No.	Time	Source	Destination	Protocol	Length	Info
154	6.092384	100.64.176.202	128.119.245.12	TCP	54	52666 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
155	6.092755	100.64.176.202	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
156	6.093450	128.119.245.12	100.64.176.202	TCP	66	80 → 52667 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM ...
157	6.093556	100.64.176.202	128.119.245.12	TCP	54	52667 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
158	6.347390	128.119.245.12	100.64.176.202	TCP	66	80 → 52668 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM ...
159	6.347530	100.64.176.202	128.119.245.12	TCP	54	52668 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
160	6.367079	128.119.245.12	100.64.176.202	TCP	60	80 → 52666 [ACK] Seq=1 Ack=497 Win=30336 Len=0
161	6.369681	128.119.245.12	100.64.176.202	TCP	1434	80 → 52666 [ACK] Seq=1 Ack=497 Win=30336 Len=1380 [TCP segment of a r...

> Frame 155: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on
> Ethernet II, Src: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c), Dst: HuaweiTe_8a:5...
> Internet Protocol Version 4, Src: 100.64.176.202, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52666, Dst Port: 80, Seq: 1, Ack:
> Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Length	Info
151	5.929120	IntelCor_a1:aa:7c	HuaweiTe_8a:5d:45	0x0800	66	IPv4
152	6.070963	IntelCor_a1:aa:7c	HuaweiTe_8a:5d:45	0x0800	66	IPv4
153	6.092215	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	0x0800	66	IPv4
154	6.092384	IntelCor_a1:aa:7c	HuaweiTe_8a:5d:45	0x0800	54	IPv4
155	6.092755	IntelCor_a1:aa:7c	HuaweiTe_8a:5d:45	0x0800	550	IPv4
156	6.093450	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	0x0800	66	IPv4
157	6.093556	IntelCor_a1:aa:7c	HuaweiTe_8a:5d:45	0x0800	54	IPv4
158	6.347390	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	0x0800	66	IPv4

> Frame 155: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on
> Ethernet II, Src: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c), Dst: HuaweiTe_8a:5...
> Data (536 bytes)

1. 我的电脑的 48 位以太网地址是多少？

c4:23:60:a1:aa:7c

155 6.092755	IntelCor_a1:aa:7c	HuaweiTe_8a:5d:45	0x0800	550
156 6.093450	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	0x0800	66
157 6.093556	IntelCor_a1:aa:7c	HuaweiTe_8a:5d:45	0x0800	54
158 6.347390	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	0x0800	66

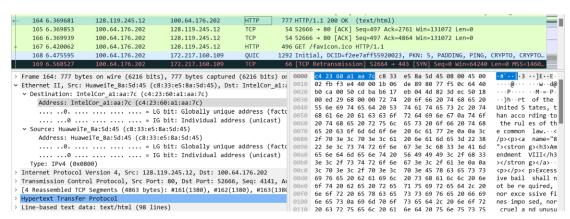> Frame 155: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) or
∨ Ethernet II, Src: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c), Dst: HuaweiTe_8a:5...
   > Destination: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
   > Source: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
     Type: IPv4 (0x0800)

2. 目的地址的 48 位以太网地址是多少？这是 gaia.cs.umass.edu 的以太网地址吗？这是什么设备的以太网地址？

c8:33:e5:8a:5d:45，这个不是 gaia.cs.umass.edu 的以太网地址，而是子网的路由器的地址。

3. 给出数据帧的十六进制数，这对应于哪个上层协议？

0x0800，表示上层协议为 IPv4。

∨ Ethernet II, Src: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c), Dst: HuaweiTe_8a:5...
   > Destination: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
   > Source: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
     Type: IPv4 (0x0800)

4. 从以太帧开始到"GET"中的 ASCII 码的"G"字出现间隔的字节数？

计数，一共 16*3+7=55

```
0000  c8 33 e5 8a 5d 45 c4 23  60 a1 aa 7c 08 00 45 00    ·3··]E·#  `··|··E·
0010  02 18 5f 56 40 00 40 06  00 00 64 40 b0 ca 80 77    ··_V@·@·  ··d@···w
0020  f5 0c cd ba 00 50 4d 82  3b fc b6 17 da d8 50 18    ·····PM·  ;·····P·
0030  02 00 8c 99 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
```


5. 以太网源地址是什么？这是你的电脑的地址吗或者是 gaia.cs.umass.edu 的？

c8:33:e5:8a:5d:45 ，这个不是 gaia.cs.umass.edu 的以太网地址，而是子网的路由器的地址。

161 6.369681	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	0x0800	1434
162 6.369681	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	0x0800	1434
163 6.369681	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	0x0800	1434
164 6.369681	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	0x0800	777
165 6.369853	IntelCor_a1:aa:7c	HuaweiTe_8a:5d:45	0x0800	54
166 6.369939	IntelCor_a1:aa:7c	HuaweiTe_8a:5d:45	0x0800	54
167 6.420062	IntelCor_a1:aa:7c	HuaweiTe_8a:5d:45	0x0800	496

```
> Frame 161: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits
v Ethernet II, Src: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45), Dst: IntelCor_a1:a
    v Destination: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
        Address: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (fact
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    v Source: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
        Address: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (fact
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

6. 以太网目的地址是什么？这是你的电脑的地址吗？

c4:23:60:a1:aa:7c，这是我主机的地址。

7. 给出数据帧的十六进制数，这对应于哪个上层协议？

0x0800，表示上层协议为 IPv4。

```
∨ Source: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
    Address: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (facto
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

8. 从以太帧开始到"OK"中的 ASCII 码的"O"字出现间隔的字节数?

16*4+4=68

```
0000  c4 23 60 a1 aa 7c c8 33  e5 8a 5d 45 08 00 45 00   ·#`··|·3 ··]E··E·
0010  05 8c f3 e1 40 00 1b 06  db fb 80 77 f5 0c 64 40   ····@··· ···w··d@
0020  b0 ca 00 50 cd ba b6 17  da d8 4d 82 3d ec 50 10   ···P···· ··M·=·P·
0030  00 ed ed 5d 00 00 48 54  54 50 2f 31 2e 31 20 32   ···]··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D ate: Mon
0050  2c 20 31 31 20 44 65 63  20 32 30 32 33 20 30 36   , 11 Dec  2023 06
0060  3a 31 37 3a 30 32 20 47  4d 54 0d 0a 53 65 72 76   :17:02 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
```

```
Microsoft Windows [Version 10.0.22631.2792]
(c) Microsoft Corporation. All rights reserved.

C:\Users\CindyWu>c:\windows\system32\arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

9. 其中物理地址为 **ff-ff-ff-ff-ff-ff** 的两个为广播地址，物理地址前缀为 **01-00-5e** 的这五个为组播地址，物理地址为 **c8 -33-e5-8a-5d-45** 的为单播地址。

```
Interface: 100.64.176.202 --- 0x8
  Internet Address      Physical Address      Type
  100.64.128.1          c8-33-e5-8a-5d-45     dynamic
  100.64.147.150        c8-33-e5-8a-5d-45     dynamic
  100.64.149.73         c8-33-e5-8a-5d-45     dynamic
  100.64.153.167        c8-33-e5-8a-5d-45     dynamic
  100.64.170.13         c8-33-e5-8a-5d-45     dynamic
  100.64.172.158        c8-33-e5-8a-5d-45     dynamic
  100.64.176.34         c8-33-e5-8a-5d-45     dynamic
  100.64.176.134        c8-33-e5-8a-5d-45     dynamic
  100.64.176.172        c8-33-e5-8a-5d-45     dynamic
  100.64.177.125        c8-33-e5-8a-5d-45     dynamic
  100.64.177.230        c8-33-e5-8a-5d-45     dynamic
  100.64.179.234        c8-33-e5-8a-5d-45     dynamic
  100.64.191.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

No.	Time	Source	Destination	Protocol	Length	Info
313	5.260015	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	ARP	56	Who has 100.64.176.202? Tell 100.64.128.1
314	5.260031	IntelCor_a1:aa:7c	HuaweiTe_8a:5d:45	ARP	42	100.64.176.202 is at c4:23:60:a1:aa:7c
315	5.302320	183.47.101.54	100.64.176.202	OICQ	393	OICQ Protocol
316	5.302743	100.64.176.202	183.47.101.54	OICQ	97	OICQ Protocol
317	5.307721	20.198.147.210	100.64.176.202	TCP	60	443 → 51457 [ACK] Seq=1 Ack=555 Win=64128 Len=0
318	5.309288	20.198.147.210	100.64.176.202	TLSv1.3	1434	Server Hello, Change Cipher Spec, Application Data
319	5.309288	20.198.147.210	100.64.176.202	TCP	1434	443 → 51457 [PSH, ACK] Seq=1381 Ack=555 Win=64128 Len=1380 [TCP segme...
320	5.309288	20.198.147.210	100.64.176.202	TCP	1390	443 → 51457 [PSH, ACK] Seq=2761 Ack=555 Win=64128 Len=1336 [TCP segme...

```
> Frame 313: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on int
v Ethernet II, Src: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45), Dst: IntelCor_a1:a
  v Destination: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
      Address: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (facto
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
      Address: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (facto
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000
> Address Resolution Protocol (request)
```

```
0000  c4 23 60 a1 aa 7c c8 33  e5 8a 5d 45 08 06 00 01   ·#`··|·3 ··]E····
0010  08 00 06 04 00 01 c8 33  e5 8a 5d 45 64 40 80 01   ·······3 ··]Ed@··
0020  c4 23 60 a1 aa 7c 64 40  b0 ca 00 00 00 00 00 00   ·#`··|d@ ········
0030  00 00 00 00 00 00 00 00                            ········
```

10. 包含 ARP 请求消息的以太网帧中源和目标地址的十六进制值是什么？
源地址：c8:33:e5:8a:5d:45   目的地址：c4:23:60:a1:aa:7c

313 5.260015	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	ARP	56
314 5.260031	IntelCor_a1:aa:7c	HuaweiTe_8a:5d:45	ARP	42
315 5.302320	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	0x0800	393
316 5.302743	IntelCor_a1:aa:7c	HuaweiTe_8a:5d:45	0x0800	97
317 5.307721	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	0x0800	66
318 5.309288	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	0x0800	1434
319 5.309288	HuaweiTe_8a:5d:45	IntelCor_a1:aa:7c	0x0800	1434

```
> Frame 313: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on int
∨ Ethernet II, Src: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45), Dst: IntelCor_a1:a
    ∨ Destination: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
        Address: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (facto
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    ∨ Source: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
        Address: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (facto
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Trailer: 00000000000000000000000000000000
> Address Resolution Protocol (request)
```

11. 以太网帧上层协议 16 进制值是什么?

```
        .... ...0 .... .... .... .... = IG
    Type: ARP (0x0806)
    Trailer: 00000000000000000000000000000000
> Address Resolution Protocol (request)
```

0x0806,表示 ARP

12. 回答问题:

1) 分析可知一共有 20 个字节

2) 操作码的值:为 1

3) 包含了发送方的 IP 地址信息吗?:包含了

```
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
Sender IP address: 100.64.128.1
```

4）**ARP 请求中哪里看出要查询 IP 的以太网地址?**

从 TARGET MAC address 和 IP address 可以看出来。

```
Target MAC address: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
Target IP address: 100.64.176.202
```

13.

1）20 个字节

2）操作码的值：为 2

3）

```
Opcode: reply (2)
Sender MAC address: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
Sender IP address: 100.64.176.202
Target MAC address: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
Target IP address: 100.64.128.1
```

14. 源地址：c4:23:60:a1:aa:7c   目的地址： c8:33:e5:8a:5d:45

15. 因为 ARP 查询分组是在广播帧中发送的，而响应分组是单播。

EXTRA1

会导致本地主机无法与该 IP 地址对应的节点建立连接

EXTRA2

```
C:\Users\CindyWu>netsh interface ipv4 show interfaces

Idx     Met        MTU          State                Name
---  ----------  ----------  ------------  -------------------------
  8          35        1500  connected     WLAN
  1          75  4294967295  connected     Loopback Pseudo-Interface 1
 17          65        1500  disconnected  蓝牙网络连接
  6          25        1500  disconnected  本地连接* 3
  4          25        1500  disconnected  本地连接* 4
```

```
C:\Users\CindyWu>netsh interface ipv4 show interface 8

Interface WLAN Parameters
-------------------------------------------------------
IfLuid                                 : wireless_32768
IfIndex                                : 8
State                                  : connected
Metric                                 : 35
Link MTU                               : 1500 bytes
Reachable Time                         : 31500 ms
Base Reachable Time                    : 30000 ms
Retransmission Interval                : 1000 ms
DAD Transmits                          : 3
Site Prefix Length                     : 64
Site Id                                : 1
Forwarding                             : disabled
Advertising                            : disabled
Neighbor Discovery                     : enabled
Neighbor Unreachability Detection      : enabled
Router Discovery                       : dhcp
Managed Address Configuration          : enabled
Other Stateful Configuration           : enabled
Weak Host Sends                        : disabled
Weak Host Receives                     : disabled
Use Automatic Metric                   : enabled
Ignore Default Routes                  : disabled
Advertised Router Lifetime             : 1800 seconds
Advertise Default Route                : disabled
Current Hop Limit                      : 0
Force ARPND Wake up patterns           : disabled
Directed MAC Wake up patterns          : disabled
ECN capability                         : application
RA Based DNS Config (RFC 6106)         : disabled
DHCP/Static IP coexistence             : disabled
```

Basic reachable time 为 30000ms，所求为 30000ms