CS 494/594 Internetworking Protocols: Homework 5 (Winter 2022)
Portland State University
Due Date: 3/12/2022 11:59 pm PST

Name:_________Parth Parashar_____________________________________
Circle One: 494 [✓ ***594***]
594 Students: Please review **only one** of the following three papers.

Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Ste- fan Savage, "Experimental Security Analysis of a Modern Automobile", 2010 IEEE Symposium on Security and Privacy.

http://www.autosec.org/pubs/cars-oakland2010.pdf

Roger Dingledine, Nick Mathewson, "Tor: The Second-Generation Onion Router", Steven Murdoch, Paul Syverson, Usenix Security, 2004.

https://svn-archive.torproject.org/svn/projects/design-paper/tor-design.pdf

Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, "Practical network Support for IP Traceback." ACM SIGCOMM 2000, Stockholm, Sweden.

https://cseweb.ucsd.edu/~savage/papers/Sigcomm00.pdf

Paper Review

On

Experimental Security Analysis of a Modern Automobile

By Parth Parashar

In the current time, the vehicles are modernized and enhanced for the current technology and requirement. In the past two decades, the automobile industry has changed a lot. The modern vehicles are not only a mechanical, but it also contains many digital computers and hardware components through many internal networks. one recent estimate suggests that the typical luxury sedan now contains over 100 MB of binary code spread across 50–70 independent computers Electronic Control Units (ECUs) in automotive vernacular in turn communicating over one or more shared internal network buses.

Most of the current vehicles are computer controlled to a significant degree and virtually all new cars are now pervasively computerized. Digital control, in the form of self-contained embedded systems called Engine Control Units (ECUs), dynamically measuring the oxygen present in exhaust fumes, the ECU could then adjust the fuel/oxygen mixture before combustion, thereby improving efficiency and reducing pollutants. Such systems have been integrated into virtually every aspect of a car's functioning and diagnostics, including the throttle, transmission, brakes, passenger climate and lighting controls, external lights, entertainment, and so on, causing the term ECU to be generalized to Electronic Control Units.

There are many potential fragilities of the automotive environment, which provide valuable contributions toward framing the vehicle security and privacy problem space which, notably in outlining the security limitations of the popular CAN bus protocol which is a possible direction for securing vehicle components.

There can be a potential malicious attack on the vehicle, where intruders can attach a malicious component into a car's internal network though OBD-II port. Can be used for a brief period of connectivity to embed the malware within the car's existing components and then disconnect.

As we experimentally evaluating the security of individual car components, in the meanwhile assess the security properties of the CAN bus. A CAN packet does not include addresses in the traditional sense and instead supports a publish-and-subscribe communications model. The CAN ID header is used to indicate the packet type, and each packet is both physically and logically broadcast to all nodes, which then decide for themselves whether to process the packets. The underlying CAN protocol has several inherent weaknesses that are common to any implementation, like Broadcast nature, Fragility to DoS, No Authenticator Fields and Weak Access Control.

In the end we can conclude that, there are list of complex challenges that to be addressed which are extent of the damage when an intruder manipulates the ECU, ease of attack, unenforced access controls and attack amplification. Regarding security, are just a few of many potential defensive directions and associated tensions. There are deep-rooted tussles surrounding the security of cyber-physical vehicles. More likely, there is a spectrum of solutions that each trade off critical values.

1. (25 points) ISP #1 provides exclusive Internet connectivity to ISP #2 with customers A, B, C, and D. Suppose ISP#1 gives ISP #2 a range of addresses to use from 206.81.0.0 to 206.81.255.255 (Given in prefix/mask notation as 206.81.0.0/16). ISP #2 turns around and allocates the entire range to its 4 customers A, B, C, and D in contiguous, equal-sized chunks. Fill in the four allocations ISP #2 makes to its customers in prefix/mask notation.

Customer	Allocation (prefix/mask)
A	____.______.______.______/______

Customer	Allocation (prefix/mask)
B	___.____._____._____/_____
C	___.____._____._____/_____
D	___.____._____._____/_____

Answer: -

Customer	Allocation (prefix/mask)
A	206.81.0.0/18
B	206.81.64.0/18
C	206.81.128.0/18
D	206.81.192.0/18

2. (25 points) Multiple Access Protocols

Suppose nodes A and B are on the same 10 Mbps Ethernet segment and the propagation delay between the two nodes is 225 bit times. Suppose A and B send frames at the same time, the frames collide, and then A and B randomly choose their own values of K in the CSMA/CD algorithm. Assuming no other nodes are active, can retransmissions from A and B collide. For our purposes, it suffices to work out the following example. Suppose A and B begin transmission at t=0 bit times. They both detect collisions at t= 225 bit times. They finish transmitting a jam signal at t=225+48=273 bit times. Suppose $K_A=0$ and $K_B=1$.

Hints: Note that the random backoff component of scheduling delay is K * 512 bit times. Also note that the minimum Ethernet frame size is 512 bits.

a) At what time does B schedule its retransmission (in bit times)?

Answer: - when B finishes transmitting the jam signal + (512 * K_B

= 273 + 512 * 1

= 785-bit times

b) At what time does A begin transmission (in bit times)?

Answer: - when B finishes transmitting the jam signal + propagation time from A to B

= 273 + 225

= 498-bit times

c) At what time does A's signal reach B?

Answer: - time when A begins to transmit (b from above) + propagation time from A to B

= 498 + 225

= 723-bit times

d) Does B refrain from transmitting?

Answer: - Minimum ethernet frame size = 512
Time taken from transmission = 512-bit times
Time taken for A to finish transmission = time taken to begin + propagation time
= 498 + 512 = 1010 bit-times
Time taken for B to finish transmission = time taken to begin + propagation time
= 723 + 512 = 1235- bit times
Since B is higher than A, it refrains from transmitting.

3. (25 points) Protocol Perils

a) The Wikileaks website was hit with a massive distributed denial of service attack (DDoS) attack after the site published its first installment of US diplomatic cables. Describe 3 different ways in which such attacks can be launched.

Answer: - There are three ways to launch a denial of service (DDoS) attack:

1. Application layer attack
2. Volume-based attack
3. Protocol attack.

1 Application Layer Attack

This is a DDoS attack that focuses on a specific vulnerability and targets the application, preventing the application from delivering content to users. This attack sends many requests to the server that initially seem to be valid, causing the server to crash. The number of requests per second is used to determine the strength of this attack. Sloworis and HTTP Flood are two examples of application layer attacks. Sloworis is a system in which a web server shuts down another web server. Connecting to the target server keeps the connection to the server open, but sends only partial requests and ultimately consumes the entire connection capacity. HTTP flood attack from a crashing web server.

2. Volume-based attacks Volume-based attacks are the most common compared to

application layer and protocol attacks. In this case, hackers use many computers and internet connections to flood the targeted website and clog its bandwidth. As a result, valid traffic is blocked and hackers can easily destroy your website. The

UDP flood is an example of a volume-based attack. In a UDP flood attack, a hacker overloads a random port on the target host and the server cannot handle the volume of requests and goes down. 3. Protocol attack. The

protocol attack attempts to run out of server resources rather than bandwidth. Protocol attacks can also target intermediaries between servers and websites. B. Firewalls, load balancers, etc. SmurfDDoS is an example of a protocol attack. Hackers use the Internet Control Message Protocol (ICMP) to target spoofed IP addresses and broadcast them to the computer network. If there are many devices on the transferred network, the target computer will be flooded with traffic.

b) Host A wants to send a large file of F bits to host B securely (i.e., protect the confidentiality and integrity of packets). A and B are connected by two routers R1 and R2. A TCP flow is initiated by A towards B and all packets are forwarded by routers R1 and R2. We assume that A and B never exchanged information in the past and that there is no other communication channel between A and B. Is it possible for the routers (R1 or R2) to inject content in the TCP flow without causing a loss of any original packets sent from A to B? If yes, explain how. If no, explain why.

Answer: - Yes, the router (R1 or R2) can insert content into the TCP flow without losing the original packet sent from A to B.

Transmission Control Protocol (TCP) is a protocol that guarantees data transmission and maintains the order of packets after delivery. TCP uses acknowledgments (ACKs) and sequence numbers to ensure that packets are delivered in the correct order. This initiates a 3-way handshake between endpoint hosts A and B.

TCP hijacking occurs when an attacker breaks into a path or performs ARP spoofing. The attacker then drops the packet while using one of the existing connections and accepts the connection. The following scenario occurs when an attacker is in the abducted connection path. However, if an attacker is not in the abduction path, an attacker uses an IP address to send a BS packet. A then compares the TCP sequence number with the system stack sequence number, sends an ACK packet to get numbers. The ACK Storm occurs when an ACK packet is continuously converted. Attackers can not be able to abduct connections for ACK storms. B, on the other hand, resyncs and successfully transfers the large file F.

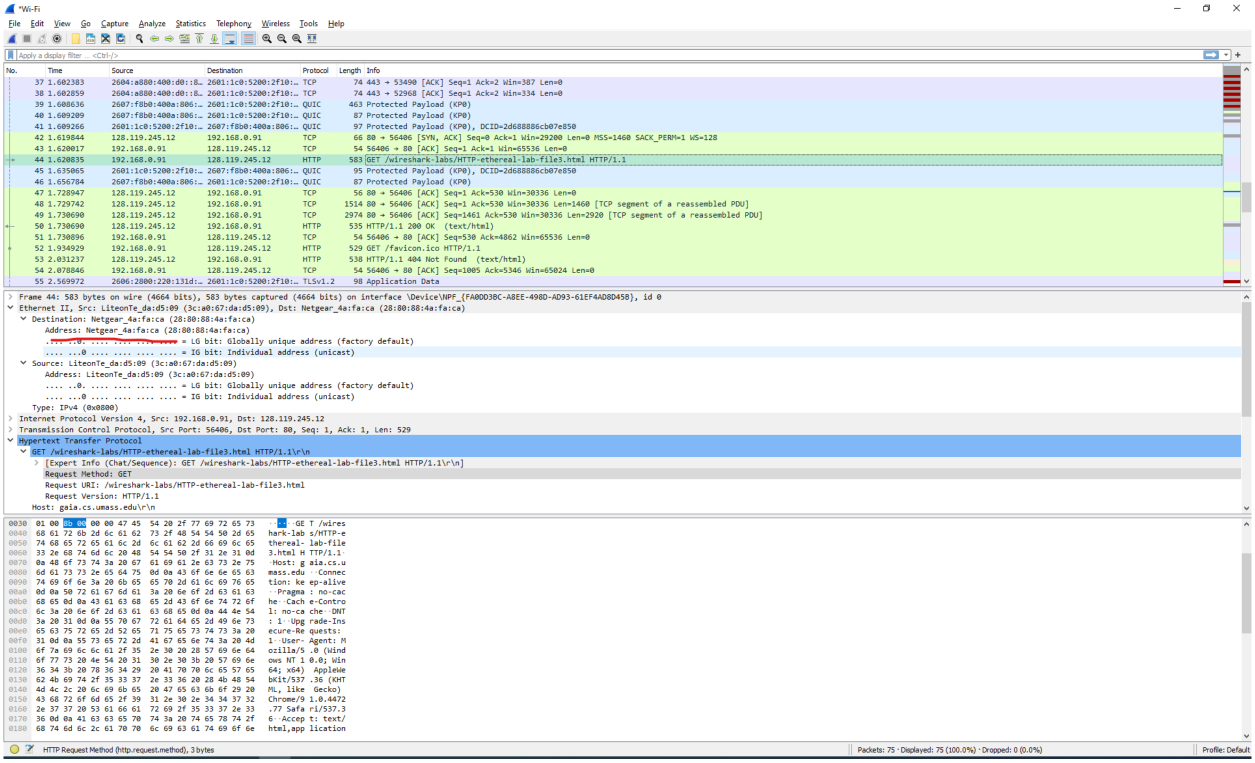
4. (25 points) Wireshark Lab: Ethernet and ARP

1) **What is the 48-bit Ethernet address of your computer?**
   Answer:
   48-bit ethernet address of my computer is 3c:a0:67:da:d5:09

2) **What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no).**

What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]

Answer:



```
No.    Time     Source                Destination           Protocol  Length Info
    37 1.602383 2604:a880:400:d0::8… 2601:1c0:5200:2f10:… TCP         74 443 → 53490 [ACK] Seq=1 Ack=2 Win=387 Len=0
    38 1.602859 2604:a880:400:d0::8… 2601:1c0:5200:2f10:… TCP         74 443 → 52968 [ACK] Seq=1 Ack=2 Win=334 Len=0
    39 1.608636 2607:f8b0:400a:806:… 2601:1c0:5200:2f10:… QUIC       463 Protected Payload (KP0)
    40 1.609209 2607:f8b0:400a:806:… 2601:1c0:5200:2f10:… QUIC        87 Protected Payload (KP0)
    41 1.609266 2601:1c0:5200:2f10:… 2607:f8b0:400a:806:… QUIC        97 Protected Payload (KP0), DCID=2d688886cb07e850
    42 1.619844 128.119.245.12       192.168.0.91          TCP         66 80 → 56406 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
    43 1.620017 192.168.0.91         128.119.245.12        TCP         54 56406 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
    44 1.620835 192.168.0.91         128.119.245.12        HTTP       583 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
    45 1.635065 2601:1c0:5200:2f10:… 2607:f8b0:400a:806:… QUIC        95 Protected Payload (KP0), DCID=2d688886cb07e850
    46 1.656784 2607:f8b0:400a:806:… 2601:1c0:5200:2f10:… QUIC        87 Protected Payload (KP0)
    47 1.728947 128.119.245.12       192.168.0.91          TCP         56 80 → 56406 [ACK] Seq=1 Ack=530 Win=30336 Len=0
    48 1.729742 128.119.245.12       192.168.0.91          TCP       1514 80 → 56406 [ACK] Seq=1 Ack=530 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
    49 1.730690 128.119.245.12       192.168.0.91          TCP       2974 80 → 56406 [ACK] Seq=1461 Ack=530 Win=30336 Len=2920 [TCP segment of a reassembled PDU]
    50 1.730690 128.119.245.12       192.168.0.91          HTTP       535 HTTP/1.1 200 OK  (text/html)
    51 1.730896 192.168.0.91         128.119.245.12        TCP         54 56406 → 80 [ACK] Seq=530 Ack=4862 Win=65536 Len=0
    52 1.934929 192.168.0.91         128.119.245.12        HTTP       529 GET /favicon.ico HTTP/1.1
    53 2.031237 128.119.245.12       192.168.0.91          HTTP       538 HTTP/1.1 404 Not Found  (text/html)
    54 2.078846 192.168.0.91         128.119.245.12        TCP         54 56406 → 80 [ACK] Seq=1005 Ack=5346 Win=65024 Len=0
    55 2.569972 2606:2800:220:131d:… 2601:1c0:5200:2f10:… TLSv1.2     98 Application Data
```

```
> Frame 44: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface \Device\NPF_{FA0DD3BC-A8EE-498D-AD93-61EF4AD8D45B}, id 0
v Ethernet II, Src: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09), Dst: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
  v Destination: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
      Address: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
      Address: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.0.91, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56406, Dst Port: 80, Seq: 1, Ack: 1, Len: 529
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-ethereal-lab-file3.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
```

```
0030  01 00 8b 00 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-lab s/HTTP-e
0050  74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal- lab-file
0060  33 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   3.html H TTP/1.1·
0070  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   ·Host: g aia.cs.u
0080  6d 61 73 73 2e 65 64 75  0d 0a 43 6f 6e 6e 65 63   mass.edu ··Connec
0090  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
00a0  0d 0a 50 72 61 67 6d 61  3a 20 6e 6f 2d 63 61 63   ··Pragma : no-cac
00b0  68 65 0d 0a 43 61 63 68  65 2d 43 6f 6e 74 72 6f   he··Cach e-Contro
00c0  6c 3a 20 6e 6f 2d 63 61  63 68 65 0d 0a 44 4e 54   l: no-ca che··DNT
00d0  3a 20 31 0d 0a 55 70 67  72 61 64 65 2d 49 6e 73   : 1··Upg rade-Ins
00e0  65 63 75 72 65 2d 52 65  71 75 65 73 74 73 3a 20   ecure-Re quests: 
00f0  31 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   1··User- Agent: M
0100  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 57 69 6e 64   ozilla/5 .0 (Wind
0110  6f 77 73 20 4e 54 20 31  30 2e 30 3b 20 57 69 6e   ows NT 1 0.0; Win
0120  36 34 3b 20 78 36 34 29  20 41 70 70 6c 65 57 65   64; x64)  AppleWe
0130  62 4b 69 74 2f 35 33 37  2e 33 36 20 28 4b 48 54   bKit/537 .36 (KHT
0140  4d 4c 2c 20 6c 69 6b 65  20 47 65 63 6b 6f 29 20   ML, like  Gecko) 
0150  43 68 72 6f 6d 65 2f 39  31 2e 30 2e 34 34 37 32   Chrome/9 1.0.4472
0160  2e 37 37 20 53 61 66 61  72 69 2f 35 33 37 2e 33   .77 Safa ri/537.3
0170  36 0d 0a 41 63 63 65 70  74 3a 20 74 65 78 74 2f   6··Accep t: text/
0180  68 74 6d 6c 2c 61 70 70  6c 69 63 61 74 69 6f 6e   html,app lication
```

HTTP Request Method (http.request.method), 3 bytes | Packets: 75 · Displayed: 75 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

The 48-bit destination address is 28:80:88:4a:fa:ca is not the address of gaia.cs.umass.edu.It is the address of my Netgear device Destination: **Netgear**_4a:fa:ca (28:80:88:4a:fa:ca)

3) **Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?**

Answer:

The hex value for the Frame type field is 0x0800 which, corresponds to the IP protocol

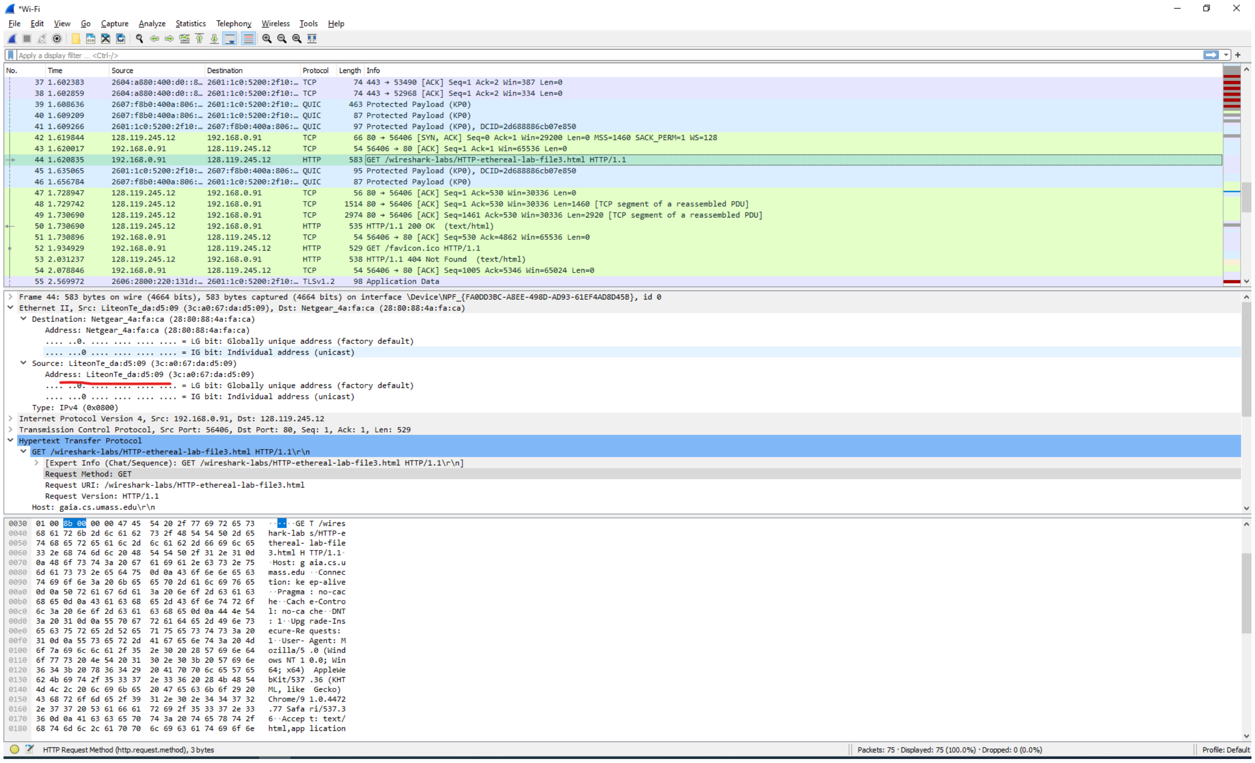
4) **How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?**

Answer:

The ASCII “G” appears 52 bytes from the start of the Ethernet frame. There are 14 B Ethernet frame, then 20 bytes of IP header followed by 20 bytes of TCP header.

5) **What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?**

Answer:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source                 Destination            Protocol Length Info
  37 1.602383  2604:a880:400:d0::8…   2601:1c0:5200:2f10:…   TCP        74 443 → 53490 [ACK] Seq=1 Ack=2 Win=387 Len=0
  38 1.602859  2604:a880:400:d0::8…   2601:1c0:5200:2f10:…   TCP        74 443 → 52968 [ACK] Seq=1 Ack=2 Win=334 Len=0
  39 1.608636  2607:f8b0:400a:806:…   2601:1c0:5200:2f10:…   QUIC      463 Protected Payload (KP0)
  40 1.609209  2607:f8b0:400a:806:…   2601:1c0:5200:2f10:…   QUIC       87 Protected Payload (KP0)
  41 1.609266  2601:1c0:5200:2f10:…   2607:f8b0:400a:806:…   QUIC       97 Protected Payload (KP0), DCID=2d688886cb07e850
  42 1.619844  128.119.245.12         192.168.0.91           TCP        66 80 → 56406 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  43 1.620017  192.168.0.91           128.119.245.12         TCP        54 56406 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  44 1.620835  192.168.0.91           128.119.245.12         HTTP      583 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
  45 1.635065  2601:1c0:5200:2f10:…   2607:f8b0:400a:806:…   QUIC       95 Protected Payload (KP0), DCID=2d688886cb07e850
  46 1.656784  2607:f8b0:400a:806:…   2601:1c0:5200:2f10:…   QUIC       87 Protected Payload (KP0)
  47 1.728947  128.119.245.12         192.168.0.91           TCP        56 80 → 56406 [ACK] Seq=1 Ack=530 Win=30336 Len=0
  48 1.729742  128.119.245.12         192.168.0.91           TCP      1514 80 → 56406 [ACK] Seq=1 Ack=530 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
  49 1.730690  128.119.245.12         192.168.0.91           TCP      2974 80 → 56406 [ACK] Seq=1461 Ack=530 Win=30336 Len=2920 [TCP segment of a reassembled PDU]
  50 1.730690  128.119.245.12         192.168.0.91           HTTP      535 HTTP/1.1 200 OK  (text/html)
  51 1.730896  192.168.0.91           128.119.245.12         TCP        54 56406 → 80 [ACK] Seq=530 Ack=4862 Win=65536 Len=0
  52 1.934929  192.168.0.91           128.119.245.12         HTTP      529 GET /favicon.ico HTTP/1.1
  53 2.031237  128.119.245.12         192.168.0.91           HTTP      538 HTTP/1.1 404 Not Found  (text/html)
  54 2.078846  192.168.0.91           128.119.245.12         TCP        54 56406 → 80 [ACK] Seq=1005 Ack=5346 Win=65024 Len=0
  55 2.569972  2606:2800:220:131d:…   2601:1c0:5200:2f10:…   TLSv1.2    98 Application Data
```

```
> Frame 44: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface \Device\NPF_{FA0DD3BC-A8EE-498D-AD93-61EF4AD8D45B}, id 0
v Ethernet II, Src: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09), Dst: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
  v Destination: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
      Address: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
      Address: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.0.91, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56406, Dst Port: 80, Seq: 1, Ack: 1, Len: 529
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-ethereal-lab-file3.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
```

```
0030  01 00 8b 00 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-lab s/HTTP-e
0050  74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal- lab-file
0060  33 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   3.html H TTP/1.1·
0070  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   ·Host: g aia.cs.u
0080  6d 61 73 73 2e 65 64 75  0d 0a 43 6f 6e 6e 65 63   mass.edu ··Connec
0090  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
00a0  0d 0a 50 72 61 67 6d 61  3a 20 6e 6f 2d 63 61 63   ··Pragma : no-cac
00b0  68 65 0d 0a 43 61 63 68  65 2d 43 6f 6e 74 72 6f   he··Cach e-Contro
00c0  6c 3a 20 6e 6f 2d 63 61  63 68 65 0d 0a 44 4e 54   l: no-ca che··DNT
00d0  3a 20 31 0d 0a 55 70 67  72 61 64 65 2d 49 6e 73   : 1··Upg rade-Ins
00e0  65 63 75 72 65 2d 52 65  71 75 65 73 74 73 3a 20   ecure-Re quests: 
00f0  31 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   1··User- Agent: M
0100  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 57 69 6e 64   ozilla/5 .0 (Wind
0110  6f 77 73 20 4e 54 20 31  30 2e 30 3b 20 57 69 6e   ows NT 1 0.0; Win
0120  36 34 3b 20 78 36 34 29  20 41 70 70 6c 65 57 65   64; x64)  AppleWe
0130  62 4b 69 74 2f 35 33 37  2e 33 36 20 28 4b 48 54   bKit/537 .36 (KHT
0140  4d 4c 2c 20 6c 69 6b 65  20 47 65 63 6b 6f 29 20   ML, like  Gecko) 
0150  43 68 72 6f 6d 65 2f 39  31 2e 30 2e 34 34 37 32   Chrome/9 1.0.4472
0160  2e 37 37 20 53 61 66 61  72 69 2f 35 33 37 2e 33   .77 Safa ri/537.3
0170  36 0d 0a 41 63 63 65 70  74 3a 20 74 65 78 74 2f   6··Accep t: text/
0180  68 74 6d 6c 2c 61 70 70  6c 69 63 61 74 69 6f 6e   html,app lication
```

HTTP Request Method (http.request.method), 3 bytes | Packets: 75 · Displayed: 75 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

The ethernet address 3c:a0:67:da:d5:09 is of the LiteonTe router and its not the ethernet address of my computer nor it is of gaia.cs.umass.edu

6) **What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?**
Answer:
The destination address in the Ethernet frame is 28:80:88:4a:fa:ca. Yes, it is the ethernet of my computer.

7) **Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?**

Answer:
The hex value for the Frame type field is 0x0800. This value corresponds to the IP protocol

8) **How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?**

Answer:

The ASCII “O” appears 52 bytes from the start of the Ethernet frame. there are 14 bytes of Ethernet frame, then 20 bytes of IP header followed by 20 bytes of TCP header.

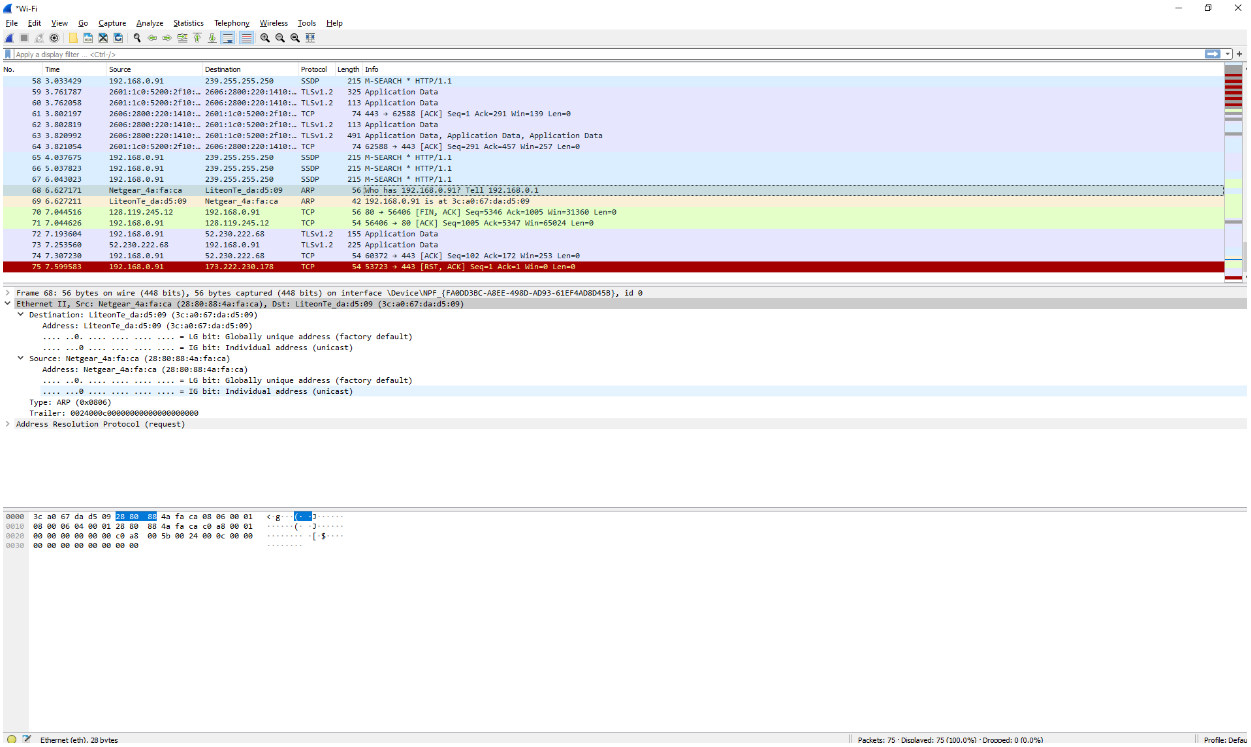
9) **Write down the contents of your computer’s ARP cache. What is the meaning of each column value?**

Answer:

Internet address -is the IP address,
Physical Address -is the MAC address
Type - is the protocol type

10) . **What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?**

Answer:



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source                 Destination            Protocol  Length Info
   58 3.033429   192.168.0.91           239.255.255.250        SSDP       215 M-SEARCH * HTTP/1.1
   59 3.761787   2601:1c0:5200:2f10:…   2606:2800:220:1410:…   TLSv1.2    325 Application Data
   60 3.762058   2601:1c0:5200:2f10:…   2606:2800:220:1410:…   TLSv1.2    113 Application Data
   61 3.802197   2606:2800:220:1410:…   2601:1c0:5200:2f10:…   TCP         74 443 → 62588 [ACK] Seq=1 Ack=291 Win=139 Len=0
   62 3.802819   2606:2800:220:1410:…   2601:1c0:5200:2f10:…   TLSv1.2    113 Application Data
   63 3.820992   2606:2800:220:1410:…   2601:1c0:5200:2f10:…   TLSv1.2    491 Application Data, Application Data, Application Data
   64 3.821054   2601:1c0:5200:2f10:…   2606:2800:220:1410:…   TCP         74 62588 → 443 [ACK] Seq=291 Ack=457 Win=257 Len=0
   65 4.037675   192.168.0.91           239.255.255.250        SSDP       215 M-SEARCH * HTTP/1.1
   66 5.037823   192.168.0.91           239.255.255.250        SSDP       215 M-SEARCH * HTTP/1.1
   67 6.043023   192.168.0.91           239.255.255.250        SSDP       215 M-SEARCH * HTTP/1.1
   68 6.627171   Netgear_4a:fa:ca       LiteonTe_da:d5:09      ARP         56 Who has 192.168.0.91? Tell 192.168.0.1
   69 6.627211   LiteonTe_da:d5:09      Netgear_4a:fa:ca       ARP         42 192.168.0.91 is at 3c:a0:67:da:d5:09
   70 7.044516   128.119.245.12         192.168.0.91           TCP         56 80 → 56406 [FIN, ACK] Seq=5346 Ack=1005 Win=31360 Len=0
   71 7.044626   192.168.0.91           128.119.245.12         TCP         54 56406 → 80 [ACK] Seq=1005 Ack=5347 Win=65024 Len=0
   72 7.193604   192.168.0.91           52.230.222.68          TLSv1.2    155 Application Data
   73 7.253560   52.230.222.68          192.168.0.91           TLSv1.2    225 Application Data
   74 7.307230   192.168.0.91           52.230.222.68          TCP         54 60372 → 443 [ACK] Seq=102 Ack=172 Win=253 Len=0
   75 7.599583   192.168.0.91           173.222.230.178        TCP         54 53723 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
> Frame 68: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{FA0DD3BC-A8EE-498D-AD93-61EF4AD8D45B}, id 0
v Ethernet II, Src: Netgear_4a:fa:ca (28:80:88:4a:fa:ca), Dst: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
  v Destination: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
      Address: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
      Address: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Trailer: 0024000c000000000000000000000
> Address Resolution Protocol (request)
```

```
0000  3c a0 67 da d5 09 28 80  88 4a fa ca 08 06 00 01   <·g···(· ·J······
0010  08 00 06 04 00 01 28 80  88 4a fa ca c0 a8 00 01   ······(· ·J······
0020  00 00 00 00 00 00 c0 a8  00 5b 00 24 00 0c 00 00   ········ ·[·$····
0030  00 00 00 00 00 00 00 00                            ········
```

The hex value for source is 28:80:88:4a:fa:ca and destination address is 3c:a0:67:da:d5:09

11) Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

Answer:

The hex value for the Ethernet Frame type field is 0x0806

12) Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

Answer:

The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame

b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

Answer:

The hex value for opcode field withing the ARP-payload of the request is 0x0001

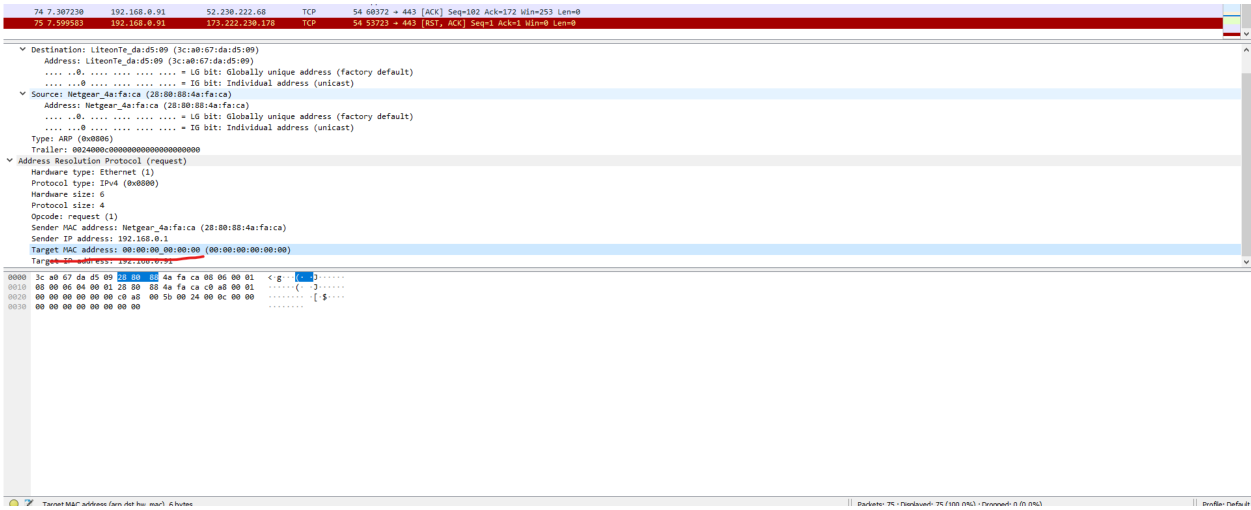
c) **Does the ARP message contain the IP address of the sender?**

Answer:

Yes, the ARP message containing the IP address 192.168.0.91 for the sender.

d) **Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?**

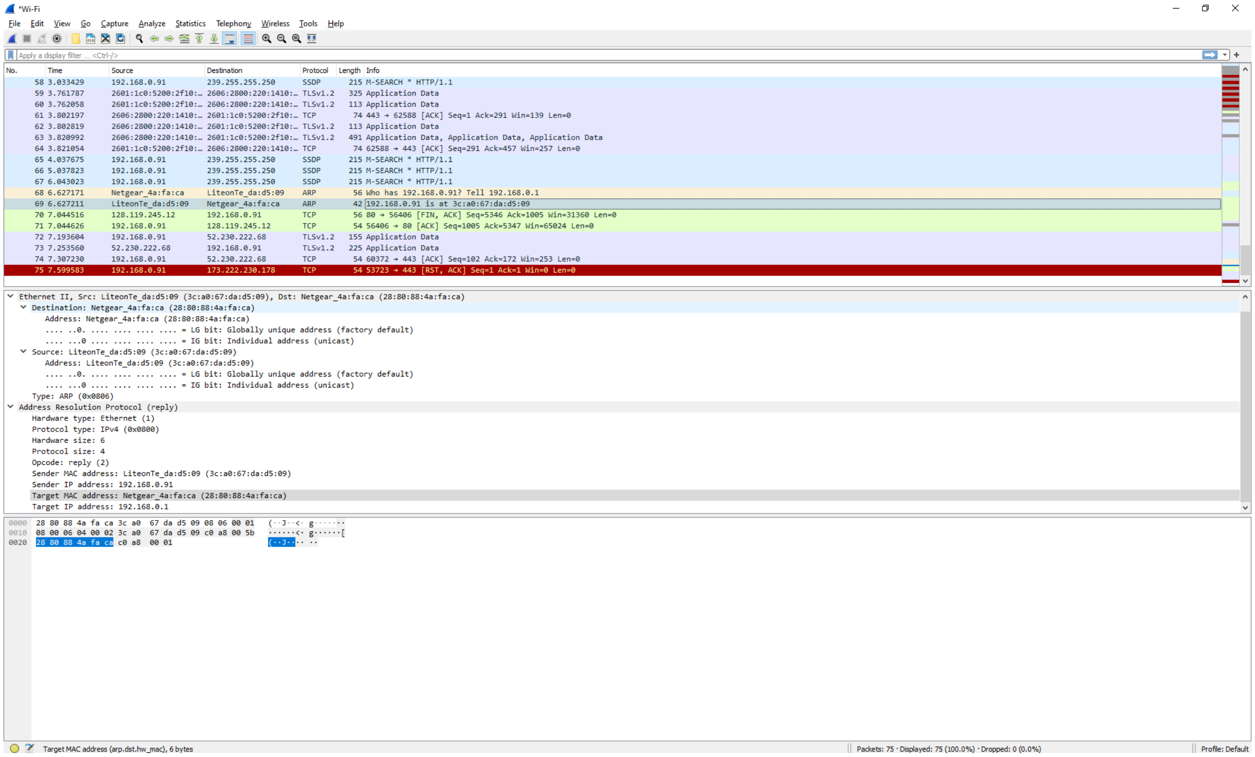
Answer:



```
 74 7.307230    192.168.0.91    52.230.222.68    TCP    54 60372 → 443 [ACK] Seq=102 Ack=172 Win=253 Len=0
 75 7.599583    192.168.0.91    173.222.230.178  TCP    54 53723 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

  v Destination: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
      Address: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
      Address: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Trailer: 0024000c0000000000000000000
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
    Sender IP address: 192.168.0.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.91

0000  3c a0 67 da d5 09 28 80  88 4a fa ca 08 06 00 01   <·g···(· ·J······
0010  08 00 06 04 00 01 28 80  88 4a fa ca c0 a8 00 01   ······(· ·J······
0020  00 00 00 00 00 00 c0 a8  00 5b 00 24 00 0c 00 00   ········ ·[·$····
0030  00 00 00 00 00 00 00 00                            ········

Target MAC address (arp.dst.hw_mac), 6 bytes    Packets: 75 · Displayed: 75 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

The field "Target MAC address" is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.0.1) is being queried.

13) **Now find the ARP reply that was sent in response to the ARP request.**


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time      Source                Destination           Protocol Length Info
   58 3.033429  192.168.0.91          239.255.255.250       SSDP      215 M-SEARCH * HTTP/1.1
   59 3.761787  2601:1c0:5200:2f10:…  2606:2800:220:1410:…  TLSv1.2   325 Application Data
   60 3.762058  2601:1c0:5200:2f10:…  2606:2800:220:1410:…  TLSv1.2   113 Application Data
   61 3.802197  2606:2800:220:1410:…  2601:1c0:5200:2f10:…  TCP        74 443 → 62588 [ACK] Seq=1 Ack=291 Win=139 Len=0
   62 3.802819  2606:2800:220:1410:…  2601:1c0:5200:2f10:…  TLSv1.2   113 Application Data
   63 3.820992  2606:2800:220:1410:…  2601:1c0:5200:2f10:…  TLSv1.2   491 Application Data, Application Data, Application Data
   64 3.821054  2601:1c0:5200:2f10:…  2606:2800:220:1410:…  TCP        74 62588 → 443 [ACK] Seq=291 Ack=457 Win=257 Len=0
   65 4.037675  192.168.0.91          239.255.255.250       SSDP      215 M-SEARCH * HTTP/1.1
   66 5.037823  192.168.0.91          239.255.255.250       SSDP      215 M-SEARCH * HTTP/1.1
   67 6.043023  192.168.0.91          239.255.255.250       SSDP      215 M-SEARCH * HTTP/1.1
   68 6.627171  Netgear_4a:fa:ca      LiteonTe_da:d5:09     ARP        56 Who has 192.168.0.91? Tell 192.168.0.1
   69 6.627211  LiteonTe_da:d5:09     Netgear_4a:fa:ca      ARP        42 192.168.0.91 is at 3c:a0:67:da:d5:09
   70 7.044516  128.119.245.12        192.168.0.91          TCP        56 80 → 56406 [FIN, ACK] Seq=5346 Ack=1005 Win=31360 Len=0
   71 7.044626  192.168.0.91          128.119.245.12        TCP        54 56406 → 80 [ACK] Seq=1005 Ack=5347 Win=65024 Len=0
   72 7.193604  192.168.0.91          52.230.222.68         TLSv1.2   155 Application Data
   73 7.253560  52.230.222.68         192.168.0.91          TLSv1.2   225 Application Data
   74 7.307230  192.168.0.91          52.230.222.68         TCP        54 60372 → 443 [ACK] Seq=102 Ack=172 Win=253 Len=0
   75 7.599583  192.168.0.91          173.222.230.178       TCP        54 53723 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
Ethernet II, Src: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09), Dst: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
  Destination: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
    Address: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
    Address: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
    .... ..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: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
  Sender IP address: 192.168.0.91
  Target MAC address: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
  Target IP address: 192.168.0.1
```

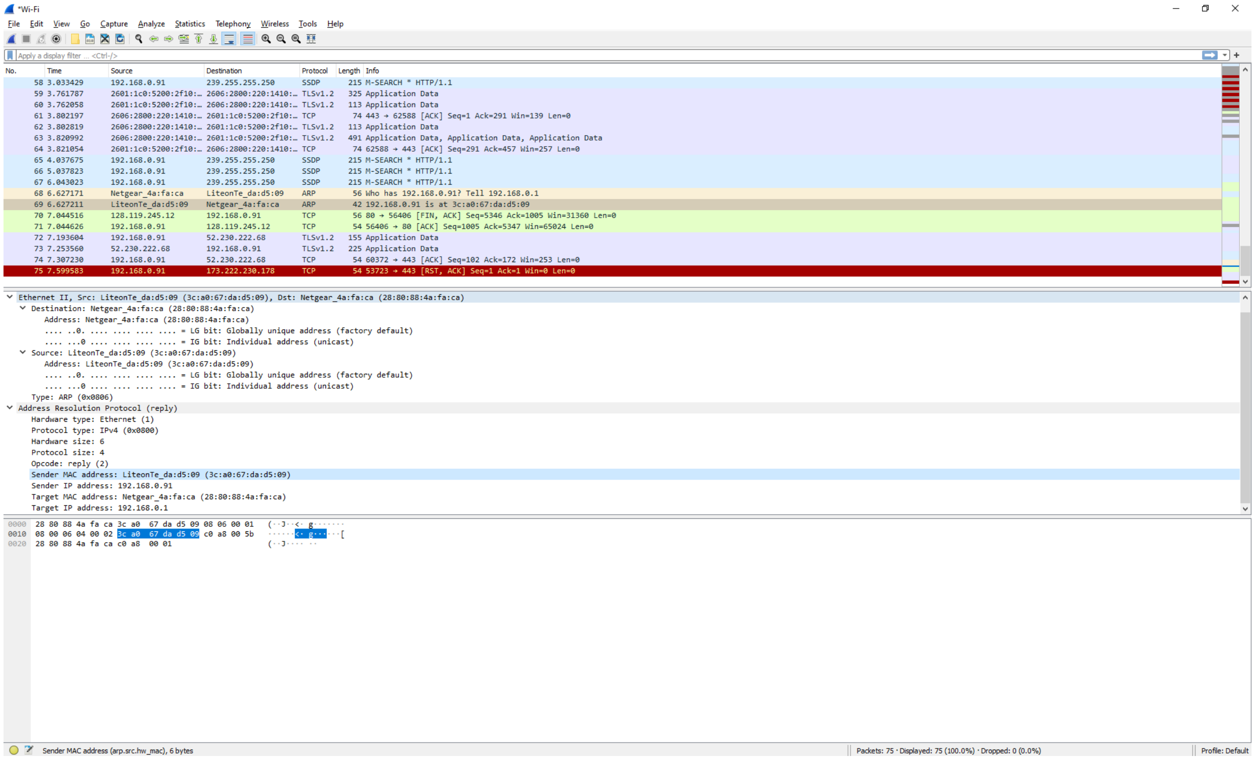
```
0000  28 80 88 4a fa ca 3c a0  67 da d5 09 08 06 00 01   (··J··<· g·······
0010  08 00 06 04 00 02 3c a0  67 da d5 09 c0 a8 00 5b   ······<· g······[
0020  28 80 88 4a fa ca c0 a8  00 01                     (··J···· ··
```

Target MAC address (arp.dst.hw_mac), 6 bytes | Packets: 75 · Displayed: 75 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

a) **How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?**
Answer:
The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

b) **What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?**
Answer:
The hex value for opcode field withing the ARP-payload of the request is 0x0002, for reply.

c) Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?
Answer:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source               Destination          Protocol Length Info
   58 3.033429  192.168.0.91         239.255.255.250      SSDP     215 M-SEARCH * HTTP/1.1
   59 3.761787  2601:1c0:5200:2f10:… 2606:2800:220:1410:… TLSv1.2  325 Application Data
   60 3.762058  2601:1c0:5200:2f10:… 2606:2800:220:1410:… TLSv1.2  113 Application Data
   61 3.802197  2606:2800:220:1410:… 2601:1c0:5200:2f10:… TCP       74 443 → 62588 [ACK] Seq=1 Ack=291 Win=139 Len=0
   62 3.802819  2606:2800:220:1410:… 2601:1c0:5200:2f10:… TLSv1.2  113 Application Data
   63 3.820992  2606:2800:220:1410:… 2601:1c0:5200:2f10:… TLSv1.2  491 Application Data, Application Data, Application Data
   64 3.821054  2601:1c0:5200:2f10:… 2606:2800:220:1410:… TCP       74 62588 → 443 [ACK] Seq=291 Ack=457 Win=257 Len=0
   65 4.037675  192.168.0.91         239.255.255.250      SSDP     215 M-SEARCH * HTTP/1.1
   66 5.037823  192.168.0.91         239.255.255.250      SSDP     215 M-SEARCH * HTTP/1.1
   67 6.043023  192.168.0.91         239.255.255.250      SSDP     215 M-SEARCH * HTTP/1.1
   68 6.627171  Netgear_4a:fa:ca     LiteonTe_da:d5:09    ARP       56 Who has 192.168.0.91? Tell 192.168.0.1
   69 6.627211  LiteonTe_da:d5:09    Netgear_4a:fa:ca     ARP       42 192.168.0.91 is at 3c:a0:67:da:d5:09
   70 7.044516  128.119.245.12       192.168.0.91         TCP       56 80 → 56406 [FIN, ACK] Seq=5346 Ack=1005 Win=31360 Len=0
   71 7.044626  192.168.0.91         128.119.245.12       TCP       54 56406 → 80 [ACK] Seq=1005 Ack=5347 Win=65024 Len=0
   72 7.193604  192.168.0.91         52.230.222.68        TLSv1.2  155 Application Data
   73 7.253560  52.230.222.68        192.168.0.91         TLSv1.2  225 Application Data
   74 7.307230  192.168.0.91         52.230.222.68        TCP       54 60372 → 443 [ACK] Seq=102 Ack=172 Win=253 Len=0
   75 7.599583  192.168.0.91         173.222.230.178      TCP       54 53723 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
Ethernet II, Src: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09), Dst: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
  Destination: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
    Address: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
    Address: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
    .... ..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: LiteonTe_da:d5:09 (3c:a0:67:da:d5:09)
  Sender IP address: 192.168.0.91
  Target MAC address: Netgear_4a:fa:ca (28:80:88:4a:fa:ca)
  Target IP address: 192.168.0.1
```

```
0000  28 80 88 4a fa ca 3c a0  67 da d5 09 08 06 00 01   (··J··<· g·······
0010  08 00 06 04 00 02 3c a0  67 da d5 09 c0 a8 00 5b   ······<· g······[
0020  28 80 88 4a fa ca c0 a8  00 01                     (··J···· ··
```

```
Sender MAC address (arp.src.hw_mac), 6 bytes    Packets: 75 · Displayed: 75 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

The answer to the earlier ARP request appears in the "Sender MAC address" field, which contains the Ethernet address 3c:a0:67:da:d5:09 for the sender with IP address 192.168.0.1

14) What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?
Answer:

The hex value for source is LiteonTe_da:d5:09 (3c:a0:67:da:d5:09) and the destination is Netgear_4a:fa:ca (28:80:88:4a:fa:ca)

15) Open the ethernet-ethereal-trace-1 trace file in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the

ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

Answer:

There is no reply in this trace, because we are not at the machine that sent the request. The ARP request is broadcast, but the ARP reply is sent back directly to the sender's Ethernet address.