Sample Lab Report

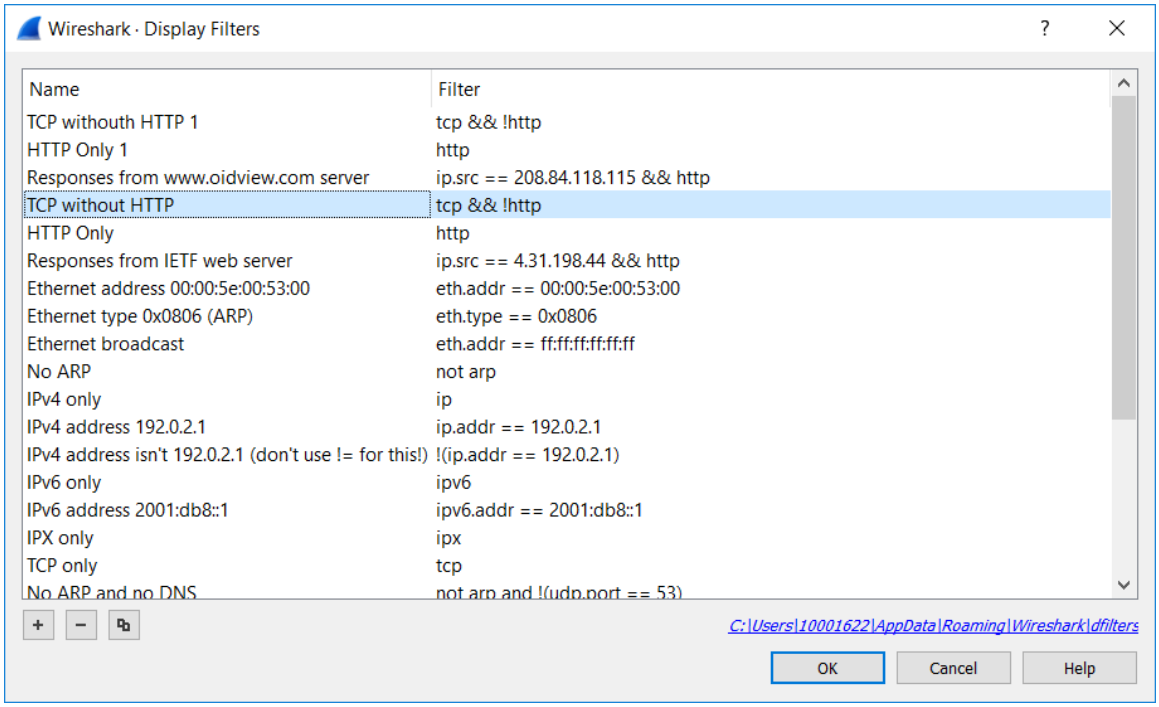
Lab Exercise 4: Filtering Packets

(The answers to all questions are screen shots similar to the ones shown below.)

Question 1, part A.

Create a new *display* filter called “TCP without HTTP” that only displays TCP traffic which does NOT contain HTTP…

Confirm the value of the regular expression in the filter string – any logical equivalent is OK, parenthesis not required. Wireshark allows “and” as a substitute for “&&”, and ‘not” as a substitute for “!”.

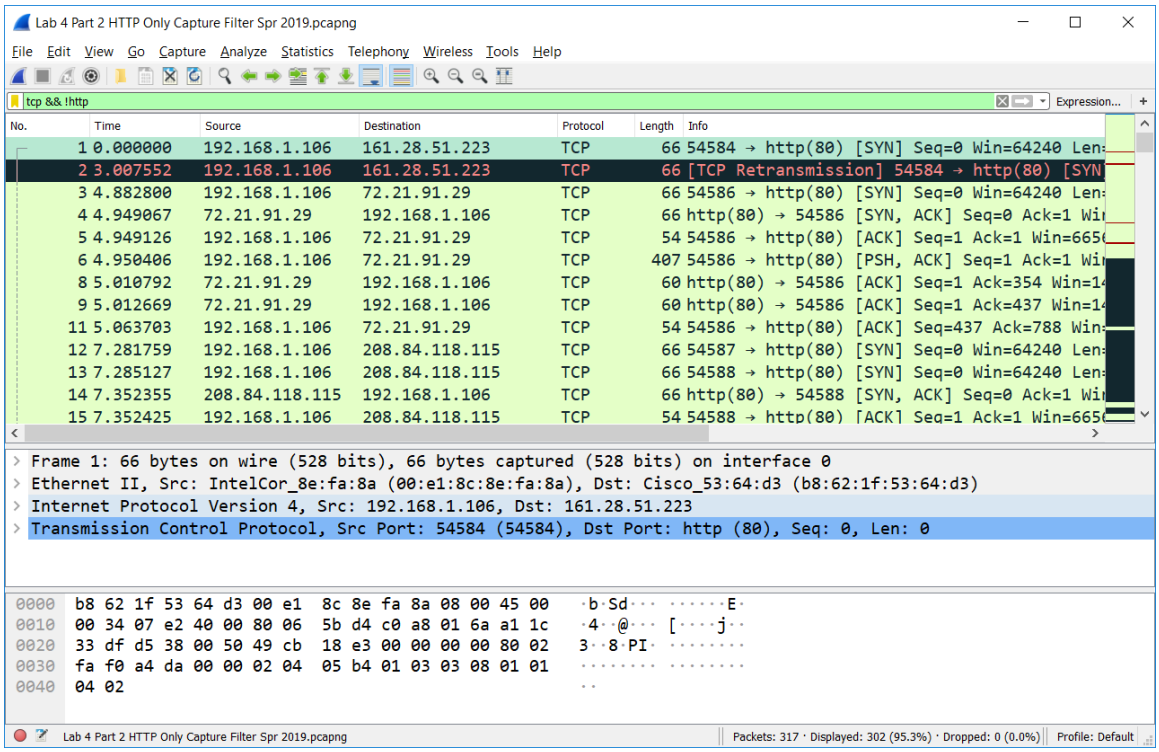


(Wireshark v3.0)

(CONTINUED ON NEXT PAGE)

Question 1, part B.

Verify the Protocol field is "TCP" in all cases.



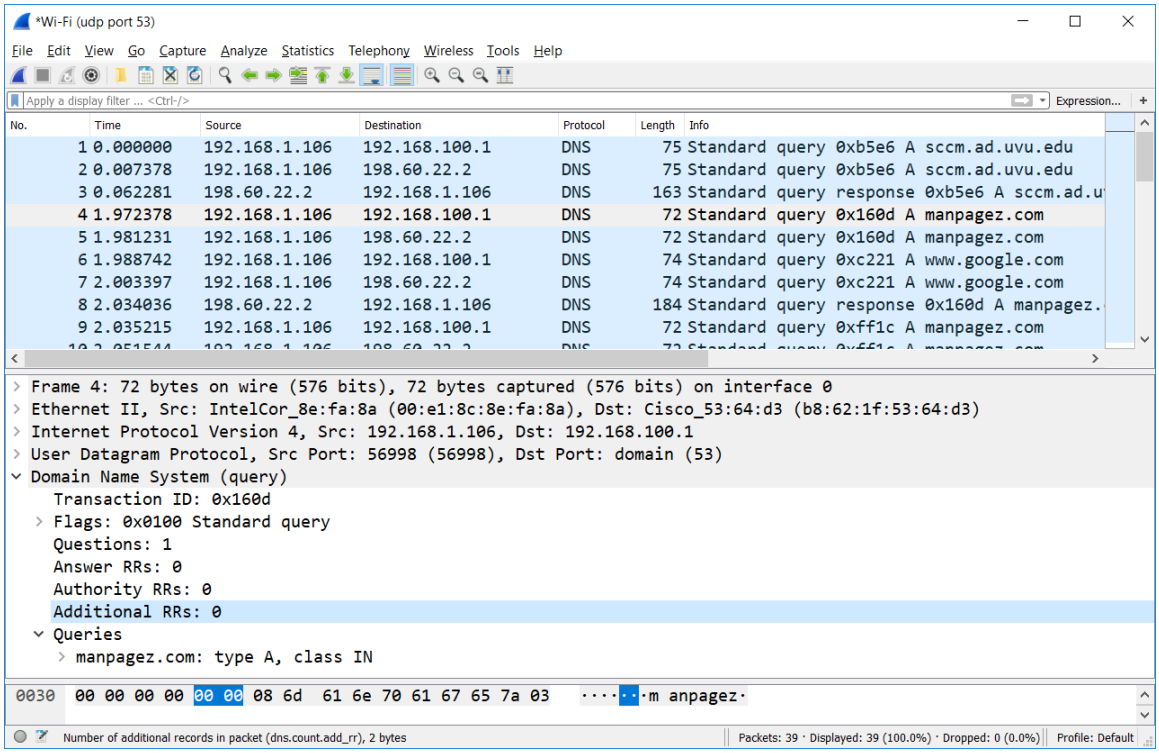
(Wireshark v3.0)

(CONTINUED ON NEXT PAGE)

Question 2.

Using the techniques explained in the **Capture Filters** section above, create a *capture* filter that will collect only DNS messages…

Verify that a domain name is visible in the Packet Details pane, as highlighted below. A display filter similar to `dns.qry.name == manpagez.com` *may be needed in some cases.*



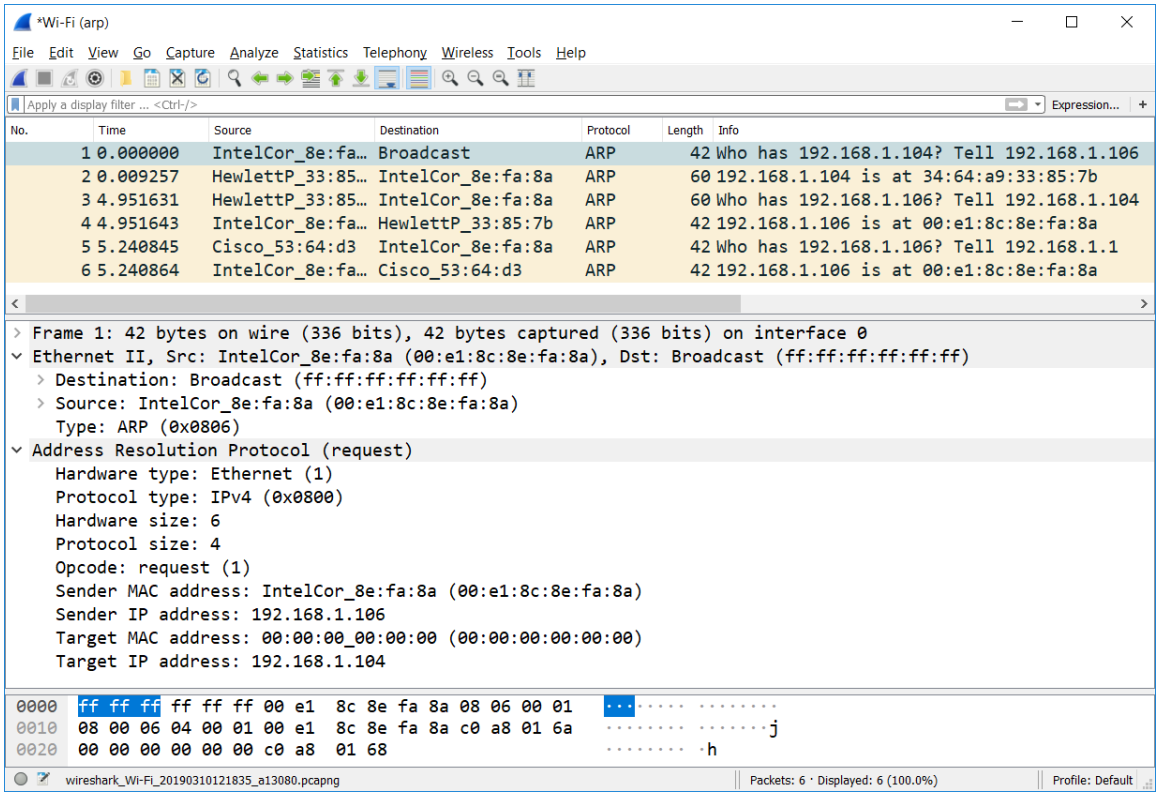
(Wireshark v3.0)

(CONTINUED ON NEXT PAGE)

Question 3.

Build an ARP capture filter and save it…

Verify that an ARP request is visible in Packet Details pane, as shown below.



(Wireshark 3.0)

Lab Test Log

3/25/17 Used Wireshark v2.2.5 on Windows 7

10/28/18 Used Wireshark v2.6.4 on Windows 10

3/9/19 Used Wireshark v3.0.0 on Windows 10

10/26/19 Used Wireshark v3.0.5 on Windows 10