

Sample Lab Report

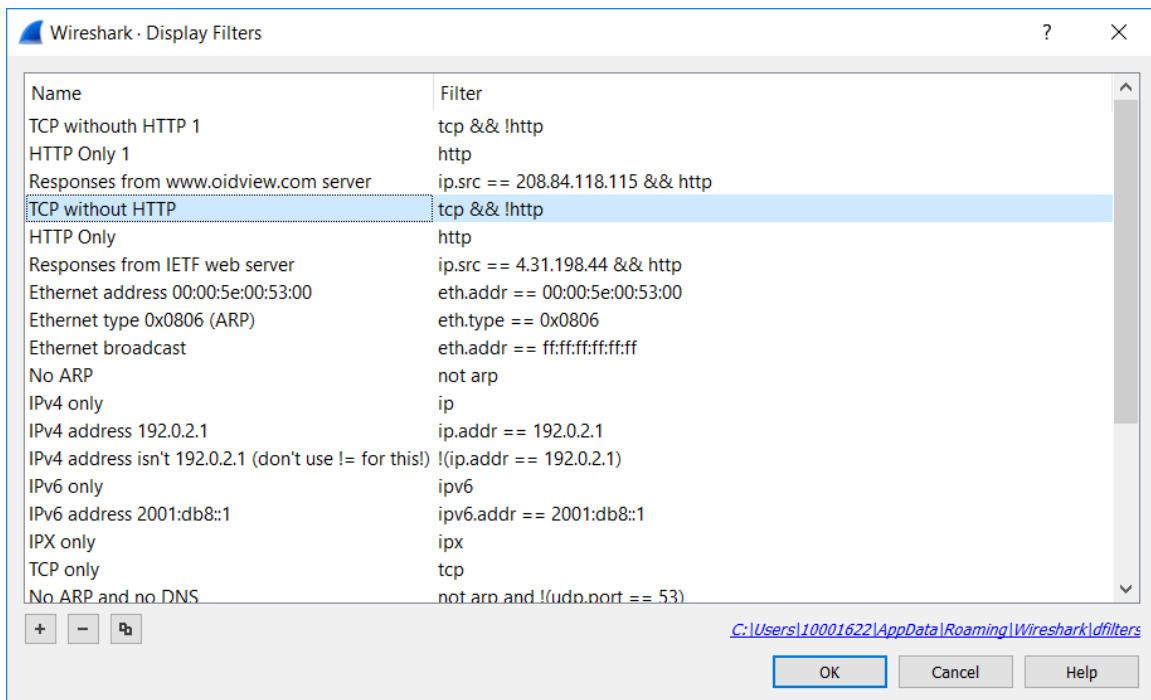
Lab Exercise 4: Filtering Packets

(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.

Lab 4 Part 2 HTTP Only Capture Filter Spr 2019.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp && !http

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.106	161.28.51.223	TCP	66	54584 → http(80) [SYN] Seq=0 Win=64240 Len=0
2	3.007552	192.168.1.106	161.28.51.223	TCP	66	[TCP Retransmission] 54584 → http(80) [SYN] Seq=0 Win=64240 Len=0
3	4.882800	192.168.1.106	72.21.91.29	TCP	66	54586 → http(80) [SYN] Seq=0 Win=64240 Len=0
4	4.949067	72.21.91.29	192.168.1.106	TCP	66	http(80) → 54586 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
5	4.949126	192.168.1.106	72.21.91.29	TCP	54	54586 → http(80) [ACK] Seq=1 Ack=1 Win=6656 Len=0
6	4.950406	192.168.1.106	72.21.91.29	TCP	407	54586 → http(80) [PSH, ACK] Seq=1 Ack=1 Win=6656 Len=407
8	5.010792	72.21.91.29	192.168.1.106	TCP	60	http(80) → 54586 [ACK] Seq=1 Ack=354 Win=1460 Len=0
9	5.012669	72.21.91.29	192.168.1.106	TCP	60	http(80) → 54586 [ACK] Seq=1 Ack=437 Win=1460 Len=0
11	5.063703	192.168.1.106	72.21.91.29	TCP	54	54586 → http(80) [ACK] Seq=437 Ack=788 Win=6656 Len=0
12	7.281759	192.168.1.106	208.84.118.115	TCP	66	54587 → http(80) [SYN] Seq=0 Win=64240 Len=0
13	7.285127	192.168.1.106	208.84.118.115	TCP	66	54588 → http(80) [SYN] Seq=0 Win=64240 Len=0
14	7.352355	208.84.118.115	192.168.1.106	TCP	66	http(80) → 54588 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
15	7.352425	192.168.1.106	208.84.118.115	TCP	54	54588 → http(80) [ACK] Seq=1 Ack=1 Win=6656 Len=0

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: IntelCor_8e:fa:8a (00:e1:8c:8e:fa:8a), Dst: Cisco_53:64:d3 (b8:62:1f:53:64:d3)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 161.28.51.223
> Transmission Control Protocol, Src Port: 54584 (54584), Dst Port: http (80), Seq: 0, Len: 0

0000 b8 62 1f 53 64 d3 00 e1 8c 8e fa 8a 08 00 45 00 .b.Sd... ..E.
0010 00 34 07 e2 40 00 80 06 5b d4 c0 a8 01 6a a1 1c .4.@... [...j..
0020 33 df d5 38 00 50 49 cb 18 e3 00 00 00 00 80 02 3...8.PI.....
0030 fa f0 a4 da 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02 ..

Lab 4 Part 2 HTTP Only Capture Filter Spr 2019.pcapng

Packets: 317 · Displayed: 302 (95.3%) · Dropped: 0 (0.0%) Profile: Default

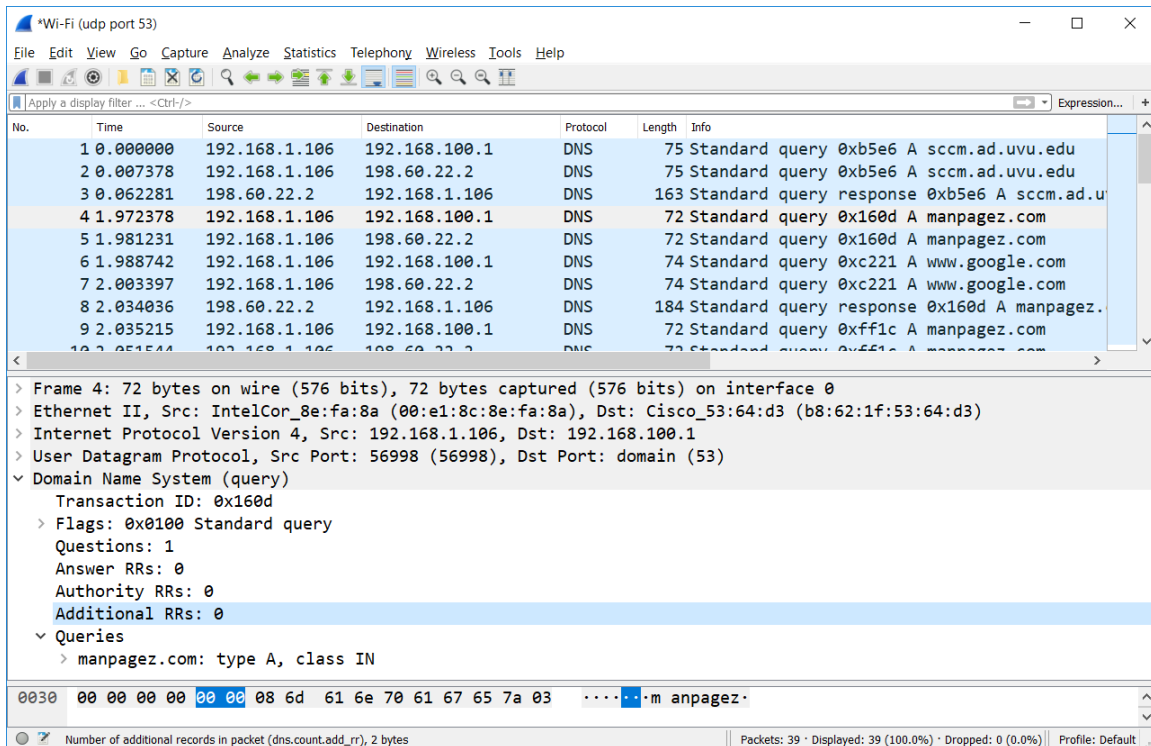
(Wireshark v3.0)

(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.

The image shows the Wireshark 3.0 interface with a packet capture filter applied. The packet list pane shows six packets, all of which are ARP requests. The first packet is selected, and the packet details pane shows the following information:

- Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: IntelCor_8e:fa:8a (00:e1:8c:8e:fa:8a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Source: IntelCor_8e:fa:8a (00:e1:8c:8e:fa:8a)
 - Type: ARP (0x0806)
- Address Resolution Protocol (request)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: request (1)
 - Sender MAC address: IntelCor_8e:fa:8a (00:e1:8c:8e:fa:8a)
 - Sender IP address: 192.168.1.106
 - Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 - Target IP address: 192.168.1.104

The packet bytes pane shows the raw data of the selected packet, which is an ARP request. The first three bytes are ff ff ff, indicating a broadcast destination. The packet is 42 bytes long.

(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