado asimétrico con clave pública.

Con los sistemas de clave simétrica esto era inviable o bien muy complejo. Dado que los sistemas de clave pública son lentos, en vez de firmar digitalmente el mensaje completo, se incluirá una operación con la clave privada del emisor sobre un hash de dicho mensaje.

Para comprobar la identidad en destino se descifra la firma R con la clave pública del emisor E Al mensaje en claro recibido M se le aplica la misma función hash que en emisión. Si los valores son iguales, la firma es auténtica y el mensaje íntegro

4.1.2.7.1. Principales algoritmos de Hash más usados

- **MD5 Message Digest 5** Algoritmo sencillo basado en mejoras de MD4 y MD2
- **SHA-1 Secure Hash Algorithm** similar a MD5 pero más lento y fuerte a ataques, tiene una complejidad algorítmica

4.1.2.8. SSH

Secure Shell SSH es un protocolo de red para la comunicación segura de datos, servicios de shell remoto y otros servicios de red segura entre dos computadoras en red que se conecta mediante un canal seguro a través de una red insegura.

Protocolos, que envían la información, en particular, las contraseñas, en texto plano, haciéndolas susceptibles a la intercepción y divulgación mediante el análisis de paquetes. El cifrado que se utiliza por SSH está diseñado para garantizar la confidencialidad e integridad de datos a través de una red no segura, como la Internet.

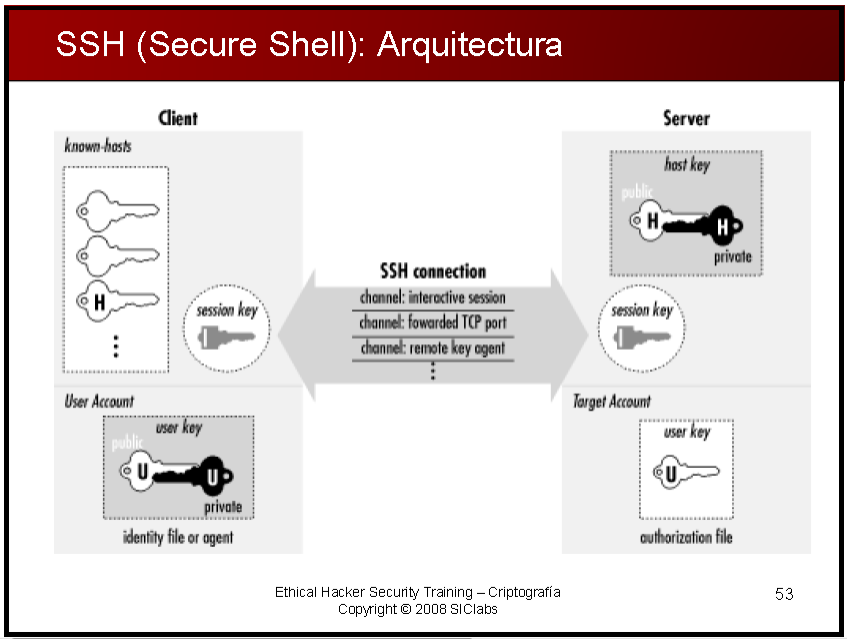


Figura 6 SSH Secure Shell – Imágen tomada de Ethical Hacker Security Training

SSH se trata de un cliente y el servidor que utiliza criptografía de clave pública para proporcionar sesiones encriptados.

SSH ha recibido una amplia aceptación como el mecanismo de seguridad para acceder a sistema remotos de forma interactiva. La versión original de SSH se

convirtió en una empresa comercial y, aunque la versión original sigue siendo de libre disposición, la licencia se ha vuelto más restrictiva.

Una versión libre de SSH compatibles con el software **OpenSSH** desarrollado por el proyecto **OpenBSD** OS, se puede obtener desde la siguiente dirección web www.openssh.com.

Figura 7 OpenSSH - Imagen tomada de la página web oficial de http://www.openssh.com/

PuTTY es una alternativa gratuita para el software comercial SSH para Windows. Originalmente desarrollado para los protocolos de texto plano tales como Telnet, **PuTTY** es muy popular entre los administradores del sistema y se puede descargar de la siguiente dirección web.

www.chiark.greenend.org.uk/ ~ sgtatham / putty /.

4.1.2.9. Seguridad IP (IPSec)

IPSec es un protocolo a nivel de red que incorpora la seguridad en los protocolos IPv4 e IPv6 directamente en el nivel de paquetes, mediante la ampliación de la cabecera del paquete IP.

Esto permite la posibilidad de encriptar cualquier protocolo de capa superior. Se ha incorporado en dispositivos de enrutamiento, cortafuegos y los clientes para asegurar las redes de confianza entre sí. IPSec ofrece varios medios para la autenticación y cifrado, el apoyo a una gran cantidad de cifrado de llaves públicas de autenticación y cifrado de claves simétrico. Puede funcionar en

modo de túnel para proporcionar una nueva cabecera IP que las máscaras de la fuente original y de destino, además de los datos transmitidos.

4.1.2.10. OpenVPN

OpenVPN es un túnel SSL VPN de protocolo, que permite cifrar tanto el contenido de un paquete y sus cabeceras IP. OpenVPN utiliza un único puerto TCP o UDP, por lo tanto, puede ser más fácil de usar en entornos difíciles con NAT y las arquitecturas de cortafuegos. Además, puede actuar como un puente de red virtual en una capa de nivel 2.

4.2. Manifestar la importancia y el uso de la herramienta Wireshark

Con los diferentes usos que tiene la herramienta Wireshark se demuestra la gran importancia en su implementación y utilización para solucionar diferentes necesidades y problemas que se presentan o puedan presentar en una red, para que los administradores de redes o simplemente usuarios sepan resolver diferentes tipos de dificultades.

4.2.1. Uso de Wireshark para Solucionar problemas de red

El uso de Wireshark para solucionar problemas de red es saber cómo funciona la red en condiciones normales, lo que le permitirá reconocer con rapidez las operaciones inusuales y anormales que se puedan presentar.

Una forma de saber cómo funciona su red normalmente es usar un programa de sniffer en varios puntos de la red. Esto permitirá tener una idea de los protocolos que se ejecutan en la red, los dispositivos en cada segmento, y los ordenadores que envían y reciben los datos con mayor frecuencia.

Una vez que se tiene claro de cómo funciona una red a la que puede desarrollar una estrategia de manera que pueda solucionar los problemas de la red.

Esto puede abordar el problema metódicamente y resolverlo con una interrupción mínima para los clientes o usuarios. Con la solución de problemas, algunos minutos dedicados a la evaluación de los síntomas puede ahorrar horas de tiempo perdido en seguimiento por el mal enfoque del problema.

Un buen enfoque para solucionar problemas de red consiste en lo siguientes pasos:

1. Reconocer los síntomas que producen el problema
2. Definir el problema
3. Analizar el problema
4. Aislar el problema
5. Identificar y probar la causa del problema
6. Resolver el problema
7. Verifique que el problema ha sido resuelto

4.2.2. Uso de Wireshark en una arquitectura de red

Examinar en algunas de las arquitecturas de red y puntos críticos de Wireshark. La ubicación de la red es fundamental para un análisis adecuado y la solución de problemas. Lo más importante es asegurarse de que están en el segmento de red adecuado.

4.2.3. Uso de Wireshark para Administración de Sistemas

Los administradores de sistemas son conocidos por preguntar si hay algún problema con la red, y los administradores de red se caracterizan por decir que el problema está dentro del sistema.

En medio de este de problemas de culpa la verdad está a la espera de ser descubierto por Wireshark.

4.2.4. Uso de Wireshark para la Administración de Seguridad

¿Es este protocolo seguro? Una de las tareas más comunes de los administradores de seguridad, Wireshark es la herramienta ideal para su uso.

Una de las características Wireshark más populares y útiles es el reensamblaje de paquetes, lo que nos permite ver el contenido de los datos intercambiados. Para protocolos como Telnet y FTP, Wireshark muestra claramente el nombre de usuario y contraseña para la conexión, sin ningún tipo de montaje.

Para los protocolos desconocidos, el reensamblaje de paquetes se puede utilizar el montaje, capturar el tráfico a través de Wireshark o cualquier otra herramienta y luego cargar el archivo de captura en Wireshark y botón derecho del ratón en cualquier paquete de la conexión. Seleccione la opción TCP Stream, se abrirá la ventana con todas las comunicaciones que se produjeron en ese período de sesiones. Lo puede ayudar a seleccionar la opción ASCII, y si el protocolo es ruidoso, puede elegir una conversación emisor, receptor, o de toda la pantalla.

4.2.5. Uso de Wireshark como un IDS en una red

A pesar de que existen herramientas propiamente especializados de código abierto para la detección de intrusos en redes. Wireshark, excepto para usar como un sistema IDS, sería capaz de alertar sobre cualquier otro criterio. Considere de Wireshark las siguientes reglas para la detección de intrusos:

Conexiones de base de datos hacia su base de datos desde otros sistemas como sus servidores Web.

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

Los intentos de utilizar una conexión remota hacia su escritorio (RDC) desde el exterior de red o el uso de Wireshark como un escuchador de las conexiones a una dirección IP no utilizada.

4.2.6. Uso de Wireshark como un detector para la transmisión de información privilegiada

Toda empresa tiene información confidencial y patentada, no hay ninguna razón por la cual no se puede usar Wireshark para detectar la transmisión de información.

Podría utilizar Wireshark para capturar todo el tráfico saliente en un lapso del puerto y luego usar Wireshark con la función buscar paquetes. Sin embargo, esto podría crear una gran cantidad de tráfico.

Para reducir la cantidad de tráfico capturado, puede utilizar la captura de filtros para excluir el tráfico en los que no se esperan que la información de propiedad sea transferida a través de las consultas de DNS y el tráfico de red interna.

4.3. Describir el procedimiento para la implementación de la herramienta Wireshark para su utilización en redes.

Todo el procedimiento necesario para la implementación y utilización de Wireshark esta resumida en los siguientes pasos a detallados a continuación:

01.- Cumplir con los requisitos especificados para su instalación

02.- Disponer de una conexión de Red para su implementación

03.- Protocolos utilizados en la red sean soportados por Wireshark

04.- Sistemas Operativos sean compatibles con la versión de Wireshark

05.- Descargar o disponer el software de Wireshark + librerías

06.- Obtener permisos de Usuario en el sistema

07.- Instalación de Wireshark en equipos Host

08.- Seleccionar la interfaz de red que utilizaremos

09.- Seleccionar la ubicación en la red en donde se va a trabajar

4.3.1. Paso 1 - Cumplir con los requisitos especificados para su instalación

Requerimientos de Sistema para instalar Wireshark

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

- Procesador a 400 MHz o más rápido
- 128 MB de memoria RAM o superior
- 80 MB de espacio de almacenamiento disponible solamente para instalación
- Para guardar capturas de paquetes de datos se requieren mayor cantidad de espacio en disco duro
- Tarjeta de red NIC que admita modo promiscuo
- WinPcap controlador de captura
- Software Wireshark

4.3.2. Paso 2 - Disponer de una conexión de Red para su implementación

Requerimientos de Red para la Implementación de Wireshark

Para la implementación de la herramienta de wireshark en una red es necesario contar con una conexión a red.

Red puede estar formada físicamente con equipos reales o como virtualmente con equipos virtuales corriendo dentro de un mismo equipo

Utilizando cualesquier topología de red conocida

Conformada con un equipo o más, aunque se puede probar en un solo sistema.

La red puede estar conectada mediante cableado estructurada e inalámbrica.

Wireshark permite capturar paquetes de datos remotamente.

4.3.3. Paso 3 - Protocolos utilizados en la red sean soportados por Wireshark

Protocolos soportados

Cuando un analizador de red lee los datos de la red necesita saber cómo interpretar lo que ve y luego mostrar los resultados en un formato fácil de leer. .Esto se conoce como protocolo de decodificación. A menudo, el número de protocolos que un sniffer puede leer y mostrar determina su fuerza, por lo que la mayoría de los sniffers comerciales puede admitir cientos de varios protocolos. Wireshark es muy competitivo en esta área, con su actual soporte de más de 750 protocolos. Nuevos protocolos se están agregando constantemente por diversos colaboradores en el proyecto Wireshark.

Decodifica el protocolo, también conocido como disectores, se puede añadir directamente en el código o como complementos.

4.3.4. Paso 4 - Sistemas Operativos sean compatibles con la versión de Wireshark

Sistemas Operativos con sus plataformas Compatibles:

- Apple Mac OS X
- Microsoft Windows
- Debian GNU/Linux
- FreeBSD
- Gentoo Linux
- HP-UX
- Mandriva Linux
- NetBSD
- OpenPKG
- Red Hat Fedora/Enterprise Linux

- rPath Linux
- Sun Solaris/i386
- Sun Solaris/Sparc
- Canonical Ubuntu
- Novell / OpenSUSE, SUSE Linux

4.3.5. Paso 5 - Descargar o disponer el software de Wireshark + librerías

4.3.5.1. WinPcap

WinPcap consiste en un controlador, que extiende el sistema operativo para proporcionar acceso de bajo nivel de red, y una biblioteca que se utiliza para acceder fácilmente a las capas de red de bajo nivel, esta permite a las aplicaciones capturar y transmitir paquetes de red sin pasar por la pila de protocolos, y tiene otras características útiles, como es un capturador de paquetes y motor de filtrado de código fuente abierto, incluyendo filtrado de paquetes a nivel kernel, un motor de estadísticas de red y apoyo para la captura de paquetes remotos.

Información tomada el 20/09/2011 - 15:00pm de la página web oficial de WinPcap http://www. winpcap.org /

El controlador de captura WinPcap es la implementación de Windows del pcap capturador de paquetes de aplicaciones de programación y de interfaz (API). En pocas palabras, este conductor interactúa con el sistema operativo para capturar los datos en bruto del paquete, se aplican filtros, y cambiar la tarjeta de entrada y salida de modo promiscuo.

4.3.5.2. ¿Cómo Obtener la librería WinPcap para Wireshark?

Aunque se puede descargar WinPcap por separado desde la siguiente dirección web.

http://www. winpcap.org /

Figura 8 WinPcap - Imagen tomada de la página web oficial de WinPcap http://www. winpcap.org/

Es mejor instalar WinPcap desde el paquete de instalación de Wireshark, ya que la versión incluida de WinPcap se ha probado para trabajar con Wireshark.

Figura 9 Descargar WinPcap para Windows - Imagen tomada de la página web oficial de WinPcap http://www. winpcap.org /

4.3.5.3. Cómo Obtener Wireshark Para Sistemas Windows

Figura 10 Wireshark - Imagen tomada de la página web oficial de Wireshark http://www.wireshark.org/

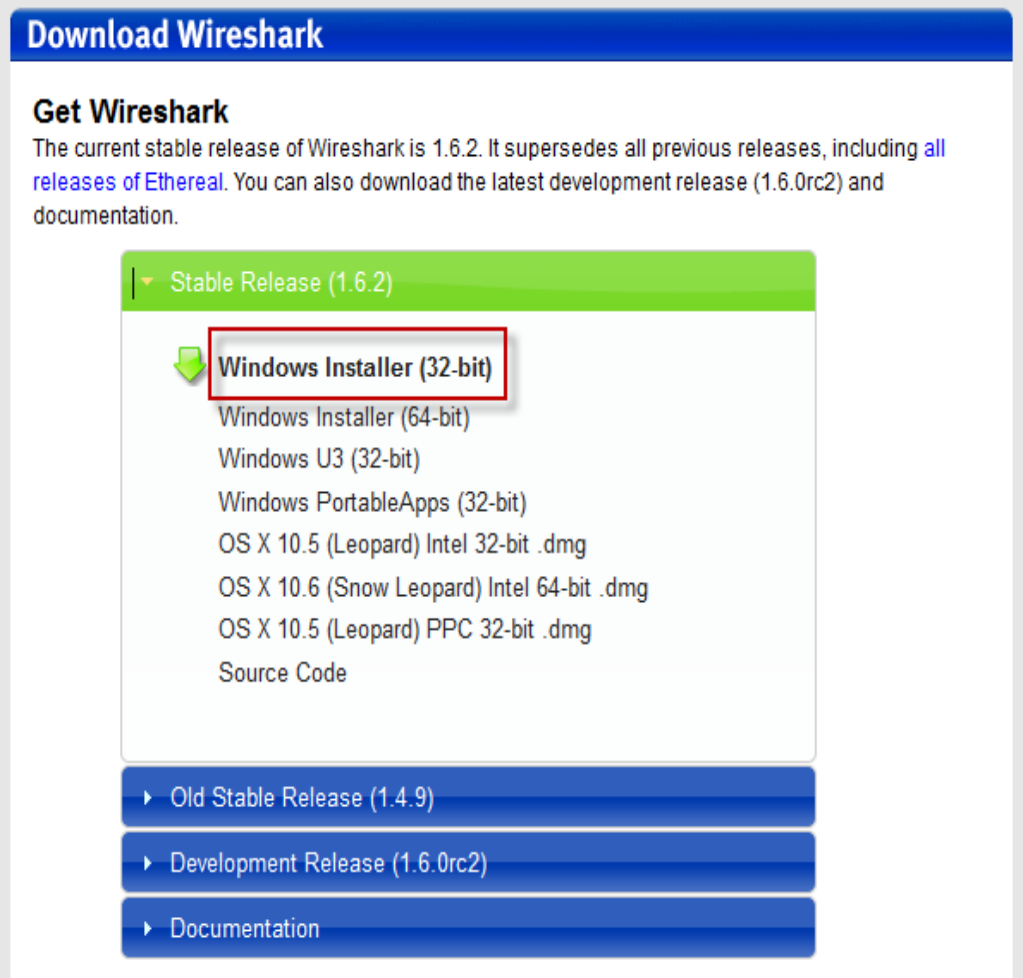


Figura 11 Descargar Wireshark para Windows - Imagen tomada de la página web oficial de Wireshark http://www.wireshark.org/

4.3.5.4. Obtener Wireshark para Sistemas Linux

Obtener los paquetes de instalación RPM para sistemas que tengan instalado como sistema operativo Linux, en este caso se demostrara como obtener Wireshark para Fedora versión 14.

Figura 12 Descargar Wireshark para Linux - Imagen tomada de la página web http://www.wireshark.org/ el día lunes 20 de septiembre del 2011 15:35 pm

En la figura de la izquierda se muestra los paquetes estándares de terceros, disponibles los links en la página web oficial de Wireshark.

Seleccionamos Red Hat / Fedora Linux damos clic para continuar.

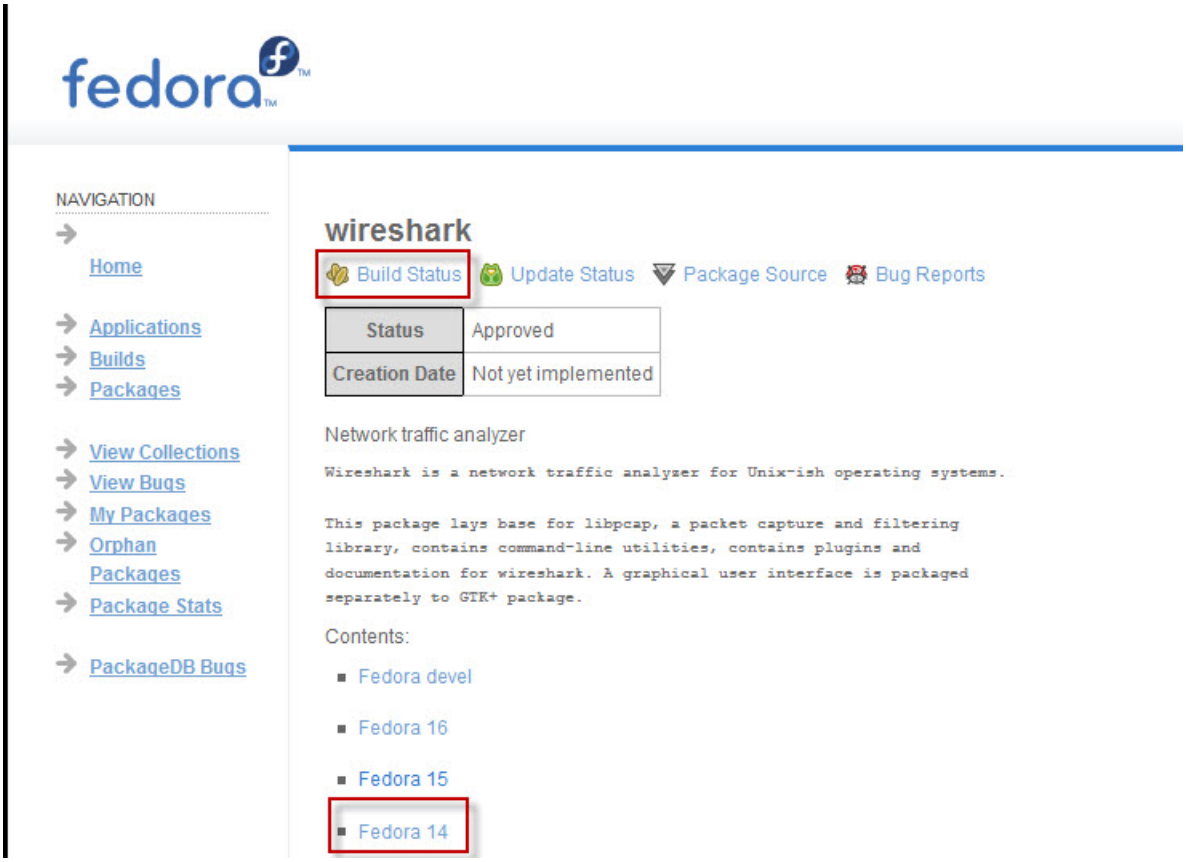


Figura 13 Imagen tomada de la página web https://admin.fedoraproject.org/pkgdb/acls/name/wireshark el día lunes 20 de septiembre del 2011 15:35 pm

En la siguiente pantalla seleccionamos la versión del sistema operativo Fedora, cabe recalcar que para el análisis y captura de paquetes de datos en una red trabajaremos con sistemas operativos Fedora 14 entones damos clic en Build Status para que nos muestre todos los paquetes disponibles construidos actualmente hasta la fecha actual.

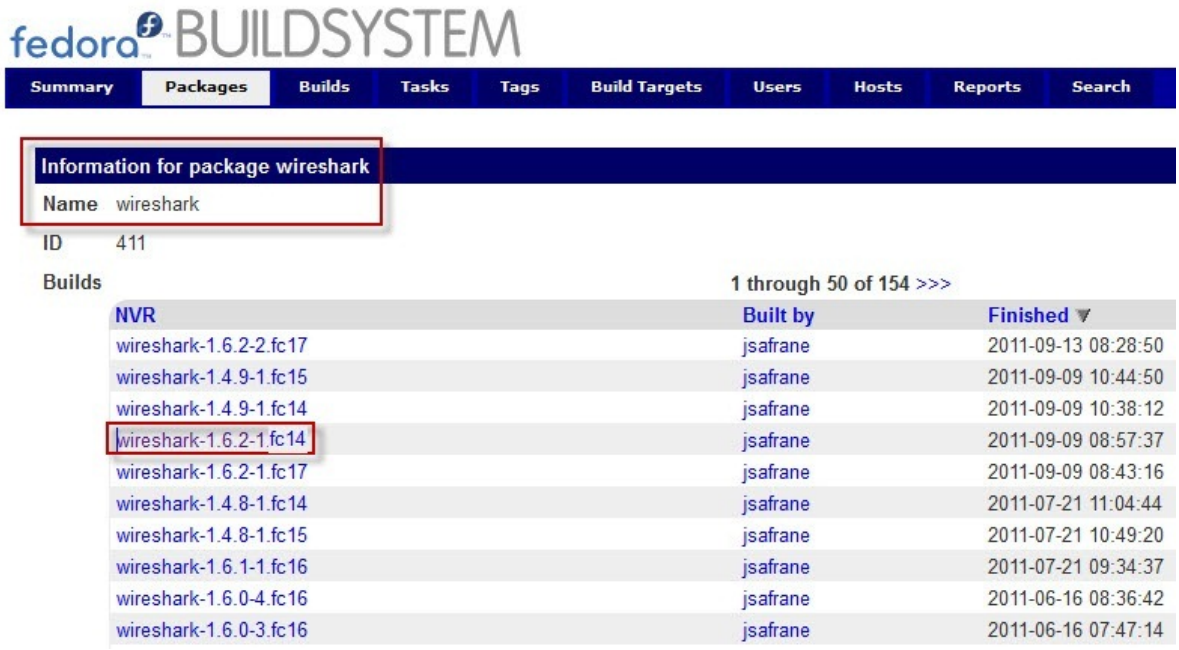


Figura 14 Listado de Paquetes de Wireshark para Fedora - Imagen tomada de la página web https://admin.fedoraproject.org/pkgdb/acls/name/wireshark el día lunes 20 de septiembre del 2011 15:35 pm

En la pantalla web observamos en la parte superior información de los paquetes de wireshark, seleccionamos wireshark 1.6.2.1 fc 14 damos clic para continuar.

Figura 15 Información del Paquete de Wireshark - Imagen tomada de la página web https://admin.fedoraproject.org/pkgdb/acls/name/wireshark el día lunes 20 de septiembre del 2011 15:35 pm

Seleccionamos los paquetes RPM dependiendo de la arquitectura disponible del equipo que pueden ser de 32 o 64 bits, necesitaremos el paquete RPM de

la herramienta wireshark mas con las interfaces wireshark-gnome y las dependencias necesarias que se muestran en el recuadro superior. Seleccionamos dando clic en cada uno de los links para comenzar su descarga.

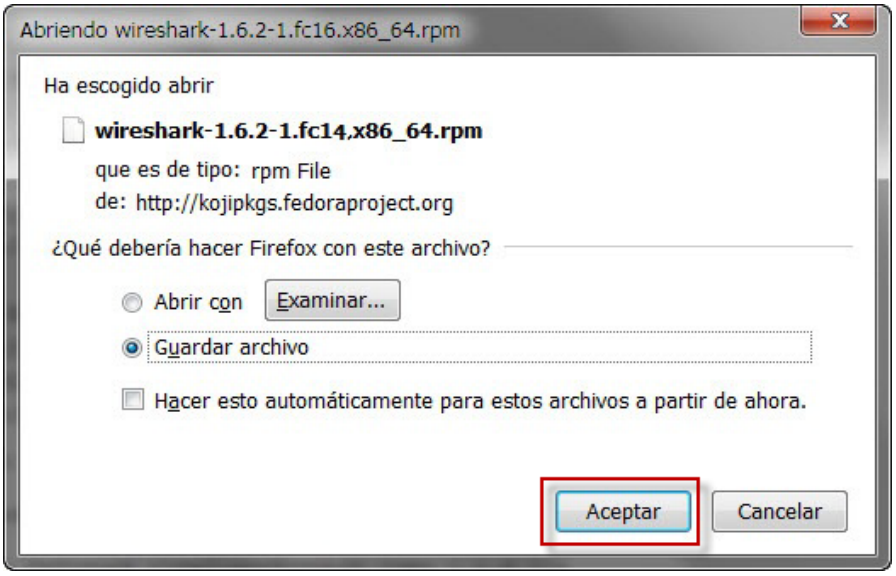


Figura 16 Ventana para abrir o guardar paquetes RPM para sistemas Linux

Guardamos en el equipo todos los paquetes RPM descargados de la página web https://admin.fedoraproject.org/pkgdb/acls/name/wireshark necesarios en el equipo para su posterior proceso de instalación de Wireshark.

4.3.6. Paso 6 - Obtener permisos de Usuario en el sistema

Si no se disponen de permisos de usuario en el sistema que se encuentra instalado Wireshark, lo más seguro es que no se podrá trabajar con la herramienta para el análisis y captura de paquete de datos en una red.

Para la instalación, configuración de wireshark, y los diferentes dispositivos de red que dispone el equipo, también son necesarios tener permisos de usuario, en caso de no tenerlos o no conseguirlos no es recomendable trabajar con la implementación y utilización de Wireshark.

4.3.7. Paso 7 - Instalación de Wireshark en equipos Host

Para la instalación en equipos con sistemas operativos Microsoft Windows se detalla paso a paso el procedimiento de instalación de Wireshark en el anexo número 1.

- Ver Anexo Número 1
- Instalación de Wireshark en sistemas Windows - Pagina 92

Para la instalación en equipos con sistemas Linux se detalla paso a paso el procedimiento de instalación de Wireshark en el anexo número 2.

- Ver Anexo Número 2
- Instalación de Wireshark en sistemas Linux - Pagina 99

4.3.8. Paso 8 - Seleccionar la interfaz de red que utilizaremos

Disponer de una interfaz de red en modo promiscuo es uno de los requisitos, ahora seleccionaremos la interfaz de red que emplearemos o necesitamos, wireshark desde su interfaz gráfica permite seleccionar los dispositivos de red disponibles para realizar análisis y capturas de paquetes de datos. Esto depende del equipo donde se va a trabajar con Wireshark, porque los equipos disponen de diferentes tipos de dispositivos de interfaces de red.

Figura 17 Imagen que muestra un listado de dispositivos de interfaces de red disponibles

Figura 18 Imagen tomada de Wireshark que muestra la lista de interfaces disponibles

4.3.9. Paso 9 - Seleccionar la ubicación en la red en donde se va a trabajar

Cuando la solución de problemas de red, puede moverse entre diferentes armarios de cableado o incluso edificios diferentes. Por esta razón, es beneficioso ejecutar Wireshark en un ordenador portátil.

4.3.9.1. Sniffing alrededor de Hubs

Sniffing en una red que tiene instalado un hub es importante para cualquier analista de paquetes.

El tráfico enviado a través de un concentrador pasa por todos los puertos conectados a ese hub. Por lo tanto, para analizar el tráfico que discurre por un ordenador conectado a un concentrador, todo lo que necesitas hacer es conectar un analizador de paquetes a un puerto vacío en el Hub.

Wireshark será capaz de ver todas las comunicaciones hacia y desde ese equipo, así como todas las comunicaciones entre cualquier otro dispositivo conectado a ese hub.

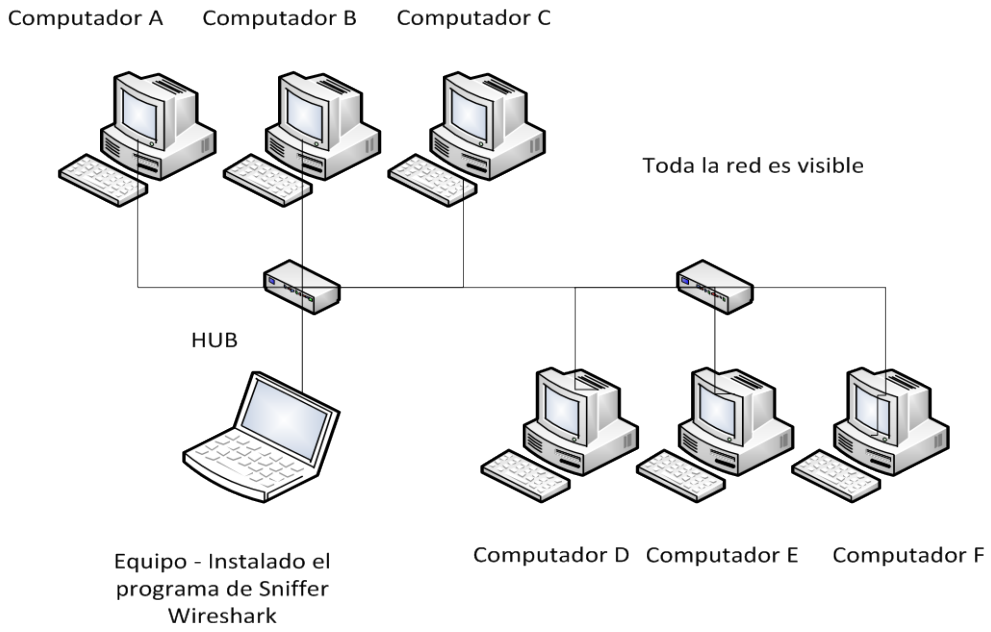


Figura 19 Sniffing con Wireshark en un concentrador de red ofrece una visibilidad ilimitada de toda la red

4.3.9.2. Sniffing en un entorno de Switch

Los Switches es el tipo más común de dispositivo de conexión que se utiliza en entornos de red modernos. Ellos proporcionan una forma eficiente de transporte de datos a través de diferentes tipos de tráfico como broadcast, unicast, y multidifusión. Adicional los Switches permiten la comunicación full-duplex es decir, que las máquinas pueden enviar y recibir datos simultáneamente.

Desafortunadamente para los analistas de paquetes, los Switches añaden un nuevo nivel de complejidad. Cuando se conecta un sniffer a un puerto en un Switch, se puede ver sólo el tráfico de difusión y el tráfico transmitido y recibido por su equipo.

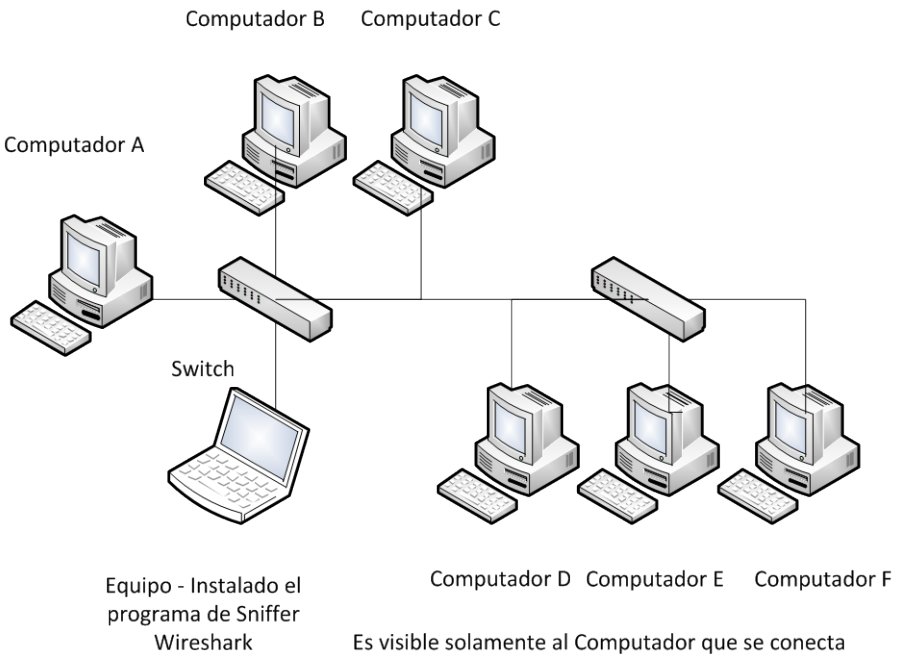


Figura 20 La visibilidad en una red conmutada se limita al puerto que se conecta.

4.3.9.3. Sniffing en un Entorno Router

Todas las técnicas para aprovechar el cable en una red conmutada se encuentran disponibles en redes enrutadas, En entornos enrutados es importante la colocación de rastreadores cuando se está solucionando un problema que abarca varios segmentos de red.

El dominio de un dispositivo de transmisión se extiende hasta que se llega a un router, punto en el cual se entrega el tráfico. En situaciones donde los datos deben atravesar varios routers, es importante analizar el tráfico en todos los lados del router.

Cuando el escenario es amplio, entones cuando se trata de varios routers y segmentos de red, entonces se debe mover el programa de sniffer Wireshark instalado en un equipo portátil para obtener una imagen completa.

4.4. Proceso de captura de los paquetes de datos mediante filtros de búsqueda utilizando Wireshark.

4.4.1. ¿Dónde Realizar la Captura de Datos?

El primer paso para poder conocer la red será definir dónde analizar el tráfico. Además, Wireshark permite analizar, capturar el tráfico remotamente. La pregunta que surge es en dónde instalarlo.

A pesar de parecer lógico instalar Wireshark en el propio servidor de ficheros para analizar el tráfico que transita por ese segmento de red, nos encontraremos con situaciones en las cuales no podamos tener acceso físico al servidor o simplemente, por motivos de seguridad.

Existen algunas alternativas en el uso de técnicas que permitan llevar a cabo una captura de tráfico sin necesidad de portar Wireshark al propio servidor.

4.4.2. Modo Promiscuo

Para poder capturar paquetes en una red, se necesita una tarjeta de interfaz de red (NIC) que soporta un controlador en modo promiscuo. El modo promiscuo es lo que permite a una tarjeta ver todos los paquetes que cruzan en la red.

Podemos asegurar que la captura de todo el tráfico mediante el modo promiscuo de la NIC. Cuando funciona en modo promiscuo, la tarjeta pasa a cada paquete que se ve en el procesador principal, independientemente de la dirección. Una vez que el paquete llega a la CPU, entonces puede ser tomado por una aplicación de sniffing de paquetes para su análisis y captura.

NIC más modernos soportan el modo promiscuo, y Wireshark incluye los controladores de **libpcap** / **WinPcap**, que le permite pasar su tarjeta de red en modo promiscuo directamente desde la interfaz gráfica de Wireshark.

Se debe tener un sistema operativo que soporte el uso de modo promiscuo. La mayoría de sistemas operativos no permiten utilizar una tarjeta de red en modo promiscuo si no se disponen privilegios de usuario en un sistema, entonces no se debe realizar cualquier tipo de captura de paquetes en la red.

El modo promiscuo de una NIC no es necesario únicamente, para un programa sniffer cuando solamente se desea ver el tráfico que se envía directamente en la red. (Sanders, 2011)

4.4.3. Capturar los paquetes de datos

Para la captura de paquetes de datos en primer lugar se deben obtener los paquetes con Wireshark, para esto se debe realizar la captura de los primeros paquetes empleando el siguiente procedimiento a continuación.

1. Abrir Wireshark. Una vez que se encuentre instalado con éxito Wireshark en su sistema, para comenzar a familiarizarse con la herramienta. Puede finalmente llegar a abrir por completo el sniffer de paquetes y ver su funcionamiento. Wireshark no es muy interesante la primera vez que se ejecuta.

2. Desde el menú principal en el menú desplegable, seleccione Capturar y luego Interfaces. Usted debe ver a un diálogo que muestra las distintas interfaces que pueden ser utilizados para capturar los paquetes de datos, junto con sus respectivas direcciones IP.

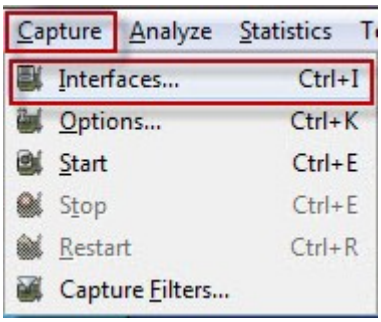


Figura 21 Imagen obtenida de Wireshark muestra el menú Captura/Interfaces.

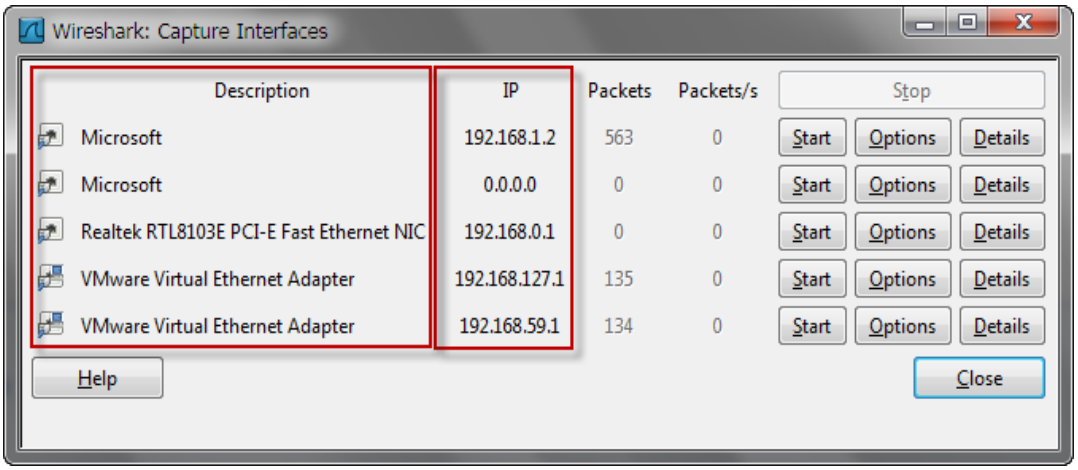


Figura 22 Imagen obtenida de Wireshark muestra en pantalla las interfaces de captura con su IP

3.- Elegir la interfaz que desea utilizar, como se muestra en la Figura y haga clic en Inicio, o simplemente haga clic en la interfaz en la sección Lista de interfaz de la página de bienvenida. Los datos deben comenzar a llenar la ventana.

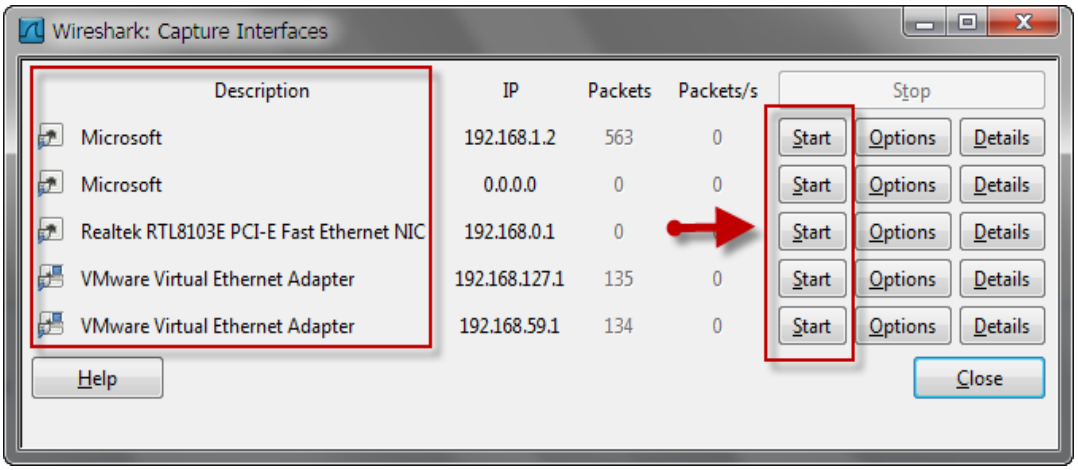


Figura 23 Imagen obtenida de Wireshark Permite Seleccionar una interfaz para llevar a cabo la captura de paquetes de datos

4. Una vez iniciado la captura esperar el tiempo que sea necesario y después detener la captura y ver los datos, para esto hacer clic en el botón Detener captura desde el menú desplegable.

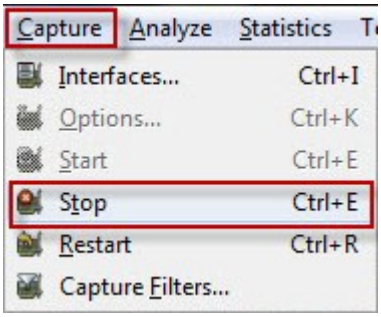


Figura 24 Imagen obtenida de Wireshark muestra el menú Captura/Parar capturas

Una vez que se complete estos pasos, el proceso de captura habrá terminado, la ventana principal de Wireshark debe mostrar una gran cantidad de datos capturados.

4.4.4. Ventana principal de Wireshark

La ventana de Wireshark principal. Aquí es donde se muestran todos los paquetes capturados y se divide en un formato más comprensible. No existe una separación visual de los protocolos en capas diferentes, todos los paquetes se muestran como son recibidos en la red.

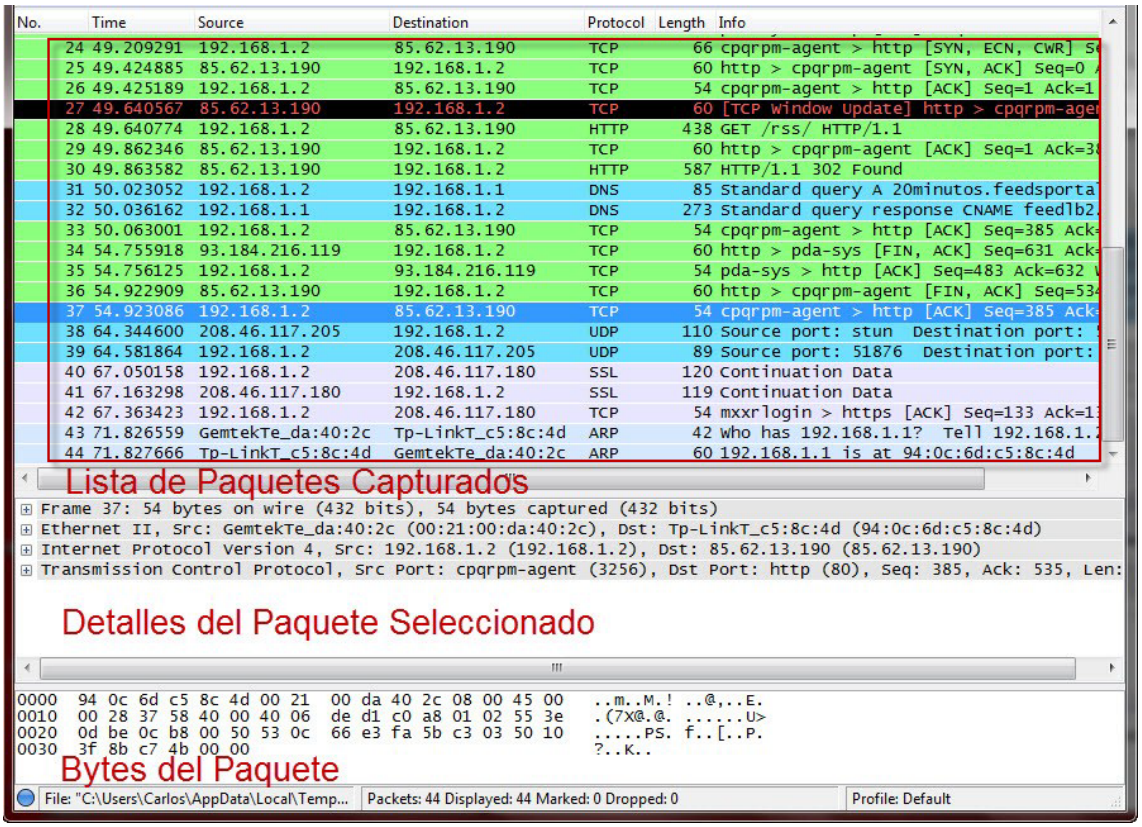


Figura 25 Imagen que muestra la ventana principal de Wireshark con un diseño de tres paneles.

Los tres paneles en la ventana principal de Wireshark dependen uno del otro. Con el fin de ver los detalles de un solo paquete individualmente.

4.4.4.1. Lista de paquetes Capturados

El panel superior muestra una tabla que contiene una lista con todos los paquetes de la captura actual. Tiene columnas que contienen:

- Número de paquete – enumera en secuencia cada paquete capturado
- Tiempo - El tiempo relativo fue capturado el paquete,
- Fuente – De que dirección fue obtenido el paquete
- Destino – A qué dirección estaba dirigido el paquete,
- Protocolo usado por el paquete.
- Longitud del paquete
- Alguna información general que se encuentra en el paquete.

4.4.4.2. Detalles del paquete Seleccionado

En el panel central contiene una presentación jerárquica de la información sobre un solo paquete. Esta pantalla se puede contraer y expandir para mostrar toda la información recopilada acerca de un paquete individual.

4.4.4.3. Bytes del paquete

En el panel inferior, es el más confuso, muestra un paquete en su forma cruda, sin procesar, es decir muestra como el paquete aparece a medida que viaja a través de la red. Una área de visualización que proporciona información sobre la cantidad de paquetes en la captura actual.

4.4.5. Configuración de Wireshark para capturar paquetes de Datos

1.- La lista desplegable permite seleccionar la interfaz de captura es donde se puede seleccionar la interfaz de red a configurar. En la lista desplegable de la izquierda permite especificar si la interfaz es local o remota.

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

3.- Los botones en la parte derecha de la sección de captura le permiten acceder a la configuración inalámbrica y remota según corresponda. Debajo de ellos está la opción de tamaño del búfer, que está disponible sólo en sistemas que ejecutan Microsoft Windows. Se puede especificar la cantidad de datos de captura de paquetes que se almacenan en la memoria intermedia antes de que se escriban en el disco.

5.- Las tres casillas de verificación en el lado izquierdo del cuadro de diálogo le permite activar o desactivar el modo promiscuo siempre activada por defecto, la captura de paquetes en el momento experimental en formato pcap-ng y limitar el tamaño de cada paquete de captura por bytes.

6.- La opción Filtro de captura le permite especificar un filtro de captura, para capturar solamente lo especificado en el filtro de búsqueda de paquetes.

7.- La sección de captura de archivos permite almacenar de forma automática la captura de paquetes en un archivo, en lugar de su captura y luego guardar el archivo. Ofrecen mucha más flexibilidad en la gestión de cuántos paquetes se guardan.

Puede guardar un archivo único o un conjunto de archivos, o incluso utilizar un búfer para manejar el número de los archivos creados. Para activar esta opción, introduzca una ruta de acceso completa y el nombre en el cuadro de texto del archivo. Cuando se captura una gran cantidad de tráfico o la realización de capturas a largo plazo, los conjuntos de archivos pueden resultar útiles.

8.- En la sección Opciones de visualización controla el número de paquetes que se muestran como están siendo capturados. La lista de actualizaciones de

paquetes en la opción de tiempo real se explica por sí mismo y se puede combinar con el desplazamiento automático en la opción de captura en vivo. Cuando ambas opciones están activadas, todos los paquetes capturados se muestran en la pantalla, con las capturas más recientemente se muestran al instante pero requieren más cantidad de procesamiento.

9.- Wireshark permite detener las capturas automáticamente cumpliendo ciertos factores desencadenantes., Se pueden desencadenar en base al tamaño de los paquetes, por intervalos de tiempo como segundos, minutos hasta días y por el número de paquetes.

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

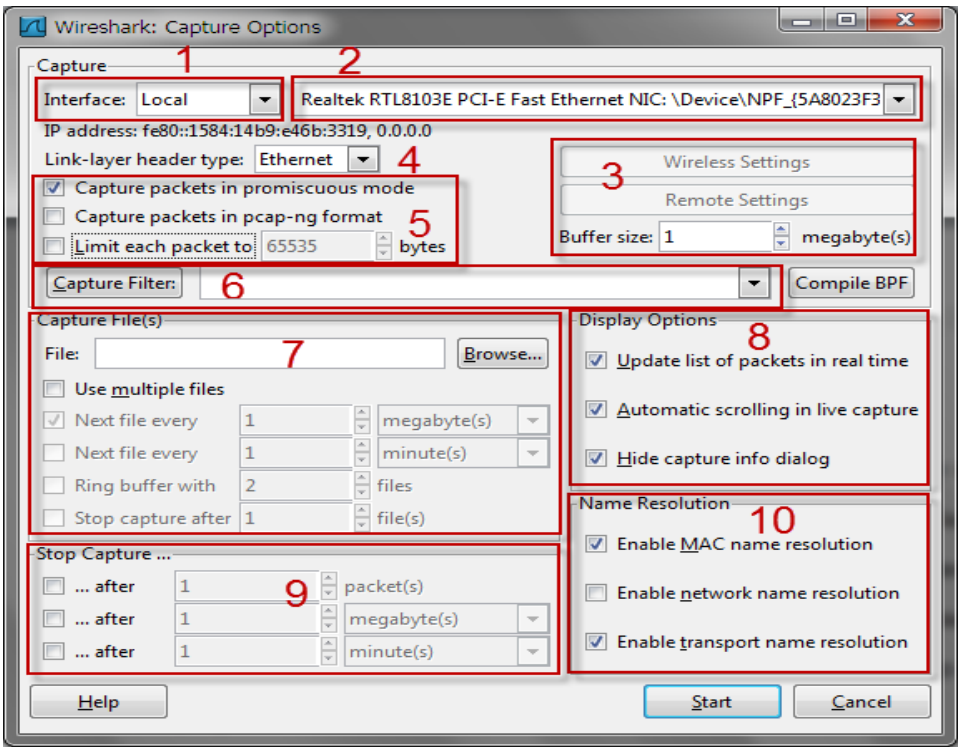


Figura 26 Ventana de configuración de Wireshark para capturar paquetes de datos.

4.4.6. Utilización de Colores en los Paquetes de datos con Wireshark

Cada paquete se muestra como un color determinado por una razón. Estos colores reflejan el protocolo del paquete. Por ejemplo, todo el tráfico UDP es azul, y todo el tráfico HTTP está en verde.

El código de colores permite diferenciar rápidamente entre los diferentes protocolos de modo que no se necesita leer el campo de protocolo en el panel de lista de paquetes para cada paquete individual.

Esta manera acelera enormemente el tiempo que toma navegar a través de los archivos de captura de gran tamaño.

Wireshark hace que sea fácil de ver los colores que se asignan a cada protocolo a través de la ventana para colorear reglas, Para abrir esta ventana, seleccione Ver en el menú desplegable principal y hacer clic en Reglas para colorear.

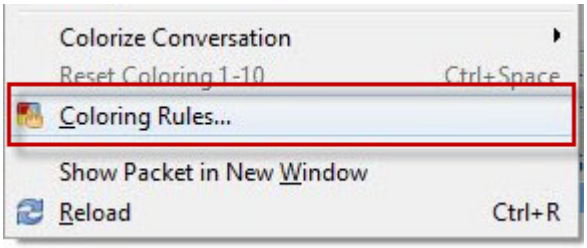


Figura 27 Imagen obtenida de Wireshark muestra el menú Ver/Reglas para Colorear.

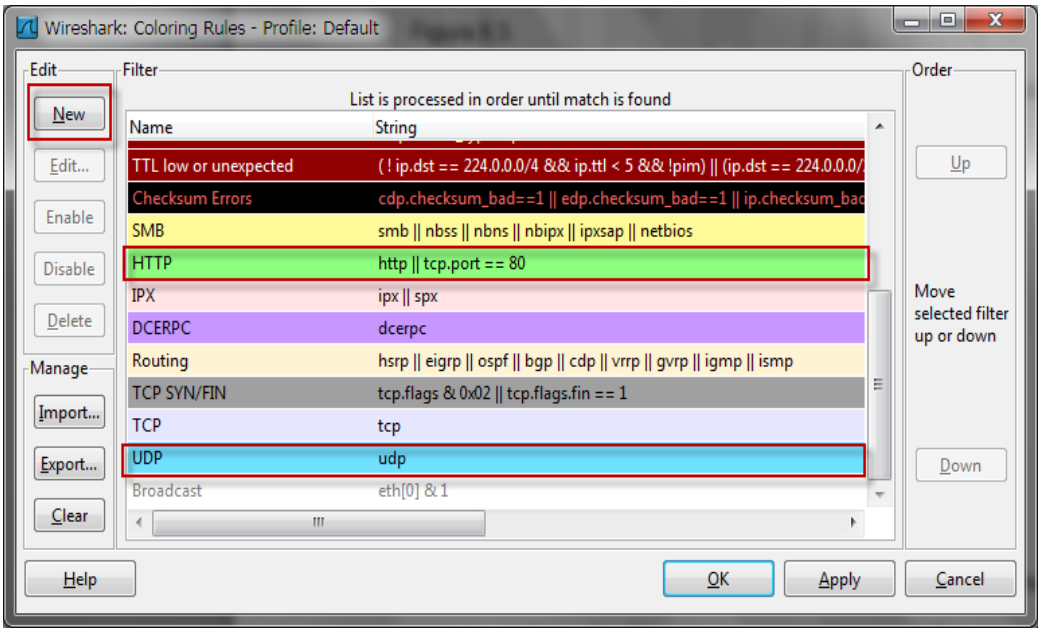


Figura 28 Ventana colorear reglas de Wireshark permite ver, modificar y crear nuevos colores para los paquetes.

4.4.7. Filtrado de Paquetes de Datos

Los filtros permiten especificar exactamente qué paquetes tenemos disponibles para su análisis. Un filtro es una expresión que define los criterios para la inclusión o exclusión de los paquetes.

Los filtros de captura se utilizan durante el actual proceso de captura de paquetes. Una de las razones principales para el uso de un filtro de captura es el rendimiento.

4.4.7.1. Filtrado durante la captura

Una utilizados en la captura de paquetes, y que se utiliza cuando se muestran los paquetes.

Los filtros de captura se especifica cuando los paquetes están siendo capturadas y se captura únicamente los paquetes que se especifican para la inclusión / exclusión en la expresión dada.

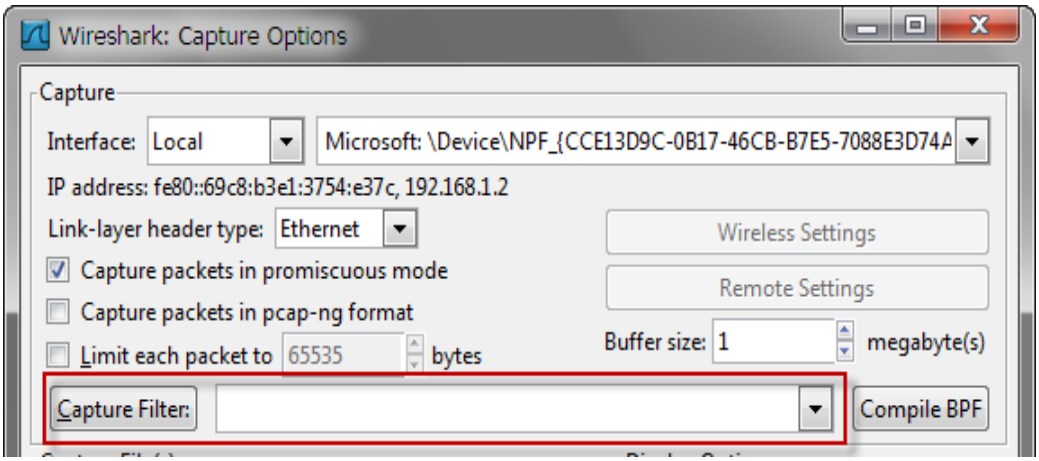


Figura 29 Ventana de Wireshark para configurar los filtros de captura de paquetes

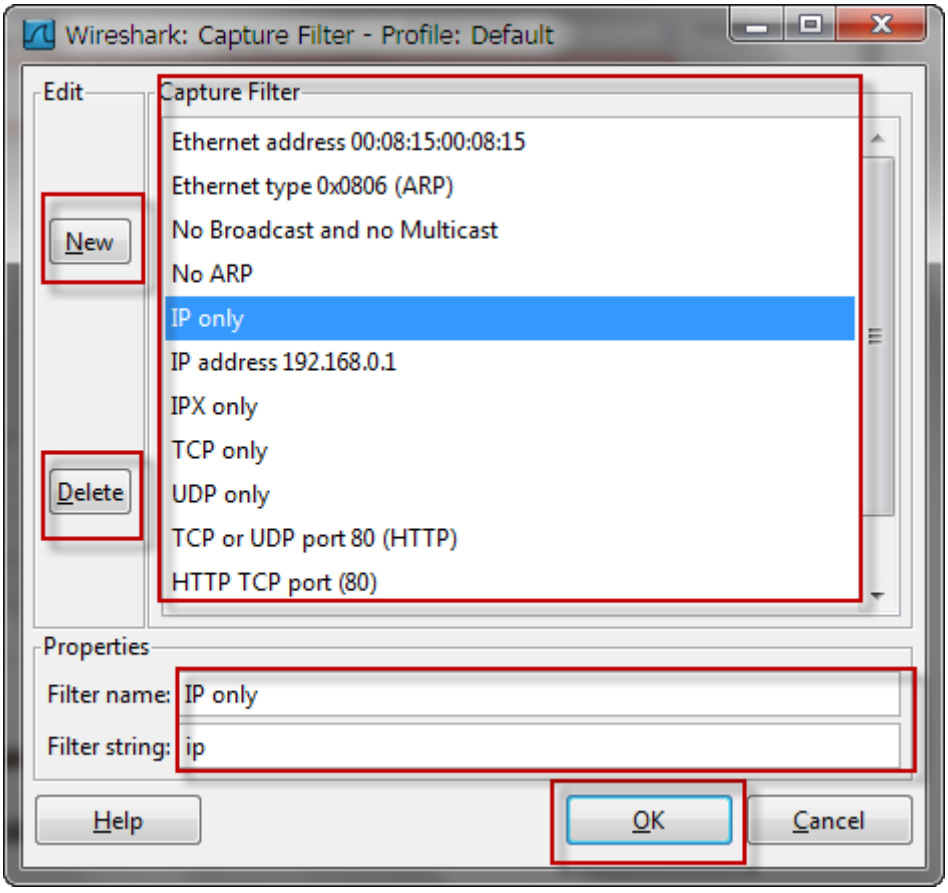


Figura 30 Ventana de Wireshark permite crear nuevos o borrar los filtros para captura de paquetes

4.4.7.2. El filtrado de paquetes durante la visualización

Filtros de pantalla se aplican a un conjunto existente de los paquetes capturados con el fin de ocultar los paquetes no deseados o mostrar los paquetes que desee sobre la base de la expresión especificada

Los Filtros de pantalla le permiten concentrarse en los paquetes que están interesados en ocultar, mientras que los que actualmente carente de interés. Que le permiten seleccionar los paquetes por:

- Protocolo
- La presencia de un campo
- Los valores de los campos
- Una comparación entre los campos

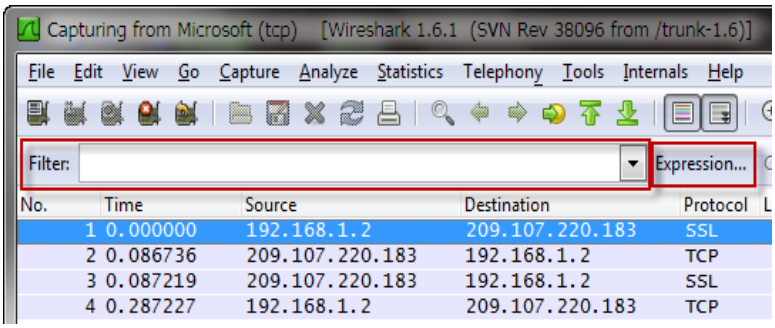


Figura 31 Imagen tomada de Wireshark muestra los filtros de captura de paquetes durante la visualización

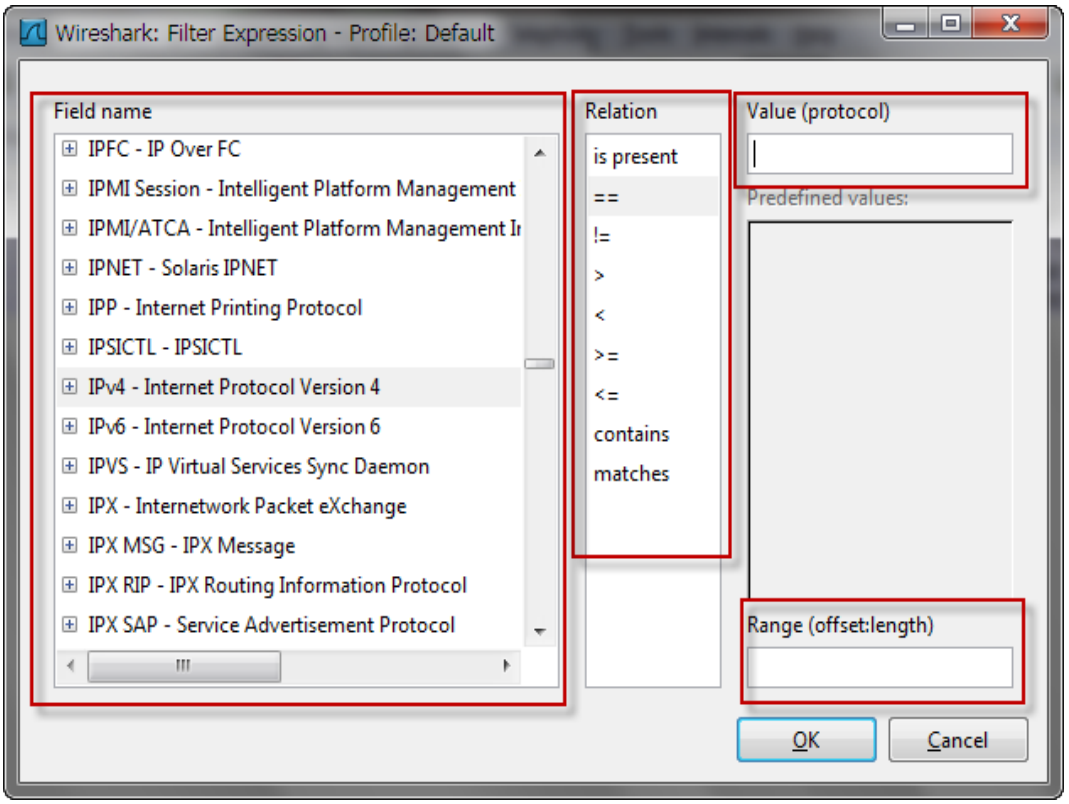


Figura 32 Imagen tomada de Wireshark muestra la ventana para configurar los filtros con relación de captura de paquetes durante la visualización

4.4.8. Guardar Paquete de Datos

Wireshark puede guardar el paquete de datos en su formato nativo de archivos **libpcap** y en los formatos de archivo de algunos otros analizadores de protocolos, para que otras herramientas puedan leer los datos de captura.

Formatos de archivo tienen diferentes precisiones de fecha y hora Los siguientes formatos de archivos con sus extensiones puede ser guardados por Wireshark:

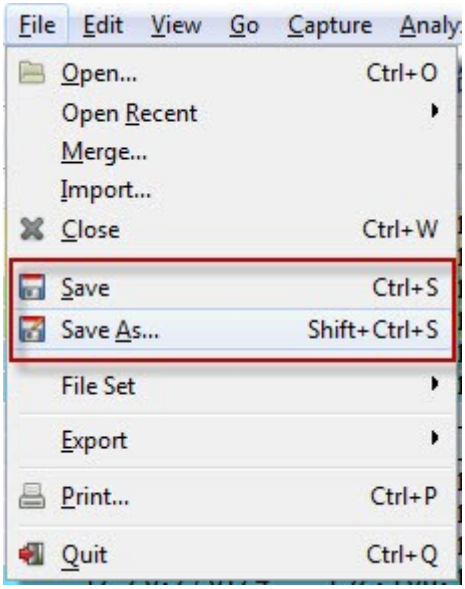


Figura 33 Imagen tomada de Wireshark muestra el menú Archivo/Guardar y Guardar Como para los paquetes de datos capturados

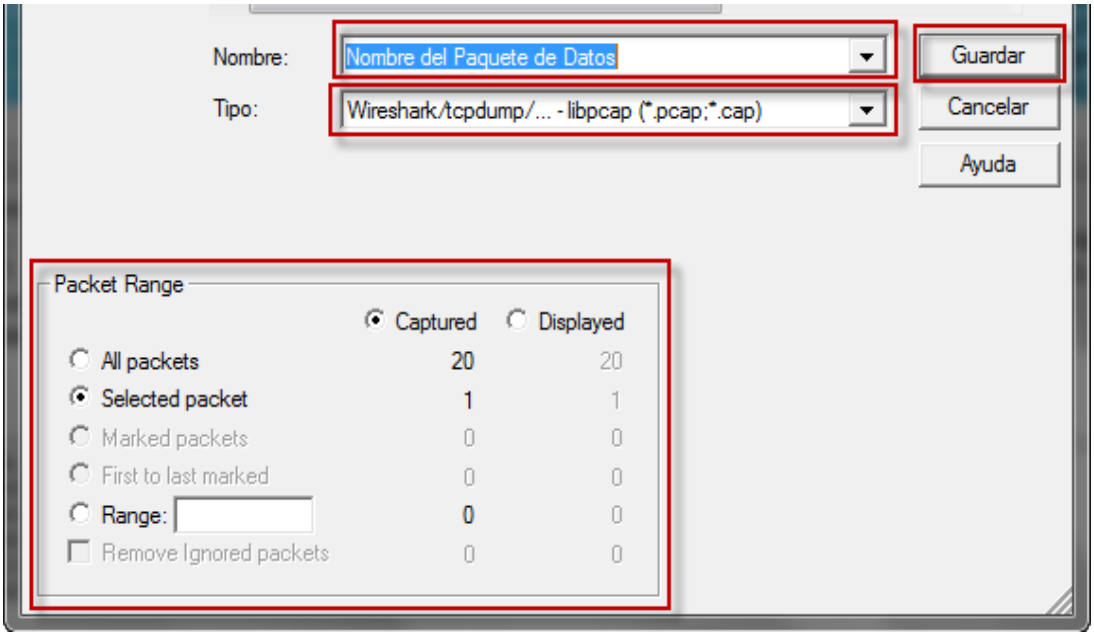


Figura 34 Imagen tomada de Wireshark muestra la ventana para Guardar los paquetes de datos con diferentes opciones

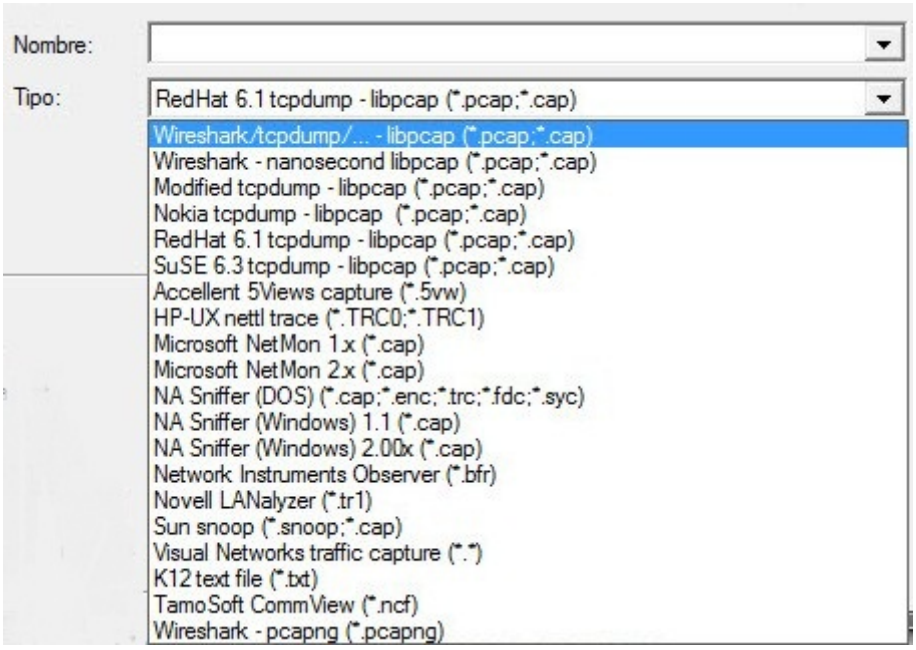


Figura 35 Imagen tomada de Wireshark muestra todas las extensiones disponible para guardar un archivo de captura

libpcap, tcpdump y varias otras herramientas que utilizan el formato de captura de tcpdump (*. pcap, *. cap, *. dmp)

4.4.9. Exportando a otros Formatos los Paquetes de Datos

Wireshark permite exportar los paquetes de datos capturados en diferentes formatos para su visualización en otros medios de comunicación o para importar a otras herramientas de análisis de paquetes.

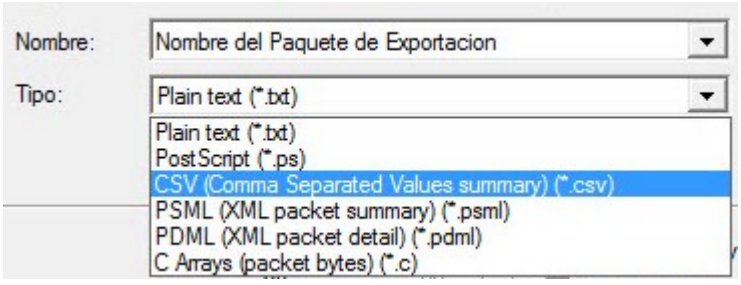


Figura 36 Imagen tomada de Wireshark muestra todas las extensiones disponibles para el archivo de exportación

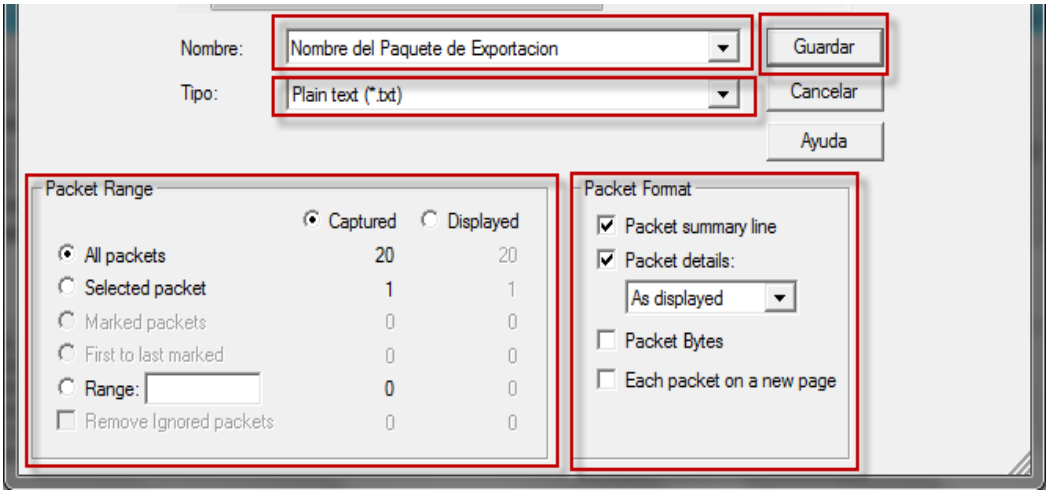


Figura 37 Imagen tomada de Wireshark muestra el ventana para seleccionar los paquetes de datos que se van a exportar a otro formato

Para exportar la captura de paquetes, seleccione Archivo de exportación, a continuación, seleccionar el formato del archivo exportado. Se mostrara un cuadro de diálogo Guardar como contiene las opciones relacionadas con ese formato específico.

4.5. Realizar el análisis de los paquetes de datos capturados de la red para su argumentación y registro.

Por lo general, se realizarán varias capturas en distintos momentos, los paquetes se guardan y analizan todos a la vez. Por lo tanto, Wireshark permite guardar los archivos de captura para su posterior análisis. También puede combinar varios archivos de captura.

4.5.1. Análisis de Paquetes

El análisis de paquetes, a menudo referido como la detección de paquetes o de análisis de protocolo, se describe el proceso de captura e interpretación de datos en tiempo real a medida que fluye a través de una red con el fin de entender mejor lo que está sucediendo en la red.

El análisis de paquetes se realiza generalmente mediante un analizador de paquetes, en este caso Wireshark una herramienta utilizada para la captura de datos en bruto de la red que va a través del cable.

El análisis de paquetes puede ayudar con lo siguiente:

- Comprender las características de la red
- Aprendizaje que está en una red
- Determinar quién o qué está utilizando el ancho de banda disponible
- Identificación del uso de la red en horas pico
- Identificación de posibles ataques o actividades maliciosas

Todos los problemas de la red se derivan a nivel de paquete, Para entender mejor los problemas de red. En este nivel de paquetes, no hay verdaderos secretos sólo los datos encriptados. Cuanto más podamos hacer el análisis a nivel de paquetes, podemos controlar la red y resolver sus problemas.

Porque capturar los paquetes de datos cuando no existe nada malo en la red. No tiene qué ser por problemas para llevar a cabo el análisis de paquetes. De hecho, la mayoría de los analistas de paquetes dedican más tiempo en analizar el tráfico sin problemas que el tráfico en el que se encuentra el problema.

Con el fin de encontrar anomalías en la actividad diaria de la red, se debe conocer la actividad normal de la red todos los días. Es necesario un punto de referencia para comparar con el fin de ser capaces de solucionar con eficacia el tráfico de red. Cuando la red está funcionando correctamente, usted puede configurar su línea base de modo que conozca el tráfico en un estado normal.

4.5.2. Fusionar Archivos de Captura

Ciertos tipos de análisis requieren la capacidad de combinar varios archivos de captura. Esta es una práctica común cuando se comparan dos flujos de datos o la combinación de las corrientes del mismo tráfico que fueron capturados por separado.

Para combinar los archivos de captura, abra uno de los archivos de captura que desea combinar y seleccione Archivo - Combinar para abrir el cuadro de diálogo de fusión con la captura de archivos. Seleccione el nuevo archivo que desea combinar en el archivo ya está abierto, y luego seleccionar el método a utilizar para la fusión de los archivos.

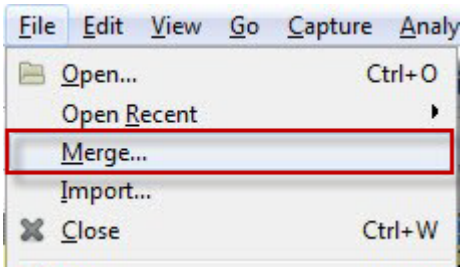


Figura 38 Imagen obtenida de Wireshark muestra el menú de plegable Archivo/Fusionar archivos capturados.

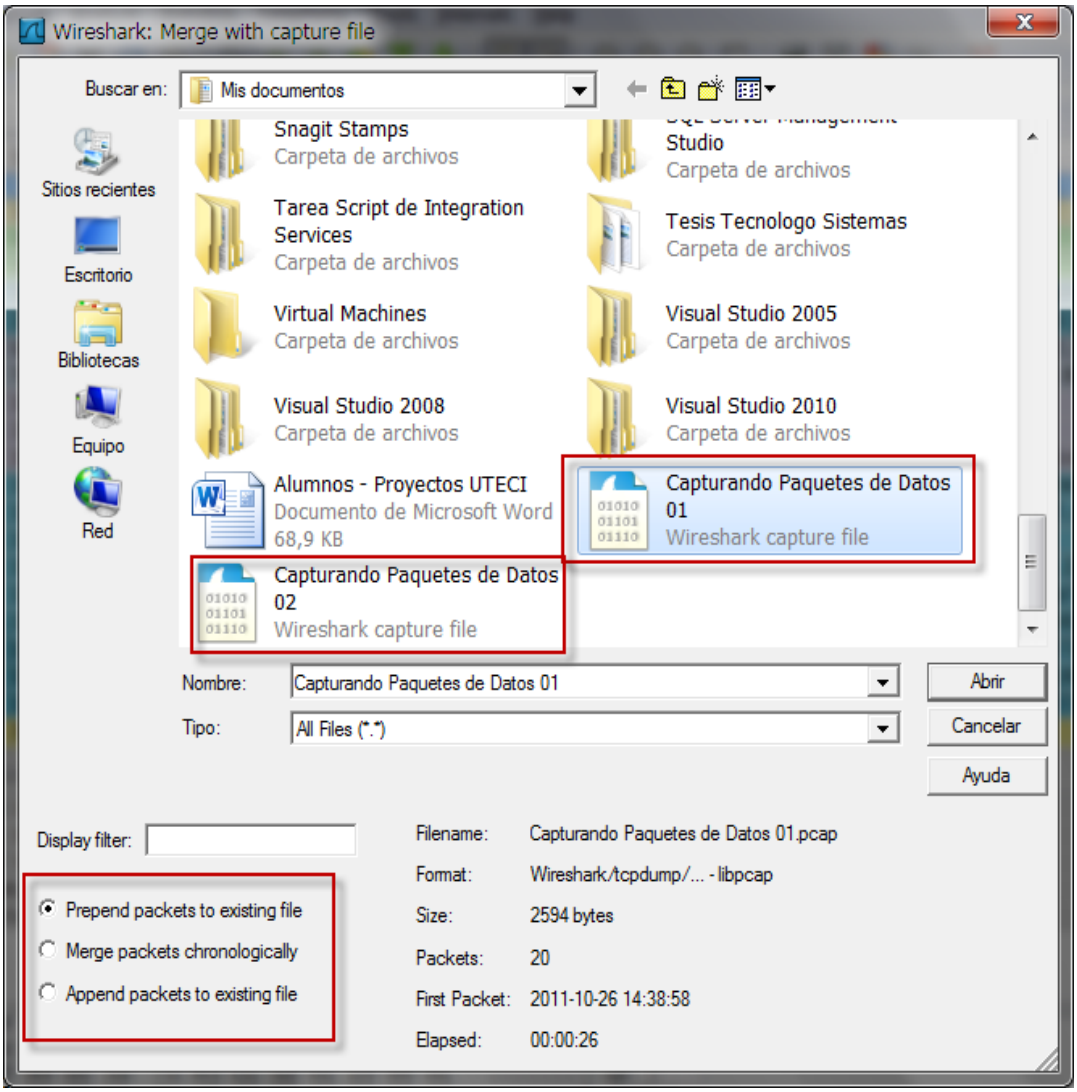


Figura 39 El cuadro de dialogo de fusión de archivos de captura permite combinar dos archivos de captura.

4.5.3. Imprimir Paquetes Capturados

Aunque la mayoría de análisis se llevará a cabo en la pantalla del ordenador, es posible que sea necesario imprimir los datos capturados. Imprimir paquetes hace que rápidamente se pueda hacer referencia a su contenido mientras se hace el análisis de otros.

Wireshark permite imprimir los paquetes capturados a un archivo PDF es también muy conveniente, especialmente en la preparación de informes.

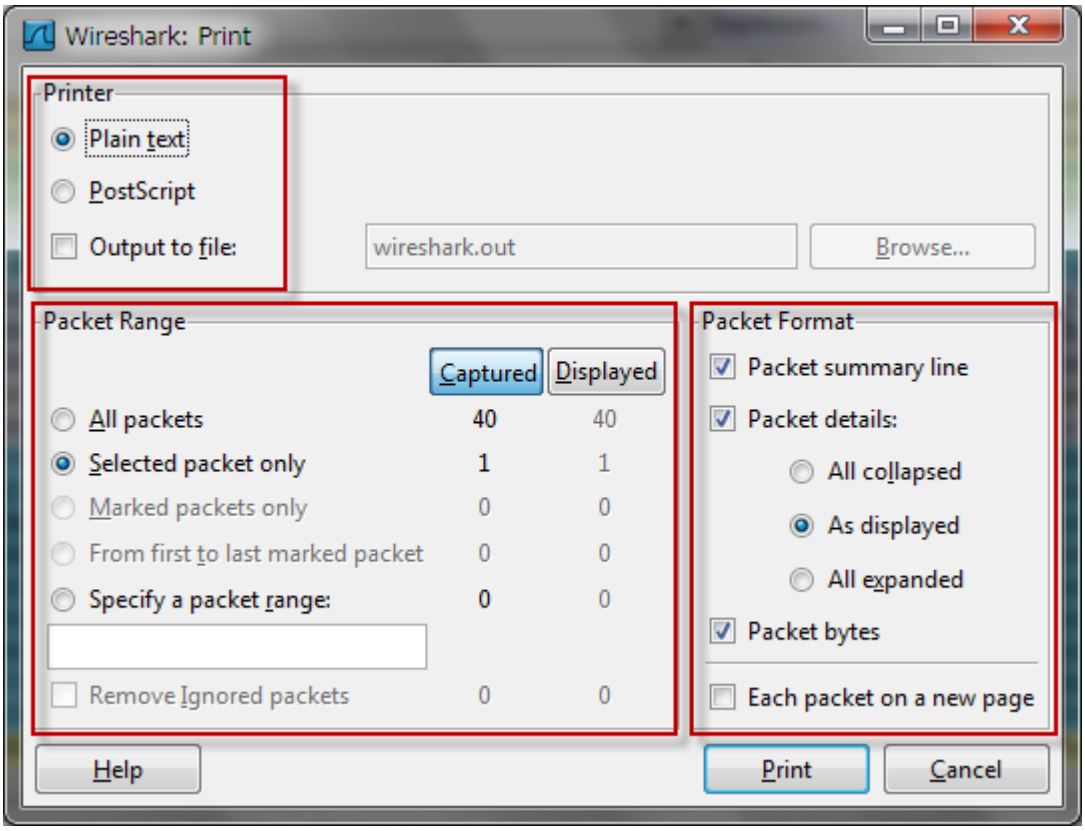


Figura 40 Imagen obtenida de Wireshark muestra la ventana de configuración de impresión de archivos capturados.

Para imprimir los paquetes capturados, abra el cuadro de diálogo de impresión seleccionando Archivo Imprimir desde el menú principal. Verá el cuadro de diálogo de impresión.

4.5.4. Búsqueda de Paquetes de Datos Capturados

Situaciones que implican un gran número de paquetes capturados. Como el número de estos paquetes se convierte en miles y hasta millones, para explorar a través de paquetes de manera más eficiente. Para ello, Wireshark permite encontrar y marcar los paquetes que cumplan ciertos criterios. También puede imprimir los paquetes para una fácil referencia.

El cuadro de dialogo buscar paquetes de Wireshark permite encontrar los paquetes que coincidan con determinados criterios, abrir el cuadro de diálogo buscar paquetes, pulsando CTRL-F.

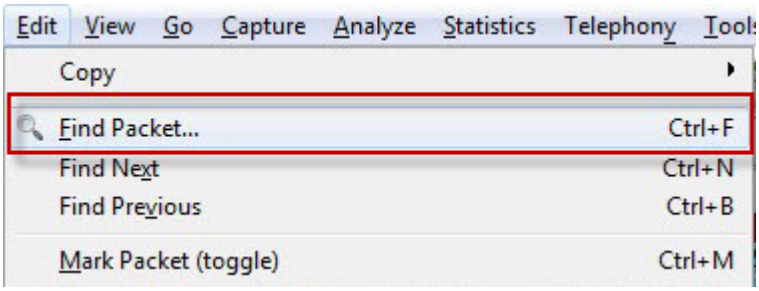


Figura 41 Tomada de Wireshark muestra el menú Archivo/ Encontrar Paquetes Capturados

Este cuadro de diálogo de búsqueda, ofrece tres opciones para encontrar los paquetes:

1.- La opción de filtro de pantalla permite introducir un filtro basado en expresiones que encuentra únicamente los paquetes que cumplen con esa expresión.

2.- Las búsquedas por valor hexagonal esta opción encuentra paquetes con un número hexadecimal con bytes separados por dos puntos el valor que se especifique.

3.- La opción busca de cadenas de paquetes, es necesario especificar el texto con una cadena

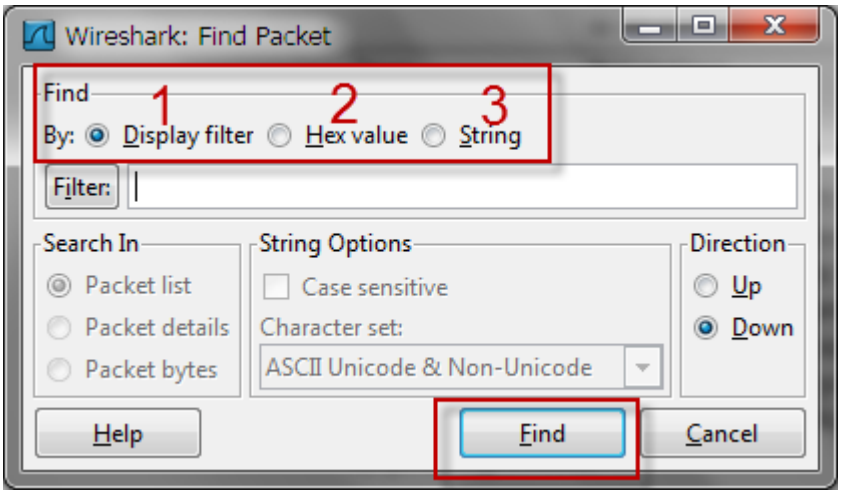


Figura 42 Búsqueda de paquetes en Wireshark en base a los criterios especificados

4.5.5. Marcado de paquetes

Después de haber encontrado los paquetes que coincidan con los criterios de búsqueda, puede marcar solamente los de interés particular. Por ejemplo, es posible que desee marcar paquetes para poder guardar los paquetes por separado o para encontrar de forma rápida en base a la coloración.

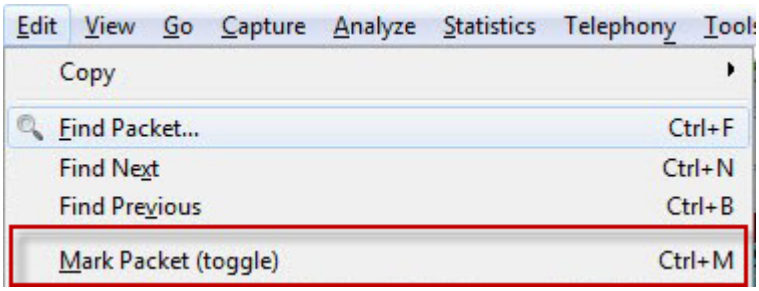
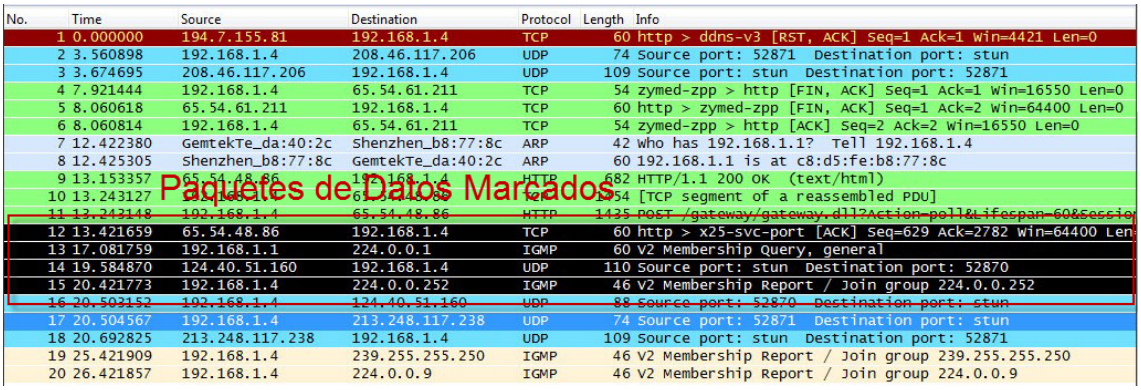


Figura 43 Tomada de Wireshark muestra el menú Editar/ Marcar Paquetes

Paquetes marcados se destacan por un fondo negro y texto en blanco, También es posible resolver sólo los paquetes marcados al guardar las capturas de paquetes.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	194.7.155.81	192.168.1.4	TCP	60	http > ddns-v3 [RST, ACK] Seq=1 Ack=1 Win=4421 Len=0
2	3.560898	192.168.1.4	208.46.117.206	UDP	74	Source port: 52871 Destination port: stun
3	3.674695	208.46.117.206	192.168.1.4	UDP	109	Source port: stun Destination port: 52871
4	7.921444	192.168.1.4	65.54.61.211	TCP	54	zymed-zpp > http [FIN, ACK] Seq=1 Ack=1 Win=16550 Len=0
5	8.060618	65.54.61.211	192.168.1.4	TCP	60	http > zymed-zpp [FIN, ACK] Seq=1 Ack=2 Win=64400 Len=0
6	8.060814	192.168.1.4	65.54.61.211	TCP	54	zymed-zpp > http [ACK] Seq=2 Ack=2 Win=16550 Len=0
7	12.422380	GemtekTe_da:40:2c	Shenzhen_b8:77:8c	ARP	42	who has 192.168.1.1? Tell 192.168.1.4
8	12.425305	Shenzhen_b8:77:8c	GemtekTe_da:40:2c	ARP	60	192.168.1.1 is at c8:d5:fe:b8:77:8c
9	13.153357	65.54.48.86	192.168.1.4	HTTP	682	HTTP/1.1 200 OK (text/html)
10	13.243127	192.168.1.4	65.54.48.86	TCP	1254	[TCP segment of a reassembled PDU]
11	13.243148	192.168.1.4	65.54.48.86	HTTP	1435	POST /gateway/gateway.dll?Action=poll&Lifespan=60&Sessio
12	13.421659	65.54.48.86	192.168.1.4	TCP	60	http > x25-svc-port [ACK] Seq=629 Ack=2782 Win=64400 Len
13	17.081759	192.168.1.1	224.0.0.1	IGMP	60	V2 Membership Query, general
14	19.584870	124.40.51.160	192.168.1.4	UDP	110	Source port: stun Destination port: 52870
15	20.421773	192.168.1.4	224.0.0.252	IGMP	46	V2 Membership Report / Join group 224.0.0.252
16	20.503152	192.168.1.4	124.40.51.160	UDP	88	Source port: 52870 Destination port: stun
17	20.504567	192.168.1.4	213.248.117.238	UDP	74	Source port: 52871 Destination port: stun
18	20.692825	213.248.117.238	192.168.1.4	UDP	109	Source port: stun Destination port: 52871
19	25.421909	192.168.1.4	239.255.255.250	IGMP	46	V2 Membership Report / Join group 239.255.255.250
20	26.421857	192.168.1.4	224.0.0.9	IGMP	46	V2 Membership Report / Join group 224.0.0.9

Figura 44 Imagen tomada de Wireshark muestra la lista de Marcar Paquetes

Para marcar un paquete, haga clic derecho en la el panel Lista de paquetes y seleccione marcar en el menú emergente o haga clic en un paquete en el panel Lista de paquetes y presione CTRL-M. Para desmarcar un paquete, para cambiar esto salir con CTRL-M de nuevo. Puede marcar tantos paquetes como

desee en una captura. Para saltar hacia delante y hacia atrás entre los paquetes marcados, pulse SHIFT-CTRL-N y SHIFT-CTRL-B, respectivamente.

4.5.6. Gráficos

Los gráficos son importantes en el análisis y una de las mejores maneras de obtener una visión general de un conjunto de datos. Wireshark incluye una serie de características gráficas diferentes para ayudar en la comprensión de la captura de datos.

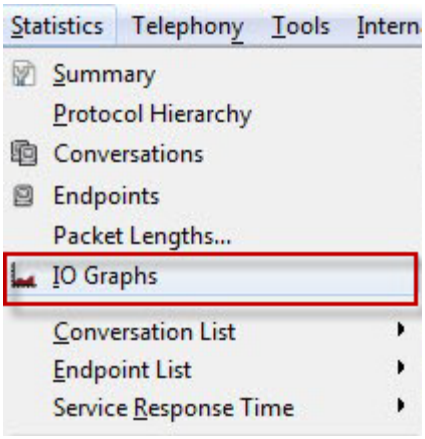


Figura 45 Tomada de Wireshark muestra el menú Estadísticas/Gráficos IO

La ventana de gráficos de Wireshark permite graficar el rendimiento de los datos en una red. Se puede utilizar gráficos como para encontrar picos y momentos de calma en el rendimiento de datos, descubrir retrasos en los protocolos de actuación individual, y para comparar los flujos de datos simultáneos.

La ventana de gráficos muestra una vista gráfica del flujo de datos en el transcurso del archivo de captura.

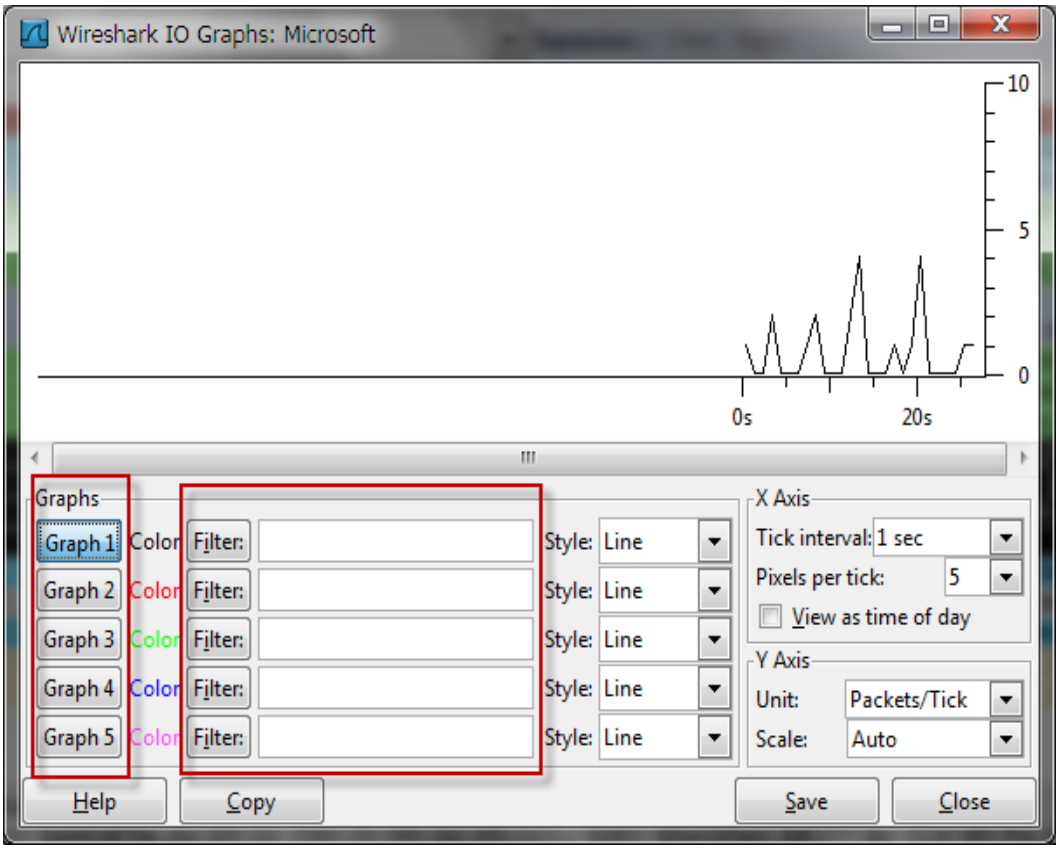


Figura 46 Tomada de Wireshark muestra los gráficos de IO

Las opciones configurables en la parte inferior de esta ventana. Permite crear hasta cinco gráficos con sus filtros únicos utilizando la misma sintaxis como una pantalla de filtro de captura y además especificar los colores de visualización de los filtros, para diferenciar más fácilmente las tendencias de rendimiento entre estos los diferentes tipos de protocolos.

4.5.7. Estadísticas de jerarquía de protocolos

La ventana de estadísticas de jerarquía de protocolos es para una mejor visión de la situación, podemos ver los protocolos de la capa de aplicación que se utiliza con las conexiones TCP y UDP. Se visualizan porcentajes de completado de los paquetes y el tamaño en bytes, para abrir la ventana de jerarquía de protocolos haga clic desde el menú estadísticas.

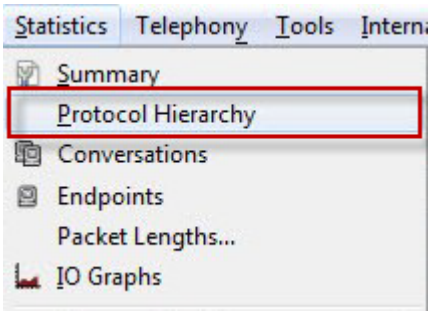


Figura 47 Tomada de Wireshark muestra el menú estadísticas/Jerarquías de protocolos

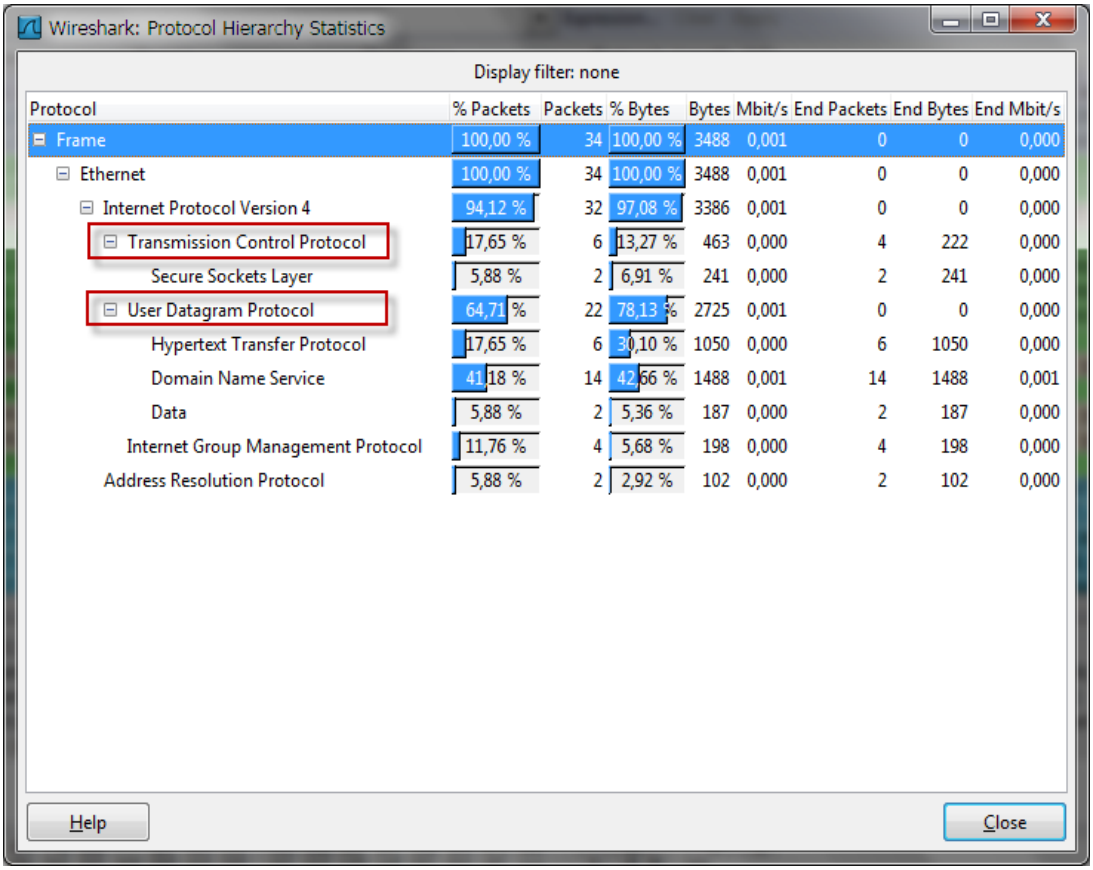


Figura 48 La ventana de estadísticas de jerarquía de protocolos muestra la distribución de los protocolos de la captura de paquetes.

5. CAPITULO V - CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Es importante indicar también que las funcionalidades utilizadas en el presente informe solo representan una pequeña parte de todo el potencial que pueda ofrecernos Wireshark, y cuyo objetivo principal es servir de guía orientativa para cualquier administrador que necesite detectar, analizar o solucionar anomalías de red.

Concluyendo con este trabajo escrito sobre el análisis y captura de paquetes de datos en una red mediante Wireshark, se ha demostrado la importancia de la herramienta de software, algunas de sus características más funcionales, los usos que puede tener, además se mencionó la compatibilidad de sistemas operativos, protocolos con los que trabaja Wireshark. Los administradores de redes o usuarios pueden emplear este modelo para guía en sus análisis de redes siguiendo el procedimiento de instalación e implementación.

Todos los problemas de las redes surgen a partir del paquete de datos, por eso lo importante de realizar el análisis y captura de paquetes de datos con una herramienta de software que se ajuste a las necesidades del administrador de redes como también a toda la arquitectura que compone la red, toda la parte lógica como software y la parte física como hardware.

Wireshark es una herramienta poderosa para guardar, combinar, exportar los paquetes de datos para su posterior análisis de los mismos nos presenta diversa forma para trabajar con los mismos, para imprimirlos, dos maneras de

visualización, nos genera gráficos y además nos muestra cuadros estadísticos para comparaciones.

5.2. Recomendaciones

Los análisis de tráfico, o también llamados análisis de paquetes es recomendable realizarlo continuamente, no esperar que se presente el problema para poder actuar, esto ocasionaría la toma de mucho tiempo en descubrir el error, además de costos económicos que involucrarían pérdidas para la empresa.

Entonces se recomienda tener una línea base de la red para saber cómo trabaja en circunstancias normales, para hacer comparaciones con los futuros análisis de la red, esto ayudaría a descubrir anomalía a tiempo y poder actuar frente a esa amenaza.

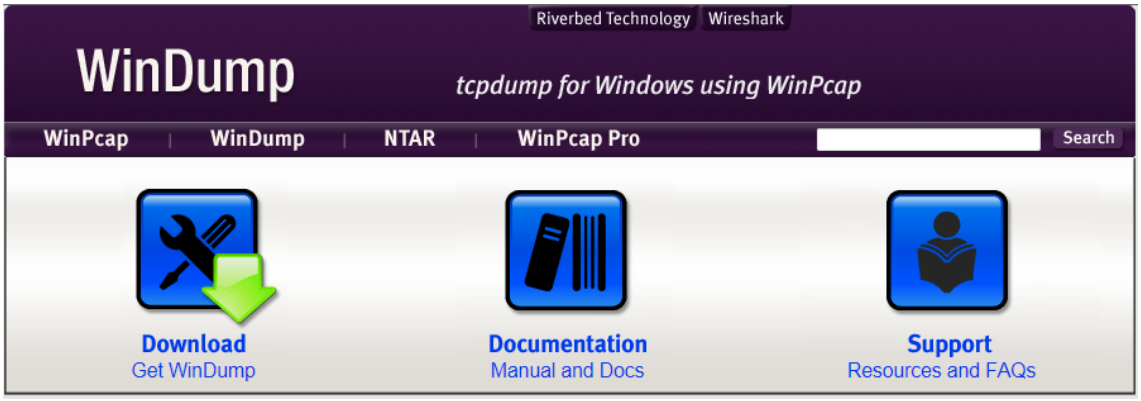
Aunque la herramienta Wireshark se utiliza principalmente en este análisis y captura de paquetes de datos en una red existen una gran cantidad de herramientas adicionales que trabajar combinadas que serán muy útiles para realizar análisis de paquetes, ya sea para la solución de problemas generales, redes lentas, problemas de seguridad, o redes inalámbricas. Recomiendo algunas de las herramientas de análisis de paquetes útiles y otros recursos de aprendizaje de análisis de paquetes.

Recomiendo utilizar la herramienta Wireshark, aunque existen varias herramientas que son útiles para el análisis y captura de paquetes, además de

Wireshark. A continuación se enumeran algunos de los nombres de herramientas que se han encontrado útiles.

tcpdump y Windump

La herramienta tcpdump considerada como facto para la captura de paquetes y utilidad de análisis por una multitud, tcpdump es totalmente basado en texto. Windump es simplemente una distribución de tcpdump que se ha reconstruido para Windows. http://www.tcpdump.org/.



http://www.winpcap.org/windump/.

CloudShark

CloudShark desarrollado por QA Café es un recurso en línea para compartir las capturas de paquetes con los demás. CloudShark es un sitio web que muestra los archivos de captura de red dentro de su navegador. Se puede capturar, subir archivos y enviar los enlaces a sus colegas para un análisis compartido.

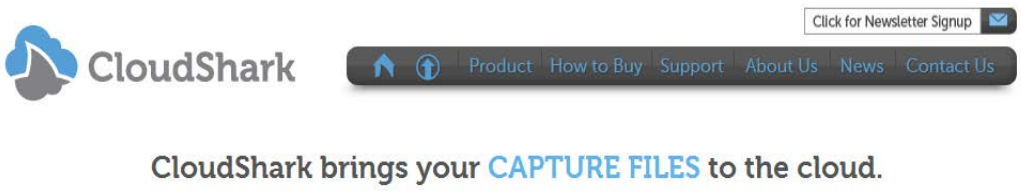


Figura 49 Imagen obtenida desde la página web oficial http://www.cloudshark.org/

http://www.cloudshark.org/.

Bibliografía Y Web grafía

Bibliografía

Bibliografía

Borja, M. (2011). *Análisis de Trafico con Wireshark.* España: El Instituto Nacional de Tecnologías de la Comunicación, INTECO.

Kar, D. C., & Syed, M. R. (2011). *Network Security, Administration and Management: Advancing Technology and Practice.* Hershey, Pennsylvania: Published by IGI Global.

Orebaugh, A., Ramirez, G., Burke, J., Pesce, L., Morris, G., & Wright, J. (2007). *Wireshark & Ethereal Network Protocol Analyzer Toolkit.* Rockland, Massachusetts: Syngress Publishing, Inc.

Sanders, C. (2011). *Practical Packet Analysis - Using Wireshark to Solve Real-World Network Problems.* San Francisco, California: No Starch Press, Inc.

Shimonski, R. J., Eaton, W., Khan, U., Gordienko, Y., Ouellet, E., & Cook, R. (2002). *Sniffer Pro - Network Optimization And Troubleshooting Handbook.* Rockland, Massachusetts: Syngress Publishing, Inc.

Web grafía

Web grafía - Fuentes Consultadas

Documentación de Winpcap. (25 de 10 de 2010).

Obtenido de http://www.winpcap.org/docs/default.htm

Cloudshark. (25 de 10 de 2011). Obtenido de http://www.cloudshark.org/

Colasoft. (25 de 10 de 2011).

Obtenido de http://www.colasoft.com/packet_builder/

Documentación de Wireshark. (25 de 10 de 2011).

Obtenido de http://www.wireshark.org/docs/

Documentos de Windump. (25 de 10 de 2011).

Obtenido de http://www.winpcap.org/windump/docs/default.htm

Libro de Wireshark. (25 de 10 de 2011).

Obtenido de http://www.wiresharktraining.com/book.html

Netdude. (25 de 10 de 2011). Obtenido de http://www.netdude.sourceforge.net/

Networkminer. (25 de 10 de 2011).

Obtenido de http://www.networkminer.sourceforge.net/

Pcapr. (25 de 10 de 2011). Obtenido de http://www.pcapr.net/

Riverbed. (25 de 10 de 2011).

Obtenido de http://www.cacetech.com/downloads.html

Scapy. (25 de 10 de 2011). Obtenido de http://www.secdev.org/projects/scapy/

Syngress. (25 de 10 de 2011). Obtenido de http://www.syngress.com

TCPdump. (25 de 10 de 2011). Obtenido de http://www.tcpdump.org/.

Windump. (25 de 10 de 2011). Obtenido de http://www.winpcap.org/windump/.

Winpcap. (25 de 10 de 2011). Obtenido de http://www.winpcap.org/

Wireshark Developer & User Conference. (25 de 10 de 2011).

Obtenido de http://www.sharkfest.wireshark.org/

Wireshark en Español. (25 de 10 de 2011).

Obtenido de http://www.wireshark.es/

Wireshark University. (25 de 10 de 2011).

Obtenido de http://www.wiresharktraining.com/

Wireshark. (25 de 10 de 2011). *Wireshark*.

Obtenido de http://www.wireshark.org

Glosario de Términos

DNS.- ***Domain Name System*** *Sistema de* Nombres de Dominio utiliza una base de datos que almacena información asociada a nombres de dominio usos más comunes son la asignación de nombres de dominio a direccione IP de Internet.

DNS Records.- Esta lista de tipos de registro DNS proporciona una visión general de los tipos de registros de recursos, registros de base de datos almacenados

DoS.- ***Denial of Service*** ataque de denegación de servicio, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema.

Dúplex.- Sistema de telecomunicaciones que es capaz de enviar y recibir mensajes de forma simultánea.

Ethereal.- Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones.

GPL.- ***General Public License*** de GNU Licencia Pública General es una licencia creada por la Free Software Foundation y

está orientada principalmente a proteger la libre distribución, modificación y uso de software. El software cubierto por esta licencia es software libre y protegido de intentos de apropiación.

Half-duplex.- significa que el método o protocolo de envío de información es bidireccional pero no simultáneo.

HUB.- Conocido como **concentrador** o ***hub*** es un dispositivo que permite centralizar el cableado de una red y poder ampliarla. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.

IDS.- ***Intrusion Detection System*** Sistema de detección de intrusos es un dispositivo o programa usado para detectar accesos no autorizados a un computador o a una red

IP.- ***Internet Protocol***.- es un protocolo de internet

LAN.- ***Local Área Network*** Red de área local

MAC.- ***Media Access Control,*** la dirección MAC es un control de acceso al medio es un identificador o dirección física que corresponde de forma única a una tarjeta o dispositivo de red.

Modo Promiscuo.- En informática, es aquel en el que una computadora conectada a una red compartida, tanto la basada en cable de cobre como la basada en tecnología inalámbrica, captura todo el tráfico que circula por ella. Está relacionado

con los programas de sniffers que se basan en este modo para realizar su trabajo.

NIC.- ***network interface card***; tarjeta de interfaz de red es una tarjeta de red o adaptador de red permite la comunicación y compartir recursos entre dos o más computadoras.

OSI.- ***open system interconnection*** es el modelo de interconexión de sistemas abiertos, es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización en el año 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

OSSIN.- ***Open Source Security Información Management***, es una colección de herramientas bajo la licencia GPL, diseñadas para ayudar a los administradores de red en la seguridad de las computadoras, detección de intrusos y prevención.

Proxy.- En una red informática, es un programa o dispositivo que realiza una acción en representación de otro, Sirve para interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc.

Routers.- **E**s como un encaminador, enrutador, direccionador o ruteador, es un dispositivo de hardware usado para la interconexión de redes informáticas que permite asegurar

el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar.

RPM.- ***Package Manager Red Hat Package Manager***, es una herramienta de administración de paquetes pensada básicamente para GNU/Linux. Es capaz de instalar, actualizar, desinstalar, verificar y solicitar programas. RPM es el formato de paquete de partida del Linux Standard Base.

SCADA.- ***Supervisory Control And Data Acquisition*** Control de Supervisión y Adquisición de Datos.

Sniffer.- Es un programa para monitorear y analizar el tráfico en una red de computadoras. También puede ser empleado para capturar datos que son transmitidos en una red ilícitamente.

SSH.- ***Secure Shell*** **-** es un protocolo de red para la comunicación segura de datos, Servicios seguros entre dos computadoras que se conecta mediante un canal seguro a través de una red

Switch.- Conocido como **conmutador** o ***switch*** es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

TCP.- ***Transmission Control Protocol*** Protocolo de Control de Transmisión es uno de los protocolos fundamentales en Internet. Muchos programas dentro de una red de datos compuesta por computadoras pueden usar TCP para crear *conexiones* entre ellos a través de las cuales puede enviarse un flujo de datos.

El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.

Tcpdump.- Es una herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red.

VoIP. - ***Voice over Internet Protocol*** Voz sobre protocolo de internet

WHOIS.- **E**s un protocolo TCP basado en petición/repuesta que se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en Internet.

YUM.- ***Yellowdog Updater, Modified*** es una herramienta libre de gestión de paquetes para sistemas Linux basados en RPM. YUM es una utilidad para línea de comandos, otras herramientas proveen a YUM de una interfaz gráfica de usuario.

ANEXOS

Anexo 1 - Manual de Instalación de Wireshark en Sistemas Windows

Comenzar el proceso de instalación haciendo doble clic en el instalador: Wireshark setup

Figura 50 Instalación de Wireshark en Microsoft Windows Paso N°1 – Tomada de Wireshark

La primera pantalla es de bienvenida general para el asistente de configuración. Haga clic en Siguiente para continuar.

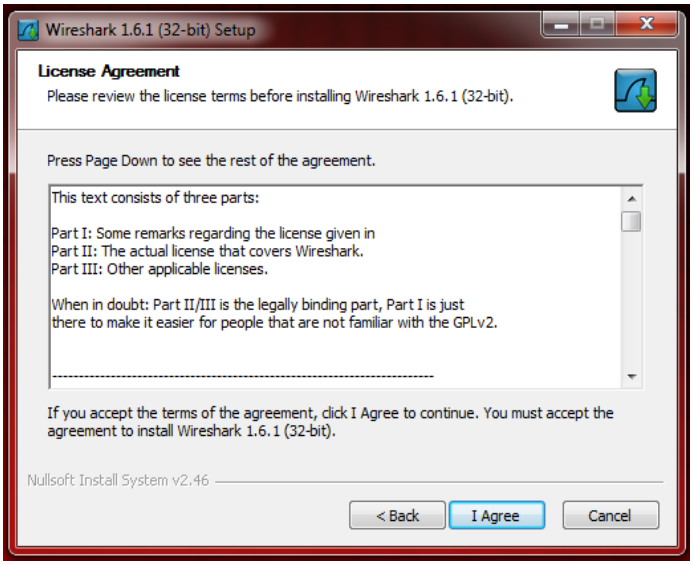


Figura 51 Instalación de Wireshark en Microsoft Windows Paso N°2 – Tomada de Wireshark

La siguiente pantalla es el Acuerdo General de licencia pública GNU de Wireshark. Después de leer todas las condiciones de la licencia, haga clic en Estoy de acuerdo para aceptar la licencia y continuar.

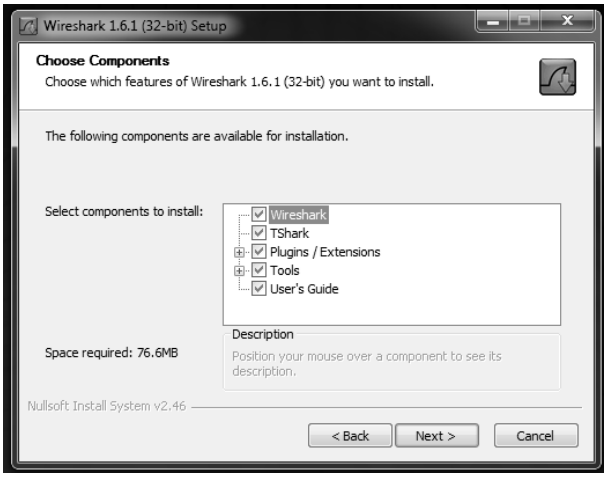


Figura 52 Instalación de Wireshark en Microsoft Windows Paso N°3 – Tomada de Wireshark

La siguiente pantalla le permite elegir los componentes para instalar Wireshark. El aditamento contiene otros programas empaquetados por defecto por Wireshark. Los componentes requieren 76.6MB de espacio libre en disco, tener también un adecuado espacio libre para almacenar sus archivos de captura. Haga clic en Siguiente para continuar.

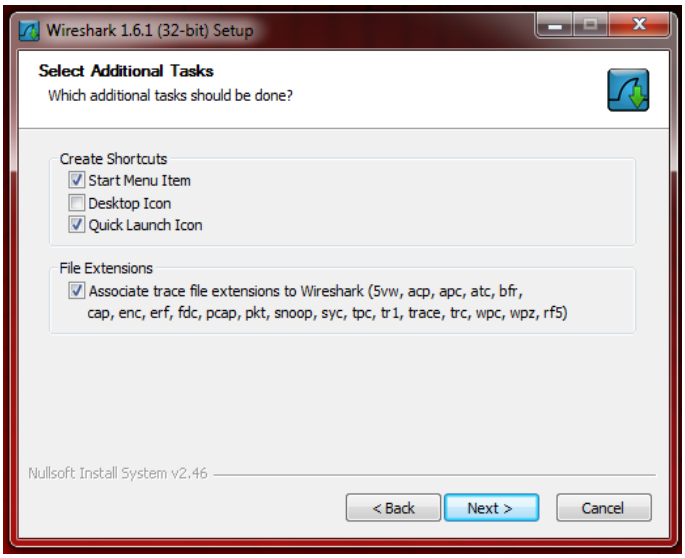


Figura 53 Instalación de Wireshark en Microsoft Windows Paso N°4 – Tomada de Wireshark

En la siguiente pantalla permite seleccionar tareas adicionales como crear accesos directos y extensiones de los archivos que se van asociar directamente con Wireshark, Haga clic en Siguiente para continuar.

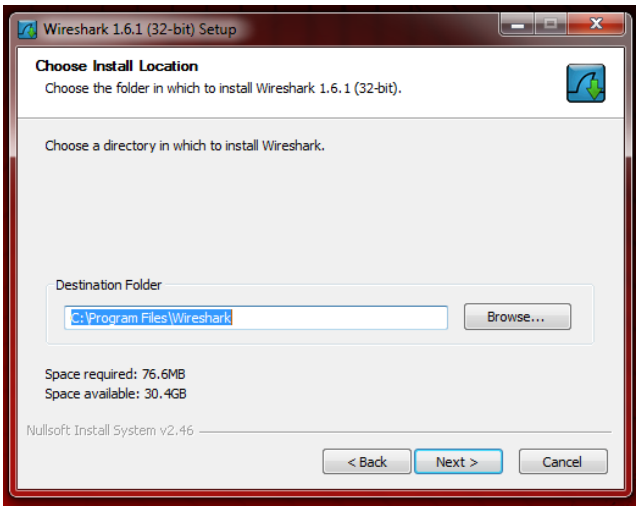


Figura 54 Instalación de Wireshark en Microsoft Windows Paso N°5 – Tomada de Wireshark

Escoger la localización en donde se realizara la instalación de Wireshark, por defecto se hace en el directorio Archivos de Programa/Wireshark. Haga clic en Siguiente para continuar.

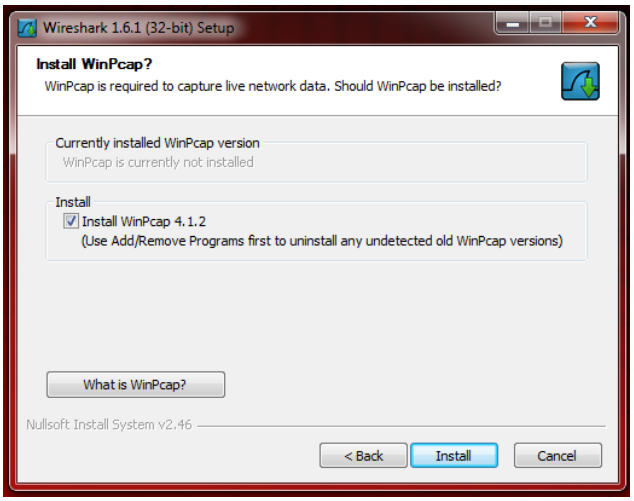


Figura 55 Instalación de Wireshark en Microsoft Windows Paso N°6 – Tomada de Wireshark

En la siguiente pantalla permite instalar las librerías WinCap necesarias para realizar la captura de paquetes de datos, La versión de WinCap viene probada para trabajar con Wireshark. Marcar la opción de instalar y Haga clic en Siguiente para continuar.

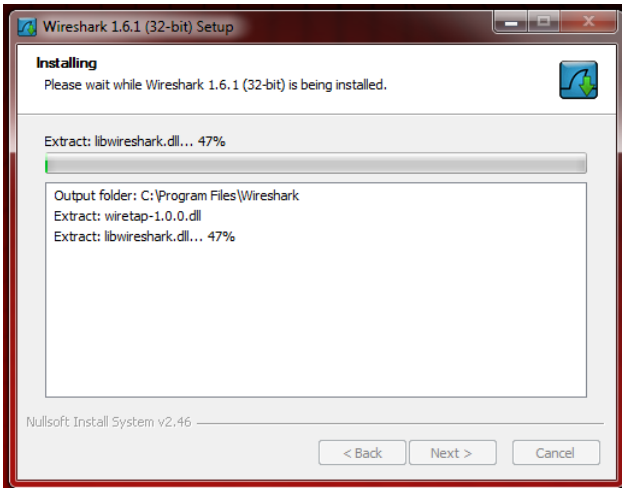


Figura 56 Instalación de Wireshark en Microsoft Windows Paso N°7 – Tomada de Wireshark

En la siguiente pantalla muestra el inicio de la instalación de Wireshark en el sistema

Figura 57 Instalación de Wireshark en Microsoft Windows Paso N°8 – Tomada de Wireshark

En la siguiente pantalla muestra el inicio de la instalación de las librerías WinCap, que es necesaria para el objetivo de este trabajo en análisis y captura de paquetes de datos en una red, Haga clic en siguiente para continuar.

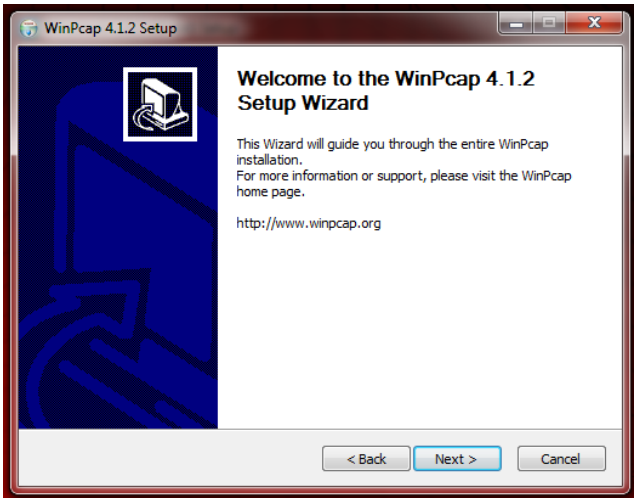


Figura 58 Instalación de Wireshark en Microsoft Windows Paso N°9 – Tomada de Wireshark

Presentación de la pantalla de bienvenida al asistente de instalación de WinCap, Haga clic en siguiente para continuar.

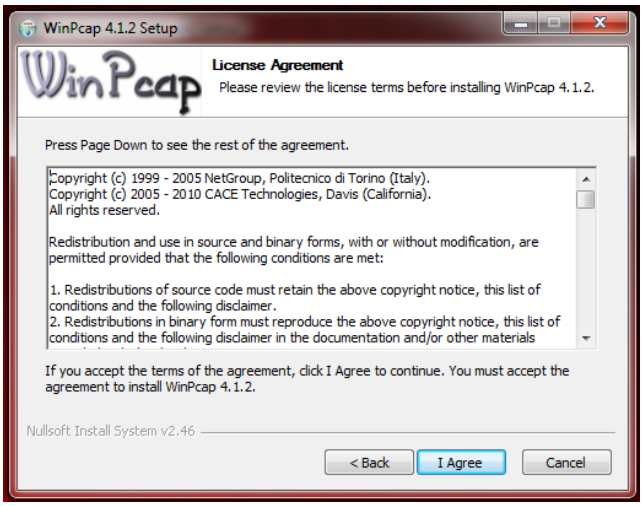


Figura 59 Instalación de Wireshark en Microsoft Windows Paso N°10 – Tomada de Wireshark

Leer y aceptar las condiciones de la licencia de WinCap, haga clic en Estoy de acuerdo para aceptar los términos de la licencia y continuar.

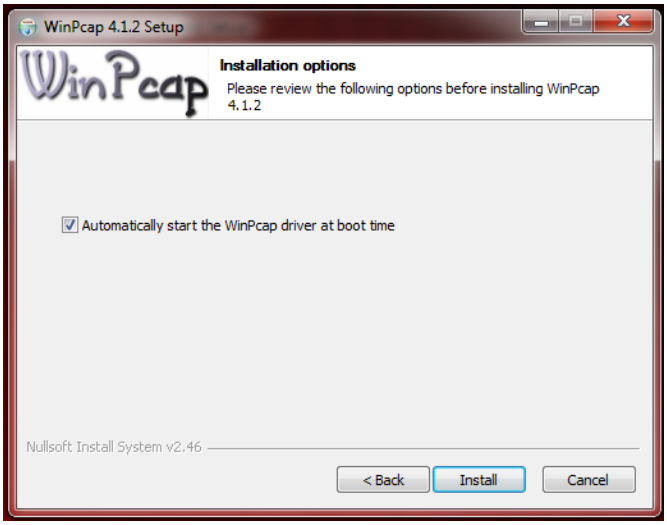


Figura 60 Instalación de Wireshark en Microsoft Windows Paso N°11 – Tomada de Wireshark

Elegir si se iniciara automáticamente los controladores de WinCap en el tiempo de reinicio. Haga clic en siguiente para continuar.

Figura 61 Instalación de Wireshark en Microsoft Windows Paso N°12 – Tomada de Wireshark

En esta pantalla siguiente muestra que las librerías WinCap han completado el asistente la instalación, Haga clic en Terminar para continuar.

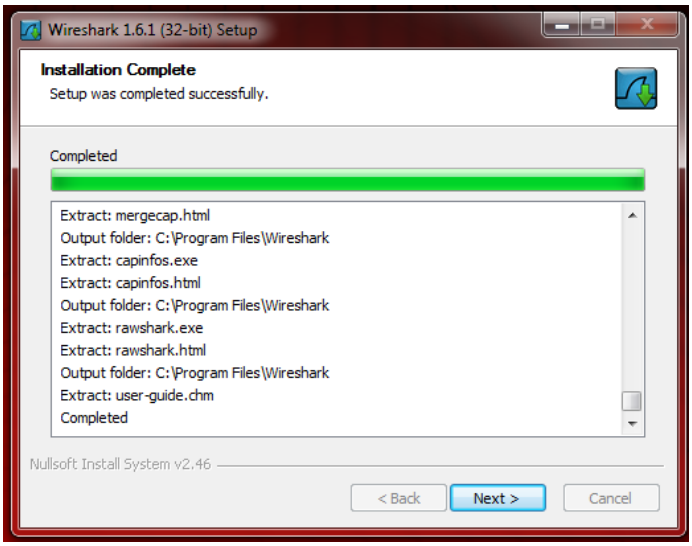


Figura 62 Instalación de Wireshark en Microsoft Windows Paso N°13 – Tomada de Wireshark

La pantalla siguiente muestra que la instalación de Wireshark se ha realizado satisfactoriamente. Haga clic en siguiente para continuar.

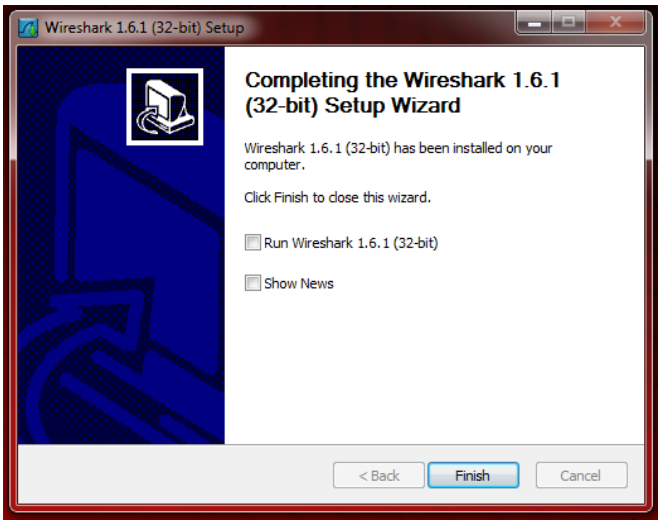


Figura 63 Instalación de Wireshark en Microsoft Windows Paso N°14 – Tomada de Wireshark

El asistente ha completado la instalación de Wireshark indicando que se la herramienta se instalado correctamente en la computadora, las dos casilleros de selección son opcionales ejecutar wireshark después de cerrar el asistente y mostrar noticias en la web sobre Wireshark. Haga en clic en terminar para cerrar el asistente.

Anexo 2 Manual de Instalación de Wireshark en Sistemas Linux

Para la instalación de Wireshark en sistemas Linux emplearemos el método YellowDog Updater, Modifier YUM es una herramienta de código abierto, basada en línea de comandos para la gestión de paquetes utilidad para paquetes RPM compatible con sistemas Linux. Este es un método automático de la instalación, actualización y la eliminación de paquetes RPM. Para el ejemplo se realiza el proceso de instalación de Wireshark en Fedora 14.

Figura 64 Instalación de Wireshark en sistemas Linux Paso N°01 – Tomada de Fedora 14

En la siguiente pantalla muestra como abrir una ventana de terminal en Fedora 14 para poder trabajar con línea de comandos. Haga clic en Terminal para continuar.

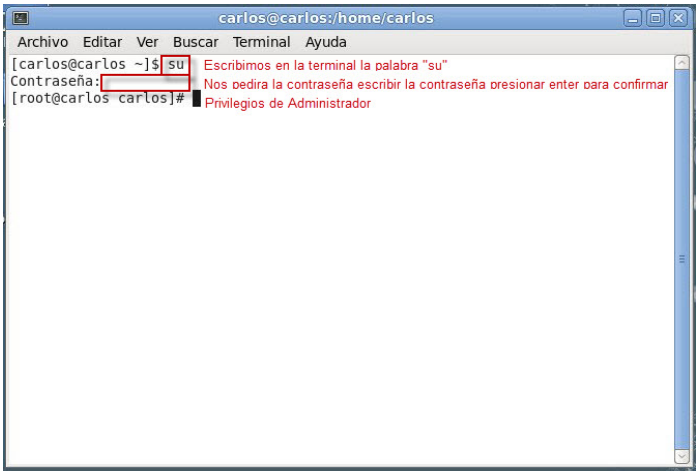


Figura 65 Instalación de Wireshark en sistemas Linux Paso N°02 – Tomada de Fedora 14

En la pantalla de terminal escribimos la palabra “SU” es una utilidad de los sistemas operativos de tipo Linux que permite usar el intérprete de comandos de otro usuario como Administrador sin necesidad de cerrar la sesión. Para la instalación necesitaremos permisos de administrador, en caso se debe pedir autorización al administrador de los sistemas, en la siguiente línea pedirá que

introduzcamos la contraseña de administrador, presionamos enter para confirmar.

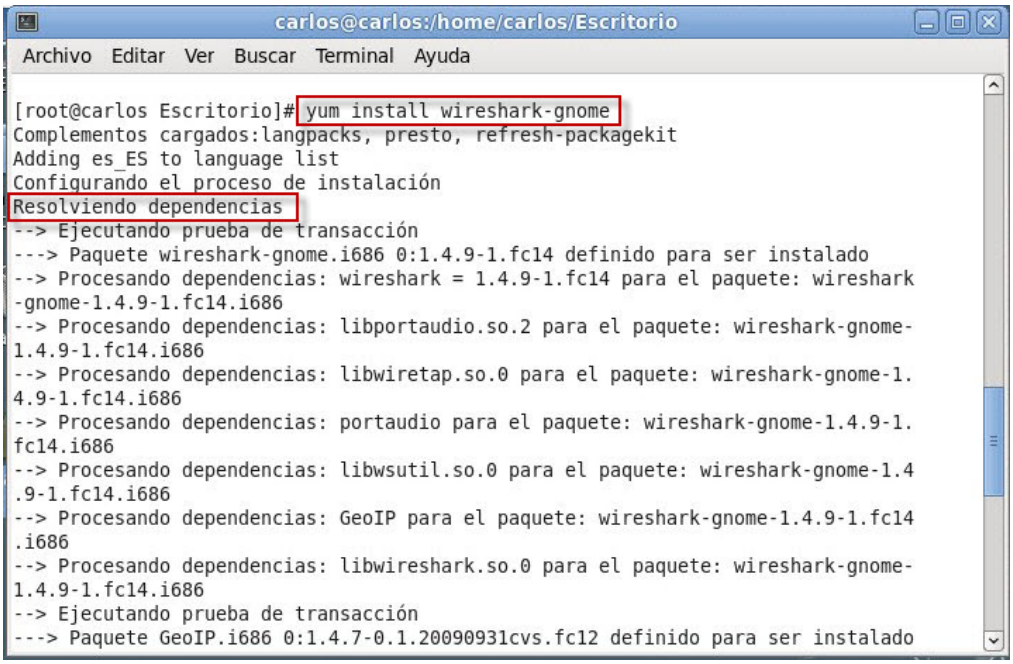


Figura 66 Instalación de Wireshark en sistemas Linux Paso N°03 – Tomada de Fedora 14

En la pantalla de terminal escribimos la siguiente línea **Yum install wireshark-gnome** después presionamos enter enseguida empieza a cargar todos los complementos necesarios y resuelve todas las dependencias en cambio con paquetes RPM la instalación de Wireshark puede ser un proceso muy complicado debido a las dependencias, YUM se encarga de las dependencias automáticamente y hace todo el trabajo.

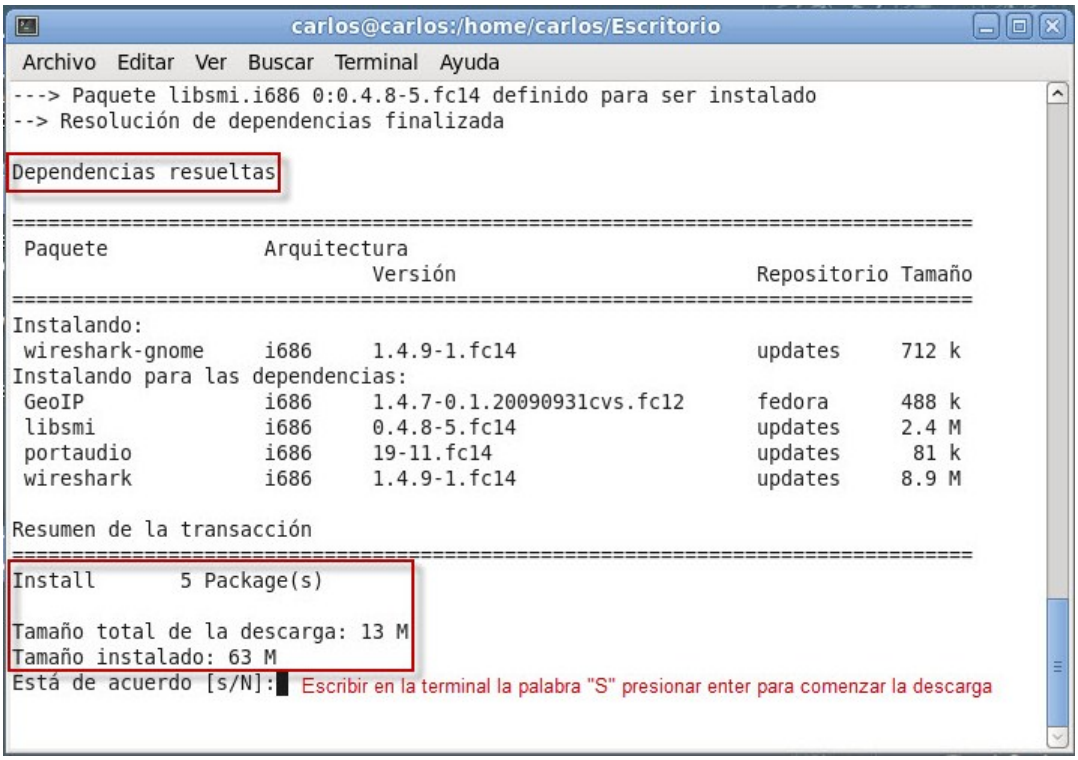


Figura 67 Instalación de Wireshark en sistemas Linux Paso N°04 – Tomada de Fedora 14

En esta pantalla se muestra como todas las dependencias han sido resueltas y a continuación se muestra todos los paquetes necesarios con su arquitectura esto depende del equipo en donde se realiza la instalación, versión del paquete, repositorio indica si es actualización en caso de existir el paquete, caso contrario una instalación de un nuevo paquete y el tamaño del mismo.

En el cuadro de abajo se muestra el resumen de la transacción como numero de paquetes, tamaño total de la descarga, y el tamaño que actualmente se encuentra instalado en el equipo. Escriba la palabra “S” para dar inicio al proceso de descarga y continuar.

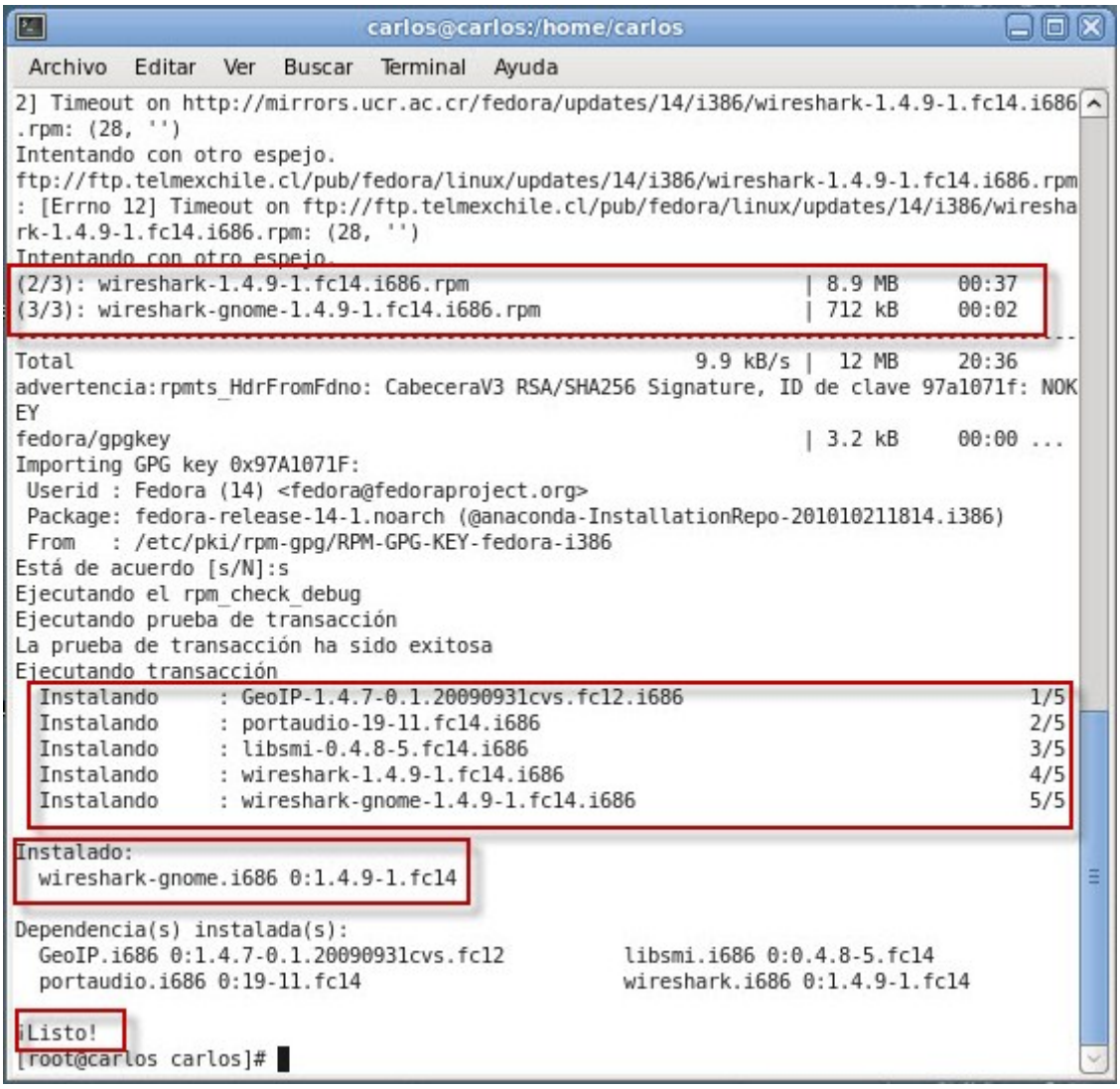


Figura 68 Instalación de Wireshark en sistemas Linux Paso N°05 – Tomada de Fedora 14

Se muestra los paquetes RPM descargados e inicia el proceso de instalación uno por uno hasta completar todo el proceso, en el último recuadro muestra instalado correctamente wireshark y nos muestra un mensaje listo indicando que la herramienta Wireshark está preparada para su uso.

Anexo 3 Formato de la Encuesta

1.-.Sabe que es un software analizador de Red

[ ] Si [ ] No

2.- Conoce Herramientas de Software para el análisis de Redes.

[ ] Si [ ] No

Cuales

_____

_____

3.- ¿Ha trabajado antes con alguna herramienta de software para el análisis de Redes?

[ ] Si [ ] No

4.- ¿Seleccione con qué frecuencia se debería realiza un análisis en la red?

[ ] Continuamente

[ ] Parcialmente

[ ] Solamente cuando se presenta un problema en la red

5.- ¿Conoce que es Wireshark?

[ ] Si [ ] No

6.- Ha empleado Wireshark en una Red

[ ] Si [ ] No

7.- Con la utilización de un analizador de red cree UD. que ayudarían a solucionar los problemas dentro de una red.

[ ] Si [ ] No

¿Por qué?

_____

_____

8.- Estaría de acuerdo que en una red se implemente un software informático para el análisis de redes.

[ ] Si [ ] No

¿Por qué?

_____

_____