Trabajo Práctico Grupal Entregable N° 1

Fecha de Entrega: Lunes 8 de Septiembre

Redes de Computadoras 1
Departamento de Ingeniería de Computadoras
Facultad de Informática - Universidad Nacional del Comahue

1. Introducción a Wireshark

La herramienta básica para observar los mensajes intercambiados entre entidades de protocolo en ejecución se llama **rastreador de paquetes** o **sniffer**. Como sugiere el nombre, un rastreador de paquetes captura ("olfatea") mensajes enviados/recibidos desde/por su computadora; normalmente también almacenará y/o mostrará el contenido de los distintos campos de protocolo en estos mensajes capturados. El rastreador en sí es pasivo, observa los mensajes enviados y recibidos por las aplicaciones y protocolos que se ejecutan en su computadora, pero nunca envía paquetes por sí mismo.

La Fig. 1 muestra la estructura de un sniffer de paquetes. La Fig. 1 muestra las ventanas del programa Wireshark.

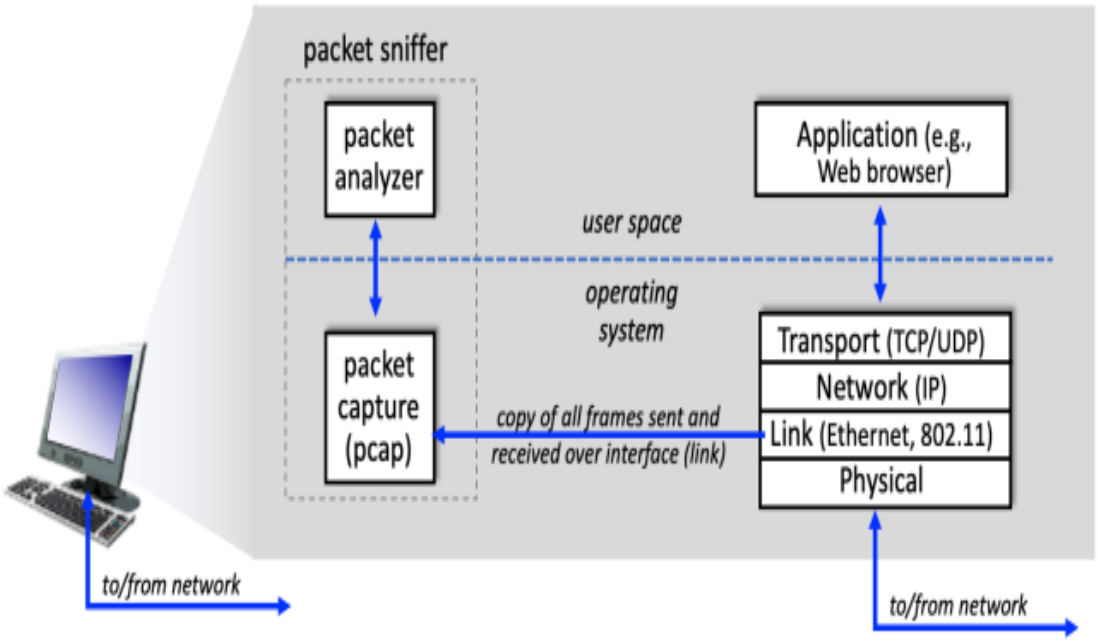

Figura 1: Estructura de un sniffer

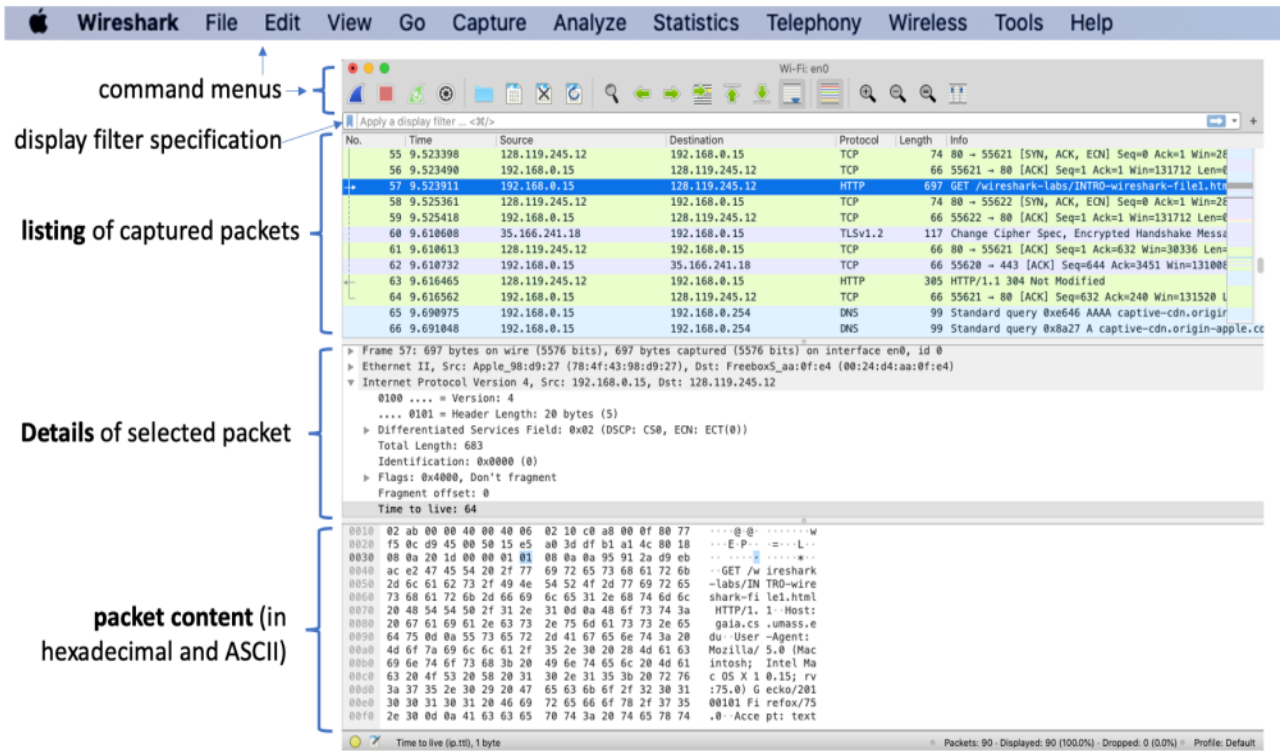

Figura 2: Ventanas de Wireshark

2. ARP

Abrir el archivo *ethernet-ethereal-trace-1* (disponible en PEDCO) con Wireshark y contestar las siguientes preguntas:

1. ¿Cuáles son los valores hexadecimales para las direcciones de origen y destino en la trama Ethernet que contiene el mensaje de Consulta ARP del primer paquete?
2. Proporcione el valor hexadecimal para el campo Tipo de trama Ethernet de dos bytes, del primer paquete. ¿A qué protocolo de capa superior corresponde?
3. ¿Cuál es el valor del campo *opcode* en la consulta ARP del primer paquete? ¿A qué corresponde ese *opcode*?
4. Ahora busque la respuesta ARP que se envió con motivo de la solicitud ARP del primer paquete. ¿A cuántos bytes desde el principio de la trama Ethernet comienza el campo de código de operación ARP?
5. ¿Cuál es la MAC del host que contesta la consulta del primer paquete?
6. Observar la consulta ARP del paquete 6. ¿Por qué no hay respuesta a esa consulta?

3. Ethernet

Abrir el archivo *ethernet-ethereal-trace-1* (disponible en PEDCO) con Wireshark y contestar las siguientes preguntas:

1. Indique la dirección MAC Origen y Destino del paquete 7.
2. Indique la dirección IP Origen y Destino del paquete 7.
3. ¿A qué IP corresponde la MAC Destino indicada en el punto anterior?

4. Popurrí

Abrir el archivo *ethernet-ethereal-trace-1* (disponible en PEDCO) con Wireshark y contestar las siguientes preguntas:

1. El paquete 10, contiene un GET. A qué protocolo de Capa de Aplicación corresponde ese mensaje?
2. ¿Qué protocolo de capa de transporte utiliza ese protocolo de capa de aplicación?
3. ¿Cuál es la IP del servidor que atiende esa solicitud?
4. ¿Puede identificar la dirección MAC del servidor web que atiende esa solicitud?

5. ICMP

Abrir el archivo *ICMP-ethereal-trace-1* (disponible en PEDCO) con wireshark:

1. En el paquete 3, ¿cuál es el valor del campo Protocol de la cabecera IP? ¿A qué protocolo corresponde?
2. ¿Cuál es la función principal de dicho protocolo?
3. Si observamos la cabecera de este protocolo, ¿Cuál es la principal diferencia entre el paquete 3 y 4?

Abrir el archivo *ICMP-ethereal-trace-2* (disponible en PEDCO) con wireshark:

1. ¿A qué IP le hace ping el cliente en esta traza?
2. ¿Esa IP responde el ping enseguida? ¿Por qué?
3. ¿Quién le contesta al cliente la primera vez? ¿Y la cuarta vez?
4. Logra la respuesta del ping en algún momento? Si lo logra, ¿en qué numero de paquete?
5. ¿El campo *Response Time* es parte del protocolo?