北京郵電大學

计算机网络实验报告

题目: IP 和 TCP 数据分组的捕获和解析

姓　　名 　郑毓恒

学　　院 　计算机学院

专　　业 　计算机科学与技术

班　　级 　2020211302

学　　号 　2020211262

任课教师 　蒋砚军

2022 年 6 月

实验内容和实验目的

（1） 捕获在连接 Internet 过程中产生的网络层分组：DHCP 分组，ARP 分组，IP 数据分组，ICMP 分组。

（2） 分析各种分组的格式，说明各种分组在建立网络连接过程中的作用。

（3） 分析 IP 数据分组分片的结构。通过本次实验了解计算机上网的工作过程，学习各种网络层分组的格式及其作用，理解长度大于 1500 字节 IP 数据组分片传输的结构。

（4）分析 TCP 建立连接，拆除连接和数据通信的流程。

实验设备环境

1 台装有 Windows 操作系统的 PC 机，要求能够连接到 Internet，并安装 WireShark 软件。

实验步骤

（1） 准备工作

启动计算机，连接网络确保能够上网。开启 WireShark，选中所用网卡，开启监控。

（2）捕获和分析网络层分组

通过设置显示过滤器和在 DOS 窗口执行命令，捕获各类分组，并分析各类分组的格式和作用。

（3）分析数据分组分片的传输过程

制作大于 8000 字节的 IP 数据分组并发送，捕获后分析其分片传输的分片结构。

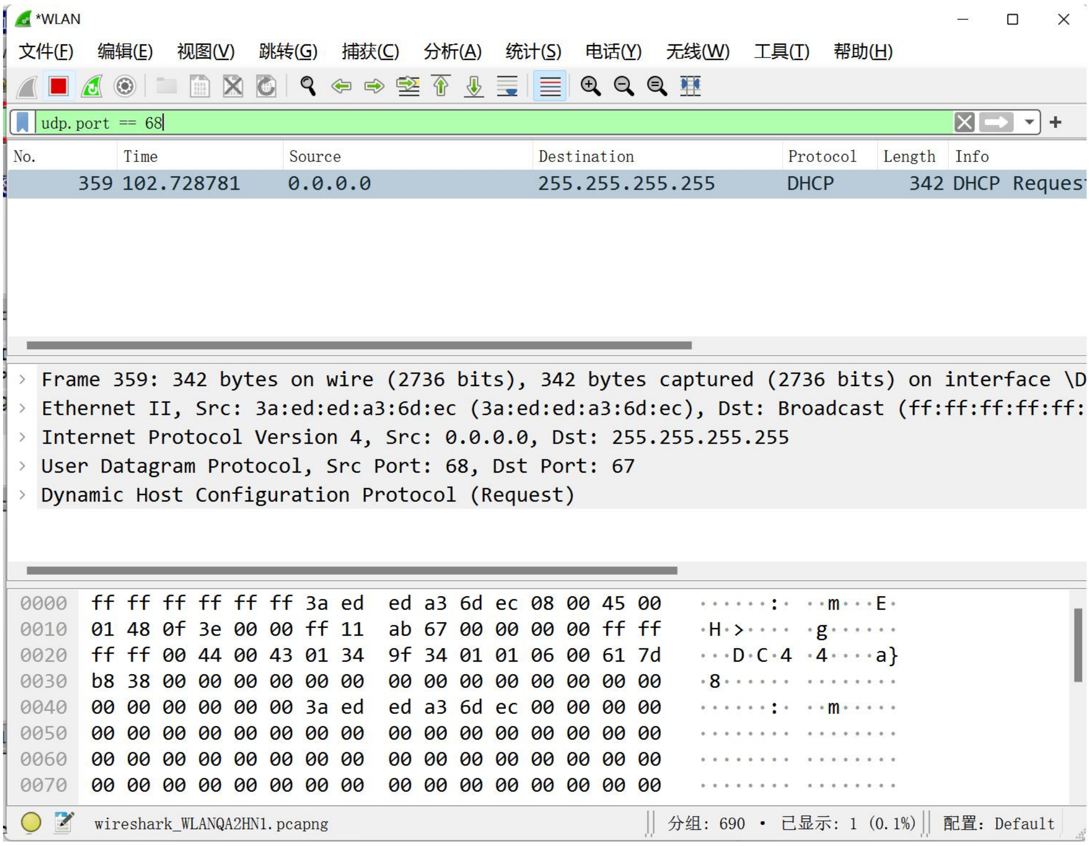
（4）分析 TCP 通信过程

观察 TCP 建立连接的三次握手，数据通信和优雅方式拆除连接的流程。

实验内容

（1）捕获 DHCP 报文

DHCP，动态主机配置协议，是一个局域网的网络协议。使用 UDP 协议工作，统一使用两个 IANA 分配的端口：67（服务器端），68（客户端）。DHCP 允许手动和自动的 IP 地址分配，使客户端动态的获得 IP 地址、Gateway 地址、DNS 服务器地址等信息。



udp.port == 68

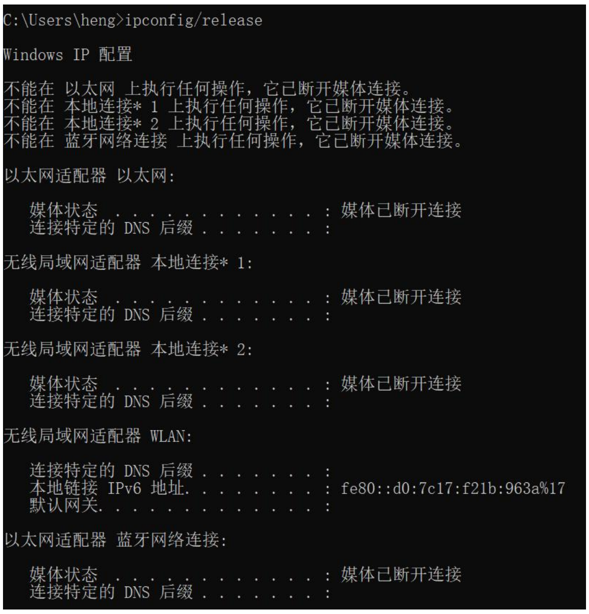
```
No.        Time          Source           Destination        Protocol  Length  Info
      359 102.728781     0.0.0.0          255.255.255.255    DHCP         342 DHCP Reques
```

```
> Frame 359: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \D
> Ethernet II, Src: 3a:ed:ed:a3:6d:ec (3a:ed:ed:a3:6d:ec), Dst: Broadcast (ff:ff:ff:ff:ff:
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Request)
```

```
0000  ff ff ff ff ff ff 3a ed  ed a3 6d ec 08 00 45 00   ······:· ··m···E·
0010  01 48 0f 3e 00 00 ff 11  ab 67 00 00 00 00 ff ff   ·H·>···· ·g······
0020  ff ff 00 44 00 43 01 34  9f 34 01 01 06 00 61 7d   ···D·C·4 ·4····a}
0030  b8 38 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·8······ ········
0040  00 00 00 00 00 00 3a ed  ed a3 6d ec 00 00 00 00   ······:· ··m·····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

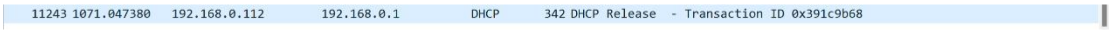
wireshark_WLANQA2HN1.pcapng || 分组：690 • 已显示：1 (0.1%) || 配置：Default

在 WireShark 工作画面 Filter 设置 udp.port == 68，只显示 UDP 端口 68 的 DHCP 报文。



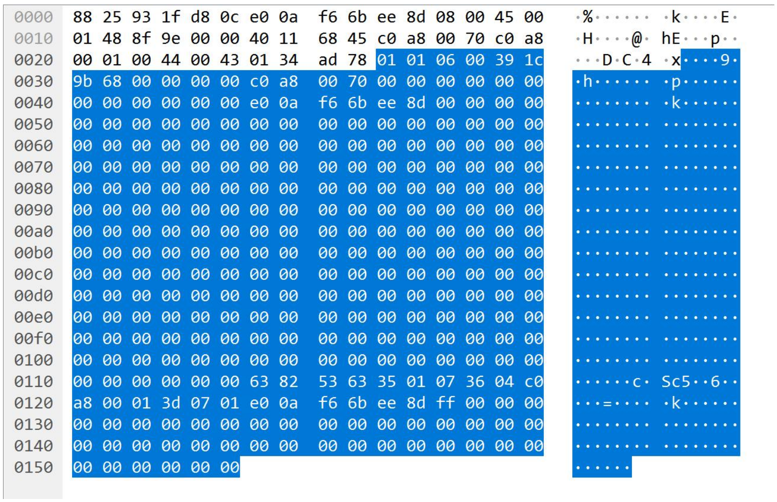
```
C:\Users\heng>ipconfig/release

Windows IP 配置

不能在 以太网 上执行任何操作，它已断开媒体连接。
不能在 本地连接* 1 上执行任何操作，它已断开媒体连接。
不能在 本地连接* 2 上执行任何操作，它已断开媒体连接。
不能在 蓝牙网络连接 上执行任何操作，它已断开媒体连接。

以太网适配器 以太网:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 本地连接* 1:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 本地连接* 2:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::d0:7c17:f21b:963a%17
   默认网关. . . . . . . . . . . . . :

以太网适配器 蓝牙网络连接:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
```

然后，在 DOS 窗口执行命令 ipconfig/release，释放已经申请的 IP 地址。



```
11243 1071.047380   192.168.0.112   192.168.0.1   DHCP   342 DHCP Release  - Transaction ID 0x391c9b68
```

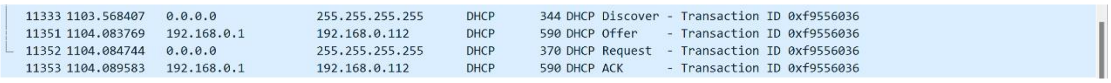
WireShark 中显示截获到一个 DHCP Release 数据分组。



```
0000  88 25 93 1f d8 0c e0 0a  f6 6b ee 8d 08 00 45 00   ·%······ ·k····E·
0010  01 48 8f 9e 00 00 40 11  68 45 c0 a8 00 70 c0 a8   ·H····@· hE···p··
0020  00 01 00 44 00 43 01 34  ad 78 01 01 06 00 39 1c   ···D·C·4 ·x····9·
0030  9b 68 00 00 00 00 c0 a8  00 70 00 00 00 00 00 00   ·h······ ·p······
0040  00 00 00 00 00 00 e0 0a  f6 6b ee 8d 00 00 00 00   ········ ·k······
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 07 36 04 c0   ······c· Sc5··6··
0120  a8 00 01 3d 07 01 e0 0a  f6 6b ee 8d ff 00 00 00   ···=···· ·k······
0130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0150  00 00 00 00 00 00                                  ······
```

```
Frame 11243: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
Internet Protocol Version 4, Src: 192.168.0.112, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Release)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x391c9b68
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 192.168.0.112
    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: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Release)
    Option: (54) DHCP Server Identifier (192.168.0.1)
    Option: (61) Client identifier
    Option: (255) End
    Padding:
0000000000000000000000000000000000000000000000000000000000000000000…
```

该 DHCP Release 分组的 内容如上。DHCP 客户端向 DHCP 服务器发送 Release 报文，告知服务器用户不再需要分配 IP 地址，请求释放对应的 IP 地址。



```
11333 1103.568407   0.0.0.0          255.255.255.255     DHCP      344 DHCP Discover - Transaction ID 0xf9556036
11351 1104.083769   192.168.0.1      192.168.0.112       DHCP      590 DHCP Offer    - Transaction ID 0xf9556036
11352 1104.084744   0.0.0.0          255.255.255.255     DHCP      370 DHCP Request  - Transaction ID 0xf9556036
11353 1104.089583   192.168.0.1      192.168.0.112       DHCP      590 DHCP ACK      - Transaction ID 0xf9556036
```

再执行 ipconfig/renew，请求网络连接。可以在 WireShark 上看到 DHCP 的四次握手的过程。

```
Frame 46487: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0969c471
    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: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Discover)
    Option: (61) Client identifier
    Option: (50) Requested IP Address (192.168.0.112)
    Option: (12) Host Name
    Option: (60) Vendor class identifier
    Option: (55) Parameter Request List
    Option: (255) End
```

客户端请求 IP，发送以上 DHCP Discover 分组。此时客户端还没有 IP 地址，因此 IP 是 0.0.0.0，需要通过 DHCP 获得一个合法地址。同时，DHCP 服务器的地址对客户端来说还是未知的，因此客户端以广播形式（IP: 255.255.255.255）发送 DHCP Discover 报文来寻找服务器。以上内容可见，报文内容包含客户端的 MAC 地址和计算机名，分别是 e0:0a:f6:6b:ee:8d 和 LiteonTe_6b:ee:8d，以便服务器确定报文由哪个客户端发送。

```
Frame 46494: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on
interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c), Dst: LiteonTe_6b:ee:8d
(e0:0a:f6:6b:ee:8d)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.112
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0969c471
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.0.112
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Offer)
    Option: (54) DHCP Server Identifier (192.168.0.1)
    Option: (51) IP Address Lease Time
    Option: (6) Domain Name Server
    Option: (1) Subnet Mask (255.255.255.0)
    Option: (3) Router
    Option: (255) End
    Padding:
0000000000000000000000000000000000000000000000000000000000000000000000
000…
```

服务器响应，发送以上 DHCP Offer 分组。服务器接收到来自客户端的 Discover 报文后，它就在自己的 IP 地址池中查找是否有合法的 IP 地址提供给客户端。如有，服务器就将此 IP 地址（此处为 192.168.0.112）做上标记，加入到 Offer 报文中，然后向先前从 Discover 得知的 MAC 地址发送 Offer 报文。

```
Frame 46495: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on
interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0969c471
    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: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Request)
    Option: (61) Client identifier
    Option: (50) Requested IP Address (192.168.0.112)
    Option: (54) DHCP Server Identifier (192.168.0.1)
    Option: (12) Host Name
    Option: (81) Client Fully Qualified Domain Name
    Option: (60) Vendor class identifier
    Option: (55) Parameter Request List
    Option: (255) End
```

客户端选择 IP,发送以上 DHCP Request 分组。客户端从接收到的 DHCP Offer 报文中获取 IP 地址，将 DHCP Request 报文广播到所有的服务器，表明它接受提供的内容，DHCP Request 报文包括为客户端提供 IP 配置的服务器的服务标示符（服务器 IP 地址，此处为 192.168.0.1）。服务器查看服务器标识符字段，以确定提供的 IP 地址是否被接受。如果被接受，服务器将该地址保留，这样该地址就不能提供给另一个客户端。如果被拒绝，则服务器将会取消并保留其 IP 地址以提供给下一个申请 IP 请求。

```
Frame 46496: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on
interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c), Dst: LiteonTe_6b:ee:8d
(e0:0a:f6:6b:ee:8d)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.112
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0969c471
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.0.112
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (ACK)
    Option: (54) DHCP Server Identifier (192.168.0.1)
    Option: (51) IP Address Lease Time
    Option: (6) Domain Name Server
    Option: (1) Subnet Mask (255.255.255.0)
    Option: (3) Router
    Option: (255) End
    Padding:
000000000000000000000000000000000000000000000000000000000000000000000
000…
```

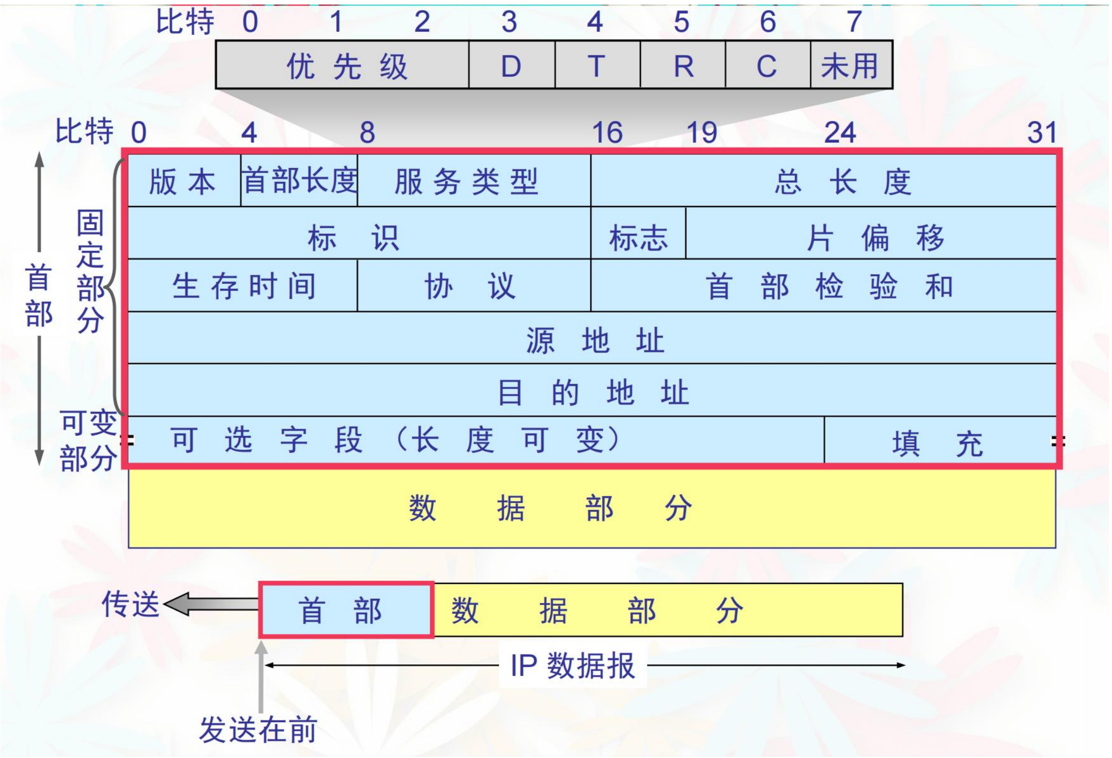
服务器确认分配，发送 DHCP ACK 分组。服务器接收到 DHCP Request 后，以 DHCP ACK 的形式向客户端发送成功的确认。该消息包含有 IP 地址的有效租约和其他可配置的信息。当客户机收到 DHCP ACK 时，它就配置了 IP 地址，完成 TCP/IP 的初始化。完成 DHCP 的四次握手。

（2）捕获 IP 数据分组

IP，网际互连协议，是 TCP/IP 体系的网络层协议，是为计算机网络相互连接进行通信而设计的协议。在 Filter 输入 ip.src eq IP 或 ip.dst eq IP，使 WireShark 只显示输入 IP 发送的或送往该 IP 的分组。本次实验使用 211.68.69.240，即 www.bupt.edu.cn 的 IP 地址，捕获该网站的 IP 数据分组。

```
Frame 46226: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface
\Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c), Dst: LiteonTe_6b:ee:8d
(e0:0a:f6:6b:ee:8d)
    Destination: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
        Address: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
        Address: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 211.68.69.240, Dst: 192.168.0.112
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xef38 (61240)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 51
    Protocol: TCP (6)
    Header Checksum: 0x7e3e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 211.68.69.240
    Destination Address: 192.168.0.112
Transmission Control Protocol, Src Port: 443, Dst Port: 13164, Seq: 7665, Ack:
1437, Len: 0
```

以上为捕获的 IP 数据分组之一。



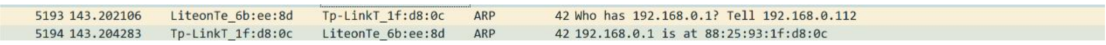
IPv4 首部分组格式如上。

字段	内容
版本	使用 IPv4 协议
首部长度	20 字节
服务类型	0x00 (DSCP: CS0，ECN: Not-ECT)
总长度	52
标识	0xef38 (61240)
标志	0x40，不分片
片偏移	0
生存时间	51
协议	TCP (6)
首部检验和	0x7e3e
源地址	211.68.69.240
目的地址	192.168.0.112

分析捕获到的 IP 数据分组，得到以上结果。

（3）捕获 ARP 分组

ARP，地址解析协议，是根据 IP 地址 获取 物理地址 的一个 TCP/IP 协议 。在 Filter 输入 arp，使 WireShark 只显示 ARP 分组。与捕获 DHCP 分组时一样，断开网络连接，再重连。



```
5193 143.202106    LiteonTe_6b:ee:8d    Tp-LinkT_1f:d8:0c    ARP    42 Who has 192.168.0.1? Tell 192.168.0.112
5194 143.204283    Tp-LinkT_1f:d8:0c    LiteonTe_6b:ee:8d    ARP    42 192.168.0.1 is at 88:25:93:1f:d8:0c
```

WireShark 捕获到以上两个 ARP 分组。

```
Frame 5193: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
    Sender IP address: 192.168.0.112
    Target MAC address: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
    Target IP address: 192.168.0.1
```

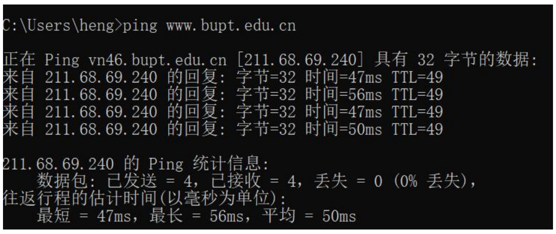
第一个 ARP 分组内容如上。该分组是从本计算机向服务器发送的 ARP 请求，查询 IP 地址 192.180.0.1 的物理地址。

```
Frame 5194: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c), Dst: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
    Sender IP address: 192.168.0.1
    Target MAC address: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
    Target IP address: 192.168.0.112
```

第二个 ARP 分组内容如上。该分组是服务器向主机发送的回复，主机获得 IP 地址 192.180.0.1 物理地址。

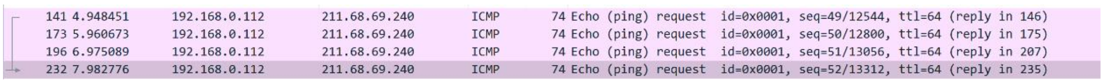
（3）捕获 ICMP 分组

ICMP，因特网控制报文协议，是一种面向无连接的协议，用于传输出错报告控制信息。ICMP 属于网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。



```
C:\Users\heng>ping www.bupt.edu.cn

正在 Ping vn46.bupt.edu.cn [211.68.69.240] 具有 32 字节的数据:
来自 211.68.69.240 的回复: 字节=32 时间=47ms TTL=49
来自 211.68.69.240 的回复: 字节=32 时间=56ms TTL=49
来自 211.68.69.240 的回复: 字节=32 时间=47ms TTL=49
来自 211.68.69.240 的回复: 字节=32 时间=50ms TTL=49

211.68.69.240 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 = 47ms，最长 = 56ms，平均 = 50ms
```

在 Filter 输入 icmp，使其只显示 ICMP 分组。在 DOS 窗口输入 ping www.bupt.edu.cn，计算机向 IP 地址 211.68.69.240 发送 ping 请求并得到回复。

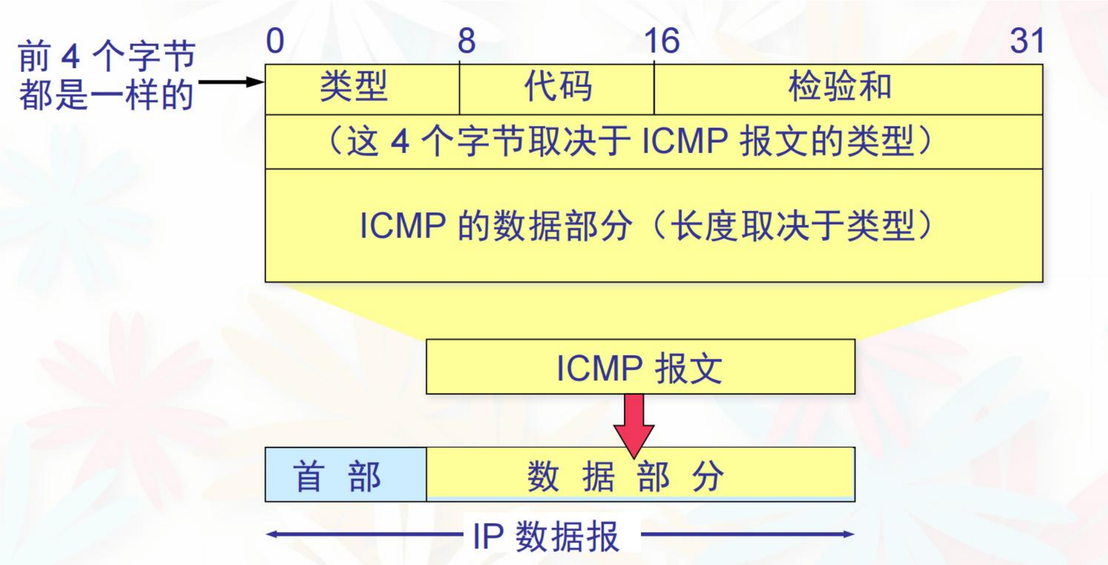


```
141 4.948451   192.168.0.112   211.68.69.240   ICMP   74 Echo (ping) request  id=0x0001, seq=49/12544, ttl=64 (reply in 146)
173 5.960673   192.168.0.112   211.68.69.240   ICMP   74 Echo (ping) request  id=0x0001, seq=50/12800, ttl=64 (reply in 175)
196 6.975089   192.168.0.112   211.68.69.240   ICMP   74 Echo (ping) request  id=0x0001, seq=51/13056, ttl=64 (reply in 207)
232 7.982776   192.168.0.112   211.68.69.240   ICMP   74 Echo (ping) request  id=0x0001, seq=52/13312, ttl=64 (reply in 235)
```

WireShark 捕获以上四个 ICMP 分组。

```
Frame 232: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
Internet Protocol Version 4, Src: 192.168.0.112, Dst: 211.68.69.240
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d27 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 52 (0x0034)
    Sequence Number (LE): 13312 (0x3400)
    [Response frame: 235]
    Data (32 bytes)
```

ICMP 分组的内容如上。

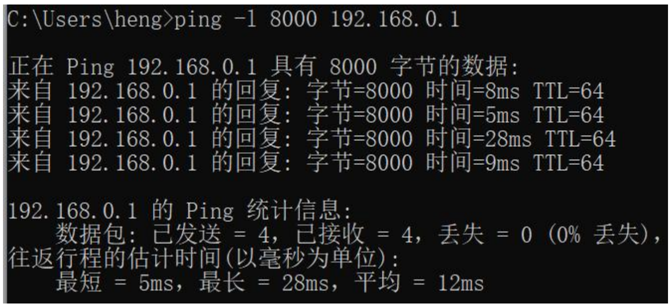


ICMP 报文的格式如上。

字段内容	内容
类型	8 (Echo (ping) request)
代码	0
检验和	0x4d27

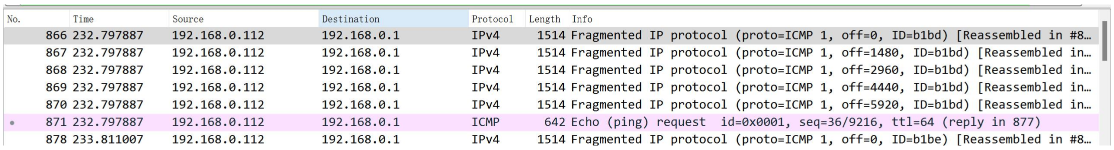
分析捕获的 ICMP 的内容，得到以上结果。

数据分组的分片传输过程



```
C:\Users\heng>ping -l 8000 192.168.0.1

正在 Ping 192.168.0.1 具有 8000 字节的数据:
来自 192.168.0.1 的回复: 字节=8000 时间=8ms TTL=64
来自 192.168.0.1 的回复: 字节=8000 时间=5ms TTL=64
来自 192.168.0.1 的回复: 字节=8000 时间=28ms TTL=64
来自 192.168.0.1 的回复: 字节=8000 时间=9ms TTL=64

192.168.0.1 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 = 5ms，最长 = 28ms，平均 = 12ms
```

在 Filter 输入 ip.dst eq 192.168.0.1，用来过滤 IP。然后在 DOS 窗口，输入 ping –l 8000 192.168.0.1，发送了四个长度为 8000 字节的数据分组。



No.	Time	Source	Destination	Protocol	Length	Info
866	232.797887	192.168.0.112	192.168.0.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=b1bd) [Reassembled in #8…
867	232.797887	192.168.0.112	192.168.0.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=b1bd) [Reassembled in…
868	232.797887	192.168.0.112	192.168.0.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=b1bd) [Reassembled in…
869	232.797887	192.168.0.112	192.168.0.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=b1bd) [Reassembled in…
870	232.797887	192.168.0.112	192.168.0.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5920, ID=b1bd) [Reassembled in…
871	232.797887	192.168.0.112	192.168.0.1	ICMP	642	Echo (ping) request id=0x0001, seq=36/9216, ttl=64 (reply in 877)
878	233.811007	192.168.0.112	192.168.0.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=b1be) [Reassembled in #8…

每个发送的数据分组被分为 5 个 IPv4 数据分组和一个 ICMP 分组。

```
Frame 866: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
Internet Protocol Version 4, Src: 192.168.0.112, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0xb1bd (45501)
    Flags: 0x20, More fragments
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x21a2 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.112
    Destination Address: 192.168.0.1
    [Reassembled IPv4 in frame: 871]
Data (1480 bytes)
```

第一个分片的内容如上。

```
Frame 867: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
Internet Protocol Version 4, Src: 192.168.0.112, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0xb1bd (45501)
    Flags: 0x20, More fragments
    ...0 0101 1100 1000 = Fragment Offset: 1480
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x20e9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.112
    Destination Address: 192.168.0.1
    [Reassembled IPv4 in frame: 871]
Data (1480 bytes)
```

第二个分片的内容如上。

```
Frame 868: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
Internet Protocol Version 4, Src: 192.168.0.112, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0xb1bd (45501)
    Flags: 0x21, More fragments
    ...0 1011 1001 0000 = Fragment Offset: 2960
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x2030 [validation disabled]
```

```
        [Header checksum status: Unverified]
        Source Address: 192.168.0.112
        Destination Address: 192.168.0.1
        [Reassembled IPv4 in frame: 871]
Data (1480 bytes)
```

第三个分片的内容如上。

```
Frame 869: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on
interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c
(88:25:93:1f:d8:0c)
Internet Protocol Version 4, Src: 192.168.0.112, Dst: 192.168.0.1
        0100 .... = Version: 4
        .... 0101 = Header Length: 20 bytes (5)
        Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
                0000 00.. = Differentiated Services Codepoint: Default (0)
                .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport
(0)
        Total Length: 1500
        Identification: 0xb1bd (45501)
        Flags: 0x22, More fragments
        ...1 0001 0101 1000 = Fragment Offset: 4440
        Time to Live: 64
        Protocol: ICMP (1)
        Header Checksum: 0x1f77 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.0.112
        Destination Address: 192.168.0.1
        [Reassembled IPv4 in frame: 871]
Data (1480 bytes)
```

第四个分片的内容如上。

```
Frame 870: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on
interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c
(88:25:93:1f:d8:0c)
Internet Protocol Version 4, Src: 192.168.0.112, Dst: 192.168.0.1
        0100 .... = Version: 4
        .... 0101 = Header Length: 20 bytes (5)
        Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
                0000 00.. = Differentiated Services Codepoint: Default (0)
                .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport
(0)
        Total Length: 1500
        Identification: 0xb1bd (45501)
        Flags: 0x22, More fragments
        ...1 0111 0010 0000 = Fragment Offset: 5920
        Time to Live: 64
        Protocol: ICMP (1)
        Header Checksum: 0x1ebe [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.0.112
        Destination Address: 192.168.0.1
        [Reassembled IPv4 in frame: 871]
Data (1480 bytes)
```

第五个分片的内容如上。

```
Frame 871: 642 bytes on wire (5136 bits), 642 bytes captured (5136 bits) on
interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c
(88:25:93:1f:d8:0c)
Internet Protocol Version 4, Src: 192.168.0.112, Dst: 192.168.0.1
        0100 .... = Version: 4
        .... 0101 = Header Length: 20 bytes (5)
        Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
                0000 00.. = Differentiated Services Codepoint: Default (0)
                .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport
(0)
        Total Length: 628
        Identification: 0xb1bd (45501)
        Flags: 0x03
        ...1 1100 1110 1000 = Fragment Offset: 7400
        Time to Live: 64
        Protocol: ICMP (1)
        Header Checksum: 0x416d [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.0.112
        Destination Address: 192.168.0.1
        [6 IPv4 Fragments (8008 bytes): #866(1480), #867(1480), #868(1480),
#869(1480), #870(1480), #871(608)]
Internet Control Message Protocol
```

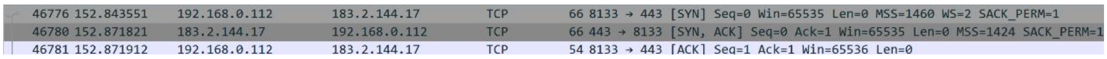
第六个分片的内容如上。

前五个分片的长度为 1500 字节，减去 IP 数据分组的首部长度 20 字节，每个分组的数据长度是 1480 字节，五个就是 7400 字节。第六个分组长度为 628 字节，除了减去 IP 首部的 20 字节外，还需减去 ICMP 部分的 8 字节，数据长度为 600 字节。六个分片的数据长度为 8000 字节，总长度符合，分片正确。

TCP 通信过程

建立连接

在 Filter 输入 tcp，使其只显示 TCP 分组。



```
46776 152.843551   192.168.0.112   183.2.144.17    TCP   66 8133 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
46780 152.871821   183.2.144.17    192.168.0.112   TCP   66 443 → 8133 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1424 SACK_PERM=1
46781 152.871912   192.168.0.112   183.2.144.17    TCP   54 8133 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

WireShark 捕获的 TCP 分组中，观察到以上三个分组，是本地主机（IP 地址 192.168.0.112）和 IP 地址 183.2.144.17 建立连接的三次握手的过程。

```
Frame 46776: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
Internet Protocol Version 4, Src: 192.168.0.112, Dst: 183.2.144.17
Transmission Control Protocol, Src Port: 8133, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 8133
    Destination Port: 443
    [Stream index: 52]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1881205284
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x002 (SYN)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0xeb25 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    [Timestamps]
```

第一个 TCP 分组的内容如上。这是第一次握手，客户端给服务器发送一个 SYN 段，请求建立连接，等待服务器确认。

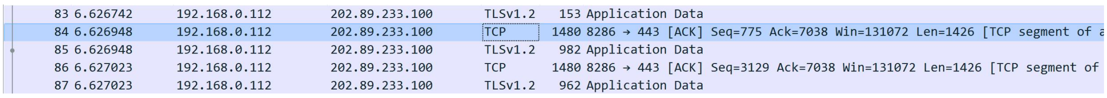
```
Frame 46780: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface
\Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c), Dst: LiteonTe_6b:ee:8d
(e0:0a:f6:6b:ee:8d)
Internet Protocol Version 4, Src: 183.2.144.17, Dst: 192.168.0.112
Transmission Control Protocol, Src Port: 443, Dst Port: 8133, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 8133
    [Stream index: 52]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 783385543
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1881205285
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x012 (SYN, ACK)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0x38b8 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), Maximum segment size, No-Operation (NOP),
No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
    [Timestamps]
    [SEQ/ACK analysis]
```

第二个 TCP 分组的内容如上。这是第二次握手，服务器返回客户端 SYN+ACK 段，表示确认收到客户端的 SYN 段，发送 SYN 段也请求客户端建立连接。

```
Frame 46781: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
Internet Protocol Version 4, Src: 192.168.0.112, Dst: 183.2.144.17
Transmission Control Protocol, Src Port: 8133, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
    Source Port: 8133
    Destination Port: 443
    [Stream index: 52]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1881205285
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 783385544
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
    Window: 32768
    [Calculated window size: 65536]
    [Window size scaling factor: 2]
    Checksum: 0xf967 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
```

第三个TCP分组的内容如上。这是第三次握手。客户端收到服务器的回复后，向服务器发送ACK分段，完成三次握手，建立连接。

通信过程

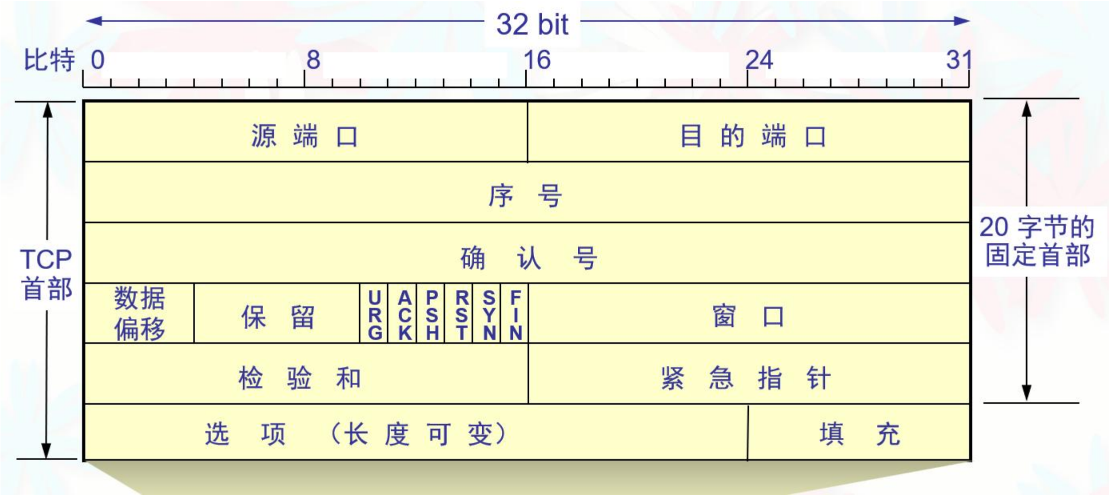


```
    83 6.626742     192.168.0.112       202.89.233.100      TLSv1.2    153 Application Data
    84 6.626948     192.168.0.112       202.89.233.100      TCP       1480 8286 → 443 [ACK] Seq=775 Ack=7038 Win=131072 Len=1426 [TCP segment of a
    85 6.626948     192.168.0.112       202.89.233.100      TLSv1.2    982 Application Data
    86 6.627023     192.168.0.112       202.89.233.100      TCP       1480 8286 → 443 [ACK] Seq=3129 Ack=7038 Win=131072 Len=1426 [TCP segment of
    87 6.627023     192.168.0.112       202.89.233.100      TLSv1.2    962 Application Data
```

WireShark 捕获到的 TCP 分组中，观察到一个通信过程中传输数据的 TCP 分组（图中第二个）。

```
Frame 84: 1480 bytes on wire (11840 bits), 1480 bytes captured (11840 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
Internet Protocol Version 4, Src: 192.168.0.112, Dst: 202.89.233.100
Transmission Control Protocol, Src Port: 8286, Dst Port: 443, Seq: 775, Ack: 7038, Len: 1426
    Source Port: 8286
    Destination Port: 443
    [Stream index: 5]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 1426]
    Sequence Number: 775    (relative sequence number)
    Sequence Number (raw): 3681061716
    [Next Sequence Number: 2201    (relative sequence number)]
    Acknowledgment Number: 7038    (relative ack number)
    Acknowledgment number (raw): 3614888761
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
    Window: 512
    [Calculated window size: 131072]
    [Window size scaling factor: 256]
    Checksum: 0xd235 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (1426 bytes)
    [Reassembled PDU in frame: 85]
    TCP segment data (1426 bytes)
```

捕获到的通信中 TCP 分组的内容如上。

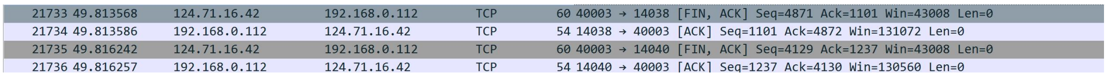


TCP 首部格式如上。

字段	内容
源端口	8286
目的端口	443
序号	775
确认号	7038
数据偏移	20 字节 (5)
标志	ACK
窗口	512
检验和	0xd235
紧急指针	0
选项	1426 字节
数据长度	1426 字节

捕获到的 TCP 分组的内容分析如上。

拆除连接



```
21733 49.813568    124.71.16.42     192.168.0.112    TCP    60 40003 → 14038 [FIN, ACK] Seq=4871 Ack=1101 Win=43008 Len=0
21734 49.813586    192.168.0.112    124.71.16.42     TCP    54 14038 → 40003 [ACK] Seq=1101 Ack=4872 Win=131072 Len=0
21735 49.816242    124.71.16.42     192.168.0.112    TCP    60 40003 → 14040 [FIN, ACK] Seq=4129 Ack=1237 Win=43008 Len=0
21736 49.816257    192.168.0.112    124.71.16.42     TCP    54 14040 → 40003 [ACK] Seq=1237 Ack=4130 Win=130560 Len=0
```

WireShark 捕获到的 TCP 分组中，观察到以上四个分组，是 IP 地址 192.168.0.1（本地主机）和 IP 地址 124.71.16.42 之间四次挥手拆除连接的过程。

```
Frame 21733: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c), Dst: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
Internet Protocol Version 4, Src: 124.71.16.42, Dst: 192.168.0.112
Transmission Control Protocol, Src Port: 40003, Dst Port: 14038, Seq: 4871, Ack: 1101, Len: 0
    Source Port: 40003
    Destination Port: 14038
    [Stream index: 34]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 4871    (relative sequence number)
    Sequence Number (raw): 1300638526
    [Next Sequence Number: 4872    (relative sequence number)]
    Acknowledgment Number: 1101    (relative ack number)
    Acknowledgment number (raw): 492798478
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x011 (FIN, ACK)
    Window: 21
    [Calculated window size: 43008]
    [Window size scaling factor: 2048]
    Checksum: 0x76e9 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
```

第一个 TCP 分组的内容如上。第一次挥手，客户端向服务器发送 FIN 分组，要求关闭 TCP 连接，等待服务器确认。

```
Frame 21734: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
Internet Protocol Version 4, Src: 192.168.0.112, Dst: 124.71.16.42
Transmission Control Protocol, Src Port: 14038, Dst Port: 40003, Seq: 1101, Ack: 4872, Len: 0
    Source Port: 14038
    Destination Port: 40003
    [Stream index: 34]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1101    (relative sequence number)
    Sequence Number (raw): 492798478
    [Next Sequence Number: 1101    (relative sequence number)]
    Acknowledgment Number: 4872    (relative ack number)
    Acknowledgment number (raw): 1300638527
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
    Window: 512
    [Calculated window size: 131072]
    [Window size scaling factor: 256]
    Checksum: 0x74fe [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
```

第二个 TCP 分组的内容如上。第二次挥手，服务器收到客户端发送的 FIN 分组后，向客户端发送 ACK 分组。此时 TCP 连接处于半关闭状态，客户端到服务器的连接释放。

```
Frame 21735: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
\Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c), Dst: LiteonTe_6b:ee:8d
(e0:0a:f6:6b:ee:8d)
Internet Protocol Version 4, Src: 124.71.16.42, Dst: 192.168.0.112
Transmission Control Protocol, Src Port: 40003, Dst Port: 14040, Seq: 4129, Ack:
1237, Len: 0
    Source Port: 40003
    Destination Port: 14040
    [Stream index: 35]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 4129    (relative sequence number)
    Sequence Number (raw): 3109122971
    [Next Sequence Number: 4130    (relative sequence number)]
    Acknowledgment Number: 1237    (relative ack number)
    Acknowledgment number (raw): 602939574
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x011 (FIN, ACK)
    Window: 21
    [Calculated window size: 43008]
    [Window size scaling factor: 2048]
    Checksum: 0x1d86 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
```

第三个 TCP 分组的内容如上。第三次挥手，服务器向客户端发送 FIN 分组，要求释放连接，等待客户端的确认。

```
Frame 21736: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0
Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: Tp-LinkT_1f:d8:0c (88:25:93:1f:d8:0c)
Internet Protocol Version 4, Src: 192.168.0.112, Dst: 124.71.16.42
Transmission Control Protocol, Src Port: 14040, Dst Port: 40003, Seq: 1237, Ack: 4130, Len: 0
    Source Port: 14040
    Destination Port: 40003
    [Stream index: 35]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1237    (relative sequence number)
    Sequence Number (raw): 602939574
    [Next Sequence Number: 1237    (relative sequence number)]
    Acknowledgment Number: 4130    (relative ack number)
    Acknowledgment number (raw): 3109122972
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
    Window: 510
    [Calculated window size: 130560]
    [Window size scaling factor: 256]
    Checksum: 0x1b9d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
```

第四个 TCP 分组的内容如上。第四次挥手，客户端收到服务器的 FIN 分组后，向服务器发送一个 ACK 分组。服务器收到 ACK 分组后，关闭连接，四次挥手完成。TCP 连接在客户端等待 2MSL 后，完全拆除。

实验总结

通过这次实验，掌握了 WireShark 软件的使用方法，学会如何捕获分组。实验中捕获并加以分析的网络层分组包括 DHCP 分组、ARP 分组、IP 数据分组、ICMP 分组和 TCP 分组，对这些分组的结构和在网络连接中的作用有了更深的认识。同时，通过发送 8000 字节的 IP 数据分组并捕获和分析，了解了分片传输的分组结构。最后通过观察网络连接中产生的 TCP 分组，发现了课上学习到的 TCP 连接的三次握手和四次挥手，学习了 TCP 建立连接、拆除连接和通信的流程。