

**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 鄭毓恒**

**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。

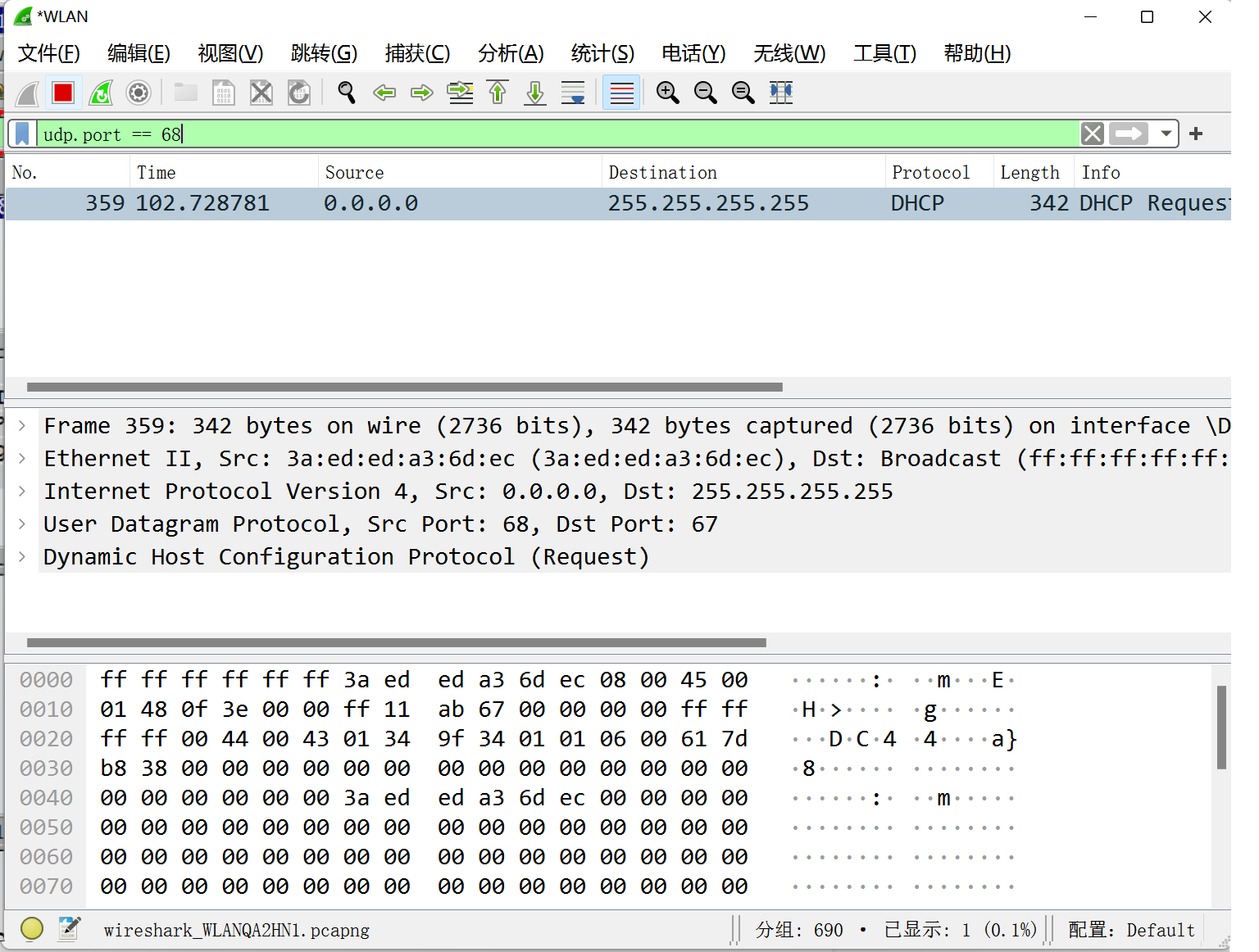
**（4）分析TCP通信过程**

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。

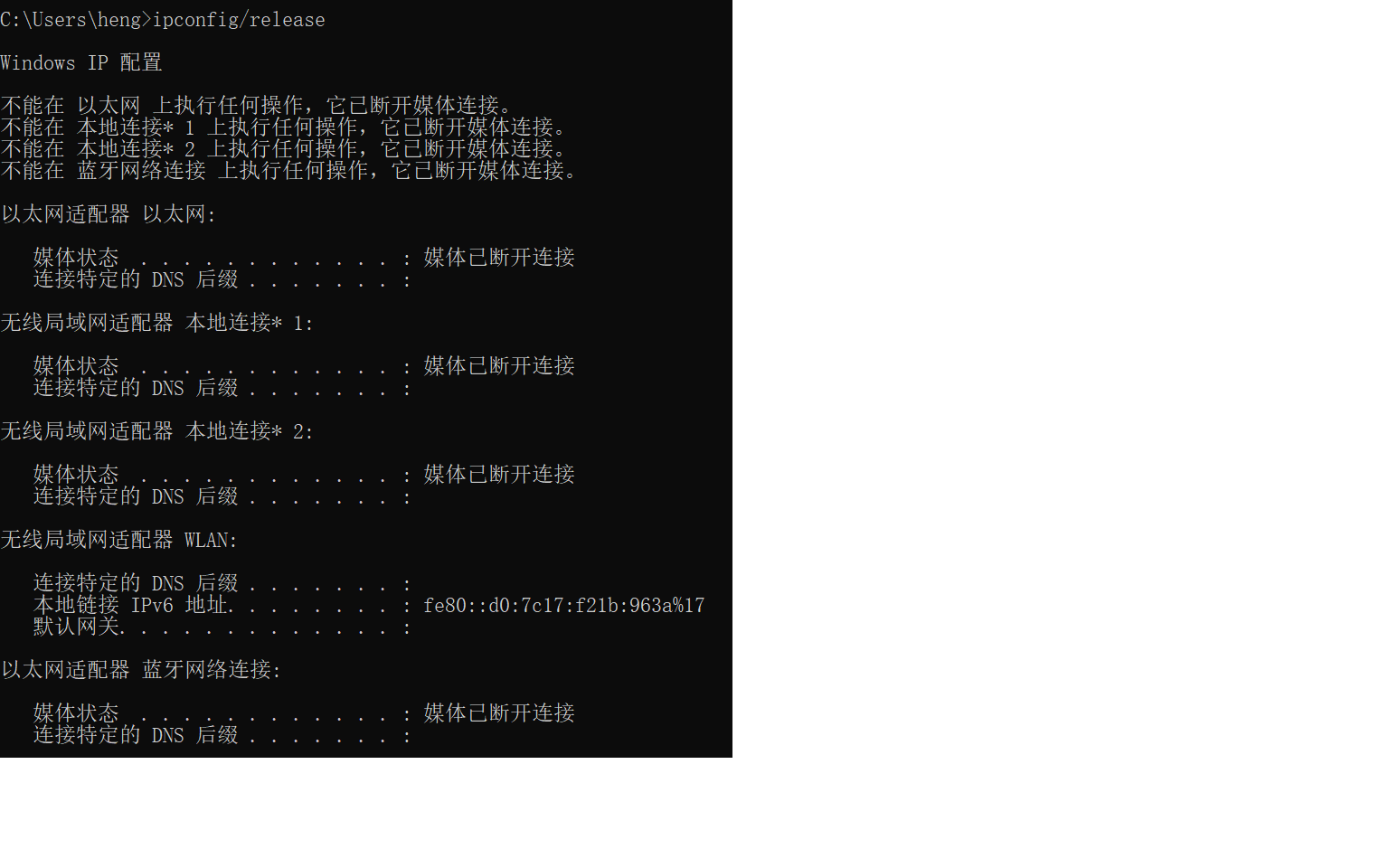
**实验内容**

**（1）捕获DHCP报文**

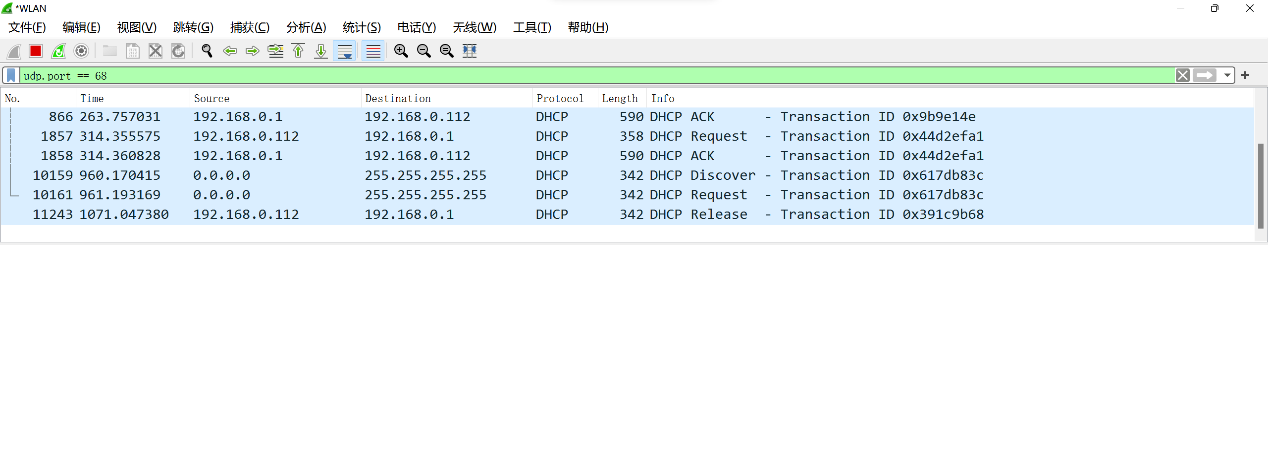
DHCP，动态主机配置协议，是一个局域网的网络协议。使用UDP协议工作，统一使用两个IANA分配的端口：67（服务器端），68（客户端）。DHCP允许手动和自动的IP地址分配，使客户端动态的获得IP 地址、Gateway 地址、DNS 服务器地址等信息。



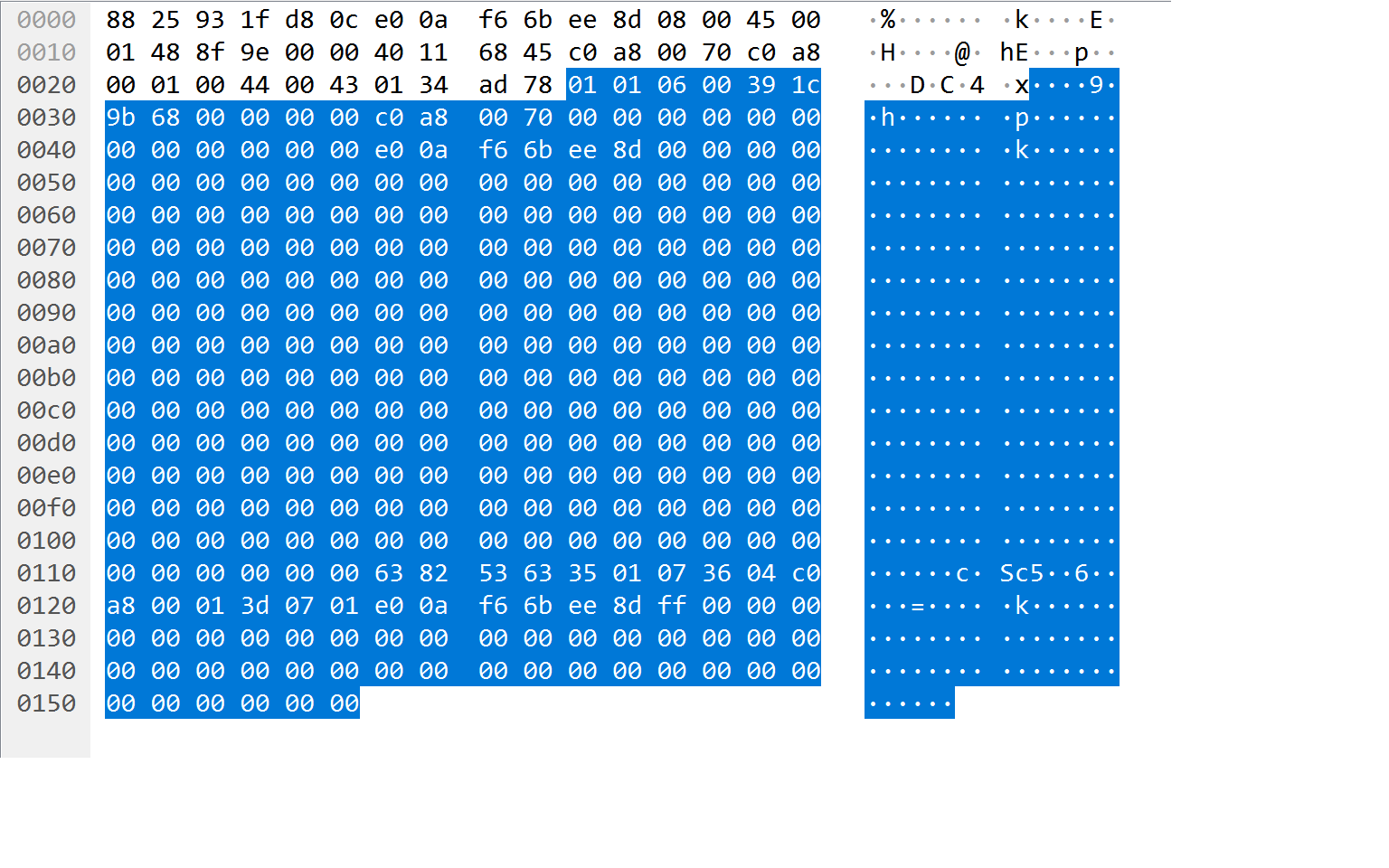
在WireShark工作画面Filter设置udp.port == 68，只显示UDP端口68的DHCP报文。



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

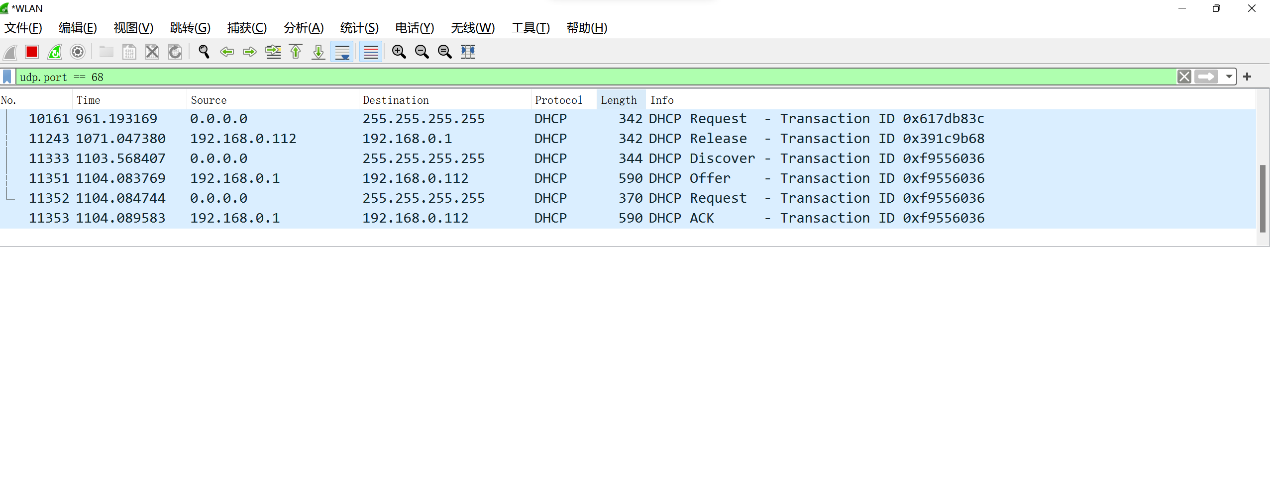


WireShark中显示截获到一个DHCP Release数据分组。



|  |
| --- |
| 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: 000000000000000000000000000000000000000000000000000000000000000000000000… |

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。



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: 000000000000000000000000000000000000000000000000000000000000000000000000… |

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: 000000000000000000000000000000000000000000000000000000000000000000000000… |

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。

1. **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。



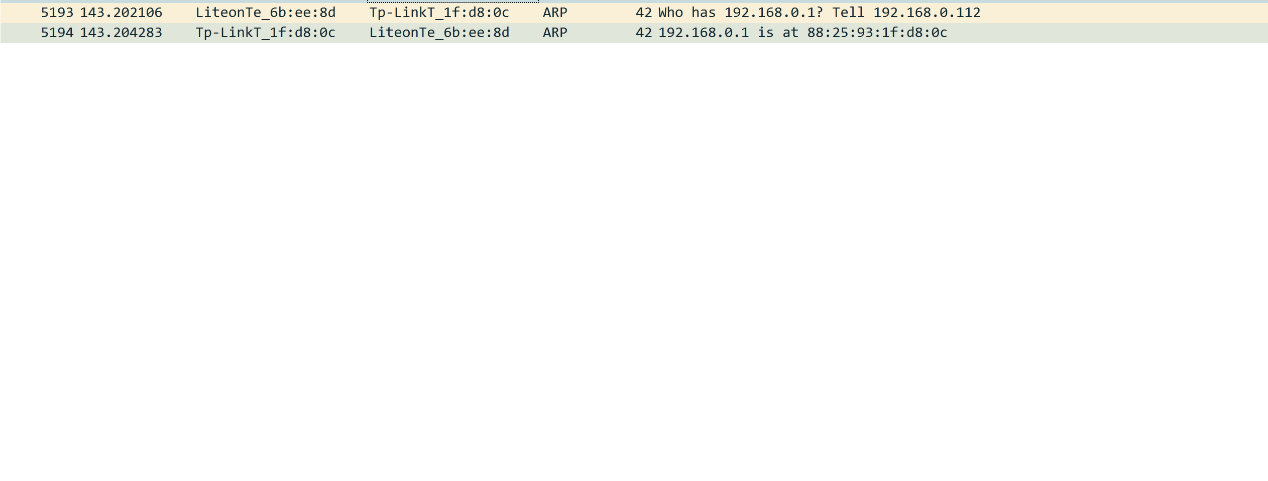
IPv4首部分组格式如上。

|  |  |
| --- | --- |
| 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。



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 |

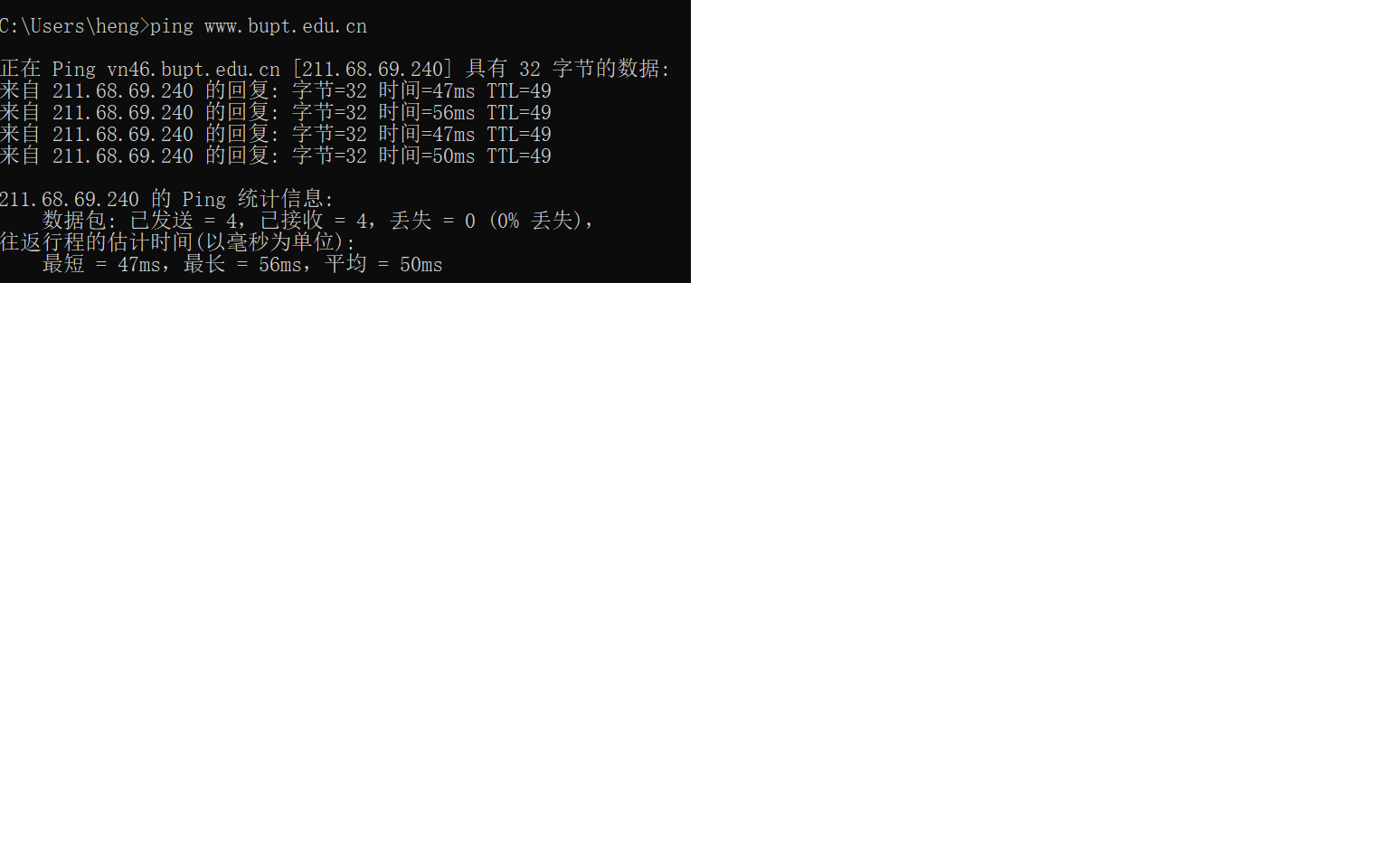
第一个ARP分组内容如上。该分组是从本计算机向服务器发送的ARP请求，查询IP地址192.180.0.1的物理地址。

|  |
| --- |
| 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 |

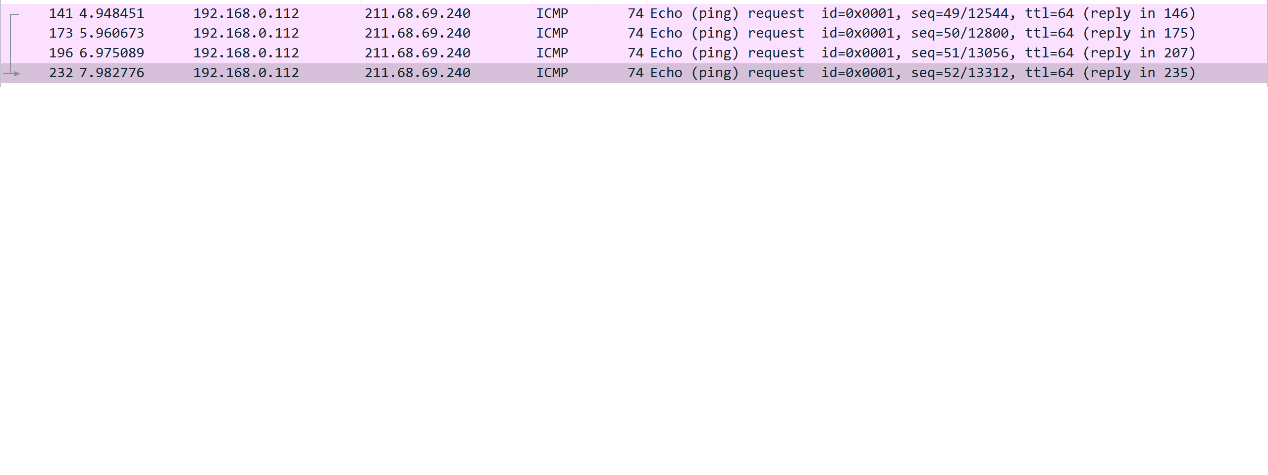
第二个ARP分组内容如上。该分组是服务器向主机发送的回复，主机获得IP地址192.180.0.1物理地址。

1. **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。



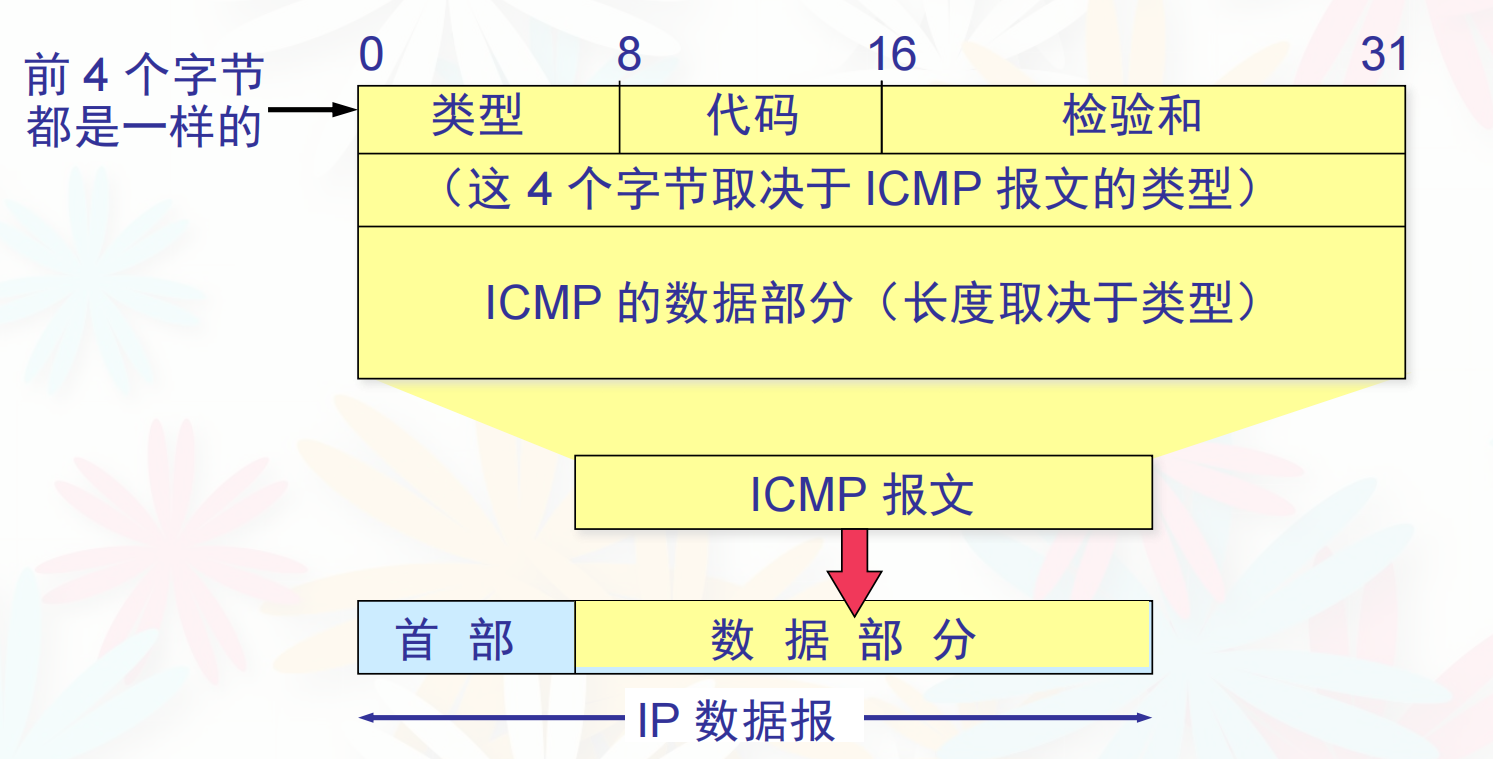
在Filter输入icmp，使其只显示ICMP分组。在DOS窗口输入ping www.bupt.edu.cn，计算机向IP地址211.68.69.240发送ping请求并得到回复。



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。

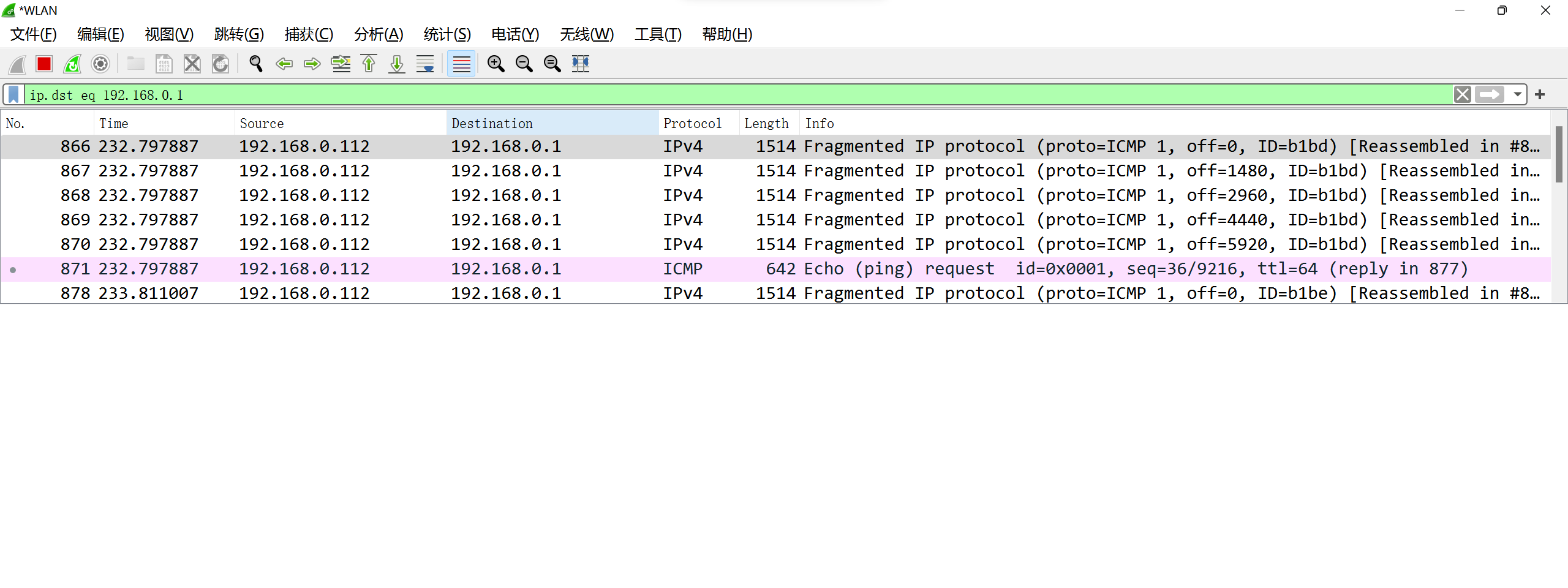
|  |  |
| --- | --- |
| 字段内容 | 内容 |
| 类型 | 8 (Echo (ping) request) |
| 代码 | 0 |
| 检验和 | 0x4d27 |

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**



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。



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 |

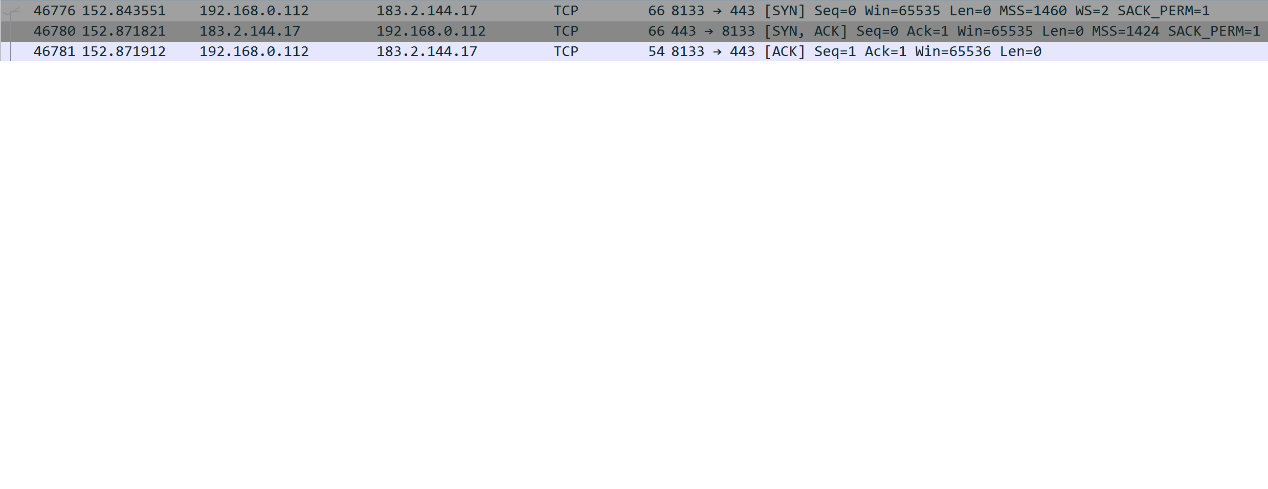
第六个分片的内容如上。

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。



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。

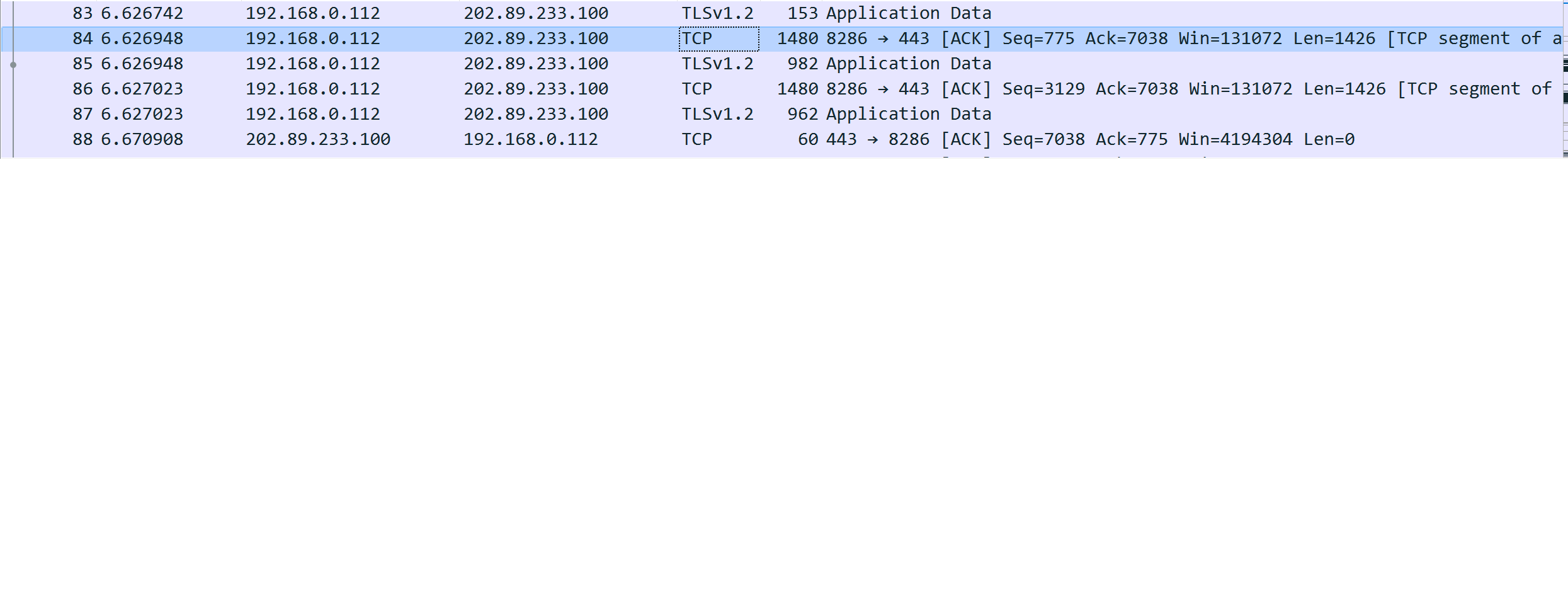
|  |
| --- |
| Frame 46780: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{ED150066-78B6-44F5-AEB0-FFA8360DCFBF}, id 0  Ethernet II, Src: Tp-LinkT\_1f:d8:0c (88:25:93:1f:d8:0c), Dst: LiteonTe\_6b:ee:8d (e0:0a:f6:6b:ee:8d)  Internet Protocol Version 4, Src: 183.2.144.17, 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。

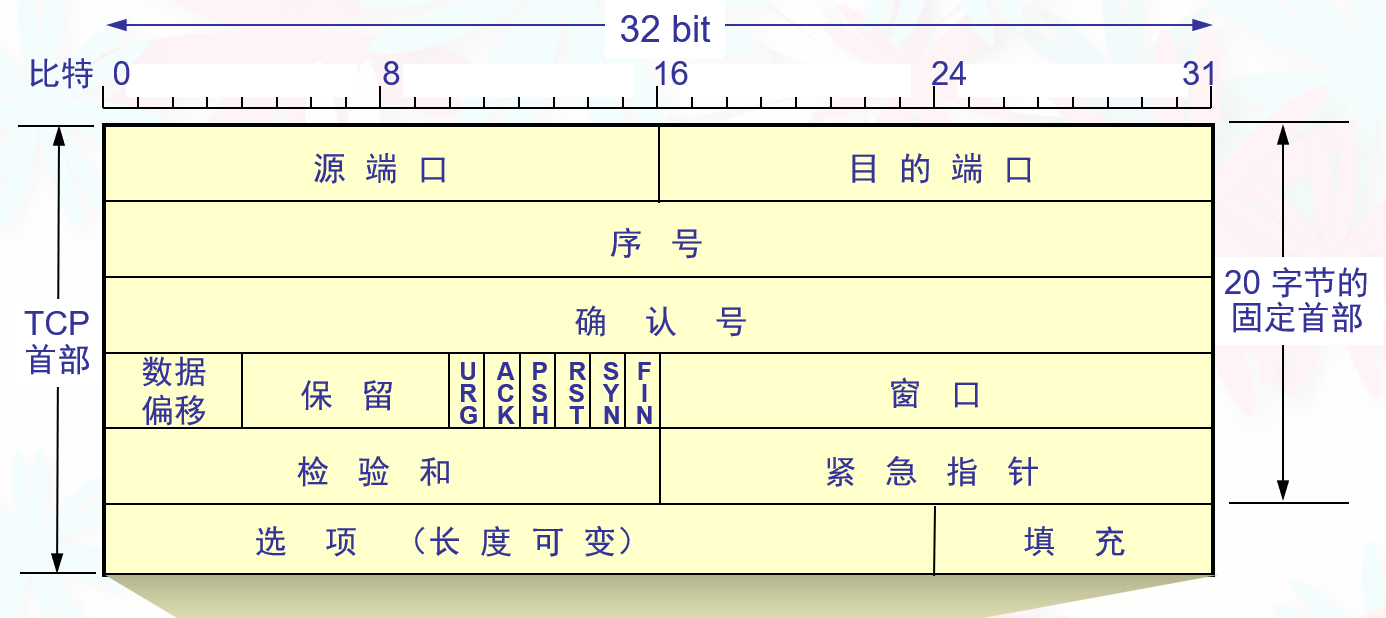
**通信过程**



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。

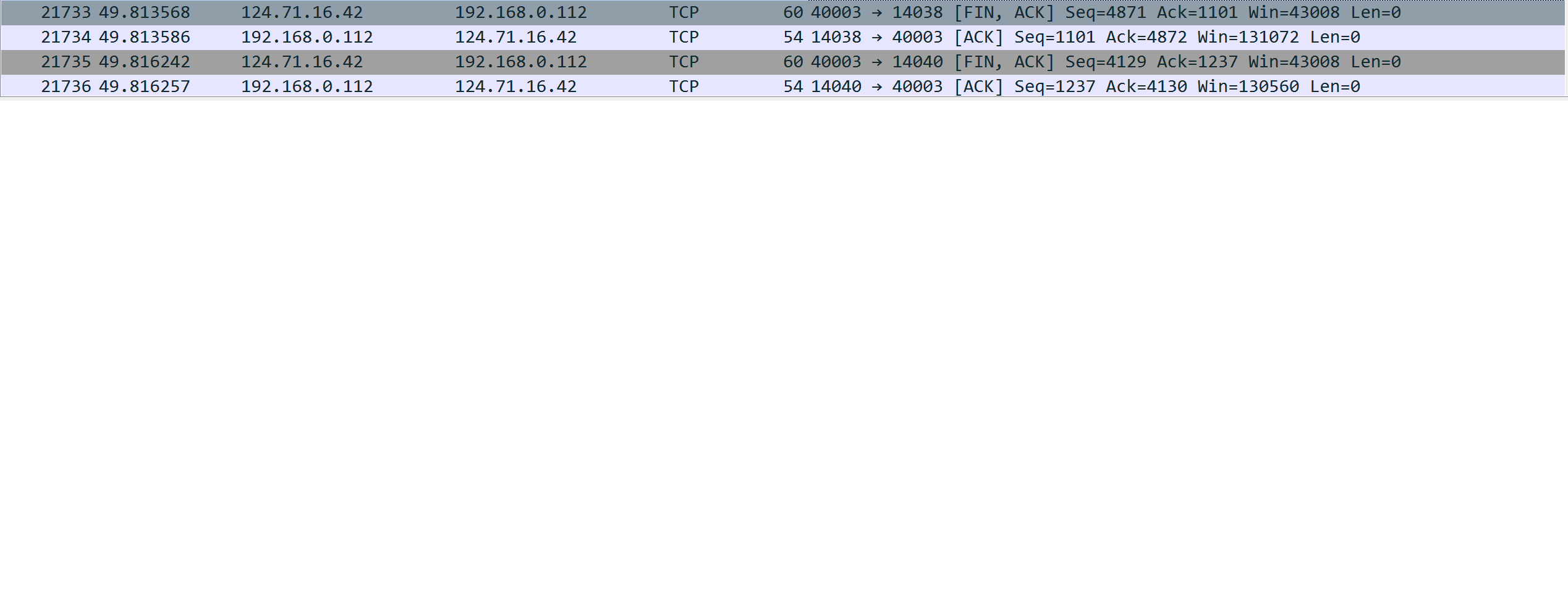


TCP首部格式如上。

|  |  |
| --- | --- |
| 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**



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。