浙江大学

# 本科实验报告

| | |
|---|---|
| 课程名称： | 计算机网络基础 |
| 姓　　名： | 应承峻 |
| 学　　院： | 计算机学院 |
| 系： | 计算机系 |
| 专　　业： | 软件工程 |
| 学　　号： | 3170103456 |
| 指导教师： | 高艺 |

2019 年　9　月 21 日

# 浙江大学实验报告

课程名称：计算机网络基础 实验类型：操作实验

实验项目名称：WireShark 软件初探和常见网络命令的使用

学生姓名：应承峻 专业：软件工程 学号：3170103456

同组学生姓名：无 指导老师：高艺

实验地点：计算机网络实验室 实验日期：2019 年 9 月 21 日

## 一、 实验目的和要求：

- 初步了解 WireShark 软件的界面和功能
- 熟悉各类常用网络命令的使用

## 二、 实验内容和原理

- Wireshark 是 PC 上使用最广泛的免费抓包工具，可以分析大多数常见的协议数据包。有 Windows 版本、Linux 版本和 Mac 版本，可以免费从网上下载
- 初步掌握网络协议分析软件 Wireshark 的使用，学会配置过滤器
- 根据要求配置 Wireshark，捕获某一类协议的数据包
- 在 PC 机上熟悉常用网络命令的功能和用法: Ping.exe，Netstat.exe, Telnet.exe, Tracert.exe, Arp.exe, Ipconfig.exe, Net.exe, Route.exe, Nslookup.exe
- 利用 WireShark 软件捕捉上述部分命令产生的数据包

## 三、 主要仪器设备

- 联网的 PC 机
- WireShark 协议分析软件

## 四、 操作方法与实验步骤

- 安装网络包捕获软件 Wireshark
- 配置网络包捕获软件，捕获所有机器的数据包
- 配置网络包捕获软件，只捕获特定类型的包
- 在 Windows 命令行方式下，执行适当的命令，完成以下功能(请以管理员身份打开命令行)：
    1. 测试到特定地址的联通性、数据包延迟时间
    2. 显示本机的网卡物理地址、IP 地址
    3. 显示本机的默认网关地址、DNS 服务器地址
    4. 显示本机记录的局域网内其它机器 IP 地址与其物理地址的对照表

5. 显示从本机到达一个特定地址的路由
6. 显示某一个域名的 IP 地址
7. 显示已经与本机建立 TCP 连接的端口、IP 地址、连接状态等信息
8. 显示本机的路由表信息，并手工添加一个路由
9. 显示本机的网络映射连接
10. 显示局域网内某台机器的共享资源
11. 使用 telnet 连接 WEB 服务器的端口，输入（<cr>表示回车）获得该网站的主页内容：

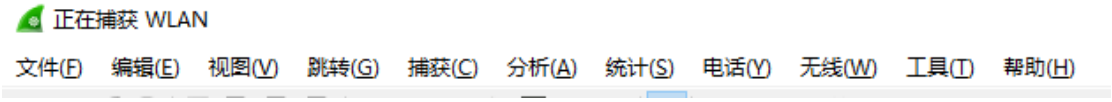
```
GET / HTTP/1.1<cr>
Host: 任意字符串<cr>
<cr>
```

- 利用 WireShark 实时观察在执行上述命令时，哪些命令会额外产生数据包，并记录这些数据包的种类。

## 五、 实验数据记录和处理

- **运行 Wireshark 软件，界面是由哪几个部分构成？各有什么作用？**

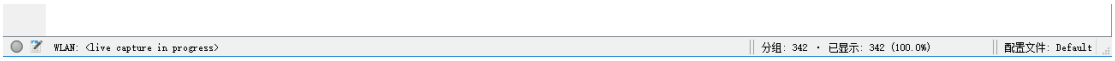
◆ 菜单栏：用于开始操作，提供一些项目功能。



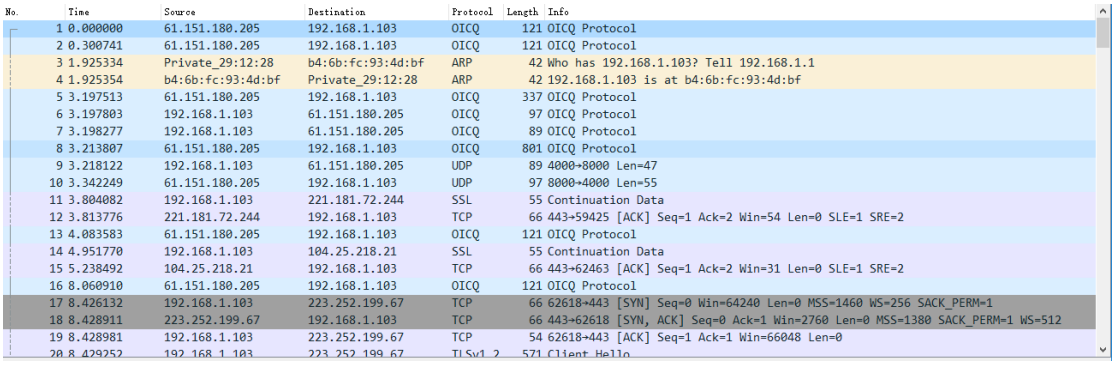

◆ 主工具栏：提供快速访问菜单中经常用到的项目的功能，如开始捕获、停止捕获、捕获选项、打开已保存的捕获文件。

◆ Filter 工具栏：用于编辑或显示过滤器。


◆ 状态栏：显示当前程序状态以及捕捉数据的更多详情。

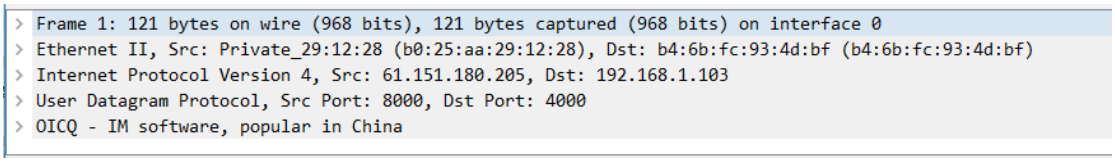



◆ Packet List 面板：显示打开文件的每个包的摘要。点击面板中的单独条目，包的其他情况将会显示在另外两个面板中。



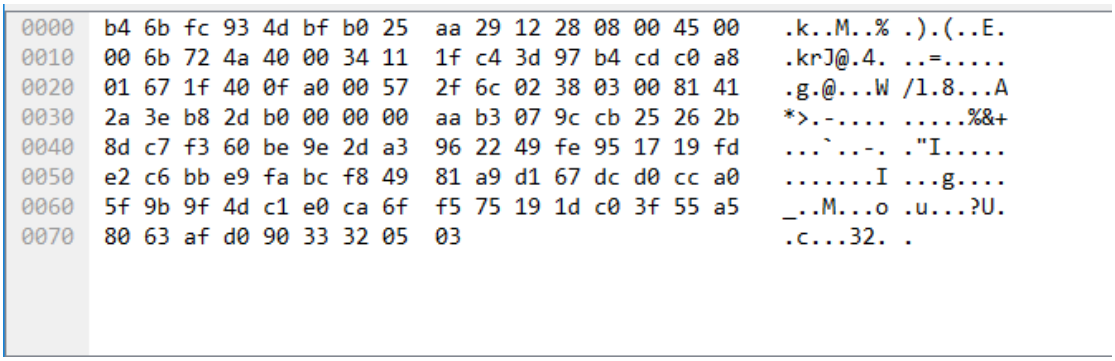
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 61.151.180.205 | 192.168.1.103 | OICQ | 121 | OICQ Protocol |
| 2 | 0.300741 | 61.151.180.205 | 192.168.1.103 | OICQ | 121 | OICQ Protocol |
| 3 | 1.925334 | Private_29:12:28 | b4:6b:fc:93:4d:bf | ARP | 42 | Who has 192.168.1.103? Tell 192.168.1.1 |
| 4 | 1.925354 | b4:6b:fc:93:4d:bf | Private_29:12:28 | ARP | 42 | 192.168.1.103 is at b4:6b:fc:93:4d:bf |
| 5 | 3.197513 | 61.151.180.205 | 192.168.1.103 | OICQ | 337 | OICQ Protocol |
| 6 | 3.197803 | 192.168.1.103 | 61.151.180.205 | OICQ | 97 | OICQ Protocol |
| 7 | 3.198277 | 192.168.1.103 | 61.151.180.205 | OICQ | 89 | OICQ Protocol |
| 8 | 3.213807 | 61.151.180.205 | 192.168.1.103 | OICQ | 801 | OICQ Protocol |
| 9 | 3.218122 | 192.168.1.103 | 61.151.180.205 | UDP | 89 | 4000→8000 Len=47 |
| 10 | 3.342249 | 61.151.180.205 | 192.168.1.103 | UDP | 97 | 8000→4000 Len=55 |
| 11 | 3.804082 | 192.168.1.103 | 221.181.72.244 | SSL | 55 | Continuation Data |
| 12 | 3.813776 | 221.181.72.244 | 192.168.1.103 | TCP | 66 | 443→59425 [ACK] Seq=1 Ack=2 Win=54 Len=0 SLE=1 SRE=2 |
| 13 | 4.083583 | 61.151.180.205 | 192.168.1.103 | OICQ | 121 | OICQ Protocol |
| 14 | 4.951770 | 192.168.1.103 | 104.25.218.21 | SSL | 55 | Continuation Data |
| 15 | 5.238492 | 104.25.218.21 | 192.168.1.103 | TCP | 66 | 443→62463 [ACK] Seq=1 Ack=2 Win=31 Len=0 SLE=1 SRE=2 |
| 16 | 8.060910 | 61.151.180.205 | 192.168.1.103 | OICQ | 121 | OICQ Protocol |
| 17 | 8.426132 | 192.168.1.103 | 223.252.199.67 | TCP | 66 | 62618→443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 18 | 8.428911 | 223.252.199.67 | 192.168.1.103 | TCP | 66 | 443→62618 [SYN, ACK] Seq=0 Ack=1 Win=2760 Len=0 MSS=1380 SACK_PERM=1 WS=512 |
| 19 | 8.428981 | 192.168.1.103 | 223.252.199.67 | TCP | 54 | 62618→443 [ACK] Seq=1 Ack=1 Win=66048 Len=0 |
| 20 | 8.429252 | 192.168.1.103 | 223.252.199.67 | TLSv1.2 | 571 | Client Hello |

◆ Packet Detail 面板：显示在 Packet list 面板中选择的包的详细信息。



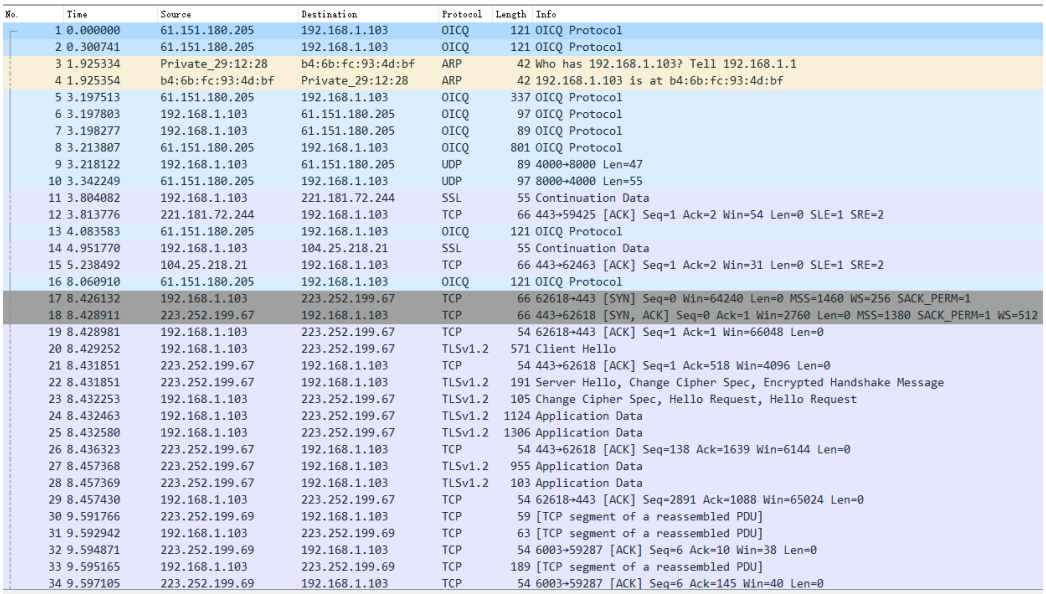
```
> Frame 1: 121 bytes on wire (968 bits), 121 bytes captured (968 bits) on interface 0
> Ethernet II, Src: Private_29:12:28 (b0:25:aa:29:12:28), Dst: b4:6b:fc:93:4d:bf (b4:6b:fc:93:4d:bf)
> Internet Protocol Version 4, Src: 61.151.180.205, Dst: 192.168.1.103
> User Datagram Protocol, Src Port: 8000, Dst Port: 4000
> OICQ - IM software, popular in China
```

◆ Packet bytes 面板：显示在 Packet list 面板选择的包的数据，以及在 Packet details 面板高亮显示的字段。



```
0000  b4 6b fc 93 4d bf b0 25  aa 29 12 28 08 00 45 00   .k..M..% .).(..E.
0010  00 6b 72 4a 40 00 34 11  1f c4 3d 97 b4 cd c0 a8   .krJ@.4. ..=.....
0020  01 67 1f 40 0f a0 00 57  2f 6c 02 38 03 00 81 41   .g.@...W /l.8...A
0030  2a 3e b8 2d b0 00 00 00  aa b3 07 9c cb 25 26 2b   *>.-.... .....%&+
0040  8d c7 f3 60 be 9e 2d a3  96 22 49 fe 95 17 19 fd   ...`..-. ."I.....
0050  e2 c6 bb e9 fa bc f8 49  81 a9 d1 67 dc d0 cc a0   .......I ...g....
0060  5f 9b 9f 4d c1 e0 ca 6f  f5 75 19 1d c0 3f 55 a5   _..M...o .u...?U.
0070  80 63 af d0 90 33 32 05  03                       .c...32. .
```

● **开始捕获网络数据包，你看到了什么？有哪些协议？**

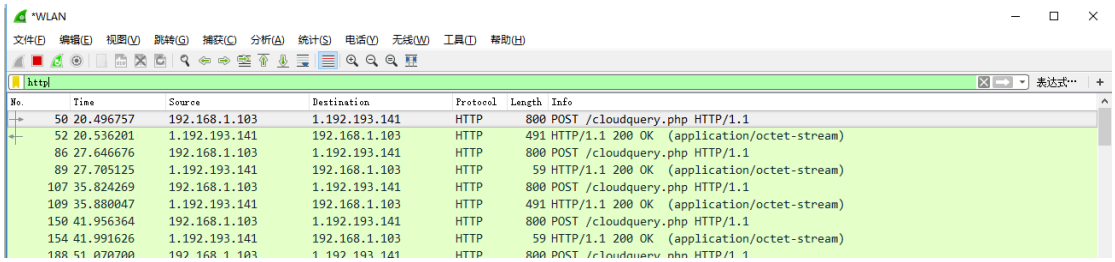


| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 61.151.180.205 | 192.168.1.103 | OICQ | 121 | OICQ Protocol |
| 2 | 0.300741 | 61.151.180.205 | 192.168.1.103 | OICQ | 121 | OICQ Protocol |
| 3 | 1.925334 | Private_29:12:28 | b4:6b:fc:93:4d:bf | ARP | 42 | Who has 192.168.1.103? Tell 192.168.1.1 |
| 4 | 1.925354 | b4:6b:fc:93:4d:bf | Private_29:12:28 | ARP | 42 | 192.168.1.103 is at b4:6b:fc:93:4d:bf |
| 5 | 3.197513 | 61.151.180.205 | 192.168.1.103 | OICQ | 337 | OICQ Protocol |
| 6 | 3.197803 | 192.168.1.103 | 61.151.180.205 | OICQ | 97 | OICQ Protocol |
| 7 | 3.198277 | 192.168.1.103 | 61.151.180.205 | OICQ | 89 | OICQ Protocol |
| 8 | 3.213807 | 61.151.180.205 | 192.168.1.103 | OICQ | 801 | OICQ Protocol |
| 9 | 3.218122 | 192.168.1.103 | 61.151.180.205 | UDP | 89 | 4000→8000 Len=47 |
| 10 | 3.342249 | 61.151.180.205 | 192.168.1.103 | UDP | 97 | 8000→4000 Len=55 |
| 11 | 3.804082 | 192.168.1.103 | 221.181.72.244 | SSL | 55 | Continuation Data |
| 12 | 3.813776 | 221.181.72.244 | 192.168.1.103 | TCP | 66 | 443→59425 [ACK] Seq=1 Ack=2 Win=54 Len=0 SLE=1 SRE=2 |
| 13 | 4.083583 | 61.151.180.205 | 192.168.1.103 | OICQ | 121 | OICQ Protocol |
| 14 | 4.951770 | 192.168.1.103 | 104.25.218.21 | SSL | 55 | Continuation Data |
| 15 | 5.238492 | 104.25.218.21 | 192.168.1.103 | TCP | 66 | 443→62463 [ACK] Seq=1 Ack=2 Win=31 Len=0 SLE=1 SRE=2 |
| 16 | 8.060910 | 61.151.180.205 | 192.168.1.103 | OICQ | 121 | OICQ Protocol |
| 17 | 8.426132 | 192.168.1.103 | 223.252.199.67 | TCP | 66 | 62618→443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 18 | 8.428911 | 223.252.199.67 | 192.168.1.103 | TCP | 66 | 443→62618 [SYN, ACK] Seq=0 Ack=1 Win=2760 Len=0 MSS=1380 SACK_PERM=1 WS=512 |
| 19 | 8.428981 | 192.168.1.103 | 223.252.199.67 | TCP | 54 | 62618→443 [ACK] Seq=1 Ack=1 Win=66048 Len=0 |
| 20 | 8.429252 | 192.168.1.103 | 223.252.199.67 | TLSv1.2 | 571 | Client Hello |
| 21 | 8.431851 | 223.252.199.67 | 192.168.1.103 | TCP | 54 | 443→62618 [ACK] Seq=1 Ack=518 Win=4096 Len=0 |
| 22 | 8.431851 | 223.252.199.67 | 192.168.1.103 | TLSv1.2 | 191 | Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 23 | 8.432253 | 192.168.1.103 | 223.252.199.67 | TLSv1.2 | 105 | Change Cipher Spec, Hello Request, Hello Request |
| 24 | 8.432463 | 192.168.1.103 | 223.252.199.67 | TLSv1.2 | 1124 | Application Data |
| 25 | 8.432580 | 192.168.1.103 | 223.252.199.67 | TLSv1.2 | 1306 | Application Data |
| 26 | 8.436323 | 223.252.199.67 | 192.168.1.103 | TCP | 54 | 443→62618 [ACK] Seq=138 Ack=1639 Win=6144 Len=0 |
| 27 | 8.457368 | 223.252.199.67 | 192.168.1.103 | TLSv1.2 | 955 | Application Data |
| 28 | 8.457369 | 223.252.199.67 | 192.168.1.103 | TLSv1.2 | 103 | Application Data |
| 29 | 8.457430 | 192.168.1.103 | 223.252.199.67 | TCP | 54 | 62618→443 [ACK] Seq=2891 Ack=1088 Win=65024 Len=0 |
| 30 | 9.591766 | 223.252.199.69 | 192.168.1.103 | TCP | 59 | [TCP segment of a reassembled PDU] |
| 31 | 9.592942 | 192.168.1.103 | 223.252.199.69 | TCP | 63 | [TCP segment of a reassembled PDU] |
| 32 | 9.594871 | 223.252.199.69 | 192.168.1.103 | TCP | 54 | 6003→59287 [ACK] Seq=6 Ack=10 Win=38 Len=0 |
| 33 | 9.595165 | 192.168.1.103 | 223.252.199.69 | TCP | 189 | [TCP segment of a reassembled PDU] |
| 34 | 9.597105 | 223.252.199.69 | 192.168.1.103 | TCP | 54 | 6003→59287 [ACK] Seq=6 Ack=145 Win=40 Len=0 |

看到了抓到的包的信息。有 TCP、UDP、ARP、HTTP、OICQ 协议等等

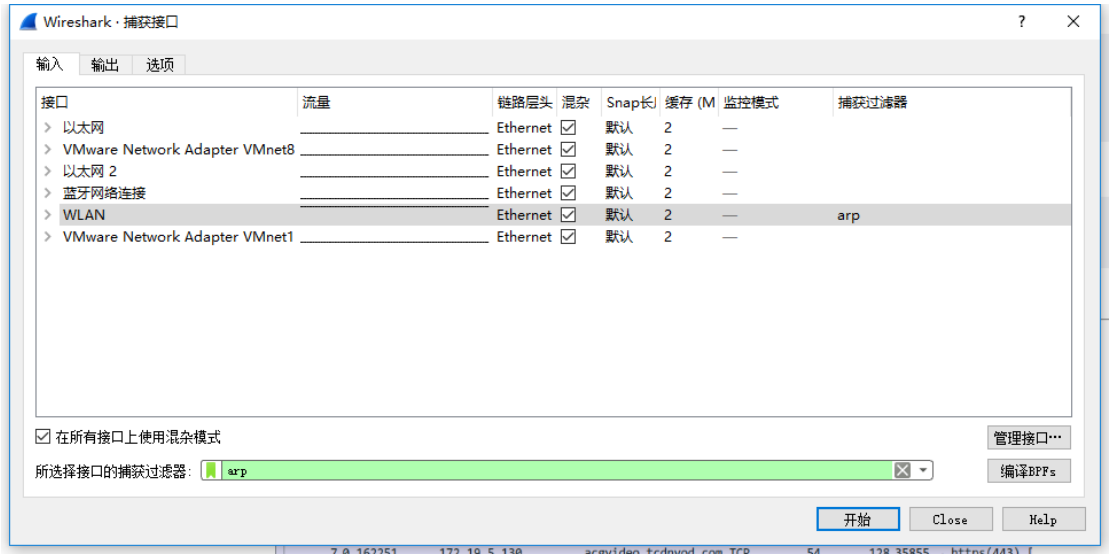
- **配置应用显示过滤器，让界面只显示某一协议类型的数据包。**

直接在 Filter 工具栏中输入需要显示的协议即可，如 http

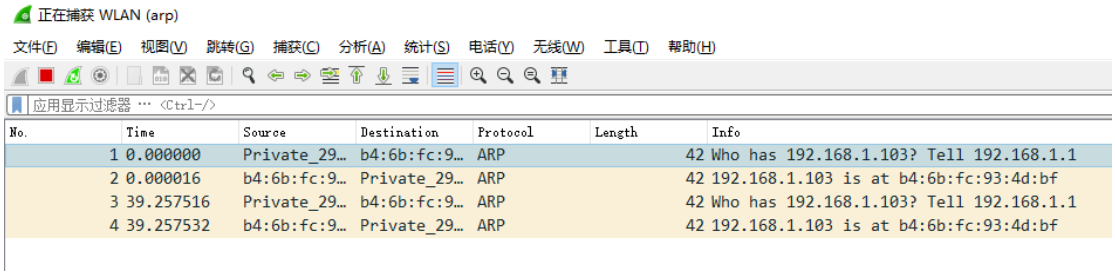



- **配置捕获过滤器，只捕获某类协议的数据包。**

在 捕获->选项 中对捕获过滤器进行配置




在捕获过滤器中选择 arp，点击开始捕获




- **利用 Ping.exe，Netstat.exe， Telnet.exe, Tracert.exe, Arp.exe, Ipconfig.exe, Net.exe, Route.exe 命令完成在实验步骤中列举的 11 个功能。**

1. 测试到特定地址的联通性、数据包延迟时间

使用 ping 命令测试个人服务器（地址 47.101.41.23）

```
C:\Windows\system32>ping 47.101.41.23

正在 Ping 47.101.41.23 具有 32 字节的数据:
来自 47.101.41.23 的回复: 字节=32 时间=12ms TTL=48
来自 47.101.41.23 的回复: 字节=32 时间=17ms TTL=48
来自 47.101.41.23 的回复: 字节=32 时间=12ms TTL=48
来自 47.101.41.23 的回复: 字节=32 时间=13ms TTL=48

47.101.41.23 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 = 12ms, 最长 = 17ms, 平均 = 13ms
```

联通性良好，数据包延迟时间约为 13ms

2. 显示本机的网卡物理地址、IP 地址

使用 ipconfig/all s 命令得到：

当前 IP 地址为 192.168.1.103

网卡物理地址为 B4-6B-FC-93-4D-BF

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . : lan
   描述. . . . . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   物理地址. . . . . . . . . . . . . : B4-6B-FC-93-4D-BF
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . . : fdbb:a874:b723::3af(首选)
   获得租约的时间  . . . . . . . . . : 2019年9月15日 14:04:21
   租约过期的时间  . . . . . . . . . : 2019年9月16日 14:04:20
   本地链接 IPv6 地址. . . . . . . . : fe80::c13b:b998:34cd:b252%9(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.1.103(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2019年9月15日 10:00:36
   租约过期的时间  . . . . . . . . . : 2019年9月16日 2:04:17
   默认网关. . . . . . . . . . . . . : 192.168.1.1
   DHCP 服务器 . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 45378556
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-24-FE-80-F1-B0-25-AA-29-12-28
   DNS 服务器  . . . . . . . . . . . : fdbb:a874:b723::1
                                       192.168.1.1
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
   连接特定的 DNS 后缀搜索列表:
                                       lan
```

3. 显示本机的默认网关地址、DNS 服务器地址

如上图，本机默认网关地址为 192.168.1.1

DNS 服务器地址为 192.168.1.1

4. 显示本机记录的局域网内其它机器 IP 地址与其物理地址的对照表

使用 arp -a 命令或 arp-g 命令

```
C:\Windows\system32>arp -a

接口: 192.168.183.1 --- 0x5
  Internet 地址         物理地址              类型
  192.168.183.254       00-50-56-ed-b9-39     动态
  192.168.183.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 192.168.1.103 --- 0x9
  Internet 地址         物理地址              类型
  192.168.1.1           b0-25-aa-29-12-28     动态
  192.168.1.255         ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 192.168.127.1 --- 0x14
  Internet 地址         物理地址              类型
  192.168.127.254       00-50-56-ff-6e-c9     动态
  192.168.127.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

5. 显示从本机到达一个特定地址的路由

使用 tracert [Addr]命令来跟踪路由

```
C:\Windows\system32>tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.a.shifen.com [183.232.231.174] 的路由:

  1     2 ms     2 ms     1 ms  OpenWrt.lan [192.168.1.1]
  2     3 ms     1 ms     5 ms  10.0.2.3
  3     2 ms    36 ms    12 ms  10.3.1.62
  4     *        *        *     请求超时。
  5     *        *        *     请求超时。
  6    17 ms    38 ms     8 ms  39.174.130.9
  7     *        *        *     请求超时。
  8     5 ms     *        4 ms  221.183.47.173
  9     *        *        *     请求超时。
 10     *        *        *     请求超时。
 11    39 ms    32 ms    36 ms  120.241.49.238
 12     *        *        *     请求超时。
 13     *        *        *     请求超时。
 14    29 ms    30 ms    38 ms  183.232.231.174

跟踪完成。
```

6. 显示某一个域名的 IP 地址

使用 nslookup 命令

```
C:\Windows\system32>nslookup www.baidu.com
服务器:  dns1.zju.edu.cn
Address:  10.10.0.21

非权威应答:
名称:    www.a.shifen.com
Addresses:  183.232.231.172
          183.232.231.174
Aliases:  www.baidu.com
```

7. 显示已经与本机建立 TCP 连接的端口、IP 地址、连接状态等信息

使用 netstat 命令，部分状态如下：

LISTEN：监听 TCP 端口的连接请求

ESTABLISHED：连接已建立

TIME-WAIT：等待中，确保 TCP 接收到连接中断请求的确认

CLOSED：没有任何连接状态

```
C:\Windows\system32>netstat

活动连接

  协议  本地地址          外部地址        状态
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52403  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52405  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52409  TIME_WAIT
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52411  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52413  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52415  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52417  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52428  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52430  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52438  TIME_WAIT
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52440  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52442  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52444  FIN_WAIT_2
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52446  TIME_WAIT
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52448  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52450  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52455  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52459  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52464  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52469  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52479  TIME_WAIT
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52482  TIME_WAIT
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52487  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52489  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52491  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52493  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52498  TIME_WAIT
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52500  TIME_WAIT
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52506  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52508  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52560  TIME_WAIT
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52562  TIME_WAIT
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52589  ESTABLISHED
  TCP    127.0.0.1:1080         DESKTOP-Q2K9ADR:52591  ESTABLISHED
  TCP    127.0.0.1:49674        DESKTOP-Q2K9ADR:49675  ESTABLISHED
  TCP    127.0.0.1:49675        DESKTOP-Q2K9ADR:49674  ESTABLISHED
  TCP    127.0.0.1:50041        DESKTOP-Q2K9ADR:55861  ESTABLISHED
  TCP    127.0.0.1:52390        DESKTOP-Q2K9ADR:54530  ESTABLISHED
  TCP    127.0.0.1:52391        DESKTOP-Q2K9ADR:52392  ESTABLISHED
  TCP    127.0.0.1:52392        DESKTOP-Q2K9ADR:52391  ESTABLISHED
  TCP    127.0.0.1:52393        DESKTOP-Q2K9ADR:52404  ESTABLISHED
  TCP    127.0.0.1:52393        DESKTOP-Q2K9ADR:52408  TIME_WAIT
  TCP    127.0.0.1:52393        DESKTOP-Q2K9ADR:52412  ESTABLISHED
  TCP    127.0.0.1:52393        DESKTOP-Q2K9ADR:52416  ESTABLISHED
  TCP    127.0.0.1:52393        DESKTOP-Q2K9ADR:52429  ESTABLISHED
  TCP    127.0.0.1:52393        DESKTOP-Q2K9ADR:52437  TIME_WAIT
```

8. 显示本机的路由表信息，并手工添加一个路由

通过 route print 来查看路由表

由于路由表较长，在这里只查看 Ipv4 的路由表，对应命令为 route print -4

```
C:\Windows\system32>route print -4
===========================================================================
接口列表
 19...b0 25 aa 29 12 28 ......Realtek PCIe GbE Family Controller
  8...b4 6b fc 93 4d c0 ......Microsoft Wi-Fi Direct Virtual Adapter
  5...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 20...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  9...b4 6b fc 93 4d bf ......Intel(R) Wireless-AC 9560 160MHz
 10...00 ff 6a 9a f6 e4 ......Sangfor SSL VPN CS Support System VNIC
  6...b4 6b fc 93 4d c3 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
  3...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.103     50
        127.0.0.0        255.0.0.0            在链路上         127.0.0.1    331
        127.0.0.1  255.255.255.255            在链路上         127.0.0.1    331
  127.255.255.255  255.255.255.255            在链路上         127.0.0.1    331
      192.168.1.0    255.255.255.0            在链路上     192.168.1.103    306
    192.168.1.103  255.255.255.255            在链路上     192.168.1.103    306
    192.168.1.255  255.255.255.255            在链路上     192.168.1.103    306
    192.168.127.0    255.255.255.0            在链路上     192.168.127.1    291
    192.168.127.1  255.255.255.255            在链路上     192.168.127.1    291
  192.168.127.255  255.255.255.255            在链路上     192.168.127.1    291
    192.168.183.0    255.255.255.0            在链路上     192.168.183.1    291
    192.168.183.1  255.255.255.255            在链路上     192.168.183.1    291
  192.168.183.255  255.255.255.255            在链路上     192.168.183.1    291
        224.0.0.0        240.0.0.0            在链路上         127.0.0.1    331
        224.0.0.0        240.0.0.0            在链路上     192.168.1.103    306
        224.0.0.0        240.0.0.0            在链路上     192.168.183.1    291
        224.0.0.0        240.0.0.0            在链路上     192.168.127.1    291
  255.255.255.255  255.255.255.255            在链路上         127.0.0.1    331
  255.255.255.255  255.255.255.255            在链路上     192.168.1.103    306
  255.255.255.255  255.255.255.255            在链路上     192.168.183.1    291
  255.255.255.255  255.255.255.255            在链路上     192.168.127.1    291
===========================================================================
永久路由:
  网络地址          网络掩码  网关地址   跃点数
          0.0.0.0          0.0.0.0    222.205.123.1     默认
===========================================================================
```

使用 route add  来添加一条路由  route add [*.*.*.*] mask [*.*.*.*] [*.*.*.*]

```
C:\Windows\system32>route add 47.101.41.23 mask 255.255.255.255 192.168.1.103
 操作完成!

C:\Windows\system32>route print -4
===========================================================================
接口列表
 19...b0 25 aa 29 12 28 ......Realtek PCIe GbE Family Controller
  8...b4 6b fc 93 4d c0 ......Microsoft Wi-Fi Direct Virtual Adapter
  5...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 20...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  9...b4 6b fc 93 4d bf ......Intel(R) Wireless-AC 9560 160MHz
 10...00 ff 6a 9a f6 e4 ......Sangfor SSL VPN CS Support System VNIC
  6...b4 6b fc 93 4d c3 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
  3...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.103     50
     47.101.41.23  255.255.255.255            在链路上     192.168.1.103     51
        127.0.0.0        255.0.0.0            在链路上         127.0.0.1    331
        127.0.0.1  255.255.255.255            在链路上         127.0.0.1    331
  127.255.255.255  255.255.255.255            在链路上         127.0.0.1    331
      192.168.1.0    255.255.255.0            在链路上     192.168.1.103    306
    192.168.1.103  255.255.255.255            在链路上     192.168.1.103    306
    192.168.1.255  255.255.255.255            在链路上     192.168.1.103    306
    192.168.127.0    255.255.255.0            在链路上     192.168.127.1    291
    192.168.127.1  255.255.255.255            在链路上     192.168.127.1    291
  192.168.127.255  255.255.255.255            在链路上     192.168.127.1    291
    192.168.183.0    255.255.255.0            在链路上     192.168.183.1    291
    192.168.183.1  255.255.255.255            在链路上     192.168.183.1    291
  192.168.183.255  255.255.255.255            在链路上     192.168.183.1    291
        224.0.0.0        240.0.0.0            在链路上         127.0.0.1    331
        224.0.0.0        240.0.0.0            在链路上     192.168.1.103    306
        224.0.0.0        240.0.0.0            在链路上     192.168.183.1    291
        224.0.0.0        240.0.0.0            在链路上     192.168.127.1    291
  255.255.255.255  255.255.255.255            在链路上         127.0.0.1    331
  255.255.255.255  255.255.255.255            在链路上     192.168.1.103    306
  255.255.255.255  255.255.255.255            在链路上     192.168.183.1    291
  255.255.255.255  255.255.255.255            在链路上     192.168.127.1    291
===========================================================================
```

9. 显示本机的网络映射连接

使用 net view 命令 不带参数

```
C:\Windows\system32>net view
服务器名称            注解

-------------------------------------------------------------------------------
\\DESKTOP-Q2K9ADR
命令成功完成。
```

10. 显示局域网内某台机器的共享资源

使用 net view [*.*.*.*]命令获取，如 net view \\192.168.1.103\

```
C:\Windows\system32>net view \\192.168.1.103\
在 \\192.168.1.103\ 的共享资源


共享名   类型   使用为   注释

-------------------------------------------------------------------------------
Users    Disk
命令成功完成。
```

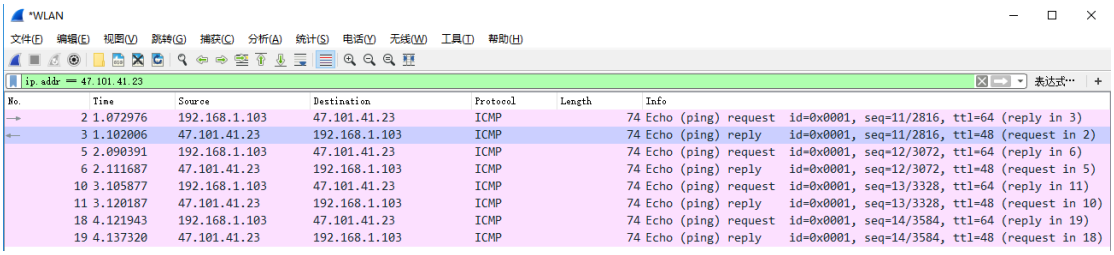
11. 使用 telnet 连接 WEB 服务器的端口，输入（<cr>表示回车）获得该网站的主页内容

命令行中使用 telnet www.baidu.com 80 在 wireshark 中观察截到得 http 请求

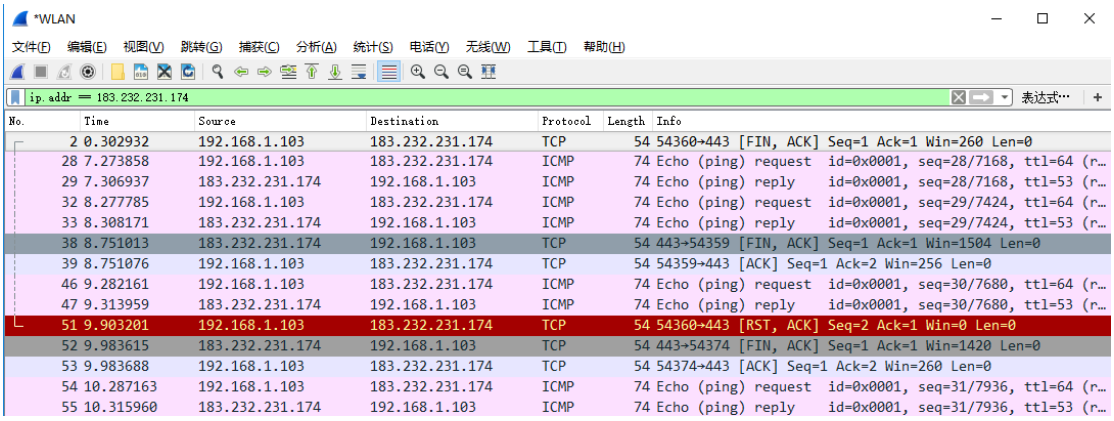
```
> Internet Protocol Version 4, Src: 1.192.193.119, Dst: 192.168.1.103
> Transmission Control Protocol, Src Port: 80, Dst Port: 52565, Seq: 1866, Ack: 1086, Len: 5
> [3 Reassembled TCP Segments (1870 bytes): #33(1388), #34(477), #35(5)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Server: nginx\r\n
    Date: Tue, 17 Sep 2019 13:20:59 GMT\r\n
    Content-Type: application/octet-stream\r\n
    Transfer-Encoding: chunked\r\n
    Connection: close\r\n
    Cache-Control: no-cache\r\n
    pragma: no-cache\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.052850000 seconds]
    [Request in frame: 29]
```

- **观察使用 Ping 命令时在 WireShark 中出现的数据包并捕获。这是什么协议？**

  Ping IP 地址时采用的是 ICMP 协议。

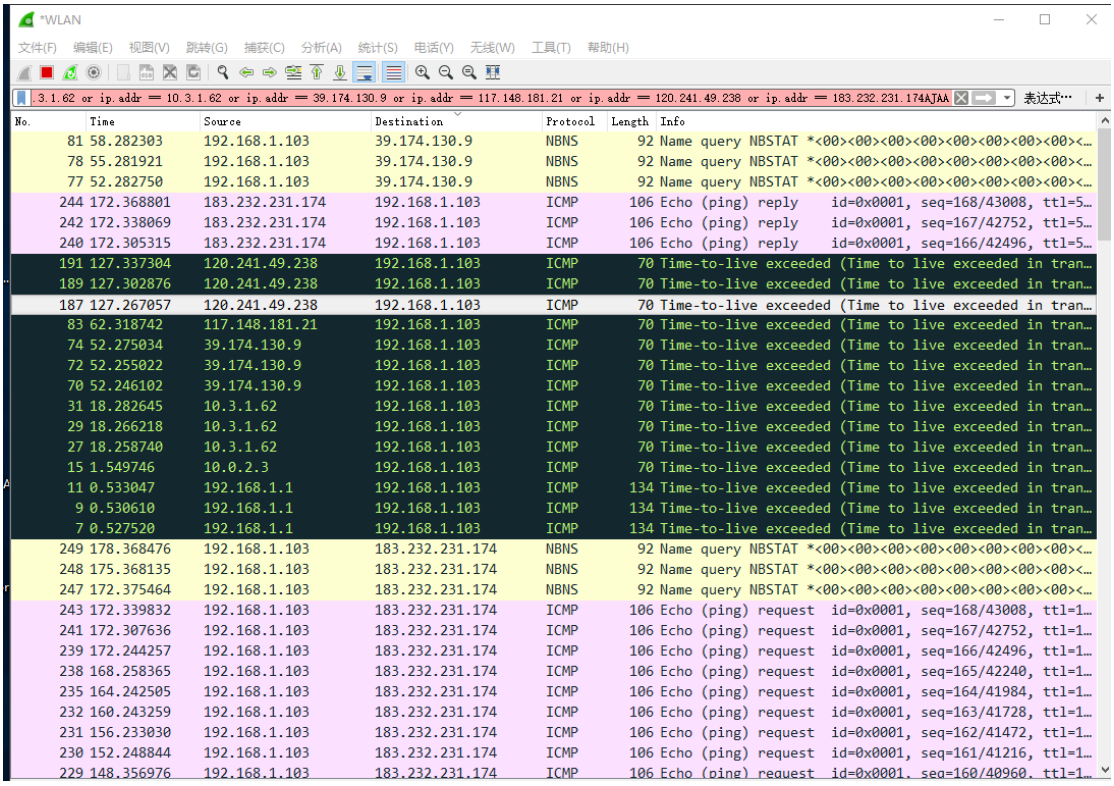



Ping 域名时采用的是 ICMP 和 TCP 协议。



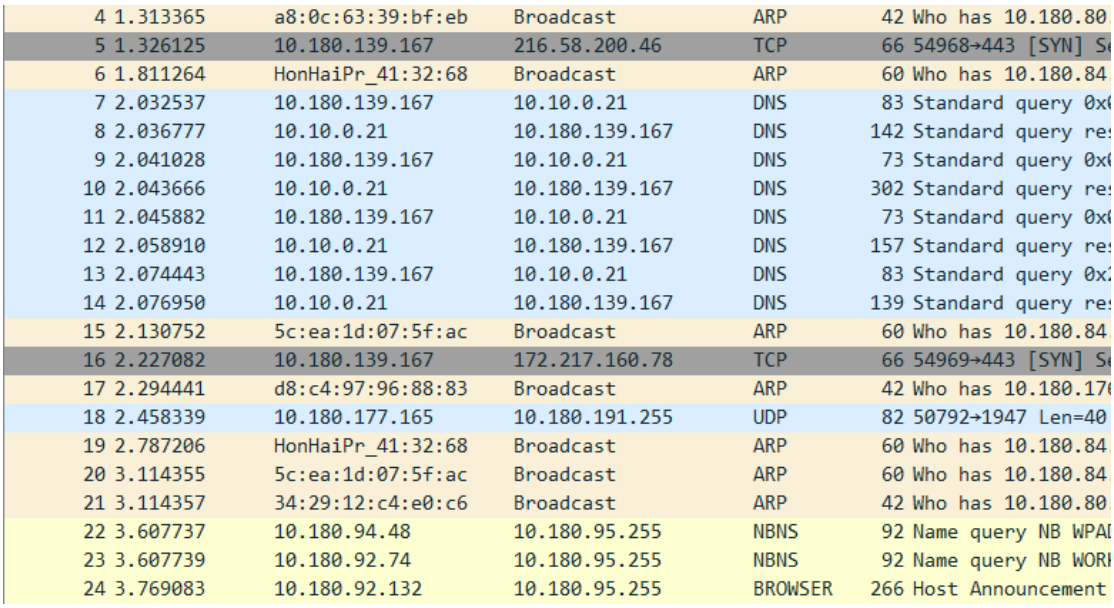

- **观察使用 Tracert 命令时在 WireShark 中出现的数据包并捕获。这是什么协议？**

捕获的数据表中协议为 ICMP 和 NBNS 协议




- **观察使用 Nslookup 命令时在 WireShark 中出现的数据包并捕获。这是什么协议？**

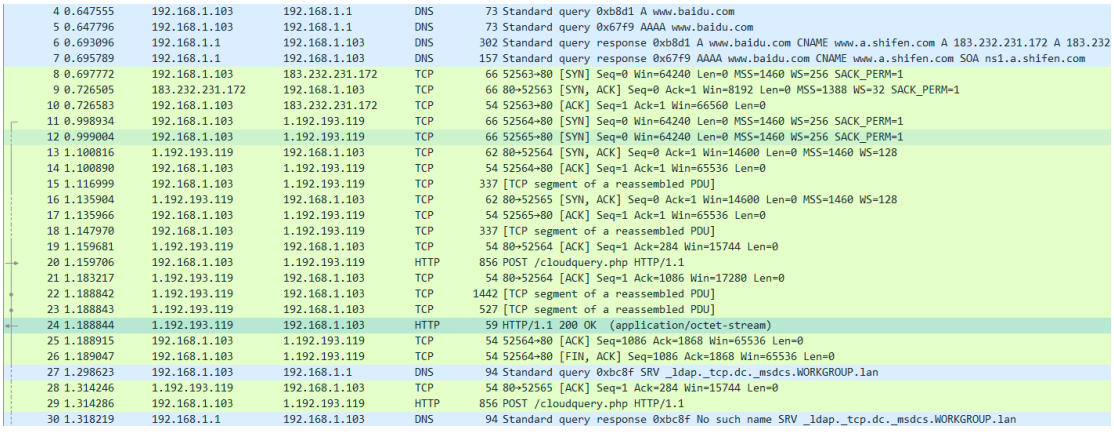
DNS、ARP、UDP、NBNS、OICQ 协议



| | | | | | |
|---|---|---|---|---|---|
| 4 | 1.313365 | a8:0c:63:39:bf:eb | Broadcast | ARP | 42 Who has 10.180.80 |
| 5 | 1.326125 | 10.180.139.167 | 216.58.200.46 | TCP | 66 54968→443 [SYN] S |
| 6 | 1.811264 | HonHaiPr_41:32:68 | Broadcast | ARP | 60 Who has 10.180.84 |
| 7 | 2.032537 | 10.180.139.167 | 10.10.0.21 | DNS | 83 Standard query 0x |
| 8 | 2.036777 | 10.10.0.21 | 10.180.139.167 | DNS | 142 Standard query re |
| 9 | 2.041028 | 10.180.139.167 | 10.10.0.21 | DNS | 73 Standard query 0x |
| 10 | 2.043666 | 10.10.0.21 | 10.180.139.167 | DNS | 302 Standard query re |
| 11 | 2.045882 | 10.180.139.167 | 10.10.0.21 | DNS | 73 Standard query 0x |
| 12 | 2.058910 | 10.10.0.21 | 10.180.139.167 | DNS | 157 Standard query re |
| 13 | 2.074443 | 10.180.139.167 | 10.10.0.21 | DNS | 83 Standard query 0x |
| 14 | 2.076950 | 10.10.0.21 | 10.180.139.167 | DNS | 139 Standard query re |
| 15 | 2.130752 | 5c:ea:1d:07:5f:ac | Broadcast | ARP | 60 Who has 10.180.84 |
| 16 | 2.227082 | 10.180.139.167 | 172.217.160.78 | TCP | 66 54969→443 [SYN] S |
| 17 | 2.294441 | d8:c4:97:96:88:83 | Broadcast | ARP | 42 Who has 10.180.17 |
| 18 | 2.458339 | 10.180.177.165 | 10.180.191.255 | UDP | 82 50792→1947 Len=40 |
| 19 | 2.787206 | HonHaiPr_41:32:68 | Broadcast | ARP | 60 Who has 10.180.84 |
| 20 | 3.114355 | 5c:ea:1d:07:5f:ac | Broadcast | ARP | 60 Who has 10.180.84 |
| 21 | 3.114357 | 34:29:12:c4:e0:c6 | Broadcast | ARP | 42 Who has 10.180.80 |
| 22 | 3.607737 | 10.180.94.48 | 10.180.95.255 | NBNS | 92 Name query NB WPAD |
| 23 | 3.607739 | 10.180.92.74 | 10.180.95.255 | NBNS | 92 Name query NB WORK |
| 24 | 3.769083 | 10.180.92.132 | 10.180.95.255 | BROWSER | 266 Host Announcement |

- **观察使用 Telnet 命令时在 WireShark 中出现的数据包并捕获。这是什么协议？**

  DNS、TCP 和 HTTP 协议



| | | | | | |
|---|---|---|---|---|---|
| 4 | 0.647555 | 192.168.1.103 | 192.168.1.1 | DNS | 73 Standard query 0xb8d1 A www.baidu.com |
| 5 | 0.647796 | 192.168.1.103 | 192.168.1.1 | DNS | 73 Standard query 0x67f9 AAAA www.baidu.com |
| 6 | 0.693096 | 192.168.1.1 | 192.168.1.103 | DNS | 302 Standard query response 0xb8d1 A www.baidu.com CNAME www.a.shifen.com A 183.232.231.172 A 183.232 |
| 7 | 0.695789 | 192.168.1.1 | 192.168.1.103 | DNS | 157 Standard query response 0x67f9 AAAA www.baidu.com CNAME www.a.shifen.com SOA ns1.a.shifen.com |
| 8 | 0.697772 | 192.168.1.103 | 183.232.231.172 | TCP | 66 52563→80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 9 | 0.726505 | 183.232.231.172 | 192.168.1.103 | TCP | 66 80→52563 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1388 WS=32 SACK_PERM=1 |
| 10 | 0.726583 | 192.168.1.103 | 183.232.231.172 | TCP | 54 52563→80 [ACK] Seq=1 Ack=1 Win=66560 Len=0 |
| 11 | 0.998934 | 192.168.1.103 | 1.192.193.119 | TCP | 66 52564→80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 12 | 0.999004 | 192.168.1.103 | 1.192.193.119 | TCP | 66 52565→80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 13 | 1.100816 | 1.192.193.119 | 192.168.1.103 | TCP | 62 80→52564 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 WS=128 |
| 14 | 1.100890 | 192.168.1.103 | 1.192.193.119 | TCP | 54 52564→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 15 | 1.116999 | 192.168.1.103 | 1.192.193.119 | TCP | 337 [TCP segment of a reassembled PDU] |
| 16 | 1.135904 | 1.192.193.119 | 192.168.1.103 | TCP | 62 80→52565 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 WS=128 |
| 17 | 1.135966 | 192.168.1.103 | 1.192.193.119 | TCP | 54 52565→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 18 | 1.147970 | 192.168.1.103 | 1.192.193.119 | TCP | 337 [TCP segment of a reassembled PDU] |
| 19 | 1.159681 | 1.192.193.119 | 192.168.1.103 | TCP | 54 80→52564 [ACK] Seq=1 Ack=284 Win=15744 Len=0 |
| 20 | 1.159706 | 192.168.1.103 | 1.192.193.119 | HTTP | 856 POST /cloudquery.php HTTP/1.1 |
| 21 | 1.183217 | 1.192.193.119 | 192.168.1.103 | TCP | 54 80→52564 [ACK] Seq=1 Ack=1086 Win=17280 Len=0 |
| 22 | 1.188842 | 1.192.193.119 | 192.168.1.103 | TCP | 1442 [TCP segment of a reassembled PDU] |
| 23 | 1.188843 | 1.192.193.119 | 192.168.1.103 | TCP | 527 [TCP segment of a reassembled PDU] |
| 24 | 1.188844 | 1.192.193.119 | 192.168.1.103 | HTTP | 59 HTTP/1.1 200 OK (application/octet-stream) |
| 25 | 1.188915 | 192.168.1.103 | 1.192.193.119 | TCP | 54 52564→80 [ACK] Seq=1086 Ack=1868 Win=65536 Len=0 |
| 26 | 1.189047 | 192.168.1.103 | 1.192.193.119 | TCP | 54 52564→80 [FIN, ACK] Seq=1086 Ack=1868 Win=65536 Len=0 |
| 27 | 1.298623 | 192.168.1.103 | 192.168.1.1 | DNS | 94 Standard query 0xbc8f SRV _ldap._tcp.dc._msdcs.WORKGROUP.lan |
| 28 | 1.314246 | 1.192.193.119 | 192.168.1.103 | TCP | 54 80→52565 [ACK] Seq=1 Ack=284 Win=15744 Len=0 |
| 29 | 1.314286 | 192.168.1.103 | 1.192.193.119 | HTTP | 856 POST /cloudquery.php HTTP/1.1 |
| 30 | 1.318219 | 192.168.1.1 | 192.168.1.103 | DNS | 94 Standard query response 0xbc8f No such name SRV _ldap._tcp.dc._msdcs.WORKGROUP.lan |

## 六、 实验结果与分析

- WireShark 的两种过滤器有什么不同？

  显示过滤器：只针对已经捕获的报文，过滤出符合过滤规则的报文

  捕获过滤器：提前设置好过滤规则，只捕获符合过滤规则的报文。

- 哪些网络命令会产生在 WireShark 中产生数据包，为什么？

  Ping, Telnet.exe, Tracert.exe, Nslookup.exe 命令会产生数据包，因为这些命令需

要向对应的服务器发起请求并由本机接受响应，因此会产生数据包。

- Ping 发送的是什么类型的协议数据包？什么时候会出现 ARP 消息？Ping 一个域名和 Ping 一个 IP 地址出现的数据包有什么不同？

  Ping 发送的是 ICMP 协议数据包。

  Ping 的域名在计算机内没有被缓存时会出现 ARP 消息，从而对域名进行解析。

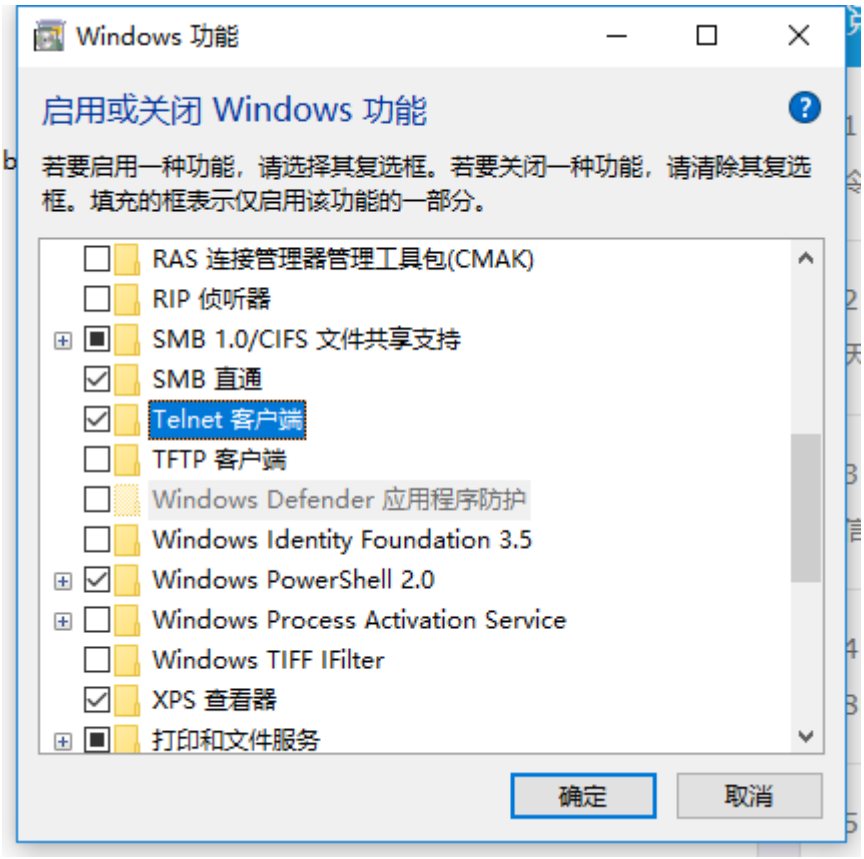
  不同：如果计算机内没有缓存 Ping 域名对应的 IP 地址时， 命令会先对域名进行解析。

## 七、 讨论、心得

1. 一开始进去时软件提示找不到接口，上网查询解决方案后得知是 NPF 服务没有启动，因此需要启动 NPF 服务，然后重启 WireShark 软件。启动的命令如下：


   但是这样的方式只能在这一次启动 NPF 服务，电脑重启之后需要重新启动。设置自动启动的命令为：sc config npf start=auto

2. Filter 工具栏中过滤器是区分大小写的。如 http 不能写成 HTTP 否则会报错。
3. 实验中没有出现 IP 过滤的操作。在这里补充一下，如果想让界面只显示某个 IP 地址的数据包，则需要使用过滤器： ip.addr == x.x.x.x 或 ip.src 或 ip.dst
4. 使用 telnet 命令时，系统提示不是内部或外部命令，也不是可运行的程序或批处理文件。此时需要在启用或关闭 Window 功能中勾选 Telnet 客户端选项。


Windows 功能
启用或关闭 Windows 功能
若要启用一种功能，请选择其复选框。若要关闭一种功能，请清除其复选框。填充的框表示仅启用该功能的一部分。
RAS 连接管理器管理工具包(CMAK)
RIP 侦听器
SMB 1.0/CIFS 文件共享支持
SMB 直通
Telnet 客户端
TFTP 客户端
Windows Defender 应用程序防护
Windows Identity Foundation 3.5
Windows PowerShell 2.0
Windows Process Activation Service
Windows TIFF IFilter
XPS 查看器
打印和文件服务
确定
取消