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

Question 2-2.
What protocols are listed for your browsing session to www.chapellu.com?
HTTP, ARP, TCP, DNS, IGMv3, LLMNR,MDNS, UDP.

Now configure Wireshark to capture all your ICMP traffic, and save your traffic to a file called myicmp.pcapng. Again, ping and browse www.chapellu.com. Stop the capture and examine the trace file contents.

Question 2-3.
How many ICMP packets did you capture?
36

Question 2-4.
What ICMP Type and Code numbers are listed in your trace file?
Code 0, Requet and Reply