# 实验报告

院　系　计算机学院　　学号　19335174　　姓名　施天予

班　级　19

【实验题目】WireShark **实验**

【实验目的】通过 WireShark 分析 IP 协议(Option)、ICMP 协议、ARP 协议、DHCP 协议、DNS 协议、TCP 协议。

【注意事项】

多个包要截一个**总图**（排序或用 ICMP 作为过滤条件），例如：

```
 7 1.87487500 192.168.0.8    10.22.16.201   ICMP   114 Echo (ping) request  id=0x0001, seq=11700/46125, ttl=64 (reply in 8)
 8 1.88007700 10.22.16.201   192.168.0.8    ICMP   114 Echo (ping) reply    id=0x0001, seq=11700/46125, ttl=252 (request in 7)
11 2.88836800 192.168.0.8    10.22.16.201   ICMP   114 Echo (ping) request  id=0x0001, seq=11701/46381, ttl=64 (reply in 12)
12 2.89294600 10.22.16.201   192.168.0.8    ICMP   114 Echo (ping) reply    id=0x0001, seq=11701/46381, ttl=252 (request in 11)
17 3.94400800 192.168.0.8    10.22.16.201   ICMP   114 Echo (ping) request  id=0x0001, seq=11702/46637, ttl=64 (no response found!)
18 3.94981900 10.22.16.201   192.168.0.8    ICMP   114 Echo (ping) reply    id=0x0001, seq=11702/46637, ttl=252 (request in 17)
20 4.99512300 192.168.0.8    10.22.16.201   ICMP   114 Echo (ping) request  id=0x0001, seq=11703/46893, ttl=64 (reply in 21)
21 5.00011300 10.22.16.201   192.168.0.8    ICMP   114 Echo (ping) reply    id=0x0001, seq=11703/46893, ttl=252 (request in 20)
```

所有截包要求展开 IP 协议和内部协议，如果有多个，只用选择其中一个，例如：

```
Ethernet II, Src: 60:6d:c7:c6:68:21 (60:6d:c7:c6:68:21), Dst: 1c:68:7e:c2:36:c5 (1c:68:7e:c2:36:c5)
Internet Protocol Version 4, Src: 192.168.0.8 (192.168.0.8), Dst: 10.22.16.201 (10.22.16.201)
    Version: 4
    Header Length: 60 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 100
    Identification: 0xd1e3 (53731)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x7a01 [validation disabled]
    Source: 192.168.0.8 (192.168.0.8)
    Destination: 10.22.16.201 (10.22.16.201)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊟ Options: (40 bytes), Time Stamp, End of Options List (EOL)
    ⊟ Time Stamp (36 bytes)
      ⊞ Type: 68
        Length: 36
        Pointer: 5
        Overflow: 0
        Flag: Time stamp and address
        Address = -, time stamp = 0
        Address = -, time stamp = 0
        Address = -, time stamp = 0
        Address = -, time stamp = 0
      ⊞ End of Options List (EOL)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x1fa7 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 11700 (0x2db4)
    Sequence number (LE): 46125 (0xb42d)
    [Response frame: 8]
  ⊟ Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
      [Length: 32]
```

BE = 大端序

LE = 小端序

上面分别用 BE 和 LE 表示同一个数，这里是 BE 有效（本来 Intel 采用 LE，不知道这里为什么是 BE 有效）。

注意每一步都要保存截包文件

过滤条件：ip.addr == 172.18.187.251 && tcp.port==59161　（具体的可以见 WireShark.pdf）

【实验任务】

1、 (IP.pcapng)IP Option 和 ICMP 协议。

**命令：ping -r 4 域名**

[Ping 总图]

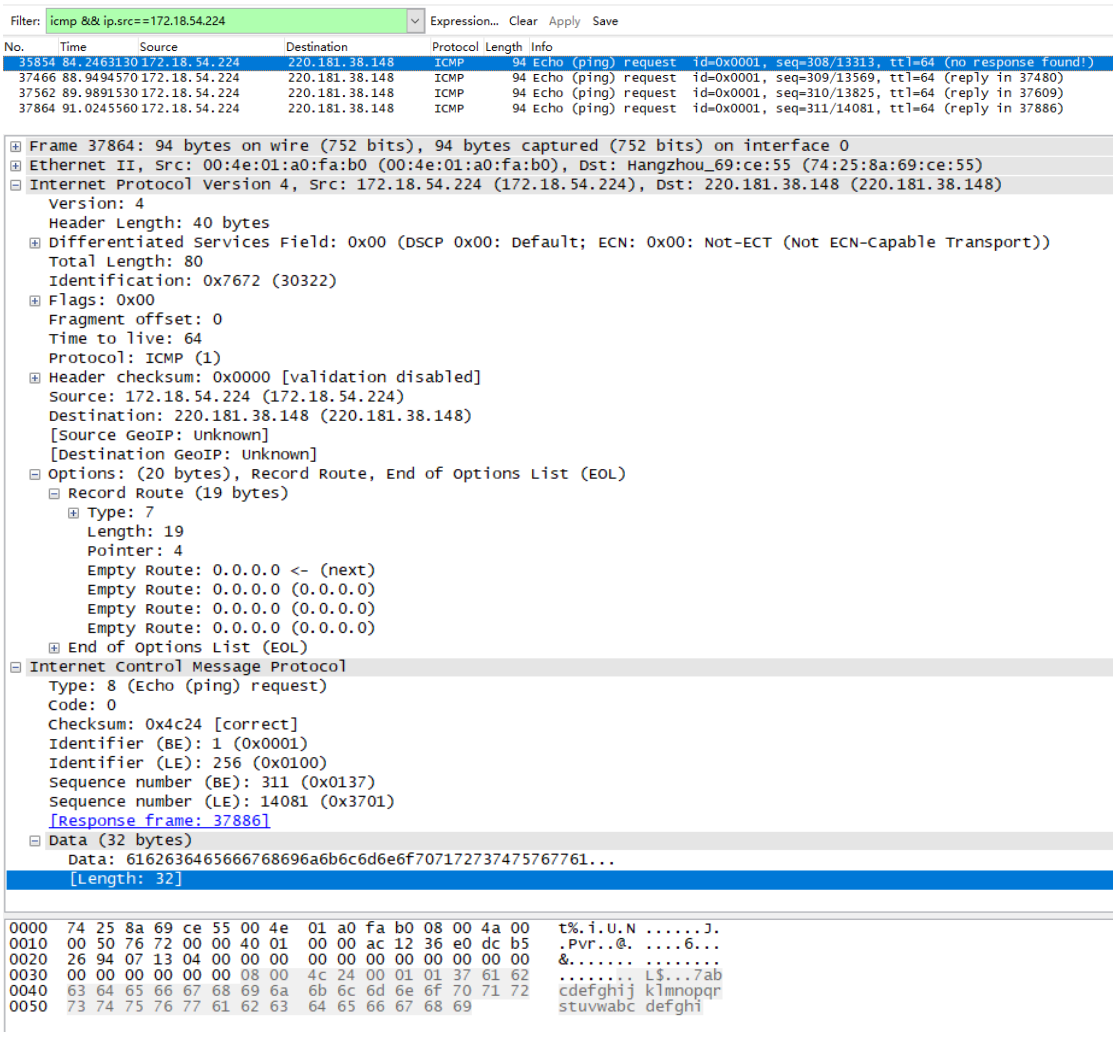
Filter: icmp && ip.addr==172.18.54.224　Expression... Clear Apply Save

```
No.   Time        Source          Destination     Protocol Length Info
35854 84.2463130  172.18.54.224   220.181.38.148  ICMP       94 Echo (ping) request  id=0x0001, seq=308/13313, ttl=64 (no response found!)
37466 88.9494570  172.18.54.224   220.181.38.148  ICMP       94 Echo (ping) request  id=0x0001, seq=309/13569, ttl=64 (reply in 37480)
37480 89.0828250  220.181.38.148  172.18.54.224   ICMP       94 Echo (ping) reply    id=0x0001, seq=309/13569, ttl=47 (request in 37466)
37562 89.9891530  172.18.54.224   220.181.38.148  ICMP       94 Echo (ping) request  id=0x0001, seq=310/13825, ttl=64 (reply in 37609)
37609 90.0810250  220.181.38.148  172.18.54.224   ICMP       94 Echo (ping) reply    id=0x0001, seq=310/13825, ttl=47 (request in 37562)
37864 91.0245560  172.18.54.224   220.181.38.148  ICMP       94 Echo (ping) request  id=0x0001, seq=311/14081, ttl=64 (reply in 37886)
37886 91.1221140  220.181.38.148  172.18.54.224   ICMP       94 Echo (ping) reply    id=0x0001, seq=311/14081, ttl=47 (request in 37864)
```

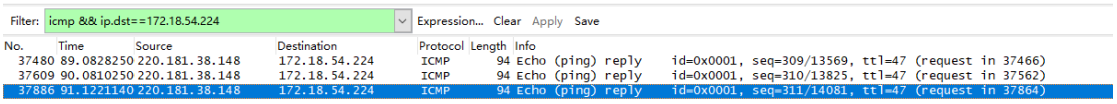
# 实验报告

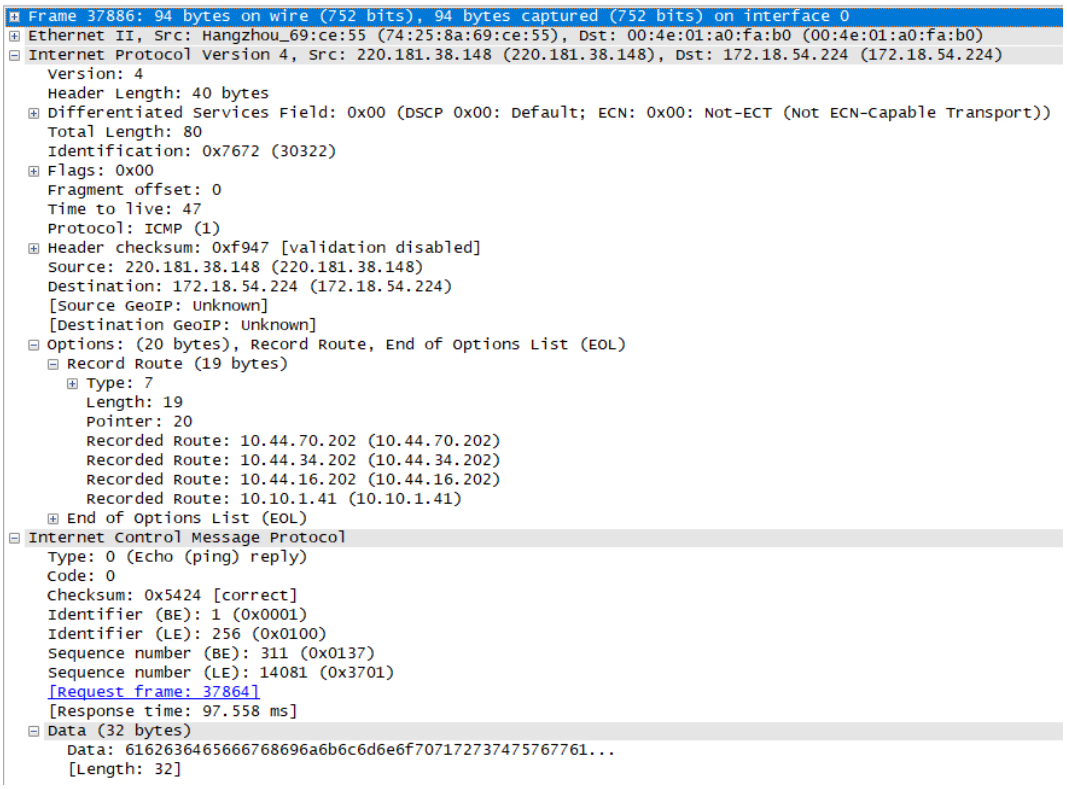
```
C:\Users\DELL>ping -r 4 baidu.com

正在 Ping baidu.com [220.181.38.148] 具有 32 字节的数据:
请求超时。
来自 220.181.38.148 的回复: 字节=32 时间=133ms TTL=47
    路由: 10.44.70.202 ->
          10.44.34.202 ->
          10.44.16.202 ->
          10.10.1.41
来自 220.181.38.148 的回复: 字节=32 时间=92ms TTL=47
    路由: 10.44.70.202 ->
          10.44.34.202 ->
          10.44.16.202 ->
          10.10.1.41
来自 220.181.38.148 的回复: 字节=32 时间=97ms TTL=47
    路由: 10.44.70.202 ->
          10.44.34.202 ->
          10.44.16.202 ->
          10.10.1.41

220.181.38.148 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 3, 丢失 = 1 (25% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 92ms, 最长 = 133ms, 平均 = 107ms
```

[Ping 请求包截屏]



[Ping 响应包截屏]




[针对于所截包的问题]

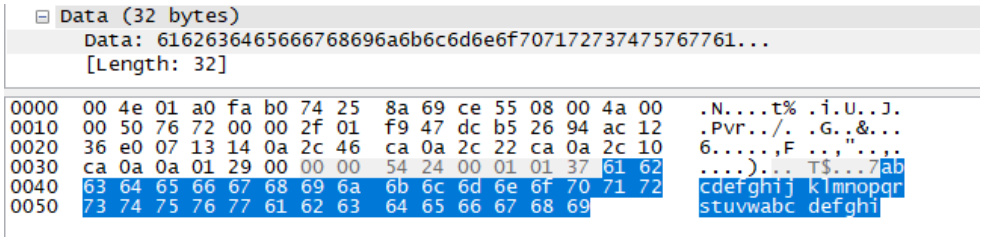
IP 选项的长度：20 bytes

ICMP 包的 Identifier：1

ICMP 包的序号：311

ICMP 包的数据部分长度：32 bytes

ICMP 包的数据部分的内容：



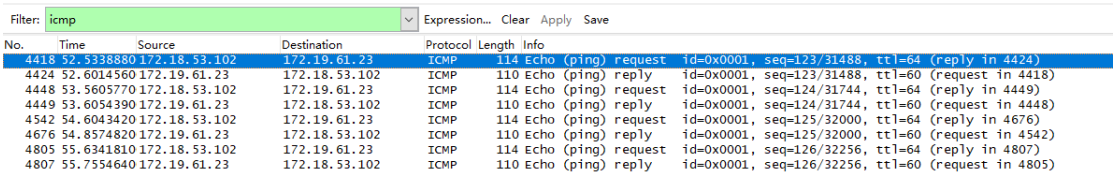

蓝色的是数据部分内容，左边十六进制表示，右边字符表示。

Identifier 是什么含义？

Identifier 是用来区分不同的 PING 进程地。但在 Windows 中 icmp Identifier 固定不变，windows 系统不根据 Identifier 来区别 ping 进程，它是根据 Sequence Number field 来区分的。

命令：ping -s 4 域名

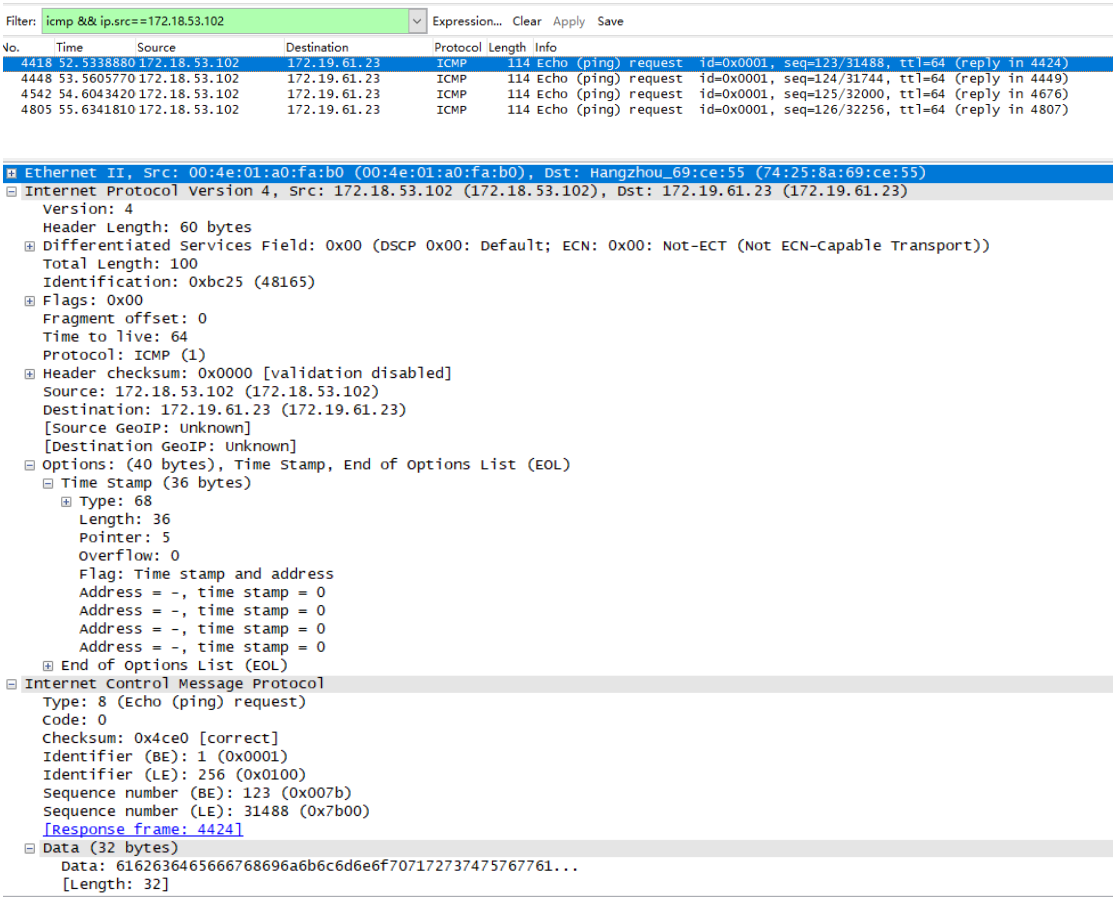
[Ping 总图]



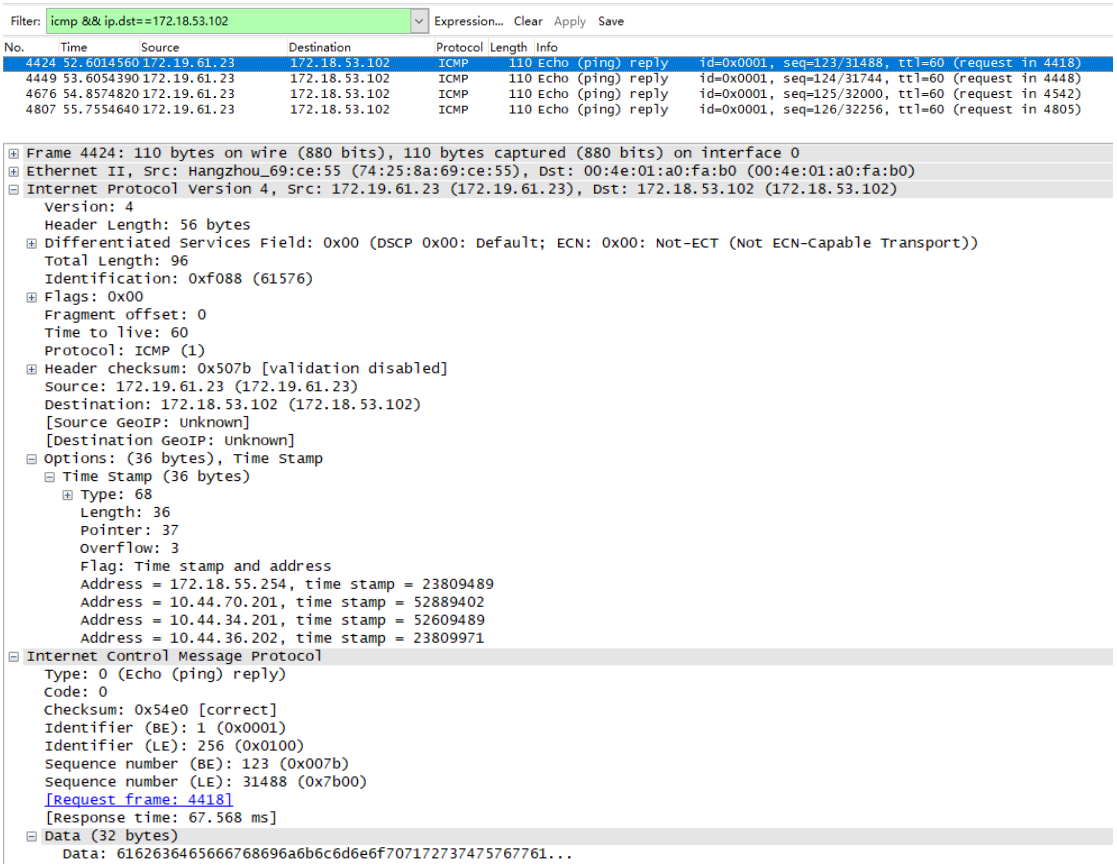
# 实验报告

```
C:\Users\DELL>ping -s 4 172.19.61.23

正在 Ping 172.19.61.23 具有 32 字节的数据:
来自 172.19.61.23 的回复: 字节=32 时间=67ms TTL=60
    时间戳: 172.18.55.254 : 23809489 ->
                  10.44.70.201 : 52889402 ->
                  10.44.34.201 : 52609489 ->
                  10.44.36.202 : 23809971
来自 172.19.61.23 的回复: 字节=32 时间=45ms TTL=60
    时间戳: 172.18.55.254 : 23810516 ->
                  10.44.70.201 : 52890432 ->
                  10.44.34.201 : 52610509 ->
                  10.44.36.202 : 23811000
来自 172.19.61.23 的回复: 字节=32 时间=253ms TTL=60
    时间戳: 172.18.55.254 : 23811560 ->
                  10.44.70.201 : 52891482 ->
                  10.44.34.201 : 52611559 ->
                  10.44.36.202 : 23812065
来自 172.19.61.23 的回复: 字节=32 时间=121ms TTL=60
    时间戳: 172.18.55.254 : 23812590 ->
                  10.44.70.201 : 52892502 ->
                  10.44.34.201 : 52612599 ->
                  10.44.36.202 : 23813084

172.19.61.23 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 45ms, 最长 = 253ms, 平均 = 121ms
```

[Ping 请求包截屏]



[Ping 响应包截屏]



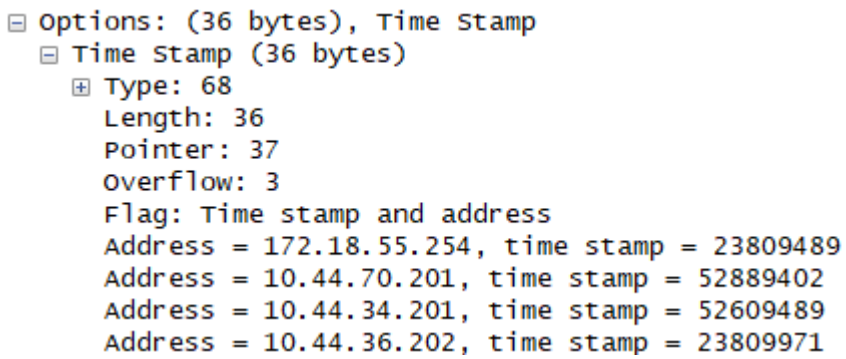

[问题]

IP 选项的长度：36 bytes

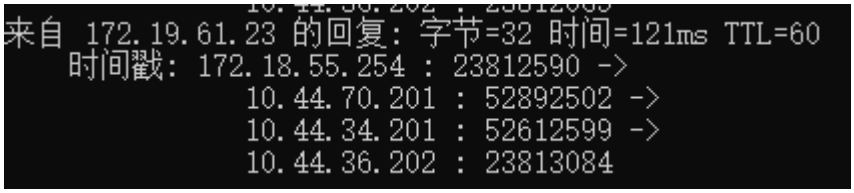
选项中的时间戳是否正确？

正确！

选项中的时间戳：




Ping 后的时间戳：



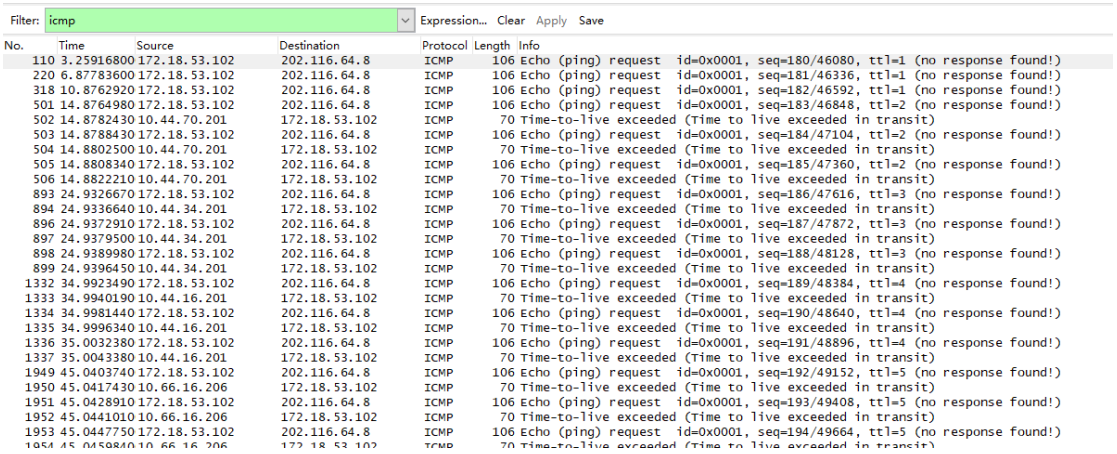

可以发现结果一致！

2、 (tracert.pcapng) ICMP 协议

命令：tracert -h 8 域名 （tracert -h 8 www.sysu.edu.cn）

# 实验报告

[tracert 总图截屏]

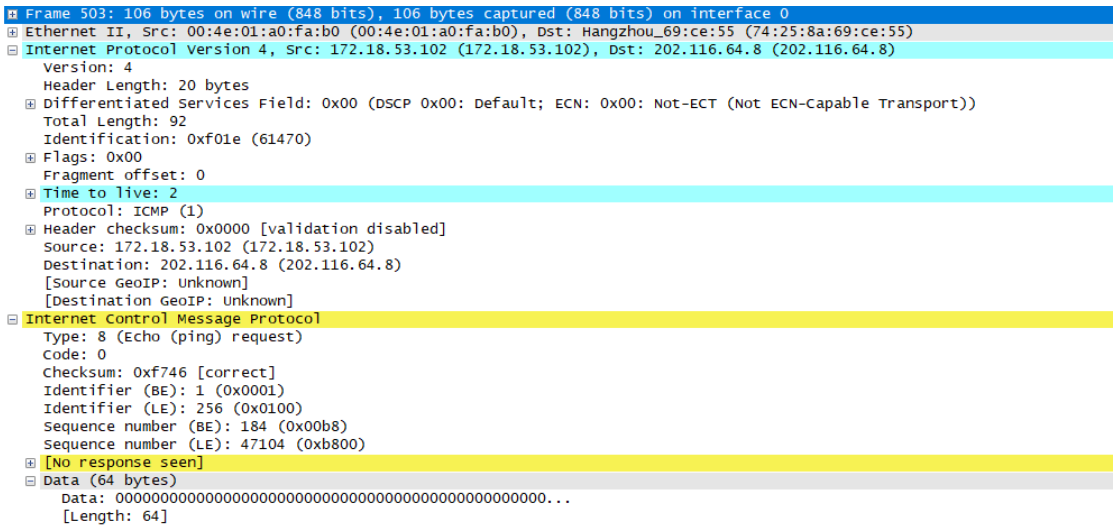


Filter: icmp  Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 110 | 3.25916800 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=180/46080, ttl=1 (no response found!) |
| 220 | 6.87783600 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=181/46336, ttl=1 (no response found!) |
| 318 | 10.8762920 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=182/46592, ttl=1 (no response found!) |
| 501 | 14.8764980 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=183/46848, ttl=2 (no response found!) |
| 502 | 14.8782430 | 10.44.70.201 | 172.18.53.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 503 | 14.8788430 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=184/47104, ttl=2 (no response found!) |
| 504 | 14.8802500 | 10.44.70.201 | 172.18.53.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 505 | 14.8808340 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=185/47360, ttl=2 (no response found!) |
| 506 | 14.8822210 | 10.44.70.201 | 172.18.53.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 893 | 24.9326670 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=186/47616, ttl=3 (no response found!) |
| 894 | 24.9336640 | 10.44.34.201 | 172.18.53.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 896 | 24.9372910 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=187/47872, ttl=3 (no response found!) |
| 897 | 24.9379500 | 10.44.34.201 | 172.18.53.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 898 | 24.9389980 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=188/48128, ttl=3 (no response found!) |
| 899 | 24.9396450 | 10.44.34.201 | 172.18.53.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 1332 | 34.9923490 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=189/48384, ttl=4 (no response found!) |
| 1333 | 34.9940190 | 10.44.16.201 | 172.18.53.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 1334 | 34.9981440 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=190/48640, ttl=4 (no response found!) |
| 1335 | 34.9996340 | 10.44.16.201 | 172.18.53.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 1336 | 35.0032380 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=191/48896, ttl=4 (no response found!) |
| 1337 | 35.0043380 | 10.44.16.201 | 172.18.53.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 1949 | 45.0403740 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=192/49152, ttl=5 (no response found!) |
| 1950 | 45.0417430 | 10.66.16.206 | 172.18.53.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 1951 | 45.0428910 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=193/49408, ttl=5 (no response found!) |
| 1952 | 45.0441010 | 10.66.16.206 | 172.18.53.102 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 1953 | 45.0447750 | 172.18.53.102 | 202.116.64.8 | ICMP | 106 | Echo (ping) request id=0x0001, seq=194/49664, ttl=5 (no response found!) |

```
C:\Users\DELL>tracert -h 8 -4 www.sysu.edu.cn

通过最多 8 个跃点跟踪
到 pisces-1.sysu.edu.cn [202.116.64.8] 的路由:

  1     *        *        *     请求超时。
  2     1 ms     1 ms     1 ms  10.44.70.201
  3     1 ms    <1 毫秒   <1 毫秒 10.44.34.201
  4     2 ms     1 ms     1 ms  10.44.16.201
  5     1 ms     1 ms     1 ms  10.66.16.206
  6     *        *        *     请求超时。
  7     1 ms     1 ms     4 ms  pisces-1.sysu.edu.cn [202.116.64.8]

跟踪完成。
```

[TTL=2 的第二个 Ping 请求包截屏]　*可以选其他包，但是要修改一下 *2 和二*



```
Frame 503: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
Ethernet II, Src: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0), Dst: Hangzhou_69:ce:55 (74:25:8a:69:ce:55)
Internet Protocol Version 4, Src: 172.18.53.102 (172.18.53.102), Dst: 202.116.64.8 (202.116.64.8)
    Version: 4
    Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 92
    Identification: 0xf01e (61470)
  Flags: 0x00
    Fragment offset: 0
  Time to live: 2
    Protocol: ICMP (1)
  Header checksum: 0x0000 [validation disabled]
    Source: 172.18.53.102 (172.18.53.102)
    Destination: 202.116.64.8 (202.116.64.8)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf746 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 184 (0x00b8)
    Sequence number (LE): 47104 (0xb800)
  [No response seen]
  Data (64 bytes)
      Data: 0000000000000000000000000000000000000000000000000000...
      [Length: 64]
```

[对应响应包截屏]

```
⊞ Frame 504: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
⊞ Ethernet II, Src: Hangzhou_69:ce:55 (74:25:8a:69:ce:55), Dst: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
⊟ Internet Protocol Version 4, Src: 10.44.70.201 (10.44.70.201), Dst: 172.18.53.102 (172.18.53.102)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 56
    Identification: 0xfade (64222)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 254
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x8eb8 [validation disabled]
    Source: 10.44.70.201 (10.44.70.201)
    Destination: 172.18.53.102 (172.18.53.102)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
  ⊟ Internet Protocol Version 4, Src: 172.18.53.102 (172.18.53.102), Dst: 202.116.64.8 (202.116.64.8)
      Version: 4
      Header Length: 20 bytes
    ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
      Total Length: 92
      Identification: 0xf01e (61470)
    ⊞ Flags: 0x00
      Fragment offset: 0
    ⊞ Time to live: 1
      Protocol: ICMP (1)
    ⊞ Header checksum: 0xdd8d [validation disabled]
      Source: 172.18.53.102 (172.18.53.102)
      Destination: 202.116.64.8 (202.116.64.8)
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
  ⊟ Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xf746
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence number (BE): 184 (0x00b8)
      Sequence number (LE): 47104 (0xb800)
```

[说明 tracert 的基本原理]

Tracert 是利用 ICMP 和 TTL 进行工作的。首先 tracert 会发出 TTL 值为 1 的 ICMP 数据报（包含 40 个字节，包括源地址、目标地址和发出的时间标签，一般会连续发 3 个包）。

Tracert 每次发出数据报时便会将 TTL 加 1（一般每次都是发 3 个数据报），来发现下一个路由器。这个动作一直重复，直到到达目的地或者确定目标主机不可到达为止。当数据报到达目的地后，目标主机并不返回超时回应数据报。当到达目的地后，目标主机会返回一个 ICMP port unreachable（端口不可达）的消息。当 tracert 收到这个消息后，就知道目的地已经到达了。

Tracert 会提取 ICMP 的超时回应数据报中的 IP 地址并作主机名解析（用-d 参数表示不解析主机名，解析主机名会耽误一些时间），然后将所经过的路由器的主机名及 IP 地址、数据报每次往返花费的时间显示出来。

通过 tracert 命令，我们便知道源地址到目的地址所经过的路径。在目标主机响应时，tracert 会显示完整的经过的路由及到每个路由所花费的时间。如果目标主机没有响应，tracert 仍会尝试寻找所经过的路径。

3、 (arp.pcapng)ARP 协议。

命令：arp -a （查看）

arp -d 192.168.0.14 （删除）

ping 默认网关或同学的电脑：先查看 ARP 缓存，删掉这台电脑的映射，然后启动截包，再 ping 它

[总图]

先 Ping 一台电脑 172.18.54.107

```
C:\Users\DELL>ping 172.18.54.107

正在 Ping 172.18.54.107 具有 32 字节的数据:
来自 172.18.54.107 的回复: 字节=32 时间<1ms TTL=128
来自 172.18.54.107 的回复: 字节=32 时间<1ms TTL=128
来自 172.18.54.107 的回复: 字节=32 时间<1ms TTL=128
来自 172.18.54.107 的回复: 字节=32 时间=1ms TTL=128

172.18.54.107 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

查看 ARP 缓存

```
172.18.54.90          2c-56-dc-35-df-80     动态
172.18.54.92          00-d8-61-6f-81-2d     动态
172.18.54.93          e8-6a-64-2b-5e-17     动态
172.18.54.94          e8-6a-64-33-2c-24     动态
172.18.54.107         8c-16-45-e4-8d-3f     动态
172.18.54.111         2c-f0-5d-a1-12-67     动态
172.18.54.115         4c-ed-fb-16-41-ba     动态
```

删除后 172.18.54.107 不存在

```
172.18.54.93          e8-6a-64-2b-5e-17     动态
172.18.54.94          e8-6a-64-33-2c-24     动态
172.18.54.111         2c-f0-5d-a1-12-67     动态
172.18.54.115         4c-ed-fb-16-41-ba     动态
```

总图

```
1127 21.2839030 00:4e:01:a0:fa:b0  Broadcast          ARP       42 Who has 172.18.54.107?  Tell 172.18.53.102
1128 21.2841720 8c:16:45:e4:8d:3f  00:4e:01:a0:fa:b0  ARP       60 172.18.54.107 is at 8c:16:45:e4:8d:3f
1129 21.2842070 172.18.53.102      172.18.54.107      ICMP      74 Echo (ping) request  id=0x0001, seq=223/57088, ttl=64 (reply in 1130)
1130 21.2848380 172.18.54.107      172.18.53.102      ICMP      74 Echo (ping) reply    id=0x0001, seq=223/57088, ttl=128 (request in 1129)
1153 22.2940720 172.18.53.102      172.18.54.107      ICMP      74 Echo (ping) request  id=0x0001, seq=224/57344, ttl=64 (reply in 1154)
1154 22.2950930 172.18.54.107      172.18.53.102      ICMP      74 Echo (ping) reply    id=0x0001, seq=224/57344, ttl=128 (request in 1153)
```

[ARP 请求包截屏] 用红线标出 ARP 协议中要查询的 IP 地址

```
⊞ Frame 1127: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
⊞ Ethernet II, Src: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
    Sender IP address: 172.18.53.102 (172.18.53.102)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.18.54.107 (172.18.54.107)
```

[ARP 响应包截屏]用红线标出所查询的 IP 地址对应的 MAC 地址

```
⊞ Frame 1128: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: 8c:16:45:e4:8d:3f (8c:16:45:e4:8d:3f), Dst: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 8c:16:45:e4:8d:3f (8c:16:45:e4:8d:3f)
    Sender IP address: 172.18.54.107 (172.18.54.107)
    Target MAC address: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
    Target IP address: 172.18.53.102 (172.18.53.102)
```

[找到一个 Gratuitous ARP 包截屏]

* 如果没有，可以试一下可以重新配置一个新的 IP 地址，再找不到就算了。

**没找到。。。**

[问题]

当 ARP 缓存没有映射时，系统对要发送的 IP 分组会怎么做？

**先广播一个 ARP 包查询这个 IP 地址对应的物理地址的映射**

ARP 协议是否采用了超时重传？

**没有**

Gratuitous ARP 包有什么用途？

**Gratuitous ARP 不同于一般的 ARP 请求，它并非想得到 IP 对应的 MAC 地址，而是当主机启动的时候，发送一个 Gratuitous arp 请求自己的 IP 地址的 MAC 地址。**

**（1）Gratuitous ARP 可以用来验证主机是否冲突**

**一个主机可以通过它来确定另一个主机是否设置了相同的 IP 地址。发送主机并不需要一定收到此请求的回答。如果收到一个回答，表示网络中存在与自身 IP 相同的主机。如果没有收到应答，则表示本机所**

使用的 IP 与网络中其它主机并不冲突。

（2）更换物理网卡

如果发送 ARP 的主机正好改变了物理地址（如更换物理网卡），可以使用此方法通知网络中其它主机及时更新 ARP 缓存。

4、 (DHCP.pcapng)DHCP 协议（ipconfig /release 清除网络配置，ipconfig /renew）

[总图]

```
625 15.8123980 0.0.0.0          255.255.255.255    DHCP    344 DHCP Discover - Transaction ID 0x69dc0ec0
706 16.8212710 172.18.55.254    172.18.54.224      DHCP    342 DHCP Offer    - Transaction ID 0x69dc0ec0
707 16.8229410 0.0.0.0          255.255.255.255    DHCP    370 DHCP Request  - Transaction ID 0x69dc0ec0
708 16.8324730 172.18.55.254    172.18.54.224      DHCP    342 DHCP ACK      - Transaction ID 0x69dc0ec0
```

[四个包]

Discover

```
954 × 936
Frame 625: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface 0
⊞ Ethernet II, Src: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊟ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 330
    Identification: 0xc356 (50006)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  ⊞ Header checksum: 0x0000 [validation disabled]
    Source: 0.0.0.0 (0.0.0.0)
    Destination: 255.255.255.255 (255.255.255.255)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
    Source Port: 68 (68)
    Destination Port: 67 (67)
    Length: 310
  ⊞ Checksum: 0x05d1 [validation disabled]
    [Stream index: 130]
⊟ Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x69dc0ec0
  ⊞ Seconds elapsed: 4
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
    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: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
  ⊟ Option: (50) Requested IP Address
      Length: 4
      Requested IP Address: 172.18.54.224 (172.18.54.224)
  ⊟ Option: (12) Host Name
      Length: 15
      Host Name: DESKTOP-I64VLE6
  ⊟ Option: (60) Vendor class identifier
      Length: 8
      Vendor class identifier: MSFT 5.0
  ⊟ Option: (55) Parameter Request List
      Length: 14
      Vendor class identifier: MSFT 5.0
      Parameter Request List Item: (3) Router
      Parameter Request List Item: (6) Domain Name Server
      Parameter Request List Item: (1) Subnet Mask
      Parameter Request List Item: (31) Perform Router Discover
      Parameter Request List Item: (33) Static Route
      Parameter Request List Item: (15) Domain Name
      Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
      Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
      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
      Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
      Parameter Request List Item: (119) Domain Search
      Parameter Request List Item: (121) Classless Static Route
```

Offer

887 × 961 1271000 172.18.55.254 172.18.54.224 DHCP 342 DHCP Offer - Transaction ID 0x69dc0ec0

```
Frame 706: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Hangzhou_69:ce:55 (74:25:8a:69:ce:55), Dst: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
Internet Protocol Version 4, Src: 172.18.55.254 (172.18.55.254), Dst: 172.18.54.224 (172.18.54.224)
    Version: 4
    Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 328
    Identification: 0x8797 (34711)
  Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
  Header checksum: 0x6c0a [validation disabled]
    Source: 172.18.55.254 (172.18.55.254)
    Destination: 172.18.54.224 (172.18.54.224)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
    Source Port: 67 (67)
    Destination Port: 68 (68)
    Length: 308
  Checksum: 0x5327 [validation disabled]
    [Stream index: 192]
Bootstrap Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x69dc0ec0
  Seconds elapsed: 4
  Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 172.18.54.224 (172.18.54.224)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 172.18.55.254 (172.18.55.254)
    Client MAC address: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  Option: (53) DHCP Message Type (Offer)
      Length: 1
      DHCP: Offer (2)
  Option: (54) DHCP Server Identifier
      Length: 4
      DHCP Server Identifier: 125.217.174.123 (125.217.174.123)
  Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (3600s) 1 hour
  Option: (1) Subnet Mask
      Length: 4
      Subnet Mask: 255.255.252.0 (255.255.252.0)
  Option: (3) Router
      Length: 4
      Router: 172.18.55.254 (172.18.55.254)
  Option: (6) Domain Name Server
      Length: 8
      Domain Name Server: 10.8.4.4 (10.8.4.4)
      Domain Name Server: 10.8.8.8 (10.8.8.8)
  Option: (255) End
      Option End: 255
    Padding
```

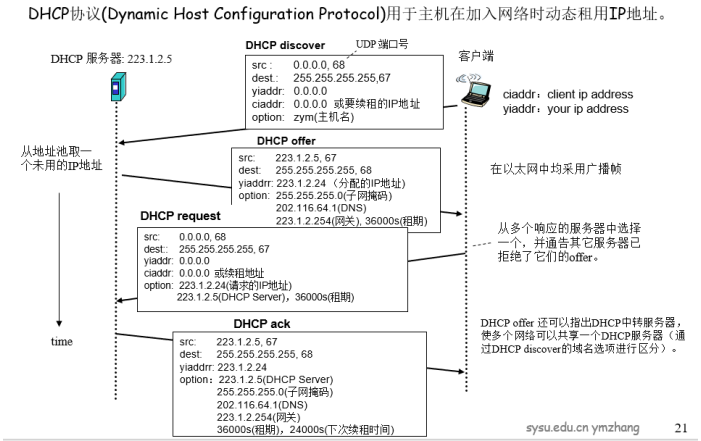
## Request

```
Frame 707: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface 0
Ethernet II, Src: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
    Version: 4
    Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 356
    Identification: 0xc357 (50007)
  Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  Header checksum: 0x0000 [validation disabled]
    Source: 0.0.0.0 (0.0.0.0)
    Destination: 255.255.255.255 (255.255.255.255)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
    Source Port: 68 (68)
    Destination Port: 67 (67)
    Length: 336
  Checksum: 0x5313 [validation disabled]
    [Stream index: 130]
Bootstrap Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x69dc0ec0
  Seconds elapsed: 4
  Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  Option: (53) DHCP Message Type (Request)
      Length: 1
      DHCP: Request (3)
  Option: (61) Client identifier
      Length: 7
      Hardware type: Ethernet (0x01)
      Client MAC address: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
  Option: (50) Requested IP Address
      Length: 4
      Requested IP Address: 172.18.54.224 (172.18.54.224)
  Option: (54) DHCP Server Identifier
      Length: 4
      DHCP Server Identifier: 125.217.174.123 (125.217.174.123)
  Option: (12) Host Name
      Length: 15
      Host Name: DESKTOP-I64VLE6
  Option: (81) Client Fully Qualified Domain Name
      Length: 18
      Flags: 0x00
      0000 .... = Reserved flags: 0x00
      .... 0... = Server DDNS: Some server updates
      .... .0.. = Encoding: ASCII encoding
      .... ..0. = Server overrides: No override
      .... ...0 = Server: Client
      A-RR result: 0
      PTR-RR result: 0
      Client name: DESKTOP-I64VLE6
  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
      Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
      Parameter Request List Item: (119) Domain Search
      Parameter Request List Item: (121) Classless Static Route
      Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
      Parameter Request List Item: (252) Private/Proxy autodiscovery
  Option: (255) End
      Option End: 255
```

## Ack

```
884 × 937708: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
⊞ Ethernet II, Src: Hangzhou_69:ce:55 (74:25:8a:69:ce:55), Dst: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
⊟ Internet Protocol Version 4, Src: 172.18.55.254 (172.18.55.254), Dst: 172.18.54.224 (172.18.54.224)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 328
    Identification: 0x879a (34714)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
  ⊞ Header checksum: 0x6c07 [validation disabled]
    Source: 172.18.55.254 (172.18.55.254)
    Destination: 172.18.54.224 (172.18.54.224)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
    Source Port: 67 (67)
    Destination Port: 68 (68)
    Length: 308
  ⊞ Checksum: 0x5027 [validation disabled]
    [Stream index: 192]
⊟ Bootstrap Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x69dc0ec0
  ⊞ Seconds elapsed: 4
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 172.18.54.224 (172.18.54.224)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 172.18.55.254 (172.18.55.254)
    Client MAC address: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊟ Option: (53) DHCP Message Type (ACK)
      Length: 1
      DHCP: ACK (5)
  ⊟ Option: (54) DHCP Server Identifier
      Length: 4
      DHCP Server Identifier: 125.217.174.123 (125.217.174.123)
  ⊟ Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (3600s) 1 hour
  ⊟ Option: (1) Subnet Mask
      Length: 4
      Subnet Mask: 255.255.252.0 (255.255.252.0)
  ⊟ Option: (3) Router
      Length: 4
      Router: 172.18.55.254 (172.18.55.254)
  ⊟ Option: (6) Domain Name Server
      Length: 8
      Domain Name Server: 10.8.4.4 (10.8.4.4)
      Domain Name Server: 10.8.8.8 (10.8.8.8)
  ⊟ Option: (255) End
      Option End: 255
    Padding
```

[对照课件]




有没有可以纠正的内容？有的话写出来。

在课件中的 DHCP offer 和 ack 是广播帧，但是在我这里其实是单播。同时课件上的租期是 36000s，而我这里实际上是 3600s.

5、 (DNS.pcapng)DNS 协议

先 ping img01.sogoucdn.com 并截屏：

```
C:\Users\DELL>ping img01.sogoucdn.com

正在 Ping 10099.stsougou.cdntip.com [117.169.98.75] 具有 32 字节的数据:
来自 117.169.98.75 的回复: 字节=32 时间=59ms TTL=51
来自 117.169.98.75 的回复: 字节=32 时间=63ms TTL=51
来自 117.169.98.75 的回复: 字节=32 时间=67ms TTL=51
来自 117.169.98.75 的回复: 字节=32 时间=41ms TTL=51

117.169.98.75 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 41ms, 最长 = 67ms, 平均 = 57ms
```

然后,在控制台用 C:>ipconfig /displaydns 查看 DNS 缓存,并截屏 img01.sogoucdn.com 的 DNS 记录:

```
  img01.sogoucdn.com
  ----------------------------------------
  记录名称. . . . . : img01.sogoucdn.com
  记录类型. . . . . : 5
  生存时间. . . . . : 146
  数据长度. . . . . : 8
  部分. . . . . : 答案
  CNAME 记录  . . . . . : img01.sogoucdn.com.cdn.dnsv1.com


  记录名称. . . . . : img01.sogoucdn.com.cdn.dnsv1.com
  记录类型. . . . . : 5
  生存时间. . . . . : 146
  数据长度. . . . . : 8
  部分. . . . . : 答案
  CNAME 记录  . . . . . : 10099.stsougou.cdntip.com


  记录名称. . . . . : 10099.stsougou.cdntip.com
  记录类型. . . . . : 1
  生存时间. . . . . : 146
  数据长度. . . . . : 4
  部分. . . . . : 答案
  A (主机)记录  . . . . : 117.169.98.75


  记录名称. . . . . : 10099.stsougou.cdntip.com
  记录类型. . . . . : 1
  生存时间. . . . . : 146
  数据长度. . . . . : 4
  部分. . . . . : 答案
  A (主机)记录  . . . . : 120.226.27.14


  记录名称. . . . . : 10099.stsougou.cdntip.com
  记录类型. . . . . : 1
  生存时间. . . . . : 146
  数据长度. . . . . : 4
  部分. . . . . : 答案
  A (主机)记录  . . . . : 36.158.190.246


  记录名称. . . . . : 10099.stsougou.cdntip.com
  记录类型. . . . . : 1
  生存时间. . . . . : 146
  数据长度. . . . . : 4
  部分. . . . . : 答案
  A (主机)记录  . . . . : 36.159.127.22
```

解释其中内容（说明如何可以从 DNS 记录中得到 img01.sogoucdn.com 的 IP 地址）：

```
记录名称. . . . . : img01.sogoucdn.com
记录类型. . . . . : 5
生存时间. . . . . : 146
数据长度. . . . . : 8
部分. . . . . : 答案
CNAME 记录 . . . . . : img01.sogoucdn.com.cdn.dnsv1.com
```

DNS 查询 img01.sogoucdn.com 的主机名要去 img01.sogoucdn.com.cdn.dnsv1.com 的记录查找

```
记录名称. . . . . : img01.sogoucdn.com.cdn.dnsv1.com
记录类型. . . . . : 5
生存时间. . . . . : 146
数据长度. . . . . : 8
部分. . . . . : 答案
CNAME 记录 . . . . . : 10099.stsougou.cdntip.com
```

DNS 查询 img01.sogoucdn.com.cdn.dnsv1.com 说要到 10099.stsougou.cdntip.com 去查询主机名

```
记录名称. . . . . : 10099.stsougou.cdntip.com
记录类型. . . . . : 1
生存时间. . . . . : 146
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 117.169.98.75

记录名称. . . . . : 10099.stsougou.cdntip.com
记录类型. . . . . : 1
生存时间. . . . . : 146
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 120.226.27.14

记录名称. . . . . : 10099.stsougou.cdntip.com
记录类型. . . . . : 1
生存时间. . . . . : 146
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 36.158.190.246

记录名称. . . . . : 10099.stsougou.cdntip.com
记录类型. . . . . : 1
生存时间. . . . . : 146
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 36.159.127.22
```

这些记录返回了 img01.sogoucdn.com 的 IP 地址

清除 DNS 记录：C:>ipconfig /flushdns 后，再 ping img01.sogoucdn.com 并截包：

[DNS 查询包]

```
Frame 835: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0), Dst: Hangzhou_69:ce:55 (74:25:8a:69:ce:55)
Internet Protocol Version 4, Src: 172.18.54.224 (172.18.54.224), Dst: 10.8.4.4 (10.8.4.4)
    Version: 4
    Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 64
    Identification: 0x9968 (39272)
  Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  Header checksum: 0x0000 [validation disabled]
    Source: 172.18.54.224 (172.18.54.224)
    Destination: 10.8.4.4 (10.8.4.4)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 58358 (58358), Dst Port: 53 (53)
    Source Port: 58358 (58358)
    Destination Port: 53 (53)
    Length: 44
  Checksum: 0xf13b [validation disabled]
    [Stream index: 46]
Domain Name System (query)
    [Response In: 837]
    Transaction ID: 0x9515
  Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    img01.sogoucdn.com: type A, class IN
        Name: img01.sogoucdn.com
        [Name Length: 18]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

[DNS 响应包]

```
Internet Protocol Version 4, Src: 10.8.4.4 (10.8.4.4), Dst: 172.18.54.224 (172.18.54.224)
    Version: 4
    Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 207
    Identification: 0x99f6 (39414)
  Flags: 0x00
    Fragment offset: 0
    Time to live: 57
    Protocol: UDP (17)
  Header checksum: 0xf629 [validation disabled]
    Source: 10.8.4.4 (10.8.4.4)
    Destination: 172.18.54.224 (172.18.54.224)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 53 (53), Dst Port: 58358 (58358)
    Source Port: 53 (53)
    Destination Port: 58358 (58358)
    Length: 187
  Checksum: 0x875c [validation disabled]
    [Stream index: 46]
Domain Name System (response)
    [Request In: 835]
    [Time: 0.001902000 seconds]
    Transaction ID: 0x9515
  Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  Queries
  Answers
    img01.sogoucdn.com: type CNAME, class IN, cname img01.sogoucdn.com.cdn.dnsv1.com
        Name: img01.sogoucdn.com
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 205
        Data length: 31
        CNAME: img01.sogoucdn.com.cdn.dnsv1.com
    img01.sogoucdn.com.cdn.dnsv1.com: type CNAME, class IN, cname 10099.stsougou.cdntip.com
    10099.stsougou.cdntip.com: type A, class IN, addr 36.159.127.22
    10099.stsougou.cdntip.com: type A, class IN, addr 117.169.98.75
    10099.stsougou.cdntip.com: type A, class IN, addr 120.226.27.14
    10099.stsougou.cdntip.com: type A, class IN, addr 36.158.190.246
```

6、 (TCP.pcapng)截取完整的 TCP 三次握手建立连接和四次挥手关闭连接的包：

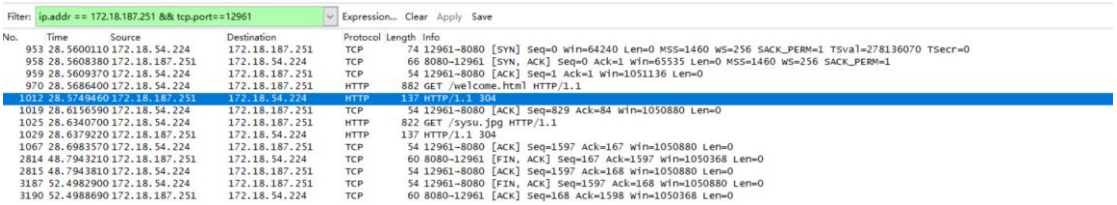
http://172.18.187.251:8080/welcome.html （要等一会）

先用过滤条件：ip.addr == 172.18.187.251

知道端口号后再用过滤条件：ip.addr == 172.18.187.251 && tcp.port==59161

第二遍要刷新一下

[总图]




[分析 1]

- 建立连接，写出标志位、相对序号、相对确认号和长度、选项：

```
953 28.5600110 172.18.54.224    172.18.187.251   TCP      74 12961-8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=278136070 TSecr=0
958 28.5608380 172.18.187.251   172.18.54.224    TCP      66 8080-12961 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
959 28.5609370 172.18.54.224    172.18.187.251   TCP      54 12961-8080 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
```

（1）C->S

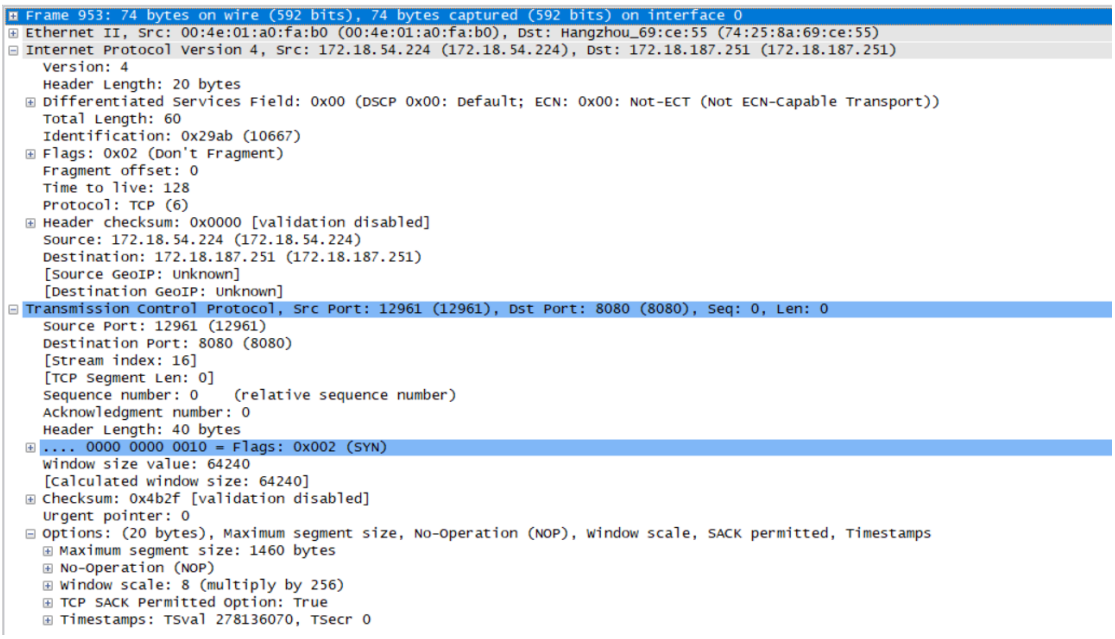
标志位：SYN

相对序号：Seq=0

相对确认号：无

长度：Len=0

选项：MSS=1460bytes WS=256 SACK_PERM=1 TSval=175800347 TSecrs=0




（2）S->C

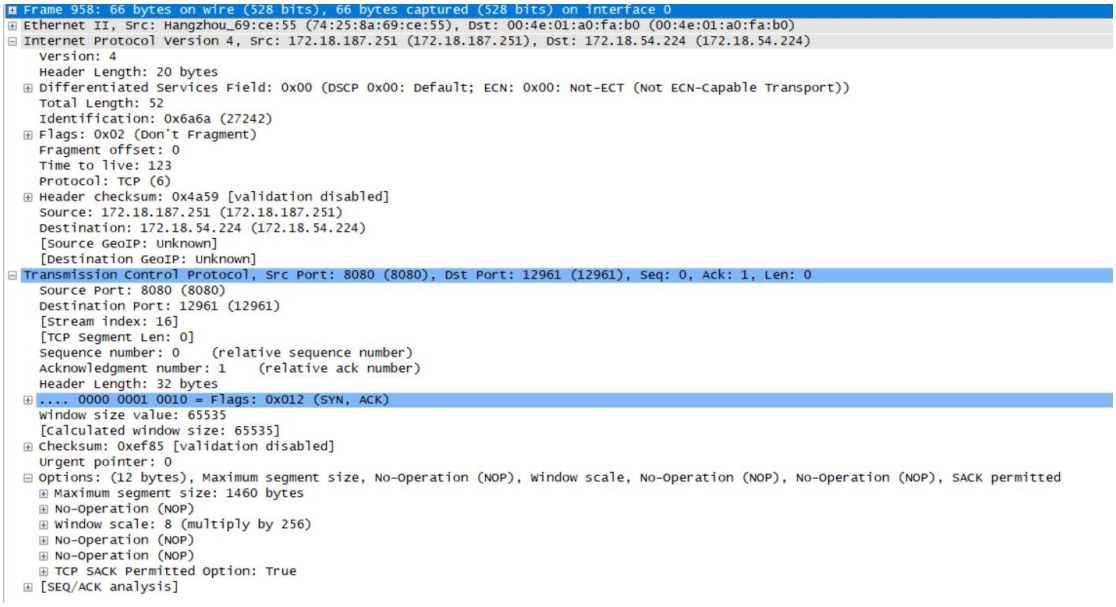
标志位：SYN ACK

相对序号：Seq=0

相对确认号：Ack=1

长度：Len=0

选项：MSS=1460bytes WS=256 SACK_PERM=1




（3）C->S

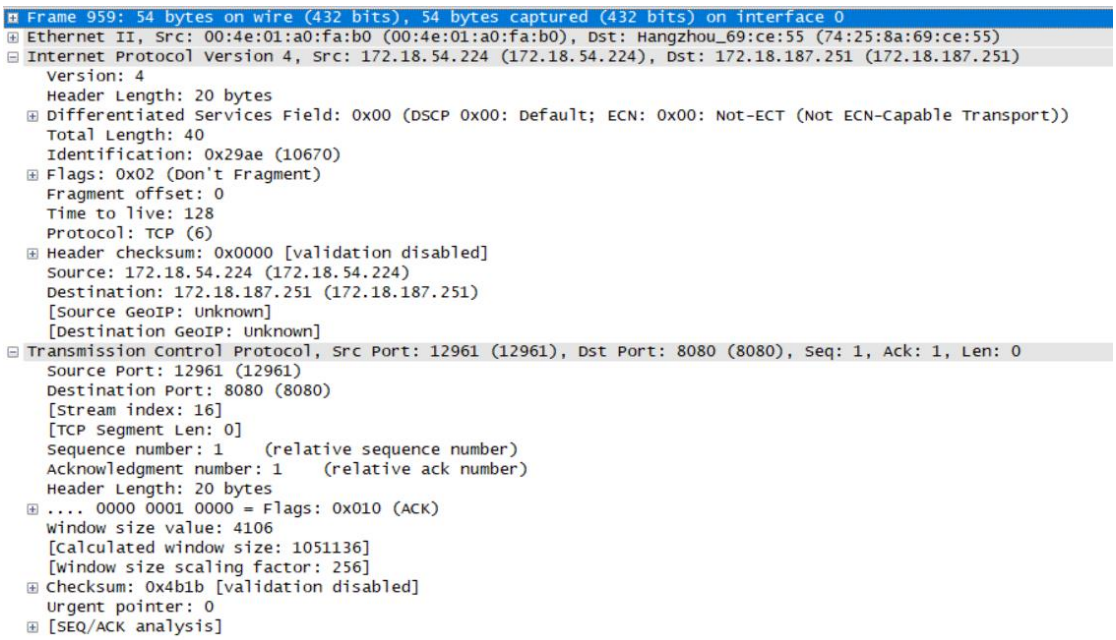
标志位：ACK

相对序号：Seq=1

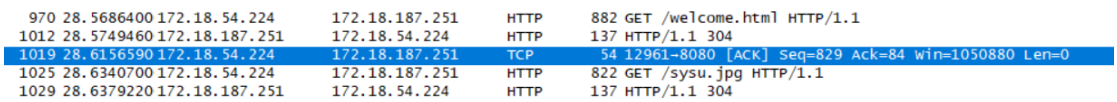
相对确认号：Ack=1

长度：Len=0

选项：无




■ 传送出数据，写出相对序号，相对确认号，长度，选项以及每一步的作用：




(1)C->S

相对序号：Seq=1

相对确认号：Ack=1

长度：Len=828

选项：无

作用：客户端请求获取 /welcome.html

```
Frame 970: 882 bytes on wire (7056 bits), 882 bytes captured (7056 bits) on interface 0
Ethernet II, Src: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0), Dst: Hangzhou_69:ce:55 (74:25:8a:69:ce:55)
Internet Protocol Version 4, Src: 172.18.54.224 (172.18.54.224), Dst: 172.18.187.251 (172.18.187.251)
    Version: 4
    Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 868
    Identification: 0x29b1 (10673)
  Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  Header checksum: 0x0000 [validation disabled]
    Source: 172.18.54.224 (172.18.54.224)
    Destination: 172.18.187.251 (172.18.187.251)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 12961 (12961), Dst Port: 8080 (8080), Seq: 1, Ack: 1, Len: 828
    Source Port: 12961 (12961)
    Destination Port: 8080 (8080)
    [Stream index: 16]
    [TCP Segment Len: 828]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 829    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header Length: 20 bytes
  .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
    Window size value: 4106
    [Calculated window size: 1051136]
    [Window size scaling factor: 256]
  Checksum: 0x4e57 [validation disabled]
    Urgent pointer: 0
  [SEQ/ACK analysis]
Hypertext Transfer Protocol
  GET /welcome.html HTTP/1.1\r\n
    Host: 172.18.187.251:8080\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36 Edg/91.0.864.54\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Purpose: prefetch\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,fr;q=0.5\r\n
```

(2)S->C

相对序号：Seq=1

相对确认号：Ack=829

长度：Len=83

选项：无

作用：服务器返回 /welcome.html

```
Frame 1012: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
Ethernet II, Src: Hangzhou_69:ce:55 (74:25:8a:69:ce:55), Dst: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
Internet Protocol Version 4, Src: 172.18.187.251 (172.18.187.251), Dst: 172.18.54.224 (172.18.54.224)
    Version: 4
    Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 123
    Identification: 0x6a6d (27245)
  Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 123
    Protocol: TCP (6)
  Header checksum: 0x4a0f [validation disabled]
    Source: 172.18.187.251 (172.18.187.251)
    Destination: 172.18.54.224 (172.18.54.224)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 8080 (8080), Dst Port: 12961 (12961), Seq: 1, Ack: 829, Len: 83
    Source Port: 8080 (8080)
    Destination Port: 12961 (12961)
    [Stream index: 16]
    [TCP Segment Len: 83]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 84    (relative sequence number)]
    Acknowledgment number: 829    (relative ack number)
    Header Length: 20 bytes
  .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
    Window size value: 4106
    [Calculated window size: 1051136]
    [Window size scaling factor: 256]
  Checksum: 0xf7ec [validation disabled]
    Urgent pointer: 0
  [SEQ/ACK analysis]
Hypertext Transfer Protocol
  HTTP/1.1 304 \r\n
    ETag: W/"153-1624332535823"\r\n
    Date: Sun, 27 Jun 2021 14:15:24 GMT\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.006306000 seconds]
    [Request in frame: 970]
    [Next request in frame: 1025]
    [Next response in frame: 1029]
```

(3)C->S

相对序号：Seq=829

相对确认号：Ack=84

长度：Len=768

选项：无

作用：客户端请求获取 /sysu.jpg

```
Frame 1025: 822 bytes on wire (6576 bits), 822 bytes captured (6576 bits) on interface 0
Ethernet II, Src: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0), Dst: Hangzhou_69:ce:55 (74:25:8a:69:ce:55)
Internet Protocol Version 4, Src: 172.18.54.224 (172.18.54.224), Dst: 172.18.187.251 (172.18.187.251)
    Version: 4
    Header Length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 808
    Identification: 0x29b3 (10675)
    Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    Source: 172.18.54.224 (172.18.54.224)
    Destination: 172.18.187.251 (172.18.187.251)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 12961 (12961), Dst Port: 8080 (8080), Seq: 829, Ack: 84, Len: 768
    Source Port: 12961 (12961)
    Destination Port: 8080 (8080)
    [Stream index: 16]
    [TCP Segment Len: 768]
    Sequence number: 829    (relative sequence number)
    [Next sequence number: 1597    (relative sequence number)]
    Acknowledgment number: 84    (relative ack number)
    Header Length: 20 bytes
    .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
    Window size value: 4105
    [Calculated window size: 1050880]
    [window size scaling factor: 256]
    Checksum: 0x4e1b [validation disabled]
    Urgent pointer: 0
    [SEQ/ACK analysis]
Hypertext Transfer Protocol
    GET /sysu.jpg HTTP/1.1\r\n
    Host: 172.18.187.251:8080\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36 Edg/91.0.864.54\r\n
    Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8\r\n
    Purpose: prefetch\r\n
    Referer: http://172.18.187.251:8080/welcome.html\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,fr;q=0.5\r\n
    Cookie: ASP.NET_SessionId=mfahowhrwvrfih3x2z1a1knj; Homework=default-groupname=19net; screen_availHeight=112; screen_availWidth=1904; Login=Password=
```

(4)S->C

相对序号：Seq=84

相对确认号：Ack=1597

长度：Len=83

选项：无

作用：服务器返回 /sysu.jpg

```
Frame 1029: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
Ethernet II, Src: Hangzhou_69:ce:55 (74:25:8a:69:ce:55), Dst: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
Internet Protocol Version 4, Src: 172.18.187.251 (172.18.187.251), Dst: 172.18.54.224 (172.18.54.224)
    Version: 4
    Header Length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 123
    Identification: 0x6a6e (27246)
    Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 123
    Protocol: TCP (6)
    Header checksum: 0x4a0e [validation disabled]
    Source: 172.18.187.251 (172.18.187.251)
    Destination: 172.18.54.224 (172.18.54.224)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 8080 (8080), Dst Port: 12961 (12961), Seq: 84, Ack: 1597, Len: 83
    Source Port: 8080 (8080)
    Destination Port: 12961 (12961)
    [Stream index: 16]
    [TCP Segment Len: 83]
    Sequence number: 84    (relative sequence number)
    [Next sequence number: 167    (relative sequence number)]
    Acknowledgment number: 1597    (relative ack number)
    Header Length: 20 bytes
    .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
    Window size value: 4103
    [Calculated window size: 1050368]
    [Window size scaling factor: 256]
    Checksum: 0xe596 [validation disabled]
    Urgent pointer: 0
    [SEQ/ACK analysis]
Hypertext Transfer Protocol
    HTTP/1.1 304 \r\n
    ETag: W/"898-1624331584456"\r\n
    Date: Sun, 27 Jun 2021 14:15:24 GMT\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.003852000 seconds]
    [Prev request in frame: 970]
    [Prev response in frame: 1012]
    [Request in frame: 1025]
```

- 释放连接，写出标志位、相对序号、相对确认号和长度、选项：

```
2814 48.7943210 172.18.187.251   172.18.54.224    TCP      60 8080→12961 [FIN, ACK] Seq=167 Ack=1597 Win=1050368 Len=0
2815 48.7943810 172.18.54.224    172.18.187.251   TCP      54 12961→8080 [ACK] Seq=1597 Ack=168 Win=1050880 Len=0
3187 52.4982900 172.18.54.224    172.18.187.251   TCP      54 12961→8080 [FIN, ACK] Seq=1597 Ack=168 Win=1050880 Len=0
3190 52.4988690 172.18.187.251   172.18.54.224    TCP      60 8080→12961 [ACK] Seq=168 Ack=1598 Win=1050368 Len=0
```

（1）S->C

标志位：FIN ACK

相对序号：Seq=167

相对确认号：Ack=1597

长度：Len=0

选项：无

```
Frame 2814: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Hangzhou_69:ce:55 (74:25:8a:69:ce:55), Dst: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
Internet Protocol Version 4, Src: 172.18.187.251 (172.18.187.251), Dst: 172.18.54.224 (172.18.54.224)
    Version: 4
    Header Length: 20 bytes
  + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 40
    Identification: 0x6a70 (27248)
  + Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 123
    Protocol: TCP (6)
  + Header checksum: 0x4a5f [validation disabled]
    Source: 172.18.187.251 (172.18.187.251)
    Destination: 172.18.54.224 (172.18.54.224)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 8080 (8080), Dst Port: 12961 (12961), Seq: 167, Ack: 1597, Len: 0
    Source Port: 8080 (8080)
    Destination Port: 12961 (12961)
    [Stream index: 16]
    [TCP Segment Len: 0]
    Sequence number: 167    (relative sequence number)
    Acknowledgment number: 1597    (relative ack number)
    Header Length: 20 bytes
  - .... 0000 0001 0001 = Flags: 0x011 (FIN, 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
    + .... .... ...1 = Fin: Set
    Window size value: 4103
    [Calculated window size: 1050368]
    [window size scaling factor: 256]
  + Checksum: 0x196f [validation disabled]
    Urgent pointer: 0
```

（2）C->S

标志位：ACK

相对序号：Seq=1597

相对确认号：Ack=168

长度：Len=0

选项：无

```
Frame 2815: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0), Dst: Hangzhou_69:ce:55 (74:25:8a:69:ce:55)
Internet Protocol Version 4, Src: 172.18.54.224 (172.18.54.224), Dst: 172.18.187.251 (172.18.187.251)
    Version: 4
    Header Length: 20 bytes
  + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 40
    Identification: 0x29b6 (10678)
  + Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  + Header checksum: 0x0000 [validation disabled]
    Source: 172.18.54.224 (172.18.54.224)
    Destination: 172.18.187.251 (172.18.187.251)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 12961 (12961), Dst Port: 8080 (8080), Seq: 1597, Ack: 168, Len: 0
    Source Port: 12961 (12961)
    Destination Port: 8080 (8080)
    [Stream index: 16]
    [TCP Segment Len: 0]
    Sequence number: 1597    (relative sequence number)
    Acknowledgment number: 168    (relative ack number)
    Header Length: 20 bytes
  - .... 0000 0001 0000 = 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
    Window size value: 4105
    [Calculated window size: 1050880]
    [Window size scaling factor: 256]
  + Checksum: 0x4b1b [validation disabled]
    Urgent pointer: 0
  + [SEQ/ACK analysis]
```

（3）C->S

标志位：FIN ACK

相对序号：Seq=1597

相对确认号：Ack=168

长度：Len=0

选项：无

```
Frame 3187: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0), Dst: Hangzhou_69:ce:55 (74:25:8a:69:ce:55)
Internet Protocol Version 4, Src: 172.18.54.224 (172.18.54.224), Dst: 172.18.187.251 (172.18.187.251)
    Version: 4
    Header Length: 20 bytes
  + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 40
    Identification: 0x29b8 (10680)
  + Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  + Header checksum: 0x0000 [validation disabled]
    Source: 172.18.54.224 (172.18.54.224)
    Destination: 172.18.187.251 (172.18.187.251)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 12961 (12961), Dst Port: 8080 (8080), Seq: 1597, Ack: 168, Len: 0
    Source Port: 12961 (12961)
    Destination Port: 8080 (8080)
    [Stream index: 16]
    [TCP Segment Len: 0]
    Sequence number: 1597    (relative sequence number)
    Acknowledgment number: 168    (relative ack number)
    Header Length: 20 bytes
  - .... 0000 0001 0001 = Flags: 0x011 (FIN, 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
    + .... .... ...1 = Fin: Set
    Window size value: 4105
    [Calculated window size: 1050880]
    [Window size scaling factor: 256]
  + Checksum: 0x4b1b [validation disabled]
    Urgent pointer: 0
```

（4）S->C

标志位：ACK

相对序号：Seq=168

相对确认号：Ack=1598

长度：Len=0

选项：无

```
Frame 3190: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Hangzhou_69:ce:55 (74:25:8a:69:ce:55), Dst: 00:4e:01:a0:fa:b0 (00:4e:01:a0:fa:b0)
Internet Protocol Version 4, Src: 172.18.187.251 (172.18.187.251), Dst: 172.18.54.224 (172.18.54.224)
    Version: 4
    Header Length: 20 bytes
  + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 40
    Identification: 0x6a72 (27250)
  + Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 123
    Protocol: TCP (6)
  + Header checksum: 0x4a5d [validation disabled]
    Source: 172.18.187.251 (172.18.187.251)
    Destination: 172.18.54.224 (172.18.54.224)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 8080 (8080), Dst Port: 12961 (12961), Seq: 168, Ack: 1598, Len: 0
    Source Port: 8080 (8080)
    Destination Port: 12961 (12961)
    [Stream index: 16]
    [TCP Segment Len: 0]
    Sequence number: 168    (relative sequence number)
    Acknowledgment number: 1598    (relative ack number)
    Header Length: 20 bytes
  - .... 0000 0001 0000 = 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
    Window size value: 4103
    [Calculated window size: 1050368]
    [Window size scaling factor: 256]
  + Checksum: 0x196e [validation disabled]
    Urgent pointer: 0
  + [SEQ/ACK analysis]
```

[分析 3]

有什么特别的发现？

Tcp 连接时客户端先发起连接，释放时服务器先释放连接（任意一方应该都可以，我这里是服务器先释放），且第一次挥手和第四次挥手的标志位不光有 FIN，还有 ACK，这与理论课讲的有点不同。

【完成情况】

是否完成以下步骤？（√完成 -未做完 ×未做）

(1) [√] (2) [√] (3) [√] (4) [√] 5[√] 6[√]

【实验体会】

写出实验过程中的问题，思考及解决方法，简述实验体会（如果有的话）。

这次实验花费了我大量的时间，不过也帮助我复习了许多计算机网络的知识。在做 ping -s 的实验时，发现什么域名都 ping 不通，后来只好换成我手机的 ip 地址，就成功了。在做 DHCP 实验时，因为我一开始是用远程桌面连接在别的电脑上，然后连接到我寝室的笔记本做实验的，而 ipconfig /release 命令会清除网络配置，所以直接把我远程桌面连接断了，让我吓了一跳，好在我后来直接回寝室在我笔记本上做实验就成功了。TCP 实验我一开始四次挥手关闭连接只截到 3 个包，没有客户端到服务器的 FIN ACK 包，不过我后来过了一天再做这个实验就能成功截到 4 个包了，有点玄学。总而言之，这次实验还是让我学到了很多知识，让我对很多协议原理的理解更加深刻了，果然是实践出真知啊！

【交实验报告】

上传网址：http://172.18.187.251/netdisk/default.aspx?vm=19net

编程实验

截止日期（不迟于）：2021 年 7 月 1 日（周四）23:00

上传文件名：学号_姓名_WireShark.doc

学号_姓名_WireShark.rar （包含所有.pcapng 文件）