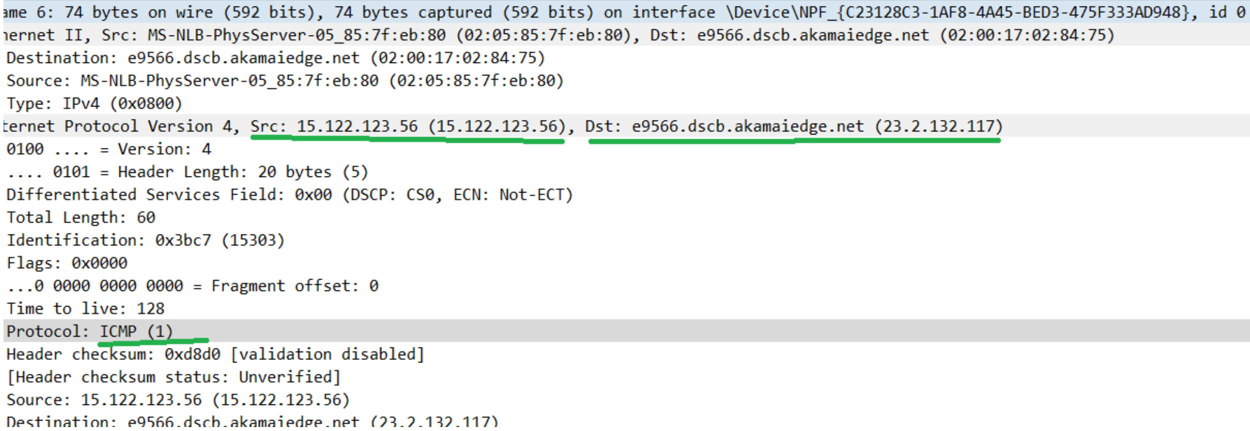
1.

a. source IP address is 15.122.123.56, destination IP address is 23.2.132.117



```
ame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{C23128C3-1AF8-4A45-BED3-475F333AD948}, id 0
hernet II, Src: MS-NLB-PhysServer-05_85:7f:eb:80 (02:05:85:7f:eb:80), Dst: e9566.dscb.akamaiedge.net (02:00:17:02:84:75)
 Destination: e9566.dscb.akamaiedge.net (02:00:17:02:84:75)
 Source: MS-NLB-PhysServer-05_85:7f:eb:80 (02:05:85:7f:eb:80)
 Type: IPv4 (0x0800)
ternet Protocol Version 4, Src: 15.122.123.56 (15.122.123.56), Dst: e9566.dscb.akamaiedge.net (23.2.132.117)
 0100 .... = Version: 4
 .... 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 60
 Identification: 0x3bc7 (15303)
 Flags: 0x0000
 ...0 0000 0000 0000 = Fragment offset: 0
 Time to live: 128
 Protocol: ICMP (1)
 Header checksum: 0xd8d0 [validation disabled]
 [Header checksum status: Unverified]
 Source: 15.122.123.56 (15.122.123.56)
 Destination: e9566.dscb.akamaiedge.net (23.2.132.117)
```

b. the upper-layer protocol is ICMP.

c. IP header length is 20 bytes.

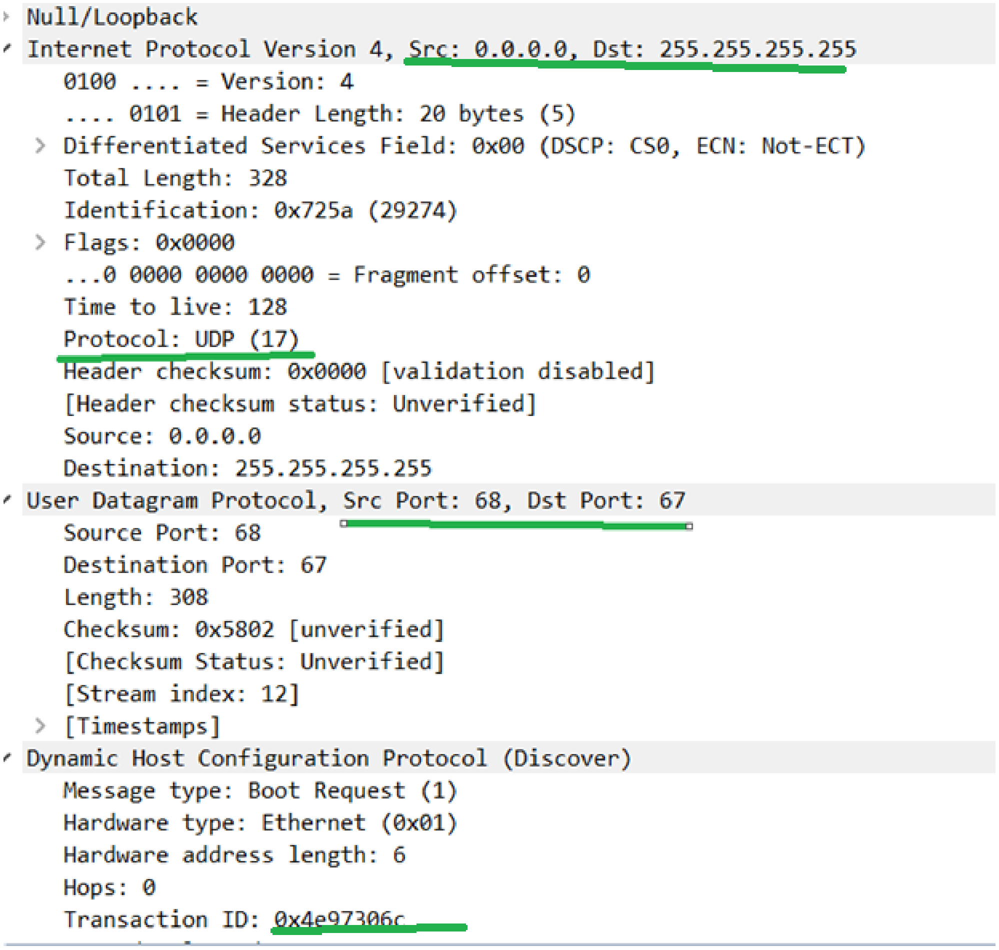
d. payload length for IP packet is total length 60 – header length 20 = 40

e. TTL is acronym of Time To Live, value is 128 in the IP packet. The TTL value is set by sender, reduced by every router on the route to the destination, if the value is reduced to zero before it reach the destination, the packet is discarded.

f. the source IP and destination IP addresses shows whether the packet is if IPv4 or IPv6 format.

2.

a. we can see from following screenshot, DHCP uses UDP in the transport layer. The reason it uses UDP rather than TCP is due to the nature of TCP and UDP, TCP transport requires pre-established connection while UDP does not, since the client server does not have an IP address therefore does not have internet access yet, it is impossible to establish a connection at the time.

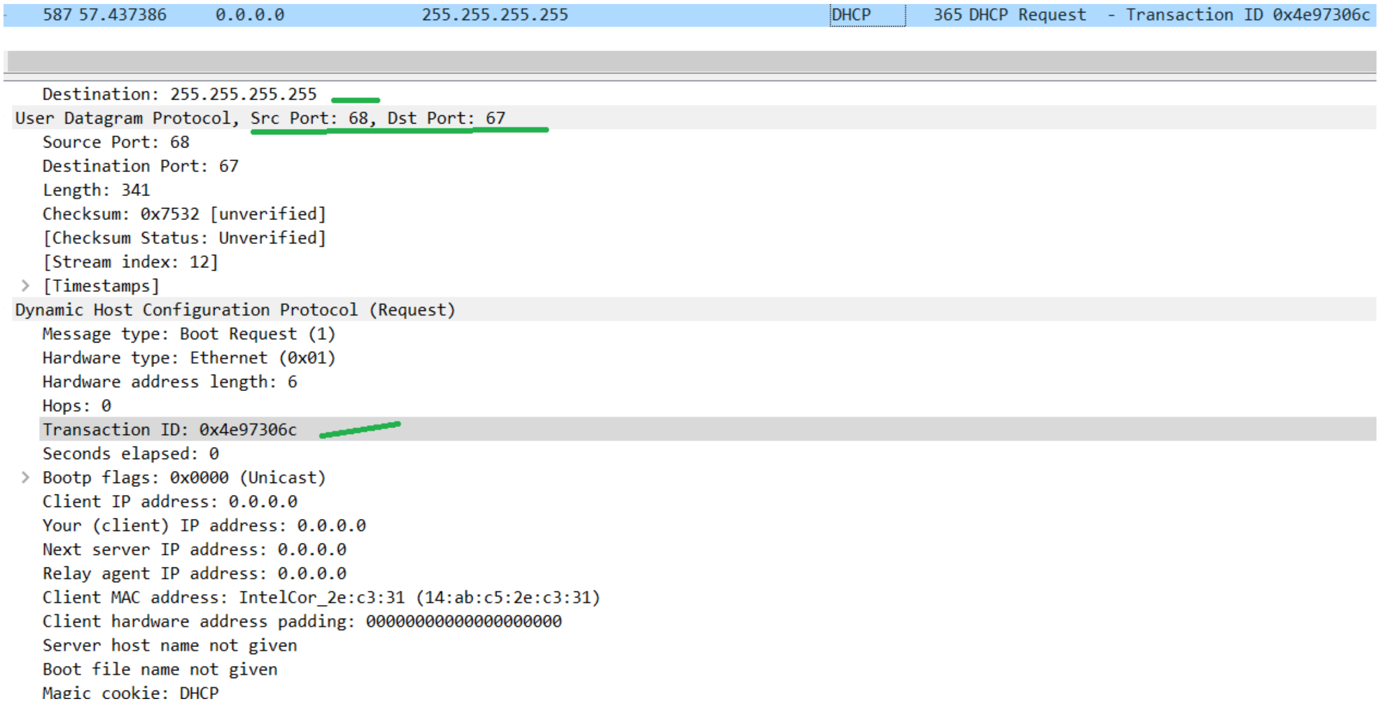


```
› Null/Loopback
⌄ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 328
     Identification: 0x725a (29274)
   › Flags: 0x0000
     ...0 0000 0000 0000 = Fragment offset: 0
     Time to live: 128
     Protocol: UDP (17)
     Header checksum: 0x0000 [validation disabled]
     [Header checksum status: Unverified]
     Source: 0.0.0.0
     Destination: 255.255.255.255
⌄ User Datagram Protocol, Src Port: 68, Dst Port: 67
     Source Port: 68
     Destination Port: 67
     Length: 308
     Checksum: 0x5802 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 12]
   › [Timestamps]
⌄ Dynamic Host Configuration Protocol (Discover)
     Message type: Boot Request (1)
     Hardware type: Ethernet (0x01)
     Hardware address length: 6
     Hops: 0
     Transaction ID: 0x4e97306c
```

b. source port is 68 and destination port is 67 as shown in the User Datagram Protocol section above.

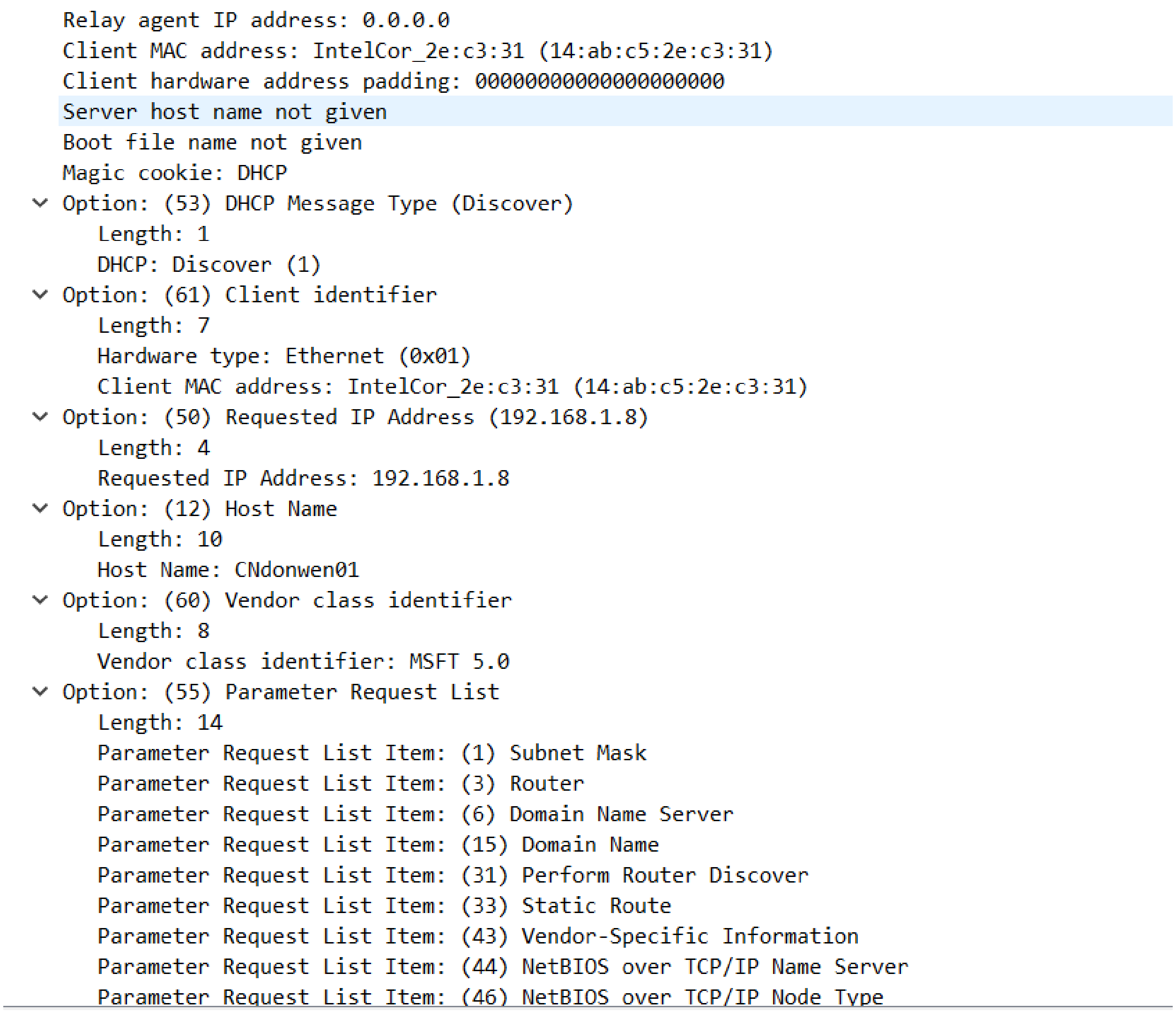
c. the transaction ID in the discovery packet is 0x4e97306c.

e. source IP is 0.0.0.0, destination IP is 255.255.255.255, Your (client) IP address is 0.0.0.0, transaction ID is 0x4e97306c, and lifetime (Time To Live) is 128



```
    587 57.437386      0.0.0.0                255.255.255.255                          DHCP         365 DHCP Request  - Transaction ID 0x4e97306c

    Destination: 255.255.255.255
 User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 341
    Checksum: 0x7532 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 12]
  > [Timestamps]
 Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4e97306c
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_2e:c3:31 (14:ab:c5:2e:c3:31)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
```

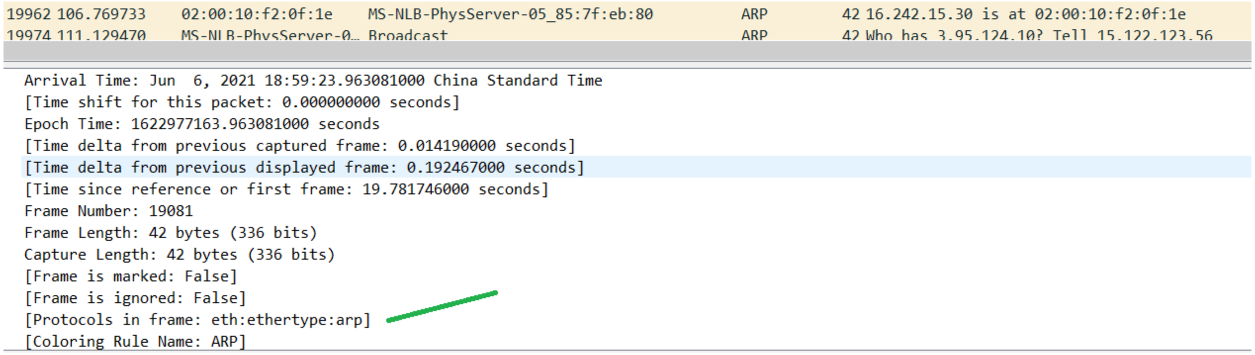
f. for unknown reason, I cannot find the offer packet but a second discovery packet as below.



```
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_2e:c3:31 (14:ab:c5:2e:c3:31)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⌄ Option: (53) DHCP Message Type (Discover)
      Length: 1
      DHCP: Discover (1)
  ⌄ Option: (61) Client identifier
      Length: 7
      Hardware type: Ethernet (0x01)
      Client MAC address: IntelCor_2e:c3:31 (14:ab:c5:2e:c3:31)
  ⌄ Option: (50) Requested IP Address (192.168.1.8)
      Length: 4
      Requested IP Address: 192.168.1.8
  ⌄ Option: (12) Host Name
      Length: 10
      Host Name: CNdonwen01
  ⌄ Option: (60) Vendor class identifier
      Length: 8
      Vendor class identifier: MSFT 5.0
  ⌄ Option: (55) Parameter Request List
      Length: 14
      Parameter Request List Item: (1) Subnet Mask
      Parameter Request List Item: (3) Router
      Parameter Request List Item: (6) Domain Name Server
      Parameter Request List Item: (15) Domain Name
      Parameter Request List Item: (31) Perform Router Discover
      Parameter Request List Item: (33) Static Route
      Parameter Request List Item: (43) Vendor-Specific Information
      Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
      Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
```

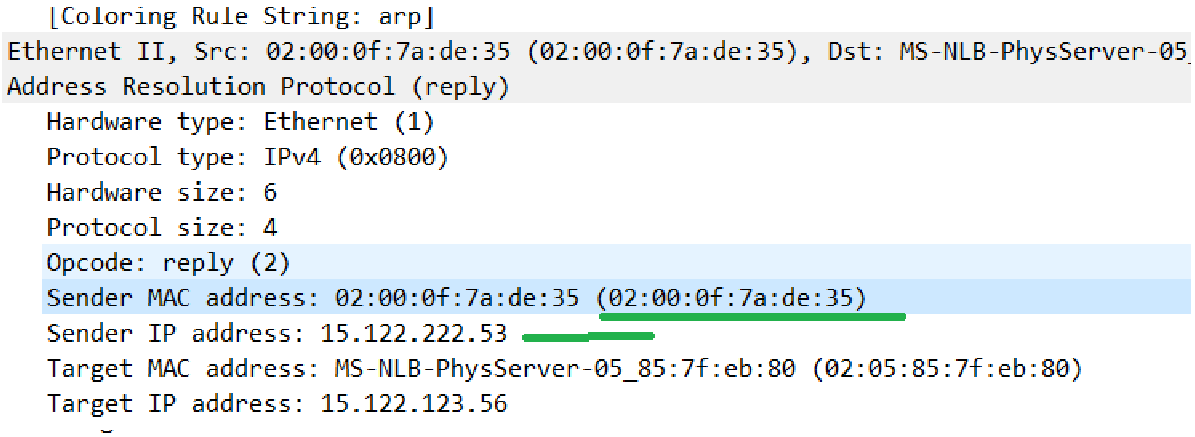
3.

a. the protocol is ARP. The broadcast MAC address is 02:05:85:7f:eb:80. The IP address is 15.122.222.53 for which the request was intended to find out MAC



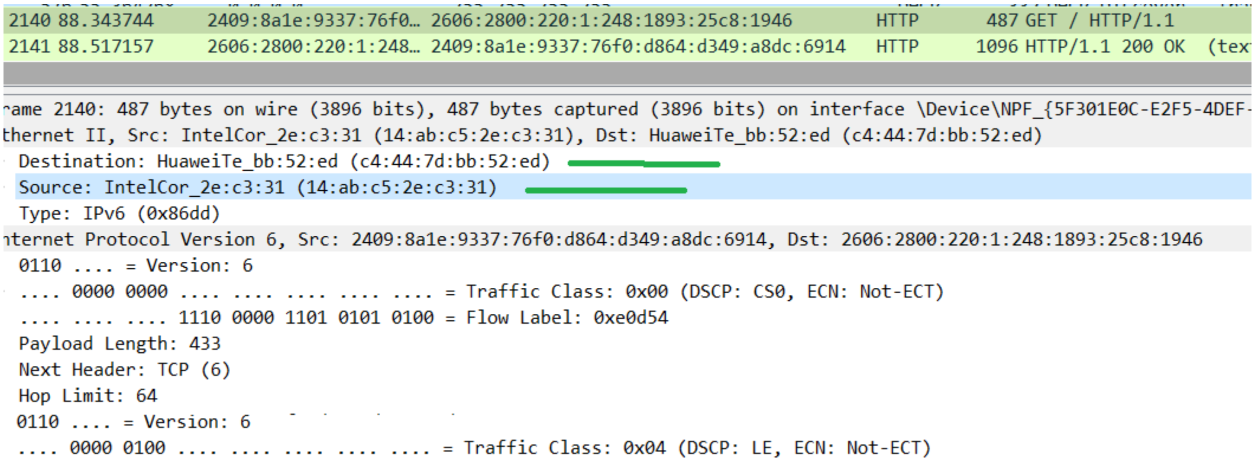
```
19962 106.769733   02:00:10:f2:0f:1e    MS-NLB-PhysServer-05_85:7f:eb:80    ARP    42 16.242.15.30 is at 02:00:10:f2:0f:1e
19974 111.129470   MS-NLB-PhysServer-0… Broadcast                           ARP    42 Who has 3.95.124.10? Tell 15.122.123.56

  Arrival Time: Jun  6, 2021 18:59:23.963081000 China Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1622977163.963081000 seconds
  [Time delta from previous captured frame: 0.014190000 seconds]
  [Time delta from previous displayed frame: 0.192467000 seconds]
  [Time since reference or first frame: 19.781746000 seconds]
  Frame Number: 19081
  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]
```

b. the sender's IP is 15.122.222.53, with MAC 02:00:0f:7a:de:35



```
   [Coloring Rule String: arp]
Ethernet II, Src: 02:00:0f:7a:de:35 (02:00:0f:7a:de:35), Dst: MS-NLB-PhysServer-05_
Address Resolution Protocol (reply)
   Hardware type: Ethernet (1)
   Protocol type: IPv4 (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: reply (2)
   Sender MAC address: 02:00:0f:7a:de:35 (02:00:0f:7a:de:35)
   Sender IP address: 15.122.222.53
   Target MAC address: MS-NLB-PhysServer-05_85:7f:eb:80 (02:05:85:7f:eb:80)
   Target IP address: 15.122.123.56
```

4. a. source MAC is 14:ab:c5:2e:c3:31, destination MAC is c4:44:7d:bb:52:ed



```
2140 88.343744   2409:8a1e:9337:76f0… 2606:2800:220:1:248:1893:25c8:1946    HTTP      487 GET / HTTP/1.1
2141 88.517157   2606:2800:220:1:248… 2409:8a1e:9337:76f0:d864:d349:a8dc:6914  HTTP     1096 HTTP/1.1 200 OK  (tex

rame 2140: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface \Device\NPF_{5F301E0C-E2F5-4DEF-
thernet II, Src: IntelCor_2e:c3:31 (14:ab:c5:2e:c3:31), Dst: HuaweiTe_bb:52:ed (c4:44:7d:bb:52:ed)
  Destination: HuaweiTe_bb:52:ed (c4:44:7d:bb:52:ed)
  Source: IntelCor_2e:c3:31 (14:ab:c5:2e:c3:31)
  Type: IPv6 (0x86dd)
nternet Protocol Version 6, Src: 2409:8a1e:9337:76f0:d864:d349:a8dc:6914, Dst: 2606:2800:220:1:248:1893:25c8:1946
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... .... .... 1110 0000 1101 0101 0100 = Flow Label: 0xe0d54
  Payload Length: 433
  Next Header: TCP (6)
  Hop Limit: 64
  0110 .... = Version: 6
  .... 0000 0100 .... .... .... .... .... = Traffic Class: 0x04 (DSCP: LE, ECN: Not-ECT)
```