The ARP traffic

- **Which frame numbers contain the request and response?**
  - Request: frame 1
  - Response: frame 2
- **What is the IP address being requested?**
  - 192.168.94.152
- **What protocol layers are involved (and why) ?**
  - eth:ethertype:arp
- **Why was only one ARP request required when there are multiple hosts?**
  - Because the request was a broadcast, therefore everybody on the network received it, and the intended destination replied directly.

The DNS traffic

- **Explain what information is contained in each frame (just summarize at a very high level a few words are fine).**
  - A host in Vmware is requesting an IPv6 address from the robust.cs.utep.edu network.
- **What is the host name being looked up and its IP address?**
  - Robust.cs.utep.edu
  - 192.168.94.152
- **What protocol layers are involved (and why)?**
  - UDP

The HTTP traffic

- **What URL is being requested?**
  - http://robust.cs.utep.edu/~freudent/test.html
- **What protocol layers are involved (and why)?**
  - TCP
  - There needs to be a constant connection between the host and the website.
- **Which frames contain messages related to establishing and closing the connection used for the HTTP traffic?**
  - Frames 10 & 12
- **What is the server's IP address and port?**
  - IP Address: 192.168.94.152
  - Port: 51562
- **What is the server's ISN?**
  - 1
- **What is the client's IP address and port?**
  - IP Address: 192.108.18.126
  - Port: 80
- **What is the client's ISN?**
  - 1
- **Which frames contain**
  - **The HTTP request**
    - 10
  - **HTTP ACK**
    - 10 & 12
  - **HTTP headers**
    - 10 & 12
  - **HTTP response**
    - 12

Tracing own interaction

- My own interaction had a considerably bigger amount of DNS, HTTP, TLSv1.2, TLSv1.3 and TCP protocols only when accessing the CS web page, *cs.utep.edu.*

- All HTTP requests were images or information in the form of text.

- DNS translated all the web pages into IP addresses that my machine could refer to in the event that I wanted to visit such sites (Facebook, Linkedin, Twitter, and other UTEP sites). By sorting the entries by protocol, we can see that all requests had an answer, yet some were not immediately answered (e.g., No. 1131 was a standard query request that was not answered until record No. 1141; while record No. 161 had its request answered in record No. 162 (AccessToCSSite file).

- What the TCP does (in a nutshell) is request a web page, and the server returns the web page in pieces (amount of "pieces" depend on the site), and the requesting machine puts all those packets together to obtain the whole web page. In my interaction accessing the courses web page, there were a ton of records with TCP protocols, but there was one that was highlighted in red: record No. 114, linked to record No. 90.
  - Record No. 90 has the 'acknowledgment' bit set to 1.
  - Record No. 114 has the 'reset' bit set to 1.

- I did a little bit of research concerning the TLSv1.2 protocol, and all the records with this protocol contain "Application data", or fragments of data; which I'd like to say is information traveling on a secured layer, maybe not sensitive data, but data that has higher priority that "regular" data, or data that does not compromise either the health of the server or my machine.

- The TLSv1.3 protocol was also encountered in my interaction, which were some "Hello" from my machine, and from the server, as well as "Application Data" or fragments of data being requested and sent.

- My captures were harder to analyze than the one provided for several reasons:
  - They have more than 500 packets (AccessToCSSiteCourseSchedule)
    - AccessToCSSite has 1630
  - They included the TLSv1.2 and TLSv1.3 protocols.
  - It was interesting to see that there were no packets with ARP protocol.