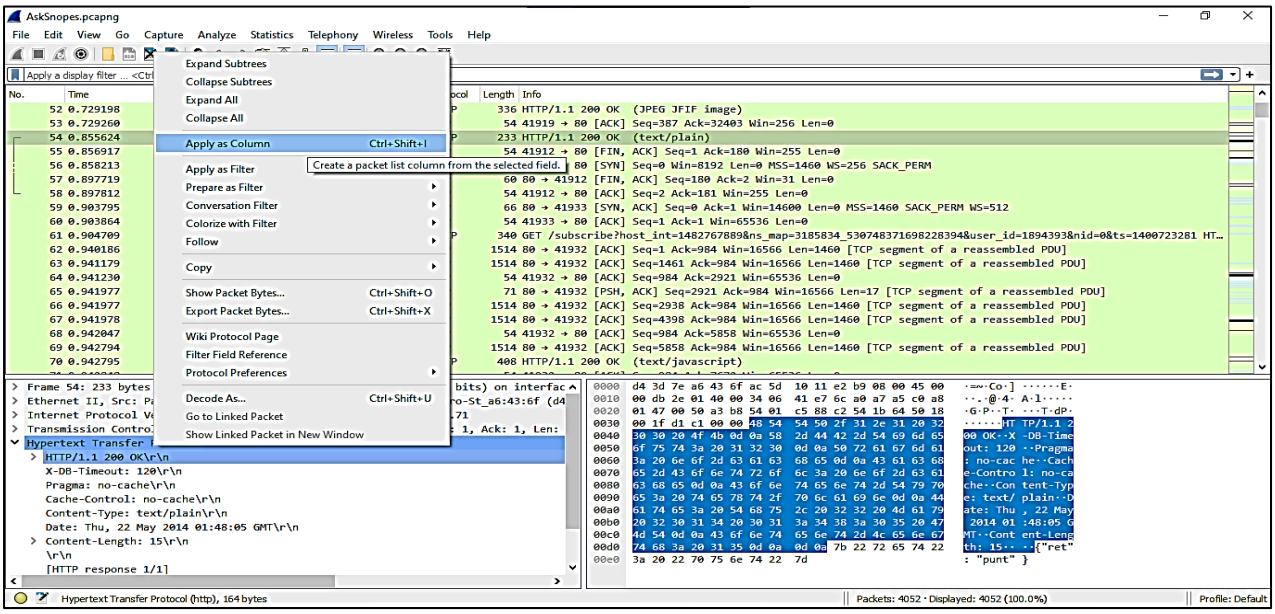
PRACTICAL NO: 05

Aim: Analyse the packets provided in lab and solve the questions using Wireshark

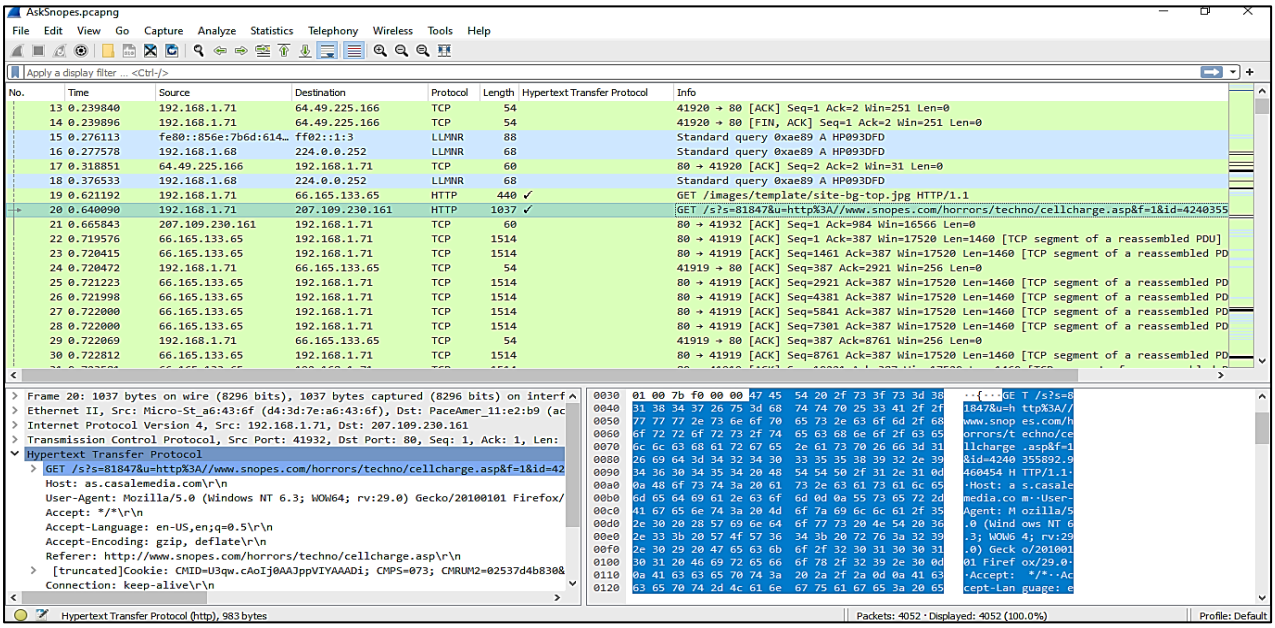
- What web server software is used by www.snopes.com?
- About what cell phone problem is the client concerned?
- According to Zillow, what instrument will Ryan learn to play?
- How many web servers are running Apache?
- What hosts (IP addresses) think that jokes are more entertaining when they are explained?

1. What web server software issued by www.snopes.com?

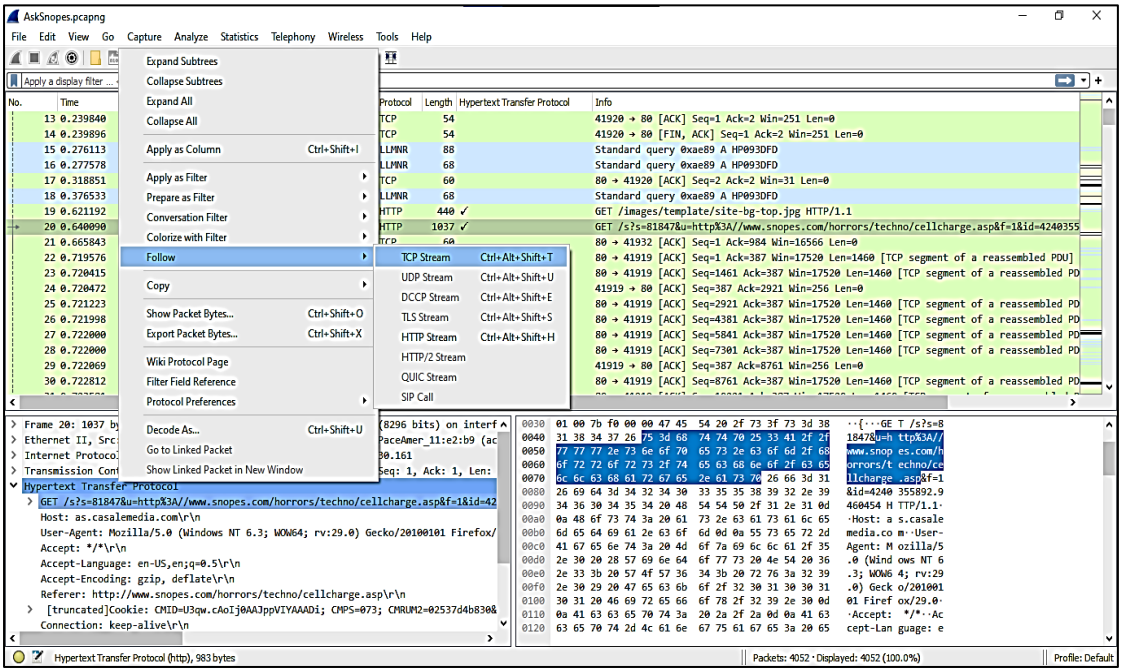
Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then Apply as Column



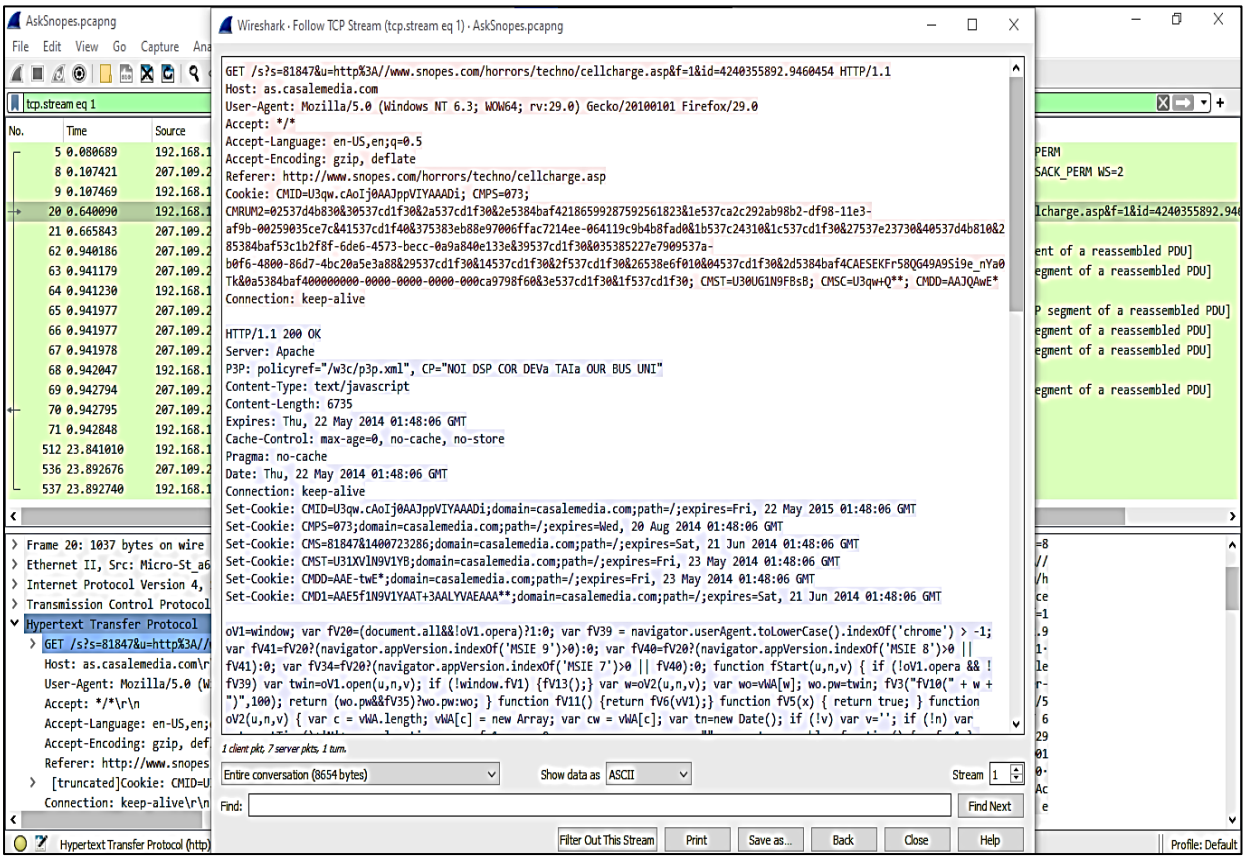
Now we can see our host www.snopes.com in host column.



Right click on the selected packet and then select Follow TCP stream.



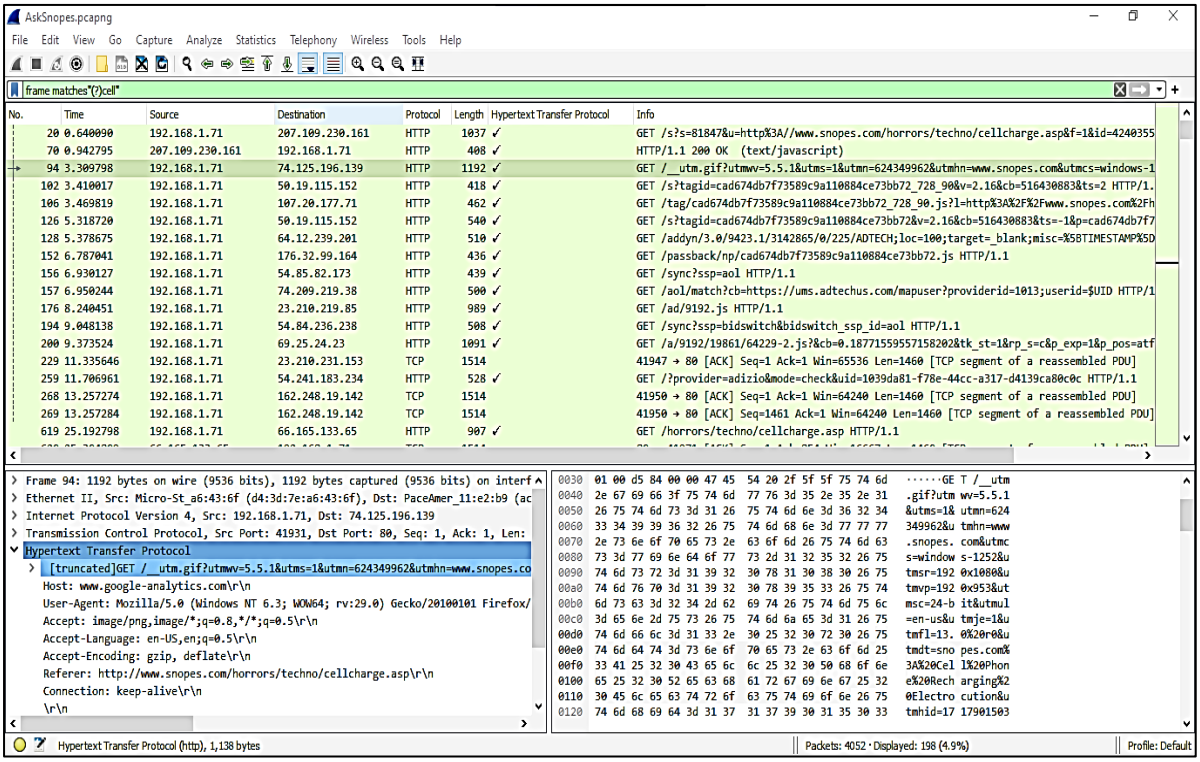
Now we can see the webserver name in server header it is Microsoft IIS 5.0



2. About what cell phone problem is the client concerned?

Apply **frame matches "(?)cell"**

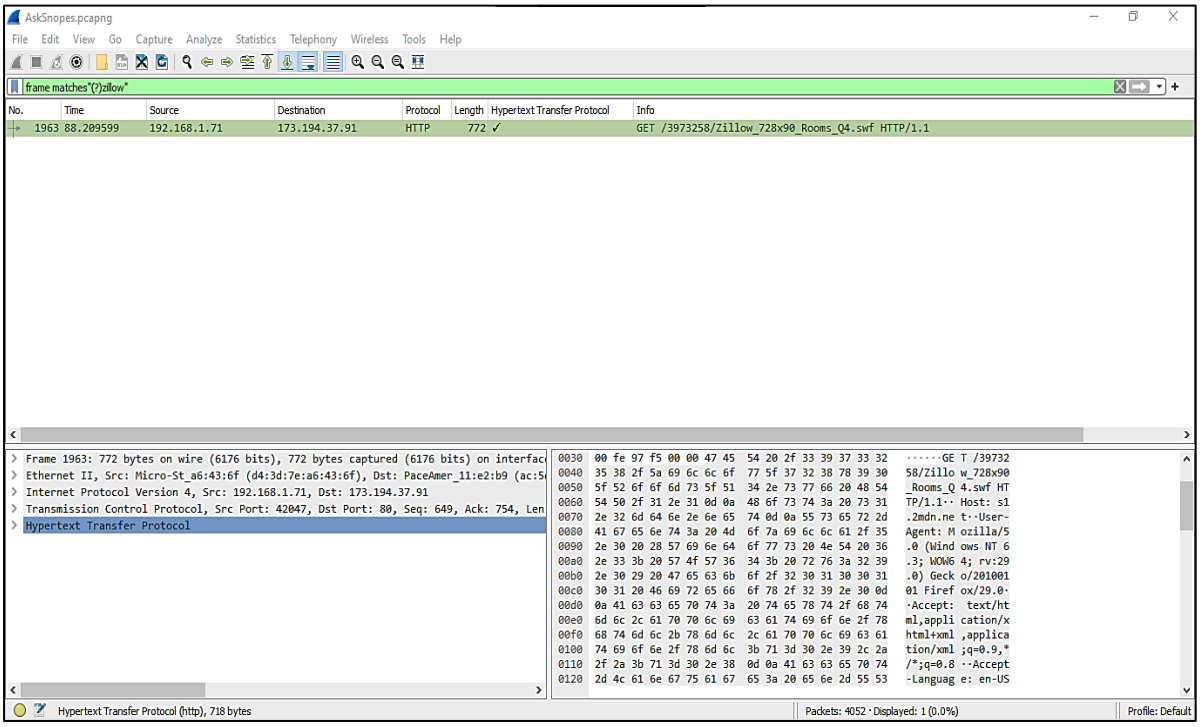
After applying the filter now, we will start to check every HTTP request. We noticed in the HTTP request cell keyword is in URL and it was about cell phone charging issue.



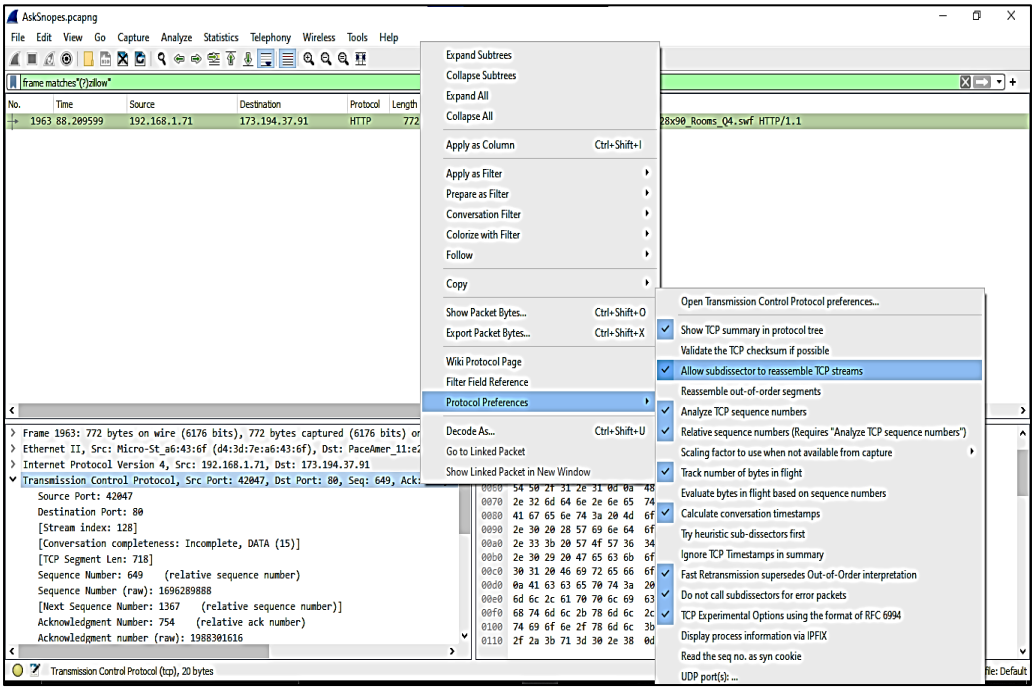
3. According to Zillow, what instrument will Ryan learn to play?

Apply **frame matches "(?) zillow".**

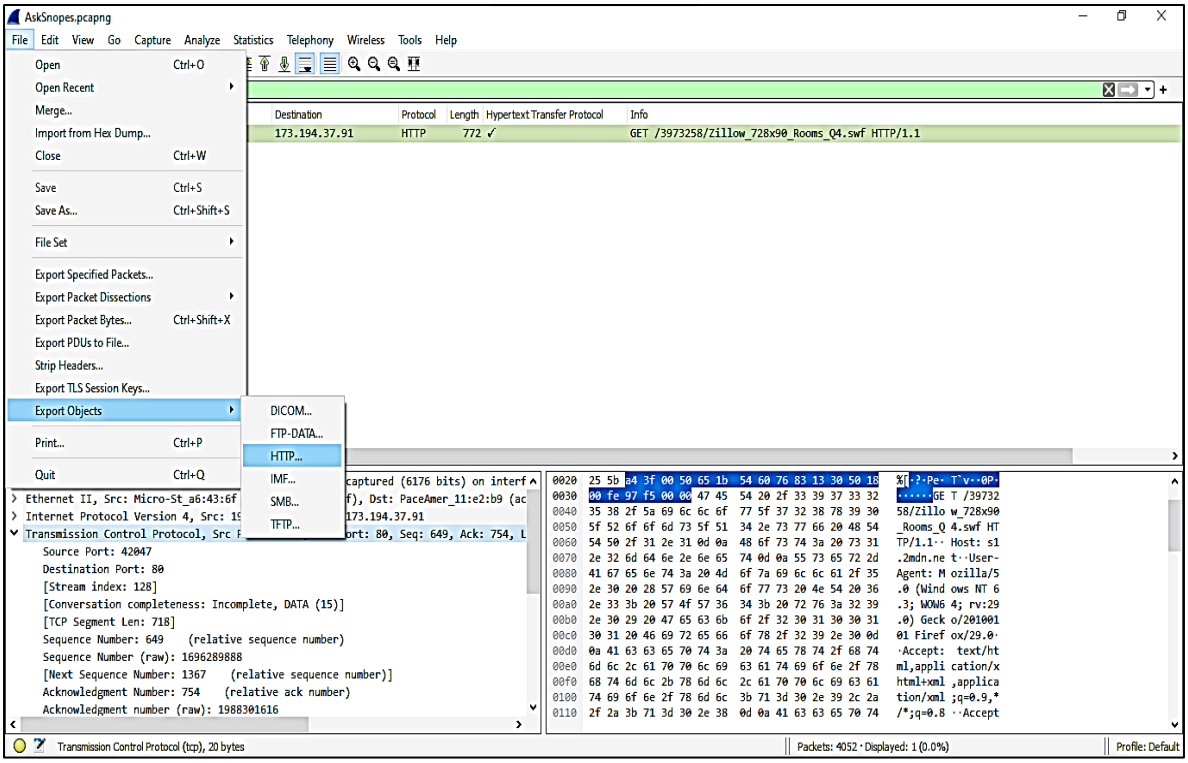
After applying the filter, we found only one packet with the Zillow keyword.



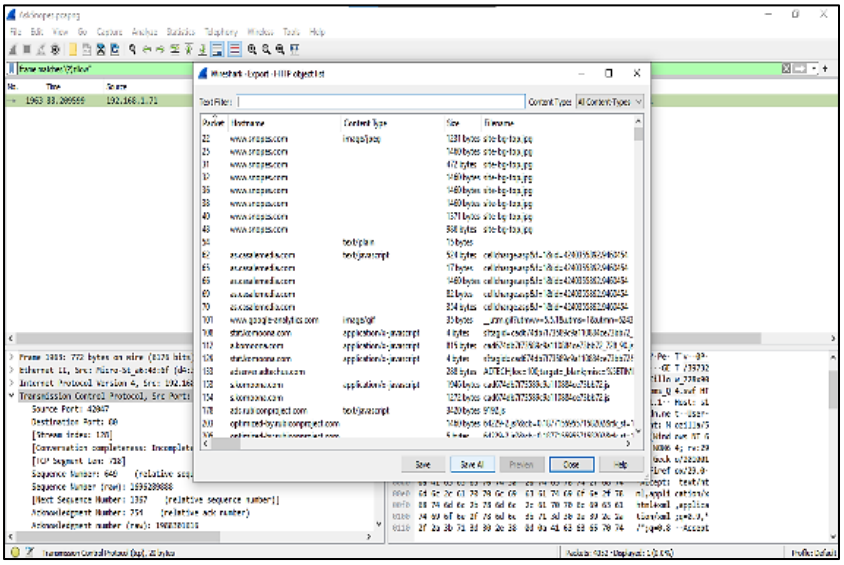
Select the packet and expand the Transmission Control Protocol tab right click on it go to Protocol Preferences and check Allow subdissector to resemble TCP stream.

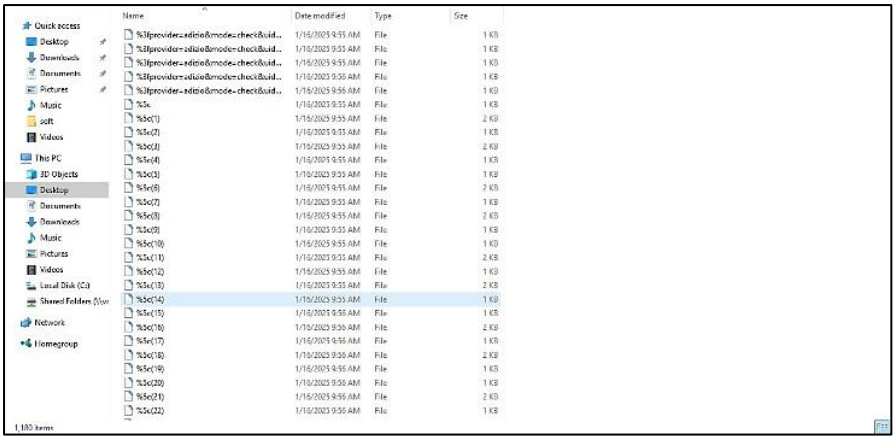


Now go to file and select **Export Objects HTTP**. It will save all objects from the packet.

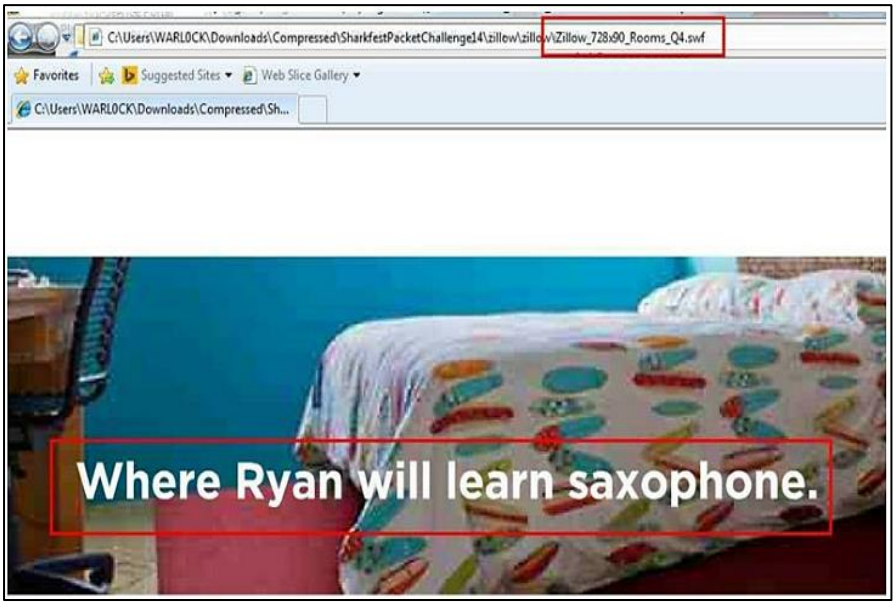


Click on **save all**.



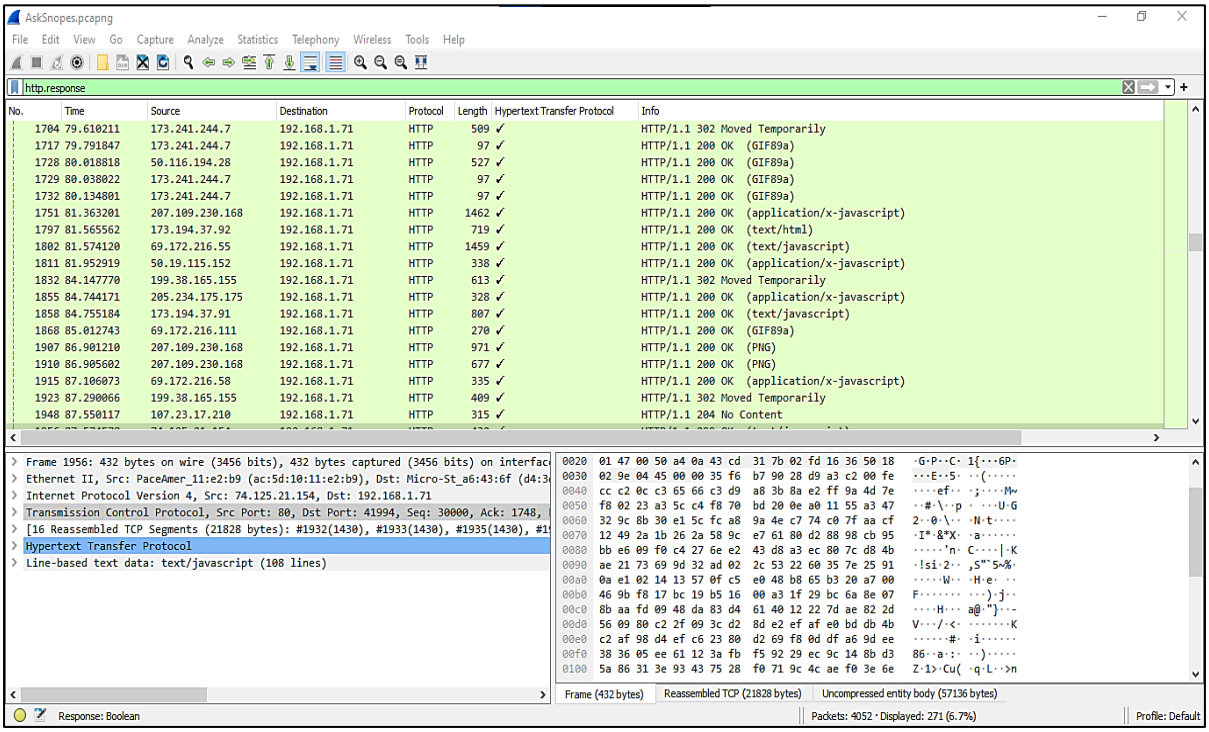


After saving all files in a directory and we found a swf file with name Zillow. After opening the flash file, we saw that Zillow was trying to learn saxophone.

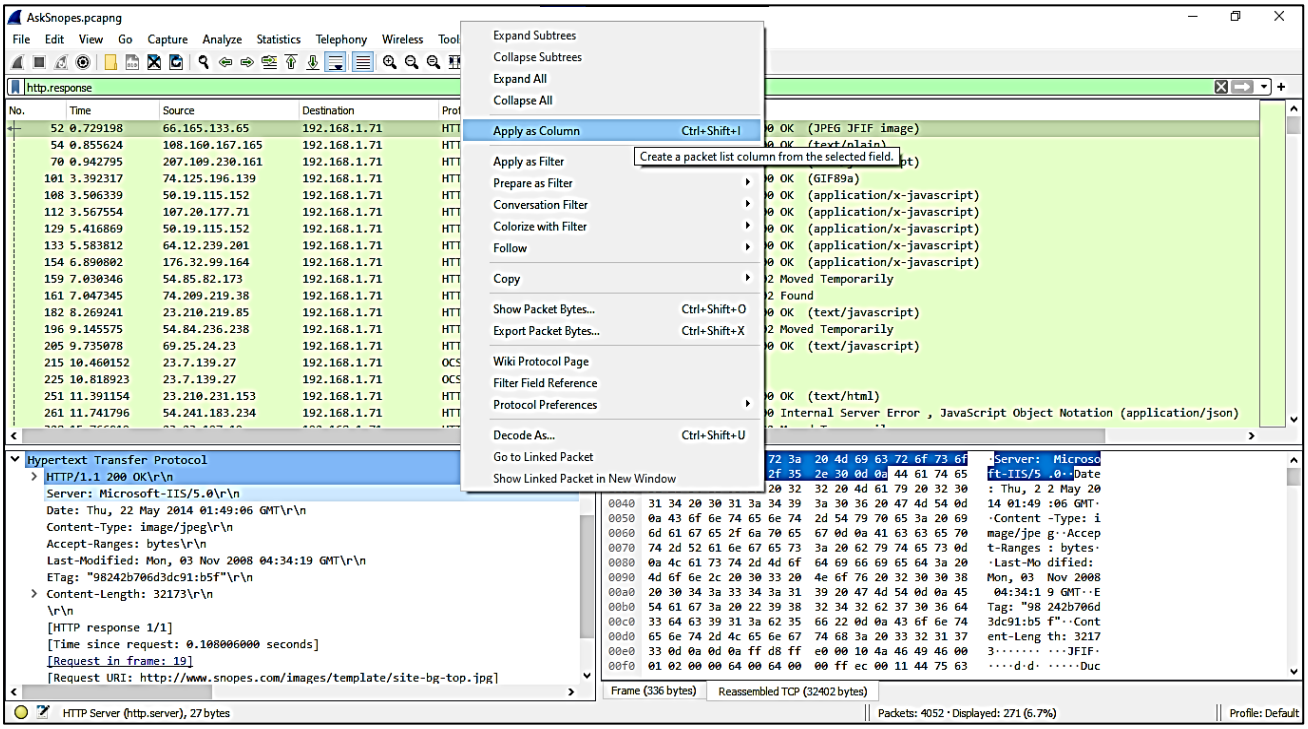


4. How many web servers are running Apache?

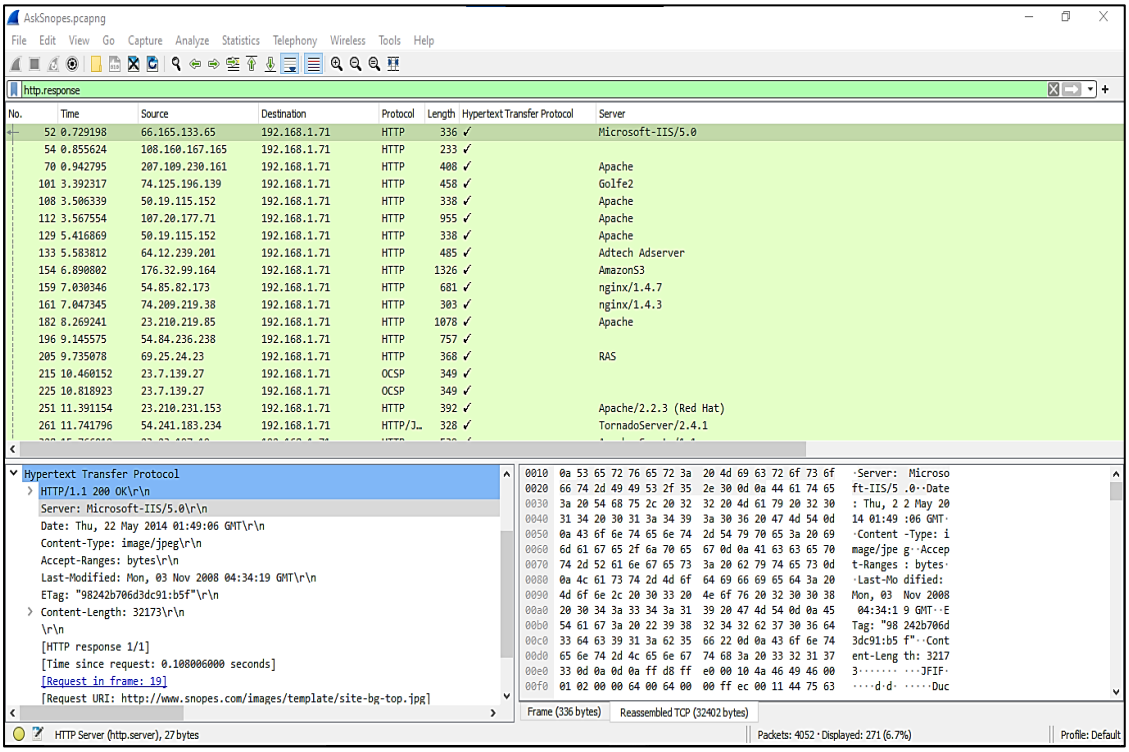
Apply filter **http.response** and we can see all http response packets.



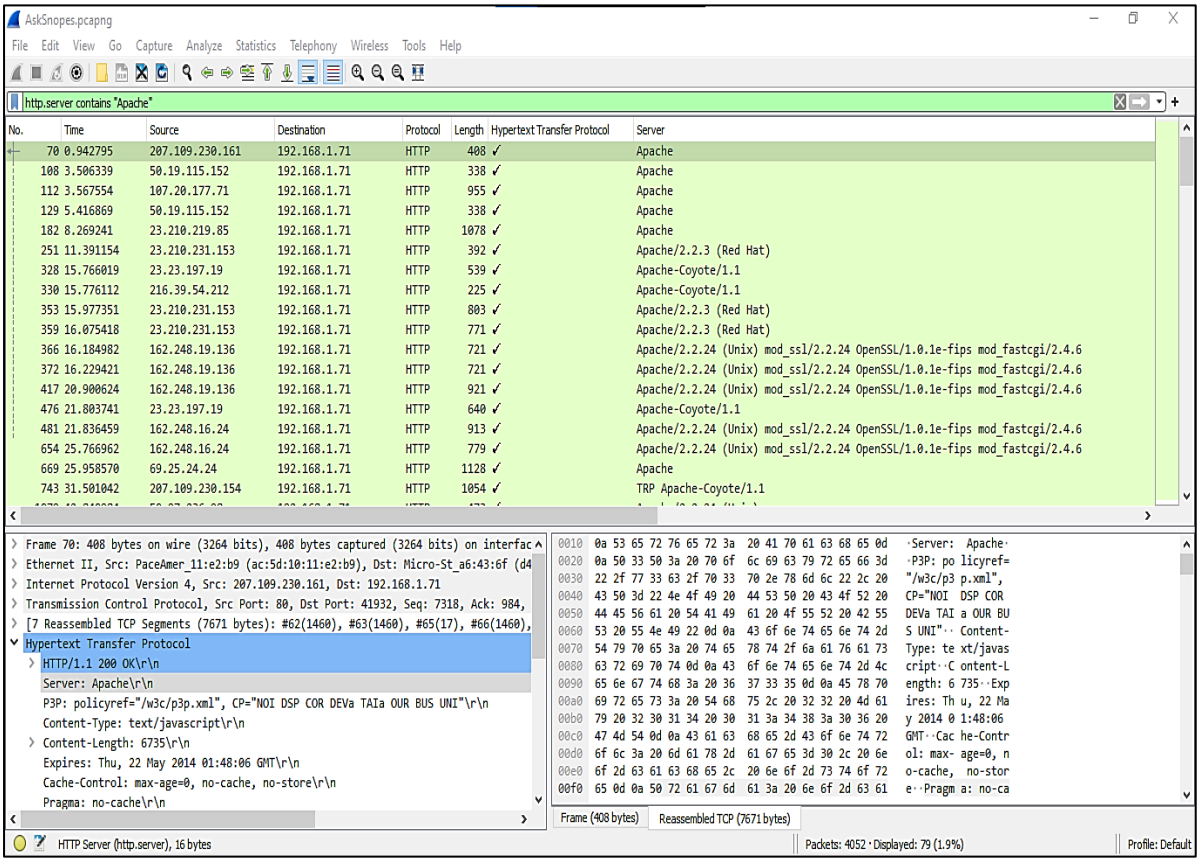
Now we will set the server header as column select any packet and right click on it then select Apply as Column.

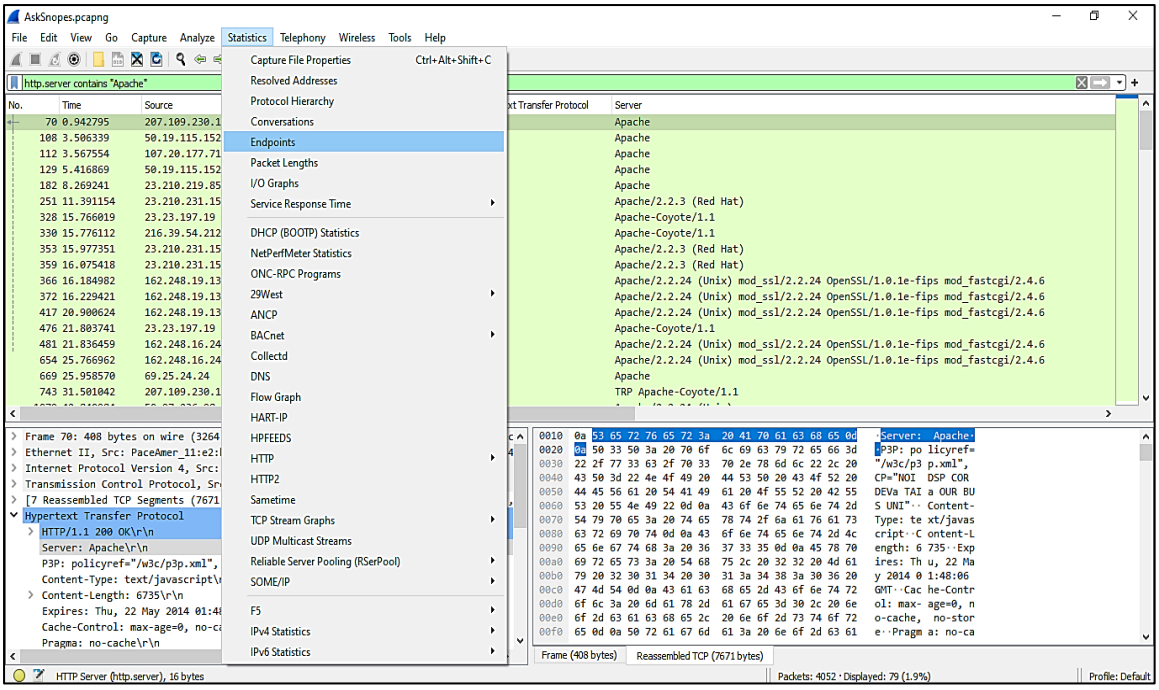


Now we can see the server column where all server name is showing.



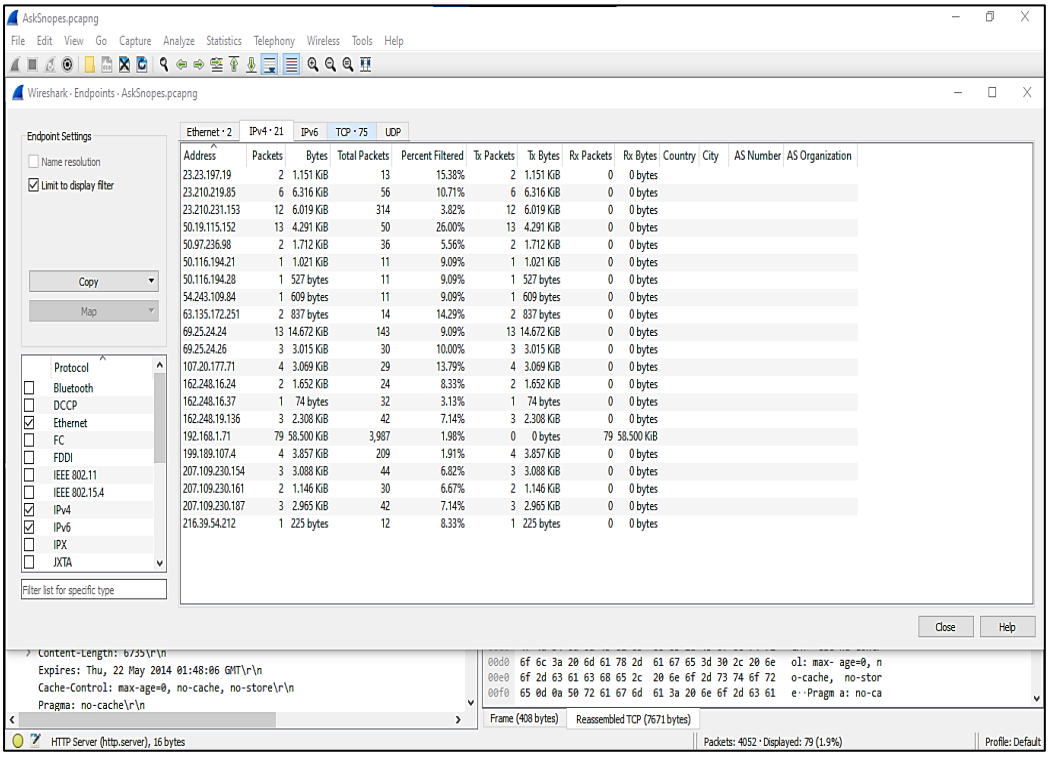
Now we have to check how many Apache packets are there we can't count manually for each packet so we will apply another filter **http.server contains "Apache"**





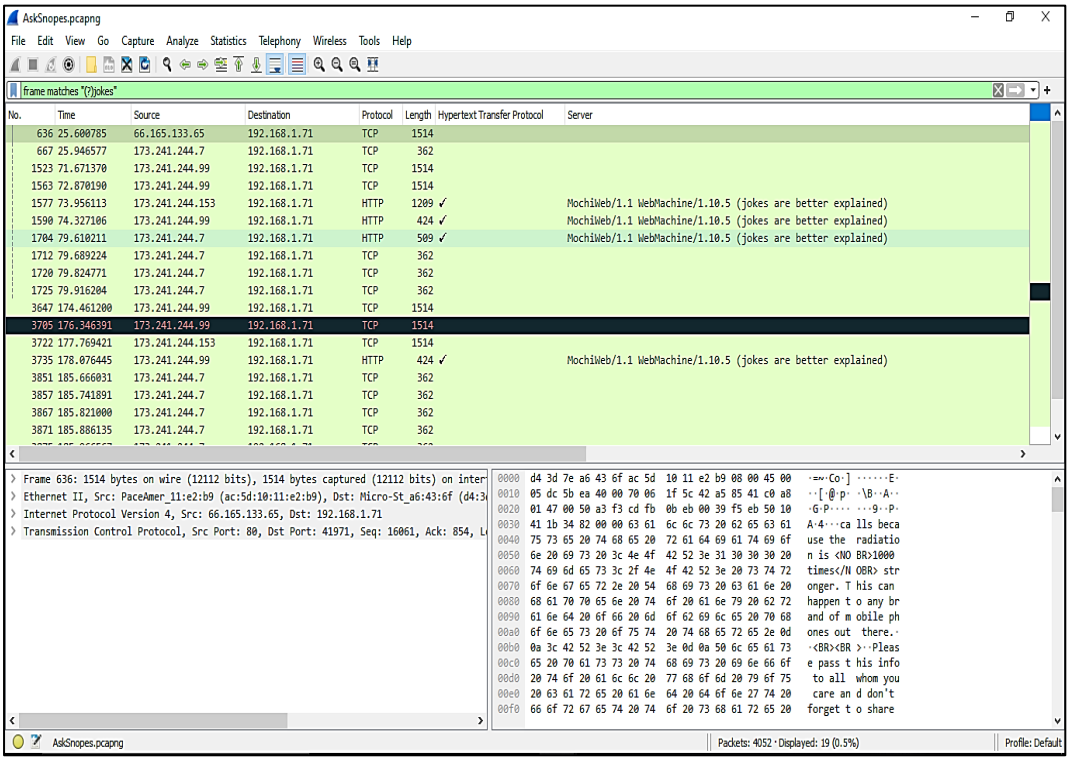
After applying filter go to **Statistics Endpoints.**

It will show all connections. Now Check the limit to display filter then it will show the actual Apache connections.



5. What hosts (IP addresses) think that jokes are more entertaining when they are explained?

Apply the filter **frame matches "(?)jokes"**



Select HyperText Transfer Protocol, then scroll down a little bit and a text stating the same as above will be there.

Thus, here the Hosts 173.241.244.153, 173.241.244.99, 173.241.244.7 think that jokes are more entertaining.