CHALLENGE 2

Open challenge101-2.pcapng and use your display filter and coloring rule skills to locate traffic based on addresses, protocols and keywords to answer these Challenge questions.

First, configure Wireshark to capture only traffic to and from your MAC address and TCP port 80, and save the traffic to a file named mybrowse.pcapng. Then ping and browse to www.chapellu.com. Stop the capture and examine the trace file contents.

Question 2-1.
Did you capture any ICMP traffic?
No se capturó tráfico ICMP.

Question 2-2.
What protocols are listed for your browsing session to www.chapellu.com?
Debemos de capturado su tráfico hacia o desde el puerto 80. La columna Protocolo solo mostrará el tráfico TCP y HTTP.

Question 2-3.
How many ICMP packets did you capture?

La cantidad de paquetes ICMP que capturó depende de la cantidad de tráfico ICMP generado por su aplicación de ping y de cualquier tráfico ICMP de fondo generado durante su proceso de captura.

Question 2-4.
What ICMP Type and Code numbers are listed in your trace file?
Debería ver Tipo 8 / Código 0 (solicitud de eco) y Tipo 0 / Código 0 (respuesta de eco).