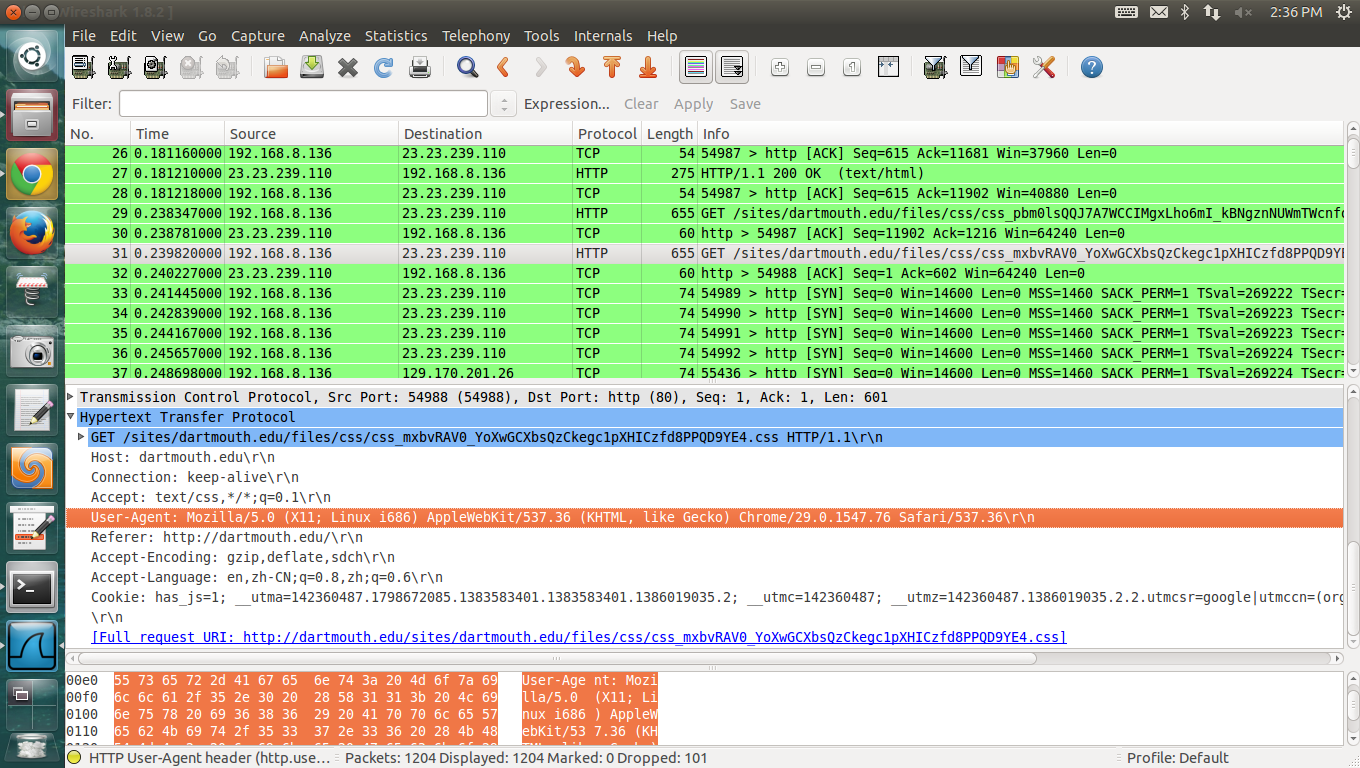
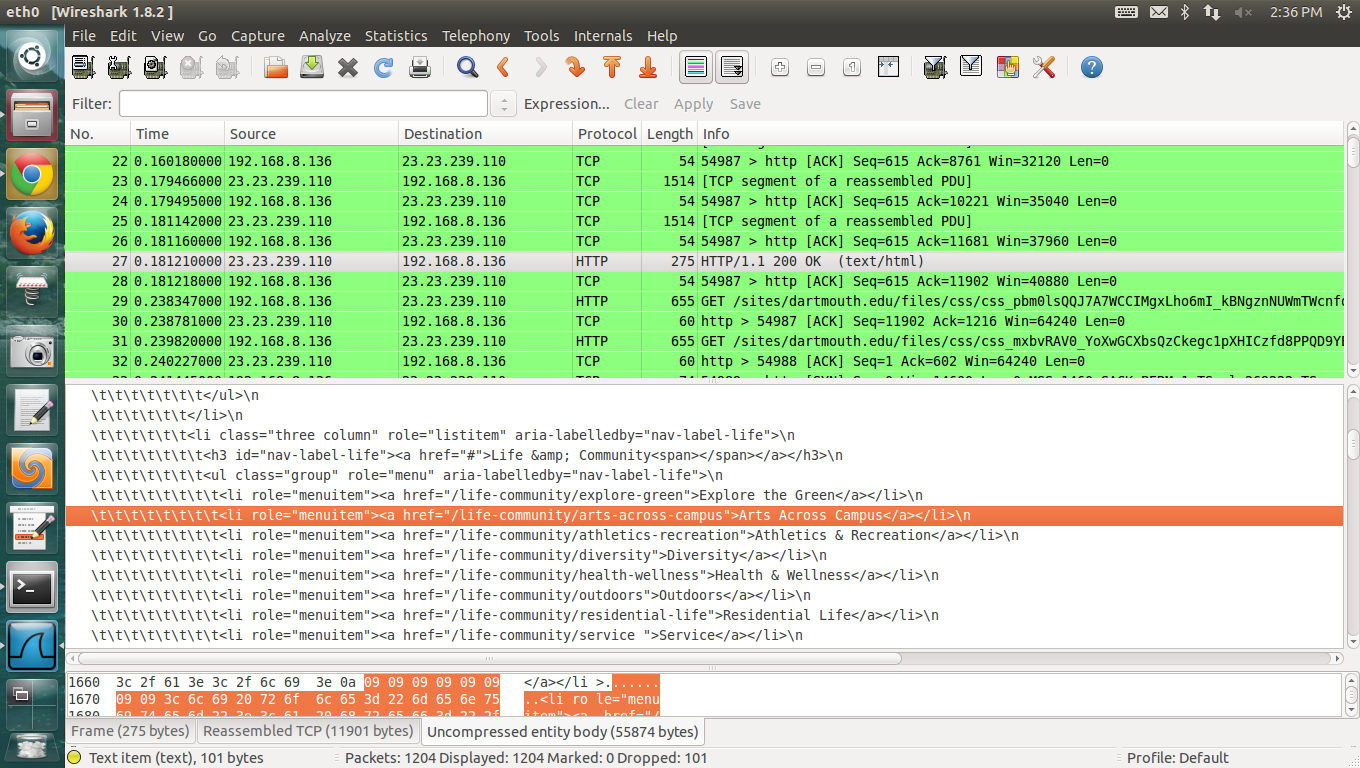
3) Examine the trace and find the exchange of packets between your machine and the web server (the host providing the web pages to your machine). Can you find an example packet in the packet exchange where the packet contains details about the type of your web browser (e.g., if it is Fire Fox, Internet Explorer, Safari, etc.) being used?

Yes, in the http protocol we can actually observe the “User-Agent” entry, which describe my OS, and the browser’s platform, etc.



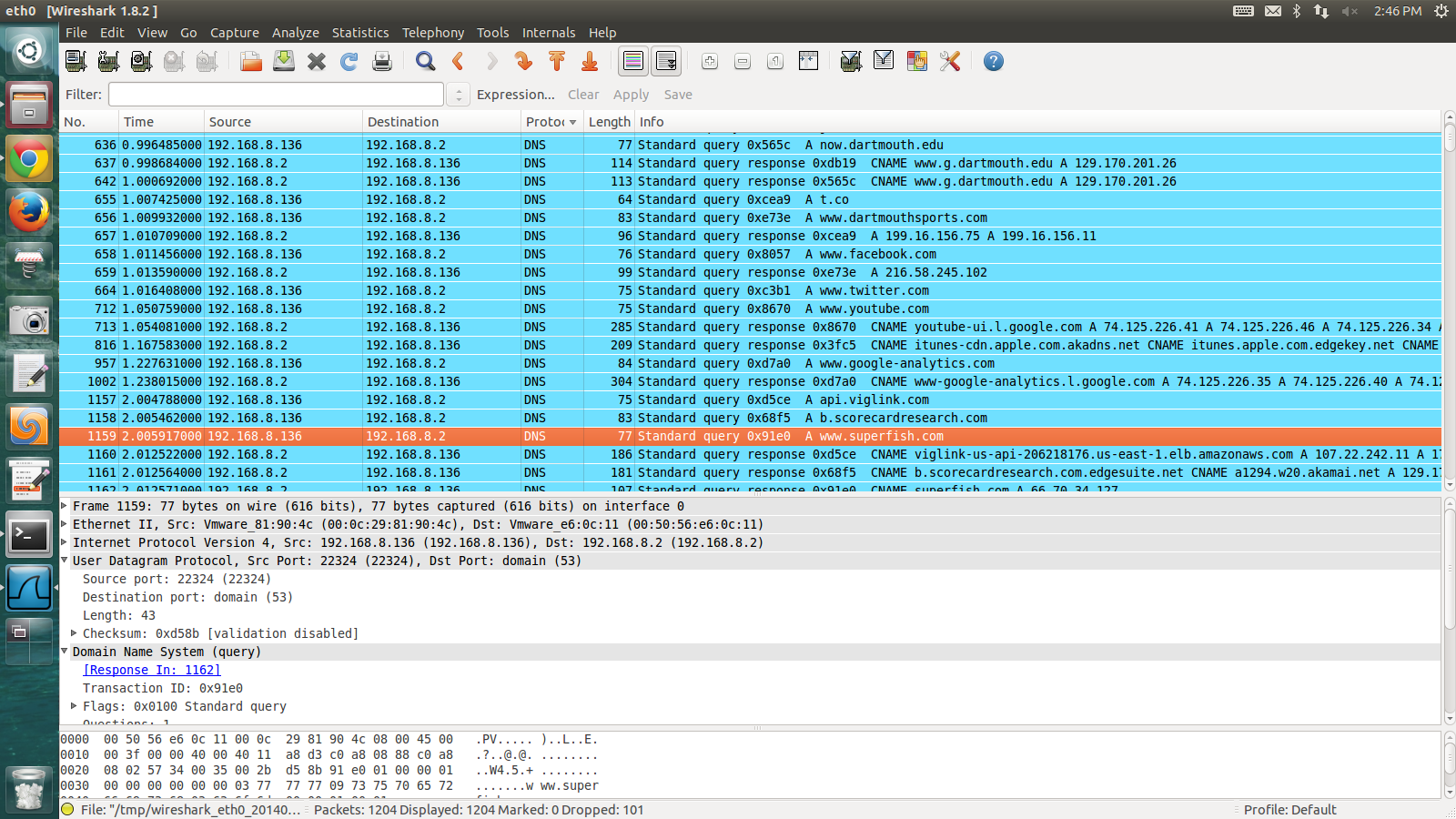
What is the value you found in the packet trace? Why do you think that the client informs the server of this information? Take a look at the source html for the page your client downloaded (i.e., http://www.dartmouth.edu). Do you see any of the attributes found in the packet (e.g.,browser type) in the html source or any of the other attributes in the same packet that contains the browser type? If you can not find these attributes in the html source why do you think that is in fact the case?

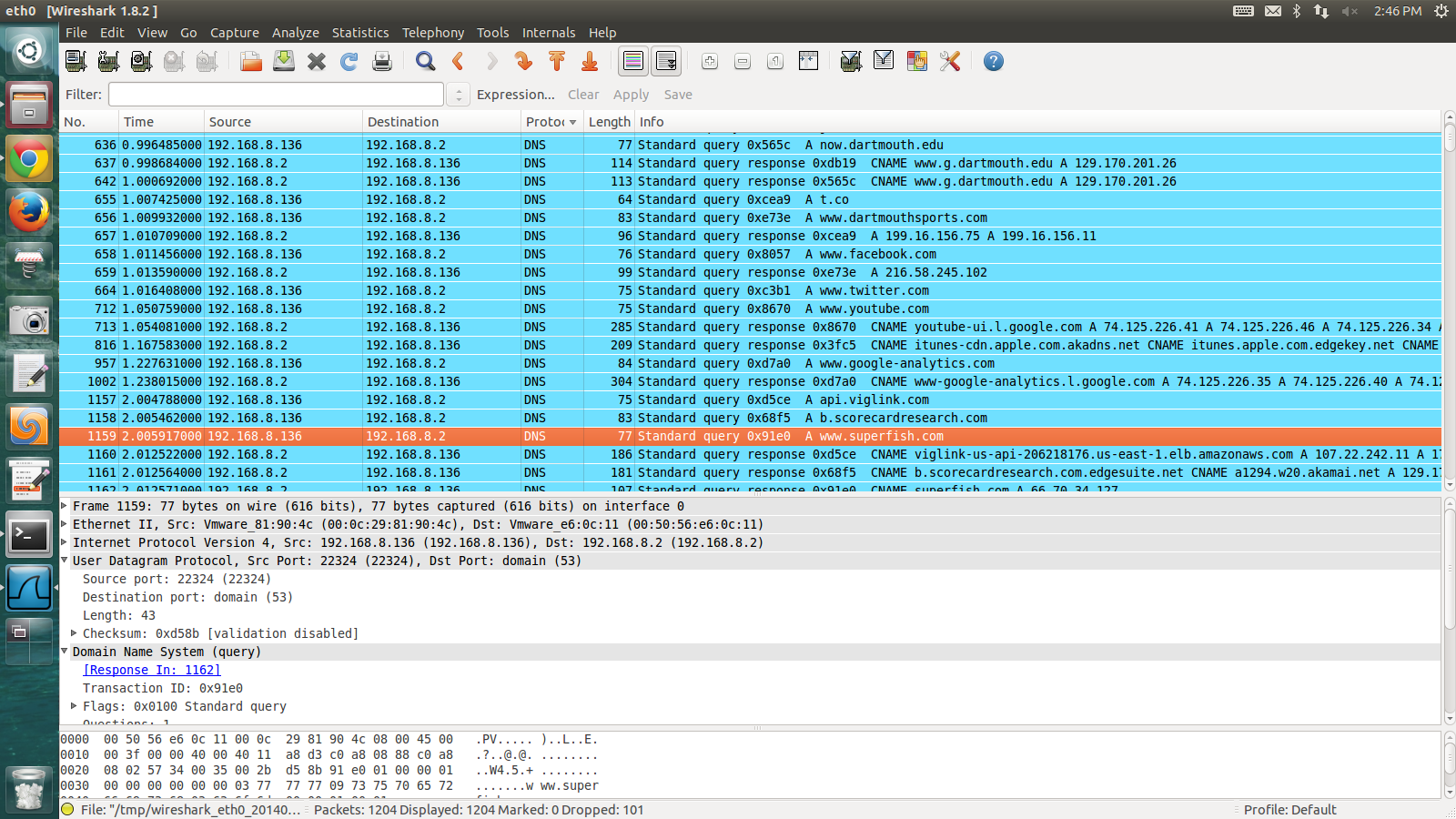
Yes I can the row html text clearly.



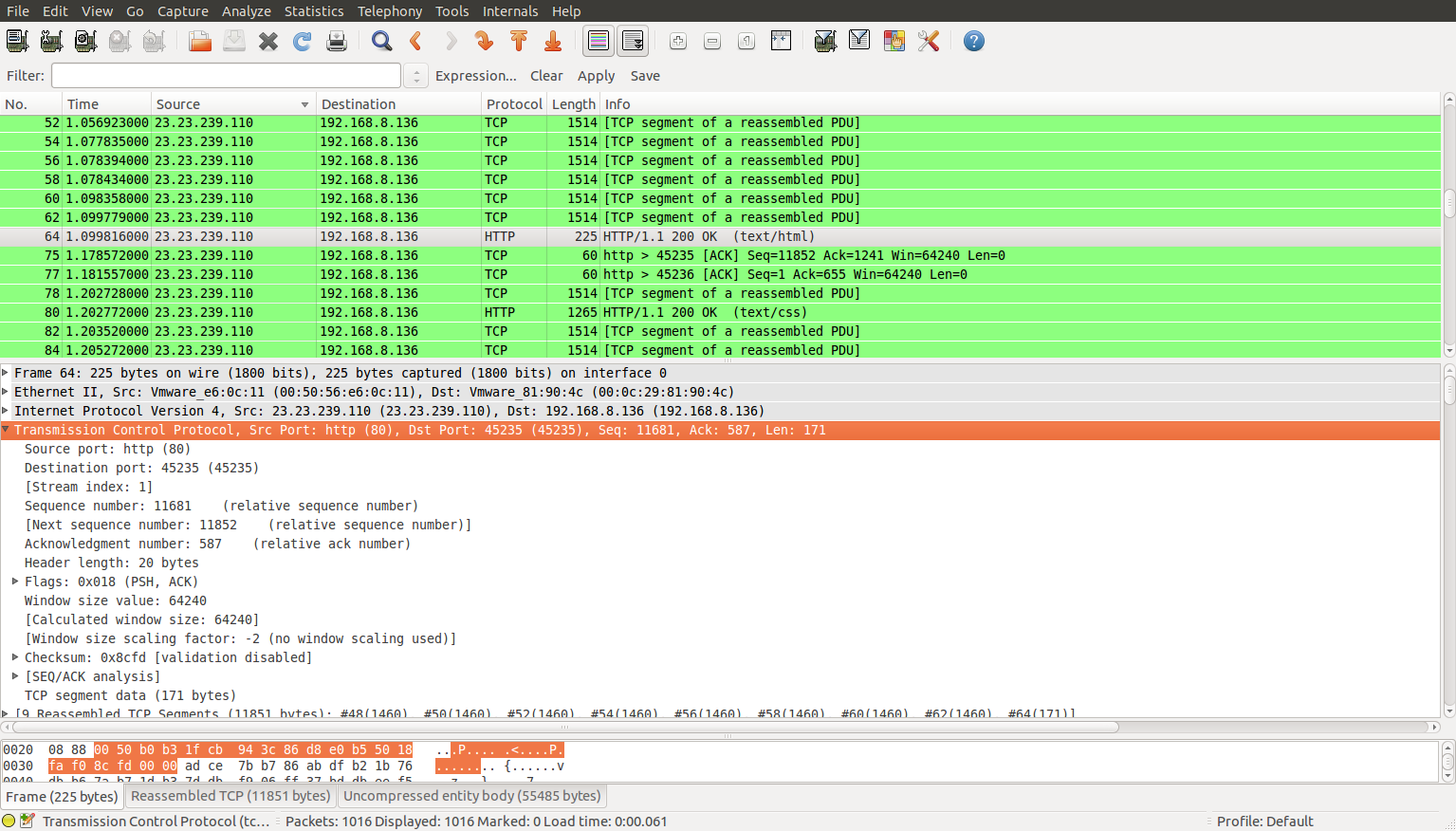
4) In the trace you can see many protocols listed. There is a lot going on under the hood (Ed. better word is bonnet). Some of these protocols are called transport protocols. Which transport protocol is used between your machine and the web server? Why would you think this one is used instead of an alternative? You will see that other protocols are captured in your trace. One such protocol is HTTP. What is the relationship between the transport protocol you identified and HTTP? Both protocols are used to satisfy your browser’s request for a web page. Why is more than one protocol used?

The following figures show the protocols used in http request and DNS request. Apparently protocols are used in a hierarchy way. What’s more, at the transport layer of DNS, it is using UDP, while http is using TCP in the transport layer.





5) In the trace you will find IP addresses within the packets. Find an example packet in the trace where the IP address associated with your machine is present. Provide this example packet with your submission (take a screen dump or cut and past the packet). Why is the IP address present in the particular packet you selected (what purpose does it serve)? How are IP addresses and port numbers used, to address what specifically?



From this screenshot you can see that this is the packet of receiving a http response. My machine address should be the destination address, with port number 45235 (probably chosen by my browser). While the server address is 23.23.239.110, with port number 80 (which is the usual port number for http request).

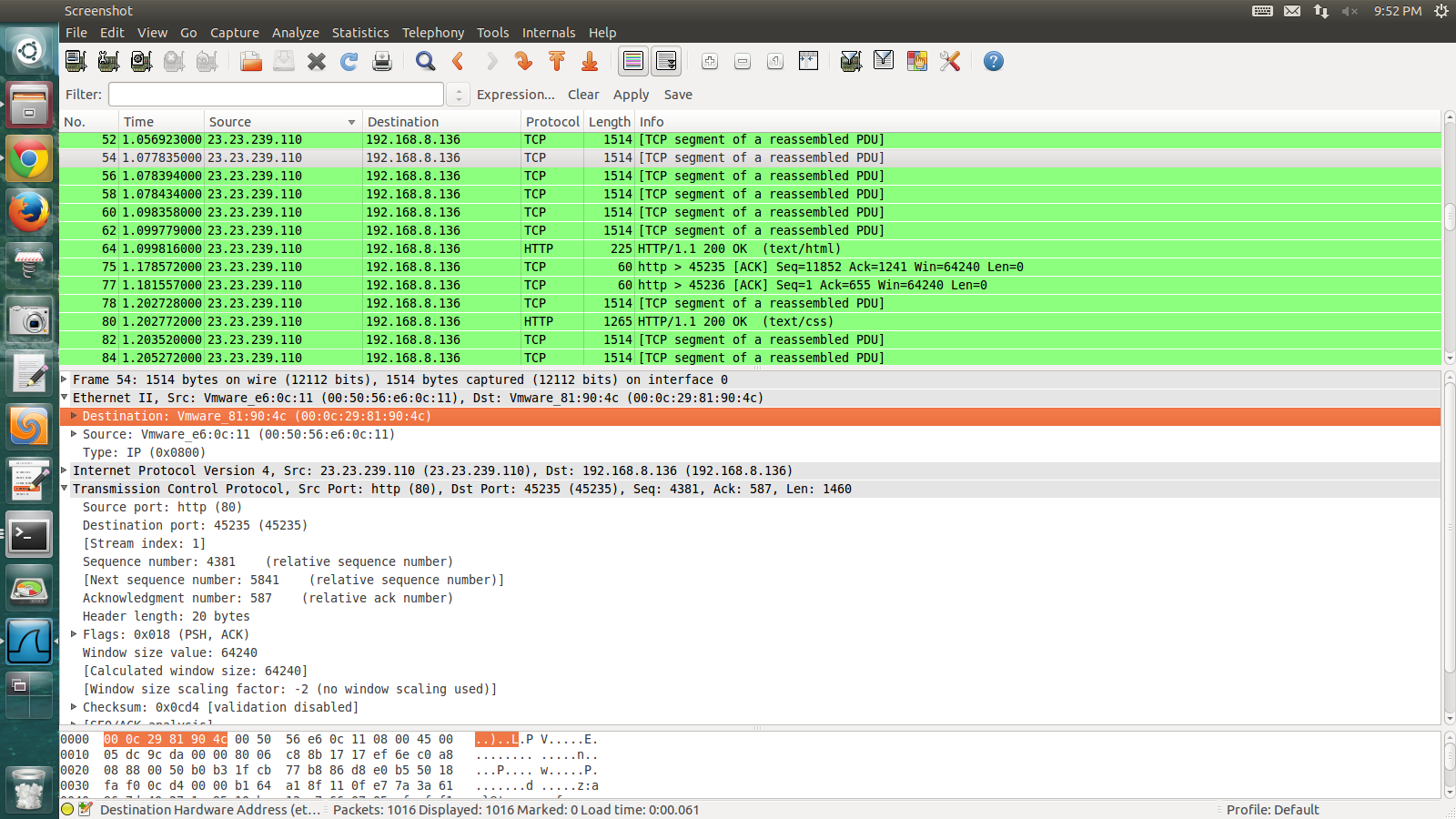
6) We discussed protocol layers in class. Which layer is the IP associated with and why isnt it associated with say the application layer? (sounds like a tricky question but why is routing at the layer it is at and not another, say, higher layer).

Network layer is associated. Because that’s how network stack is designed.

7) We have not discussed the MAC (medium access control) address in class yet. But you can find the MAC address of your machine using ifconfig on unix, Linux, windows, and OSX machines - at the command line. (Why not read the manual pages on ifconfig - a very handy command). Each node has a unique Link Layer MAC address. Can you find the MAC address for your machine in the trace. What is the MAC address of your machine? Provide a trace of the packet in which you found it (take a screen dump or cut and past the packet). Why do you think a MAC address is needed given that your machine has an IP address (it would be more precise to say that the IP address is associated with one of the network interfaces on your machine, this is true also of the MAC address).

HWaddr 00:0c:29:81:90:4c, you can observe from both following figures, in terminal or wireshark.

Because IP address basically tells us the location of the machine, but not telling us which machine it is. Theoretically unique to one machine.



8) There are an large number of protocols found in the trace - many you are not familiar with. Also, you maybe surprised at the large number of packets are being transmitted - even when your machine is idle, i.e., not doing any application layer work. Consider the short trace you just captured. You will see many different protocols listed in the trace. Excluding the HTTP and TCP protocols identify as many of the other protocols as you can. Choose a couple of these protocols from your list and describe in more detail what they are and what are they being used to support. You can use google here or go to the IETF site for more information on the Internet protocols - there are many. Recall a protocol is the core of a layer that provides a service to a higher layer try and determine what the services are for the two protocols you select from your list. Search to see if you can find an RFC for any of the protocols within your trace (one example RFC database is: <http://www.rfc-editor.org/rfc.html>). Can you find the RFCs for the two protocol selected from your trace. Dig into the RFC is there a state machine? Furthermore, do a little research and find out more about the RFC process, what role does the RFC process perform? How does it work? OK we are done. Great job! You learnt a lot.

DNS protocol, there are a lot of related RFC for DNS protocol. From this search page (<http://www.rfc-editor.org/search/rfc_search_detail.php?title=dns&pubstatus%5B%5D=Any&pub_date_type=any>), we know that the very first one is Jan 1986, written by C. Patridge, with RFC 974.

TLS v1.1, The version 1.1 of transport layer security protocol is proposed on Apr 2006.

The RFC, known as Request For Comments, acts as the role of documenting and approval of internet standards.