Lab 7

Wireshark – arp, dns, http request/reponses

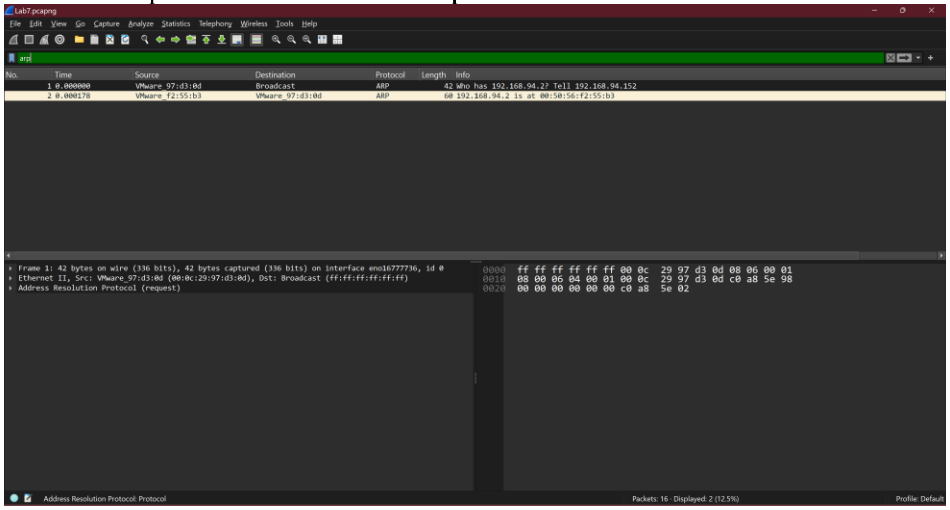
Joshua Ludolf

The traffic in the attached file includes arp, dns, and http requests and responses.

Your task: determine (using text and screenshots):

- for the ARP traffic
  - which frame numbers contain the request and response

    We have 2 packets related to ARP packets 1 & 2.


Lab7.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
No.  Time        Source             Destination        Protocol  Length  Info
   1 0.000000    VMware_97:d3:0d    Broadcast          ARP       42      Who has 192.168.94.2? Tell 192.168.94.152
   2 0.000178    VMware_f2:55:b3    VMware_97:d3:0d    ARP       60      192.168.94.2 is at 00:50:56:f2:55:b3
```

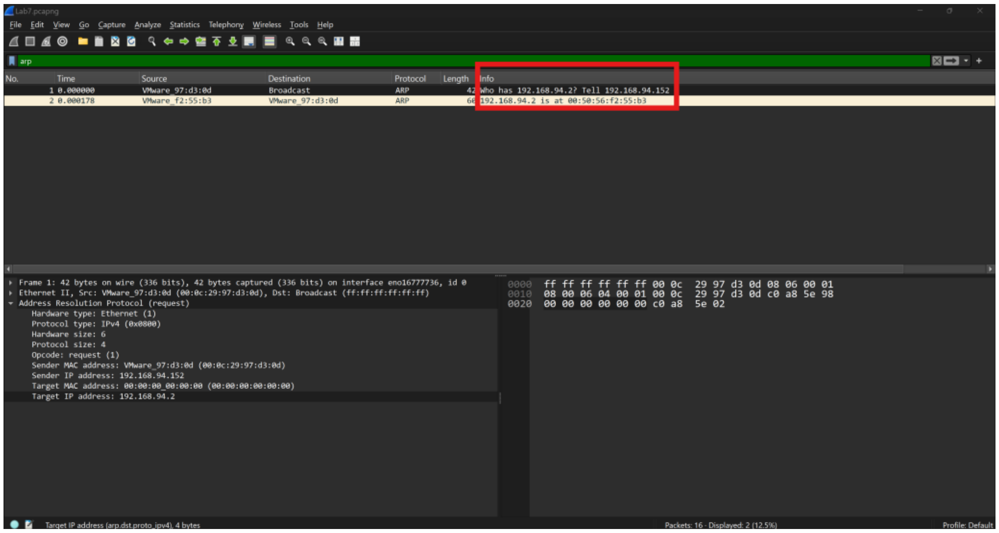
```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eno16777736, id 0
▸ Ethernet II, Src: VMware_97:d3:0d (00:0c:29:97:d3:0d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 0c  29 97 d3 0d 08 06 00 01
0010  08 00 06 04 00 01 00 0c  29 97 d3 0d c0 a8 5e 98
0020  00 00 00 00 00 00 c0 a8  5e 02
```

Address Resolution Protocol: Protocol
Packets: 16 · Displayed: 2 (12.5%)
Profile: Default

  - the ip address being requested

    192.168.94.2


Lab7.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

```
No.  Time        Source             Destination        Protocol  Length  Info
   1 0.000000    VMware_97:d3:0d    Broadcast          ARP       42      Who has 192.168.94.2? Tell 192.168.94.152
   2 0.000178    VMware_f2:55:b3    VMware_97:d3:0d    ARP       60      192.168.94.2 is at 00:50:56:f2:55:b3
```

```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eno16777736, id 0
▸ Ethernet II, Src: VMware_97:d3:0d (00:0c:29:97:d3:0d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▾ 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
```

```
0000  ff ff ff ff ff ff 00 0c  29 97 d3 0d 08 06 00 01
0010  08 00 06 04 00 01 00 0c  29 97 d3 0d c0 a8 5e 98
0020  00 00 00 00 00 00 c0 a8  5e 02
```

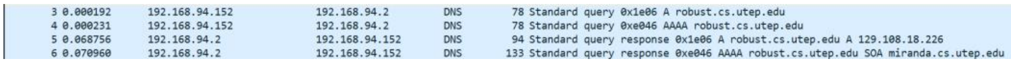
Target IP address (arp.dst.proto_ipv4), 4 bytes
Packets: 16 · Displayed: 2 (12.5%)
Profile: Default

  - which (name) protocol layers are involved (and why)

    Layer 2 and Layer 3 are involved because layer 2 has the MAC address and layer 3 has the IP address.
  - a conjecture about why the ARP was generated

    The ARP broadcasting message is usually generated when the local hub or switch (VMWare) has a packet with an unknown destination physical address. The hub/switch will send a broadcasting message to everyone and will wait for response to eventually send destination packet/frame to the unknown physical address.

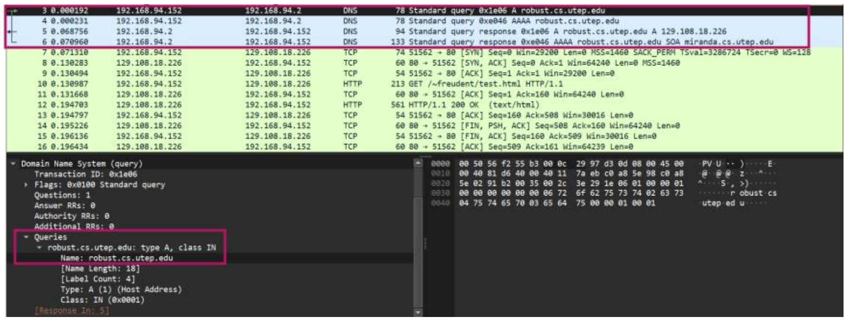
- The DNS traffic
  - what frame numbers contain what information (just summarize at a very high level - a few words are fine)
    - ❖ Frame 3 & 4 contains a query to robust.cs.utep.edu
    - ❖ Frame 5 & 6 contains a response from robust.c.utep.edu



```
3 0.000192   192.168.94.152   192.168.94.2     DNS    78 Standard query 0x1e06 A robust.cs.utep.edu
4 0.000231   192.168.94.152   192.168.94.2     DNS    78 Standard query 0xe046 AAAA robust.cs.utep.edu
5 0.068756   192.168.94.2     192.168.94.152   DNS    94 Standard query response 0x1e06 A robust.cs.utep.edu A 129.108.18.226
6 0.070960   192.168.94.2     192.168.94.152   DNS   133 Standard query response 0xe046 AAAA robust.cs.utep.edu SOA miranda.cs.utep.edu
```

  - the hostname being looked up and its ip addr

    The hostname is robust.cs.tep.edu and the IP address that responded was 192.168.94.152.



```
 3 0.000192   192.168.94.152   192.168.94.2     DNS    78 Standard query 0x1e06 A robust.cs.utep.edu
 4 0.000231   192.168.94.152   192.168.94.2     DNS    78 Standard query 0xe046 AAAA robust.cs.utep.edu
 5 0.068756   192.168.94.2     192.168.94.152   DNS    94 Standard query response 0x1e06 A robust.cs.utep.edu A 129.108.18.226
 6 0.070960   192.168.94.2     192.168.94.152   DNS   133 Standard query response 0xe046 AAAA robust.cs.utep.edu SOA miranda.cs.utep.edu
 7 0.071310   192.168.94.152   129.108.18.226   TCP    74 51562 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=3286724 TSecr=0 WS=128
 8 0.130283   129.108.18.226   192.168.94.152   TCP    60 80 → 51562 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 9 0.130494   192.168.94.152   129.108.18.226   TCP    54 51562 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
10 0.130987   192.168.94.152   129.108.18.226   HTTP  213 GET /~freudent/test.html HTTP/1.1
11 0.131668   129.108.18.226   192.168.94.152   TCP    60 80 → 51562 [ACK] Seq=1 Ack=160 Win=64240 Len=0
12 0.194703   129.108.18.226   192.168.94.152   HTTP  561 HTTP/1.1 200 OK  (text/html)
13 0.194797   192.168.94.152   129.108.18.226   TCP    54 51562 → 80 [ACK] Seq=160 Ack=508 Win=30016 Len=0
14 0.195226   129.108.18.226   192.168.94.152   TCP    60 80 → 51562 [FIN, PSH, ACK] Seq=508 Ack=160 Win=64240 Len=0
15 0.196136   192.168.94.152   129.108.18.226   TCP    54 51562 → 80 [FIN, ACK] Seq=160 Ack=509 Win=30016 Len=0
16 0.196434   129.108.18.226   192.168.94.152   TCP    60 80 → 51562 [ACK] Seq=509 Ack=161 Win=64239 Len=0
```

```
Domain Name System (query)
    Transaction ID: 0x1e06
  Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    robust.cs.utep.edu: type A, class IN
        Name: robust.cs.utep.edu
        [Name Length: 18]
        [Label Count: 4]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  [Response In: 5]
```

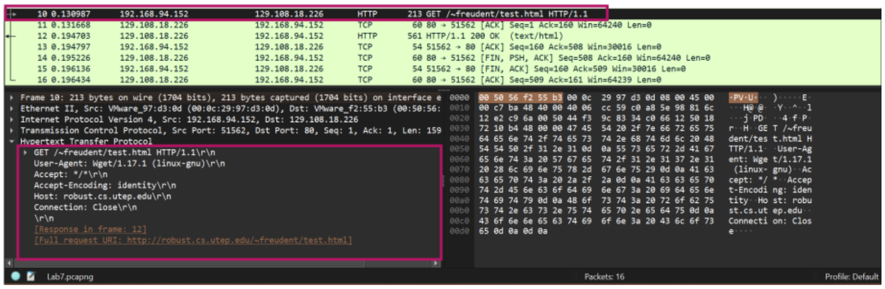
```
0000  00 50 56 f2 55 b3 00 0c  29 97 d3 0d 08 00 45 00   ·PV·U·· )·····E·
0010  00 40 81 d6 40 00 40 11  7a eb c0 a8 5e 98 c0 a8   ·@··@·@· z···^···
0020  5e 02 91 b2 00 35 00 2c  3e 29 1e 06 01 00 00 01   ^····5·, >)······
0030  00 00 00 00 00 00 06 72  6f 62 75 73 74 02 63 73   ·······r obust·cs
0040  04 75 74 65 70 03 65 64  75 00 00 01 00 01         ·utep·ed u·····
```

  - which protocol layers are involved (and why)
    - ❖ Data Link Layer (Ethernet): For physical addressing
    - ❖ Network Layer (IP): For logical addressing
    - ❖ Transport Layer (UDP): DNS typically uses UDP
    - ❖ Application Layer (DNS): For name resolution
  - Is there any information present in traffic that you might use to confirm the reason the ARP you already examined was generated?

    Yes, the DNS query to robust.cs.utep.edu (192.168.94.2) likely triggered the ARP request to resolve the gateway's MAC address.

- The http traffic
  - What URL is being requested?

    http://robust.cs.utep.edu/~freudent/test.html



```
10 0.130987  192.168.94.152   129.108.18.226   HTTP   213 GET /~freudent/test.html HTTP/1.1
11 0.131668  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [ACK] Seq=1 Ack=160 Win=64240 Len=0
12 0.194703  129.108.18.226   192.168.94.152   HTTP   561 HTTP/1.1 200 OK  (text/html)
13 0.194797  192.168.94.152   129.108.18.226   TCP     54 51562 → 80 [ACK] Seq=160 Ack=508 Win=30016 Len=0
14 0.195226  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [FIN, PSH, ACK] Seq=508 Ack=160 Win=64240 Len=0
15 0.196136  192.168.94.152   129.108.18.226   TCP     54 51562 → 80 [FIN, ACK] Seq=160 Ack=509 Win=30016 Len=0
16 0.196434  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [ACK] Seq=509 Ack=161 Win=64239 Len=0
```

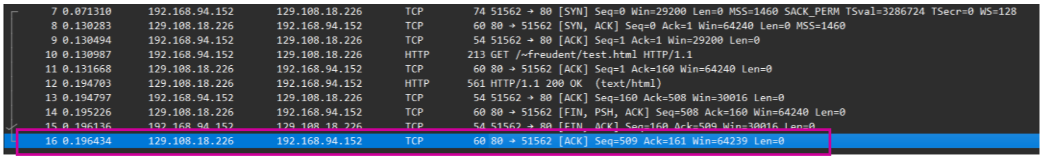
```
▸ Frame 10: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) on interface e
▸ Ethernet II, Src: VMware_97:d3:0d (00:0c:29:97:d3:0d), Dst: VMware_f2:55:b3 (00:50:56:
▸ Internet Protocol Version 4, Src: 192.168.94.152, Dst: 129.108.18.226
▸ Transmission Control Protocol, Src Port: 51562, Dst Port: 80, Seq: 1, Ack: 1, Len: 159
▾ 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]
```

```
0000  00 50 56 f2 55 b3 00 0c  29 97 d3 0d 08 00 45 00   ·PV·U··· )·····E·
0010  00 c7 ba 48 40 00 40 06  cc 59 c0 a8 5e 98 81 6c   ···H@·@· ·Y··^··l
0020  12 e2 c9 6a 00 50 44 f3  9c 83 34 c0 66 12 50 18   ···j·PD· ··4·f·P·
0030  72 10 b4 48 00 00 47 45  54 20 2f 7e 66 72 65 75   r··H··GE T /~freu
0040  64 65 6e 74 2f 74 65 73  74 2e 68 74 6d 6c 20 48   dent/tes t.html H
0050  54 54 50 2f 31 2e 31 0d  0a 55 73 65 72 2d 41 67   TTP/1.1· ·User-Ag
0060  65 6e 74 3a 20 57 67 65  74 2f 31 2e 31 37 2e 31   ent: Wge t/1.17.1
0070  20 28 6c 69 6e 75 78 2d  67 6e 75 29 0d 0a 41 63    (linux- gnu)··Ac
0080  63 65 70 74 3a 20 2a 2f  2a 0d 0a 41 63 63 65 70   cept: */ *··Accep
0090  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 69 64 65 6e   t-Encodi ng: iden
00a0  74 69 74 79 0d 0a 48 6f  73 74 3a 20 72 6f 62 75   tity··Ho st: robu
00b0  73 74 2e 63 73 2e 75 74  65 70 2e 65 64 75 0d 0a   st.cs.ut ep.edu··
00c0  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 43 6c 6f 73   Connecti on: Clos
00d0  65 0d 0a 0d 0a                                     e····
```

Lab7.pcapng   Packets: 16   Profile: Default

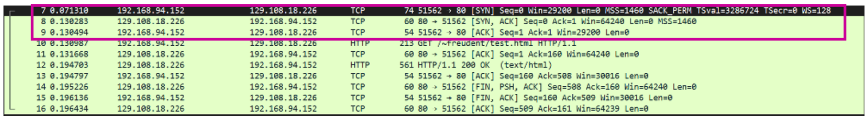
- What protocol layers are involved (and why)

    - Data Link Layer (Ethernet): For physical addressing
    - Network Layer (IP): For logical addressing
    - Transport Layer (TCP): For reliable data transfer
    - Application Layer (HTTP): For web communication



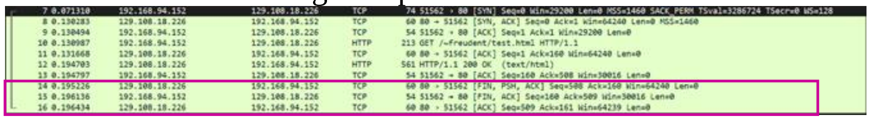
```
 7 0.071310  192.168.94.152   129.108.18.226   TCP     74 51562 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=3286724 TSecr=0 WS=128
 8 0.130283  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 9 0.130494  192.168.94.152   129.108.18.226   TCP     54 51562 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
10 0.130987  192.168.94.152   129.108.18.226   HTTP   213 GET /~freudent/test.html HTTP/1.1
11 0.131668  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [ACK] Seq=1 Ack=160 Win=64240 Len=0
12 0.194703  129.108.18.226   192.168.94.152   HTTP   561 HTTP/1.1 200 OK  (text/html)
13 0.194797  192.168.94.152   129.108.18.226   TCP     54 51562 → 80 [ACK] Seq=160 Ack=508 Win=30016 Len=0
14 0.195226  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [FIN, PSH, ACK] Seq=508 Ack=160 Win=64240 Len=0
15 0.196136  192.168.94.152   129.108.18.226   TCP     54 51562 → 80 [FIN, ACK] Seq=160 Ack=509 Win=30016 Len=0
16 0.196434  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [ACK] Seq=509 Ack=161 Win=64239 Len=0
```

- Which frames contain messages related to establishing and closing a transport used for the http traffic?
    - for the server
        - Frames 7-9 for establishing transport



```
 7 0.071310  192.168.94.152   129.108.18.226   TCP     74 51562 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=3286724 TSecr=0 WS=128
 8 0.130283  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 9 0.130494  192.168.94.152   129.108.18.226   TCP     54 51562 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
10 0.130987  192.168.94.152   129.108.18.226   HTTP   213 GET /~freudent/test.html HTTP/1.1
11 0.131668  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [ACK] Seq=1 Ack=160 Win=64240 Len=0
12 0.194703  129.108.18.226   192.168.94.152   HTTP   561 HTTP/1.1 200 OK  (text/html)
13 0.194797  192.168.94.152   129.108.18.226   TCP     54 51562 → 80 [ACK] Seq=160 Ack=508 Win=30016 Len=0
14 0.195226  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [FIN, PSH, ACK] Seq=508 Ack=160 Win=64240 Len=0
15 0.196136  192.168.94.152   129.108.18.226   TCP     54 51562 → 80 [FIN, ACK] Seq=160 Ack=509 Win=30016 Len=0
16 0.196434  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [ACK] Seq=509 Ack=161 Win=64239 Len=0
```

        - Frames 14-16 for closing transport



```
 7 0.071310  192.168.94.152   129.108.18.226   TCP     74 51562 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=3286724 TSecr=0 WS=128
 8 0.130283  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 9 0.130494  192.168.94.152   129.108.18.226   TCP     54 51562 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
10 0.130987  192.168.94.152   129.108.18.226   HTTP   213 GET /~freudent/test.html HTTP/1.1
11 0.131668  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [ACK] Seq=1 Ack=160 Win=64240 Len=0
12 0.194703  129.108.18.226   192.168.94.152   HTTP   561 HTTP/1.1 200 OK  (text/html)
13 0.194797  192.168.94.152   129.108.18.226   TCP     54 51562 → 80 [ACK] Seq=160 Ack=508 Win=30016 Len=0
14 0.195226  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [FIN, PSH, ACK] Seq=508 Ack=160 Win=64240 Len=0
15 0.196136  192.168.94.152   129.108.18.226   TCP     54 51562 → 80 [FIN, ACK] Seq=160 Ack=509 Win=30016 Len=0
16 0.196434  129.108.18.226   192.168.94.152   TCP     60 80 → 51562 [ACK] Seq=509 Ack=161 Win=64239 Len=0
```

        - ip addr
          129.108.18.226
        - port
          80
        - initial sequence number
          0
    - for the client
        - ip addr
          192.168.94.152
        - port
          51562
        - initial sequence number
          508
- Which frames contain
    - The HTTP request

Frame 10

- HTTP ACK

Frame 11

- HTTP headers

Frame 12

- HTTP response

Frame 13