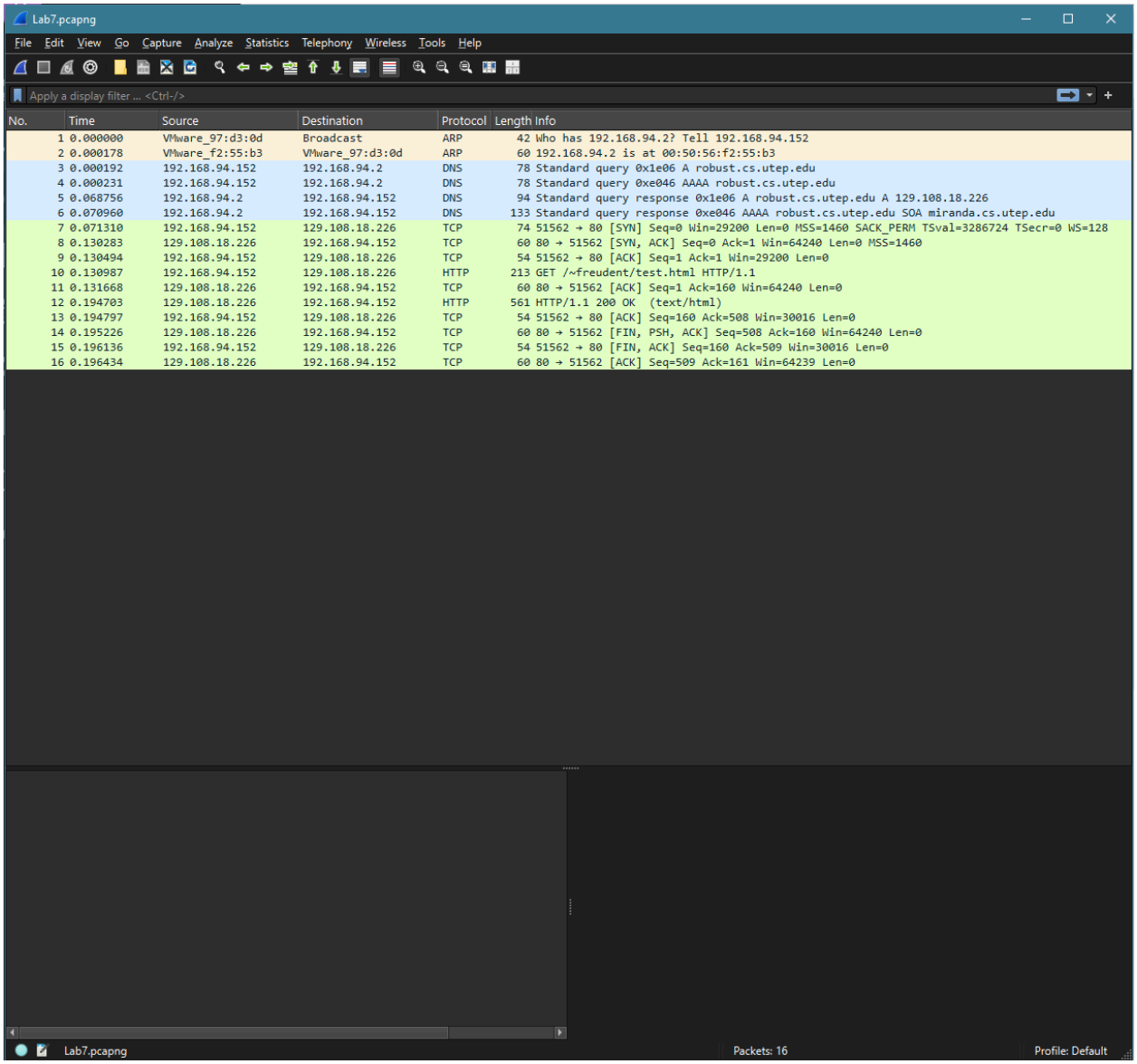
Samantha Jackson
CSCI4406_Lab7
10-15-2024

Lab 7 - Traffic Analysis Using Wireshark

Opening “Lab7.pcapng” in Wireshark

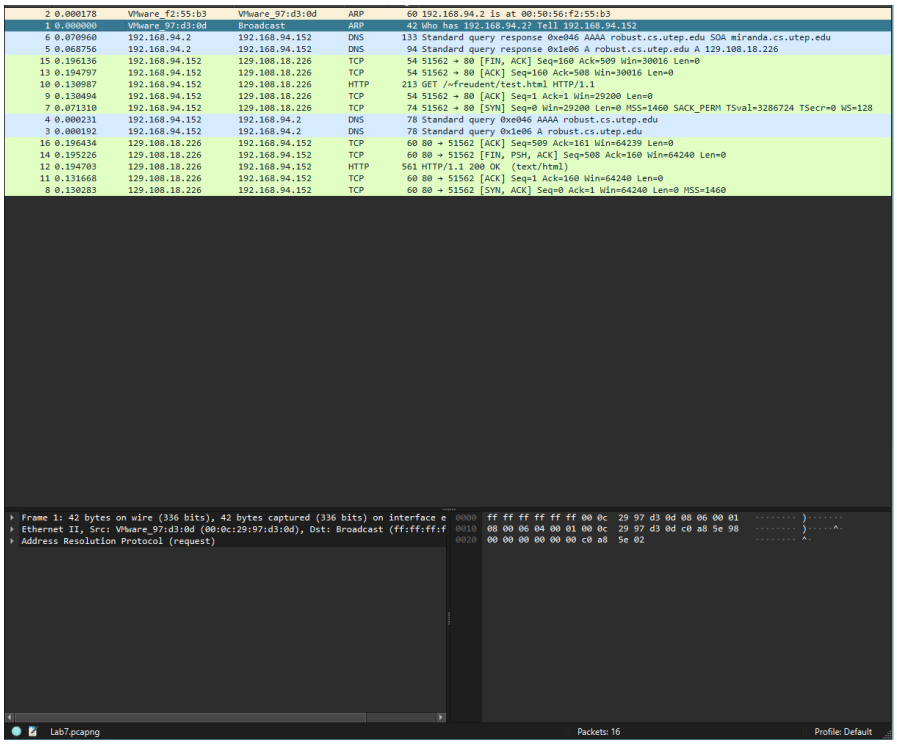
Observations/Issues: None. File downloaded and opened in Wireshark without issue.



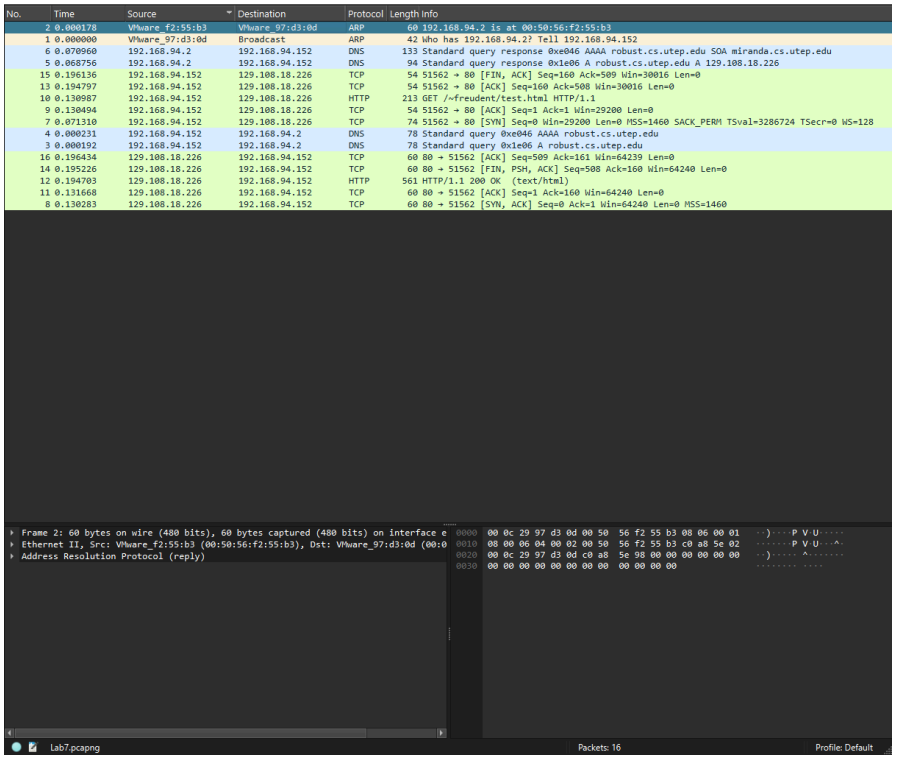
ARP Traffic

The frame numbers that contain the requests and response

Request: Frame 1



Response/Reply: Frame 2



The IP address being requested is 192.168.94.2 which can be found in the info on frame 1.

```
1 0.000000      VMware_97:d3:0d      Broadcast           ARP         42 Who has 192.168.94.2? Tell 192.168.94.152
```

The protocol layer involved is ARP (0x0806) or Address Resolution Protocol which is used typically for mapping an IP address to an Ethernet address. This involves dynamically discovering the mapping between layer 3 (network/protocol) and layer 2 (data link/hardware).

We can assume the ARP was generated to limit network traffic as it specifies an IP address to assign to an underlying Ethernet address.

```
▾ Ethernet II, Src: VMware_97:d3:0d (00:0c:29:97:d3:0d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: VMware_97:d3:0d (00:0c:29:97:d3:0d)
    Type: ARP (0x0806)
    [Stream index: 0]
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: VMware_97:d3:0d (00:0c:29:97:d3:0d)
    Sender IP address: 192.168.94.152
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.94.2
```

```
▾ Ethernet II, Src: VMware_f2:55:b3 (00:50:56:f2:55:b3), Dst: VMware_97:d3:0d (00:0c:29:97:d3:0d)
  ▸ Destination: VMware_97:d3:0d (00:0c:29:97:d3:0d)
  ▸ Source: VMware_f2:55:b3 (00:50:56:f2:55:b3)
    Type: ARP (0x0806)
    [Stream index: 1]
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: VMware_f2:55:b3 (00:50:56:f2:55:b3)
    Sender IP address: 192.168.94.2
    Target MAC address: VMware_97:d3:0d (00:0c:29:97:d3:0d)
    Target IP address: 192.168.94.152
```

DNS Traffic

Frames 3-4 requests two standard queries and Frame 5-6 respond to these standard queries with a response.

Frame number 3: Contains a Standard query 0x1e06 A robust.cs.utep.edu
Frame number 4: Contains a Standard query 0xe046 AAAA robust.cs.utep.edu
Frame number 5: Contains a Standard query response for Frame number 3 returning “A 129.108.18.226”
Frame number 6: Contains a Standard query response for Frame number 4 returning “SOA miranda.cs.utep.edu”

```
Standard query 0x1e06 A robust.cs.utep.edu
Standard query 0xe046 AAAA robust.cs.utep.edu
Standard query response 0x1e06 A robust.cs.utep.edu A 129.108.18.226
Standard query response 0xe046 AAAA robust.cs.utep.edu SOA miranda.cs.utep.edu
```

The hostname being looked up is *robust.cs.utep.edu* which is a host address and its IP is *192.168.94.2*

Destination
Broadcast
VMware_97:d3:0d
192.168.94.2
192.168.94.2
192.168.94.152
192.168.94.152
129.108.18.226
192.168.94.152
129.108.18.226
129.108.18.226
192.168.94.152
192.168.94.152
129.108.18.226
192.168.94.152
129.108.18.226
192.168.94.152

DNS protocol is part of the Application Layer (Layer 7) and Transport Layer protocol (Layer 4). Layer 7 deals with the human-computer interaction layer where applications can access network services. Layer 4 deals with time-sensitive transmissions related to DNS lookups (UDP). In this instance with the hostname *robust.cs.utpe.edu*. As it converts the domain name into an IP address.

```
▾ User Datagram Protocol, Src Port: 53, Dst Port: 37298
    Source Port: 53
    Destination Port: 37298
    Length: 60
    Checksum: 0xb5b1 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 3]
  ▸ [Timestamps]
    UDP payload (52 bytes)
```

We can assume the reason the ARP was generated to make communication possible with the hostname as it maps the hostname's IP to a MAC address. Since the host's IP address is known the ARP simply seeks to resolve the MAC address of this host.

HTTPS Traffic

The URL being requested is /~freudent/test.html (https://robust.cs.utep.edu/~freudent/test.html).

```
▾ Hypertext Transfer Protocol
  ▸ GET /~freudent/test.html HTTP/1.1\r\n
    User-Agent: Wget/1.17.1 (linux-gnu)\r\n
    Accept: */*\r\n
    Accept-Encoding: identity\r\n
    Host: robust.cs.utep.edu\r\n
    Connection: Close\r\n
    \r\n
    [Response in frame: 12]
    [Full request URI: http://robust.cs.utep.edu/~freudent/test.html]
```

HTTP protocol is involved with the Application Layer (Layer 7). This deals with the human-computer interaction layer where applications can access network services. In this instance the request is to send data between a web browser and a website. TCP protocol is involved with the Transport Layer (Layer 4) which is a connection oriented protocol which is used by HTTP. TCP is ultimately more reliable and robust than UDP.

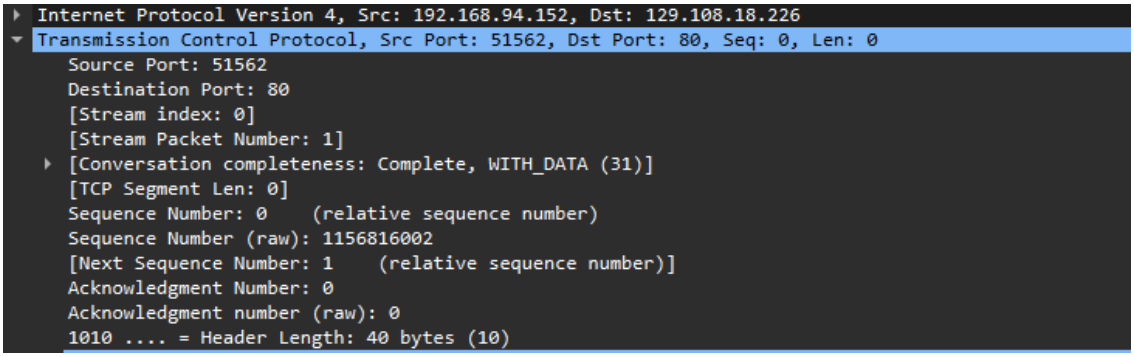
Which frames contain messages related to establishing and closing a transport used for the HTTP traffic?

- In the case of the server the SYN-ACK packet at frame 8 contains the following addresses:
  - IP Address: *Src (129.108.18.226) Dst (192.168.94.152)*
  - Port: *Src Port (80) Dst Port (51562)*
  - Initial Sequence Number: *885024273*

```
▸ Internet Protocol Version 4, Src: 129.108.18.226, Dst: 192.168.94.152
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 51562, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 51562
    [Stream index: 0]
    [Stream Packet Number: 2]
  ▸ [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 885024273
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1156816003
    0110 .... = Header Length: 24 bytes (6)
```

- In the case of the client the SYN packet at frame 7 contains the following addresses:
  - IP Address: *Src (192.168.94.152) Dst (129.108.18.226)*
  - Port: *Src Port (51562) Dst Port (80)*

- Initial Sequence Number: *1156816002*



Which frames contain

- The HTTP request: Frame 10
- HTTP ACK (Acknowledgement): Frame 9, 11, 13, 16
    - SYN, ACK: Frame 8
    - FIN, PSH, ACK: Frame 14
    - FIN, ACK: Frame 15
- HTTP headers: Frame 10, 12 (Headers are contained in request and response frames)
- HTTP response: Frame 12

This lab is very interesting. I feel like I learned a lot about the protocols in Wireshark and how the layer system works in practice. Especially how to interpret those protocols. This makes me want to learn more about Wireshark because of its utility in a wide array of circumstances for network analysis. The detailing of protocols gives the user a good idea as to what each frame of data is doing and what that says about the network traffic as a whole. It's incredibly verbose and exact in its description. This can be used to great effect in identify attack signatures and network performance.