桂 林 电 子 科 技 大 学

计算机网络 实 验 报 告

实 验 名 称 实验二 以太网帧、IP 报文分析

计算机与信息安全学院 学院

网络空间安全 专 业

姓名 白楚榆

学号 2200350101

实 验 日 期 2024 年 4 月 28 日

评语：

成绩：_____ 指导教师签名：

一．实验目的

1. 掌握 wireshark 工具的基本使用方法
2. 熟悉典型以太网报文帧格式
3. 熟悉使用 arp、ifconfig(/ipconfig)、route 工具
4. 深入理解 IP 报文结构
5. 熟悉使用 ping、traceroute(/tracert)工具
6. 了解 arp、icmp 协议基本功能

二．实验环境

1、头歌基于 Linux 的虚拟机桌面系统

2、网络报文分析工具 wireshark

3、浏览器 firefox

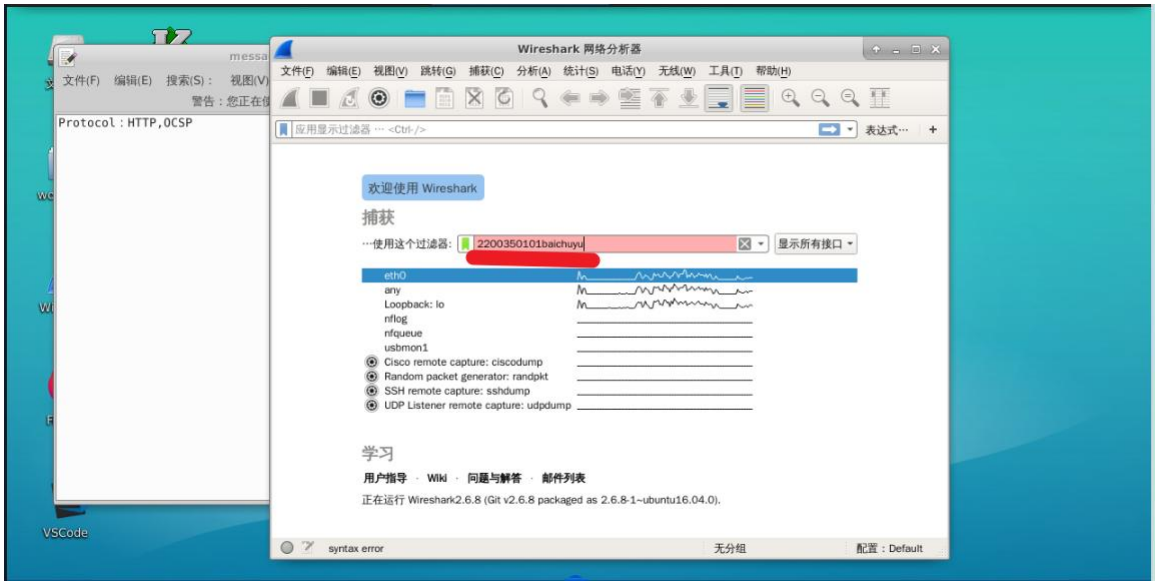
三．相关原理或知识点

1. 典型以太网报文帧格式
2. IP 报文结构
3. arp、icmp 协议基本功能
4. Ping 命令与工作原理

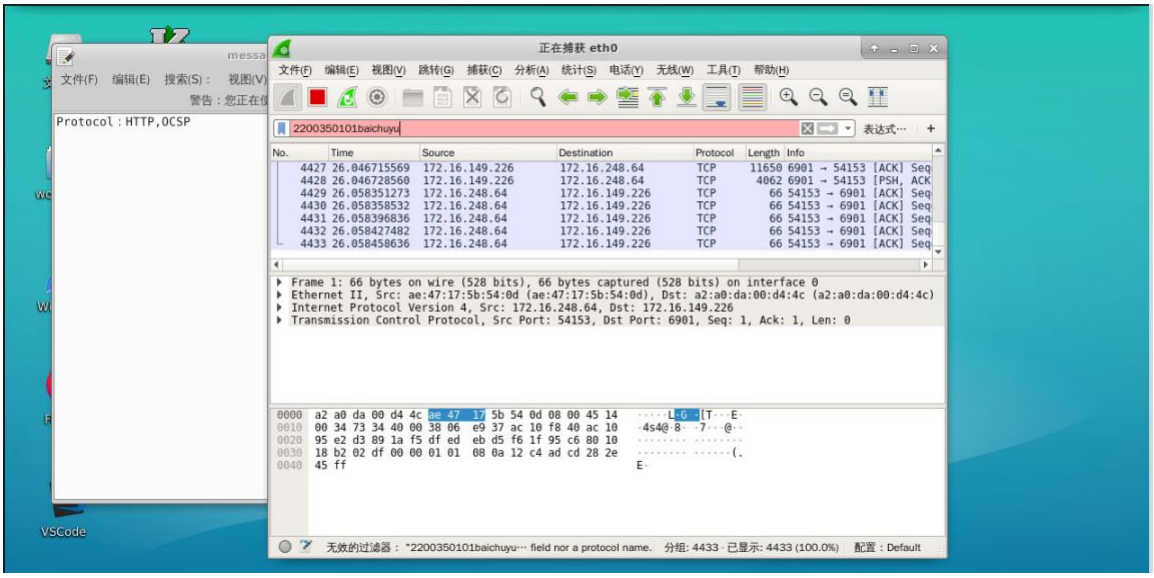
四．实验步骤

第 1 关：Wireshark 基本使用入门

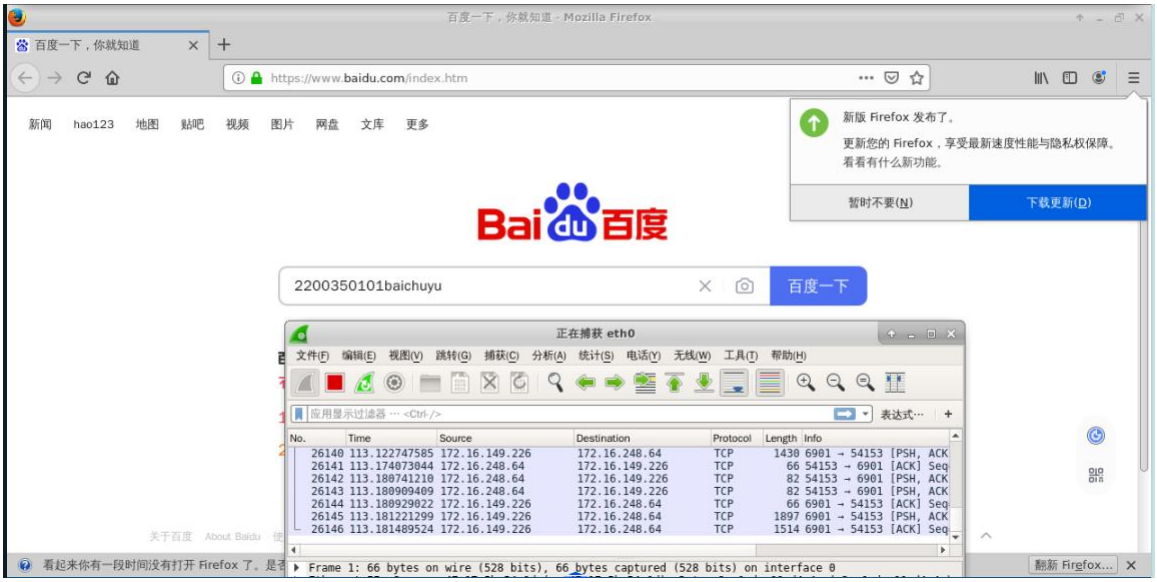
1、双击打开桌面上的工作区文件夹 workspace，再双击实训文件夹 myshixun，打开文件 message1-1.txt。



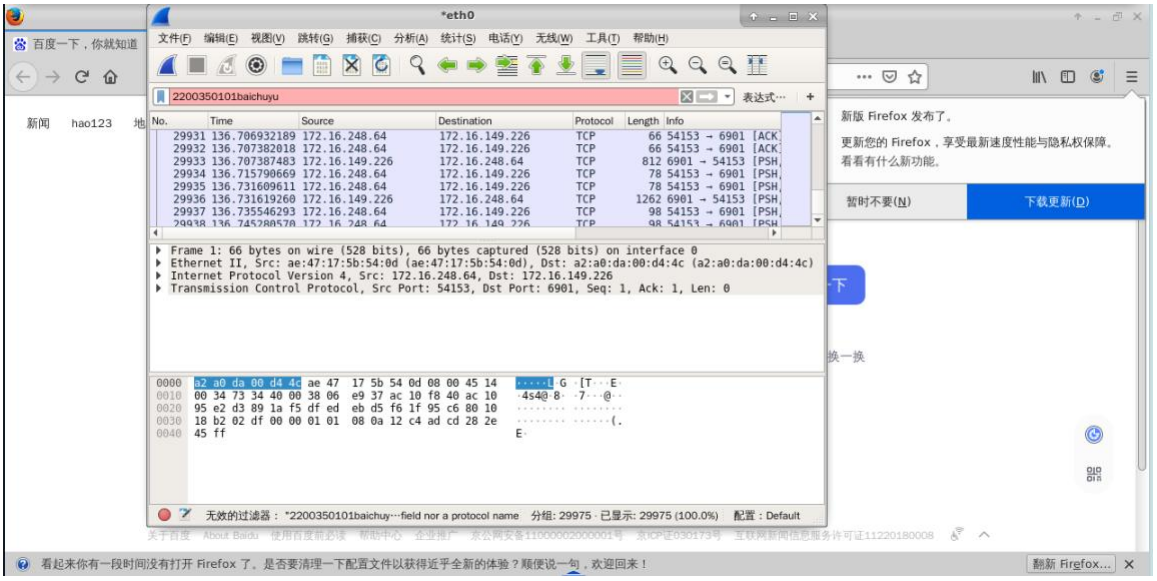
2、打开 wireshark ，开始抓取网络接口 eth0 上的分组，将窗口最小化；



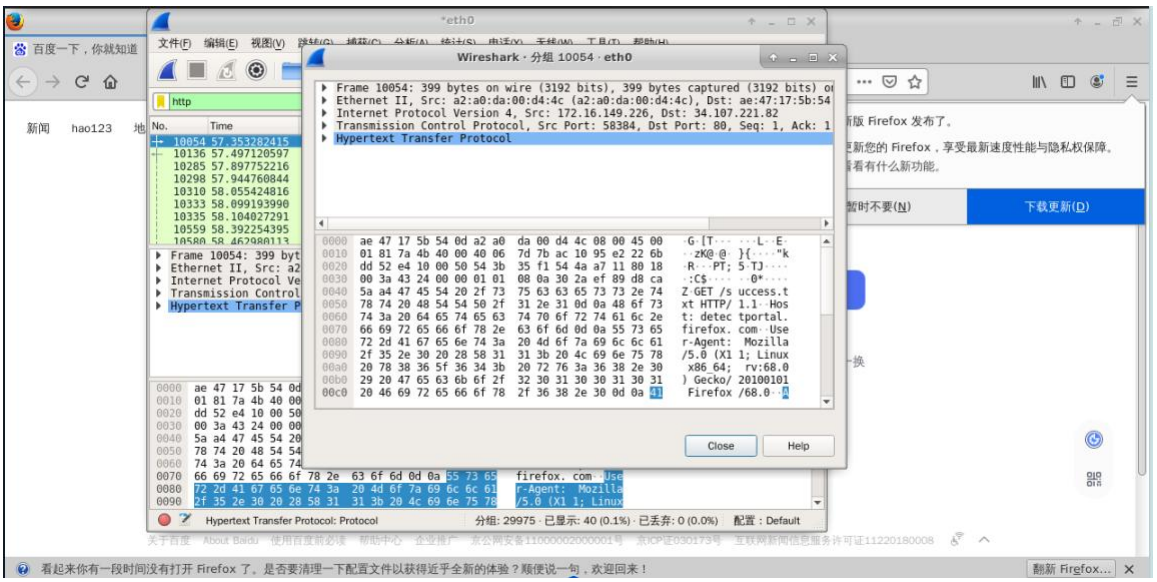
3、打开浏览器，访问 http://www.baidu.com，等待网页打开完毕；



4、切换到 Wireshark 窗口，并停止抓取分组；



5、利用分组过滤功能，过滤出 http 分组；在报文摘要窗口中点击选取第 1 个 http 报文；



6、对当前报文的头部明细窗口进行截图，保存到实验报告中，课后分析该报文，从外到内分别使用了什么

协议，对应网络体系结构的哪一层？

- Frame 10054: 数据包的编号。

- 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface 0: 数据包的大小，以字节和比特表示。

- Ethernet II, Src: a2:a0:da:00:d4:4c (a2: a0:da:00:d4:4c), Dst: ae:47:17:5b:54:0d (ae:47:17:5b:54:0d): 数据包的以太网协议头部信息，包括源 MAC 地址和目的 MAC 地址。

- Internet Protocol Version 4，Src: 172.16.149.226, Dst: 34.107.221.82: 数据包的 IP 协议头部信息，包括源 IP 地址和目的 IP 地址，使用的是 IPv4 协议。

- Transmission Control Protocol, Src Port: 58384， Dst Port: 80，Seq: 1, Ack: 1, Len: 333: 数据包的 TCP 协议头部信息，包括源端口号和目的端口号，序列号和确认号，以及数据长度。

- Hypertext Transfer Protocol: 数据包的应用层协议头部信息，使用的是 HTTP 协议。

该报文从外到内分别使用了以下协议：

（1）.以太网协议（Ethernet II）

（2）.网络层协议（IPv4）

（3）.传输层协议（TCP）

（4）.应用层协议（HTTP）

对应网络体系结构的哪一层：

（1）.以太网协议（Ethernet II）：数据链路层

（2）.网络层协议（IPv4）：网络层

（3）.传输层协议（TCP）：传输层

（4）.应用层协议（HTTP）：应用层

7、将分组列表中出现的协议名称，顺序填入 message1-1.txt 文件协议名称后面（相同协议只填写一次，用符号,分隔）并保存该文件；

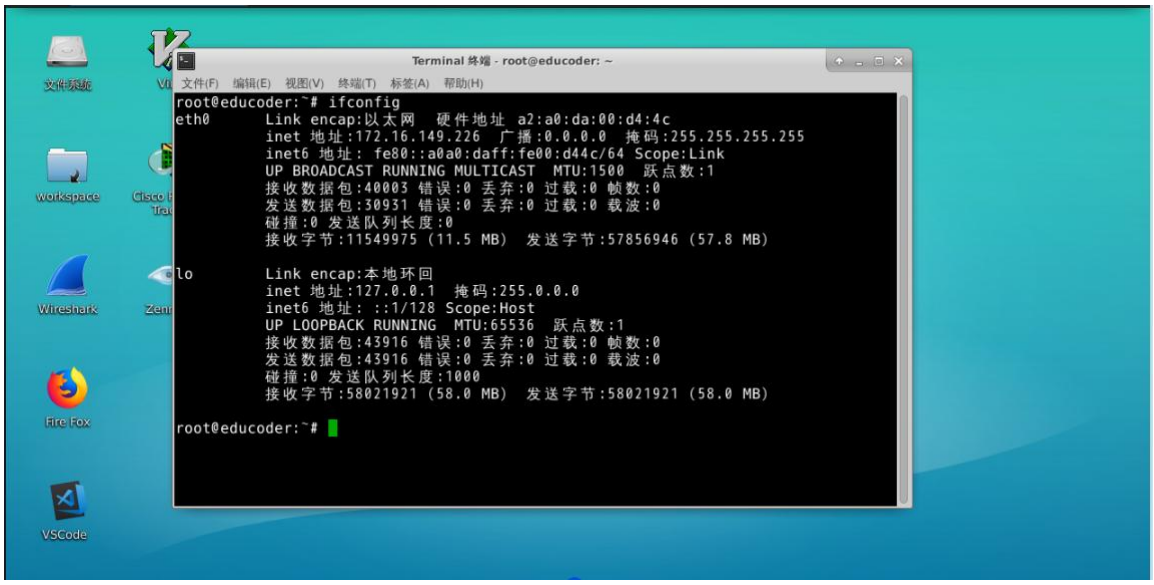
第 2 关：Ethernet 帧分析

1、打开终端工具

在平台桌面空白处，按鼠标右键，选“在此打开终端”

2、查看虚拟机 eth0 网卡的 MAC 地址、IP 地址、子网掩码，并记录到实验报告中。

使用命令：ifconfig



3、查看虚拟机网关 IP 地址

使用命令：route

对应 default 行

```
root@educoder:~# route
内核 IP 路由表
目标            网关            子网掩码        标志  跃点   引用  使用 接口
default         169.254.1.1     0.0.0.0         UG    0      0        0 eth0
```

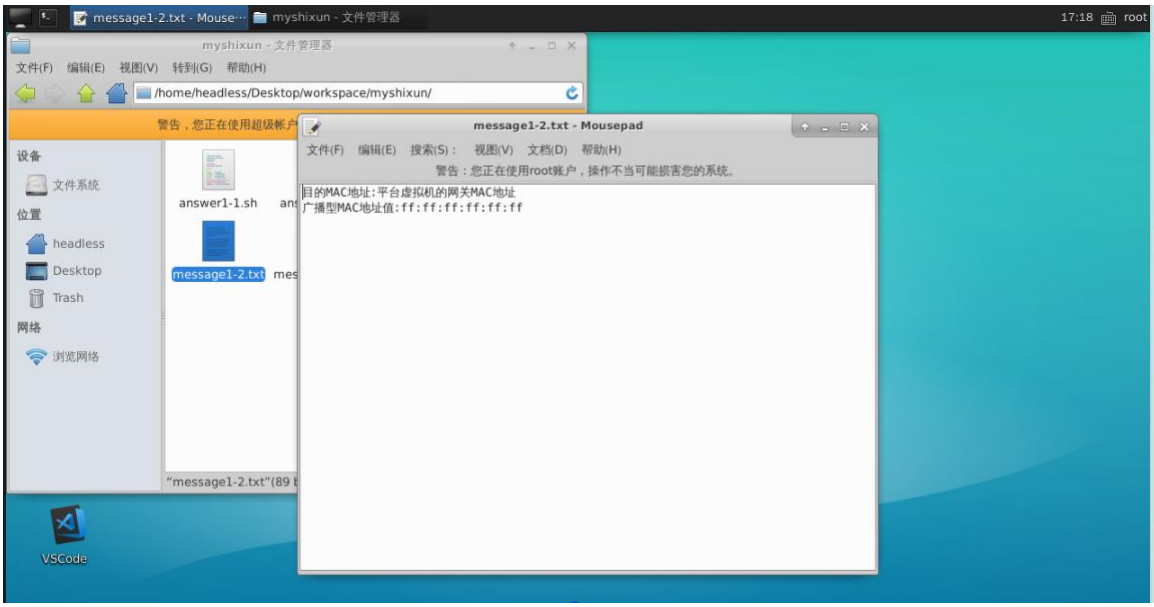
4、查看虚拟机网关 MAC 地址

使用命令：arp

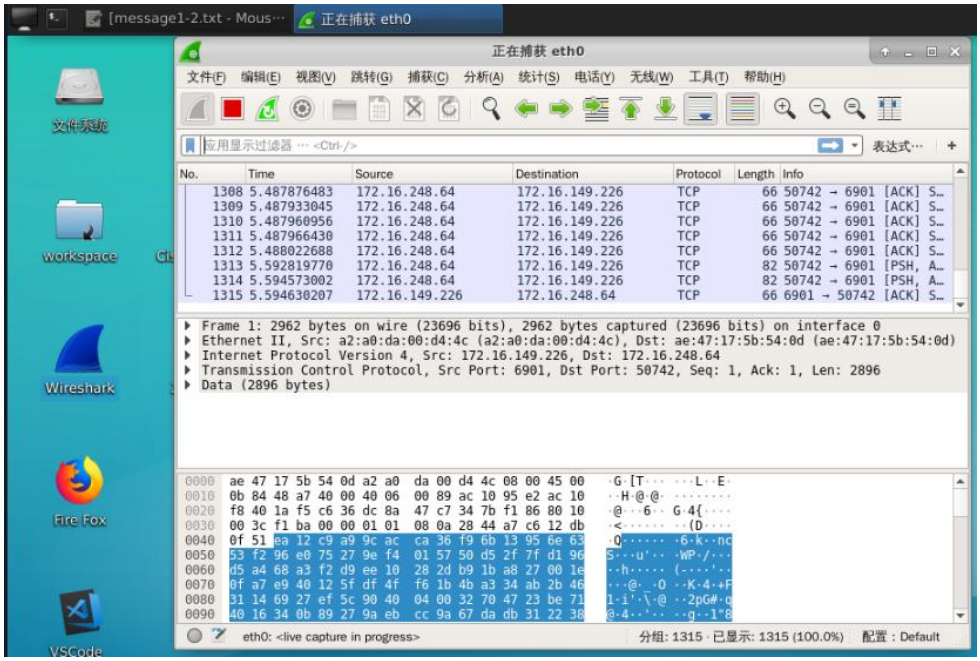
根据网关 IP 地址，查 ARP 表得到对应的 MAC 地址，记录到实验报告中。

```
root@educoder:~# arp
地址                     类型    硬件地址            标志  Mask            接口
172-16-27-72.kubelet.ku  ether   ae:47:17:5b:54:0d   C                     eth0
169.254.1.1              ether   ae:47:17:5b:54:0d   CM                    eth0
root@educoder:~#
```

5、双击打开桌面上的工作区文件夹 workspace，再双击实训文件夹 myshixun，打开文件 message1-2.txt。

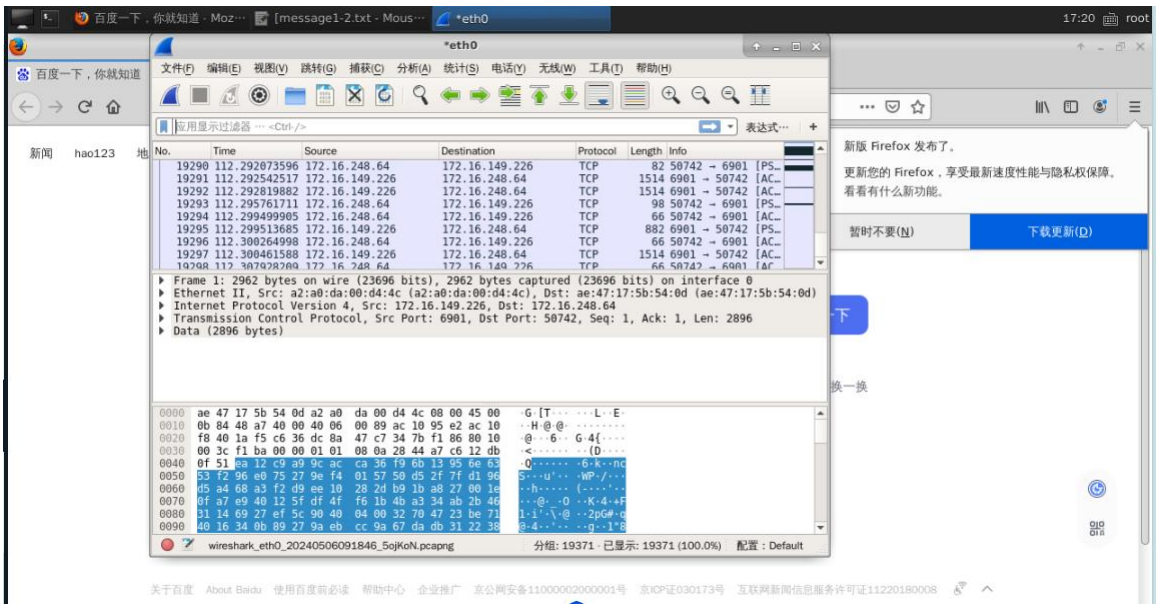


6、打开 wireshark ，开始抓取网络接口 eth0 上的分组，将窗口最小化；

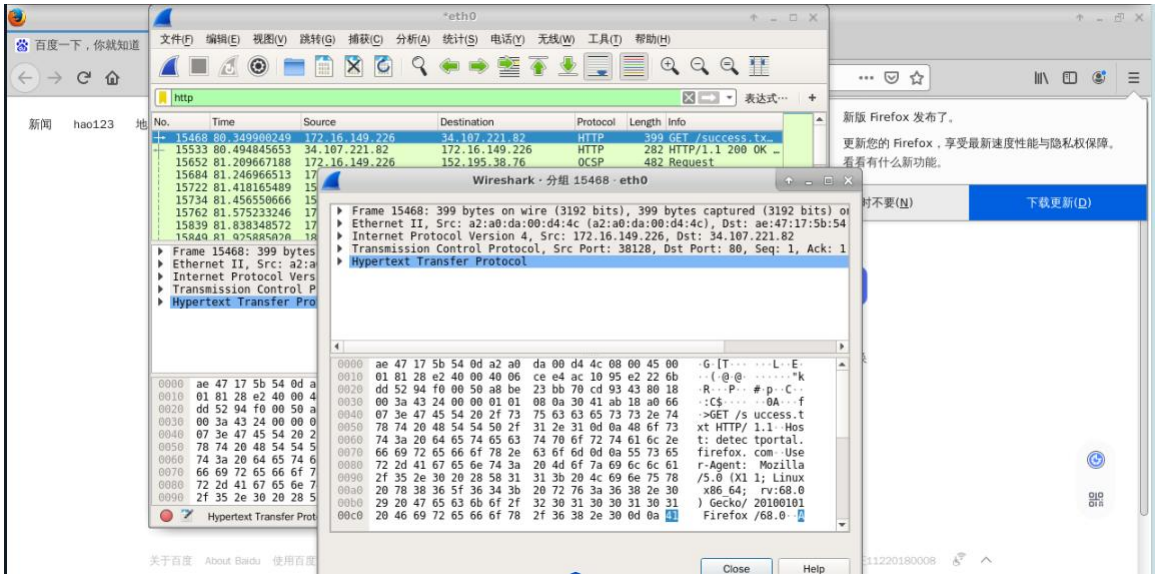


7、打开浏览器，访问 http://www.baidu.com，等待网页打开完毕；

8、切换到 Wireshark 窗口，并停止抓取分组；



9、利用分组过滤功能，过滤出 http 分组；在报文摘要窗口中点击选取第 1 个 http 报文；



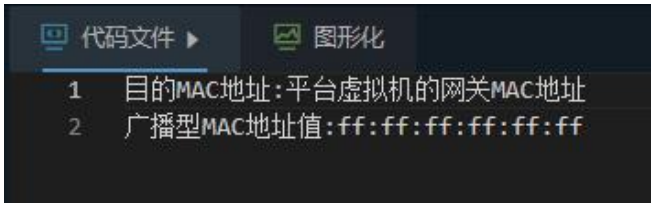
10、分析当前报文采用以太网哪种帧格式，把典型字段值记录到到实验报告中。

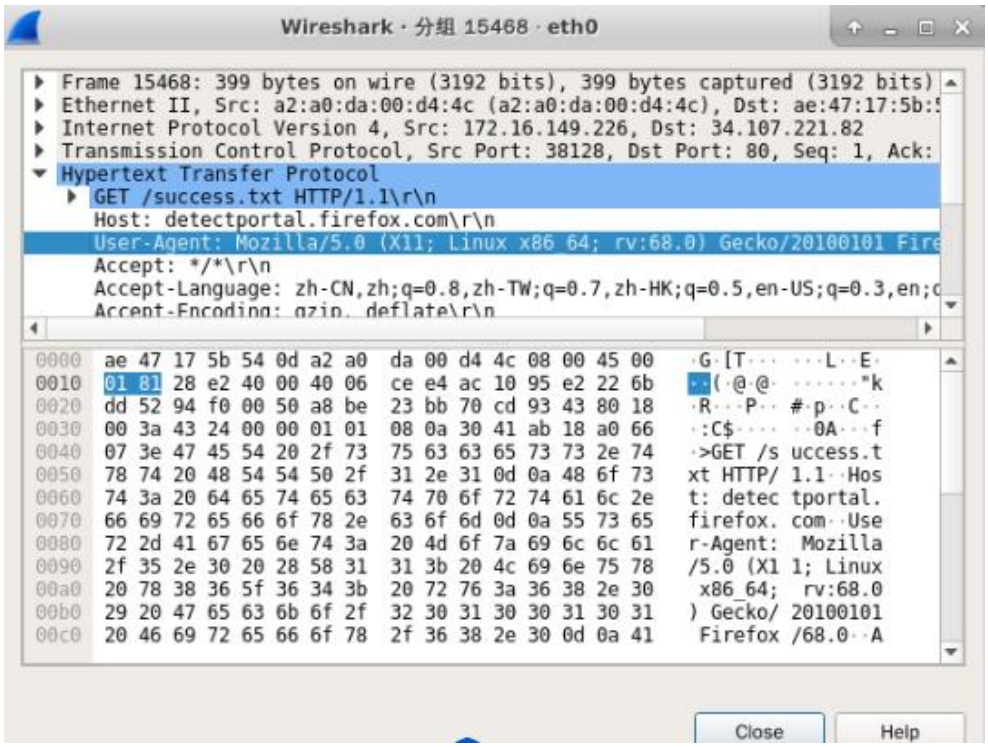
采用的是 Ethernet II 帧格式，ae 47 17 5b 54 0d

11、确定当前报文的目的 MAC 地址指向目标，并填写到文件 message1-2.txt 第一行末尾（不要破坏“冒号”之前提示内容），并保存该文件，

注意：填写内容仅限于范围（平台虚拟机、平台虚拟机的网关、百度服务器、不能确定）

12、把广播型 MAC 地址值（采用标准写法，16 进制、冒号分隔），并填写到文件 message1-2.txt 第二行末尾（不要破坏“冒号”之前提示内容），并保存该文件。

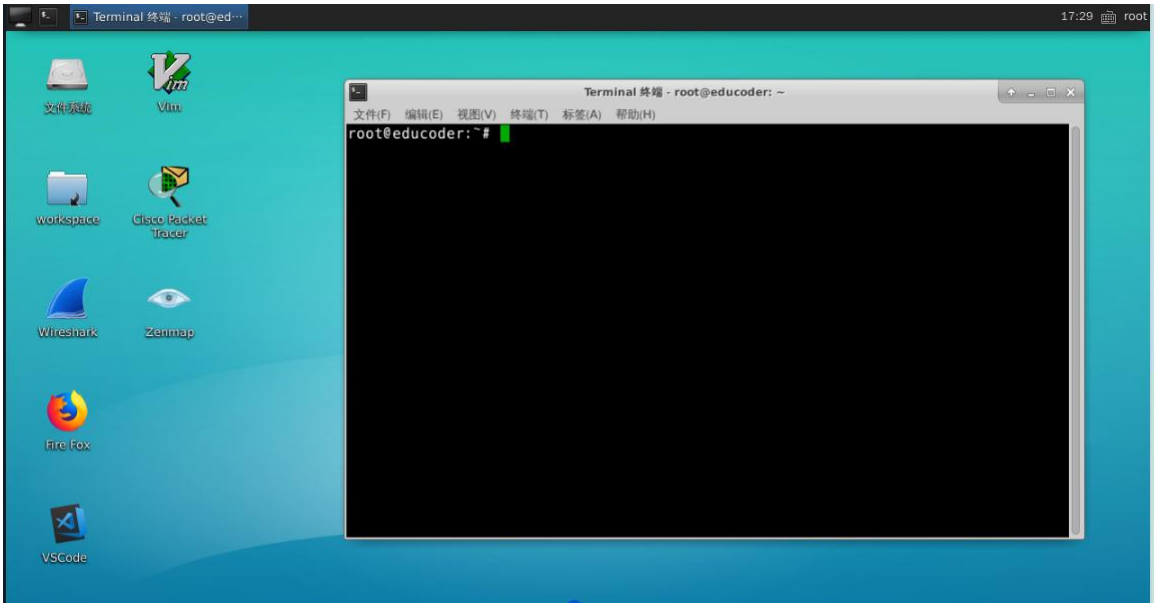




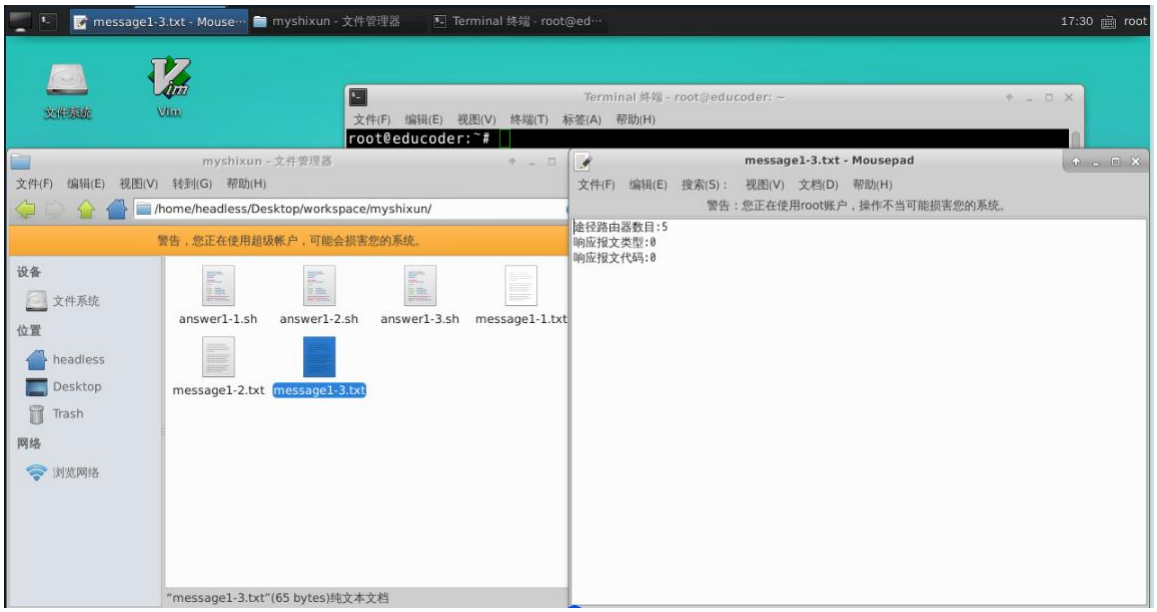
第 3 关：IP 报文分析

1、打开终端工具

在平台桌面空白处，按鼠标右键，选“在此打开终端”。



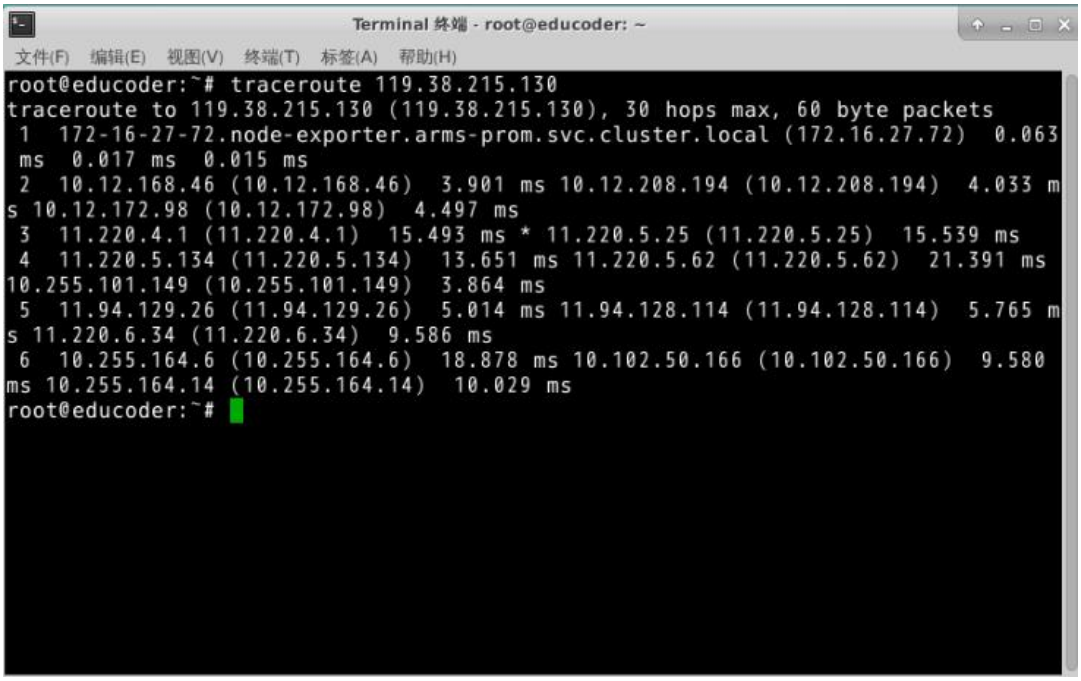
2、双击打开桌面上的工作区文件夹 workspace，再双击实训文件夹 myshixun，打开文件 message1-3.txt。



3、已知某目标机 IP 地址是 119.38.215.130，测试 IP 报文由平台虚拟机发送至目标机，沿途经过哪些路由器？

执行命令：traceroute 119.38.215.130

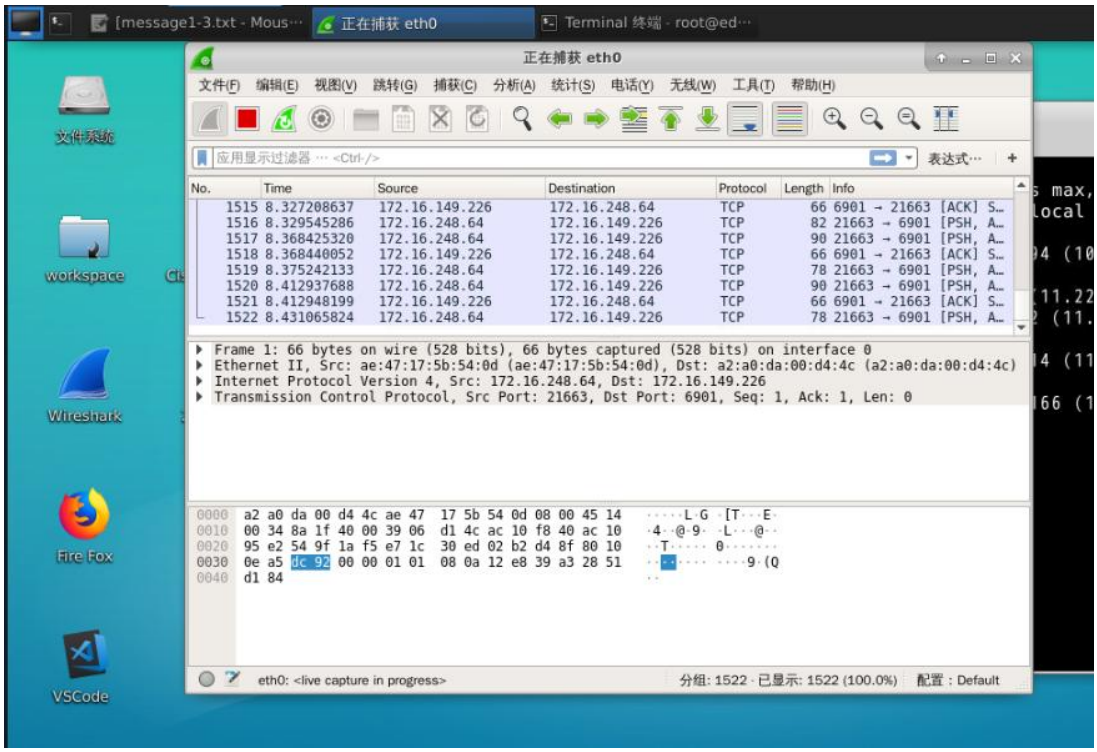
把得到的数据整理后，保存到实验报告中，课后分析沿途经过哪些路由器。



4、分析沿途所经过的路由器的数目，并填写到文件 message1-3.txt 第一行末尾（不要破坏“冒号”之前提示内容），并保存该文件。

注：有两种可能的答案，系统只认第一种（如果你的答案系统不认，可以将其减 1 再试）.

5、打开 wireshark ，开始抓取网络接口 eth0 上的分组，将窗口最小化；



6、在前面打开的终端窗口内，执行如下命令：

```
ping -c 3 -s 0 www.educoder.net
```

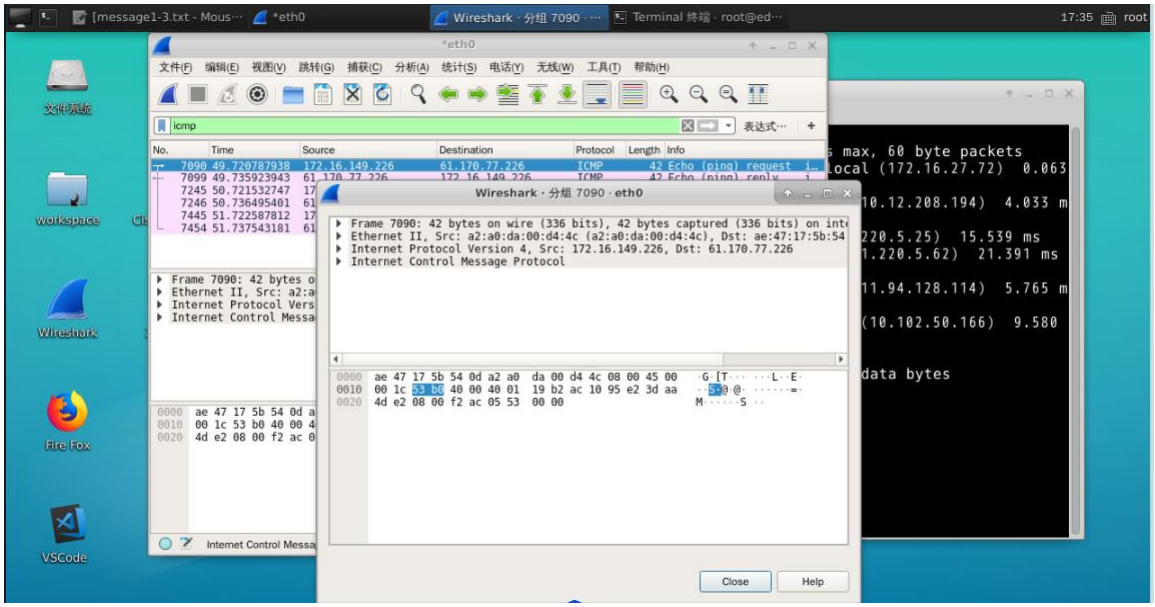
在实验报告中解释该命令行各参数的含义；

```
root@educoder:~# ping -c 3 -s 0 www.educoder.net
PING www.educoder.net.w.kunluncan.com (61.170.77.226): 0 data bytes
8 bytes from 61.170.77.226: icmp_seq=0 ttl=52
8 bytes from 61.170.77.226: icmp_seq=1 ttl=52
8 bytes from 61.170.77.226: icmp_seq=2 ttl=52
--- www.educoder.net.w.kunluncan.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
root@educoder:~#
```

把得到的数据整理后，保存到实验报告中，课后完成数据分析。

7、切换到 Wireshark 窗口，并停止抓取分组；

8、利用分组过滤功能，过滤出 icmp 分组；在报文摘要窗口中点击选取第 1 个 icmp 报文；



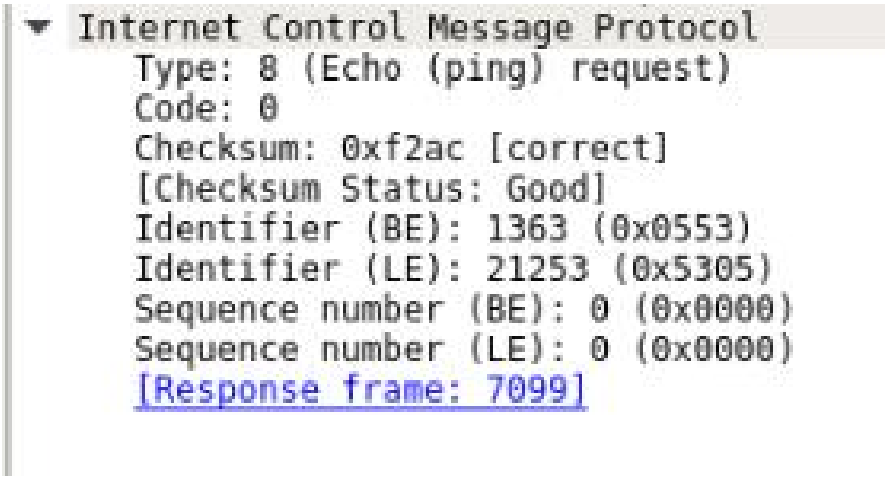
9、调节分组头部细节窗口大小，将其中 IP 报头和 ICMP 报头全部字段都展开，然后对该窗口进行截图，并粘贴到实验报告中，课后对其中主要字段进行分析解读。

```
▼ Internet Protocol Version 4, Src: 172.16.149.226, Dst: 61.170.77.226
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 28
    Identification: 0x53b0 (21424)
  ▶ Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x19b2 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.149.226
    Destination: 61.170.77.226
```

这是一个 IPv4 的数据包，其中包含了源 IP 地址和目标 IP 地址，以及其他一些信息。具体分析如下：

- 版本号为 4，表示这是 IPv4 协议。
- 头部长度为 20 字节，即 5 个 32 位字长。
- 差分服务字段为 0x14，其中 DSCP 为 Unknown，ECN 为 Not-ECT。
- 总长度为 28 字节。
- 标识符为 0x3b17，即 15127。

- 标志位为 0x4000，表示不分片。
- 存活时间为 55。
- 协议为 ICMP，即 Internet 控制报文协议。
- 头部校验和为 0xdb65。
- 源 IP 地址为 122.225.212.158。
- 目标 IP 地址为 172.16.49.192。

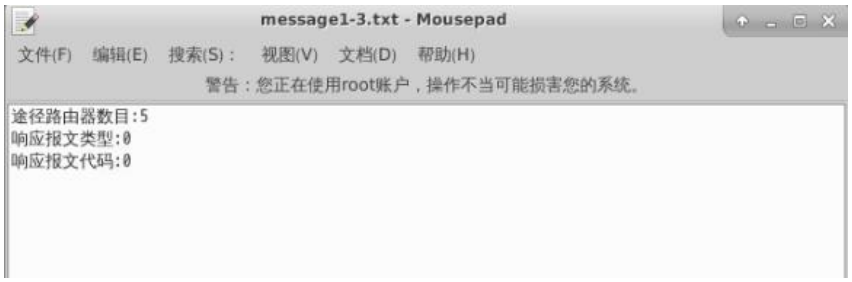


这是一个 ICMP 协议的回复报文，其中包含了以下信息：

- Type: 0，表示这是一个回复报文，而不是请求报文。
- Code: 0，表示这是一个 Echo (ping) reply。
- Checksum: 0xfdd7，表示校验和正确。
- Identifier (BE): 552 (0x0228)，表示标识符为 552。
- Identifier (LE): 10242 (0x2802)，表示标识符的小端字节序为 10242。
- Sequence number (BE): 0 (0x0000)，表示序列号为 0。
- Sequence number (LE): 0 (0x0000)，表示序列号的小端字节序为 0。

根据这些信息，我们可以确定这是一个回复报文，而不是请求报文，并且是一个 Echo (ping) reply。标识符为 552，序列号为 0。校验和正确。

10、分析第一个 icmp 响应（reply）报文，把其类型值、代码，分别填写到文件 message1-3.txt 第二、三行末尾（不要破坏“冒号”之前提示内容），并保存该文件。



五．实验结果及其分析

Wireshark 是一种免费的网络协议分析器，可以运行在使用以太网、串行(PPP 和 SLIP)、802.11 无线局域网和许多其他链路层技术的计算机上。 以太帧有很多种类型，不同类型的帧具有不同的格式和 MTU 值，但在同种物理媒体上都可同时存在。以太网中大多数的数据帧使用的是 Ethernet II 格式。通过 Wireshark 工具可以捕获网络中的 IP 报文，并分析以太帧的格式，理解各类以太帧的区别和联系。

六．实验总结

学会了通过 Wireshark 工具抓取网络数据包，然后进行 IP 报文分析。通过对 IP 报文结构深入分析和理解，掌握了网络中数据包的封装、传输和数据解析原理，更好的理解了网络的工作原理。还学会了 ping、traceroute (/tracert)等工具的使用。