

Practical 5

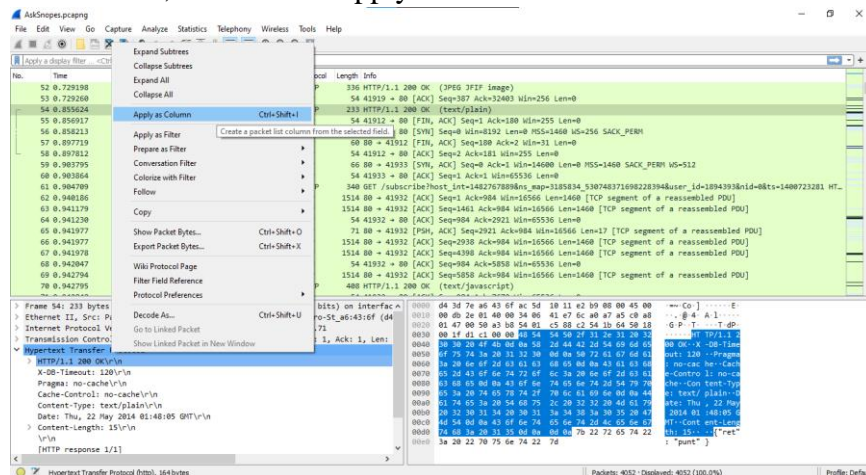
Aim: Analyse the packets provided in lab and solve the questions using Wireshark:

- 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?

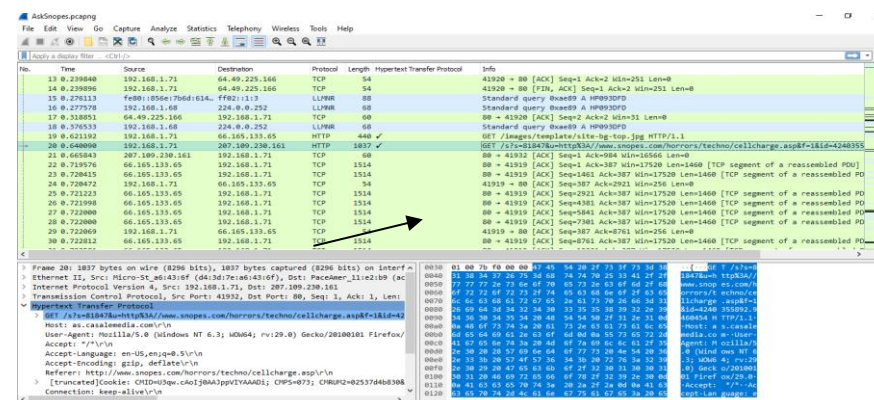
1. What web server software issued by www.snopes.com?

The domain name is available in the **Host** header. To view all domain names, we will add the Host header as a column.

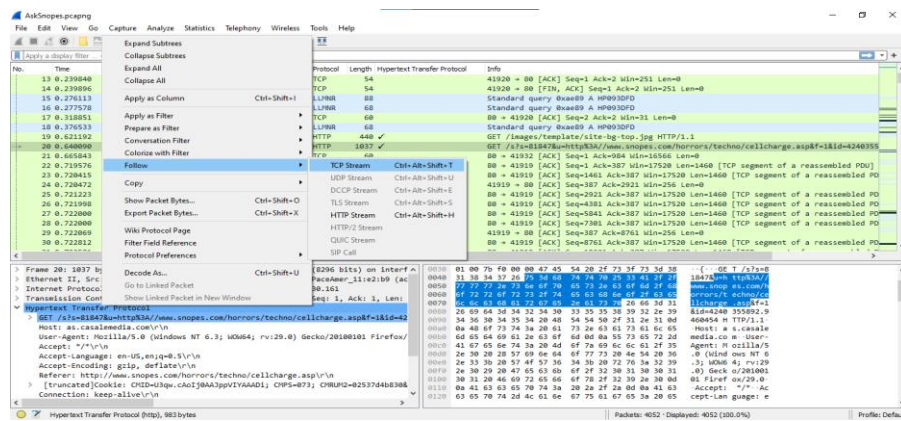
Select any HTTP request expand the HyperText Transfer Protocol section, right-click on the Host header, and choose Apply as Column.



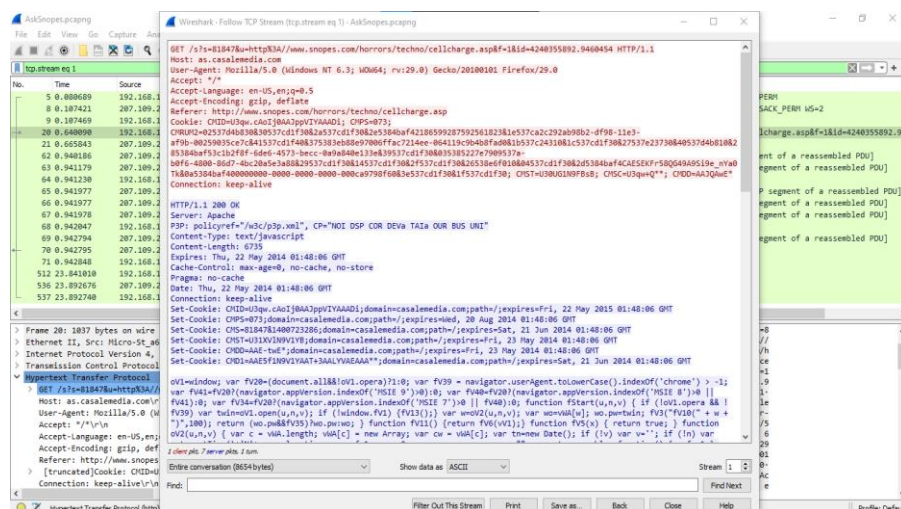
Now we can see our host www.snopes.com in host column.



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



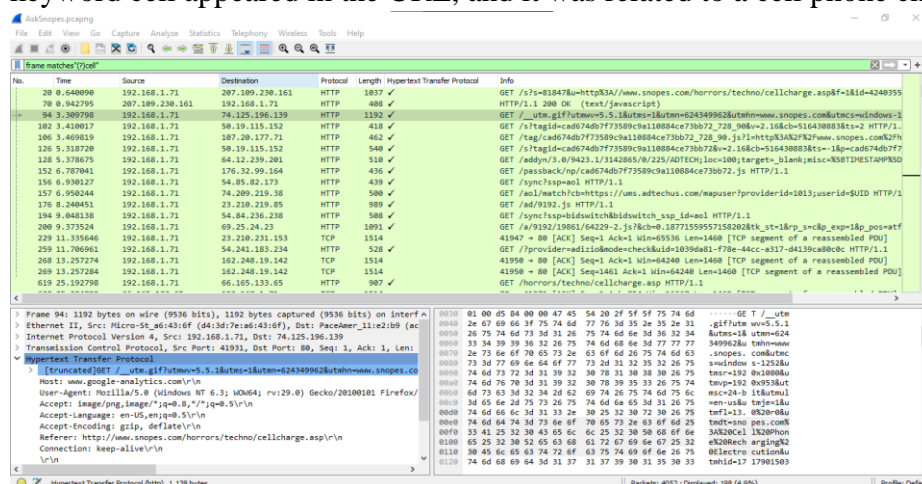
Now we can see the webserver name in server header it is Microsoft IIS 5.0



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

Apply frame matches “(?cell)”

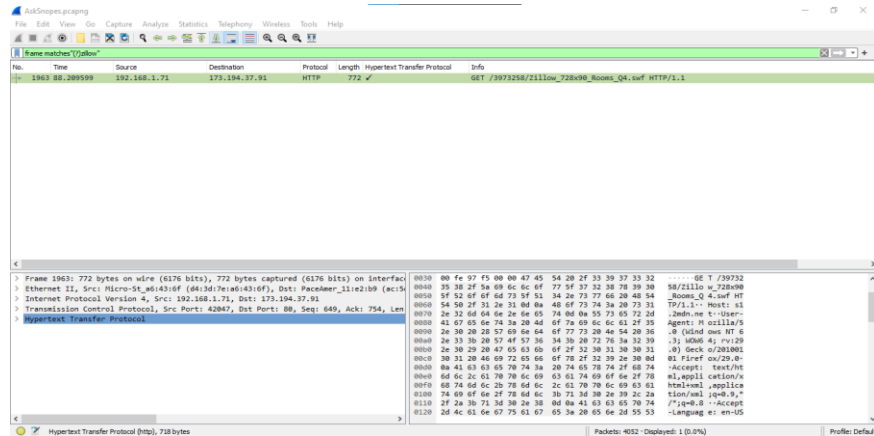
After applying the filter, we began inspecting each HTTP request. We noticed that the keyword cell appeared in the URL, and it was related to a cell phone charging issue.



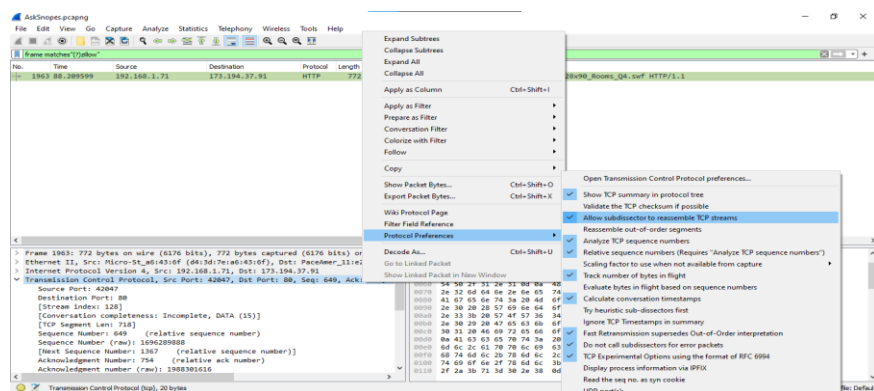
3. According to Zillow, what instrument will Ryan learn to play?

Apply frame matched “(?) zillow”.

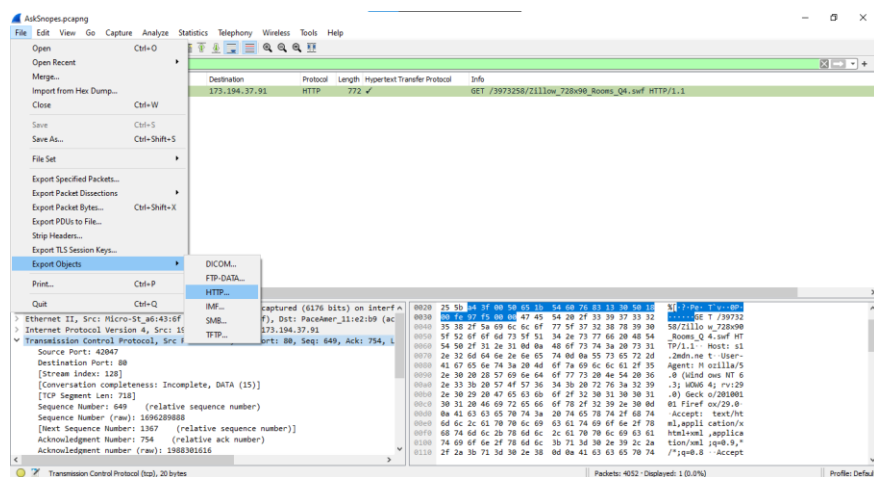
After applying the filter, we found only one packet with the Zillow keyword.



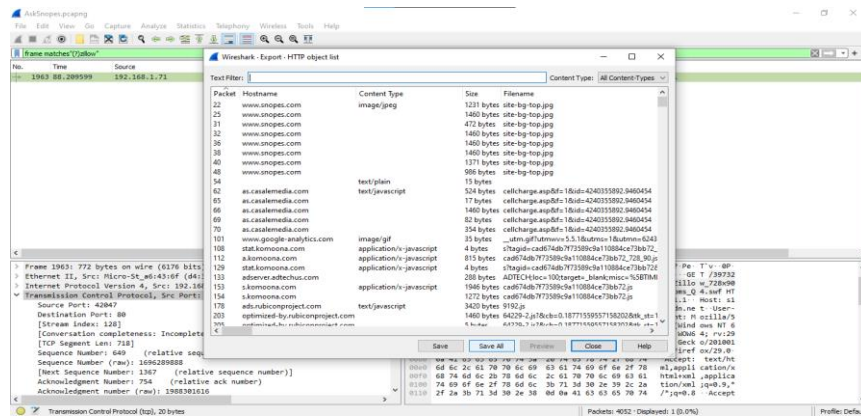
Select the packet, then expand the Transmission Control Protocol tab. Right-click on it, navigate to Protocol Preferences, and enable Allow subdissector to reassemble TCP stream



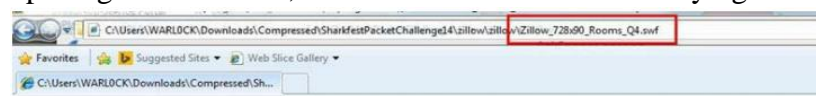
Now go to file and select **Export Objects** > **HTTP**. It will save all objects from the packet.



Click on **save all**.

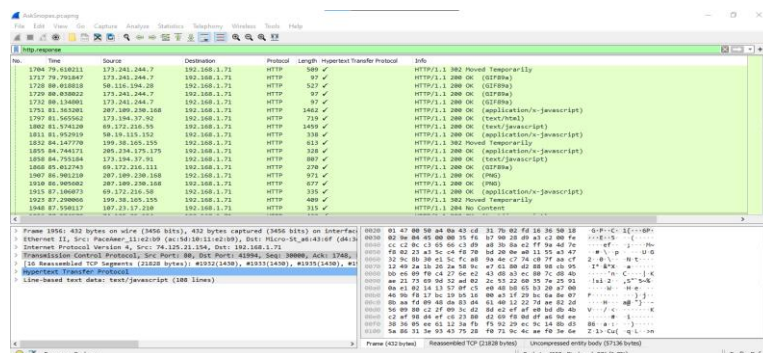


After saving all the files in a directory, we discovered an SWF file named ****Zillow****. Upon opening the Flash file, we found that ****Zillow**** was trying to learn the saxophone.**

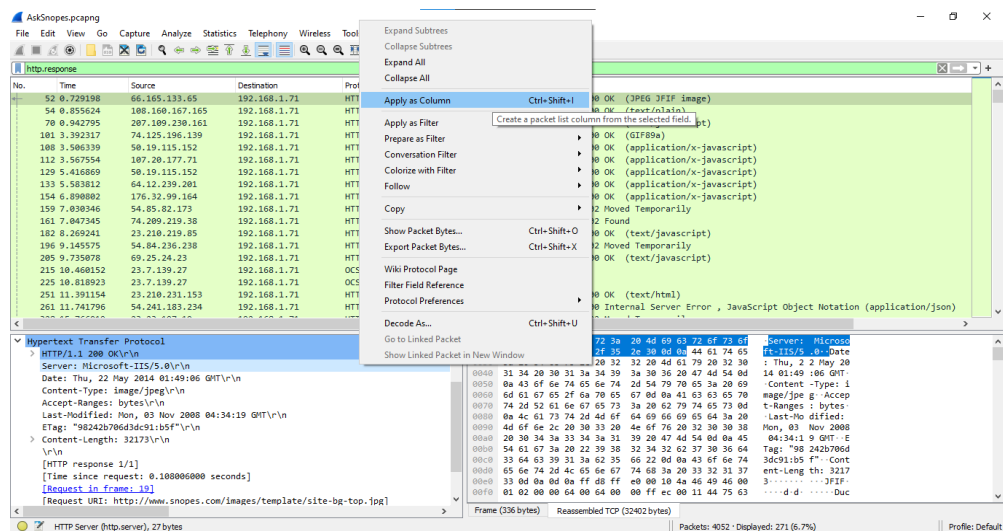


4. How many web servers are running Apache?

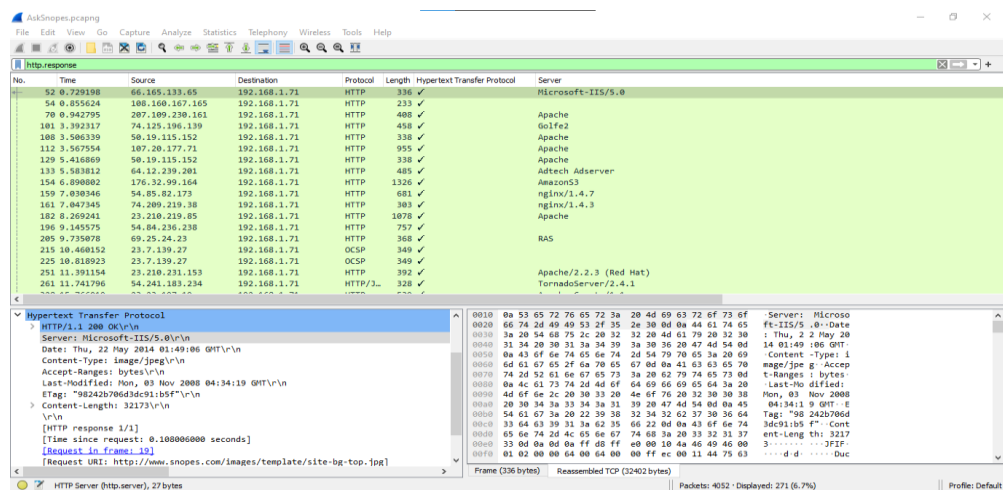
Apply filter **http. response** and we can see all http response packets.



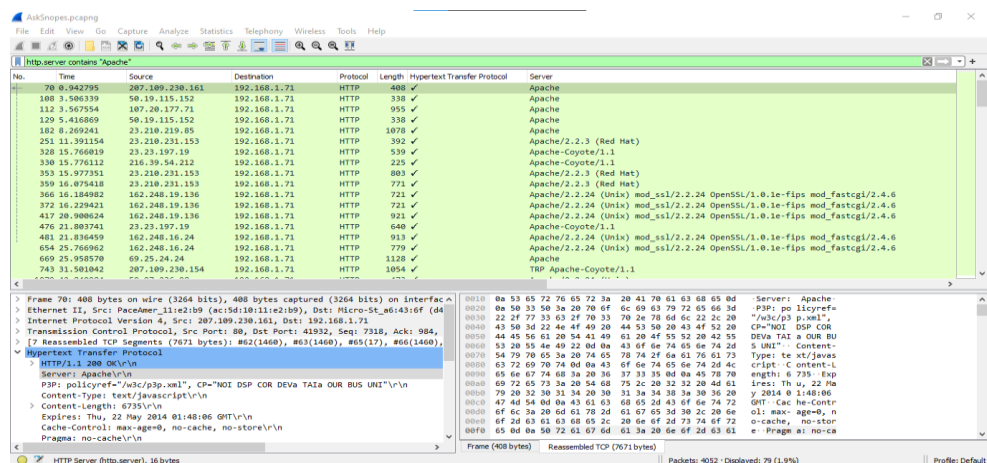
Now we will set the server header as column select any packet and right click on it then select Apply as Column.



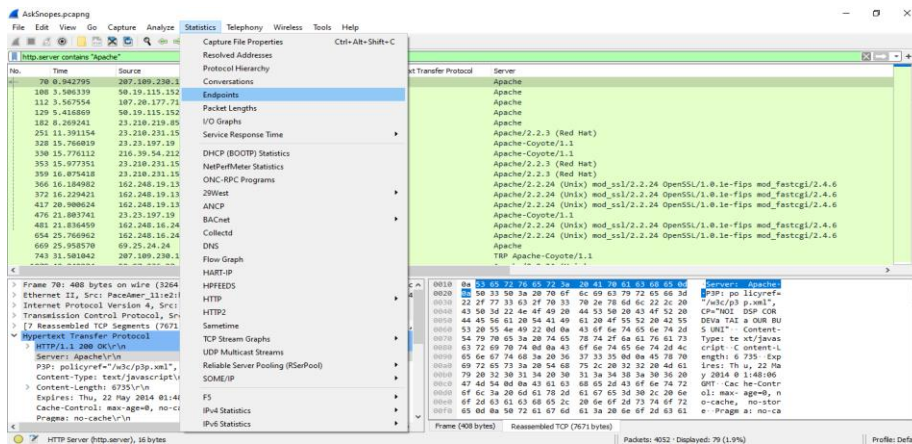
Now we can see the server column where all server name is showing.



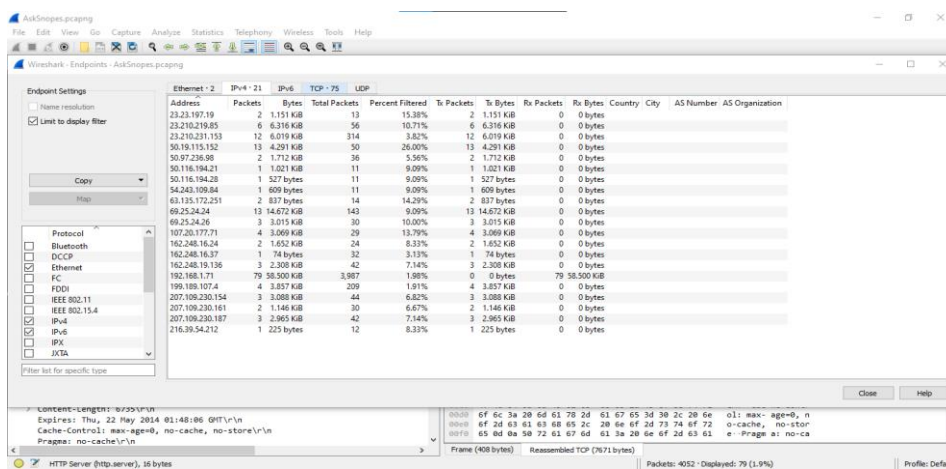
Now we have to check how many Apache packets are there we can't count manually for each packet so we will apply another filter **http.server contains "Apache"**



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



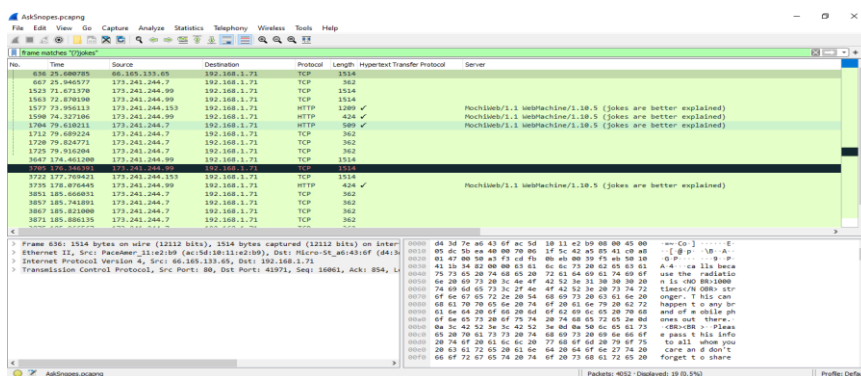
It will show all connections. Now Check the limit to display filter then it will show the actual Apache connections.



Now there are showing 21 connections, so there are actual 21 Apache servers.

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

Apply the filter frame matches "(?)jokes"



Find the HTTP packet where the server description states ****"jokes are better explained."****
Then, navigate to the ****HyperText Transfer Protocol**** section. Scroll down slightly, and you'll see the same text appearing again.

This suggests that the hosts ****173.241.244.153, 173.241.244.99, and 173.241.244.7**** believe that explaining jokes makes them more entertaining.

The screenshot shows the Wireshark interface with a packet list on the left and packet details on the right. The packet list shows several HTTP packets from 173.241.244.99 to 192.168.1.71. The selected packet is number 1575, an HTTP 200 OK response. The packet details pane shows the following information:

```

HTTP/1.1 200 OK\r\n
Set-Cookie: i=a0b60f51-8838-43d5-364e-1887b2430722; Version=1; Expires=Fri, 22-M
[truncated]Set-Cookie: pd=66482baa-af6b-11e1-8f8e-642b2800a35; 1480723359|216c7
Server: Mochiweb/1.1 webmachine/1.10.5 (jokes are better explained)\r\n
PSP: CP="CUR ADM OUR STA MID"\r\n
Date: Thu, 22 May 2014 01:49:19 GMT\r\n
Content-Type: text/html\r\n
Content-Length: 433\r\n
[Content length: 433]
Connection: close\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.078428000 seconds]
[Request in frame: 1575]
  
```

The packet details pane also shows the raw packet data in hexadecimal and ASCII format, with an arrow pointing to the ASCII representation of the 'jokes are better explained' message.