浙大城市学院实验报告

- 课程名称：计算机网络实验
- 实验项目名称：实验十一 Wireshark网络抓包基础
- 学生姓名：徐彬涵
- 专业班级：软件工程2003
- 学号：32001272
- 实验成绩：
- 指导老师：霍梅梅
- 日期：2022/05/05

一. 实验目的和要求

1. 掌握Wireshark软件的安装
2. 学习Wireshark过滤规则的设置
3. 使用Wireshark捕获Ethernet帧，并对Ethernet帧和协议数据包进行分析

二. 实验内容、原理及实验结果与分析

1、安装Wireshark软件

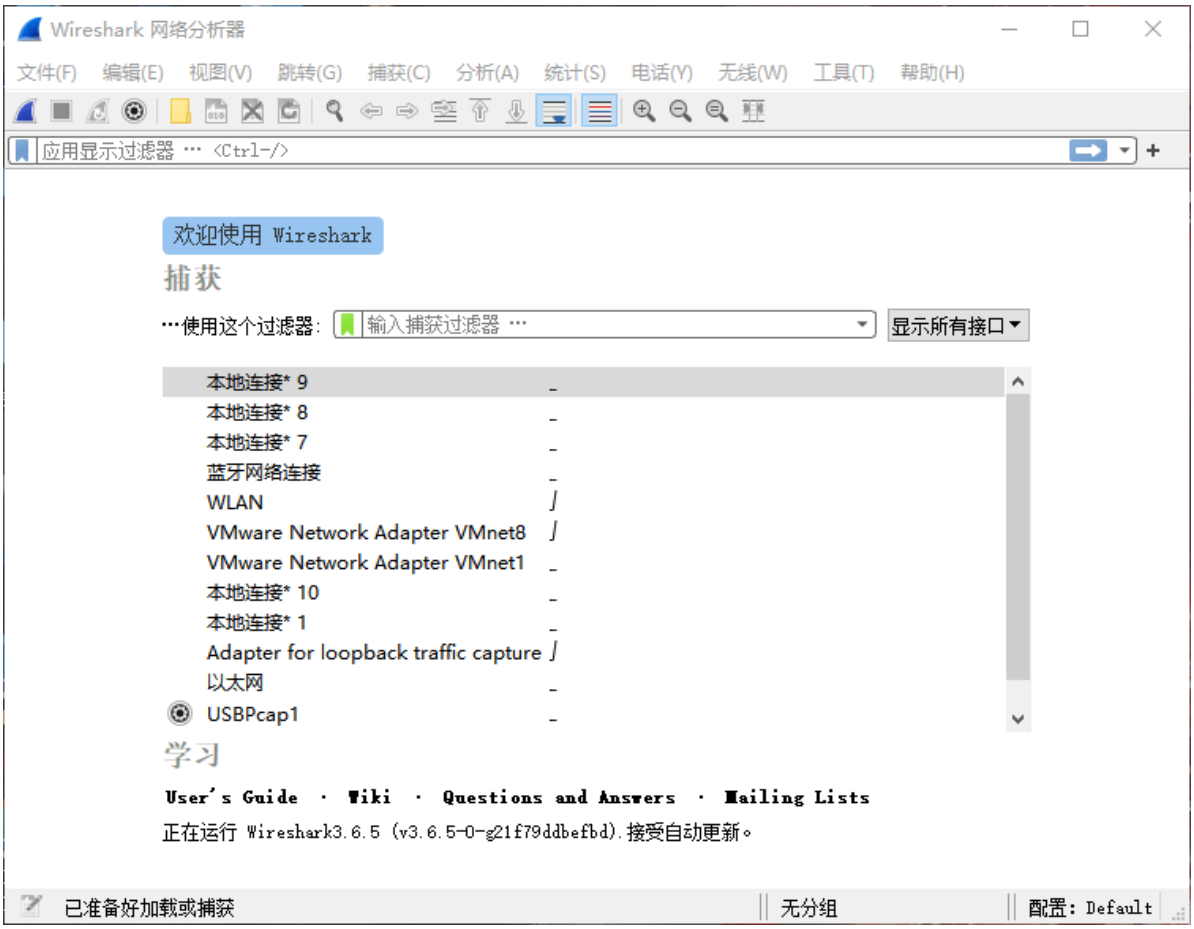
1.1 安装Wireshark

下载地址：**ftp://10.66.28.222:2007**

或 https://www.wireshark.org/download.html

参考教程：https://www.wireshark.org/docs/wsug_html_chunked/

【实验结果与分析】

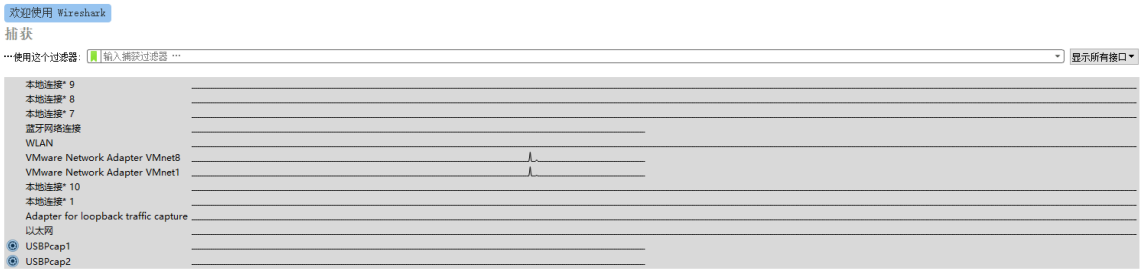


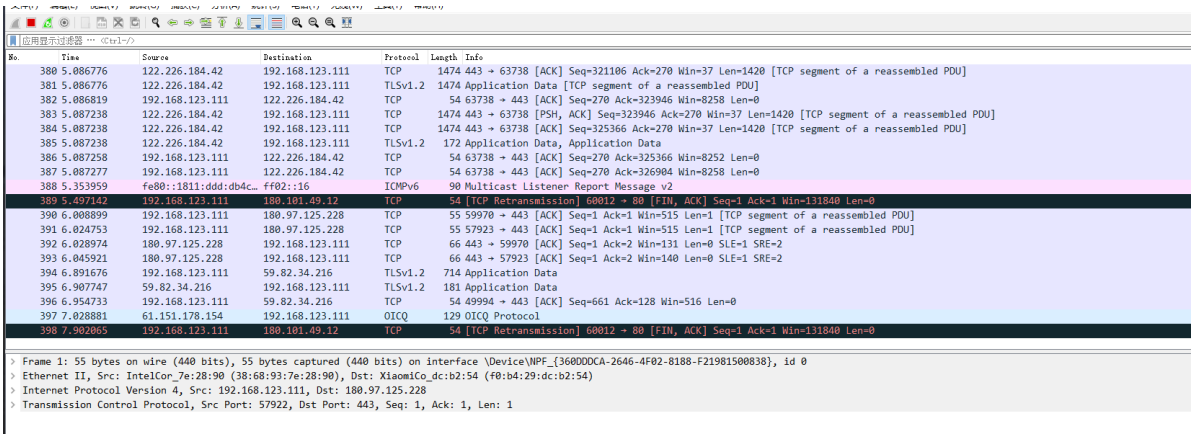
2、在Wireshark中创建并设置以下普通过滤规则

2.1 捕获本地主机收到和发出的所有数据包

【过滤规则】

空白字符

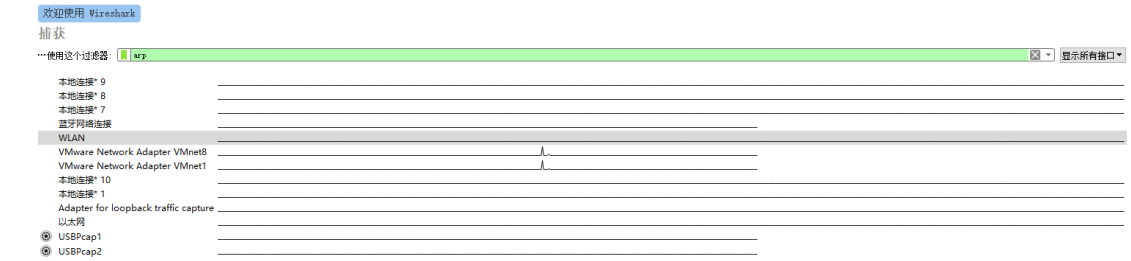


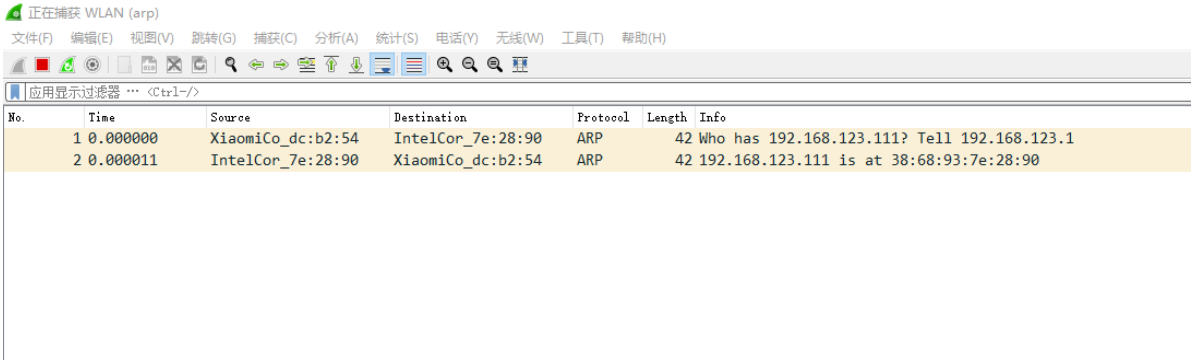


2.2 捕获本地主机收到和发出的所有ARP包

【过滤规则】

```
1 arp
```

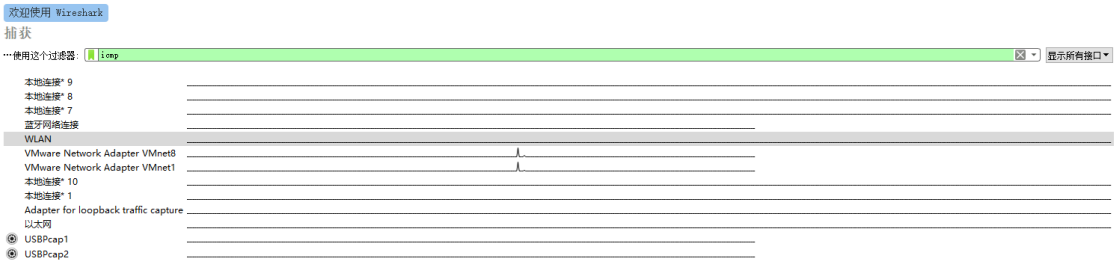


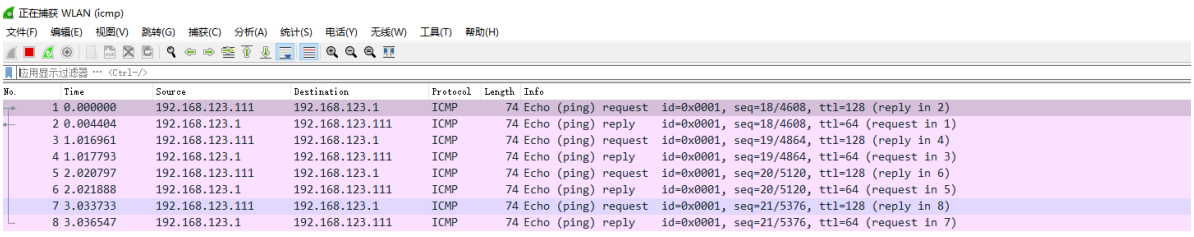


2.3 捕获局域网上所有的ICMP包

【过滤规则】

```
1 icmp
```

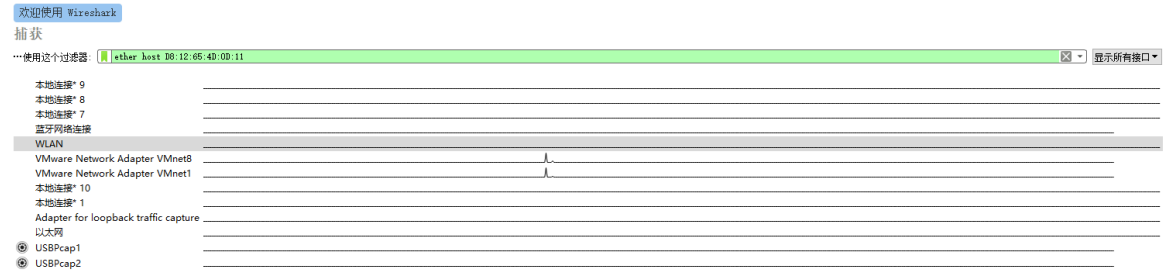


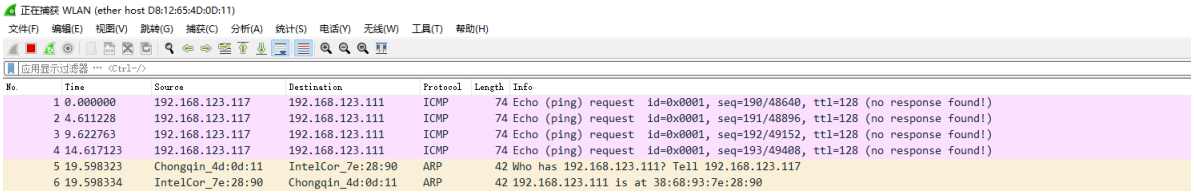


2.4 捕获MAC地址为00-06-68-16-38-80(替换成隔壁主机的MAC地址)的数据包

【过滤规则】

```
ether host D8:12:65:4D:0D:11
```

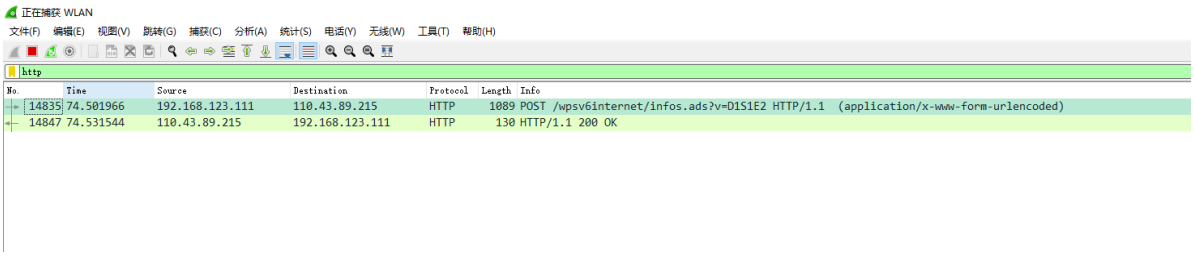




2.5 捕获本地主机收到和发出的HTTP包

【过滤规则】

```
http
```



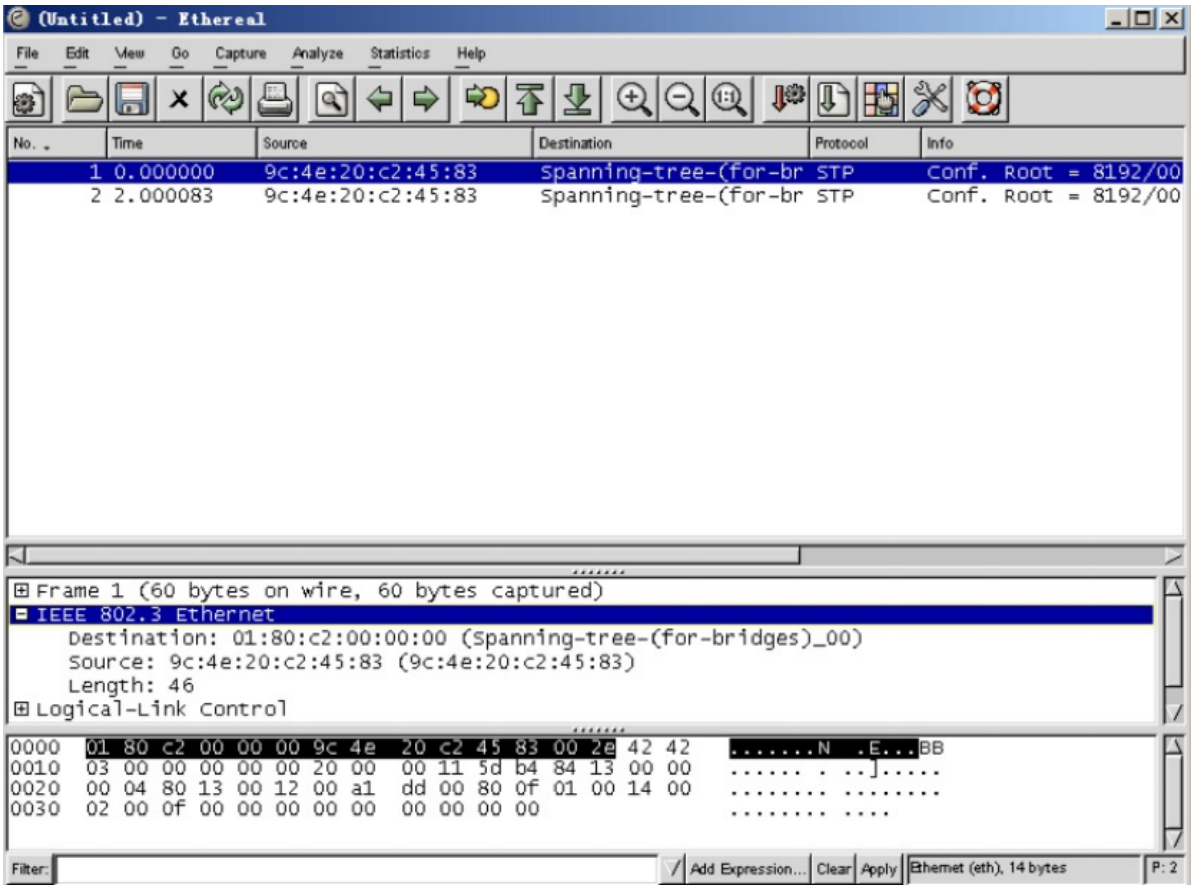
3、捕获并解析Ethernet帧及协议

3.1 捕获解析本机发出或接收的Ethernet 802.3格式的帧，并对照帧格式进行解释

【过滤规则】

```
ether[12:2]<=1500
```

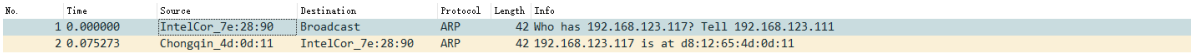
【实验结果与分析】



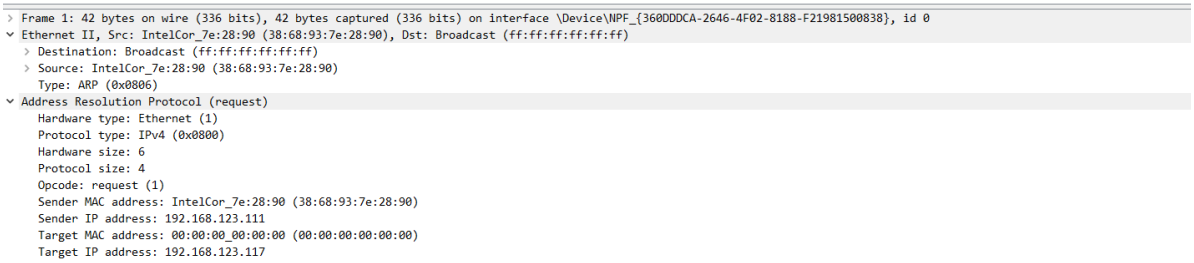
长度	6字节	6字节	2字节
字段	Destination Address（目标地址）	Source Address(源地址)	Length(长度)
值	01:80:c2:00:00:00	9c:4e:20:c2:45:83	46

3.2 捕获解析本地主机发出及收到的**ARP**数据包，解释**ARP**广播帧的内容及返回数据包信息（如**ping**一台旁边没连接过的电脑，捕获**ARP**数据包）

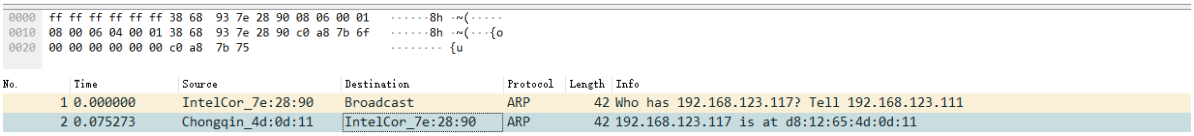
【实验结果与分析】



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	IntelCor_7e:28:90	Broadcast	ARP	42	Who has 192.168.123.117? Tell 192.168.123.111
2	0.075273	Chongqin_4d:0d:11	IntelCor_7e:28:90	ARP	42	192.168.123.117 is at d8:12:65:4d:0d:11

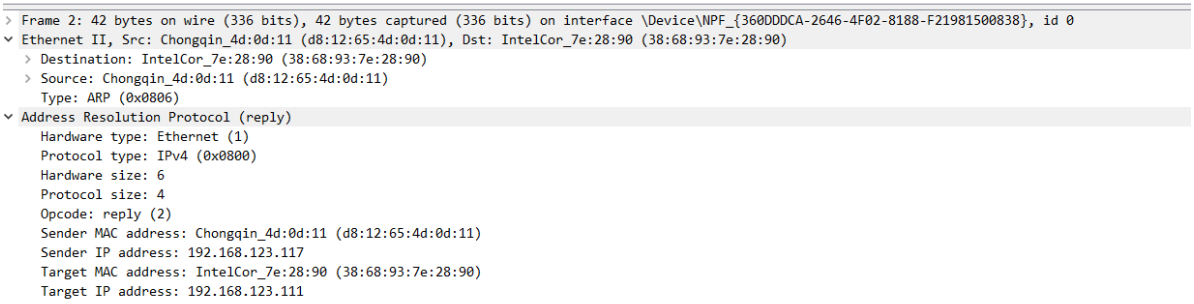


```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{360DDDCA-2646-4F02-8188-F21981500838}, id 0
v Ethernet II, Src: IntelCor_7e:28:90 (38:68:93:7e:28:90), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_7e:28:90 (38:68:93:7e:28:90)
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_7e:28:90 (38:68:93:7e:28:90)
    Sender IP address: 192.168.123.111
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.123.117
```



```
0000  ff ff ff ff ff ff 38 68  93 7e 28 90 08 06 00 01   ......8h .~(.....
0010  08 00 06 04 00 01 38 68  93 7e 28 90 c0 a8 7b 6f   ......8h .~(...{o
0020  00 00 00 00 00 00 c0 a8  7b 75                     ........ {u
```


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	IntelCor_7e:28:90	Broadcast	ARP	42	Who has 192.168.123.117? Tell 192.168.123.111
2	0.075273	Chongqin_4d:0d:11	IntelCor_7e:28:90	ARP	42	192.168.123.117 is at d8:12:65:4d:0d:11



```
> Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{360DDDCA-2646-4F02-8188-F21981500838}, id 0
v Ethernet II, Src: Chongqin_4d:0d:11 (d8:12:65:4d:0d:11), Dst: IntelCor_7e:28:90 (38:68:93:7e:28:90)
  > Destination: IntelCor_7e:28:90 (38:68:93:7e:28:90)
  > Source: Chongqin_4d:0d:11 (d8:12:65:4d:0d:11)
    Type: ARP (0x0806)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Chongqin_4d:0d:11 (d8:12:65:4d:0d:11)
    Sender IP address: 192.168.123.117
    Target MAC address: IntelCor_7e:28:90 (38:68:93:7e:28:90)
    Target IP address: 192.168.123.111
```

长度（字节）	**2**	**2**	**1**	**1**	**2**
字段	Hardware type（硬件类型）	Protocol type（协议类型）	Hardware size（硬件地址长度）	Protocol size（协议地址长度）	Opcode（操作类型）
值	0x0001	0x0800	6	4	0x0001(request)/0x0002(reply)

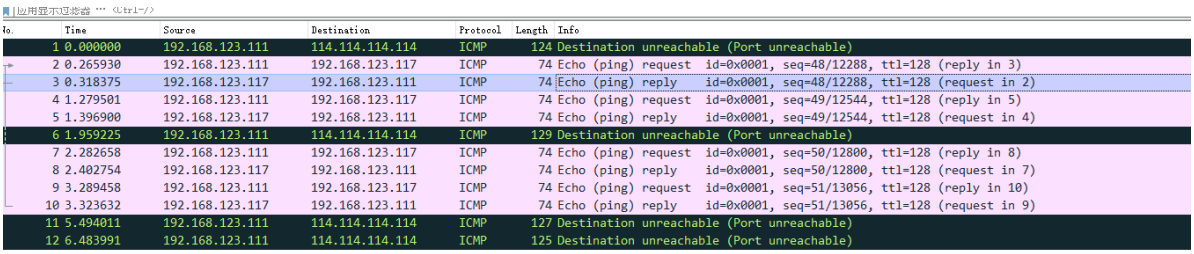
长度（字节）	6	4	6	4
字段	Sender MAC address（发送端MAC地址）	Sender IP address（发送端IP地址）	Target MAC address（目的MAC地址）	Target IP address（目的IP地址）
值	38:68:93:7e:28:90	192.168.123.111	00:00:00:00:00:00	192.168.123.117

3.3 捕获解析局域网上所有的ICMP包，并进行解释（ping一台其他主机）

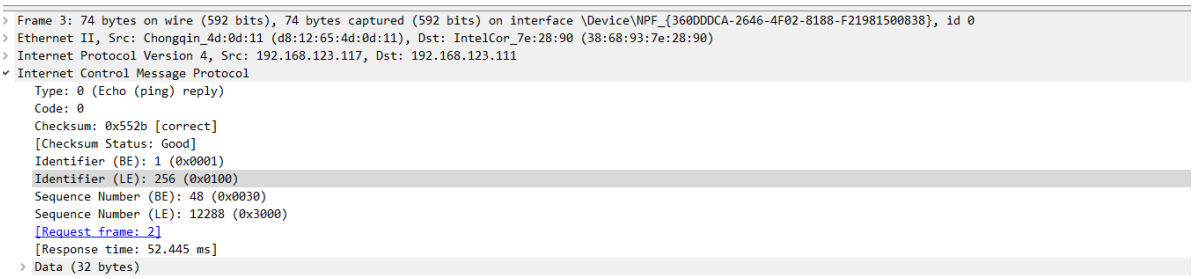
【实验结果与分析】

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.123.111	114.114.114.114	ICMP	124	Destination unreachable (Port unreachab
2	0.265930	192.168.123.111	192.168.123.117	ICMP	74	Echo (ping) request id=0x0001, seq=48/
3	0.318375	192.168.123.117	192.168.123.111	ICMP	74	Echo (ping) reply id=0x0001, seq=48/
4	1.279501	192.168.123.111	192.168.123.117	ICMP	74	Echo (ping) request id=0x0001, seq=49/
5	1.396900	192.168.123.117	192.168.123.111	ICMP	74	Echo (ping) reply id=0x0001, seq=49/
6	1.959225	192.168.123.111	114.114.114.114	ICMP	129	Destination unreachable (Port unreachab
7	2.282658	192.168.123.111	192.168.123.117	ICMP	74	Echo (ping) request id=0x0001, seq=50/
8	2.402754	192.168.123.117	192.168.123.111	ICMP	74	Echo (ping) reply id=0x0001, seq=50/
9	3.289458	192.168.123.111	192.168.123.117	ICMP	74	Echo (ping) request id=0x0001, seq=51/
10	3.323632	192.168.123.117	192.168.123.111	ICMP	74	Echo (ping) reply id=0x0001, seq=51/
11	5.494011	192.168.123.111	114.114.114.114	ICMP	127	Destination unreachable (Port unreachab
12	6.483991	192.168.123.111	114.114.114.114	ICMP	125	Destination unreachable (Port unreachab

```
> Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{360DDDCA-2646-4F02-8188
> Ethernet II, Src: IntelCor_7e:28:90 (38:68:93:7e:28:90), Dst: Chongqin_4d:0d:11 (d8:12:65:4d:0d:11)
> Internet Protocol Version 4, Src: 192.168.123.111, Dst: 192.168.123.117
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d2b [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 48 (0x0030)
    Sequence Number (LE): 12288 (0x3000)
    [Response frame: 3]
  > Data (32 bytes)
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.123.111	114.114.114.114	ICMP	124	Destination unreachable (Port unreachable)
2	0.265930	192.168.123.111	192.168.123.117	ICMP	74	Echo (ping) request id=0x0001, seq=48/12288, ttl=128 (reply in 3)
3	0.318375	192.168.123.117	192.168.123.111	ICMP	74	Echo (ping) reply id=0x0001, seq=48/12288, ttl=128 (request in 2)
4	1.279501	192.168.123.111	192.168.123.117	ICMP	74	Echo (ping) request id=0x0001, seq=49/12544, ttl=128 (reply in 5)
5	1.396900	192.168.123.117	192.168.123.111	ICMP	74	Echo (ping) reply id=0x0001, seq=49/12544, ttl=128 (request in 4)
6	1.959225	192.168.123.111	114.114.114.114	ICMP	129	Destination unreachable (Port unreachable)
7	2.282658	192.168.123.111	192.168.123.117	ICMP	74	Echo (ping) request id=0x0001, seq=50/12800, ttl=128 (reply in 8)
8	2.402754	192.168.123.117	192.168.123.111	ICMP	74	Echo (ping) reply id=0x0001, seq=50/12800, ttl=128 (request in 7)
9	3.289458	192.168.123.111	192.168.123.117	ICMP	74	Echo (ping) request id=0x0001, seq=51/13056, ttl=128 (reply in 10)
10	3.323632	192.168.123.117	192.168.123.111	ICMP	74	Echo (ping) reply id=0x0001, seq=51/13056, ttl=128 (request in 9)
11	5.494011	192.168.123.111	114.114.114.114	ICMP	127	Destination unreachable (Port unreachable)
12	6.483991	192.168.123.111	114.114.114.114	ICMP	125	Destination unreachable (Port unreachable)

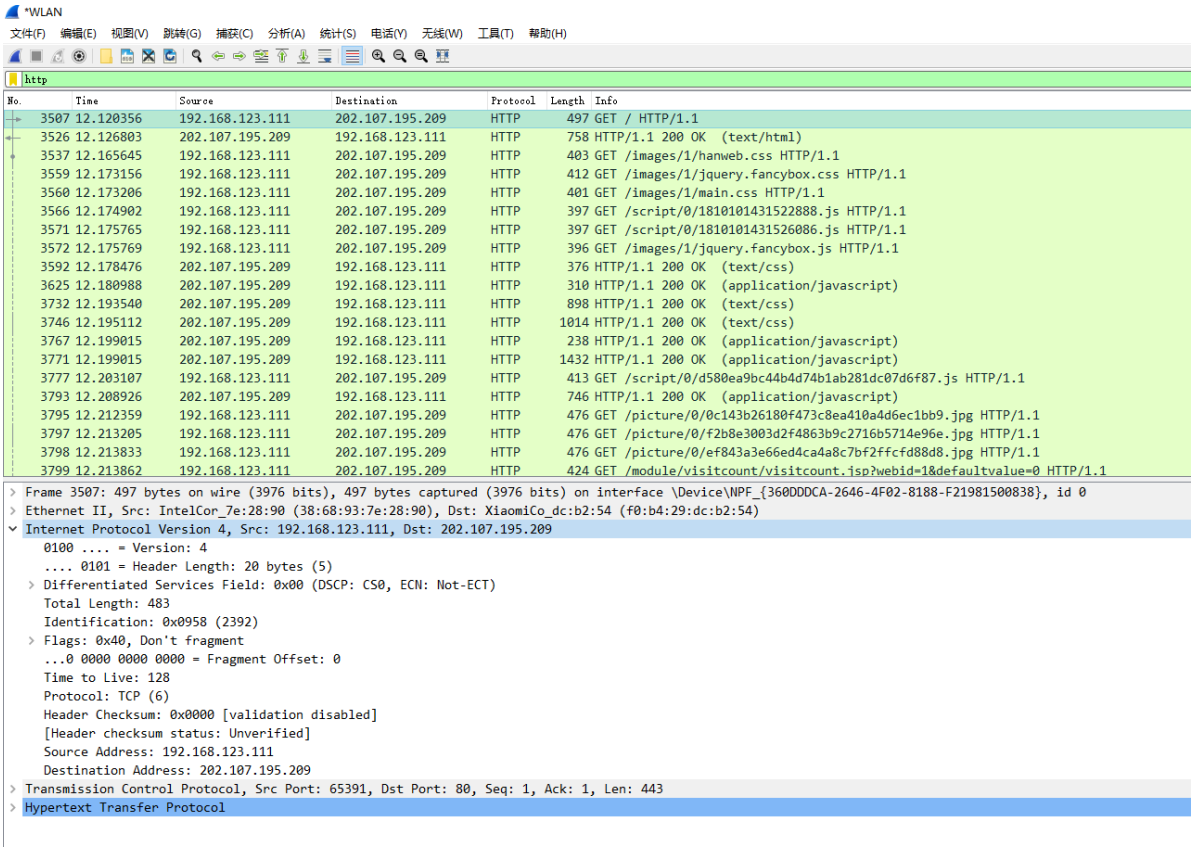


```
> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{360DDDCA-2646-4F02-8188-F21981500838}, id 0
> Ethernet II, Src: Chongqin_4d:0d:11 (d8:12:65:4d:0d:11), Dst: IntelCor_7e:28:90 (38:68:93:7e:28:90)
> Internet Protocol Version 4, Src: 192.168.123.117, Dst: 192.168.123.111
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x552b [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 48 (0x0030)
    Sequence Number (LE): 12288 (0x3000)
    [Request frame: 2]
    [Response time: 52.445 ms]
  > Data (32 bytes)
```

长度（字节）	1	1	2	2	2
字段	Type（类型）	Code（代码）	Checksum（校检和）	Identifier（标识符）	Sequence Number（序列号）
值	8	0	0x4d2b	0x0001	0x0030

3.4 对照**IP**数据包头格式，构造**HTTP**数据包，解释捕获的**IP**数据包头的内容

【实验结果与分析】



长度（位bit）	4	4	8	16	16	3
字段	Version（版本）	Header Length（首部长度）	Differentiated Services Field（服务类型）	Total Length（总长度字节数）	Identification（标识）	Flags（标志）
值	4	20	0x00	483	0x0958	0x40

长度（位bit）	13	8	8	16	32	32
字段	Fragment Offset（片偏移）	Time to Live（生存时间）	Protocol（协议）	Header Checksum（首部校验和）	Source Address（源IP地址）	Desination Address（目的IP地址）
值	0	128	TCP(6)	0x0000	192.168.123.111	202.107.195.209

三. 讨论、心得

记录实验感受、上机过程中遇到的困难及解决办法、遗留的问题、意见和建议等。