Universidad de Costa Rica

Facultad de Ingeniería

Escuela de Ciencias de la Computación e Informática

Redes de comunicación de datos

Tarea 5 Wireshark

2025

Autor

David González Villanueva C13388

I) Exercise One

a) What is the IP address of the client that initiates the conversation?

- 31.247.95.216 (se ve en el paquete 1).

b) Use the first two packets to identify the server that is going to be contacted. List the common name, and three IP addresses that can be used for the server.

- www.google.com
- 64.233.161.99
- 64.233.161.104
- 64.233.161.147

c) What is happening in frames 3, 4, and 5?

- Se establece la conexión TCP (three-way handshake):
- 3 – SYN (cliente→servidor)
- 4 – SYN + ACK (servidor→cliente)
- 5 – ACK (cliente→servidor)

d) What is happening in frames 6 and 7?

- 6 – el cliente envía el GET / HTTP/1.1 para pedir la página raíz.
- 7 – el servidor responde con un ACK TCP, confirmando la recepción de esa petición.

e) Ignore frame eight. However, for your information, frame eight is used to manage flow control.

- Es un ACK de flujo TCP (gestión de ventana), sin información HTTP.

f) What is happening in frames nine and ten? How are these two frames related?

- El Frame 9 transporta el primer segmento TCP de la respuesta.
- El Frame 10 transporta el siguiente segmento TCP —otros ~241 bytes de la misma página HTML— con la bandera PSH activada, indicando “entregar estos datos a la aplicación ahora”.
- Están relacionados porque son simplemente dos partes secuenciales de la misma PDU de respuesta HTTP en la misma conexión TCP: el frame 9 envía los bytes 1–1450 de la página, el frame 10 continúa inmediatamente después y envía los bytes 1451–1691.

g) What happens in packet 11?

- Es un ACK TCP (cliente→servidor) que confirma la recepción final de la página HTML.

h) After the initial set of packets is received, the client sends out a new request in packet 12. This occurs automatically without any action by the user. Why does this occur? See the first “hint” to the left.

- Ocurre porque el navegador, al procesar el HTML recibido, lanza automáticamente una petición para el favicon (GET /favicon.ico en el paquete 12) sin que el usuario haga nada. Es parte del comportamiento estándar de los navegadores para cargar recursos embebidos.

i) What is occurring in packets 13 through 22?

- Son segmentos TCP de datos y ACKs recíprocos que transportan partes del payload y van confirmándose para garantizar la entrega fiable.

j) Explain what happens in packets 23 through 26. See the second “hint” to the left.

- 23 – GET /favicon.ico
- 24 – HTTP/1.1 200 OK (cabecera)
- 25 – segmento(s) con los bytes del icono
- 26 – ACK final de cliente confirmando la recepción

k) In one sentence describe what the user was doing (Reading email? Accessing a web page? FTP? Other?).

- El usuario accedía a la página principal de Google, descargando el HTML y luego dos elementos embebidos: el logo y el favicon.

II) Exercise Two

a) In the first few packets, the client machine is looking up the common name (cname) of a web site to find its IP address. What is the cname of this web site? Give two IP addresses for this web site.

- www.yahoo.com
- IP: 216.109.117.106 - 216.109.117.107

b) How many packets/frames does it take to receive the web page (the answer to the first http get request only)?

- Del 7 al 22 se tarda

c) Does this web site use gzip to compress its data for sending? Does it write cookies? In order to answer these questions, look under the payload for the reassembled packet that represents the web page. This will be the last packet from question b above. Look to see if it has “Content-Encoding” set to gzip, and to see if it has a “Set-Cookie” to write a cookie.

- Utiliza ambas, puede verse en el GET que hace el cliente

d) What is happening in packets 26 and 27? Does every component of a web page have to come from the same server? See the Hint to the left.

- No necesariamente deben estar en el mismo servidor.
- Recibimos una imagen de js2.yimg.com

e) In packet 37 we see another DNS query, this time for us.i1.yimg.com. Why does the client need to ask for this IP address? Didn’t we just get this address in packet 26? (This is a trick question; carefully compare the two common names in packet 26 and 37.)

- Aunque ambos nombres de dominio contienen "yimg", son servidores diferentes. La página web que se está cargando también tiene recursos de us.i1.yimg.com, por lo que el cliente necesita la dirección IP para poder descargarlos.

f) In packet 42 we see a HTTP “Get” statement, and in packet 48 a new HTTP “Get” statement. Why didn’t the system need another DNS request before the second get statement? Click on packet 42 and look in the middle window. Expand the line titled “Hypertext Transfer Protocol” and read the “Host:” line. Compare that line to the “Host:” line for packet 48.

- Host línea 42: us.i1.yimg.com
- Host línea 48: us.i1.yimg.com
- No la necesita porque tienen el mismo host

g) Examine packet 139. It is one segment of a PDU (Packet Data Unit) that is reassembled with several other segments in packet 160. Look at packets 141, 142, and 143. Are these three packets also part of packet 160? What happens if a set of packets that are supposed to be reassembled do not arrive in a continuous stream or do not arrive in the proper order?

- Los paquetes 141 y 142 no forman parte del paquete 160.
- El paquete 143 es parte del paquete 160.
- Si un conjunto de paquetes que se supone deben ensamblarse no llegan en un flujo continuo o no llegan en el orden correcto, esto no afecta al paquete principal.

h) Return to examine frames 141 and 142. Both of these are graphics (GIF files) from the same source IP address. How does the client know which graphic to match up to each get statement? Hint: Click on each and look in the middle window for the heading line that starts with “Transmission Control Protocol”. What difference do you see in the heading lines for the two files? Return to the original “Get” statements. Can you see the same difference in the “Get” statements?

- Ambos archivos en los marcos 141 y 142 son similares y provienen de la misma dirección IP de origen. El cliente conoce el gráfico que debe coincidir con cada declaración de obtención de su "Índice de flujo". Cada uno de ellos tiene un "Índice de transmisión" diferente.

III) Exercise Three

Row	www.yahoo.com frames	my.usf.com frames	Brief Explanation of Activity
i)	1 - 2	8 - 9	DNS Request to find IP address for common name & DNS Response
ii)	3 - 5	10 - 12	Three-way handshake
iii)	– –	13 - 20	
iv)	6	21	“Get” request for web page
v)	7	22	First packet from web server with web page content.

a) Compare the destination port in the TCP packet in frame 3 with the destination port in the TCP packet in frame 12. What difference do you see? What does this tell you about the difference in the two requests?

El puerto de destino en el paquete TCP del marco 3 es **80**, mientras que el puerto de destino en el paquete TCP del marco 12 es **443**. Esta diferencia de puertos indica que las dos solicitudes están utilizando diferentes protocolos.

- **El puerto 80** es el puerto estándar para el tráfico **HTTP**, que se utiliza para la comunicación no cifrada entre un navegador web y un servidor web.
- **El puerto 443** es el puerto estándar para el tráfico **HTTPS**, que se utiliza para la comunicación cifrada entre un navegador web y un servidor web.

Esto sugiere que la solicitud en el marco 3 es para un recurso **HTTP**, mientras que la solicitud en el marco 12 es para un recurso **HTTPS**.

b) Explain what is happening in row “iii” above. Why are there no frames listed for yahoo in row “iii"?

La fila "iii" de la tabla está etiquetada como "Apretón de manos de tres vías" y muestra que no hay marcos enumerados para `www.yahoo.com`. Esto significa que no hay evidencia de que se haya capturado un apretón de manos de tres vías (SYN, SYN-ACK, ACK) para la solicitud de Yahoo.

Hay algunas posibles explicaciones para esto:

- **Captura incompleta:** La captura de Wireshark puede no haber capturado el apretón de manos inicial para la solicitud de Yahoo.
- **Entrada DNS en caché:** El cliente puede haber tenido la dirección IP de Yahoo en caché, por lo que no necesitó realizar una búsqueda de DNS (marcos 1-2) o un apretón de manos (marcos 3-5) nuevamente.

c) Look at the “Info” column on frame 6. It says: “GET / HTTP / 1.1. What is the corresponding Info field for the my.usf.com web request (frame 21)? Why doesn’t it read the same as in frame 6?

La columna "Info" en el marco 21 (my.usf.com) no es visible en la imagen proporcionada. Sin embargo, podemos suponer que también comenzará con "GET". También puede contener la ruta específica solicitada dentro del sitio web (por ejemplo, "/about/").

La razón de la diferencia es que el campo "Info" generalmente muestra el método HTTP (GET, POST, etc.) seguido de la ruta solicitada en el servidor. Si bien ambas solicitudes comienzan con "GET", podrían estar buscando diferentes recursos de los servidores respectivos (Yahoo vs. my.usf.edu).