



计算机网络实验一

计算机网络协议层

信息学部 朱婉婷
zhuwanting@bjut.edu.cn

主要内容

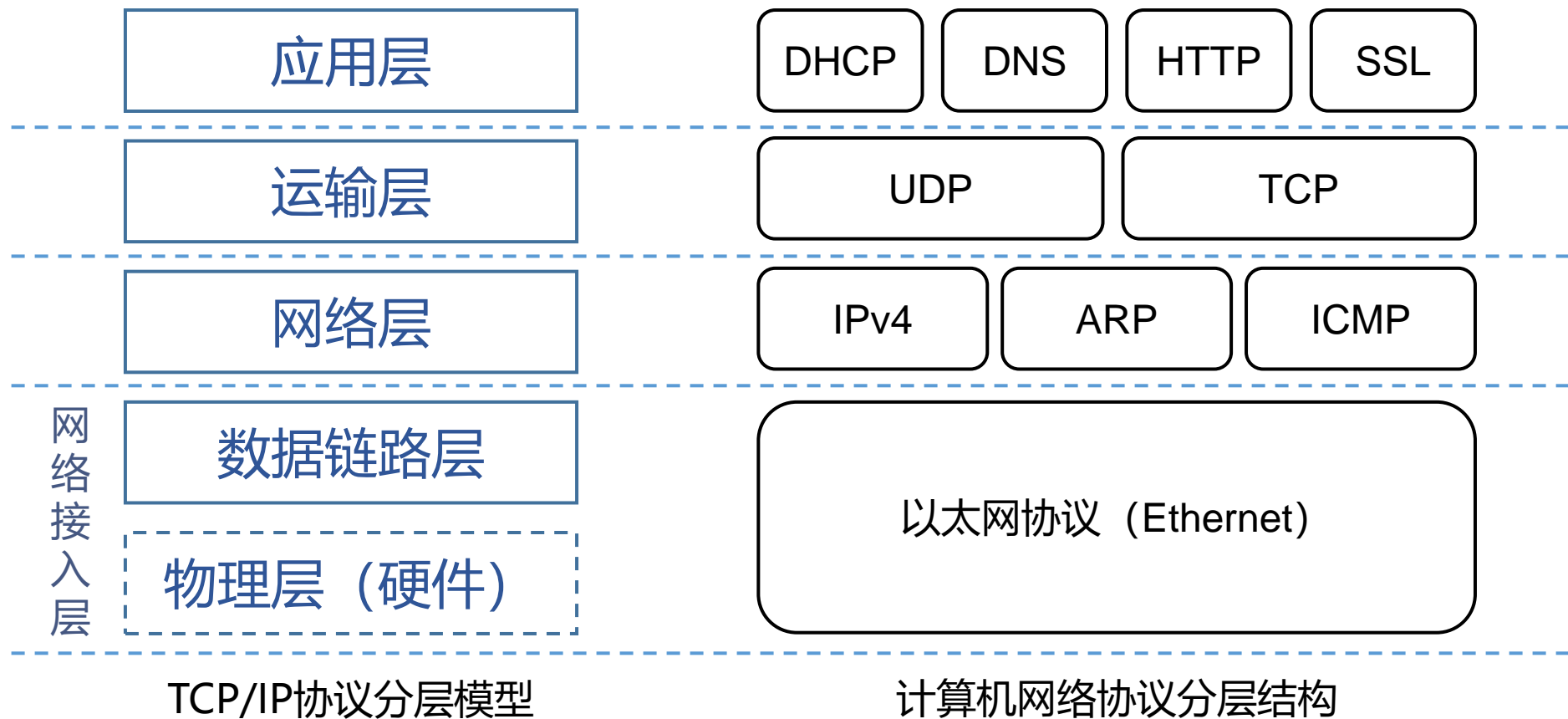
- 一、课程介绍
- 二、Wireshark的安装和使用
- 三、计算机网络协议层实验

课程介绍

- 计算机网络的配套实验课
- 9-16周，32学时，1学分
- 总共11个实验，1人1组独立完成
- 考核方式：
 - 考勤 10%
 - 实验过程 40%
 - 实验报告 50%
- 实验报告命名格式： 班级_学号_姓名_实验X
(其中X为阿拉伯数字)

实验安排

• TCP/IP协议与实验内容的对应关系



实验内容及其占总成绩比例

序号	实验项目名称	占总成绩比例
实验一	计算机网络协议层	10%
实验二	以太网协议（Ethernet）	10%
实验三	互联网协议第四版（IPv4）	10%
实验四	地址解析协议（ARP）	10%
实验五	互联网控制报文协议（ICMP）	10%
实验六	动态主机配置协议（DHCP）	10%
实验七	用户数据协议（UDP）	10%
实验八	传输控制协议（TCP）	10%
实验九	域名系统（DNS）	7%
实验十	超文本传输协议（HTTP）	7%
实验十一	安全套接字层（SSL）	6%

主要内容

一、课程简介

二、Wireshark的安装和使用

三、计算机网络协议层实验

认识抓包工具——Wireshark



- ◆ Wireshark是一款网络包分析器。
 - ✓能在多种平台上抓取和分析网络包，比如Windows、Linux和Mac等，开源且免费。
 - ✓辅助学习，可以更深入地理解网络协议。
 - ✓排查故障，可以更快地发现问题。



抓包工具的工作原理

◆ 网卡有四种工作模式

- 广播模式：网卡能够接收网络中的广播报文；
- 组播模式：网卡能够接收网络中的组播报文；
- 直接模式：网卡只能接收与自身硬件地址相匹配的单播报文；
- 混杂模式：网卡能够接收网络中的所有报文。

◆ 报文分析软件的工作原理

- 将网卡的接收模式设置为混杂模式。
- 利用计算机的网卡截获相连网络上所有的数据报文，并进行解析。

Wireshark的安装和使用

Wireshark 官方网站 <https://www.wireshark.org/>

The screenshot shows the Wireshark website's download page. At the top, the Wireshark logo is on the left, and navigation links for NEWS, Get Acquainted, Get Help, Develop, and SharkFest are on the right. The main heading is "Download Wireshark", followed by the text "The current stable release of Wireshark is 3.6.3." Below this, there are three tabs: "Stable Release (3.6.3) • March 23, 2022", "Old Stable Release (3.4.13) • March 23, 2022", and "Documentation". The "Stable Release (3.6.3)" tab is selected and highlighted with a yellow box. It contains a list of download links: "Windows Installer (64-bit)", "Windows Installer (32-bit)", "Windows PortableApps® (64-bit)", "Windows PortableApps® (32-bit)", "macOS Arm 64-bit .dmg", "macOS Intel 64-bit .dmg", and "Source Code". Below the tabs, a message states: "More downloads and documentation can be found on the downloads page." To the right of the download section, there is a "SharkFest Sponsors" area featuring advertisements for endace, FMADIO, sysdig, and SCOS, along with a Wireshark Authorized Training Partner logo for SCOS.

WIRESHARK

NEWS Get Acquainted Get Help Develop SharkFest

Download Wireshark

The current stable release of Wireshark is 3.6.3.

Stable Release (3.6.3) • March 23, 2022

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (64-bit)
- Windows PortableApps® (32-bit)
- macOS Arm 64-bit .dmg
- macOS Intel 64-bit .dmg
- Source Code

Old Stable Release (3.4.13) • March 23, 2022

Documentation

More downloads and documentation can be found on the downloads page.

SharkFest Sponsors

Always-on, scalable Packet Capture that integrates with all your tools

endace endace.com

10G 40G 100G PACKET CAPTURE

Never Drop Packets!

100Gbps 148Mpps sustained 24/7

Line Rate Full Packet Capture Hardware System

sysdig Creator of Falco

Sysdig Welcomes Gerald and the Wireshark Community

LEARN MORE

SCOS

WIRESHARK Authorized Training Partner

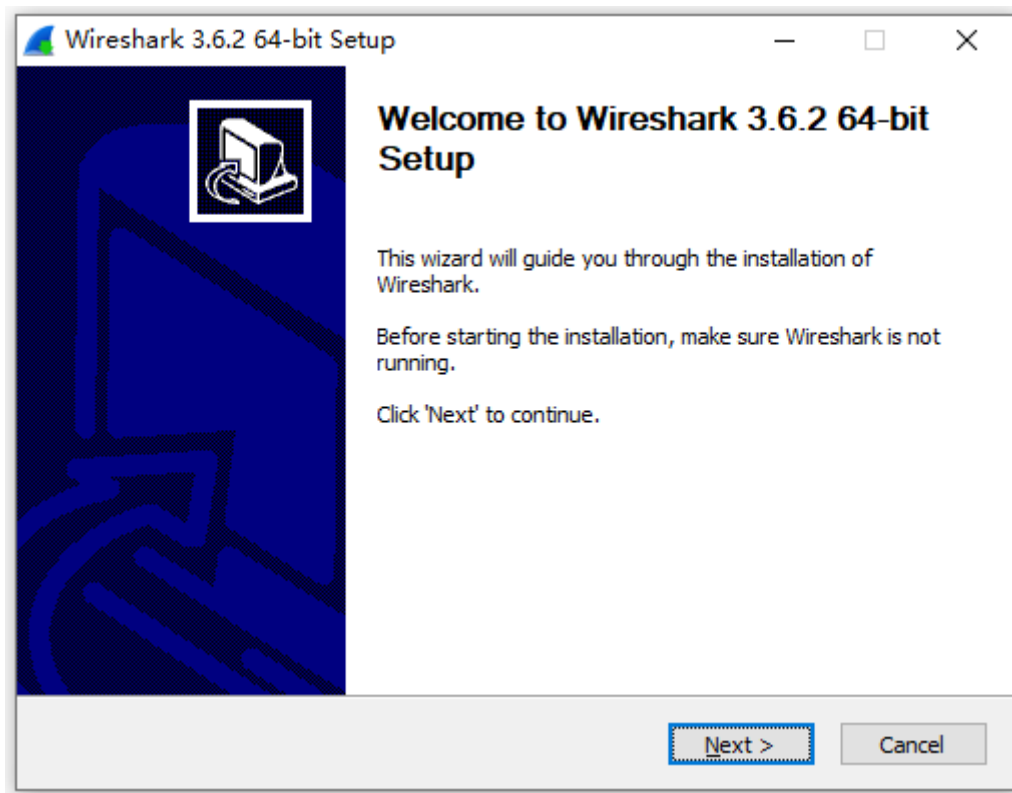
Official TCP / IP Troubleshooting Course Training & Wireshark Tools

www.scos.training

Powered by DigitalOcean

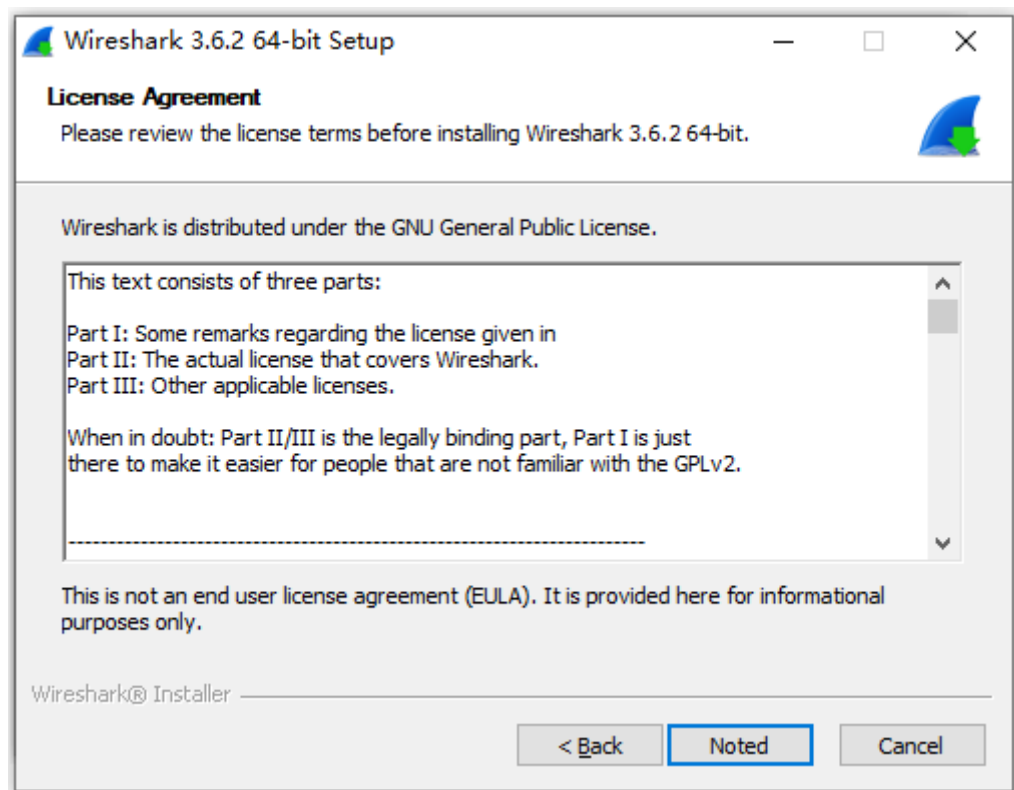
Wireshark的安装和使用

1、双击Wireshark安装包，进入安装界面，点击“Next”进入下一步：



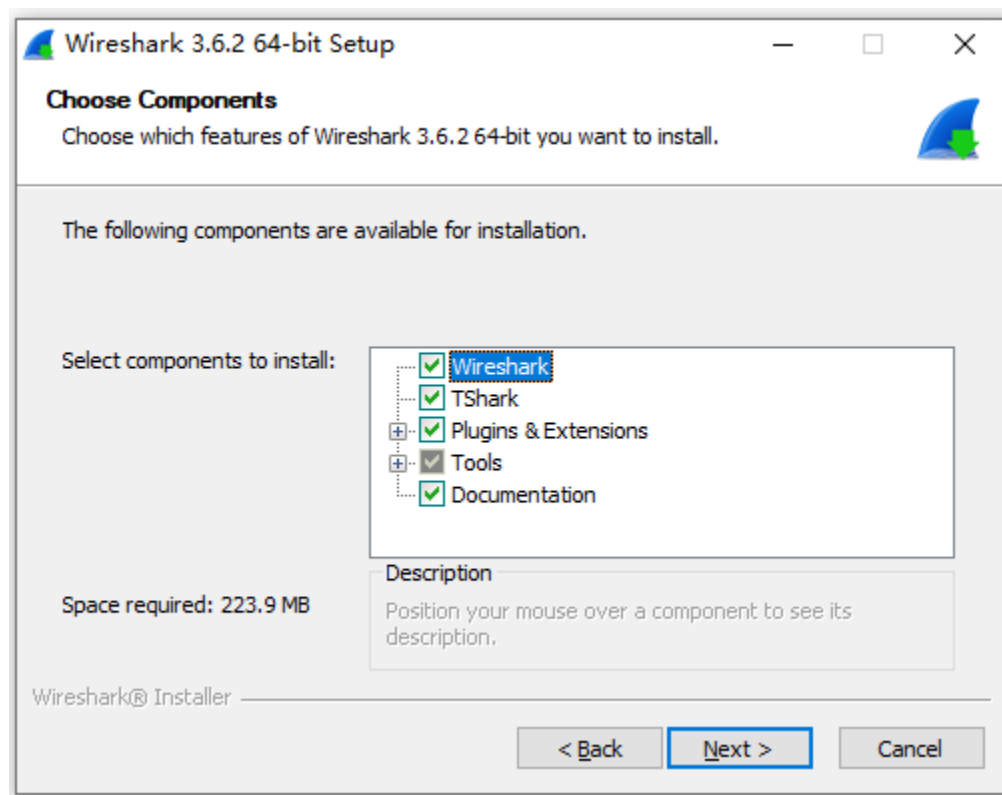
Wireshark的安装和使用

2、在接受软件许可会话框中点击 “Noted” 按钮；



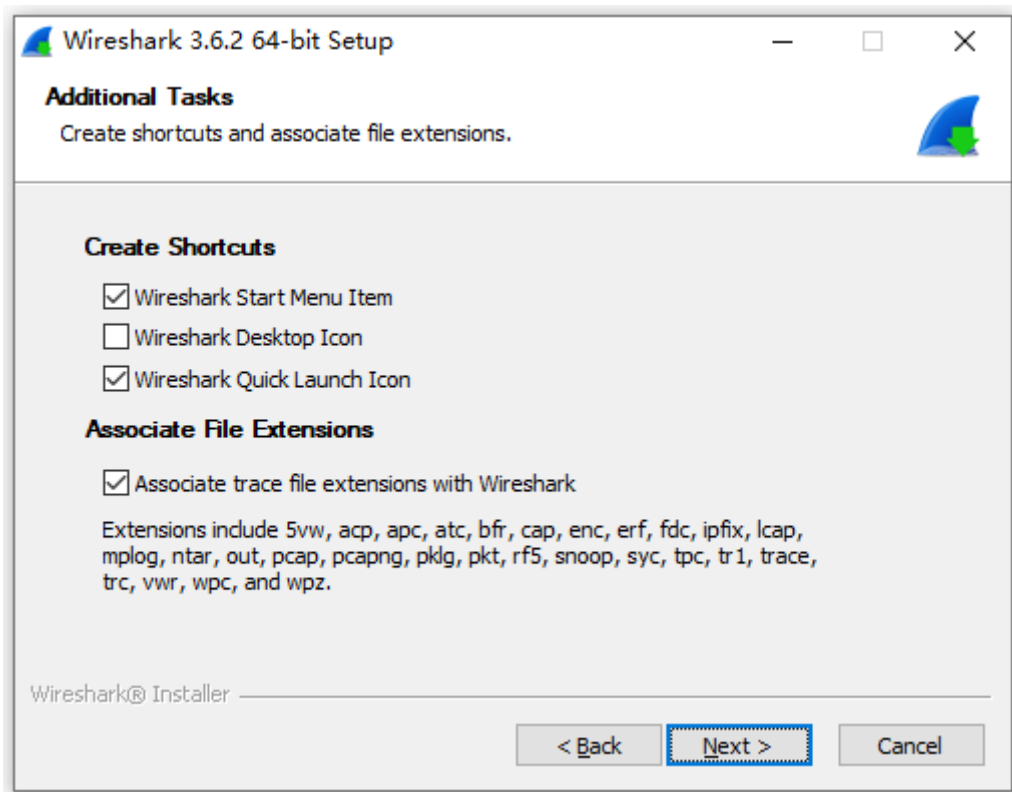
Wireshark的安装和使用

3、选择需要安装的组件，点击“Next”进行下一步：



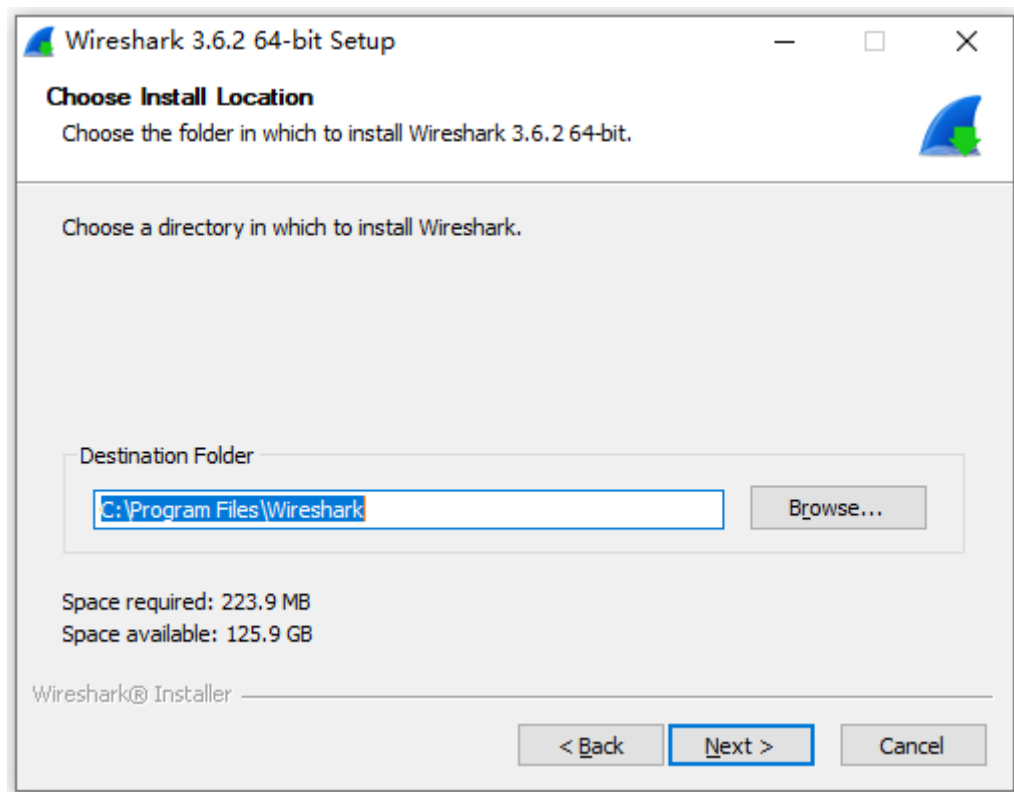
Wireshark的安装和使用

4、选择创建软件的快捷方式和文件扩展名（建议默认设置），点击“Next”进行下一步：



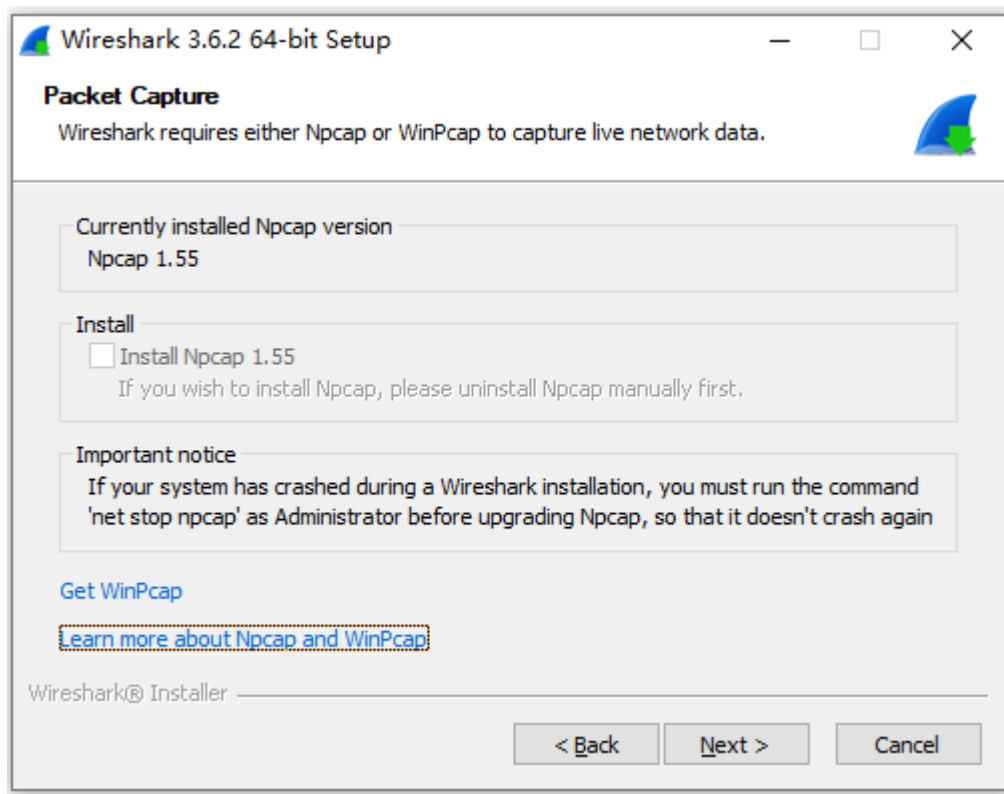
Wireshark的安装和使用

5、选择安装位置（可以修改），一般选择默认；



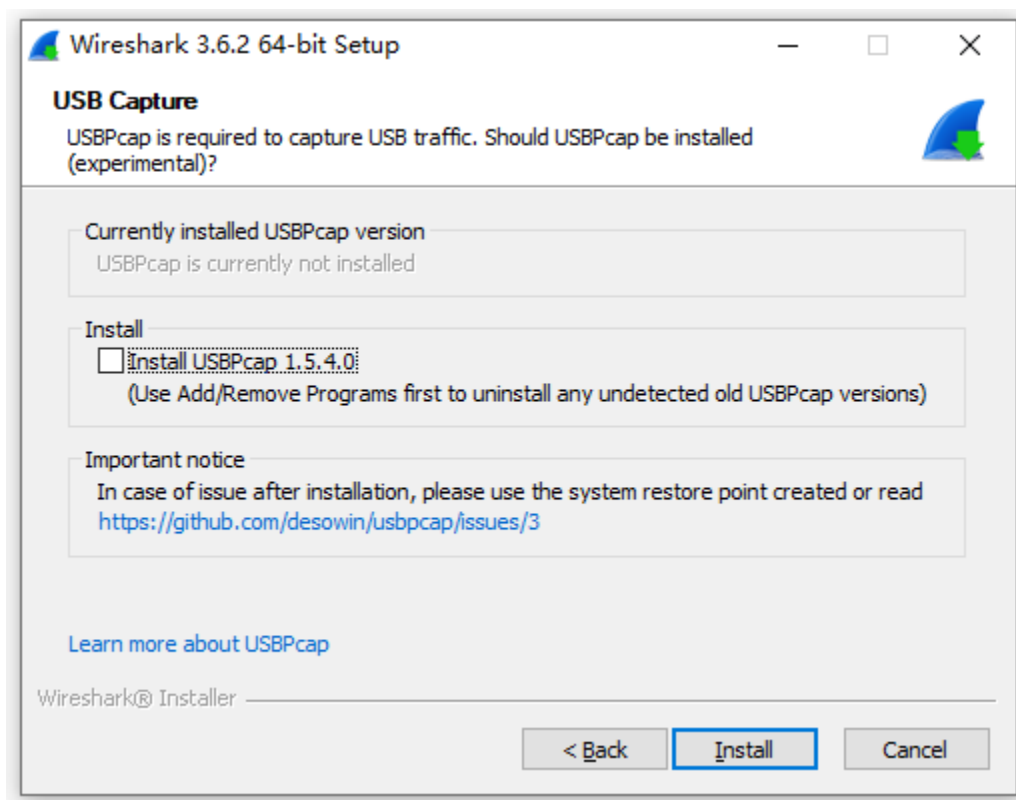
Wireshark的安装和使用

6、Npcap 和 WinPcap 是 libpcap 库的 Windows 版本。必须安装其中之一才能捕获 Windows 上的实时网络流量，首次安装时必须选中，重新安装时可不选。Npcap 支持 Windows 7 到 Windows 11。WinPcap 适用于 Windows 95 到 Windows 8。



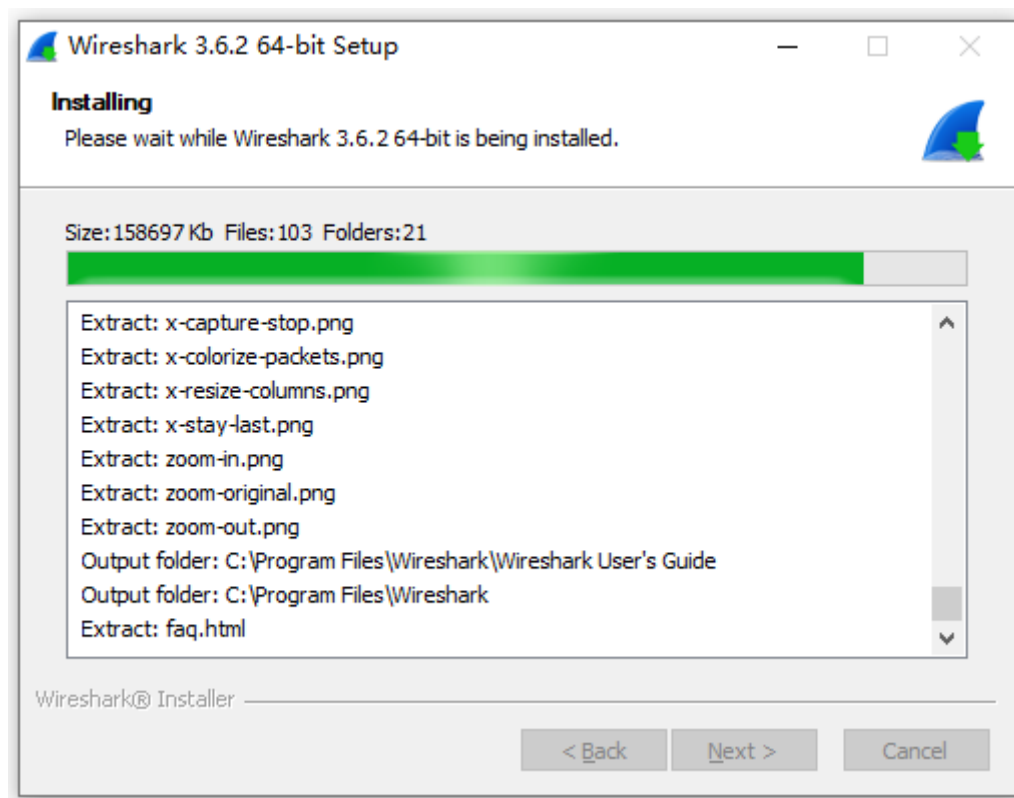
Wireshark的安装和使用

7、安装USBPcap界面，不用点击安装，直接点 “install” 进行软件安装；



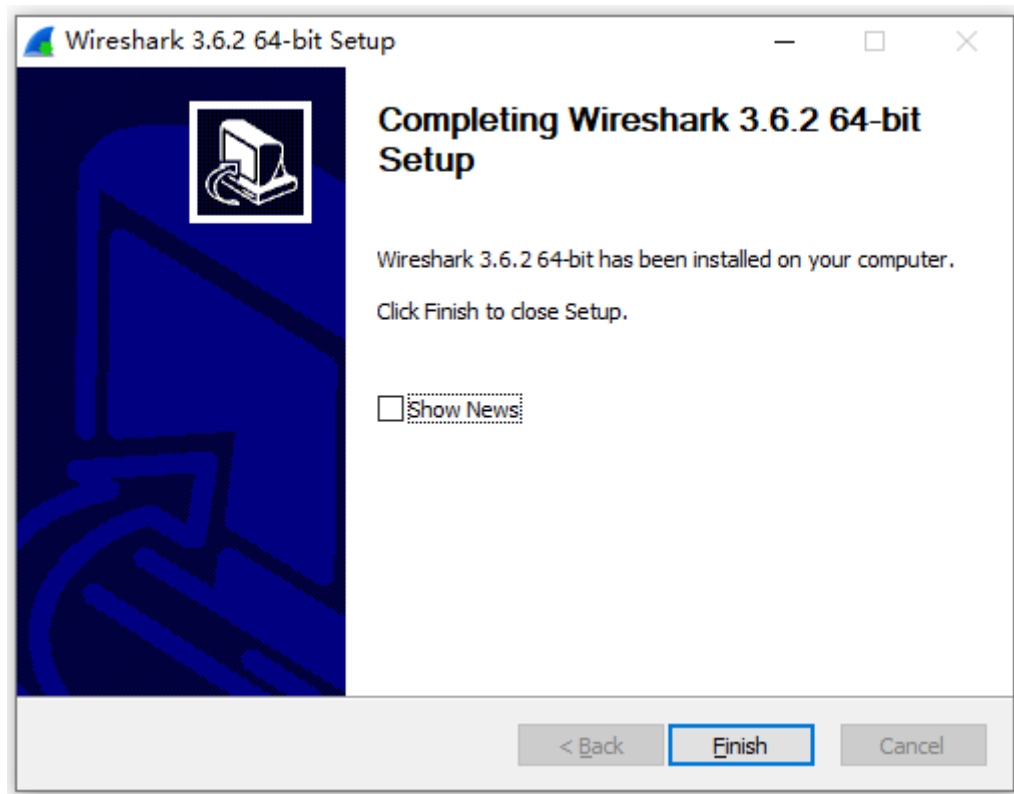
Wireshark的安装和使用

8、安装开始:



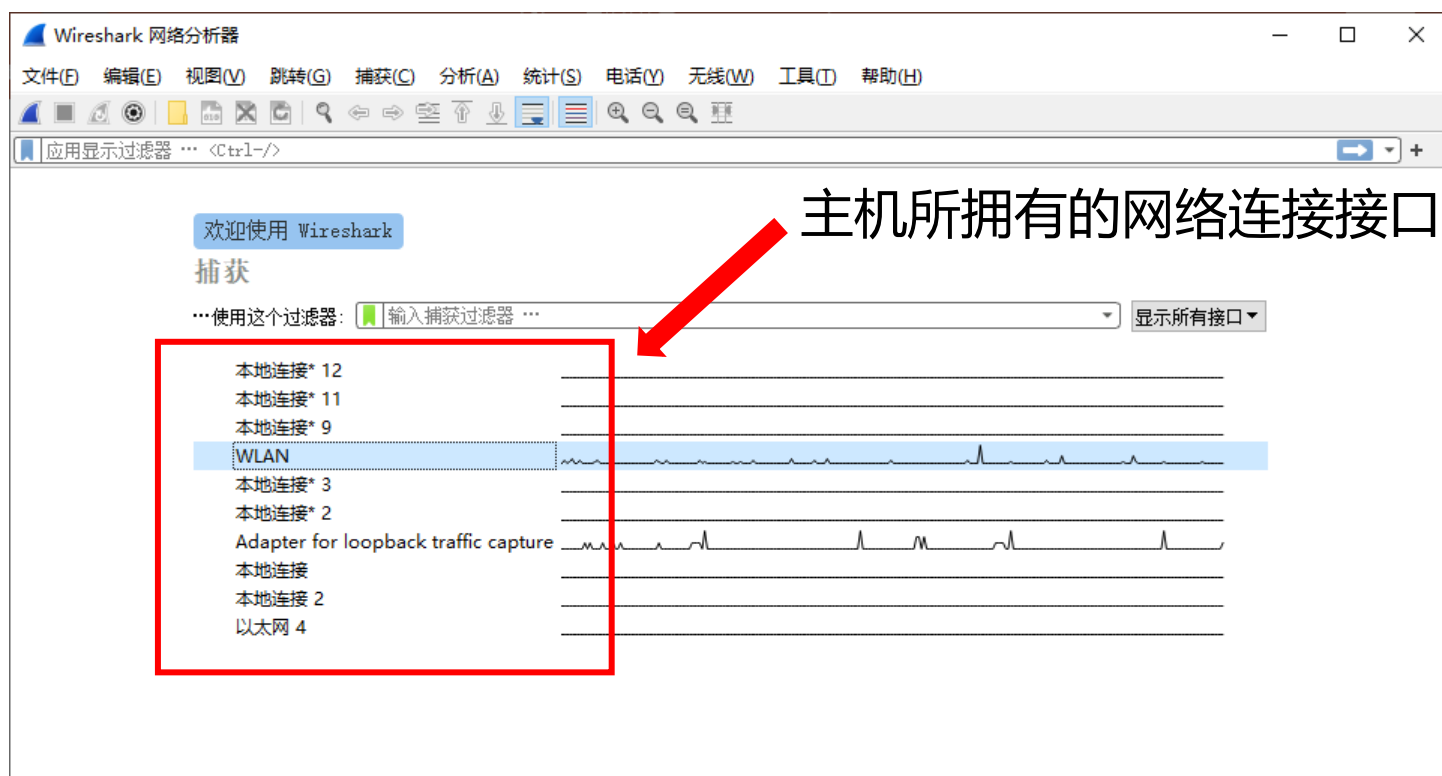
Wireshark的安装和使用

9、安装成功。



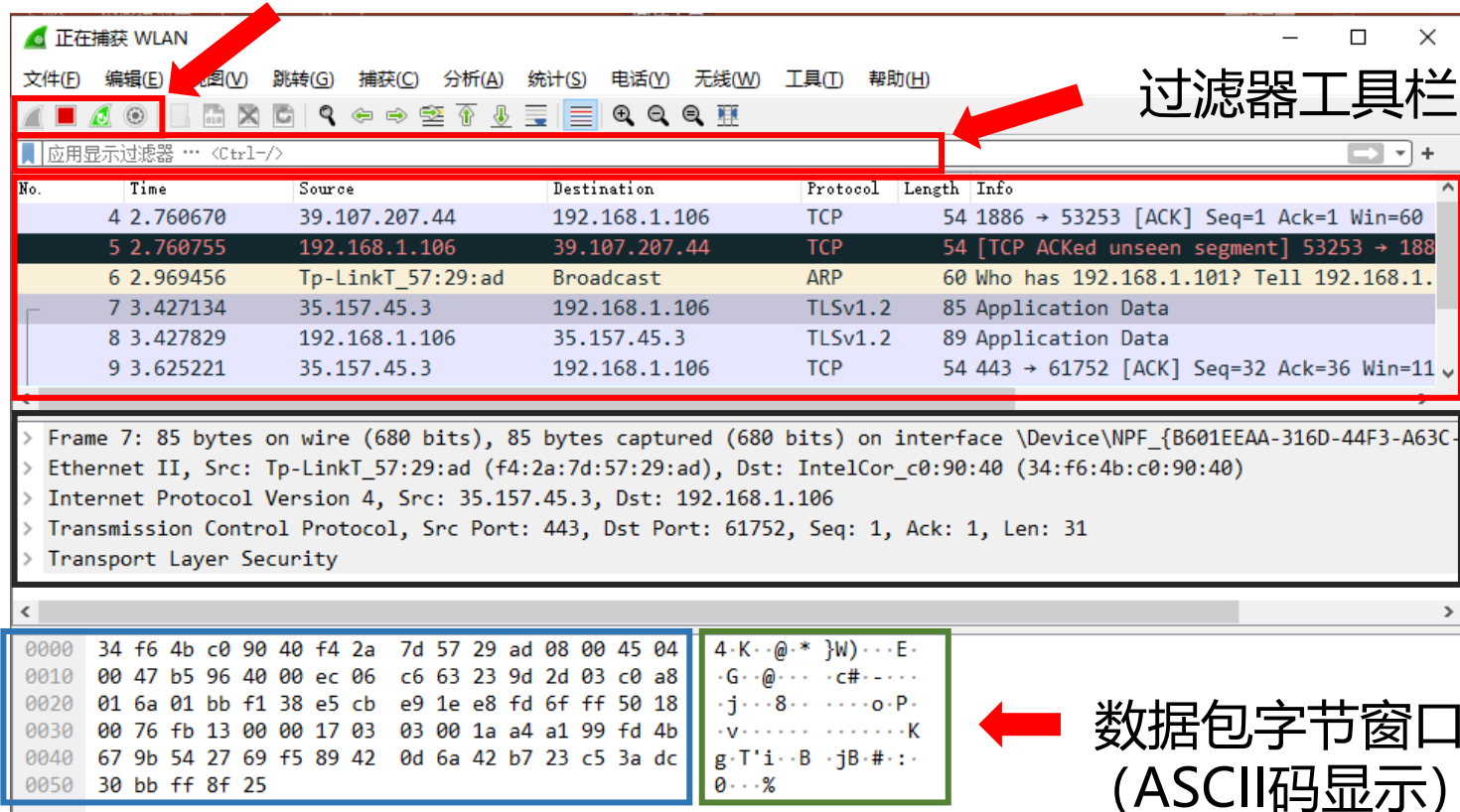
Wireshark首界面

启动Wireshark软件，在Wireshark首界面双击接口名称之后进入抓包界面。



Wireshark抓包界面

 开始捕获;  停止捕获;  重新开始当前捕获;  捕获选项。



The screenshot shows the Wireshark interface with several red arrows pointing to specific components:

- 过滤器工具栏 (Filter Toolbar):** Points to the toolbar at the top, specifically the capture control buttons (Start, Stop, Resume, Options).
- 数据包列表窗口 (Packet List Window):** Points to the table of captured packets.
- 数据包细节窗口 (Packet Details Window):** Points to the pane showing the hierarchical structure of the selected packet (Frame 7).
- 数据包字节窗口 (十六进制显示) (Packet Bytes Window - Hex Display):** Points to the left pane of the bottom section showing the raw bytes in hexadecimal.
- 数据包字节窗口 (ASCII码显示) (Packet Bytes Window - ASCII Display):** Points to the right pane of the bottom section showing the corresponding ASCII text.

No.	Time	Source	Destination	Protocol	Length	Info
4	2.760670	39.107.207.44	192.168.1.106	TCP	54	1886 → 53253 [ACK] Seq=1 Ack=1 Win=60
5	2.760755	192.168.1.106	39.107.207.44	TCP	54	[TCP ACKed unseen segment] 53253 → 188
6	2.969456	Tp-LinkT_57:29:ad	Broadcast	ARP	60	Who has 192.168.1.101? Tell 192.168.1.
7	3.427134	35.157.45.3	192.168.1.106	TLSv1.2	85	Application Data
8	3.427829	192.168.1.106	35.157.45.3	TLSv1.2	89	Application Data
9	3.625221	35.157.45.3	192.168.1.106	TCP	54	443 → 61752 [ACK] Seq=32 Ack=36 Win=11

Frame 7: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{B601EEAA-316D-44F3-A63C-...}

Ethernet II, Src: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad), Dst: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)

Internet Protocol Version 4, Src: 35.157.45.3, Dst: 192.168.1.106

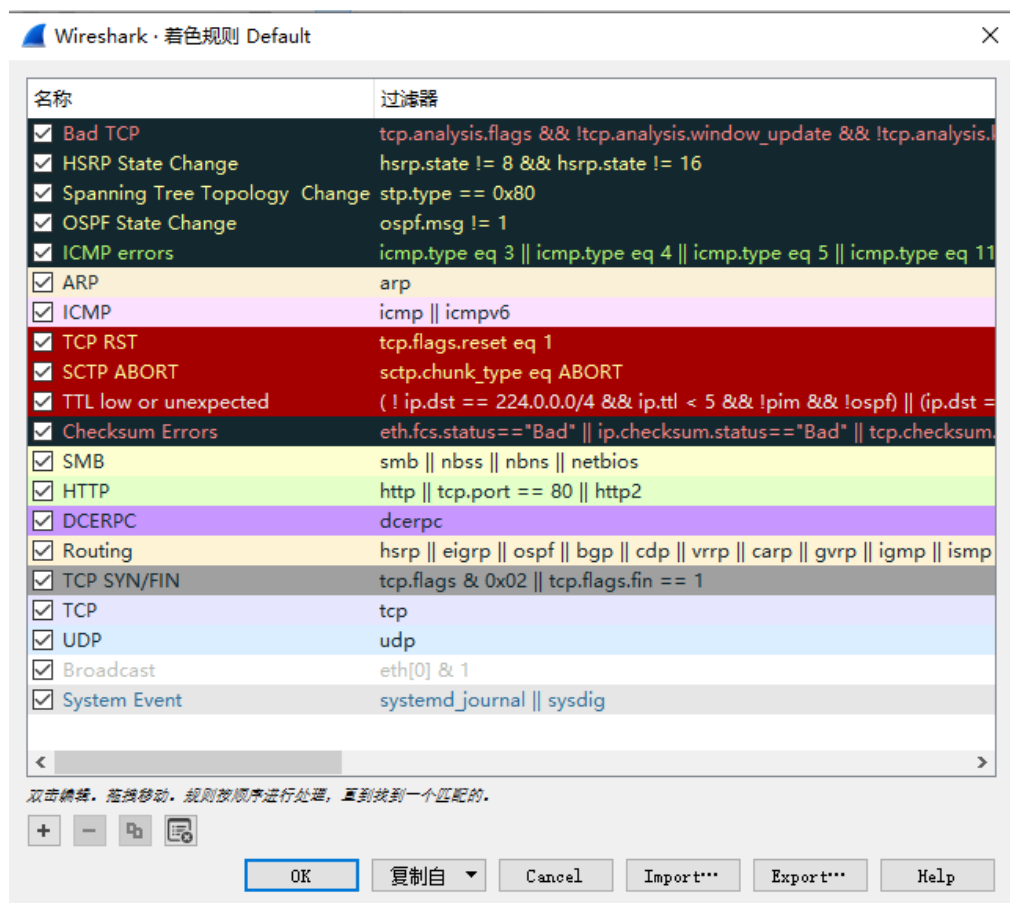
Transmission Control Protocol, Src Port: 443, Dst Port: 61752, Seq: 1, Ack: 1, Len: 31

Transport Layer Security

Offset	Hex	ASCII
0000	34 f6 4b c0 90 40 f4 2a 7d 57 29 ad 08 00 45 04	4-K..@.* }W)...E.
0010	00 47 b5 96 40 00 ec 06 c6 63 23 9d 2d 03 c0 a8	.G..@... .c#-....
0020	01 6a 01 bb f1 38 e5 cb e9 1e e8 fd 6f ff 50 18	.j...8... ..o.P.
0030	00 76 fb 13 00 00 17 03 03 00 1a a4 a1 99 fd 4b	.v..... ..K
0040	67 9b 54 27 69 f5 89 42 0d 6a 42 b7 23 c5 3a dc	g.T'i..B .jB.#..
0050	30 bb ff 8f 25	0...%

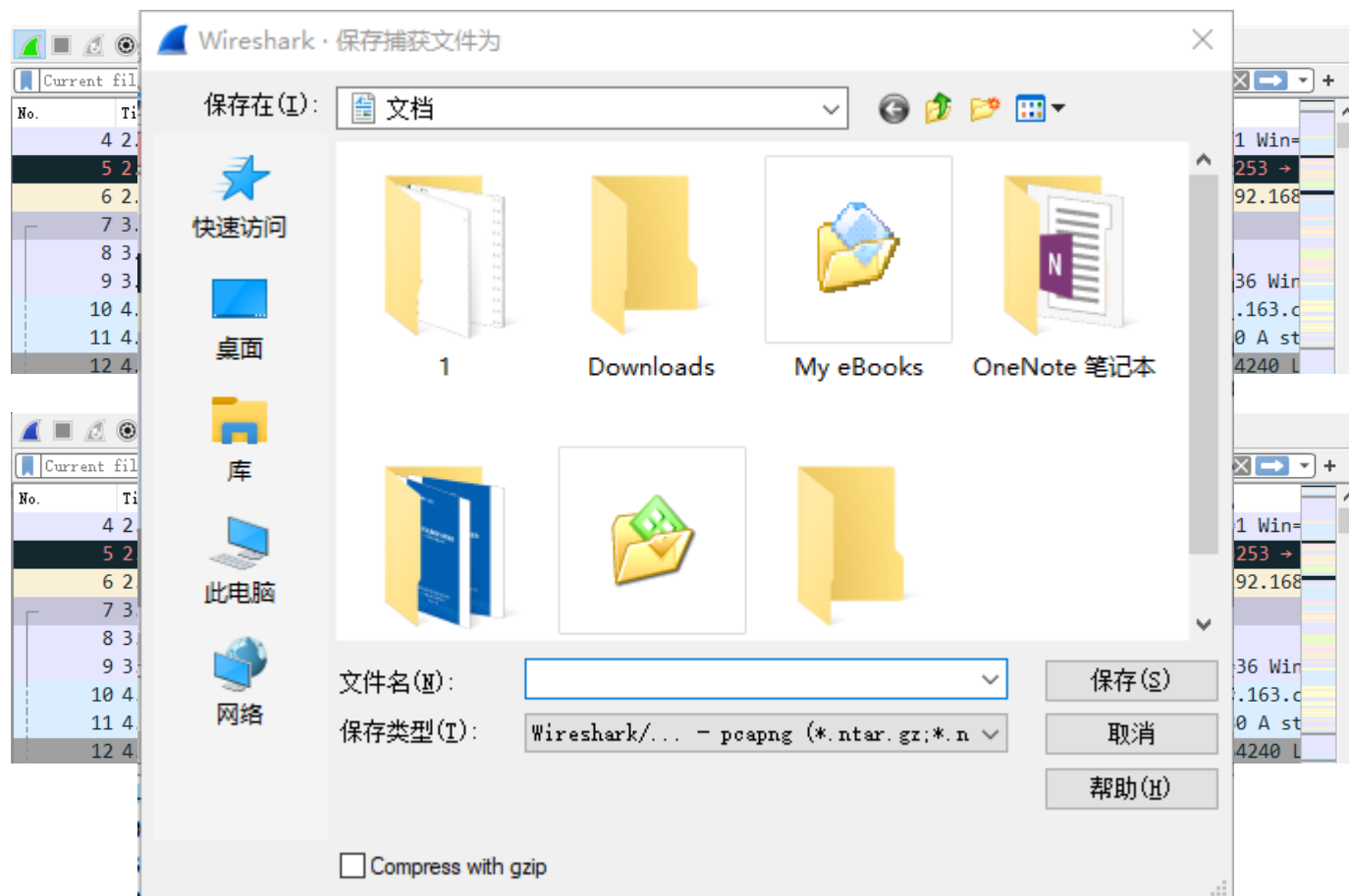
Wireshark抓包界面

- Wireshark使用不同颜色来区分不同类型的数据包。
- 可通过“视图” -> “着色规则” 进行查看和编辑。



Wireshark抓包结果保存

Wireshark的抓包结果可以保存为.pcapng、.pcap等格式的文件，便于离线分析。



Wireshark基础过滤表达式讲解

常用关键字：“eq” 和 “==” 等同，可以使用 “and” 或 “&&” 表示并且，“or” 或 “||” 表示或者。“!” 和 “not” 都表示取反。

1、针对IP地址的过滤

(1) 对源地址为192.168.0.1的包的过滤，即抓取源地址满足要求的包。表达式为：`ip.src == 192.168.0.1`

(2) 对目的地址为192.168.0.1的包的过滤，即抓取目的地址满足要求的包表达式为：`ip.dst == 192.168.0.1`

(3) 对源或者目的地址为192.168.0.1的包的过滤，即抓取满足源或者目的地址的ip地址是192.168.0.1的包。表达式为：`ip.addr == 192.168.0.1,或者 ip.src == 192.168.0.1 or ip.dst == 192.168.0.1`

(4) 要排除以上的数据包，使用 “!” 即可。表达式为：`!(表达式)`

Wireshark基础过滤表达式讲解

2、针对协议的过滤

(1) 仅仅需要捕获某种协议的数据包，表达式很简单仅仅需要把协议的名字输入即可。表达式为：`http`

(2) 需要捕获多种协议的数据包，也只需对协议进行逻辑组合即可。表达式为：`http or telnet`（多种协议加上逻辑符号的组合即可）

(3) 排除某种协议的数据包 表达式为：`not arp !tcp`

3、针对端口的过滤（视协议而定）

(1) 捕获某一端口的数据包表达式为：`tcp.port == 80`

(2) 捕获多端口的数据包，可以使用`and`来连接，下面是捕获高端口的表达式为：`udp.port >= 2048`

Wireshark基础过滤表达式讲解

4、针对长度和内容的过滤

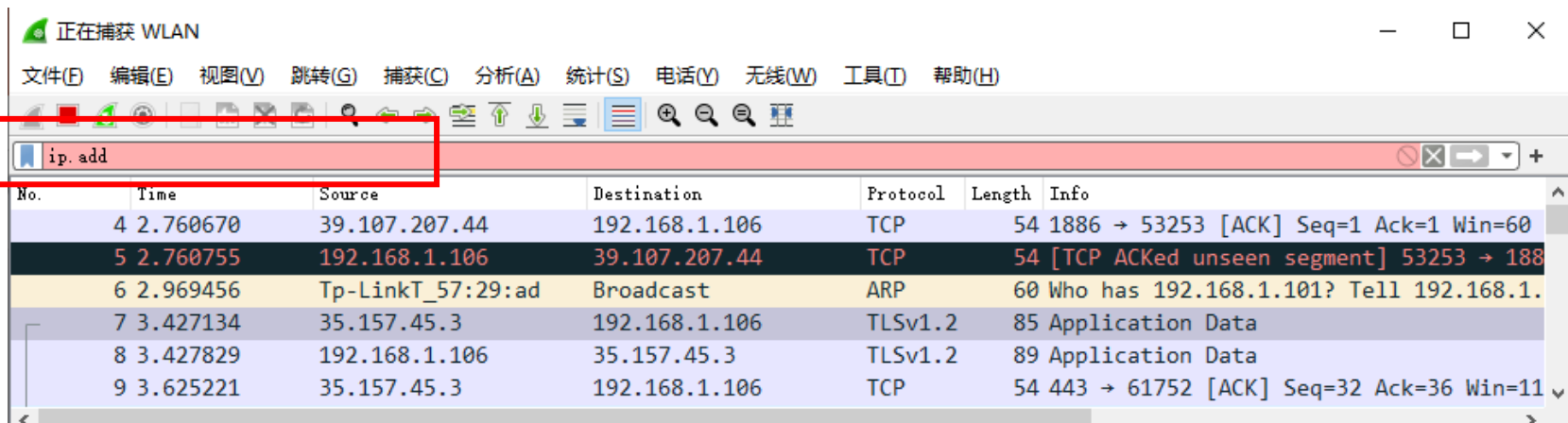
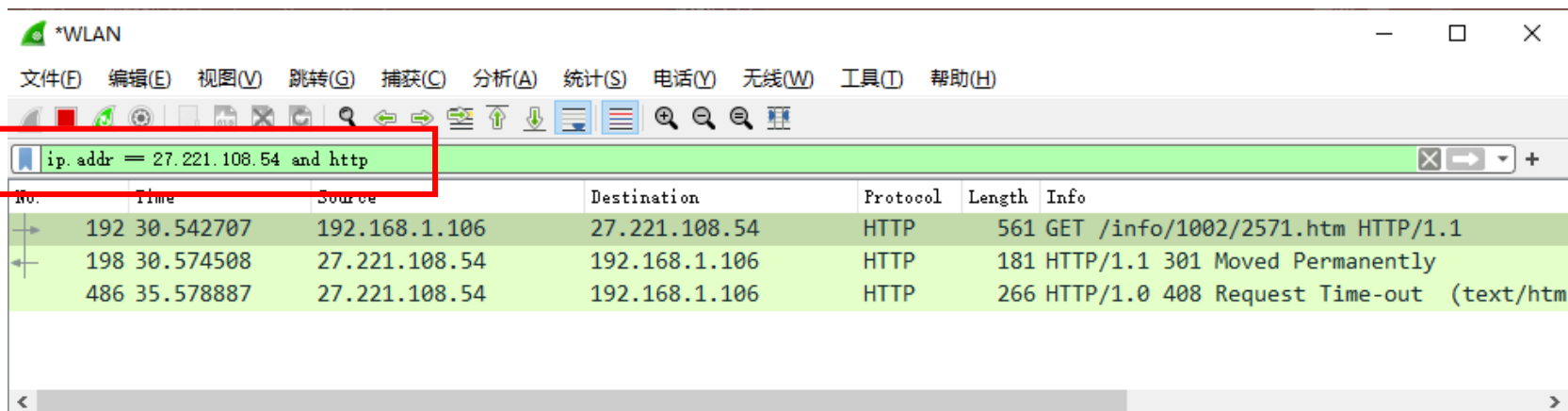
(1) 针对长度的过滤（这里的长度指定的是数据段的长度）

表达式为： `udp.length < 30` `http.content_length <= 20`

(2) 针对数据包内容的过滤

表达式为： `http.request.uri matches "vipscu"` （匹配http请求中含有vipscu字段的请求信息）

Wireshark基础过滤表达式讲解



主要内容

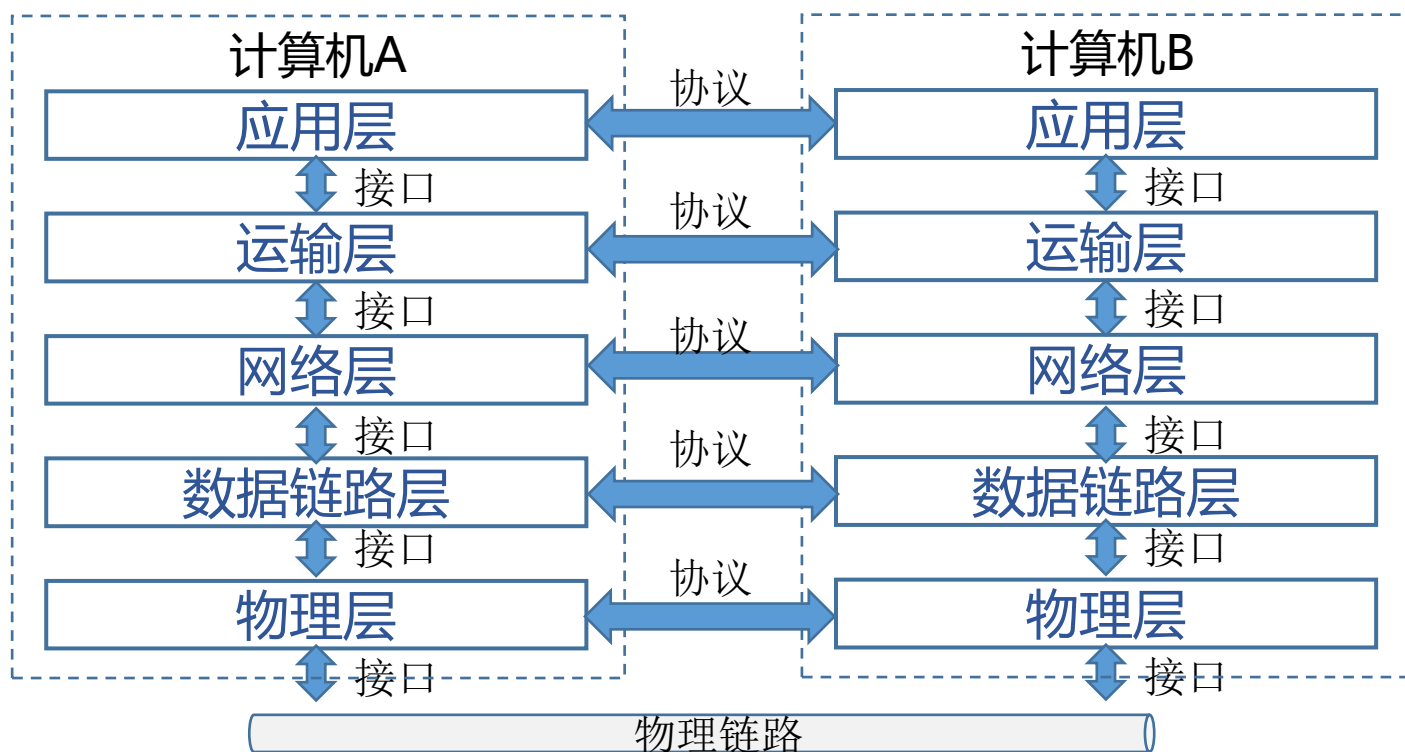
- 一、课程简介
- 二、Wireshark的安装和使用
- 三、计算机网络协议层实验

计算机网络协议

- **协议**就是计算机与计算机之间通过网络实现通信时，事先达成的一种“约定”。
- 通信协议中，通常会规定**报文首部**应该写入哪些信息、应该如何处理这些信息。相互通信的每一台计算机则根据协议，**构造**报文首部、**读取**首部内容等。
- 不同厂商的设备、不同的CPU以及不同的操作系统组成的计算机之间，只要**遵循相同的协议**就能够实现通信。

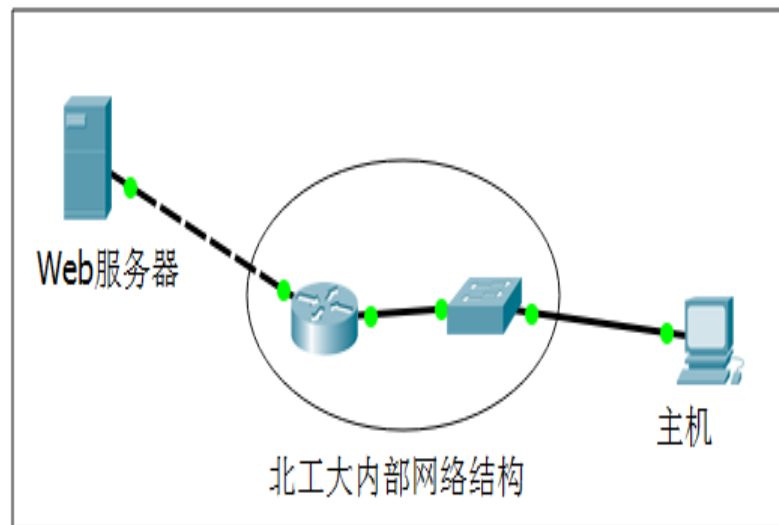
计算机网络协议

- 协议**分层模型**中，每个分层接收由它下一层所提供的特定服务，并负责向上一层提供特定服务。
- 上下层之间进行交互时所遵循的约定叫做**接口**，同一层之间交互时所遵循的约定叫做**协议**。



实验原理

- 本次实验主要是观察计算机网络协议层次。
- 实验步骤里需要访问北工大的官网地址，因此是主机和内网的Web服务器交互数据包。
- 在此过程中，使用Wireshark抓取主机与Web服务器相互通信发送的数据包。



北工大内网示意图

实验环境搭建

列出本次实验所使用的平台和相关软件，以下为例：

(打开cmd指令窗口，输入指令 “ipconfig /all”查看)

- 1、主机：联想笔记本（Win10系统）；主机IP地址：192.168.1.106；子网掩码：255.255.255.0；主机网卡MAC地址：34-F6-4B-C0-90-40。
- 2、网络连接方式：无线连接；默认网关地址：192.168.1.1。
- 3、抓包工具：Wireshark（v3.6.2）。

实验具体步骤

通过ping命令获取Web服务器的IP地址，例如：

```
C:\Users\zwt717>ping www.bjut.edu.cn
```

```
正在 Ping bjut-edu-cn.cname.saaswaf.com [122.9.167.87] 具有 32 字节的数据:
```

```
来自 122.9.167.87 的回复: 字节=32 时间=39ms TTL=39
```

```
来自 122.9.167.87 的回复: 字节=32 时间=40ms TTL=39
```

```
来自 122.9.167.87 的回复: 字节=32 时间=40ms TTL=39
```

```
来自 122.9.167.87 的回复: 字节=32 时间=41ms TTL=39
```

```
122.9.167.87 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 = 39ms, 最长 = 41ms, 平均 = 40ms
```


实验具体步骤

- 1、通过ping命令获取北京工业大学官网的IP地址27.221.108.54。

```
C:\Users\zwt717>ping www.bjut.edu.cn

正在 Ping bjut-edu-cn.cname.saaswaf.com [27.221.108.54] 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

27.221.108.54 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

实验具体步骤

思考题：分别在校园网和家庭网络中获取北京工业大学官网的IP地址，观察到所获取的IP地址不一致，分析导致这种情况发生可能存在的原因。

校园网内：172.21.94.14

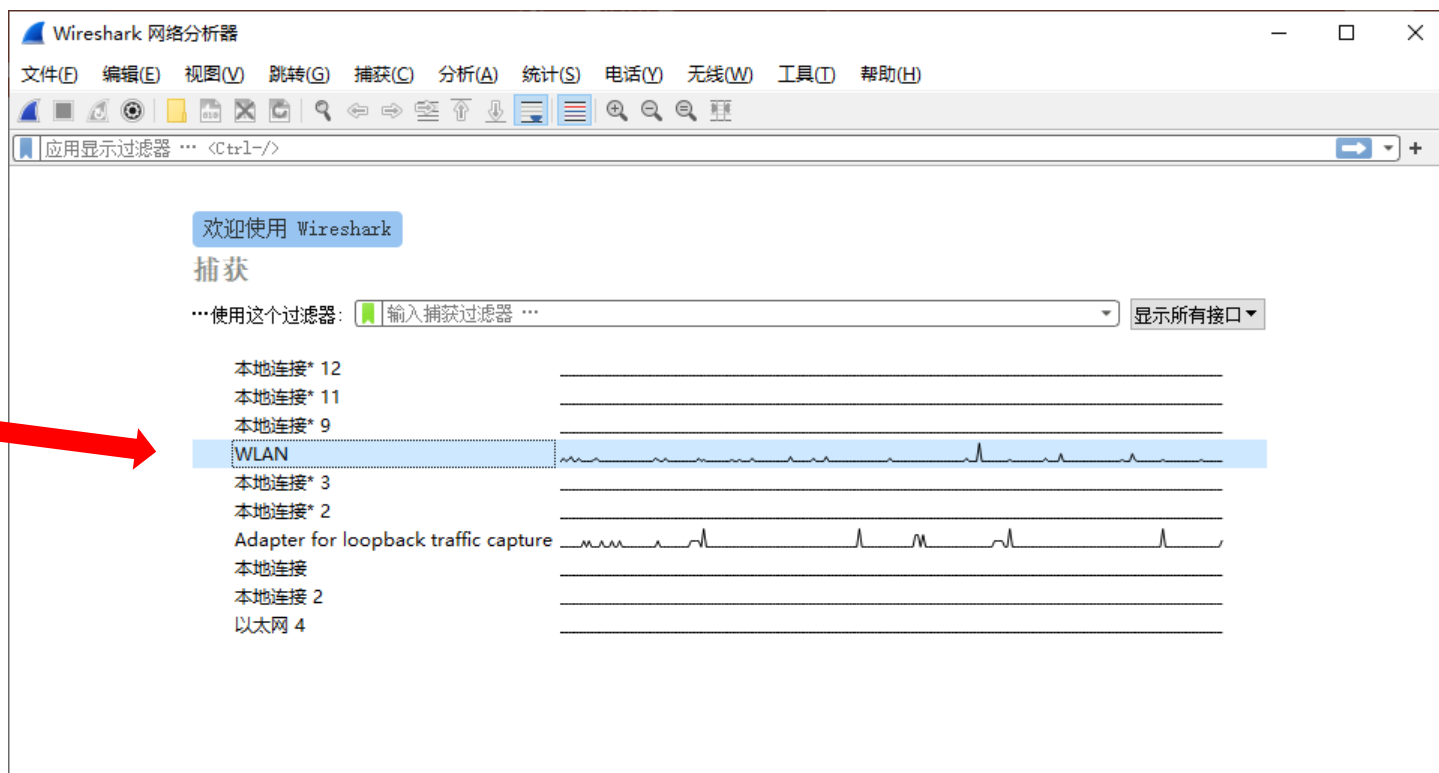
```
C:\Users\zwt>ping www.bjut.edu.cn  
正在 Ping lboutserver.bjut.edu.cn [172.21.94.14] 具有 32 字节的数据：  
请求超时。  
请求超时。
```

家庭网络：27.221.108.54

```
C:\Users\zwt717>ping www.bjut.edu.cn  
正在 Ping bjut-edu-cn.cname.saaswaf.com [27.221.108.54] 具有 32 字节的数据：  
请求超时。  
请求超时。
```

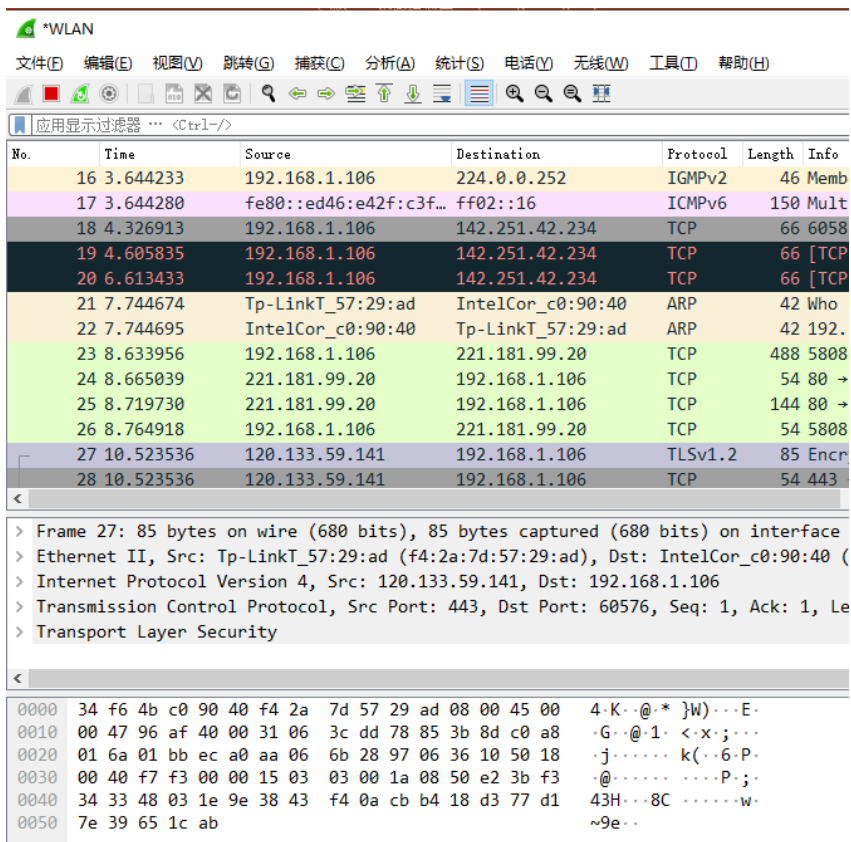
实验具体步骤

2、打开Wireshark软件，然后在首界面当中看到的是主机能够进行选择的网络接口。双击本次实验正在使用的网络接口，开始进行抓包。



实验具体步骤

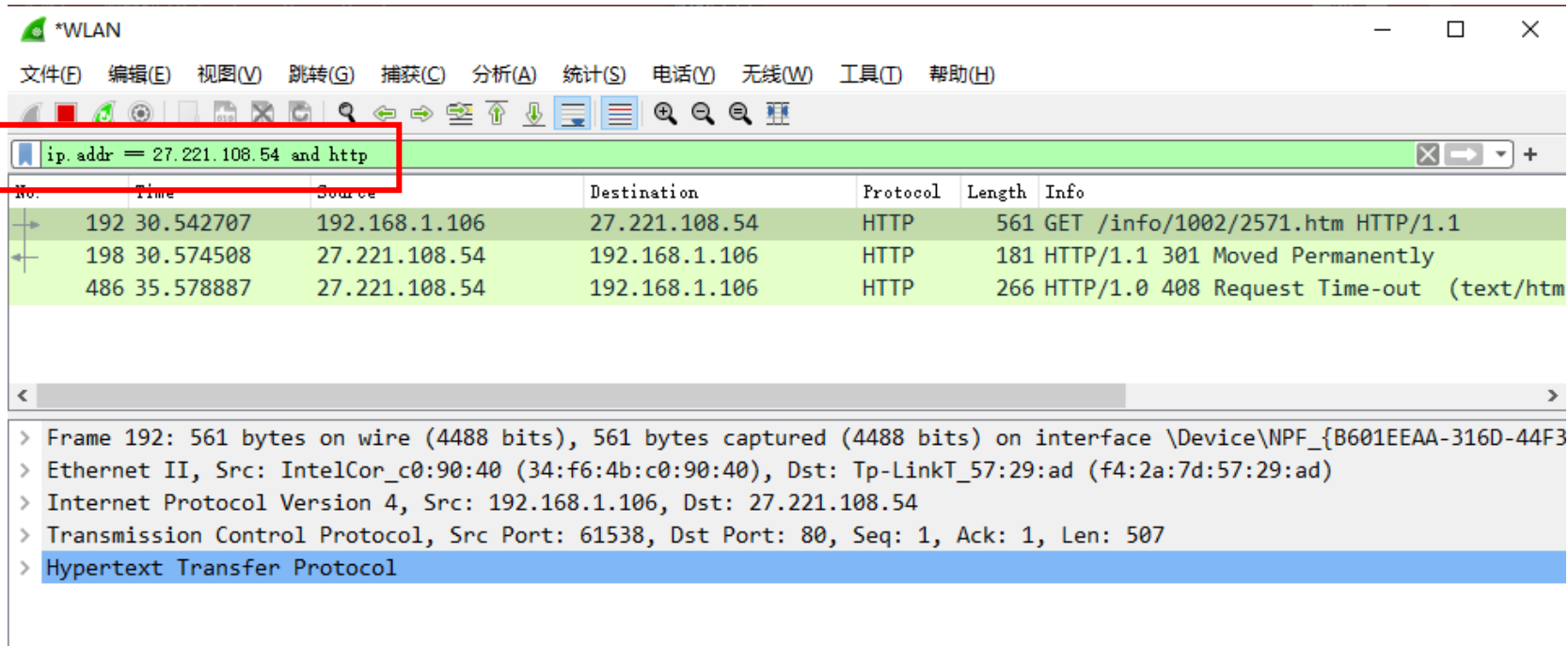
3、然后打开浏览器，在网页地址栏中输入网址，例如对北京工业大学官网进行访问，浏览校园新闻。



实验具体步骤

4、由于在对北工大官网进行访问的同时，在主机上也同时进行着其他的进程，并且这些进程有可能会进行网络通信并产生网络数据包。因此，在抓包结束后可以用显示过滤器对分组进行过滤。

过滤表达式如下：ip.addr == 27.221.108.54 and http



The image shows a Wireshark network traffic capture window titled '*WLAN'. The filter bar at the top contains the expression 'ip.addr == 27.221.108.54 and http', which is highlighted with a red box and a red arrow. Below the filter bar, a table of captured packets is displayed. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. Three packets are visible, all from 27.221.108.54 to 192.168.1.106. The first packet (No. 192) is an HTTP GET request for '/info/1002/2571.htm'. The second (No. 198) is an HTTP 301 Moved Permanently response. The third (No. 486) is an HTTP 408 Request Time-out response. The bottom pane shows the details of the selected packet (No. 192), including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
192	30.542707	192.168.1.106	27.221.108.54	HTTP	561	GET /info/1002/2571.htm HTTP/1.1
198	30.574508	27.221.108.54	192.168.1.106	HTTP	181	HTTP/1.1 301 Moved Permanently
486	35.578887	27.221.108.54	192.168.1.106	HTTP	266	HTTP/1.0 408 Request Time-out (text/html)

> Frame 192: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface \Device\NPF_{B601EEAA-316D-44F3...}

> Ethernet II, Src: IntelCor_c0:90:40 (34:f6:4b:c0:90:40), Dst: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)

> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 27.221.108.54

> Transmission Control Protocol, Src Port: 61538, Dst Port: 80, Seq: 1, Ack: 1, Len: 507

> Hypertext Transfer Protocol

实验具体步骤

5、抓包结束后在第一个窗口上点击任意一行，在第二个窗口处会显示报文的每一层的详细信息，随后对网络协议层进行分析。实例如下：

The image shows the Wireshark network traffic analysis interface. The top menu bar includes File (F), Edit (E), View (V), Jump (G), Capture (C), Analyze (A), Statistics (S), Phone (Y), Wireless (W), Tools (T), and Help (H). The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane shows three captured packets, with the first packet selected. The packet details pane shows the layers of the selected packet, with the Hypertext Transfer Protocol layer highlighted. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
192	30.542707	192.168.1.106	27.221.108.54	HTTP	561	GET /info/1002/2571.htm HTTP/1.1
198	30.574508	27.221.108.54	192.168.1.106	HTTP	181	HTTP/1.1 301 Moved Permanently
486	35.578887	27.221.108.54	192.168.1.106	HTTP	266	HTTP/1.0 408 Request Time-out (text/html)

> Frame 192: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface \Device\NPF_{B601EEAA-316D-44F3-8000-000000000000}

> Ethernet II, Src: IntelCor_c0:90:40 (34:f6:4b:c0:90:40), Dst: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)

> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 27.221.108.54

> Transmission Control Protocol, Src Port: 61538, Dst Port: 80, Seq: 1, Ack: 1, Len: 507

> Hypertext Transfer Protocol

0000 f4 2a 7d 57 29 ad 34 f6 4b c0 90 40 08 00 45 00 .*}W).4. K..@..E.
0010 02 23 8f a3 40 00 40 06 5f 0c c0 a8 01 6a 1b dd .#..@.@. _...j..
0020 6c 36 f0 62 00 50 8b 4e ab 79 ff ff 33 4c 50 18 16.b.P.N .y..3LP.
0030 02 04 f7 b4 00 00 47 45 54 20 2f 69 6e 66 6f 2fGE T /info/
0040 31 30 30 32 2f 32 35 37 31 2e 68 74 6d 20 48 54 1002/257 1.htm HT

实验结果与分析

实验结果：

No.	Time	Source	Destination	Protocol	Length	Info
192	30.542707	192.168.1.106	27.221.108.54	HTTP	561	GET /info/1002/2571.htm HTTP/1.1

> Frame 192: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface \Device\NPF_{B601EEAA-316D-44F3}
> Ethernet II, Src: IntelCor_c0:90:40 (34:f6:4b:c0:90:40), Dst: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 27.221.108.54
> Transmission Control Protocol, Src Port: 61538, Dst Port: 80, Seq: 1, Ack: 1, Len: 507
> Hypertext Transfer Protocol

实验分析：

Frame：物理层传输的数据帧概况

Ethernet II：数据链路层帧头部信息，此处使用的是以太网协议

Internet Protocol Version4：互联网层包头部信息，此处是IPv4协议

Transmission Control Protocol：传输层段头部信息，此处是TCP协议

Hypertex Transfer Protocol：应用层信息，此处是HTTP协议

