计算机网络实验二：网络层数据分组的捕获和解析 实验报告

毛子恒
2019211397
北京邮电大学 计算机学院

日期：2021 年 6 月 5 日

1 实验内容和实验环境描述

1.1 实验内容

本次实验内容：

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。

1.2 实验环境

- Windows 10 version 1909
- Wireshark Version 3.4.4
- Visual Studio Code 1.56.2

2 实验步骤和网络层分组结构分析

2.1 准备工作

启动计算机，连接网络确保能够上网。断开连接，禁用网卡。

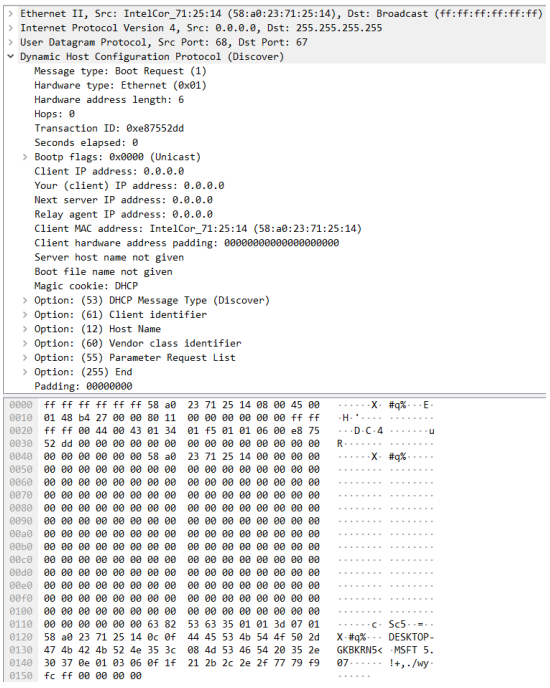
2.2 捕获和分析 DHCP 和 ARP 分组

2.2.1 捕获 DHCP 分组

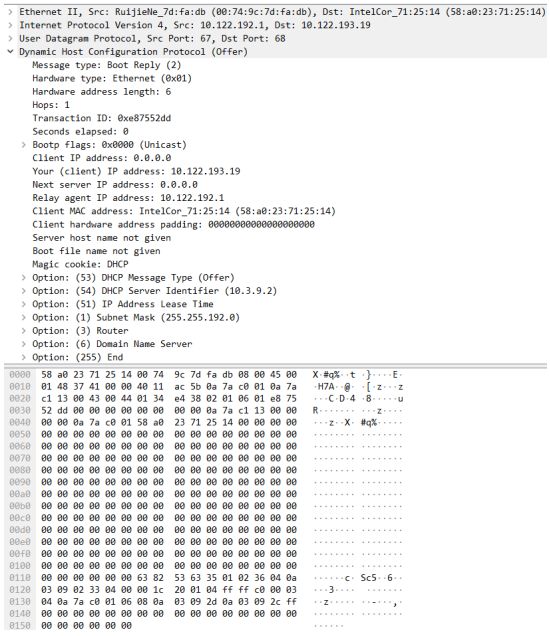
开启监控，连接网络。在 Wireshark 过滤器中输入`dhcp`，过滤出四个 DHCP 分组如图 1。四个 DHCP 分组的内容如图 2。

2	0.011739	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe87552dd
34	1.018784	10.122.192.1	10.122.193.19	DHCP	342	DHCP Offer - Transaction ID 0xe87552dd
35	1.019228	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xe87552dd
37	1.047541	10.122.192.1	10.122.193.19	DHCP	342	DHCP ACK - Transaction ID 0xe87552dd

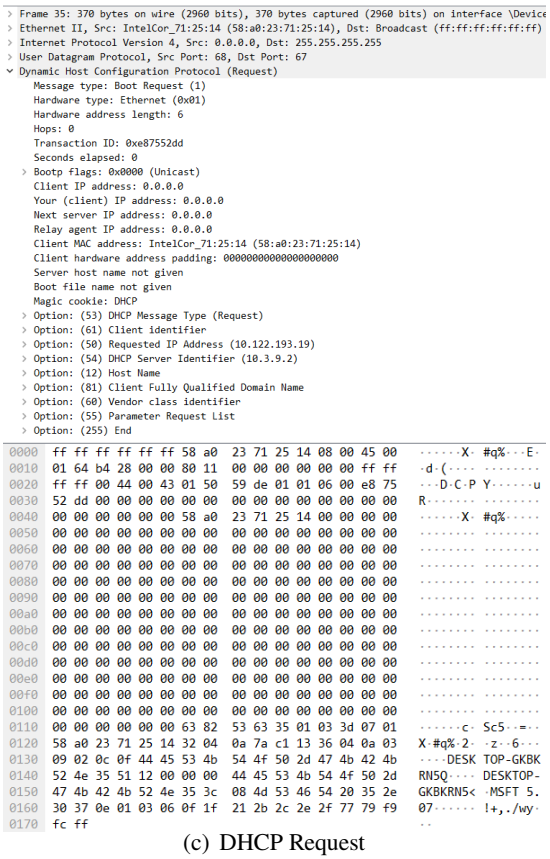
图 1: 捕获到的四个 DHCP 分组



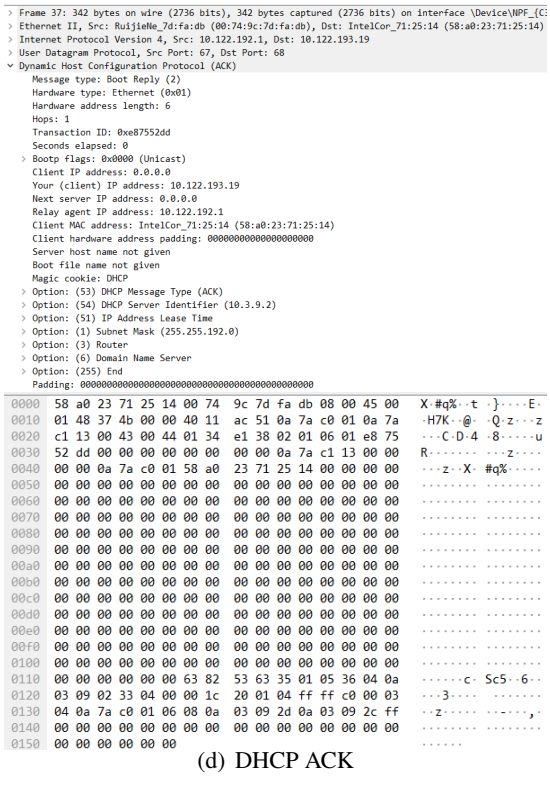
(a) DHCP Discover



(b) DHCP Offer



(c) DHCP Request



(d) DHCP ACK

图 2: 四个 DHCP 分组的内容

2.2.2 分析 DHCP 分组

序号为 2 的 DHCP 分组内容的分析如**表 1**。

表 1: DHCP Discover 分组内容分析

字段 (字节数)	内容（16 进制）	解释
OP (1)	01	消息类型：引导请求
HTYPE (1)	01	硬件地址类型：以太网
HLEN (1)	06	硬件地址长度：6
HOPS (1)	00	经过的 DHCP 中继的数目：0
XID (4)	e8 75 52 dd	处理 ID，标记一次 IP 地址请求过程：0xe87552dd
SECS (2)	00 00	从获取到 IP 地址或者续约过程开始到现在所消耗的时间：0 秒
FLAGS (2)	00 00	标记：第一位为 0，表示单播
CIADDR (4)	00 00 00 00	客户端 IP 地址：0.0.0.0 还未分配 IP 地址
YIADDR (4)	00 00 00 00	你的（客户端）IP 地址（服务器分配的地址）：0.0.0.0 仅在 Offer 和 ACK 分组中有效
SIADDR (4)	00 00 00 00	在 bootstrap 过程中下一台服务器的地址：0.0.0.0 DHCP 服务器未知
GIADDR (4)	00 00 00 00	客户端发出请求分组后经过的第一个中继的地址：0.0.0.0 没有经过中继
CHADDR (16)	58 a0 23 71 25 14	客户端的 MAC 地址：58:a0:23:71:25:14 后接 10 个字节的填充
SNAME (64)	全部为 00	为客户端分配 IP 地址的服务器域名：未给出
FILE (128)	全部为 00	为启动客户端指定的配置文件路径：未给出
magic cookie(4)	63 82 53 63	可选字段的格式：DHCP
OPTION (3)	35 01 01	DHCP 消息类型：Discover
OPTION (9)	3d 07 01 58 a0 23 71 25 14	客户端标识符：以太网，MAC 地址 58:a0:23:71:25:14
OPTION (17)	0c 0f 后略	主机名，长度为 15
OPTION (8)	3c 08 后略	供应商标识符，长度为 8
OPTION (16)	37 0e 后略	参数需求列表，长度为 14
OPTION (1)	ff	选项字段结束

序号为 34、35、37 的 DHCP 分组内容的分析如**表 2**、**表 3**和**表 4**，表中仅展示与第一个分组不同的部分。

2.2.3 分析 DHCP 的工作流程

DHCP 协议用于对连接到网络的设备自动分配 IP 地址和其他通信变量。

1. 客户端连入局域网后，向局域网内发送广播，发送一个 DHCP Discover 分组，分组内容中有本机的 MAC 地址，并在 OPTION 字段中附带一个请求参数的列表。

表 2: DHCP Offer 分组内容分析

字段 (字节数)	内容（16 进制）	解释
OP (1)	02	消息类型：引导回复
HOPS (1)	01	经过的 DHCP 中继的数目：1
YIADDR (4)	0a 7a c1 13	你的（客户端）IP 地址（服务器分配的地址）：10.122.193.19
GIADDR (4)	0a 7a c0 01	客户端发出请求分组后经过的第一个中继的地址：10.122.192.1
OPTION (3)	35 01 02	DHCP 消息类型：Offer
OPTION (6)	36 04 0a 03 09 02	DHCP 服务器标识符：10.3.9.2
OPTION (6)	33 04 00 00 1c 20	IP 地址释放时间：7200 秒
OPTION (6)	01 04 ff ff c0 00	子网掩码：255.255.192.0
OPTION (6)	03 04 0a 7a c0 01	路由器：10.122.192.1
OPTION (10)	06 08 0a 03 09 2d 0a 03 09 2c	域名服务器：10.3.9.45、10.3.9.44
OPTION (1)	ff	选项字段结束

表 3: DHCP Request 分组内容分析

字段 (字节数)	内容（16 进制）	解释
OPTION (3)	35 01 03	DHCP 消息类型：Request
OPTION (9)	3d 07 01 58 a0 23 71 25 14	客户端标识符：以太网，MAC 地址 58:a0:23:71:25:14
OPTION (6)	32 04 0a 7a c1 13	请求的 IP 地址：10.122.193.19
OPTION (6)	36 04 0a 03 09 02	DHCP 服务器标识符：10.3.9.2
省略一部分选项字段		
OPTION (1)	ff	选项字段结束

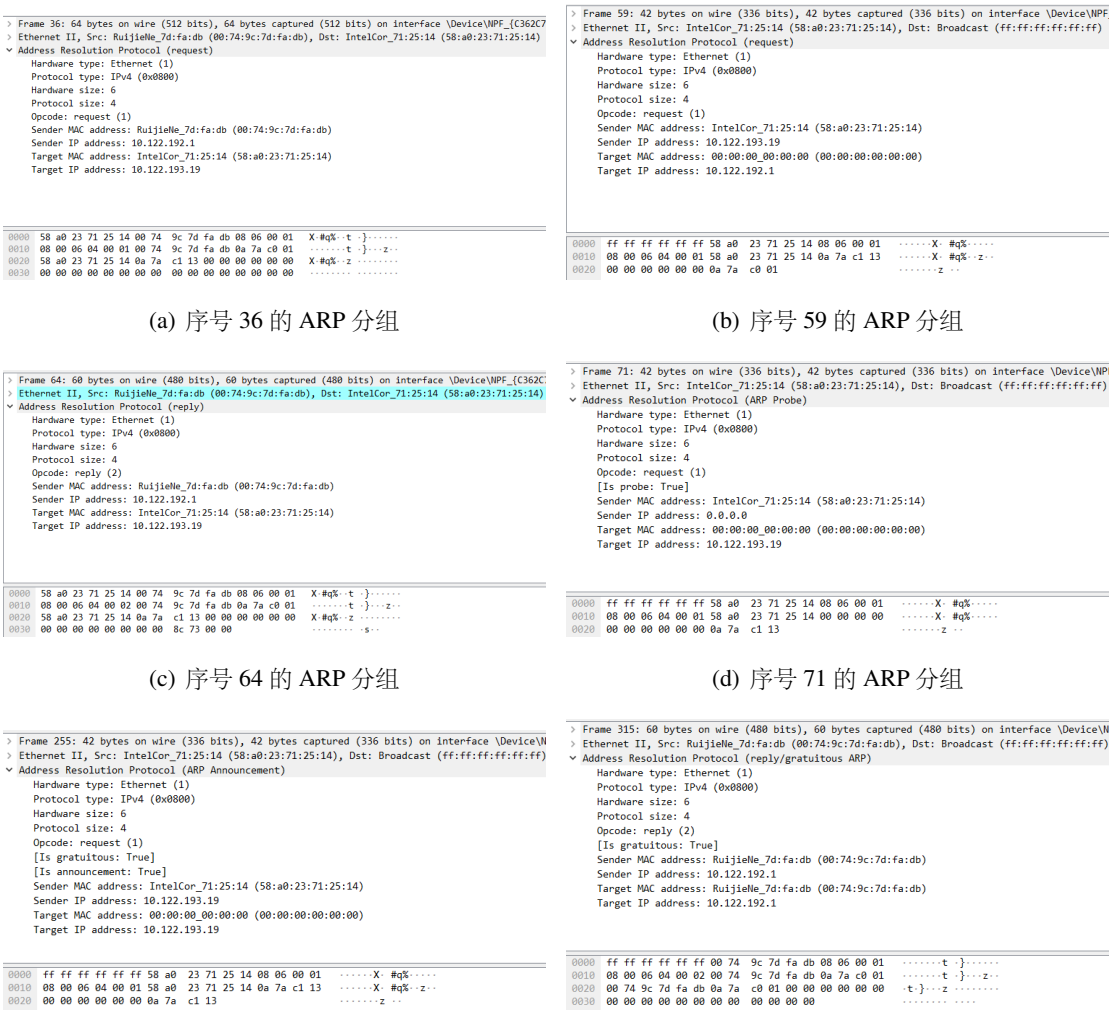
表 4: DHCP ACK 分组内容分析

字段 (字节数)	内容（16 进制）	解释
OP (1)	02	消息类型：引导回复
HOPS (1)	00	经过的 DHCP 中继的数目：1
YIADDR (4)	0a 7a c1 13	你的（客户端）IP 地址（服务器分配的地址）：10.122.193.19
GIADDR (4)	0a 7a c0 01	客户端发出请求分组后经过的第一个中继的地址：10.122.192.1
OPTION (3)	35 01 05	DHCP 消息类型：ACK
省略一部分选项字段		
OPTION (1)	ff	选项字段结束

2. 服务器为客户端分配 IP，并向之前的 MAC 地址发送 DHCP Offer 分组，分组内容中有分配的 IP 地址，分组的 OPTION 字段中附带服务器标识符、IP 租期、子网掩码等信息。
3. 客户端再次发送广播，发送一个 DHCP Request 分组，在 OPTIONS 字段中指明请求的 IP 地址和服务器标识符。
4. 服务器向客户端发送 DHCP ACK 分组确认。

2.2.4 捕获 ARP 分组

在 Wireshark 过滤器中输入`arp`，过滤出数个 ARP 分组。分组的内容如**图 3**。



(a) 序号 36 的 ARP 分组　(b) 序号 59 的 ARP 分组

(c) 序号 64 的 ARP 分组　(d) 序号 71 的 ARP 分组

(e) 序号 255 的 ARP 分组　(f) 序号 315 的 ARP 分组

图 3: ARP 分组的内容

2.2.5 分析 ARP 分组

序号为 36 的 ARP 分组内容的分析如**表 5**。

表 5: 序号为 36 的 ARP 分组内容分析

字段 (字节数)	内容（16 进制）	解释
HTYPE (2)	00 01	硬件类型：以太网
PTYPE (2)	08 00	协议类型：IPv4
HLEN (1)	06	硬件地址长度：6
PLEN (1)	04	协议地址长度：4
OPER (2)	00 01	ARP 消息类型：request
SHA (6)	00 74 9c 7d fa db	发送方 MAC 地址：00:74:9c:7d:fa:db
SPA (4)	0a 7a c0 01	发送方 IP 地址：10.122.192.1
THA (6)	58 a0 23 71 25 14	接收方 MAC 地址：58:a0:23:71:25:14
TPA (6)	0a 7a c1 13	接收方 IP 地址：10.122.193.19

2.2.6 分析 ARP 的工作流程

ARP 协议用于将网络层地址（比如 IPv4），映射到链路层地址（比如 MAC）。

1. 序号为 36 的 ARP 分组发送在 DHCP Request 和 DHCP ACK 之间，此时路由器请求 10.122.193.19 的 MAC 地址，但是此时 IP 地址还没有分配，所以本机没有回复。
2. 序号为 59 的 ARP 分组发送在 IP 地址分配完成之后，本机向局域网发送广播，请求 10.122.192.1，即路由器的 MAC 地址。
3. 序号为 64 的 ARP 分组是对第二个 ARP 的回复，其中 OPER 字段设为 2，表示一个回复分组，分组内容中发送方的部分为路由器的 IP 和 MAC 地址。
4. 序号为 71 的 ARP 分组是一个 ARP 探针 (ARP Probe) 分组，意图是探测 IP 地址在局域网中是否已经被使用，其发送方 MAC 地址被设为本机，发送方 IP 地址和接收方 MAC 地址被设为空，接收方 IP 地址设为想要探测的 IP 地址，即本机的 IP 地址。
5. 序号为 255 的 ARP 分组是一个 ARP 声明 (ARP Announcement) 分组，意图是在局域网中“声明”这个 IP 地址，除了发送方 IP 地址被设为本机 IP 之外，其他内容和 ARP Probe 分组相同，其他主机可以用发送方 IP 和 MAC 地址在 ARP 缓存中建立映射。
6. 序号为 315 的 ARP 分组是一个免费 ARP(Gratuitous ARP) 分组，分组中 OPER 字段设为 2（但是并不意味着对某个请求的回复），发送方 MAC 与接收方 MAC 相同、发送方 IP 与接收方 IP 相同。路由器向局域网广播这个分组，用于让主机更新 ARP 缓存中的映射。

2.3 捕获和分析 IP 分组

2.3.1 捕获 IP 分组

任意捕获一个 IP 分组，如**图 4**。

2.3.2 分析 IP 分组

IP 分组的分析如**表 6**。

数据部分是 UDP 分组和 DNS 查询分组，略。

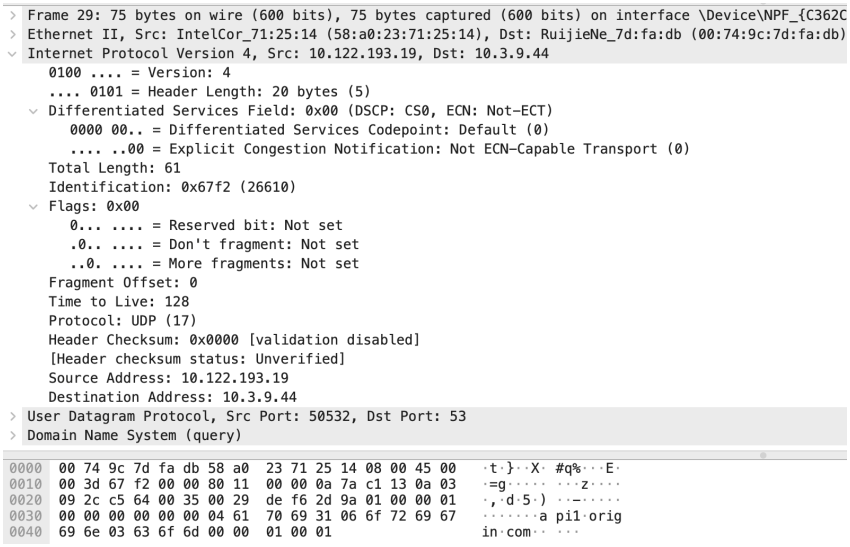


图 4: 序号为 29 的 IP 分组

表 6: 序号为 29 的 IP 分组头分析

字段 (位数)	内容（默认 16 进制）	解释
Version (4)	0100B	版本：4
IHL (4)	0101B	头部长度：20 字节
DSCP (6)	000000B	区分服务信息：默认
ECN (2)	00B	显式拥塞通知：否
Total Length (16)	00 3d	分组总长度：61 字节
Identification (16)	67 f2	分组标识：0x67f2
Flags (3)	000B	Don't Fragment（不要分段）标志位：0 More Fragments（更多的段）标志位：0
Fragment Offset (13)	0000000000000B	分段偏移量：0
TTL (8)	80	生存期：128 跳
Protocol (8)	11	协议：UDP
Header CheckSum (32)	00 00 00 00	头校验和：不验证
Source IP Address (32)	0a 7a c1 13	源地址：10.122.193.19
Destimation IP Address (32)	0a 03 09 2c	目标地址：10.3.9.44

2.3.3 捕获长 IP 分组

获取连接到 BUPT-mobile 的手机的 IP 地址为 10.21.245.157。

在 cmd 中输入指令`ping 10.21.245.157 -n 1 -l 8000`，向手机发送一个长度为 8000 的 IP 数据包。

运行结果如图 **5**。

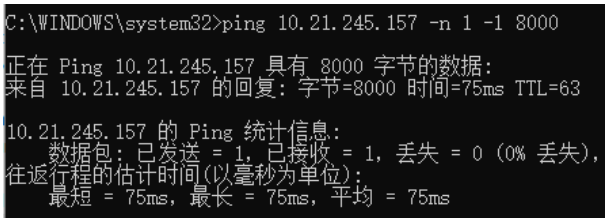


图 5: `ping`指令运行结果

在 Wireshark 过滤器中输入`ip.src eq 10.122.193.19 or ip.dst eq 10.122.193.19`，过滤出 12 个分组如图 **6**。

14	1.896422	10.122.193.19	10.21.245.157	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5b83) [Reassembled in #19]
15	1.896422	10.122.193.19	10.21.245.157	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=5b83) [Reassembled in #19]
16	1.896422	10.122.193.19	10.21.245.157	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=5b83) [Reassembled in #19]
17	1.896422	10.122.193.19	10.21.245.157	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=5b83) [Reassembled in #19]
18	1.896422	10.122.193.19	10.21.245.157	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5920, ID=5b83) [Reassembled in #19]
19	1.896422	10.122.193.19	10.21.245.157	ICMP	642	Echo (ping) request id=0x0001, seq=144/36864, ttl=128 (reply in 27)
22	1.970962	10.21.245.157	10.122.193.19	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=1fbc) [Reassembled in #27]
23	1.971941	10.21.245.157	10.122.193.19	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=1fbc) [Reassembled in #27]
24	1.971941	10.21.245.157	10.122.193.19	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=1fbc) [Reassembled in #27]
25	1.971941	10.21.245.157	10.122.193.19	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=1fbc) [Reassembled in #27]
26	1.971941	10.21.245.157	10.122.193.19	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5920, ID=1fbc) [Reassembled in #27]
27	1.971941	10.21.245.157	10.122.193.19	ICMP	642	Echo (ping) reply id=0x0001, seq=144/36864, ttl=63 (request in 19)

图 6: 捕获到的 12 个 IP 分组

限于篇幅原因，仅展示序号为 14 的 IP 分组的内容，如图 **7**。

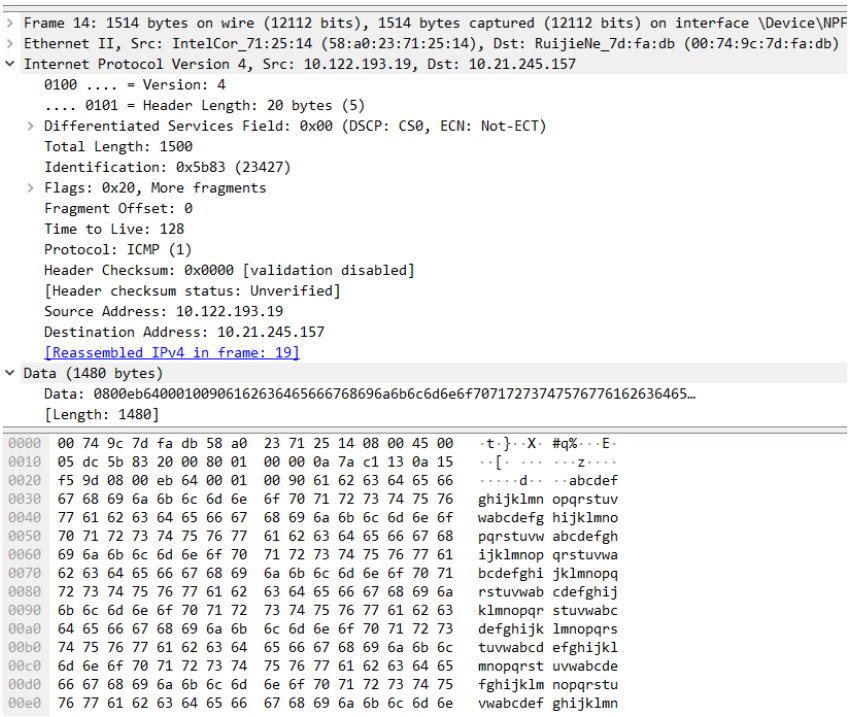


图 7: 序号为 14 的 IP 分组的内容

2.3.4 分析长 IP 分组

序号为 14 的 IP 分组的分组头部分的分析如**表 7**。

表 7: 序号为 14 的 IP 分组头分析

字段 (位数)	内容（默认 16 进制）	解释
Version (4)	0100B	版本：4
IHL (4)	0101B	头部长度：20 字节
DSCP (6)	000000B	区分服务信息：默认
ECN (2)	00B	显式拥塞通知：否
Total Length (16)	05 dc	分组总长度：1500 字节
Identification (16)	5b 83	分组标识：0x5b83
Flags (3)	001B	Don't Fragment（不要分段）标志位：0 More Fragments（更多的段）标志位：1
Fragment Offset (13)	0000000000000B	分段偏移量：0
TTL (8)	80	生存期：128 跳
Protocol (8)	01	协议：ICMP
Header CheckSum (32)	00 00 00 00	头校验和：不验证
Source IP Address (32)	0a 7a c1 13	源地址：10.122.193.19
Destimation IP Address (32)	0a 15 f5 9d	目标地址：10.21.245.157

前六个分组的分组头的大部分内容都一致，它们的 MF 标志位以及分段偏移量的对比如**表 8**。

表 8: IP 分组头对比

分组序号	MF 标志位	分段偏移量
14	1	0
15	1	$185 \times 8 = 1480$
16	1	$370 \times 8 = 2960$
17	1	$555 \times 8 = 4440$
18	1	$740 \times 8 = 5920$
19	0	$925 \times 8 = 7400$

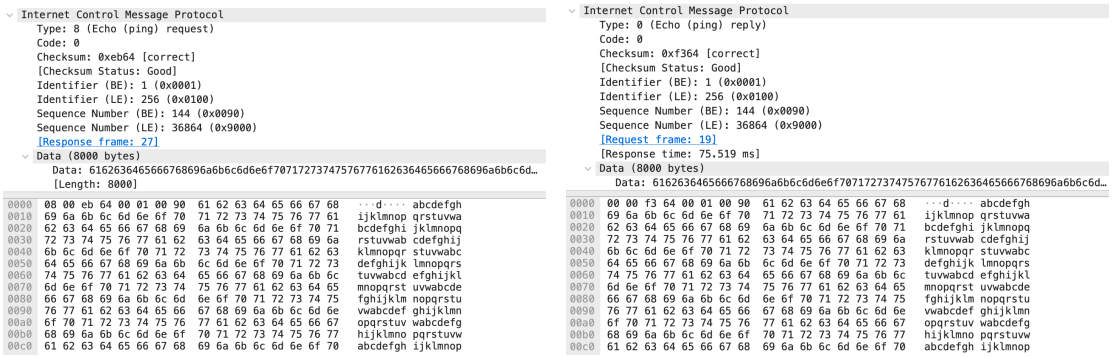
由于以太网数据链路层的 MTU 为 1500 字节，除去头之后剩余 1480 字节，正好是 8 的倍数，因此长度为 8000 字节的数据被拆分成 6 个分段，前五个的长度为 1480 字节，最后一个的长度为 600 字节，分段偏移量表示该分段在原数据段中的位置，通过 MF 标志位为 0 确定数据的结束。

2.4 捕获和分析 ICMP 分组

2.4.1 分析 ping 命令产生的 ICMP 分组

`ping`命令产生的 ICMP 分组的内容如**图 8**。

序号为 19 的 ICMP 分组头的分析如**表 9**。



(a) 序号为 19 的 ICMP 分组　　(b) 序号为 27 的 ICMP 分组

图 8: `ping`命令产生的 ICMP 分组的内容

表 9: 序号为 19 的 ICMP 分组头分析

字段 (字节数)	内容（16 进制）	解释
Type (1)	08	类型
Code (1)	00	与 Type 字段共同构成 Control Message：Echo Request
Checksum (2)	eb 64	校验和：0xeb64
Identifier (2)	00 01	标识符，用于区分不同进程 ping 消息
Sequence Number (2)	00 90	ping 请求序号

序号为 27 的 ICMP 分组是对上一个分组的回复，其分组头除了 Type 字段改为 0，表示 Echo Reply，以及校验和发生变化之外，其他和第一个 ICMP 分组头没有区别。

2.4.2 捕获 tracert 命令产生的 ICMP 分组

在 cmd 中输入指令`tracert -d 10.21.245.157`，追踪从本机到手机的路由。

运行结果如图 9。

图 9: `tracert`指令运行结果

在 Wireshark 过滤器中输入`icmp`，过滤出 12 个分组如图 10。其中有三对 TTL 为 1 的`ping`请求和回复，还有三对 TTL 为 2 的请求和回复。

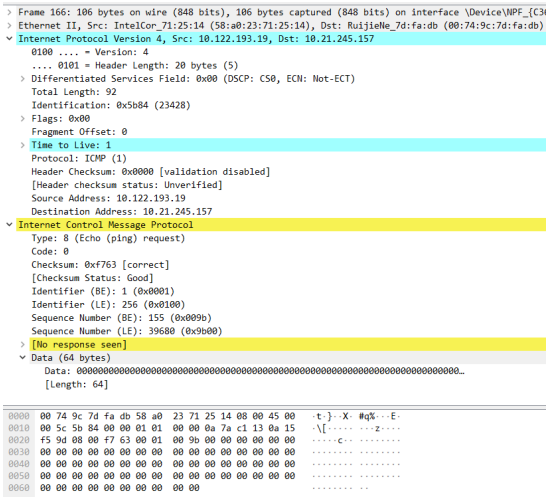
其中序号为 166、167、10、182 的 ICMP 分组的内容如图 11。

序号为 166 的分组的 IP 部分的 TTL 为 1，ICMP 分组头的分析如表 10。

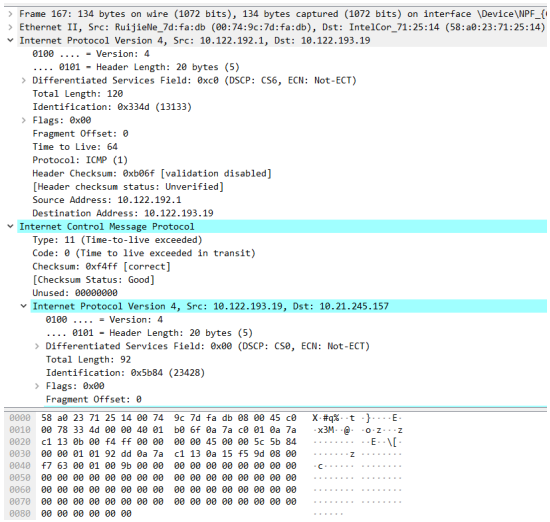
这个分组经过一跳之后，TTL 变为 0，路由器返回超时信息，即序号为 167 的分组，其数据部分附带原来分组的的 IP 头部和 8 个字节的 ICMP 头部，其 ICMP 分组分析如表 11。

166	15.741802	10.122.193.19	10.21.245.157	ICMP	106 Echo (ping) request id=0x0001, seq=155/39680, ttl=1 (no response found!)
167	15.743199	10.122.192.1	10.122.193.19	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
168	15.743540	10.122.193.19	10.21.245.157	ICMP	106 Echo (ping) request id=0x0001, seq=156/39936, ttl=1 (no response found!)
169	15.744672	10.122.192.1	10.122.193.19	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
170	15.745004	10.122.193.19	10.21.245.157	ICMP	106 Echo (ping) request id=0x0001, seq=157/40192, ttl=1 (no response found!)
171	15.746924	10.122.192.1	10.122.193.19	ICMP	134 Time-to-live exceeded (Time to live exceeded in transit)
180	16.760817	10.122.193.19	10.21.245.157	ICMP	106 Echo (ping) request id=0x0001, seq=158/40448, ttl=2 (reply in 182)
182	16.817800	10.21.245.157	10.122.193.19	ICMP	106 Echo (ping) reply id=0x0001, seq=158/40448, ttl=63 (request in 180)
184	16.819359	10.122.193.19	10.21.245.157	ICMP	106 Echo (ping) request id=0x0001, seq=159/40704, ttl=2 (reply in 185)
185	16.825162	10.21.245.157	10.122.193.19	ICMP	106 Echo (ping) reply id=0x0001, seq=159/40704, ttl=63 (request in 184)
186	16.826240	10.122.193.19	10.21.245.157	ICMP	106 Echo (ping) request id=0x0001, seq=160/40960, ttl=2 (reply in 187)
187	16.834917	10.21.245.157	10.122.193.19	ICMP	106 Echo (ping) reply id=0x0001, seq=160/40960, ttl=63 (request in 186)

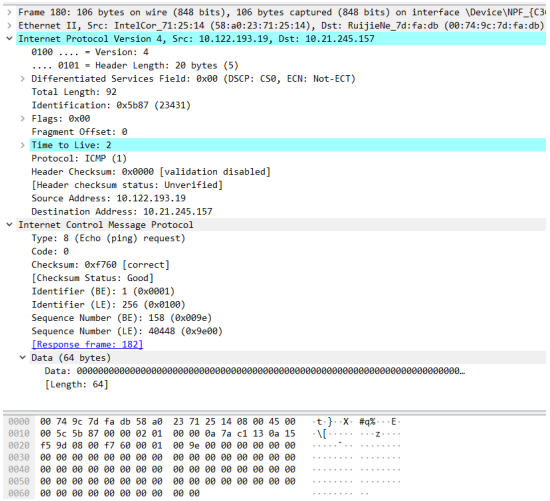
图 **10:** 捕获到的 12 个 ICMP 分组



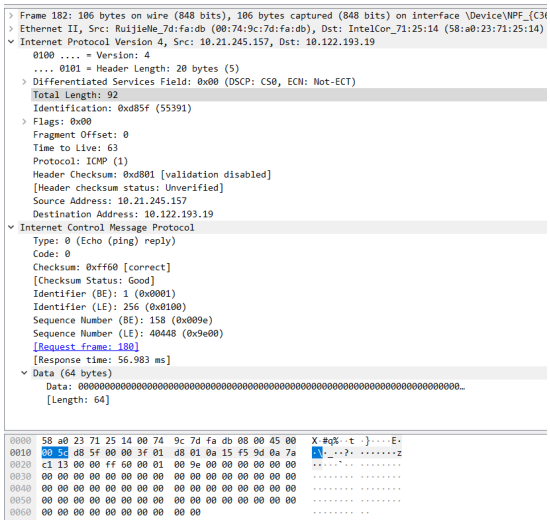
(a) 序号为 166 的 ICMP 分组



(b) 序号为 167 的 ICMP 分组



(c) 序号为 180 的 ICMP 分组



(d) 序号为 182 的 ICMP 分组

图 **11:** `tracert`命令产生的 ICMP 分组的内容

表 10: 序号为 166 的 ICMP 分组头分析

字段 (字节数)	内容（16 进制）	解释
Type (1)	08	类型
Code (1)	00	与 Type 字段共同构成 Control Message：Echo Request
Checksum (2)	f7 63	校验和：0xf763
Identifier (2)	00 01	标识符，用于区分不同进程 ping 消息
Sequence Number (2)	00 9b	ping 请求序号

表 11: 序号为 167 的 ICMP 分组分析

字段 (字节数)	内容（16 进制）	解释
Type (1)	11	类型
Code (1)	00	与 Type 字段共同构成 Control Message：TTL expired in transit
Checksum (2)	f4 ff	校验和：0xf4ff
- (4)	00 00 00 00	未使用
IPv4 报文头 (20)	略	序号为 166 的分组的 IP 头
ICMP (8)	略	序号为 166 的分组的 ICMP 头

本机经过两跳之后就能到达手机，于是 TTL 为 2 时可以收到回复。序号为 180、182 的分组的 ICMP 头分析如**表 12**、**表 13**。

表 12: 序号为 180 的 ICMP 分组头分析

字段 (字节数)	内容（16 进制）	解释
Type (1)	08	类型
Code (1)	00	与 Type 字段共同构成 Control Message：Echo Request
Checksum (2)	f7 60	校验和：0xf760
Identifier (2)	00 01	标识符，用于区分不同进程 ping 消息
Sequence Number (2)	00 9e	ping 请求序号

表 13: 序号为 182 的 ICMP 分组头分析

字段 (字节数)	内容（16 进制）	解释
Type (1)	00	类型
Code (1)	00	与 Type 字段共同构成 Control Message：Echo Reply
Checksum (2)	ff 60	校验和：0xff60
Identifier (2)	00 01	标识符，用于区分不同进程 ping 消息
Sequence Number (2)	00 9e	ping 请求序号

3 实验总结和心得体会

完成本实验大约耗费我 4 个小时的时间，其中主要的时间花费在查阅英文文档上，这使我查找和阅读英文文档的能力有所增强。

调试时，我学习并且灵活运用了 Wireshark 的筛选功能，从诸多报文中筛选需要的一部分，节省了许多时间。

在本次实验过程中，我主要查阅相关 RFC 文档、wiki 和 Wireshark 的帮助文档，通过与课本上理论知识联系，对 IP、DHCP、ARP、ICMP 协议报文的内容和部分功能有了初步的认识，对其作用原理有更深刻的理解。