**CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERIAS**

**DEPARTAMENTO DE CIENCIAS COMPUTACIONALES**

**SEMINARIO DE SOLUCIÓN DE PROBLEMAS DE REDES DE COMPUTADORAS Y PROTOCOLOS DE COMUNICACIÓN**

**SECCIÓN:** D15

**EQUIPO No.** 2

**INTEGRANTES:**

1. Gomez Casillas Hector Samuel
2. García Pérez Angel
3. Ramírez Castellanos Daniel Iván
4. Ramos Orozco Cristian Agustin

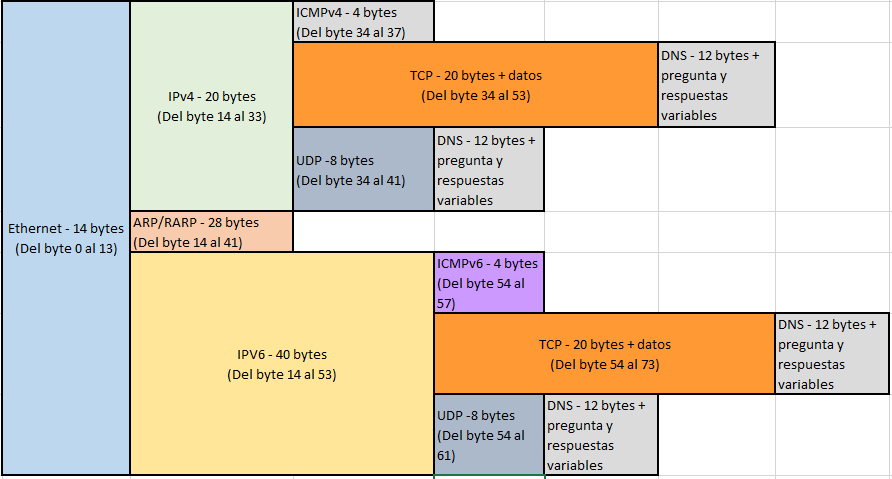
30/Noviembre/2021

**PROYECTO FINAL**

**Nombre de la práctica:** Captura de paquetes en tiempo real.

**Objetivo:** Desarrollar un Sniffer, es decir, un programa que analice los diferentes protocolos (Ethernet, IPv4, IPv6, ICMPv4, ICMPv6, ARP/RARP, TCP, UDP y DNS) en tiempo real con la lectura de la tarjeta de red.

**Introducción.**



* **Ethernet (0-13).**

Este protocolo se encuentra en la primera capa del modelo OSI y se encarga de las direcciones físicas (MAC Address), así como identificar el tipo de protocolo que seguirá (IP, o ARP).

* **IPv4 (14-33).**

Este protocolo se ubica en entre las capas de enlace y red del modelo OSI, este protocolo es uno de los más importantes pues brinda cierta información acerca de las capas mencionadas, como son las direcciones IP, la longitud que tienen los datos, si estos datos van en buen estado, si se pueden dividir los paquetes, entre otras.

* **ICMPv4 (34-37).**

Este protocolo se ubica en el mismo lugar que IP, ya que dentro de IP puede suceder que se llegue a este protocolo. ICMP controla si un paquete no puede alcanzar su destino, si su vida ha expirado, si el encabezamiento lleva un valor no permitido, si es un paquete de eco o respuesta, etc. Es decir, se usa para manejar mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado.

* **TCP (34-53).**

Este protocolo se ubica en la capa de transporte del modelo OSI. Envía cada parte como datagrama IP independiente. Cuando llegan a una máquina datagramas IP que contienen datos TCP, son entregados a la entidad TCP, que reconstruye las corrientes originales de bytes.

* **UDP (34-41).**

El protocolo UDP (User Datagram Protocol, Protocolo de datagrama de usuario) es un protocolo no orientado a conexión de la capa de transporte del modelo TCP/IP. Este protocolo es muy simple ya que no proporciona detección de errores (no es un protocolo orientado a conexión).

* **DNS.**

La cabecera de TCP o UDP deben de tener el puerto de origen o de destino número 53 para saber que lo que sigue es un paquete de DNS.

Es posible asociar nombres en lenguaje normal con direcciones numéricas gracias a un sistema llamado DNS (Domain Name System, sistema de nombres de dominio). Esta correlación entre las direcciones IP y el nombre de dominio asociado se llama resolución de nombres de dominio (o resolución de direcciones).

* **ARP/RARP (14-41).**

El protocolo ARP es un protocolo estándar específico de las redes. Su status es electivo. El protocolo de resolución de direcciones es responsable de convertir las dirección de protocolo de alto nivel(direcciones IP) a direcciones de red físicas. El módulo ARP intenta hallar la dirección en su caché. Si encuentra el par buscado, devuelve la correspondiente dirección física de 48 bits al llamador(el manejador de dispositivo). Si no lo encuentra, descarta el paquete (se asume que al ser un protocolo de alto nivel volverá a transmitirlo) y genera un broadcast de red para una solicitud ARP.

* **IPv6 (14-53).**

Este protocolo es similar a IPv4, sin embargo cuenta con características diferentes además de campos diferentes aunque algunos con el mismo funcionamiento que en IPv4. Una de las características de IPv6 es que cuenta con direcciones más grandes; siendo de 16 bytes cada una y en hexadecimal, además de ya no haber un “checksum” (suma de comprobación) ya que se considera como un protocolo más seguro.

* **ICMPv6 (54-57).**

Es una nueva versión de ICMP y es una parte importante de la arquitectura IPv6 que debe estar completamente soportada por todas las implementaciones y nodos IPv6. ICMPv6 combina funciones que anteriormente estaban subdivididas en varias partes de diferentes protocolos tales como ICMP, IGMP o ARP y además introduce algunas simplificaciones eliminando tipos de mensajes obsoletos que estaban en desuso actualmente.

* **TCP (54-73).**

Explicación dentro de la parte de IPv4

* **UDP (54-61).**

Explicación dentro de la parte de IPv4.

* **DNS.**

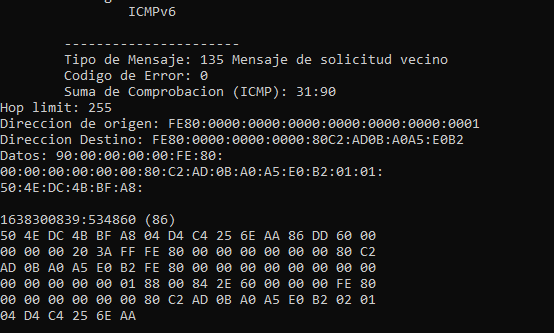
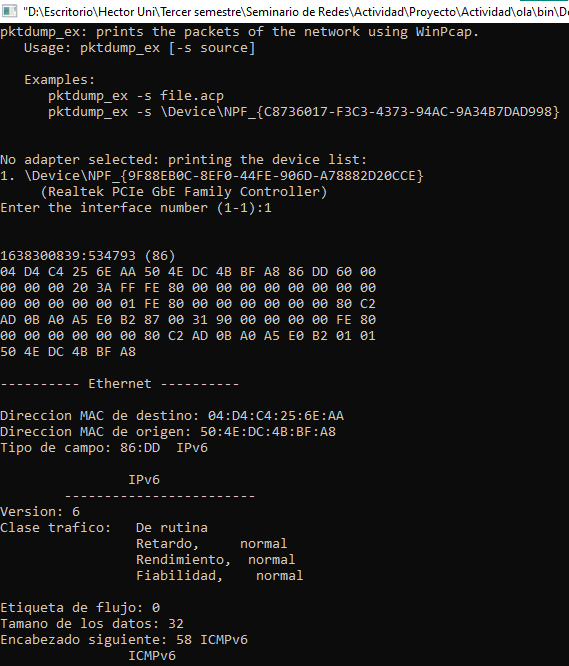
Explicación dentro de la parte de IPv4.

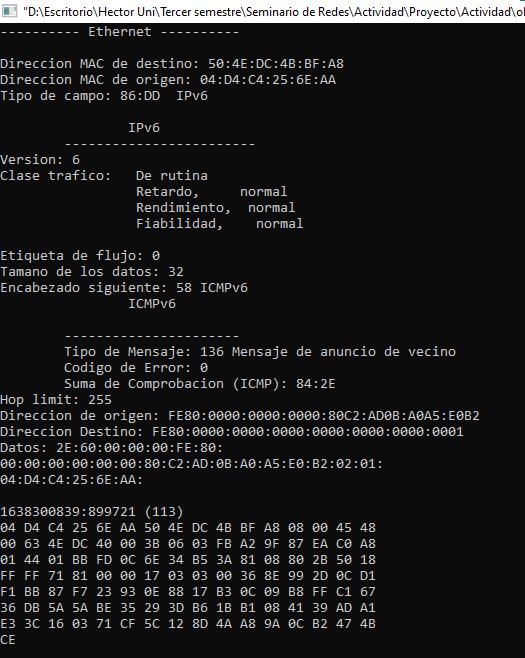
**Desarrollo.**

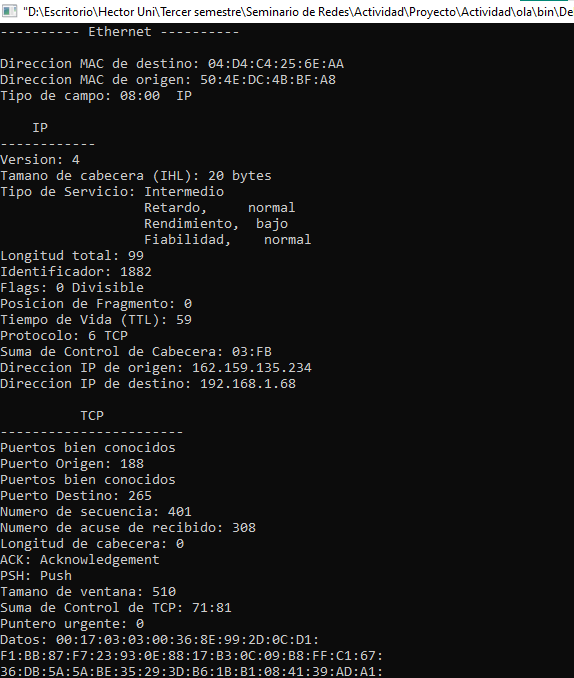
La implementación del “sniffer” se basa principalmente en la parte programada previamente de los protocolos de las diferentes capas del modelo OSI. Puesto que ya se cuenta con esta parte, solo queda la generación de los paquetes en tiempo real.

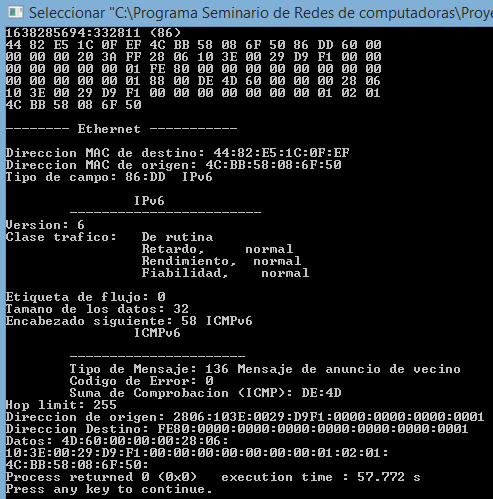
Para esto se empleó de una librería externa la cual es “pcap”; esta librería nos ayudará ya que generará mediante la tarjeta de internet de nuestra computadora, paquetes que estos a su vez pasarán por el programa y se traducen mostrándonos los diferentes protocolos ya revisados anteriormente, por lo cual es bastante importante la correcta instalación de esta librería y la vinculación con esta.

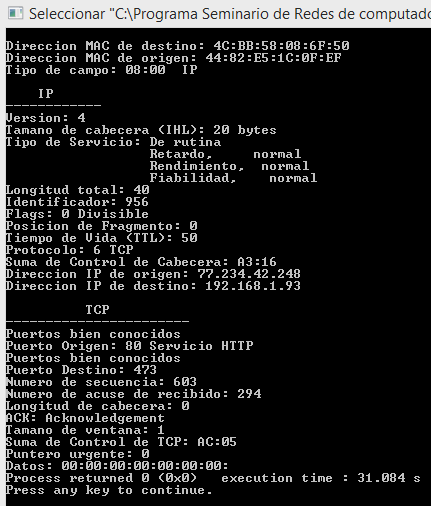
**Pantalla del Ejecutable.**

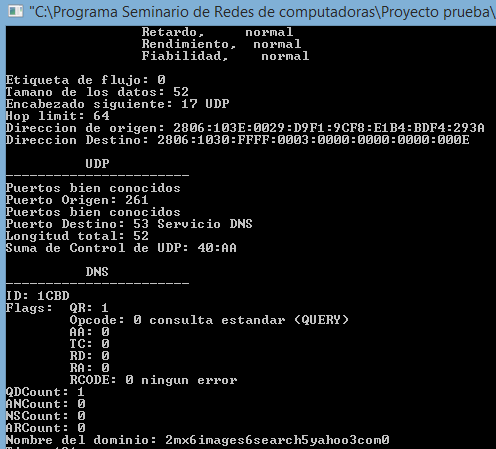
****

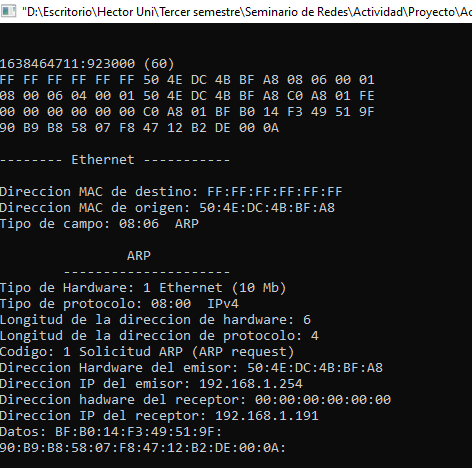
****

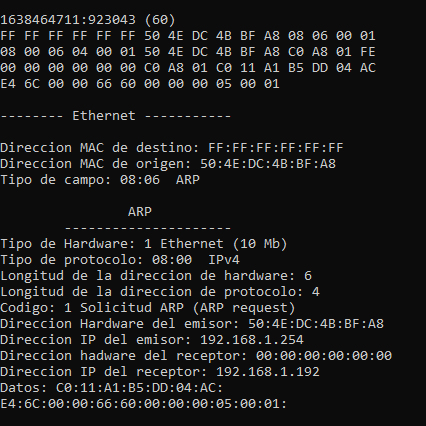
****

****

****

****

****

****

**Conclusiones.**

En esta práctica se capturaron paquetes de datos en tiempo real mediante el uso de nuestra tarjeta de internet interna de la computadora, donde una vez que muestra el paquete en hexadecimal este se traducirá en base a las diferentes capas del modelo OSI para comprender mejor la captura de estos paquetes.

Para la comprensión de estos paquetes, se estudiaron los diferentes campos de cada uno de los protocolos que se muestran; Ethernet, IPv4 y IPv6, ARP/RARP, TCP, UDP y DNS. En cada uno de estos protocolos se tomaron en cuenta el tamaño de cada uno de sus campos para después de estos implementarlos en un programa (sniffer) donde se muestren los campos correspondientes.

Como se puede observar en las ejecuciones, ya no se cuenta con un archivo en el cual los datos son los mismos, ahora se muestran diferentes datos, mostrando diferentes protocolos. En este caso se pudieron obtener todos los protocolos estudiados: Ethernet, IPv4, IPv6, ICMP, ARP, TCP, UDP y DNS. Un aspecto importante a mencionar en DNS que debido a la ejecución rápida por la lectura de los paquetes no se alcanza a mostrar todo lo demás sin embargo se alcanzó a capturar la parte donde se pueden observar los contadores, los cuales indicarán las entradas a preguntas (“question”) o respuestas (“answer”) que tendremos en este caso tenemos un question y este muestra el nombre del dominio. También podemos apreciar en las capturas el protocolo ICMPv6 así como ARP y estos fueron más comprensibles a la hora de hacer la captura de paquetes en tiempo real.

Por último, lo que aprendimos durante el curso fueron los diferentes protocolos, así como los campos de estos, aprendimos a leer y reconocer de un paquete de datos dichos campos y los protocolos que nos pueden dar y en qué consisten estos protocolos del modelo OSI.