Richard Moot
CS372
June 16, 2016

Lab 5

1. a4:5e:60:e9:58:ab
2. 38:2c:4a:9a:a6:20; This is actually my router's Ethernet address.
3. 0x0800 which indicates that it is the IP Protocol.
4. 66 bytes from the start.
5. 0x0d 0x0a 0x0d 0x0a
6. 38:2c:4a:9a:a6:20; The destination is my router.
7. a4:5e:60:e9:58:ab; My computer' card.
8. 0x0800; Signifies the IP Protocol frame.
9. 78 bytes until the OK starts.
10. 0x3e 0x0a 0x0d 0x3c
11. Source: 38:2c:4a:9a:a6:20 ; Destination: a4:5e:60:e9:58:ab
12. 0x0806 indicating an ARP request
13.
    a. 19 bytes before it reaches the opcode
    b. 0x00 0x01 indicating request
    c. Yes, its 192.168.29.1
    d. Bytes 32 through 37 consist of the targeted Ethernet address.
14.
    a. 19 bytes before it reaches the opcode
    b. 0x0002 indicating reply
    c. 7 bytes after the opcode since the 6 bytes after the opcode are utilized for the Ethernet address of the machine being queried.
15. Source: a4:5e:60:e9:58:ab ; Destination: 38:2c:4a:9a:a6:20
16. There is no reply to the ARP request because there is no match to the local machines' hardware address.

```
      6 0.467282       192.168.29.111        128.119.245.12        HTTP     496    GET /wireshark-
labs/HTTP-ethereal-lab-file3.html HTTP/1.1
Frame 6: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits) on interface 0
Ethernet II, Src: Apple_e9:58:ab (a4:5e:60:e9:58:ab), Dst: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20)
    Destination: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20)
        Address: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Apple_e9:58:ab (a4:5e:60:e9:58:ab)
        Address: Apple_e9:58:ab (a4:5e:60:e9:58:ab)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.29.111, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 62074 (62074), Dst Port: 80 (80), Seq: 1, Ack: 1, Len:
430
Hypertext Transfer Protocol
```

```
     18 0.670370       128.119.245.12        192.168.29.111        HTTP     1514   HTTP/1.1 200 OK
  (text/html)
  Frame 18: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
      Interface id: 0 (en0)
      Encapsulation type: Ethernet (1)
      Arrival Time: Jun  6, 2016 23:05:03.109835000 PDT
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1465279503.109835000 seconds
      [Time delta from previous captured frame: 0.001316000 seconds]
      [Time delta from previous displayed frame: 0.097335000 seconds]
      [Time since reference or first frame: 0.670370000 seconds]
      Frame Number: 18
      Frame Length: 1514 bytes (12112 bits)
      Capture Length: 1514 bytes (12112 bits)
      [Frame is marked: False]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
      [Coloring Rule Name: HTTP]
      [Coloring Rule String: http || tcp.port == 80 || http2]
  Ethernet II, Src: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20), Dst: Apple_e9:58:ab (a4:5e:60:e9:58:ab)
      Destination: Apple_e9:58:ab (a4:5e:60:e9:58:ab)
          Address: Apple_e9:58:ab (a4:5e:60:e9:58:ab)
          .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
          .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      Source: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20)
          Address: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20)
          .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
          .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.29.111
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes
      Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
          0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
          .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
      Total Length: 1500
      Identification: 0x4889 (18569)
      Flags: 0x02 (Don't Fragment)
          0... .... = Reserved bit: Not set
          .1.. .... = Don't fragment: Set
          ..0. .... = More fragments: Not set
      Fragment offset: 0
      Time to live: 45
      Protocol: TCP (6)
      Header checksum: 0xabd7 [validation disabled]
          [Good: False]
          [Bad: False]
      Source: 128.119.245.12
      Destination: 192.168.29.111
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
  Transmission Control Protocol, Src Port: 80 (80), Dst Port: 62334 (62334), Seq: 1, Ack: 431, Len:
  1448
      Source Port: 80
      Destination Port: 62334
      [Stream index: 2]
      [TCP Segment Len: 1448]
      Sequence number: 1    (relative sequence number)
      [Next sequence number: 1449    (relative sequence number)]
      Acknowledgment number: 431    (relative ack number)
      Header Length: 32 bytes
      Flags: 0x010 (ACK)
```

```
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: *******A****]
    Window size value: 235
    [Calculated window size: 30080]
    [Window size scaling factor: 128]
    Checksum: 0xfda2 [validation disabled]
        [Good Checksum: False]
        [Bad Checksum: False]
    Urgent pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
        No-Operation (NOP)
            Type: 1
                0... .... = Copy on fragmentation: No
                .00. .... = Class: Control (0)
                ...0 0001 = Number: No-Operation (NOP) (1)
        No-Operation (NOP)
            Type: 1
                0... .... = Copy on fragmentation: No
                .00. .... = Class: Control (0)
                ...0 0001 = Number: No-Operation (NOP) (1)
        Timestamps: TSval 2785478641, TSecr 885648124
            Kind: Time Stamp Option (8)
            Length: 10
            Timestamp value: 2785478641
            Timestamp echo reply: 885648124
    [SEQ/ACK analysis]
        [iRTT: 0.090875000 seconds]
        [Bytes in flight: 1448]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
    Date: Tue, 07 Jun 2016 06:05:03 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r
\n
    Last-Modified: Tue, 07 Jun 2016 05:59:01 GMT\r\n
    ETag: "1194-534a9e2b81404"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 4500\r\n
        [Content length: 4500]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.097335000 seconds]
    [Request in frame: 16]
Line-based text data: text/html
```

```
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
    <p><br>\n
    </p>\n
    <p></p><center><b>THE BILL OF RIGHTS</b><br>\n
      <em>Amendments 1-10 of the Constitution</em>\n
    </center>\n
    \n
    <p>The Conventions of a number of the States having, at the time of adopting\n
    the Constitution, expressed a desire, in order to prevent misconstruction\n
    or abuse of its powers, that further declaratory and restrictive clauses\n
    should be added, and as extending the ground of public confidence in the\n
    Government will best insure the beneficent ends of its institution; </p><p>  Resolved, by the
Senate and House of Representatives of the United\n
    States of America, in Congress assembled, two-thirds of both Houses concurring,\n
    that the following articles be proposed to the Legislatures of the several\n
    States, as amendments to the Constitution of the United States; all or any\n
    of which articles, when ratified by three-fourths of the said Legislatures,\n
    to be valid to all intents and purposes as part of the said Constitution,\n
    namely:    </p
```

```
      6 1.253962       AsustekC_9a:a6:20     Apple_e9:58:ab        ARP      42     Who has
192.168.29.111? Tell 192.168.29.1
Frame 6: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
    Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun  6, 2016 23:19:52.128896000 PDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1465280392.128896000 seconds
    [Time delta from previous captured frame: 0.060397000 seconds]
    [Time delta from previous displayed frame: 0.060397000 seconds]
    [Time since reference or first frame: 1.253962000 seconds]
    Frame Number: 6
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
Ethernet II, Src: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20), Dst: Apple_e9:58:ab (a4:5e:60:e9:58:ab)
    Destination: Apple_e9:58:ab (a4:5e:60:e9:58:ab)
        Address: Apple_e9:58:ab (a4:5e:60:e9:58:ab)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20)
        Address: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20)
    Sender IP address: 192.168.29.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.29.111
```

/Users/richardmoot/Documents/ARP.pcapng 29 total packets, 29 shown

```
      7 1.254018       Apple_e9:58:ab        AsustekC_9a:a6:20     ARP      42     192.168.29.111
is at a4:5e:60:e9:58:ab
Frame 7: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
    Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun  6, 2016 23:19:52.128952000 PDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1465280392.128952000 seconds
    [Time delta from previous captured frame: 0.000056000 seconds]
    [Time delta from previous displayed frame: 0.000056000 seconds]
    [Time since reference or first frame: 1.254018000 seconds]
    Frame Number: 7
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
Ethernet II, Src: Apple_e9:58:ab (a4:5e:60:e9:58:ab), Dst: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20)
    Destination: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20)
        Address: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Apple_e9:58:ab (a4:5e:60:e9:58:ab)
        Address: Apple_e9:58:ab (a4:5e:60:e9:58:ab)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Apple_e9:58:ab (a4:5e:60:e9:58:ab)
    Sender IP address: 192.168.29.111
    Target MAC address: AsustekC_9a:a6:20 (38:2c:4a:9a:a6:20)
    Target IP address: 192.168.29.1
```