**Part 1**

• The ARP traffic

o Which frame numbers contain the request and response?

**Frame 1 contained the request and frame 2 contained the response.**

o What is the IP address being requested?

**The IP address that is being requested is: 192.168.94.2**

o What protocol layers are involved (and why)?

**The protocol layers that are involved are:**

* **The Data Link Layer as it sends packets to MAC addresses, which is a protocol used in this layer.**
* **The Network Layer as it uses an IP address.**

o Why was only one ARP request required when there are multiple hosts?

**Only one ARP request was required because it sent the request to all of the hosts in the network, which caused the host that matched the IP address to respond back to the client.**

• The DNS traffic

o Explain what information is contained in each frame (just summarize at a very high level - a few words are fine).

**The information that is contained in each frame is the domain name and response of the domain name.**

o What is the hostname being looked up and its IP address?

**The hostname is: robust.cs.utep.edu.**

**The IP address is: 192.168.94.152**

o What protocol layers are involved (and why)?

**The Transport layer is involved as it uses the TCP or UDP protocol.**

• The HTTP traffic

o What URL is being requested?

**The URL that is being requested is:** [**http://robust.cs.utep.edu/~freudent/test.html**](http://robust.cs.utep.edu/~freudent/test.html)

o What protocol layers are involved (and why)?

**The protocol layers that are involved are:**

* **The Physical Layer as traffic has to flow between ethernet, wireless, fiber, or other physical connections.**
* **The Data Link Layer as it defines a protocol for interpreting the signals that pass through the physical connection.**
* **The Network layer as it connects different networks together by using routers.**
* **The Transport Layer figures out where the information needs to go once it is in the node.**
* **The Application Layer as HTTP allows applications to communicate over the network.**

o Which frames contain messages related to establishing and closing the connection used for the HTTP traffic?

**The frames are 13,14, and 16**

o What is the server's IP address and port?

**The server’s IP address and port are: 129.108.18.226 Port: 80**

o What is the server's ISN?

**The server’s ISN is 1**

o What is the client's IP address and port?

**192.168.94.152 Port: 80**

o What is the client's ISN?

**The client’s ISN is 1**

o Which frames contain

▪ The HTTP request

**Frame 10 contains the HTTP Request**

▪ HTTP ACK

**Frame 11 contains the HTTP ACK**

▪ HTTP headers

**Frame 12 contains the HTTP headers**

▪ HTTP response

**Frame 12 also contains the HTTP Response**

**Part 2**

Use wireshark to capture the interaction between your browser and the result of clicking on the “course schedule” tab of http://www.cs.utep.edu/cs/ web page. Examine this trace. Explain how HTTP is encapsulated within TCP and IP.

**The way HTTP is encapsulated within TCP and IP is by using protocols that abstract away the implementation details from the layers below it by information hiding or inclusion. HTTP is encapsulated in the TCP and IP header in the internet protocol.**

Was the trace that you captured more difficult to analyze than the provided one? Why?

**The captured trace was more difficult to analyze than the provided one as there were considerably more frames to analyze. Also, the information that is provided about each frame is somewhat cryptic, which makes it more difficult to analyze the information in the capture.**

A screenshot of a computer

Description automatically generated