

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. 8

INTEGRANTES:

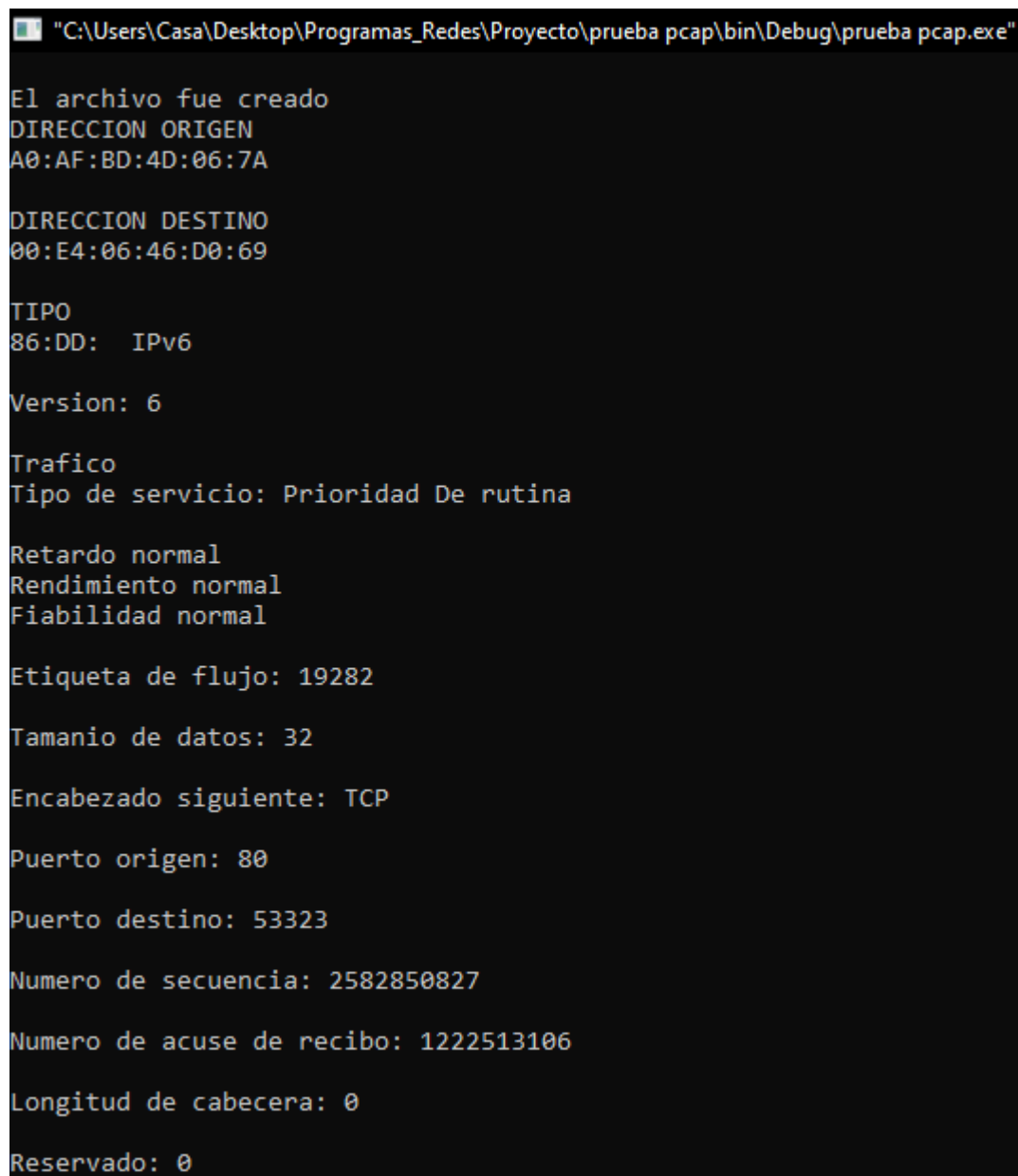
1. Reyes Rico Carlos
2. Serrano Zumaya Miguel Angel
3. Domínguez Amezcua Marco Aurelio
4. Avalos Torres Juan Carlos

Nombre del reporte: 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 y muestre cada uno de los que se vio en clase, tales como son:

Pantallas del ejecutable:



```
"C:\Users\Casa\Desktop\Programas_Redes\Proyecto\prueba pcap\bin\Debug\prueba pcap.exe"

El archivo fue creado
DIRECCION ORIGEN
A0:AF:BD:4D:06:7A

DIRECCION DESTINO
00:E4:06:46:D0:69

TIPO
86:DD:  IPv6

Version: 6

Trafico
Tipo de servicio: Prioridad De rutina

Retardo normal
Rendimiento normal
Fiabilidad normal

Etiqueta de flujo: 19282

Tamano de datos: 32

Encabezado siguiente: TCP

Puerto origen: 80

Puerto destino: 53323

Numero de secuencia: 2582850827

Numero de acuse de recibo: 1222513106

Longitud de cabecera: 0

Reservado: 0
```

Ilustración 1 IPv6 / TCP

```
"C:\Users\Casa\Desktop\Programas_Redes\Proyecto\prueba pcap\bin\Debug\prueba pcap.exe"

Reservado: 0

Banderas:

  NS : 0
  CWR : 0
  ECE : 0
  URG : 0
  ACK : 1
  PSH : 0
  RST : 0
  SYN : 0
  FIN : 0

Tamano de ventana: 501
Checksum: 0C:92
Puntero urgente: 0

Limite de salto: 1

Direccion IP origen: 0001:0005:000a:0048:00de:0011:00d1:0048:00de
Direccion IP destino: 0011:00d2:0000:00e4:0006:0046:00d0:0069:00a0

DATOS
:AF:BD:4D:06:7A:08:00:45:00:00:46:39:A7:40:00:80:06:E4:DE:C0:A8:64:57:9D:
:10:51:38:24:1D:27:01:CF:2F:57:79:54:B3:34:A1:F0:A7:BC:E9:2E:45:00:E4:06:
:54:01:BB:E8:95:B9:1F:42:1B:99:02:50:10:02:02:A9:9D:00:00:17:03:03:34:BE:
:19:C7:F1:3D:55:A4:13:12:AB:16:37:C8:B4:9B:B1:4D:39:91:D2:17:EC:18:DF:00:
:ED:E7:71:B5:2B:C7:76:D8:95:90:F0:CF:A0:B4:17:D5:09:29:37:70:79:0C:E9:2D:
:75:E8:C6:BC:59:04:1E:59:DE:85:AD:61:58:DF:92:A5:E3:C4:1E:3D:A7:91:89:E6:
:49:47:AC:77:A3:38:BE:9C:A8:21:2F:D5:5B:58:C0:D9:8D:D6:E1:FA:B1:80:67:39:
:E2:32:85:6A:D2:1F:CC:C8:7D:9E:D1:61:7E:45:25:86:EC:BB:2B:42:68:F2:35:C3:
:9D:3C:04:D9:ED:E5:8B:AD:0D:79:43:63:97:F5:72:B4:2E:D3:46:19:6A:A0:A6:57:
Process returned 0 (0x0)   execution time : 3.585 s
Press any key to continue.
```

Ilustración 2 IPv6 / TCP

```
"C:\Users\Casa\Desktop\Programas_Redes\Proyecto\prueba pcap\bin\Debug\prueba pcap.exe"

El archivo fue creado
DIRECCION ORIGEN
A0:AF:BD:4D:06:7A

DIRECCION DESTINO
00:E4:06:46:D0:69

TIPO
08:00:

Paquete IPv4

Version: 4
Tamaño: 5

Tipo de servicio: Prioridad De rutina

Retardo normal
Rendimiento normal
Fiabilidad normal

Longitud total: 112 bytes
Identificador: 16906

Banderas
Bit 0: Reservado
Bit 1: No divisible
Bit 2: Ultimo Fragmento

Posicion de fragmento: 0

Tiempo de vida: 88

Protocolo:
-----
TCP
Puerto origen: 22273
Puertos registrados

Puerto destino: 48080
Puertos registrados

Numero de secuencia: 1413618695
```

Ilustración 3 IPv4 / TCP

```

"C:\Users\Casa\Desktop\Programas_Redes\Proyecto\prueba pcap\bin\Debug\prueba pcap.exe"

Numero de secuencia: 1413618695
Numero de acuse de recibo: 3605566992
Longitud de cabecera: 11
Reservado: 22

  NS : 1
  CWR : 0
  ECE : 1
  URG : 0
  ACK : 1
  PSH : 0
  RST : 0
  SYN : 0
  FIN : 0

Tamano de ventana: 6147
Checksum: 7F:52
Puntero urgente: 64768

-----
Checksum: 00:17

Direccion IP origen: 87.1.187.208
Direccion IP destino: 84.66.28.7

DATOS
:D6:E8:96:10:B7:50:18:03:7F:52:FD:00:00:17:03:03:00:43:4B:6A:2B:28:3C:40:49:A4:01:19:CC:64:
:AD:04:B5:57:FD:DC:EE:BD:64:D2:42:91:48:8D:48:2D:3B:7C:DE:58:C4:0F:0C:55:68:57:76:64:BE:A0:
:2E:A2:E2:C0:A8:64:57:01:BB:D1:00:E0:A9:F4:BF:EB:18:E1:C1:50:18:08:00:99:BF:00:00:17:03:03:
:48:2D:4E:7A:1D:48:EE:D3:38:C5:2E:B1:CF:AB:DF:BC:19:36:8F:02:6E:B9:CE:24:4B:A0:AF:BD:4D:06:
:A8:64:57:01:BB:D1:00:E0:A9:F4:F5:EB:18:E6:CE:50:10:08:03:FD:7D:00:00:00:00:00:00:00:00:FF
Process returned 0 (0x0)   execution time : 2.425 s
Press any key to continue.

```

Ilustración 4 IPv4 / TCP

```
"C:\Users\Casa\Desktop\Programas_Redes\Proyecto\prueba pcap\bin\Debug\prueba pcap.exe"

El archivo fue creado
DIRECCION ORIGEN
FF:FF:FF:FF:FF:FF

DIRECCION DESTINO
64:FD:96:09:C4:67

TIPO
08:00:

Paquete IPv4

Version: 4
Tamano: 5

Tipo de servicio: Procesando llamada crítica y de emergencia

Retardo bajo
Rendimiento alta
Fiabilidad normal

Longitud total: 106 bytes
Identificador: 60834

Banderas
Bit 0: Reservado
Bit 1: No divisible
Bit 2: Ultimo Fragmento

Posicion de fragmento: 0

Tiempo de vida: 64

Protocolo: UDP

-----

Puerto origen: 9431 : Puertos registrados

Puerto destino: 9431 : Puertos registrados

Longitud Total: 86
Checksum: A6:F8
```

Ilustración 5 IPv4 / UDP

```
"C:\Users\Casa\Desktop\Programas_Redes\Proyecto\prueba pcap\bin\Debug\prueba pcap.exe"
Checksum: A6:F8
-----
Checksum: 69:73
Direccion IP origen: 36.215.36.215
Direccion IP destino: 0.86.166.248

DATOS
:69:73:6D:3A:2F:2F:31:39:32:2E:31:36:38:2E:31:30:30:2E:37:35:3A:39:3
:26:73:73:6C:4D:74:68:64:3D:6E:6F:6E:65:23:56:65:72:3D:32:2E:31:00:0
:D1:02:01:BB:24:F6:EB:0B:F9:99:E5:E0:50:11:01:02:FE:D0:00:00:A0:AF:0
Process returned 0 (0x0)   execution time : 4.925 s
Press any key to continue.
```

Ilustración 6 IPv4 / UDP


```
"C:\Users\Casa\Desktop\Programas_Redes\Proyecto\prueba pcap\bin\Debug\prueba pcap.exe"
El archivo fue creado
DIRECCION ORIGEN
00:E4:06:46:D0:69

DIRECCION DESTINO
A0:AF:BD:4D:06:7A

TIPO
08:00:

Paquete IPv4

Version: 4
Tamano: 5

Tipo de servicio: Prioridad De rutina

Retardo normal
Rendimiento normal
Fiabilidad normal

Longitud total: 110 bytes
Identificador: 14862

Banderas
Bit 0: Reservado
Bit 1: No divisible
Bit 2: Ultimo Fragmento

Posicion de fragmento: 0

Tiempo de vida: 128

Protocolo:
-----
TCP
Puerto origen: 53332
Puertos dinamicos o privados

Puerto destino: 443
Puertos bien conocidos
Servicio HTTPS
TCP
Protocolo TCP
```

Ilustración 9 IPv4 TCP

```
"C:\Users\Casa\Desktop\Programas_Redes\Proyecto\prueba pcap\bin\Debug\prueba pcap.exe"
T¿Protocolo TCP

Numero de secuencia: 3902153363

Numero de acuse de recibo: 1109137441

Longitud de cabecera: 5

Reservado: 16

Banderas:

  NS : 0
  CWR : 0
  ECE : 0
  URG : 0
  ACK : 1
  PSH : 1
  RST : 0
  SYN : 0
  FIN : 0

Tamano de ventana: 515
Checksum: 70:AB
Puntero urgente: 0

-----

Checksum: 17:03

Direccion IP origen: 208.84.1.187
Direccion IP destino: 232.150.34.147

DATOS
:42:1C:18:21:50:18:02:03:70:AB:00:00:17:03:03:00:41:11:A3:28:4E:D9:
:F8:04:A8:BD:76:EF:6B:02:B8:7A:FF:01:9A:F4:71:0E:C7:E2:70:86:46:94:
:C0:A8:64:57:01:BB:D0:54:42:1C:18:21:E8:96:22:D9:50:10:03:95:98:56:
:9D:F0:19:3C:C0:A8:64:57:01:BB:D0:54:42:1C:18:21:E8:96:22:D9:50:18:
:25:C9:8E:56:0B:17:BE:F5:E6:D4:00:03:C9:F5:4B:FF:3D:4F:A7:5D:4F:25:
Process returned 0 (0x0)   execution time : 5.670 s
Press any key to continue.
```

Ilustración 10 IPv4 TCP

Conclusiones:

Se logró concretar la programación de este Sniffer, en donde al final se realizó una adaptación con las librerías y la instalación de winPcap, para que pudiera leer paquetes en tiempo real desde nuestra tarjeta de wifi.

En nuestro caso se limitó a mostrar solamente 3 paquetes por cada vez que se corre el programa, para poder visualizar de una forma más orgánica como procesa cada uno de estos, pero cómo lo anexamos anteriormente, se vio cada uno de estos protocolos en tiempo real capturados por nuestra tarjeta wifi.