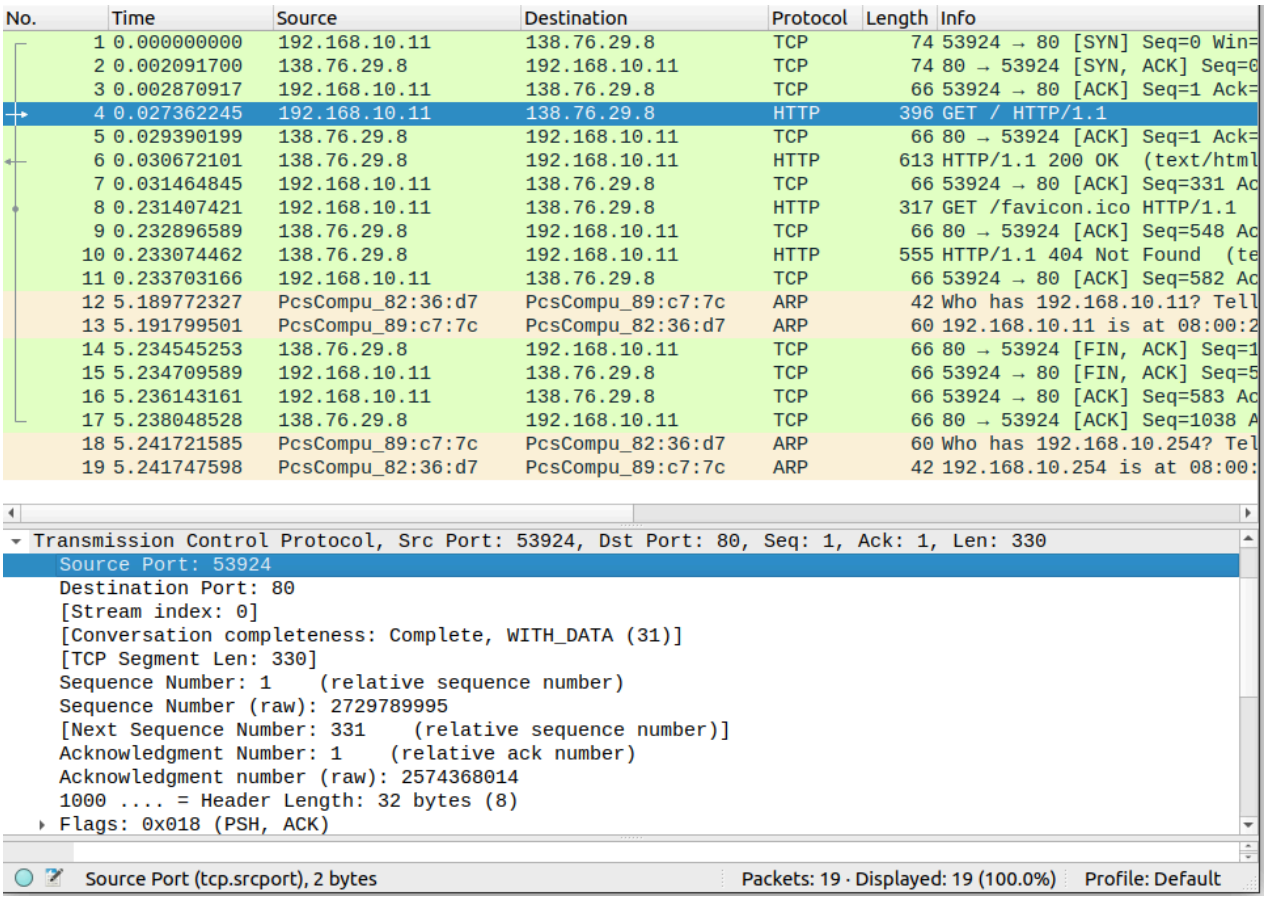
hw8

1. a) I will assume that the host has received its IP address and knows the IP address of the router since this process is usually done before ARP and the table is already filled
    1. Host looks at ARP table to get the MAC address for the first router (router 2) based on the IP address (MAC is 77-77-77-77-77-77 and dest IP is 182.162.3.1). The host then creates and sends an ethernet frame for the aformentioned MAC address
    2. The router (2) gets the frame. It unwraps it to get the datagram and determines the next step to be Router 1 (182.168.2.1). It checks the ARP table and determines this is MAC 33-33-33-33-33-33. It then creates the ethernet frame and sends it there accordingly
    3. Router 1 then gets the frame and follows a similar process. From the datagram it gets the next destination host B with IP 182.168.1.003. From there the ARP table says it is MAC 22-22-22-22-22-22 where the frame is then created and sent.
    4. Host B gets the frame and unwraps it to get the message
    b) Once again, assume DHCP is done and the address of the router is known
    1. The first step is to send an ARP query to FF-FF-FF-FF-FF-FF. This will broadcast that we are looking for where to send the packets to because we do not know where so we need to find the MAC address for Host E to send the packet to. From there, Router 2 will will recieve this packet and send a response to Host B saying to send the packsts to 77-77-77-77-77-77. This response will go to the sender of the query which is 88-88-88-88-88-88.
    2. After that everything is the same
2.

Action	Known MACs	Links sent to	Explanation
A->D	A	B, C, D	Initially the table is empty. When the packet is received, A is added to the ARP table. From there since the destination B is not known, the links are "flooded" or in other words the info is sent to all the links.
D->A	A, D	A	The switch recieves the packet and adds D to the ARP table. From there the packet is forwarded to A since A is already in the ARP table
C->A	A, D, C	A	The switch recieves the packet and adds C to the ARP table. From there the packet is forwarded to A since A is already in the ARP table
A->C	A, D, C	C	The switch recieves the packet. A is in the ARP table so it doesn't change. From there the packet is forwarded to C since C is already in the ARP table

3. Facebook updated their border gateway protocol which withdrew their IP addresses from global routing tables. Since their authoritative DNS was now unreachable, facebook.com was impossible to resolve so you could no longer access the website. This was propogated by a lot of Facebook internal servers being down so it took forever for it to come back.

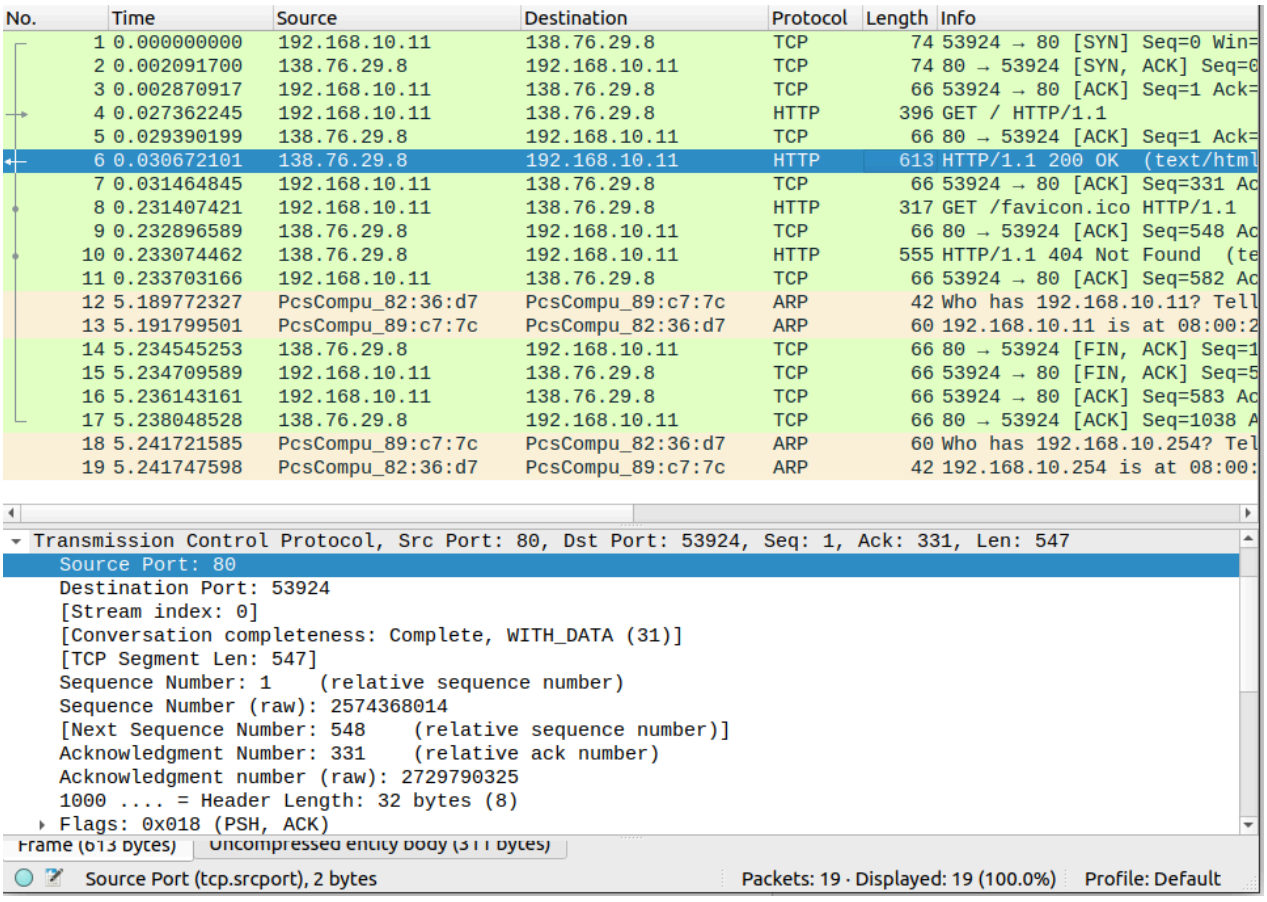
Part 2

1. 

   The source is 192.168.10.11:53924

   The dest is 138.76.29.8:80

2. .030672101

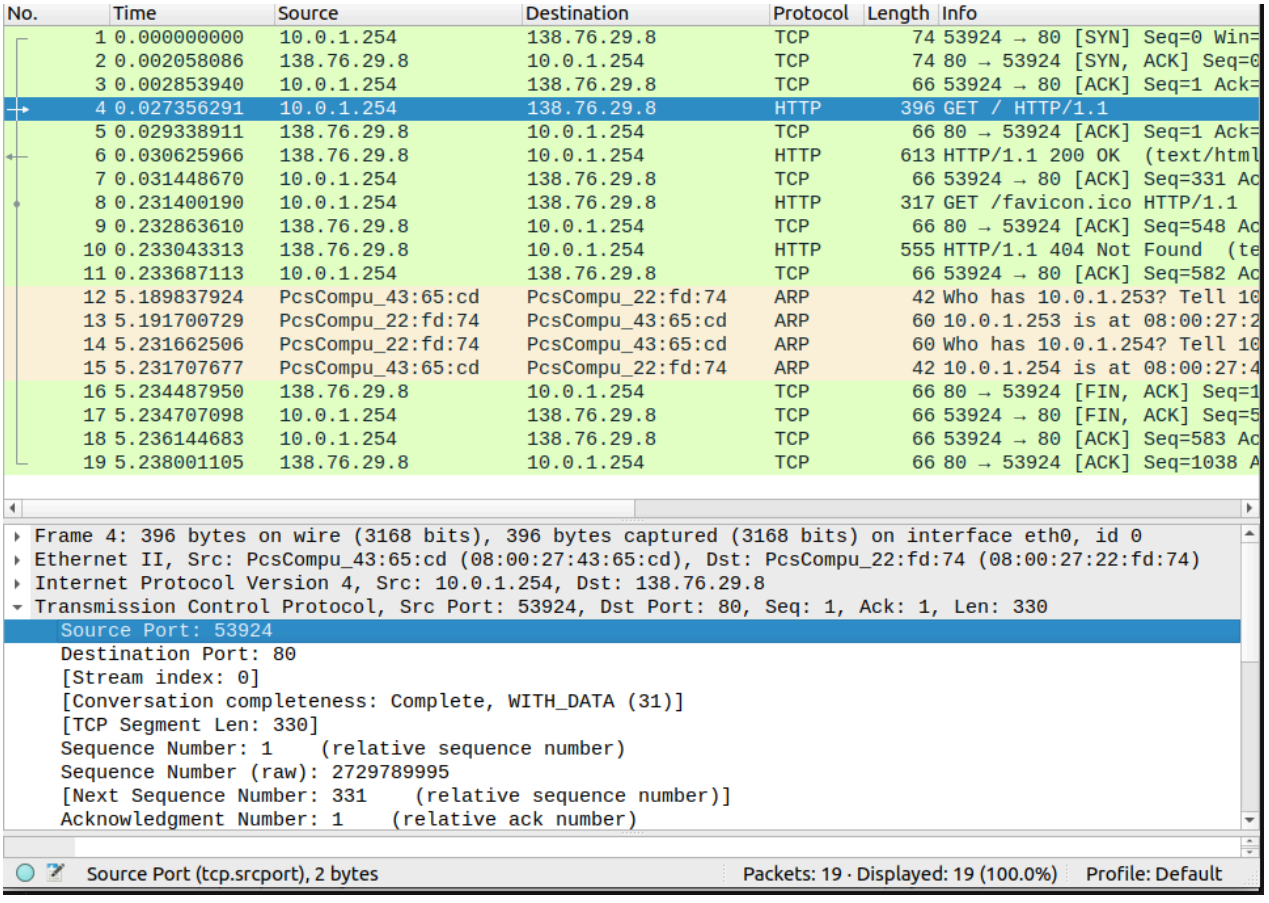


3. Same image as 2

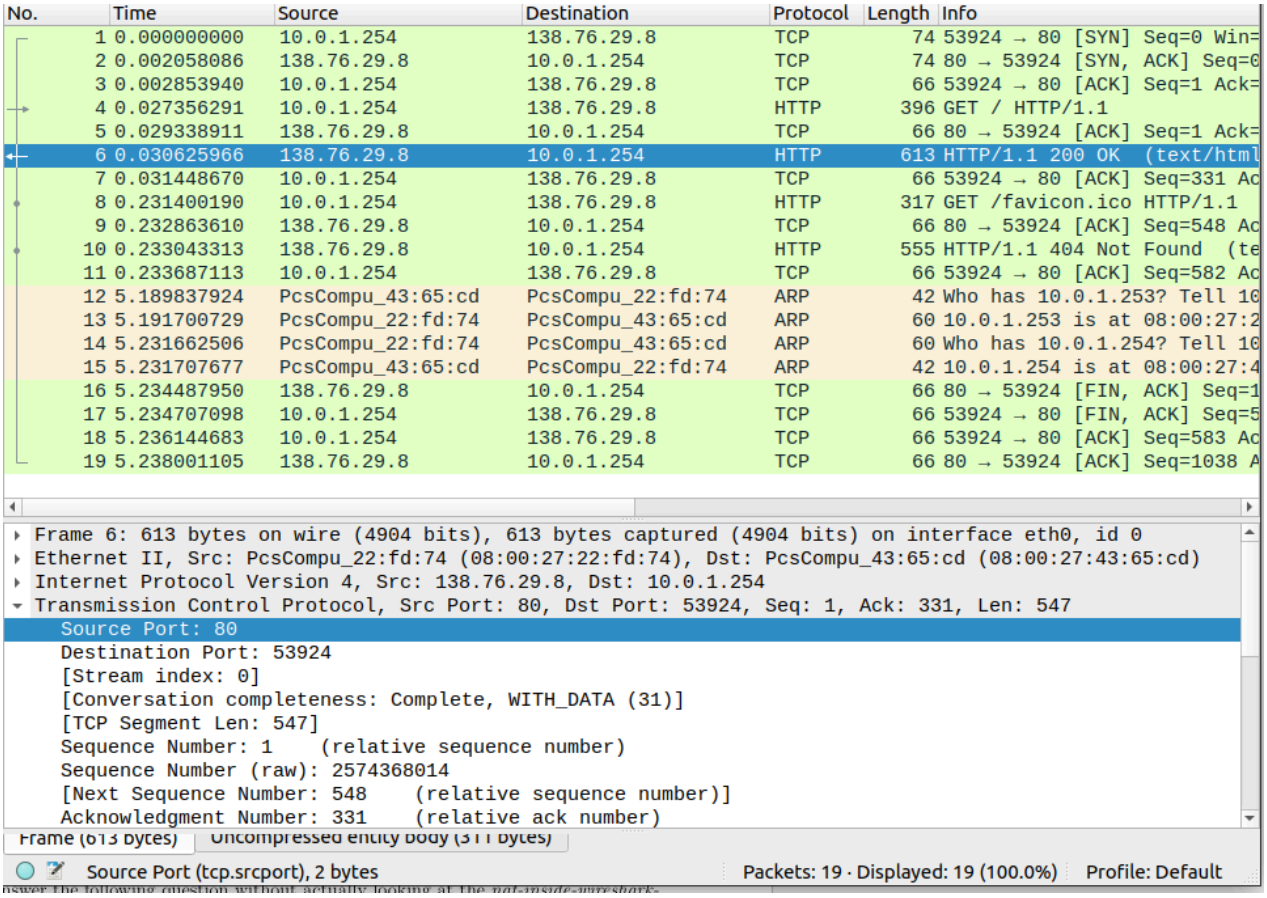
   The source is 138.76.29.8:80

   The dest is 192.168.10.11:53924

4. .027356291



5. Same pic as 4
   The source is 10.0.1.254:53924
   The dest is 138.76.29.8:80
   Interestingly, the source IP is different but the source port is not. The rest are the same
6. .030625966

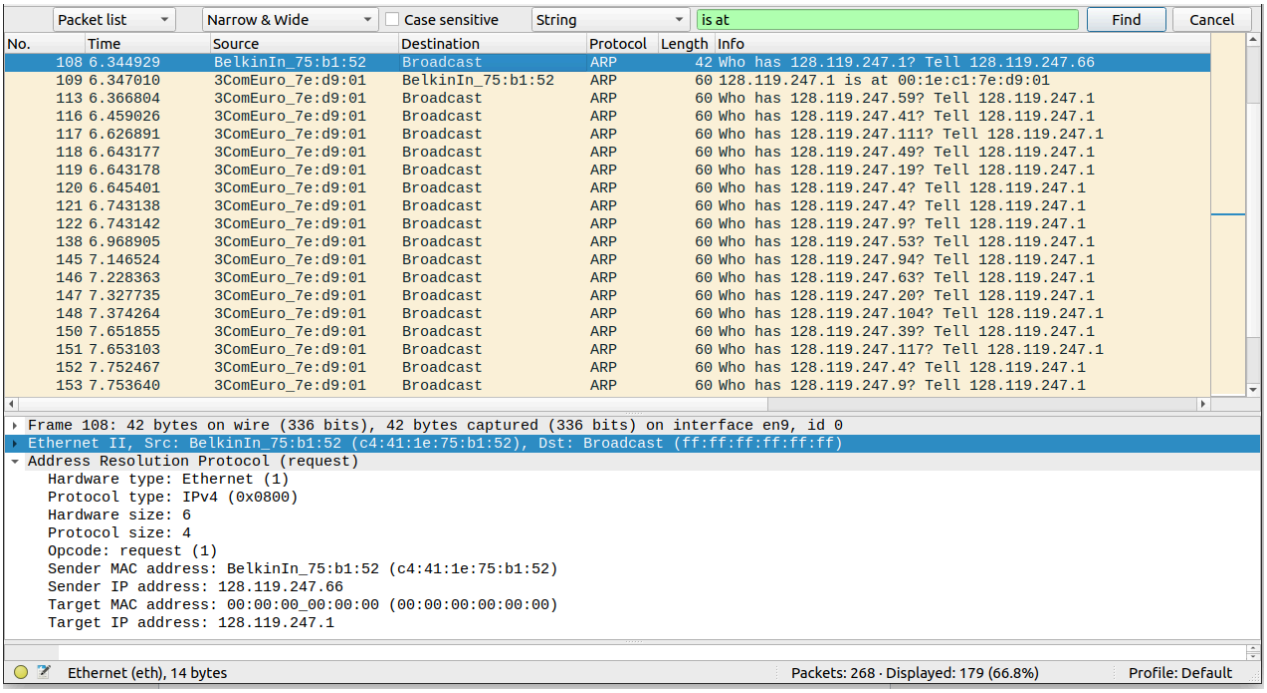


7. Same image as above
   The source is 138.76.29.8:80
   The dest is 10.0.1.254:53924
8. Since the NAT protocol essentially replaces the headers at the router with what they're supposed to be, it will be exactly how the host expects
   The source is 138.76.29.8:80
   The dest is 192.168.10.11:53924

Lab 2

This lab was a bit confusing because there was only one response to any of the ARP messages. I will assume the sender who got a response is the computer

1. c4:41:1e:75:b1:52



2. ff:ff:ff:ff:ff:ff (above picture)
3. 128.119.247.66 (above pic)
4. 128.119.247.1 (above pic)
5. 00:1e:c1:7e:d9:01