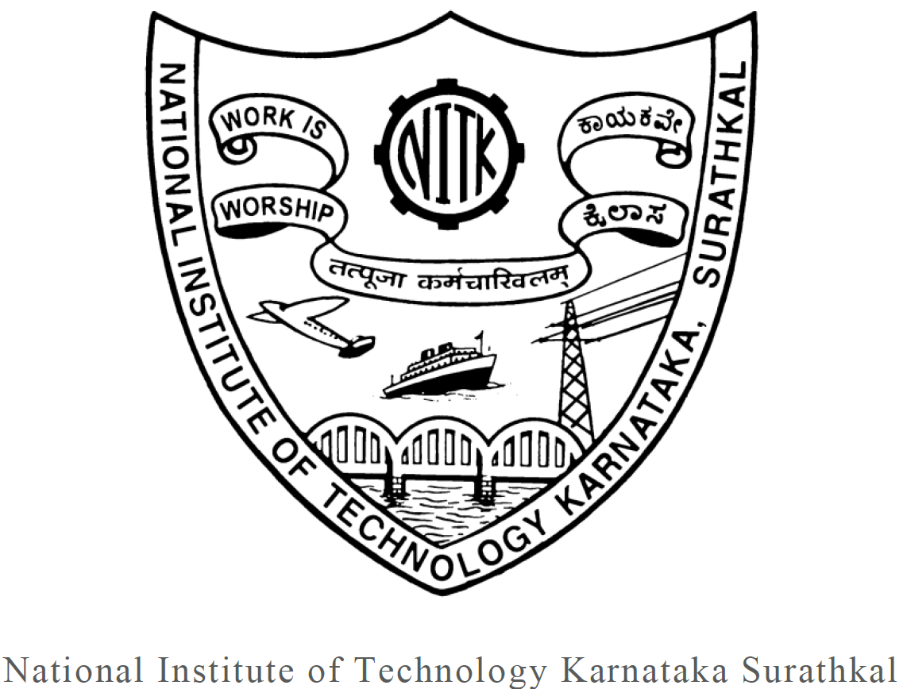
National Institute of Technology Karnataka, Surathkal

Department of Computer Science and Engineering

CS302 - Computer Networks Lab

Wireshark Assignment



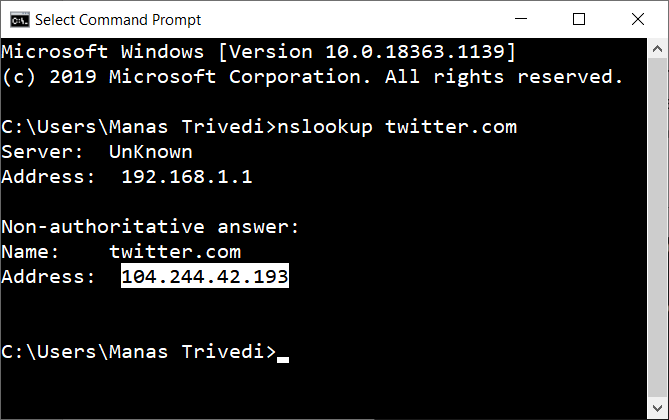
Submitted by:

Name: Manas Trivedi  
Roll no.: 181CO231  
Reg. no.: 181711

Odd Semester 2020-2021

1. Start a Wireshark capture and browse to twitter.com. Use display filtering to reduce the displayed packets to only those sent and received by your computer. How many sites are you actually interacting with when you interact with Twitter? What are they?

Finding the IP address of twitter.com,



IP address of twitter.com: 104.244.42.193

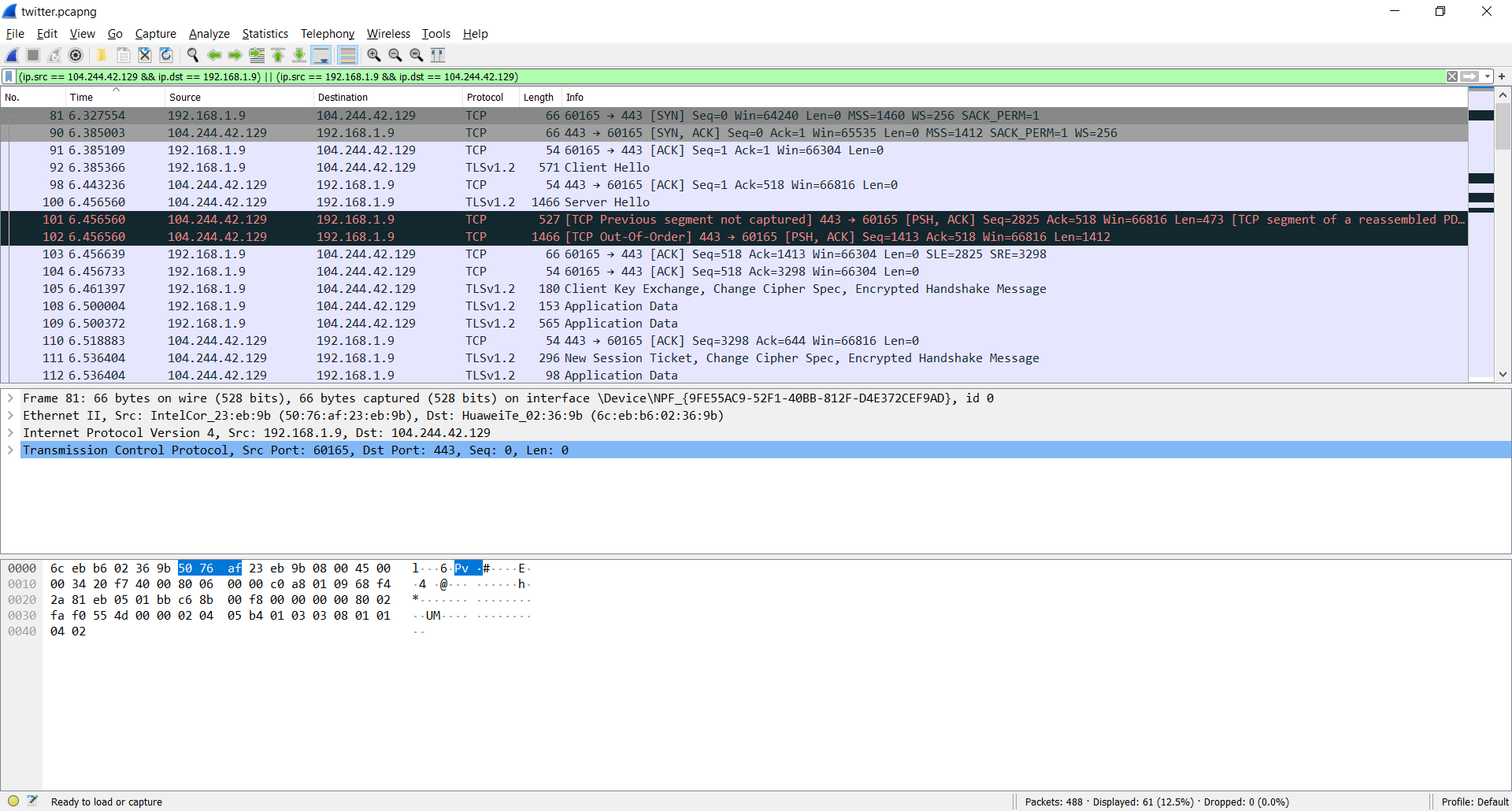
Finding IP address of computer,



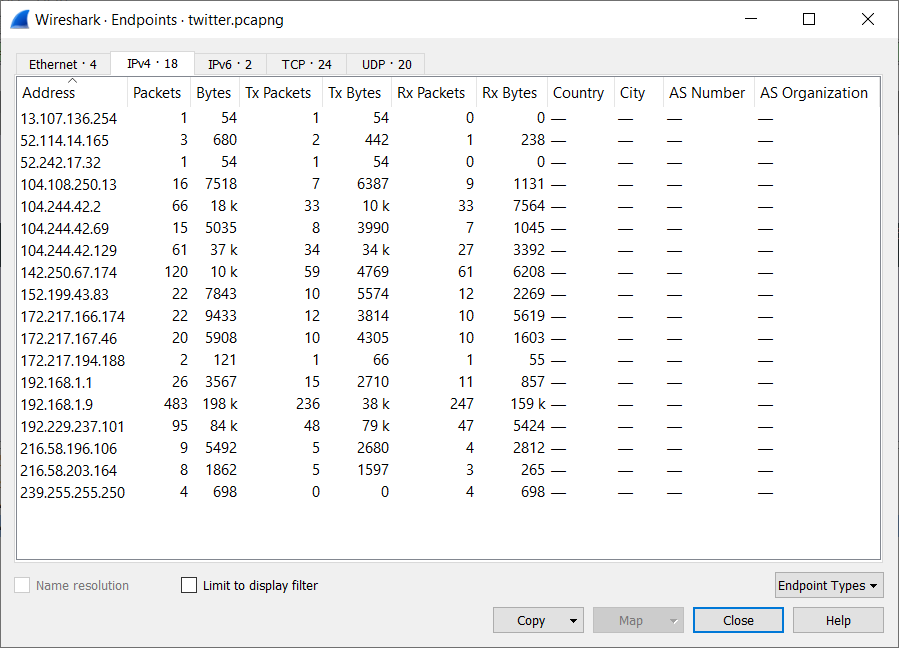
IP address of computer: 192.168.1.9

We need to apply a filter which will display only those packets which have been sent to twitter.com from the computer and vice-versa. The display filter to be applied:

(ip.src == 104.244.42.193 && ip.dst == 192.168.1.9) || (ip.src == 192.168.1.9 && ip.dst == 104.244.42.193)

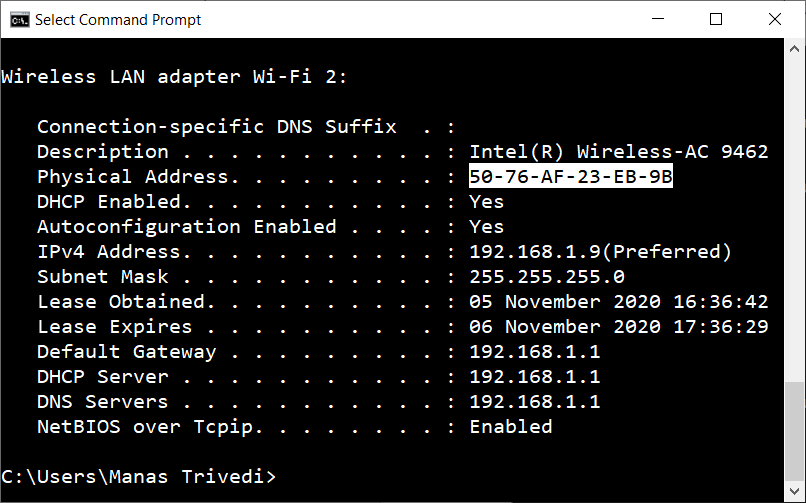


The sites interacted with when browsing to twitter.com:



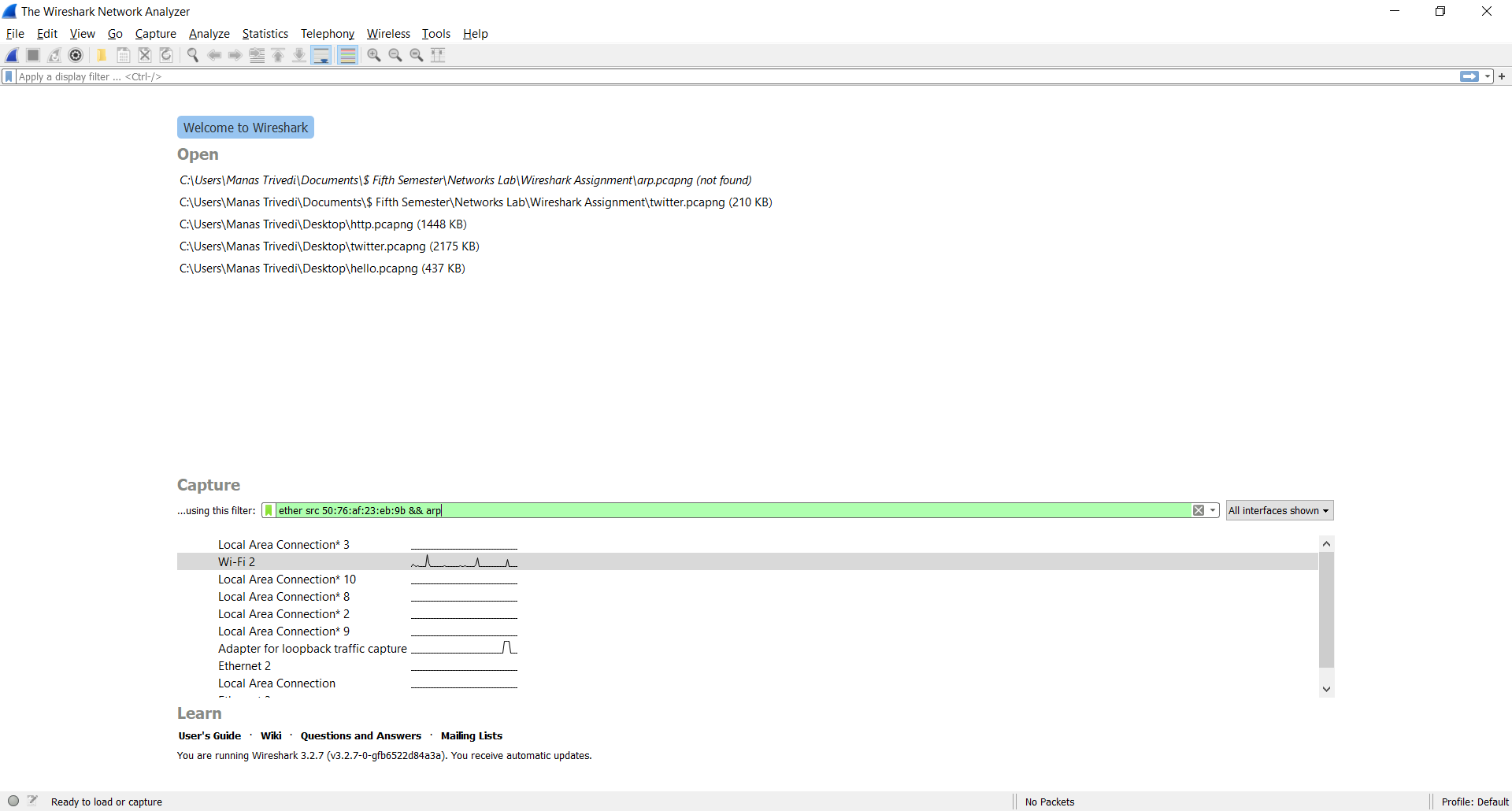
1. Write and test capture filters that capture only your machine’s ARP requests. How often are they sent (i.e., how many ARP packets your machine sends per minute, on average?). This, of course, depends on your OS and network usage pattern.

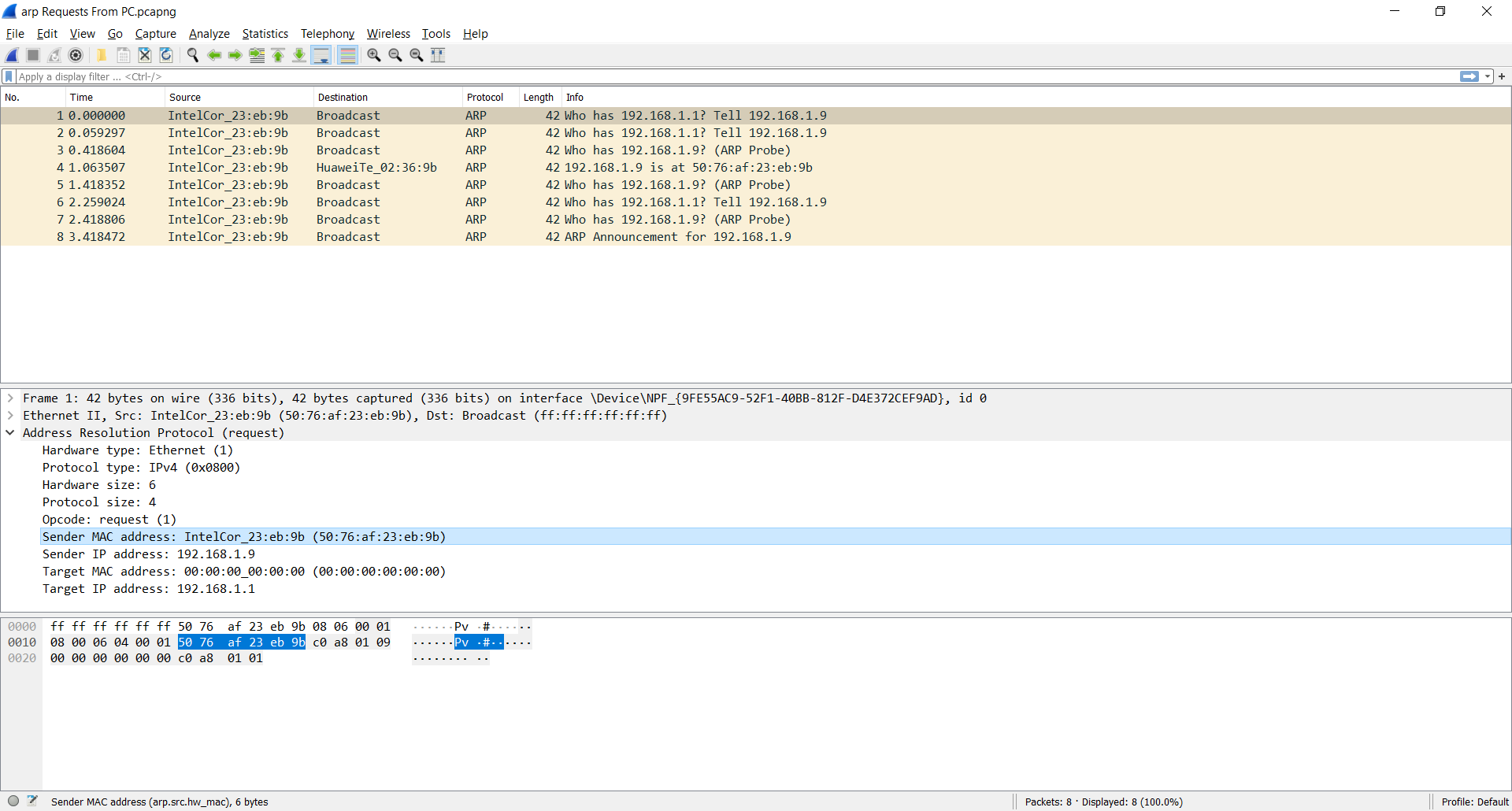
Finding MAC address of wireless LAN adapter Wi-Fi 2,

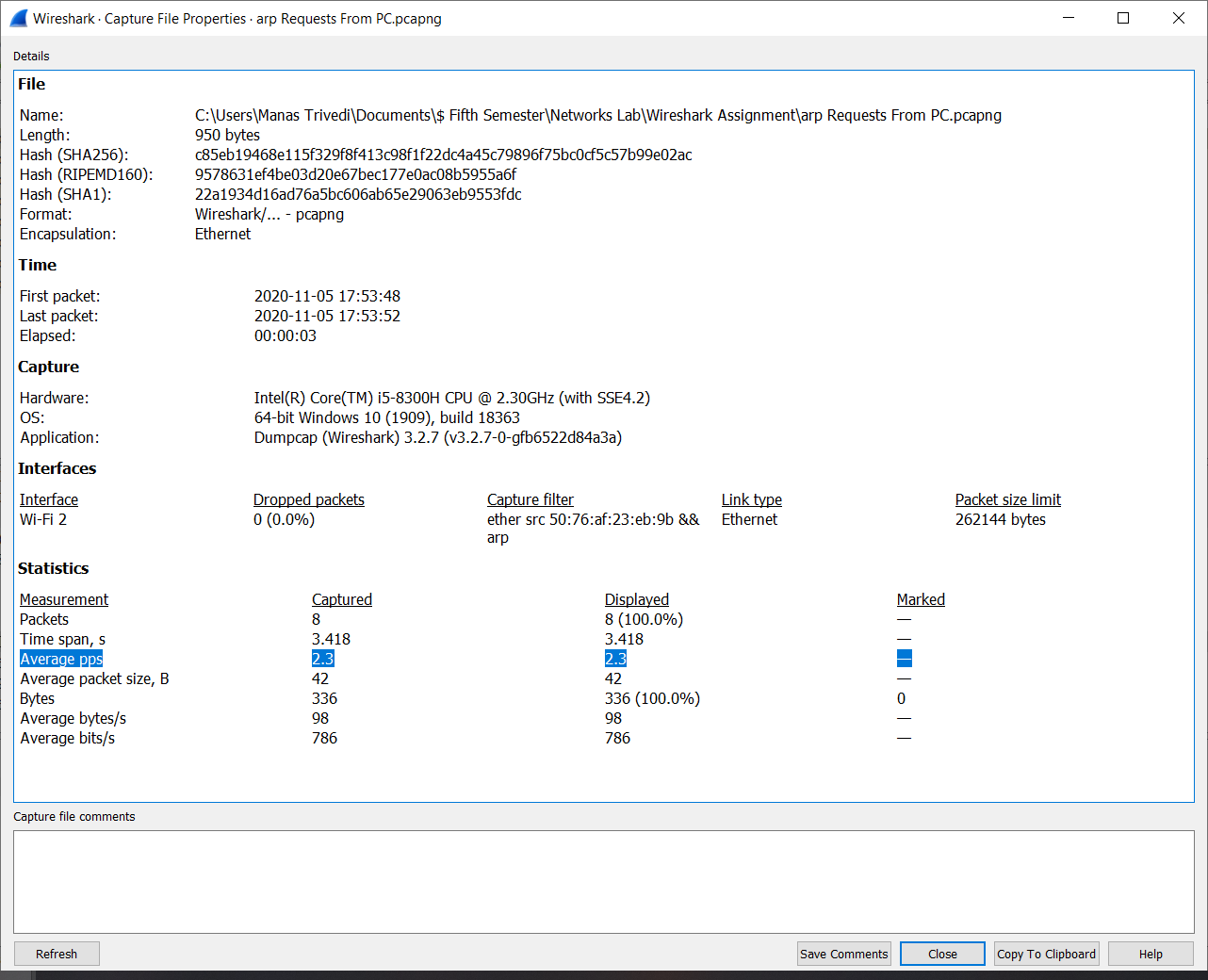


MAC address of wireless LAN adapter Wi-Fi 2: 50:76:af:23:eb:9b

Filter to capture ARP requests sent by computer: ether src 50:76:af:23:eb:9b && arp







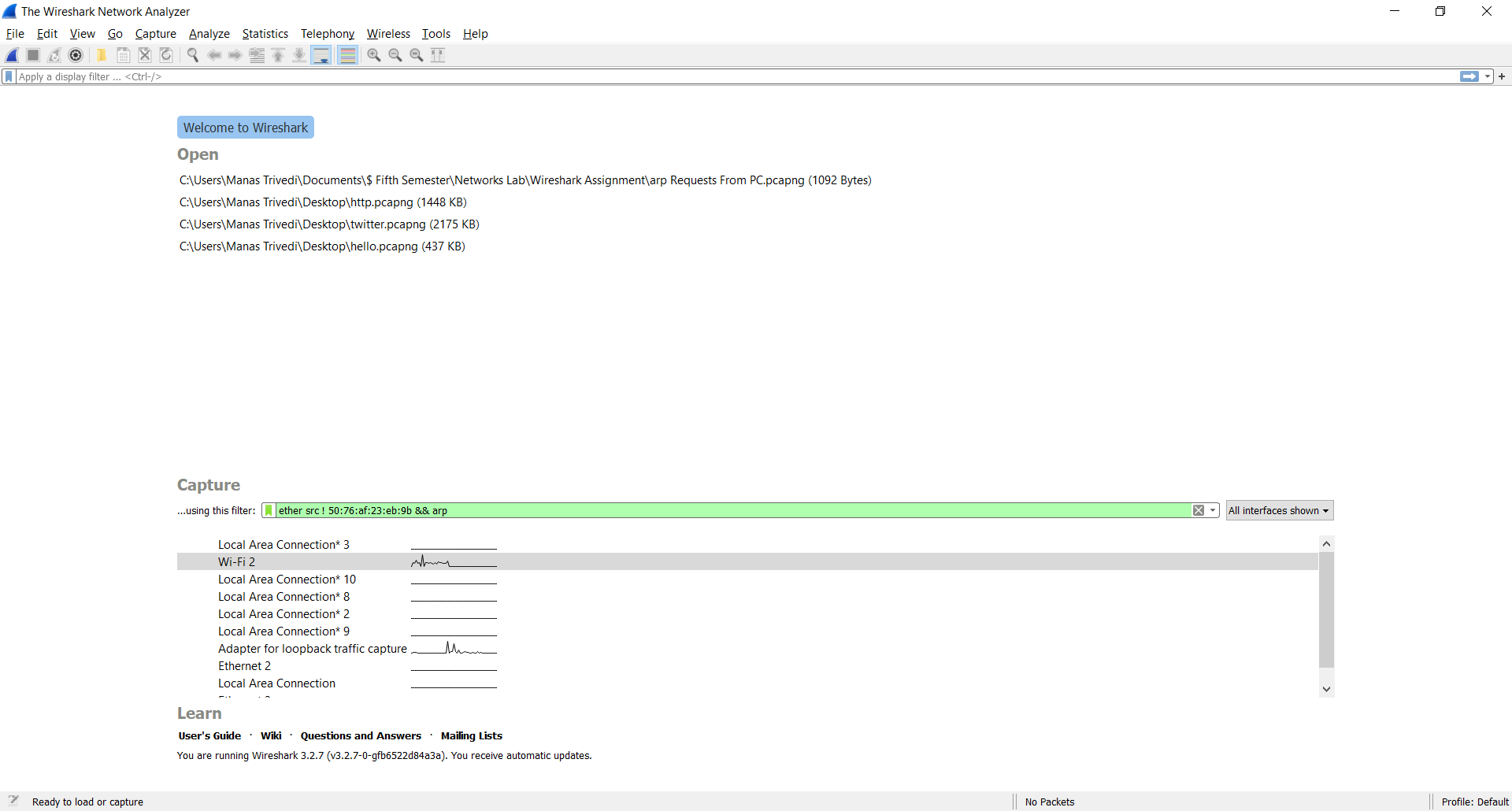
From the above image, ARP packets sent by machine per minute

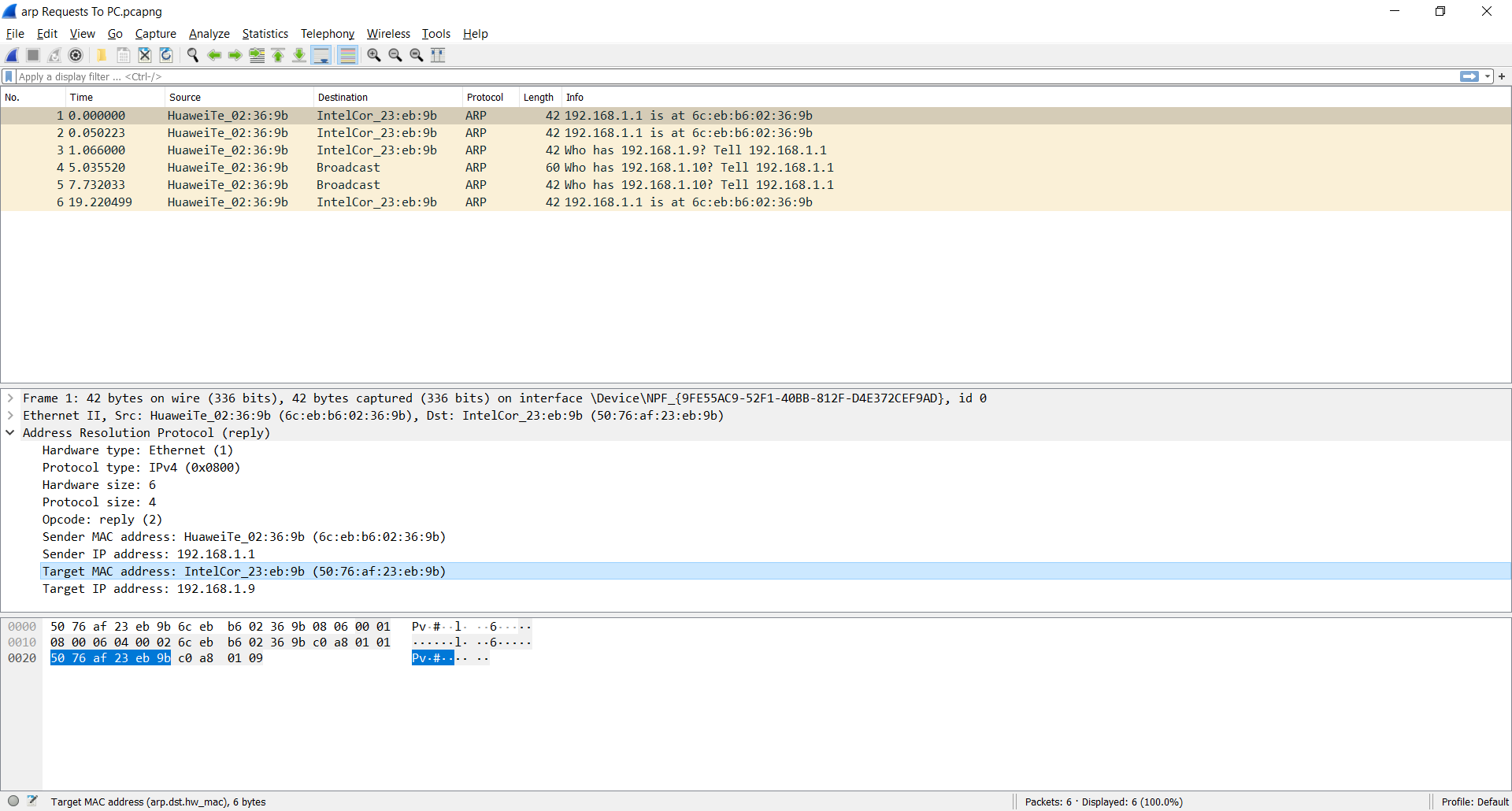
= (2.3 packets per second) \* 60

= 138 packets per minute

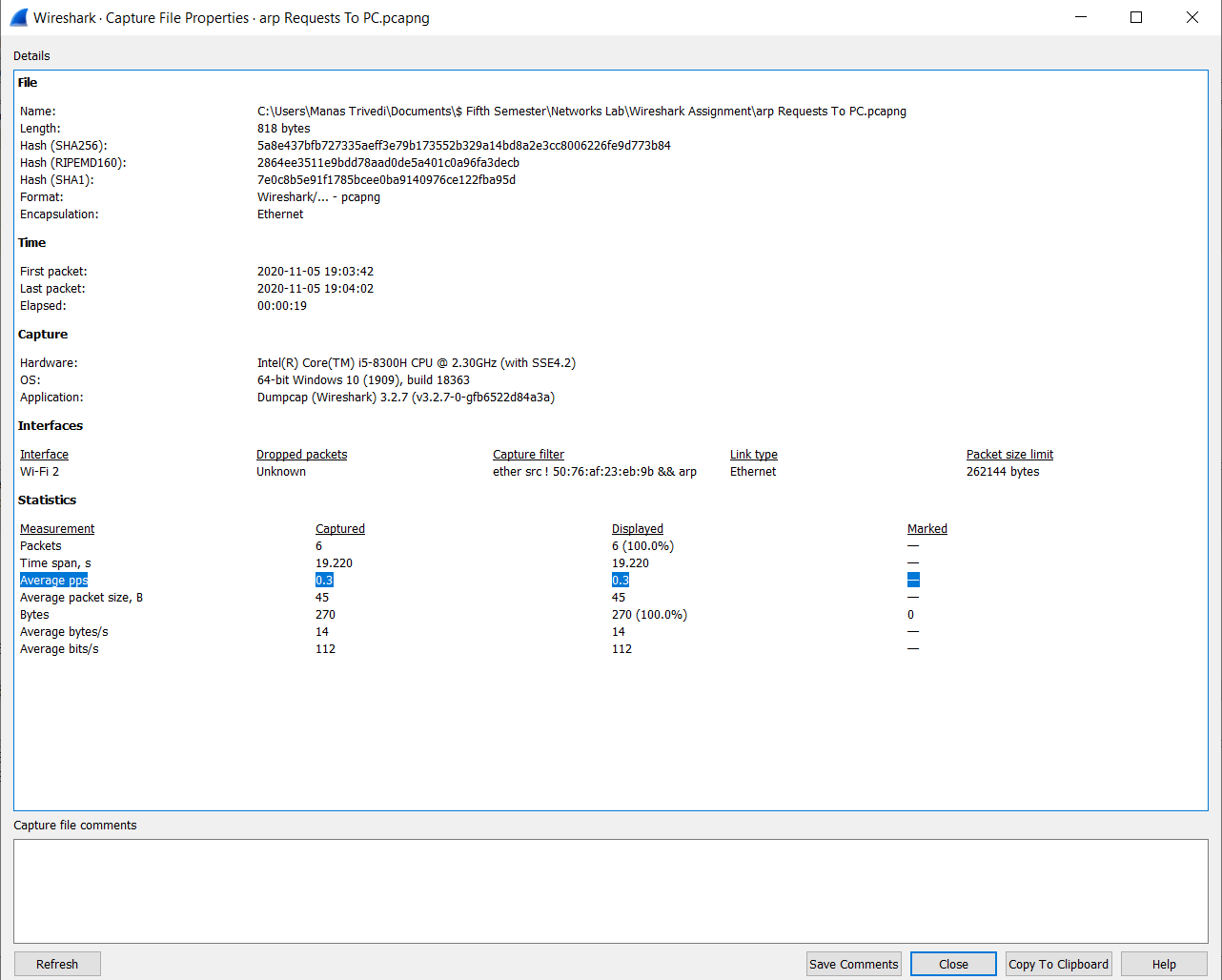
1. Write and test capture filters that capture only ARP requests sent to your computer. Who sends them, and how often?

Filter to capture ARP requests sent to computer: ether src ! 50:76:af:23:eb:9b && arp





The ARP requests received by the computer are sent by the modem, and sometimes by other devices in the local area network (usually due to broadcast).

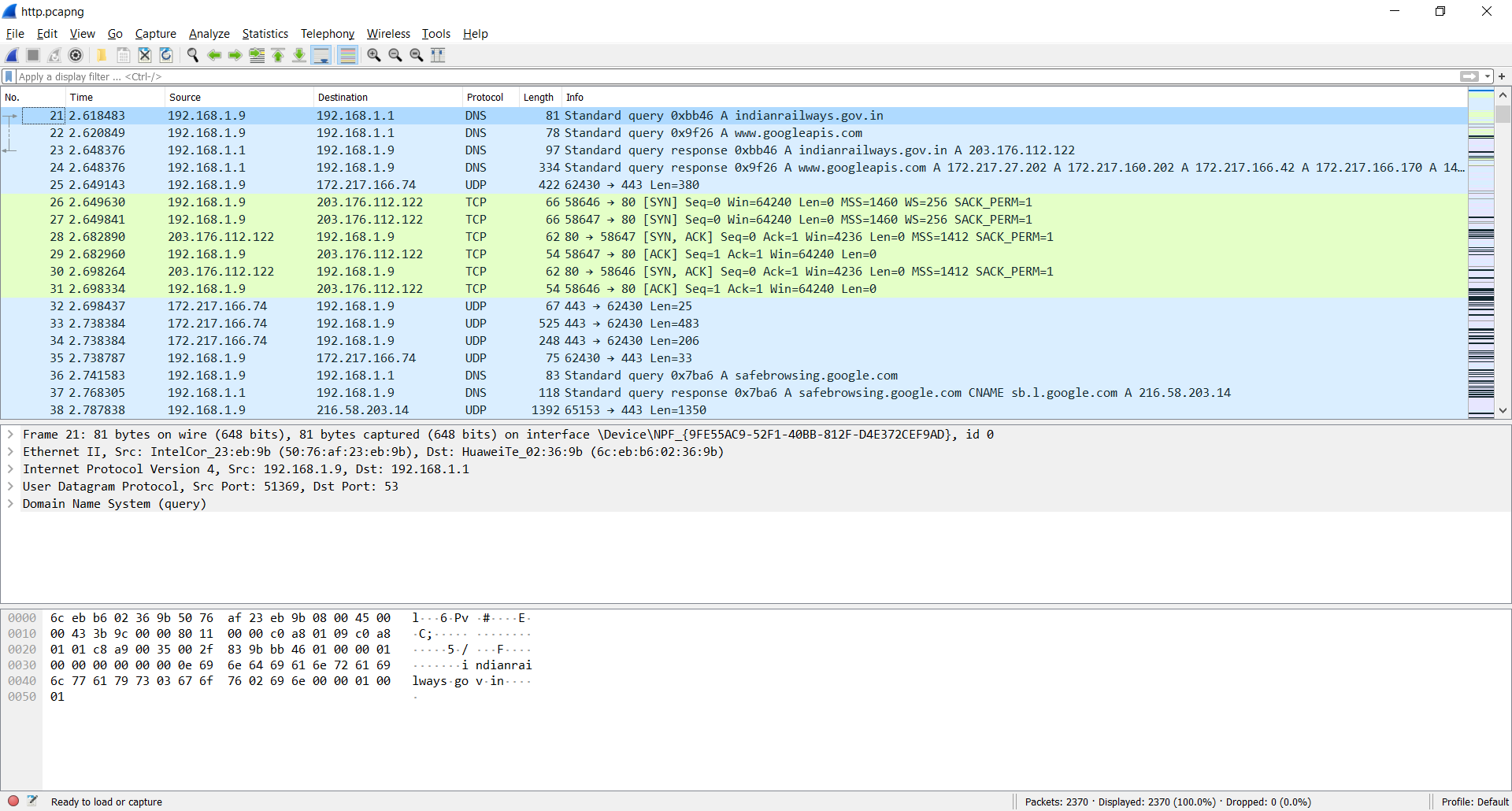


From the above image, ARP packets sent to machine per minute

= (0.3 packets per second) \* 60

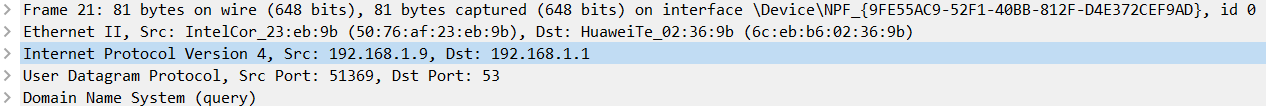
= 18 packets per minute

In this first part you will examine a packet capture for a web browsing operation. Open the capture file ‘http.cap’ (clear any display filters) and use WireShark to answer the following questions:



1. What is the IP address of the host?

The packet selected is a DNS query packet, which is sent by the computer (host) to the router. The IP address of the host, i.e. Src in the section highlighted below, is 192.168.1.9



1. What is the IP address of the router?

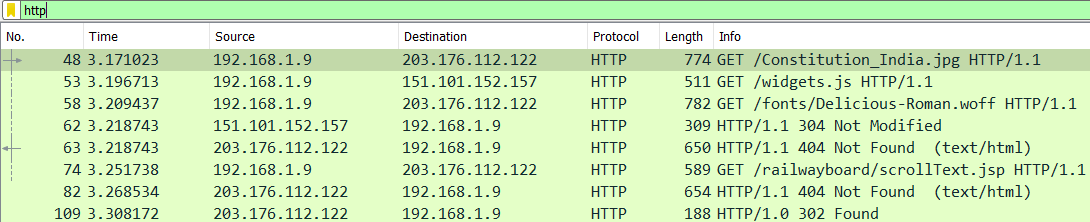
The IP address of the router, i.e. Dst, is 192.168.1.1

1. What protocol is used to resolve the website domain name?

The Domain Name Resolution (DNS) protocol is used to resolve the website domain name.

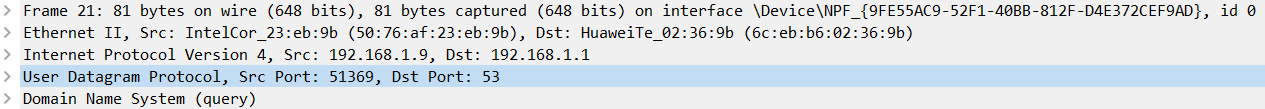
1. What is the IP address of the HTTP server?

Applying http as the display filter, the server’s IP address can be seen to be 203.176.112.122, which is the IP address of indianrailways.gov.in



1. Which transport layer protocol is used by DNS?

The details of the DNS packet selected in Q1 and Q2 have been shown once again in the following segment of the packet capture:



The transport layer protocol used by DNS is User Datagram Protocol (UDP), which is highlighted in the above picture.

1. Which well-known port is used when contacting the DNS server?

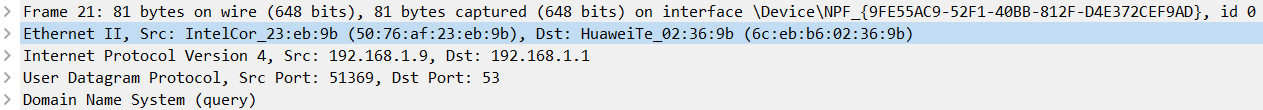
Since the selected DNS packet (from Q1) is a DNS query by the computer, the destination port number present in this packet will be the well-known port used for contacting the DNS server. This port number, i.e. Dst Port, is port 53, highlighted in the above picture.

1. Which ephemeral port does the host initiating the DNS query use?

This ephemeral port number is the Src Port in the above picture, which is port 51369.

1. What is the Ethernet address of the host?

The Ethernet II section of the details of the selected DNS packet (from Q1) is highlighted below. The ethernet address of the host (the computer which sends the DNS query), i.e. Src in the highlighted line below, is 50:76:af:23:eb:9b.

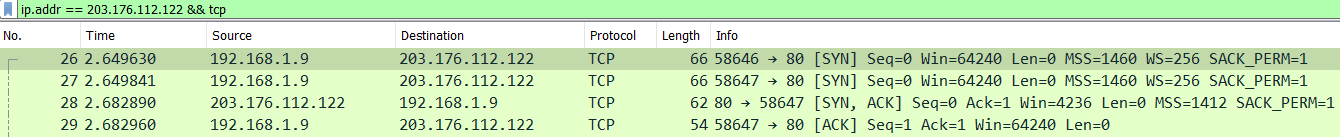


1. What is the ethernet address of the router?

The ethernet address of the router, i.e. Dst in the highlighted line in the above picture, is 6c:eb:b6:02:36:9b.

1. How long does the 3-way handshake take to complete?

The 3-way handshake happens over the TCP protocol, with the host (computer) and the server (203.176.112.122 i.e. indianrailways.gov.in) participating in the handshake. Hence, applying the following display filter: ip.addr == 203.176.112.122 && tcp



The 3-way handshake is the time between the first SYN and the first ACK

= 2.682960 – 2.649630

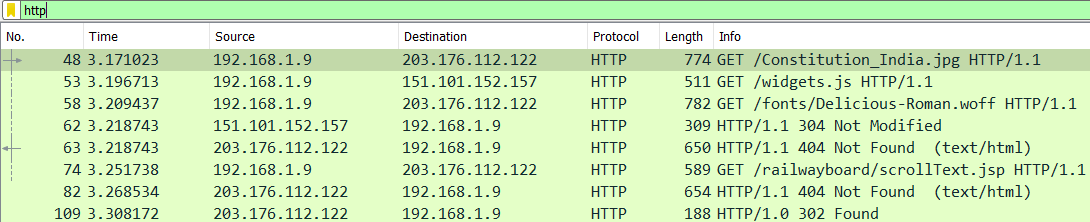
= 0.033330 seconds

1. Which website is the host machine trying to access?

The host machine is trying to access indianrailways.gov.in, whose IP address is 203.176.112.122

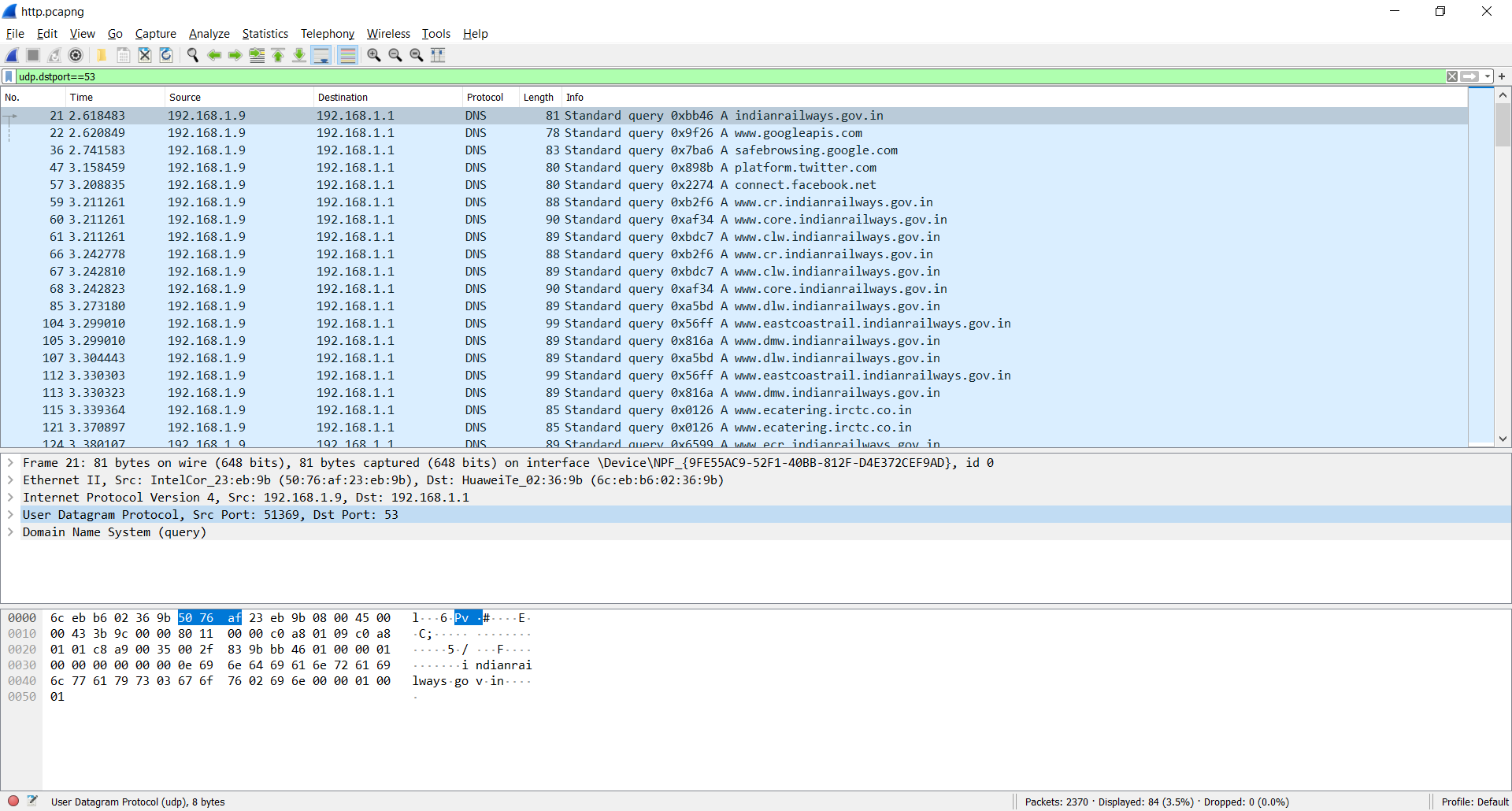
1. What version of HTTP is the browser running?

Applying http as the display filter, it can be seen that the HTTP GET requests made by the host (192.168.1.9) specify HTTP 1.1 as the HTTP version.



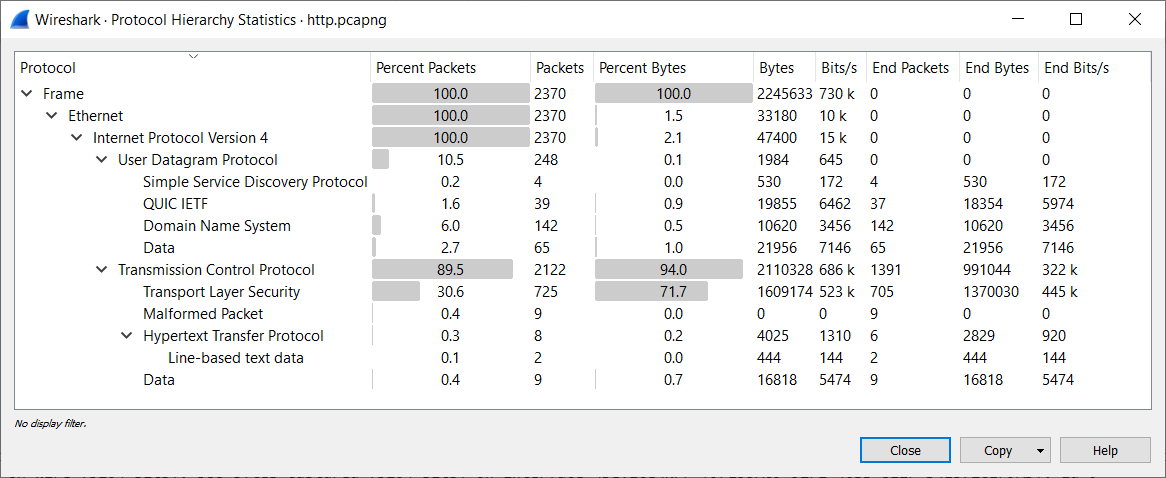
1. In the filter box enter the following query: udp.dstport==53 and click apply. What does the query mean and what are the results?

This query is used to display all the packets having UDP as the transport layer protocol, with the destination port number as 53. Port 53 is the well-known port number used for contacting the DNS server.



Result: All those packets are displayed which are DNS queries.

1. Go to Statistics -> Protocol Hierarchy and answer:



1. What percentage of frames are Ethernet frames?

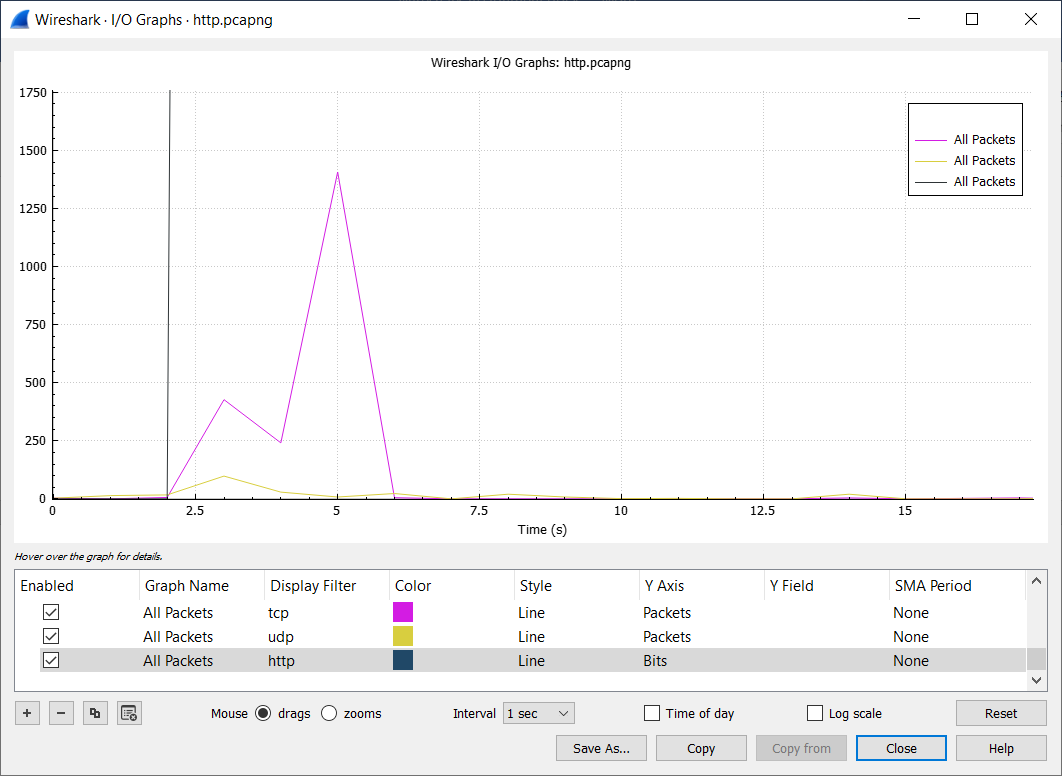
100%

1. Which transport layer protocols were present and which one made up more of the traffic?

User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) were present.

TCP made up more of the traffic (89.5%).

1. Now plot the UDP and TCP traffic as follows:
   1. Go to Statistics -> IO Graph (Adjust Interval as appropriate).
   2. Click + and add Display filter: tcp (Rest of the information can be default)
   3. Click + and add Display filter: udp (Rest of the information can be default)
   4. Click + and add Display filter: http and Y Axis: Bits (Rest of the information can be default)



Answer the following questions:

1. What is the highest number of TCP packets/sec observed? Around what time (second)?

1407 packets/sec, at t = 5 seconds.

1. What is the highest number of UDP packets/sec observed? Around what time (second)?

98 packets/sec, at t = 3 seconds.

1. What is the highest number of HTTP bits/sec observed? Around what time (second)?

3.566e+04 bits/sec, at t = 3 seconds.