**CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERÍAS**

**DEPARTAMENTO DE CIENCIAS COMPUTACIONALES**



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

**SECCIÓN:** D04

**EQUIPO No.** 2

**INTEGRANTES:**

1. Madrigal Escoto Miguel Arturo

2. Flores Ontiveros Aide Sarahi

3. Cervantes Castoño Oswaldo Gael

4. Vallejo Sierra José Ulises

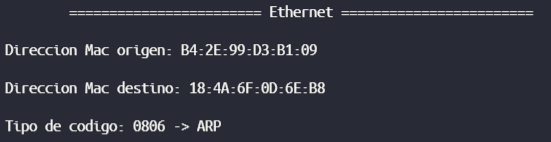
5. Fernández Román Kevin Arturo

**PRÁCTICA No.** 10

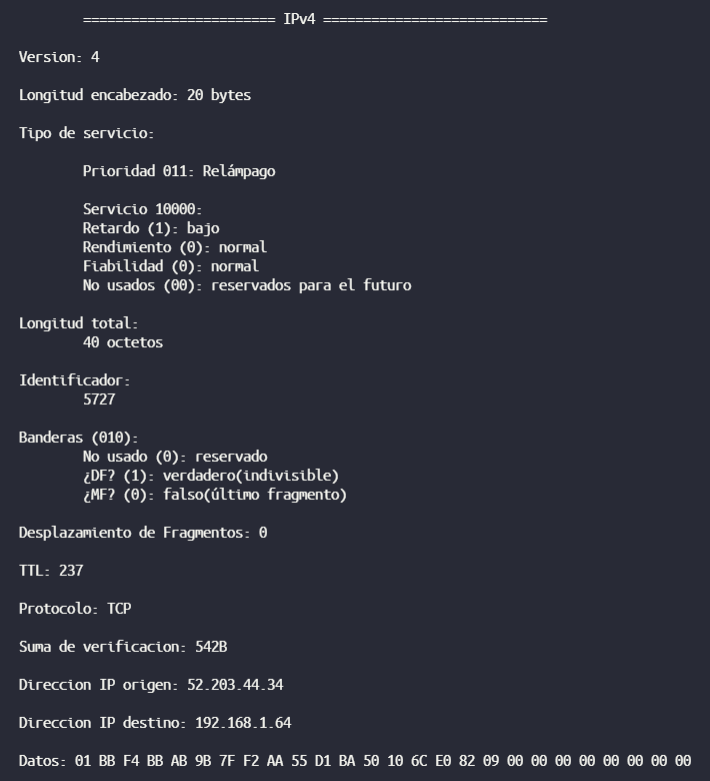
**Nombre de la práctica:** Captura de paquetes en tiempo real

**Objetivo**:

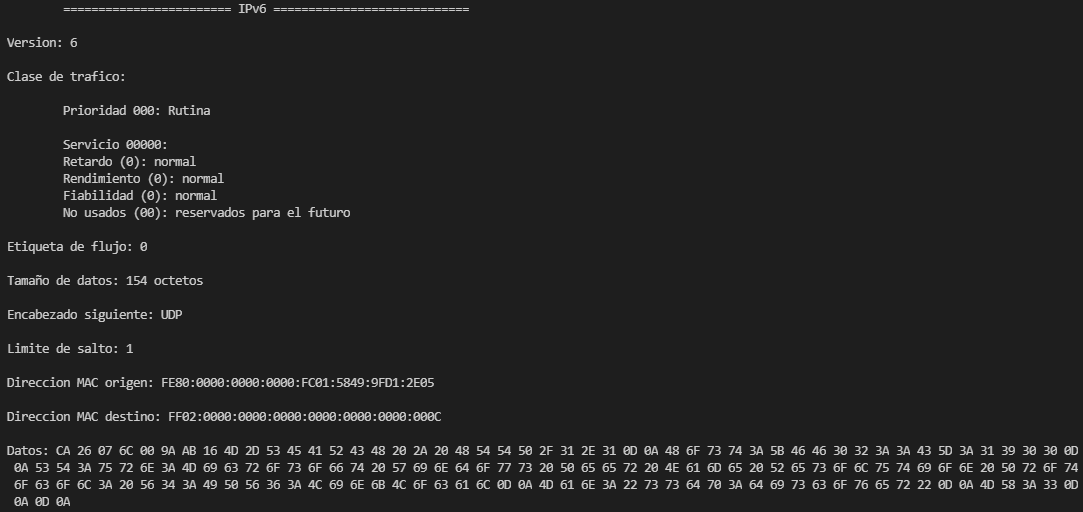
Desarrollar un Sniffer, es decir, un programa que analice los diferentes protocolos en tiempos real con la lectura de la tarjeta de red.

**Pantallas del ejecutable:**

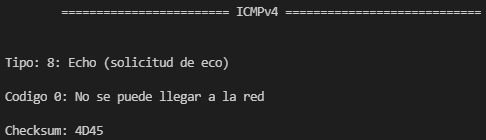
**Figura 1.0** Análisis del paquete del protocolo Ethernet



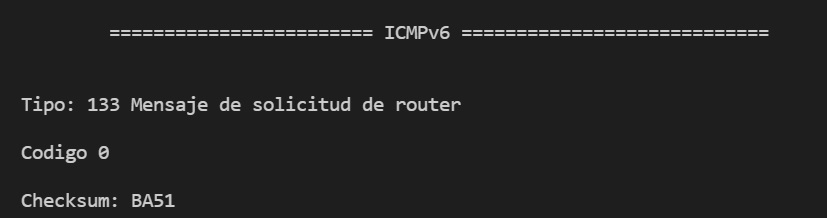
**Figura 1.1** Análisis del paquete del protocolo IPv4



**Figura 1.2** Análisis del paquete del protocolo IPv6



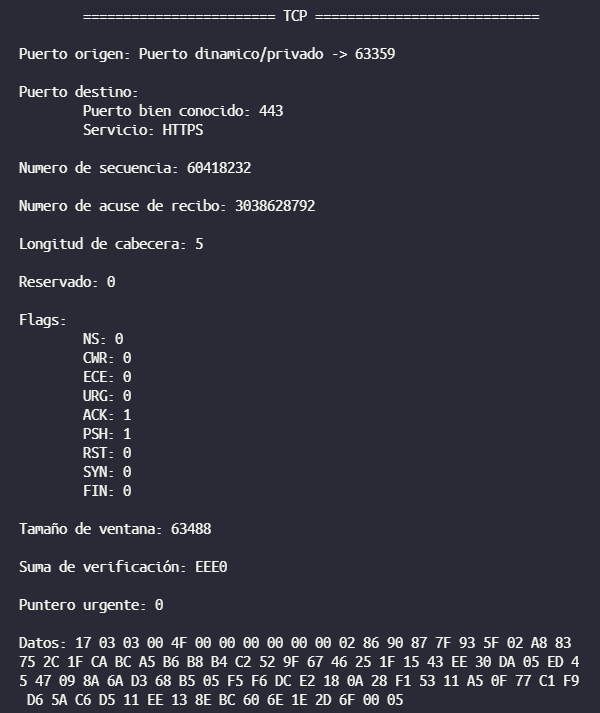
**Figura 1.3** Análisis del paquete del protocolo ICMPv4



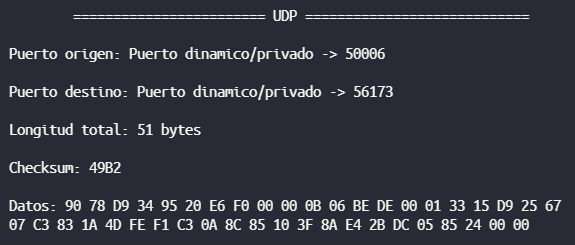
**Figura 1.4** Análisis del paquete del protocolo ICMPv6



**Figura 1.5** Análisis del paquete del protocolo ARP/RARP



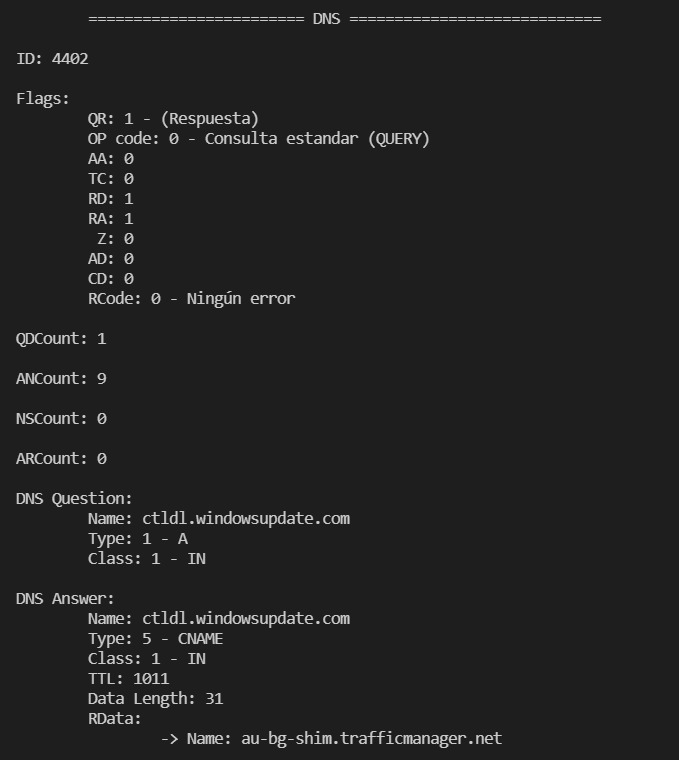
**Figura 1.6** Análisis del paquete del protocolo TCP

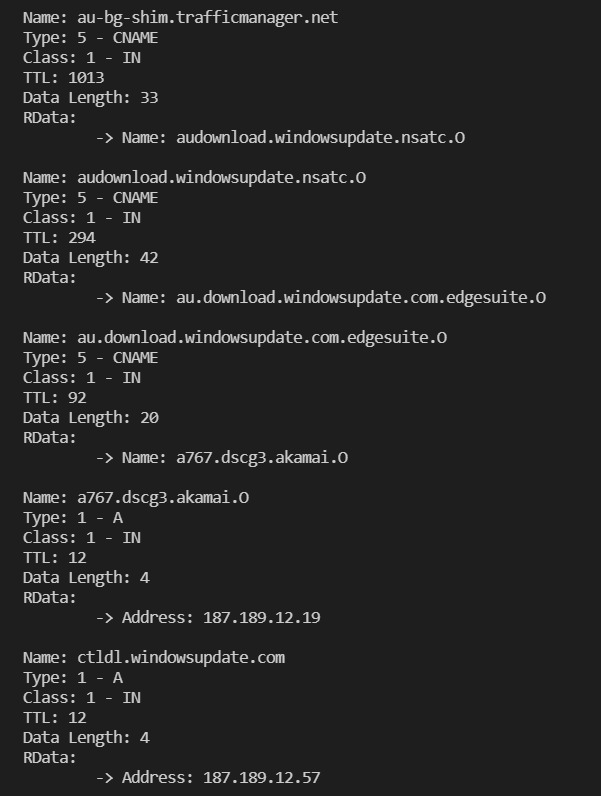


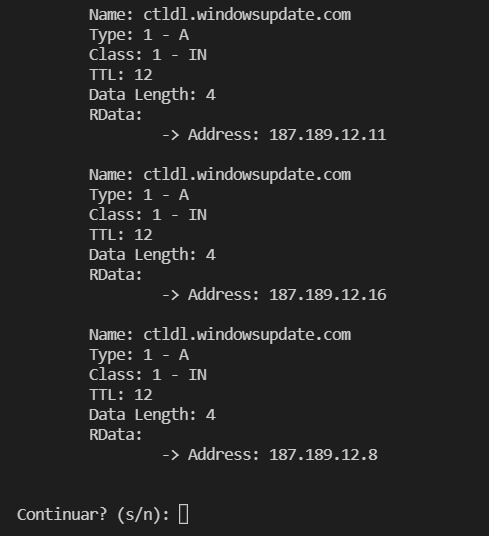
**Figura 1.7** Análisis del paquete del protocolo UDP



**Figura 1.8** Análisis del paquete del protocolo DNS (pregunta)







**Figura 1.9** Análisis del paquete del protocolo DNS (respuesta)

**Conclusiones:**

En conclusión, esta práctica fue algo compleja porque no teníamos mucha idea de que librería nos puede ser de utilidad para el análisis de paquetes en tiempo real, y nos dimos cuenta de que la librería scapy era la mejor opción por las funciones tan completas que trae, además de que su utilización es sencilla, ya que solo basta descargar la librería desde la línea de comandos y la documentación explica muy bien cómo usarla.

Tuvimos la dificultad, de que en el campo “cname” se nos desplegaban caracteres raros al hacer la lectura y obtener el cada carácter con el código ASCII; por lo cual pudimos solucionar ese problema validando si el carácter convertido este dentro de los caracteres validos para una URL, para lo cual usamos una lista con dichos caracteres válidos. Para esto nos basamos leyendo el RFC 3986, el cuál especifica los caracteres y requisitos con los que debe cumplir una URL.

En todos los protocolos al leer los paquetes en tiempo real de un archivo binario no se tuvo problema, solamente en el protocolo DNS ya que no había una respuesta para probar. Después nos dimos cuenta de que para obtener la respuesta bastaba con visitar una pagina en el navegador para que nos diera dicha respuesta y así corregimos los errores que teníamos en esa parte del DNS. Para ver dichos paquetes DNS tuvimos que hacer un filtrado como el puerto origen 53 para que nos los mostrara, ya que a veces no se muestran dichos paquetes porque predominan paquetes de otros protocolos como TCP y UDP.

**Nota:** Se anexa el código fuente en el archivo equipo2.zip