

流量分析

万里

花名：万里

曾就职于奇安信集团，担任高级渗透测试工程师，从事网络安全工作7年，参与四届全国HW行动、北京冬奥重保等活动，担任CISP-PTE、CISP-IRE出题及监考，为CNCERT、SRC平台等提交数百漏洞。专注研究前沿网络安全技术，具有丰富的实战经验。擅长技术：Web渗透、内网渗透、代码审计、Kali、安全工具开发等。



中华人民共和国网络安全法

第二十七条

任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

课程内容仅用于以防御为目的的教学演示
请勿用于其他用途，否则后果自负

1、《中华人民共和国刑法》的相关规定：

第二百八十五条规定，非法侵入计算机信息系统罪;非法获取计算机信息系统数据、非法控制计算机信息系统罪;提供侵入、非法控制计算机信息系统程序、工具罪是指，违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金;情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

第一条

非法获取计算机信息系统数据或者非法控制计算机信息系统，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节严重”：

- (一) 获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；
- (二) 获取第（一）项以外的身份认证信息五百组以上的；
- (三) 非法控制计算机信息系统二十台以上的；
- (四) 违法所得五千元以上或者造成经济损失一万元以上的；
- (五) 其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节特别严重”：

- (一) 数量或者数额达到前款第（一）项至第（四）项规定标准五倍以上的；
- (二) 其他情节特别严重的情形。

明知是他人非法控制的计算机信息系统，而对该计算机信息系统的控制权加以利用的，依照前两款的规定定罪处罚。

目录

1. Wireshark介绍
2. Wireshark安装
3. Wireshark界面介绍
4. Wireshark导航栏
5. Wireshark菜单栏
6. Wireshark过滤方式

Wireshark介绍

Wireshark (前称Ethereal) 是一个网络封包分析软件。网络封包分析软件的功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换。

支持的协议: Wireshark 在支持协议的数量方面出类拔萃，截至目前已提供了超过850种协议的支持。这些协议包括从最基础的IP协议协议和DHCP协议到高级的专用协议比如 AppleTalk 和BitTorrent等。由于Wireshark 在开源模式下进行开发，每次更新都会增加些对新协议的支持。

About Wireshark

[About](#)[Awards and Accolades](#)[Authors](#)[SharkFest](#)[SharkFest Sponsors](#)

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.

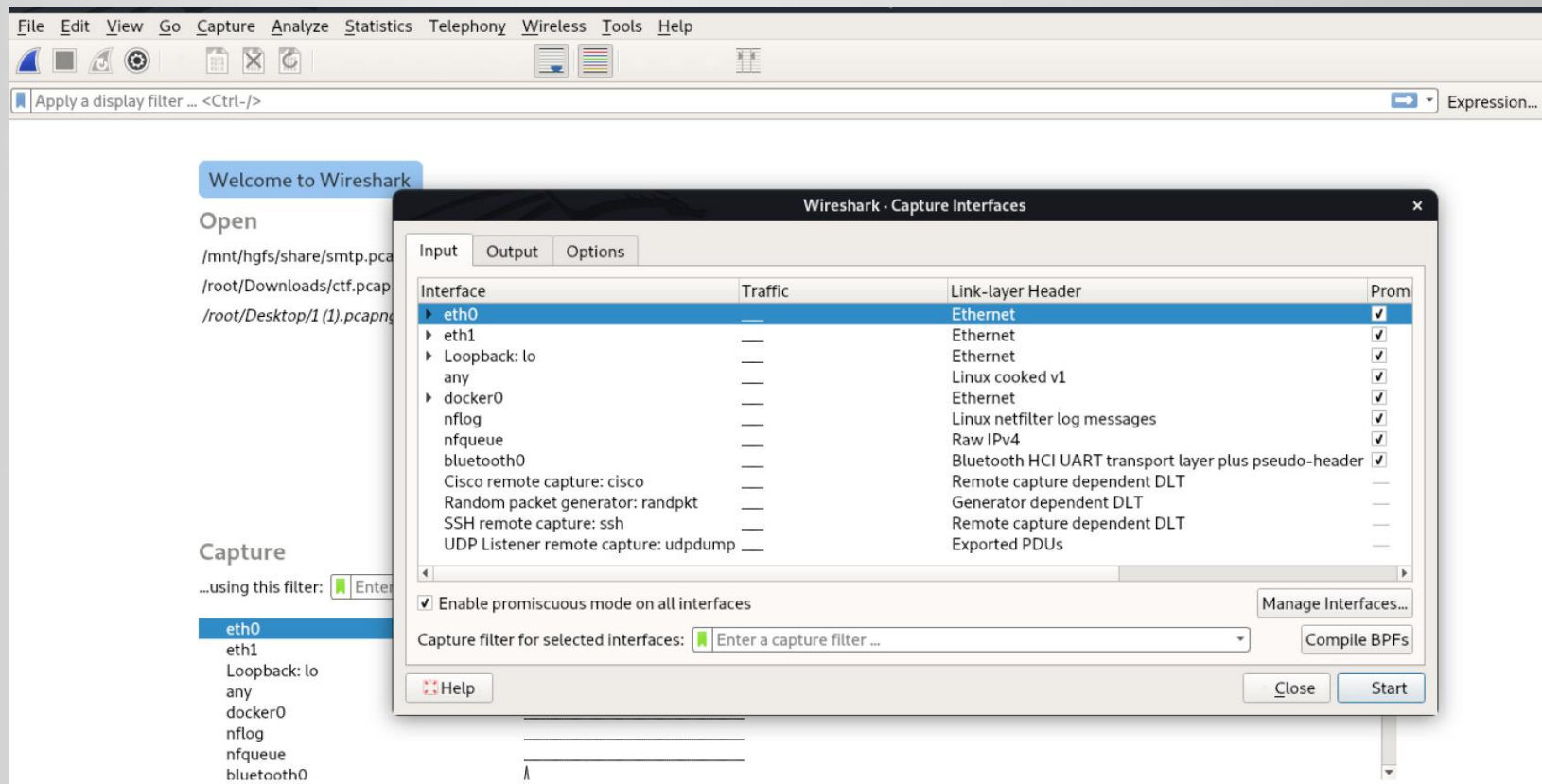
Wireshark has a rich feature set which includes the following:

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- The most powerful display filters in the industry
- Rich VoIP analysis
- Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, and many others
- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript®, CSV, or plain text

Wireshark介绍

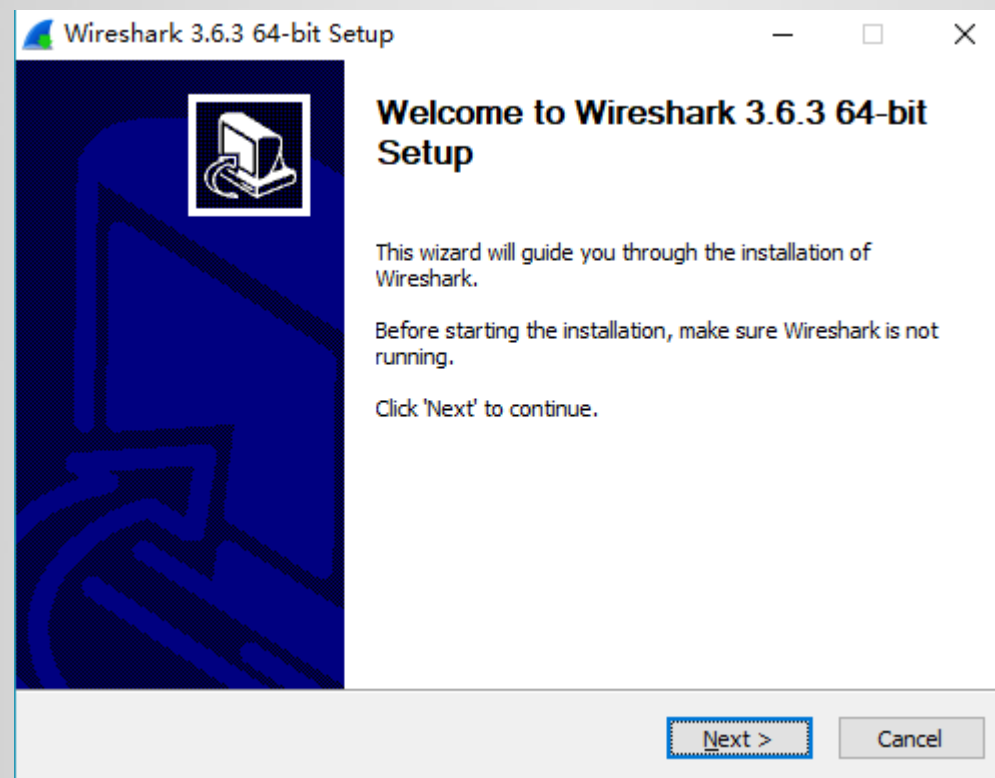
Wireshark主要应用

- 1、实时抓取数据包并
进行分析（抓包模块）
- 2、对已获取的数据包
进行流量分析



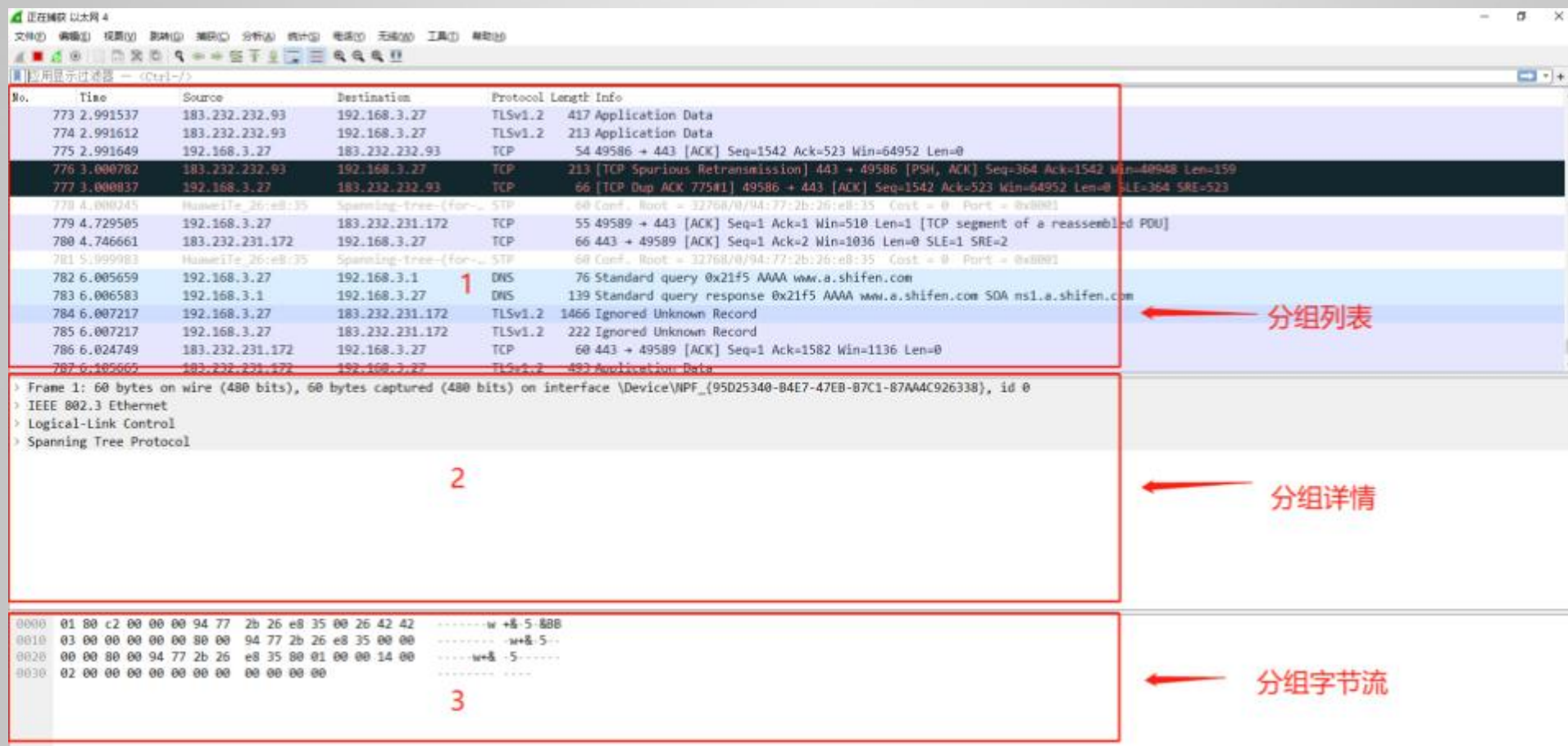
Wireshark安装

下载地址: <https://www.wireshark.org/>



Wireshark界面介绍

选择网口后进入主页面，可以看到流量包，在主页面可以看到3部分的流量数据，分别为【分组列表】【分组详情】【分组字节流】



The screenshot shows the Wireshark interface with three main sections highlighted by red boxes and numbered 1, 2, and 3. Red arrows point from the Chinese labels to these sections.

- 1 分组列表 (Packet List):** The top section showing a list of captured packets. It includes columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet is 777, a TCP segment from 192.168.3.27 to 183.232.232.93.
- 2 分组详情 (Packet Details):** The middle section showing the hierarchical structure of the selected packet. It includes fields like Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The selected packet is a TCP segment.
- 3 分组字节流 (Packet Bytes):** The bottom section showing the raw bytes of the selected packet in hexadecimal and ASCII format. The selected packet is a TCP segment.

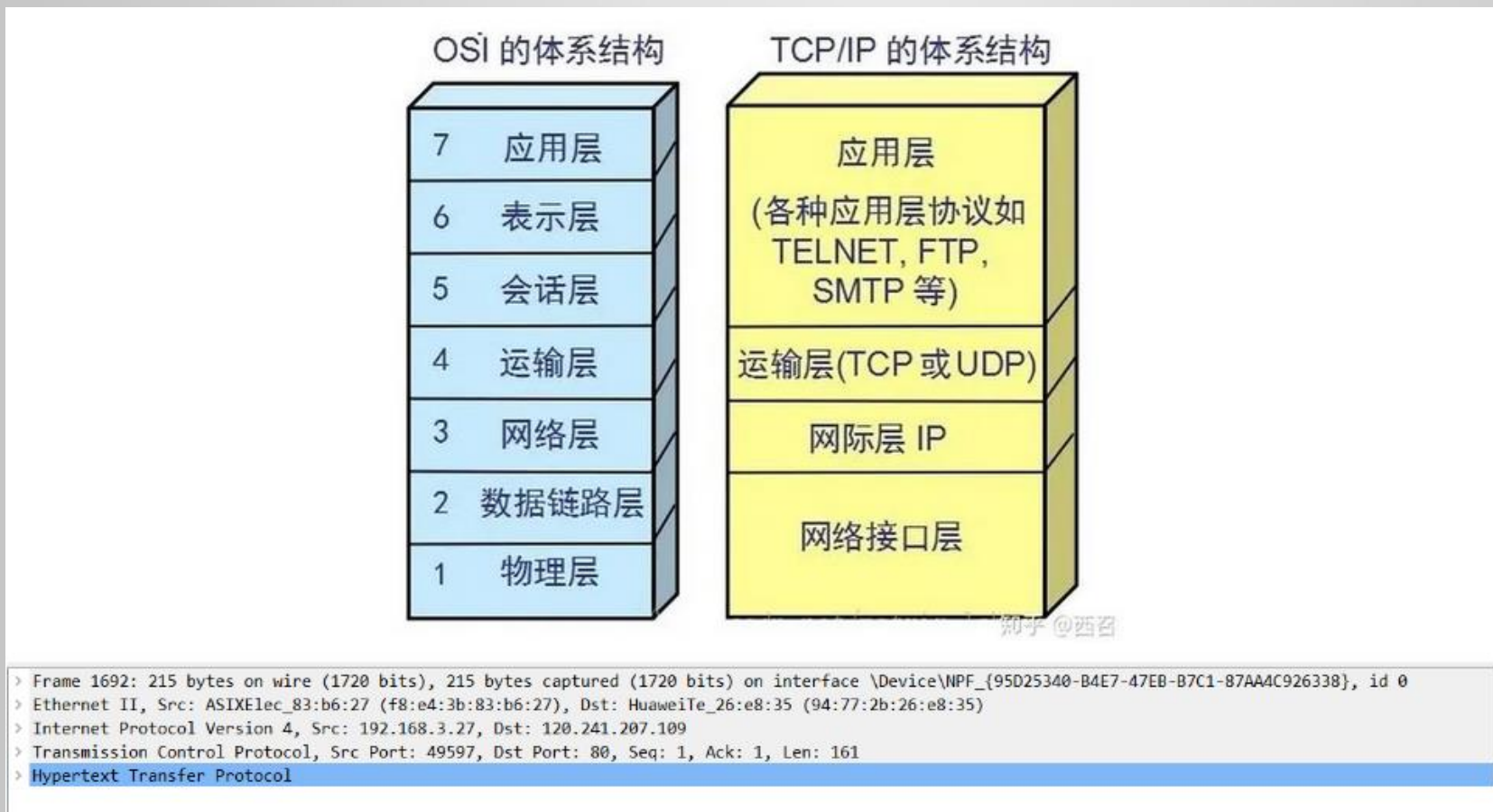
Wireshark界面介绍

分组列表：将流量以分组的形式，简单的呈现出来

No.	Time	Source	Destination	Protocol	Length	Info
985	40.385028	192.168.3.27	120.226.191.49	HTTP	453	GET /110/20403/stodownload?n=7ad2d4fa0031b66d9e09a693dc032b7a&filekey=3043020101042f302d02016e0402535a0420376164326434666130383331...
1000	40.398155	120.226.191.49	192.168.3.27	HTTP	64	HTTP/1.1 200 OK
1349	107.629819	192.168.3.27	120.196.204.37	HTTP	183	GET /wx_emoji/XlhxsCp3TPgogZ0hFe9MYuIbX6Uyeo0ibMQdHtEwJiaCeRIbdsTVLhryD5hMQkbl/ HTTP/1.1
1356	107.648324	120.196.204.37	192.168.3.27	HTTP	202	HTTP/1.1 200 OK (image/jpeg)
1384	114.481076	192.168.3.27	120.196.204.37	HTTP	182	GET /wx_emoji/74gRWCUTY3EH1eCicdA9x5V0P1nqkeEsicZ05JEGp2IDSQCChyeNuozvG6dUL8JINN7/ HTTP/1.1
1388	114.509561	120.196.204.37	192.168.3.27	HTTP	818	HTTP/1.1 200 OK (image/jpeg)
1501	132.468286	192.168.3.27	183.192.169.17	HTTP	863	POST /mntls/00005ea2 HTTP/1.1
1505	132.572104	183.192.169.17	192.168.3.27	HTTP	366	HTTP/1.1 200 OK
1692	189.551739	192.168.3.27	120.241.207.109	HTTP	215	GET /mmcrhead/lterJwKAvXBuPCxMyEoTGZM3FotKCicslNzmcY4Uhib7liabUFqCuIgd4eFtpcEqq7nfc5uL4AToTMPAYUITzrWvJjtyRCZQMs/0 HTTP/1.1
1703	189.577476	120.241.207.109	192.168.3.27	HTTP	532	HTTP/1.1 200 OK (JPEG JFIF image)
1711	189.639477	192.168.3.27	183.192.169.17	HTTP	766	POST /mntls/00005f5f HTTP/1.1
1719	189.696250	192.168.3.27	183.192.169.17	HTTP	784	POST /mntls/00005f5f HTTP/1.1
1723	189.723246	192.168.3.27	111.30.164.230	HTTP	925	POST /mntls/00005f5f HTTP/1.1
1724	189.759098	183.192.169.17	192.168.3.27	HTTP	512	HTTP/1.1 200 OK
1731	189.769700	111.30.164.230	192.168.3.27	HTTP	1096	HTTP/1.1 200 OK

Wireshark界面介绍

分组详情：将流量以TCP/IP 5层模式形式展现出来



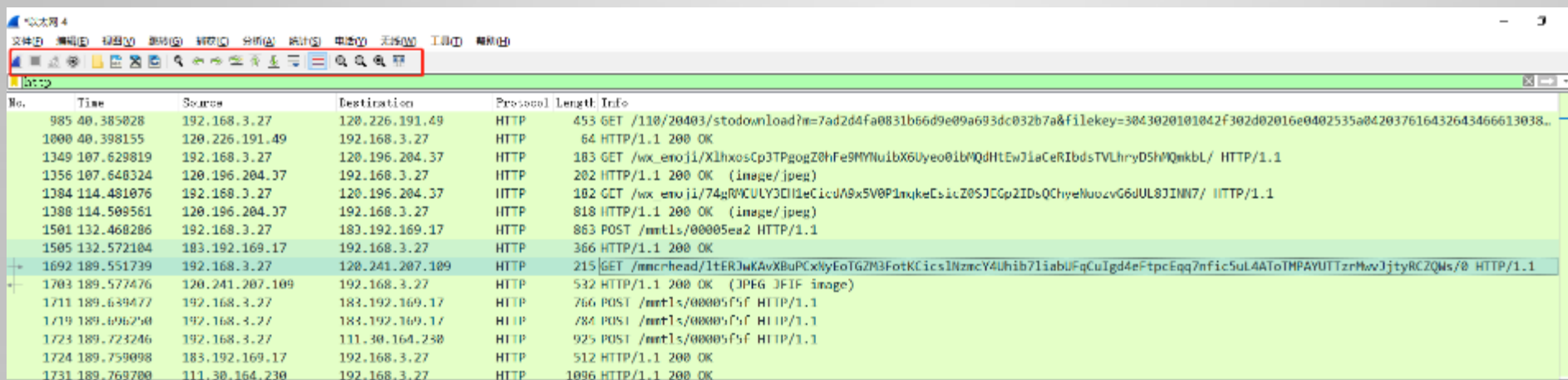
Wireshark界面介绍

分组字节流：将流量以字节流形式展现也就是16进制

0000	94 77 2b 26 e8 35 f8 e4 3b 83 b6 27 08 00 45 00	-w+&.5.. ;...'.E.
0010	00 c9 b8 9e 40 00 80 06 00 00 c0 a8 03 1b 78 f1@... ..x.
0020	cf 6d c1 bd 00 50 16 6e be 93 e2 59 a9 1a 50 18	-m...P.n ...Y..P.
0030	02 00 0c de 00 00 47 45 54 20 2f 6d 6d 63 72 68GE T /mmcrh
0040	65 61 64 2f 6c 74 45 52 4a 77 4b 41 76 58 42 75	ead/ltER JwKAvXBu
0050	50 43 78 4e 79 45 6f 54 47 5a 4d 33 46 6f 74 4b	PCxNyEoT GZM3FotK
0060	43 69 63 73 6c 4e 7a 6d 63 59 34 55 68 69 62 37	CicslNzm cY4Uhib7
0070	6c 69 61 62 55 46 71 43 75 49 67 64 34 65 46 74	liabUFqC uIgd4eFt
0080	70 63 45 71 71 37 6e 66 69 63 35 75 4c 34 41 54	pcEqq7nf ic5uL4AT
0090	6f 54 4d 50 41 59 55 54 54 7a 72 4d 77 76 4a 6a	oTMPAYUT TzrMwvJj
00a0	74 79 52 43 5a 51 57 73 2f 30 20 48 54 54 50 2f	tyRCZQWs /0 HTTP/
00b0	31 2e 31 0d 0a 48 6f 73 74 3a 20 77 78 2e 71 6c	1.1..Hos t: wx.q1
00c0	6f 67 6f 2e 63 6e 0d 0a 41 63 63 65 70 74 3a 20	ogo.cn.. Accept:
00d0	2a 2f 2a 0d 0a 0d 0a	*/*....

Wireshark导航

工具栏就是快捷工具栏的功能共 20个

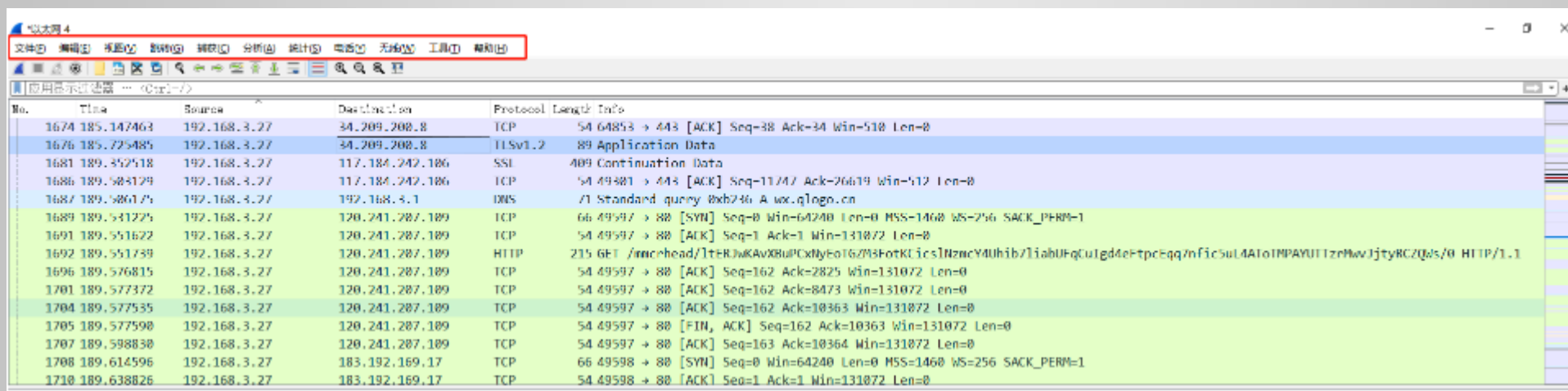


工具栏就是快捷工具栏的功能共 20个

- 1、开始捕获分组
- 2、停止捕获分组
- 3、重新开始当前捕获
- 4、捕获选项
- 5、打开以保存的捕获文件
- 6、保存捕获文件
- 7、关闭捕获文件
- 8、重新加载捕获文件
- 9、查找一个分组
- 10、转到前一分组
- 11、转到下一分组
- 12、转到特定分组
- 13、转到首个分组
- 14、转到最新分组
- 15、在实时捕获分组时，自动滚动屏幕到最新分组
- 16、使用您的着色规则来绘制分组
- 17、放大住窗口文本
- 18、收缩住窗口文本
- 19、窗口文本返回正常大小
- 20、调整分组列表已适应内容

Wireshark菜单栏

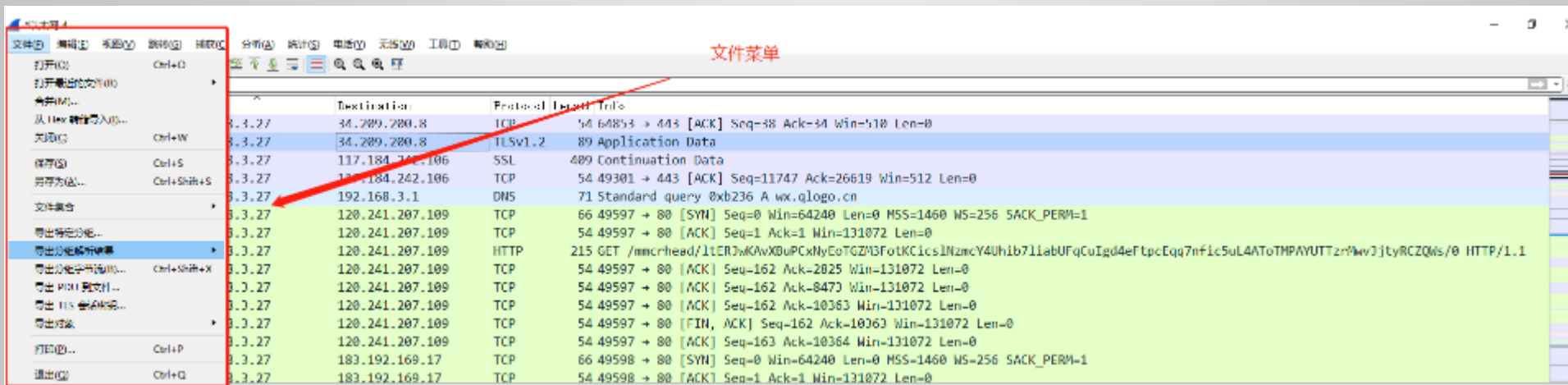
菜单栏放着常用的功能，我这里依次介绍



Wireshark菜单栏

【文件】菜单栏

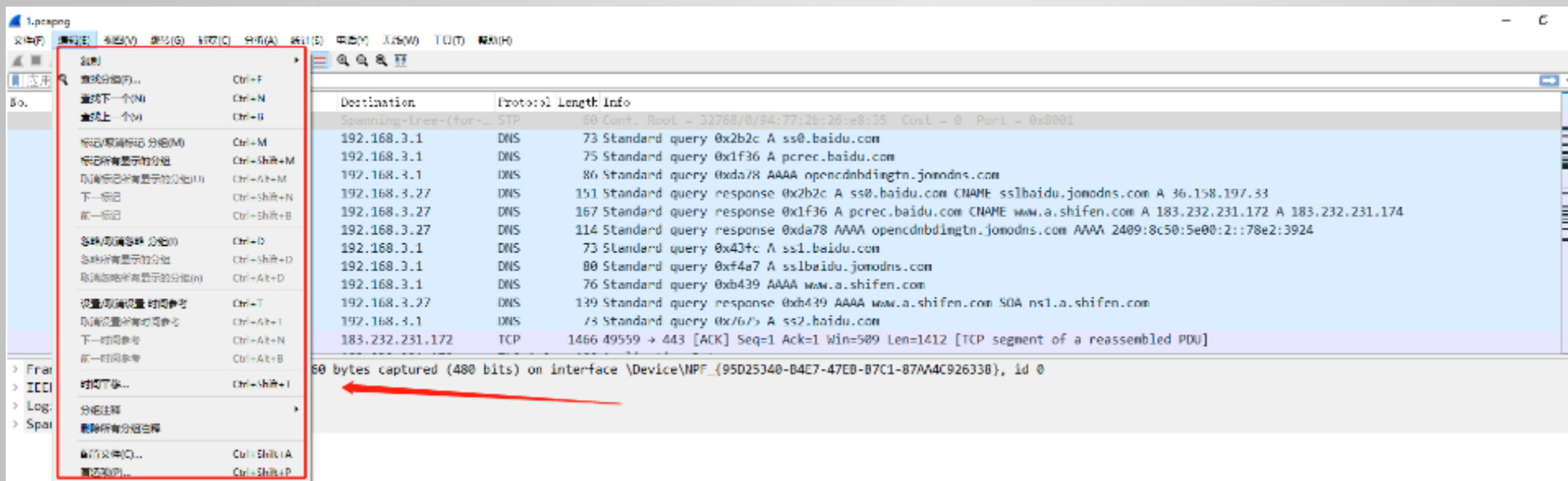
文件菜单里面包含了【打开】【打开最近】【合并】【16进制导入】【关闭】【保存】【另存为】【文件集合】【导出特定分组】【导出分组解析结果】【导出分组字节流】【导出PDU到文件】【导出TLS会话密钥】【导出到对象】【打印】【退出】等



Wireshark菜单栏

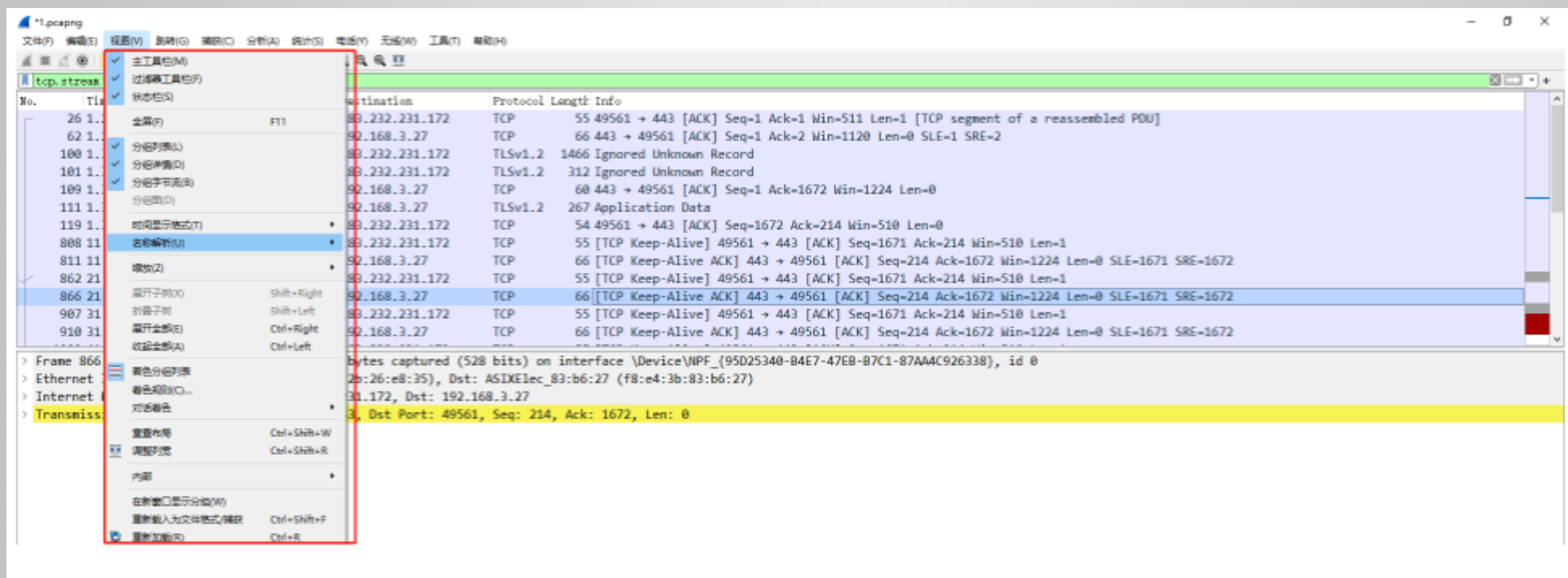
【编辑】菜单栏

包含了【复制】【查找分组】【查找下一个】【查找上一个】【标记分组】【分组注释】【配置文件】【首选项】



Wireshark菜单栏

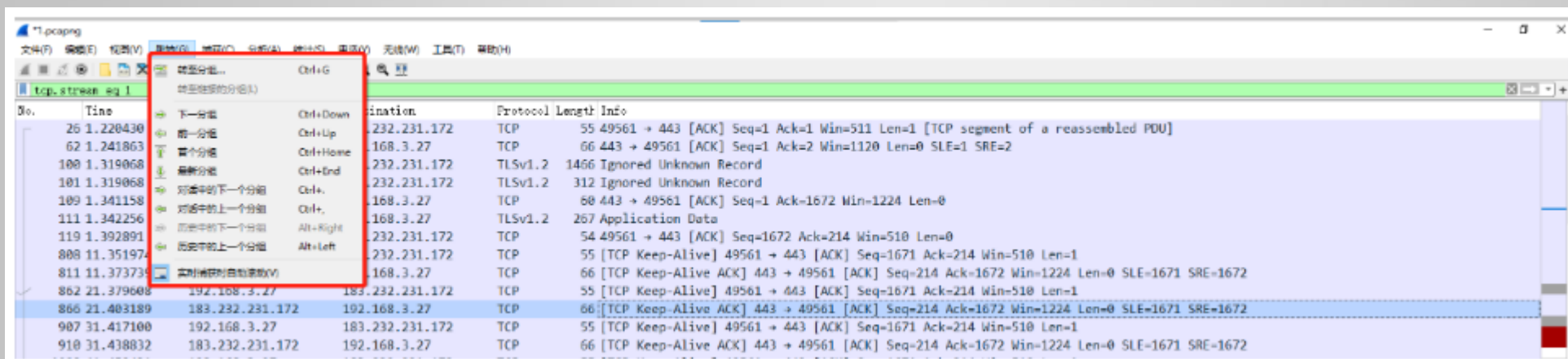
【视图】菜单栏



Wireshark菜单栏

【跳转】菜单栏

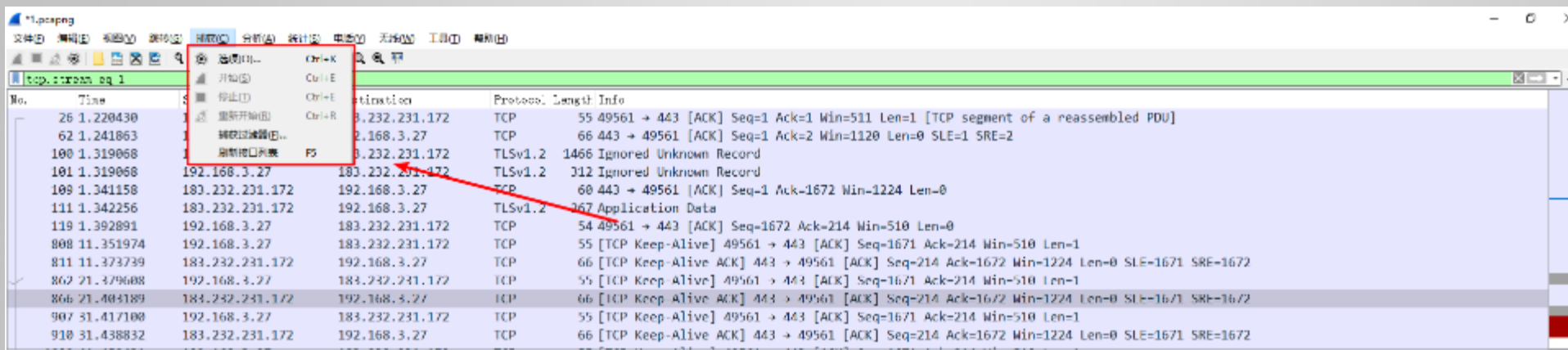
跳转菜单栏主要包括的对分组的跳转，实际就和我们的鼠标滚轮一样



Wireshark菜单栏

【捕获】菜单栏

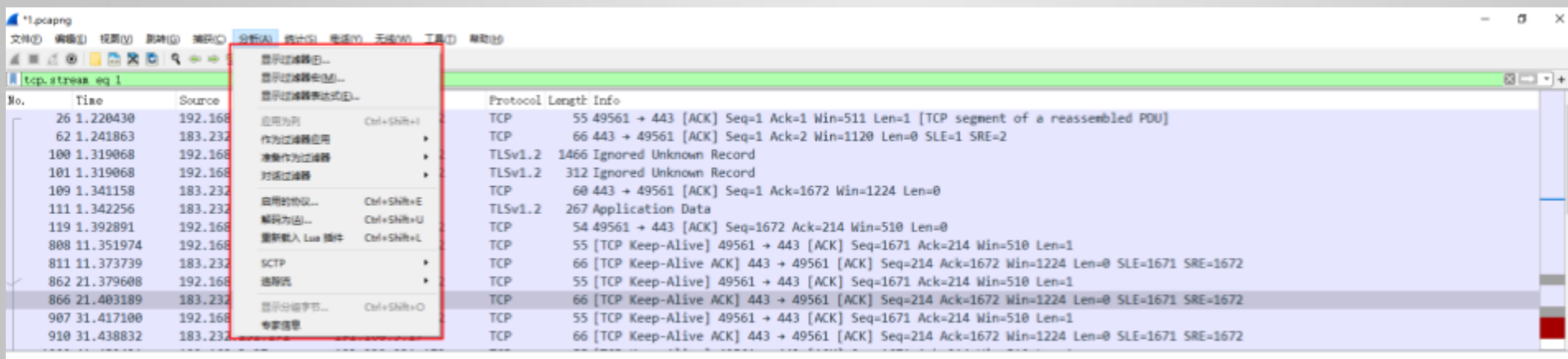
捕获菜单栏主要可以选择对网口的捕获



Wireshark菜单栏

【分析】菜单栏

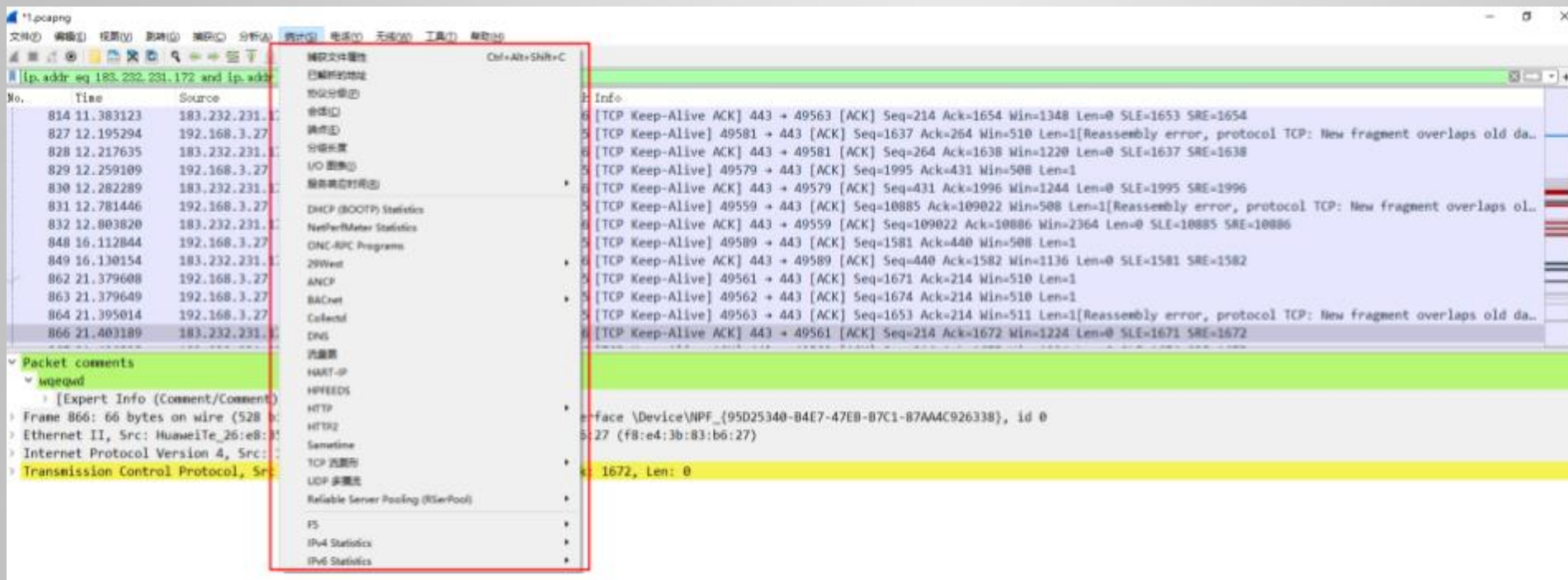
这里的功能主要是分析功能，作用比较大



Wireshark菜单栏

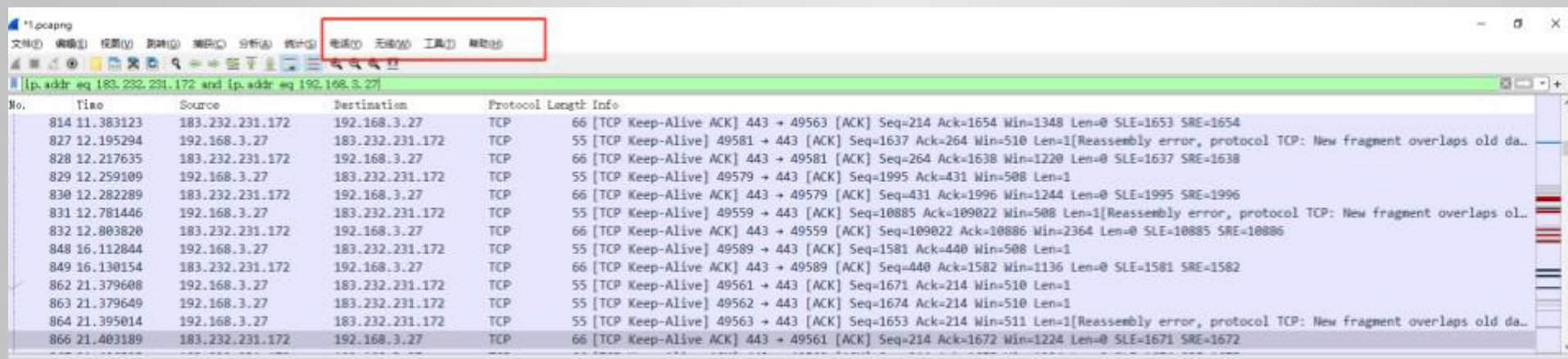
【统计】菜单栏

统计菜单栏也是经常用的【协议分级】和【会话】使用最多



Wireshark菜单栏

【其他】菜单栏



Wireshark菜单栏

【分析】菜单栏

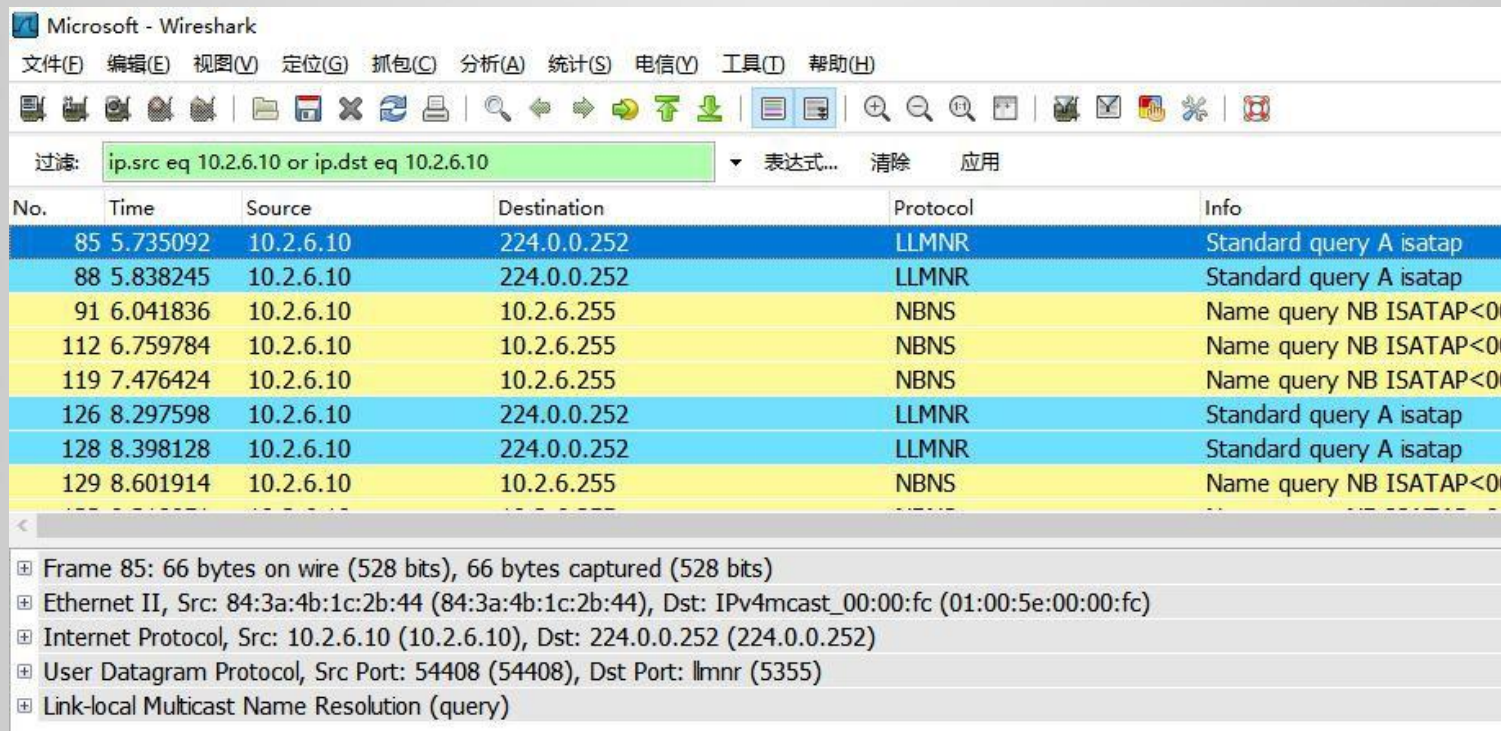
这里的功能主要是分析功能，作用比较大

Wireshark过滤方式

Wireshark过滤方式

Wireshark过滤规则及使用

1.过滤IP，如来源IP或者目标IP等于某个IP ip.src eq 10.2.6.10 or ip.dst eq 10.2.6.10



Microsoft - Wireshark

文件(F) 编辑(E) 视图(V) 定位(G) 抓包(C) 分析(A) 统计(S) 电信(Y) 工具(T) 帮助(H)

过滤: ip.src eq 10.2.6.10 or ip.dst eq 10.2.6.10 表达式... 清除 应用

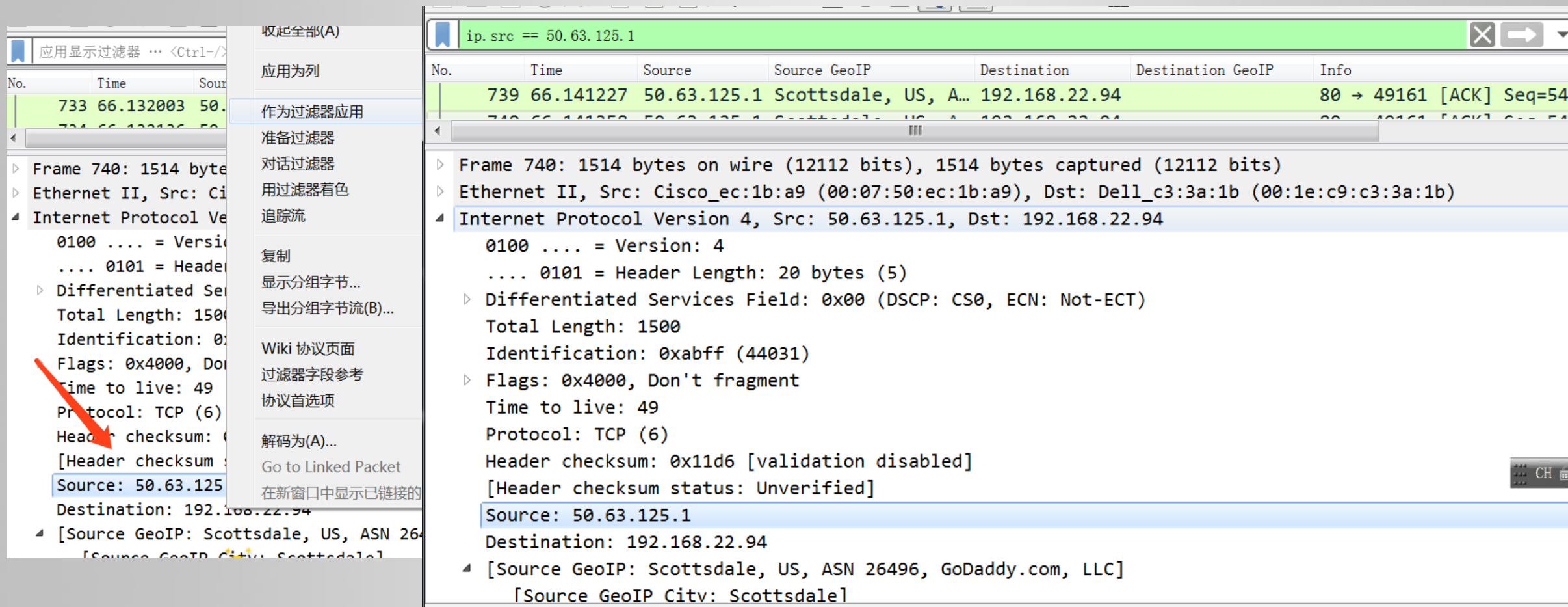
No.	Time	Source	Destination	Protocol	Info
85	5.735092	10.2.6.10	224.0.0.252	LLMNR	Standard query A isatap
88	5.838245	10.2.6.10	224.0.0.252	LLMNR	Standard query A isatap
91	6.041836	10.2.6.10	10.2.6.255	NBNS	Name query NB ISATAP<0
112	6.759784	10.2.6.10	10.2.6.255	NBNS	Name query NB ISATAP<0
119	7.476424	10.2.6.10	10.2.6.255	NBNS	Name query NB ISATAP<0
126	8.297598	10.2.6.10	224.0.0.252	LLMNR	Standard query A isatap
128	8.398128	10.2.6.10	224.0.0.252	LLMNR	Standard query A isatap
129	8.601914	10.2.6.10	10.2.6.255	NBNS	Name query NB ISATAP<0

<

- Frame 85: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
- Ethernet II, Src: 84:3a:4b:1c:2b:44 (84:3a:4b:1c:2b:44), Dst: IPv4mcast_00:00:fc (01:00:5e:00:00:fc)
- Internet Protocol, Src: 10.2.6.10 (10.2.6.10), Dst: 224.0.0.252 (224.0.0.252)
- User Datagram Protocol, Src Port: 54408 (54408), Dst Port: llmnr (5355)
- Link-local Multicast Name Resolution (query)

Wireshark过滤方式

Wireshark过滤规则及使用



The image displays the Wireshark network protocol analyzer interface. The top bar shows the active filter: `ip.src == 50.63.125.1`. The packet list on the left shows several packets, with packet 739 selected. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and TCP. A red arrow points to the 'Source' field in the packet details pane, which is highlighted in blue.

Packet List:

No.	Time	Source	Source GeoIP	Destination	Destination GeoIP	Info
733	66.132003	50.63.125.1	Scottsdale, US, A...	192.168.22.94		80 → 49161 [ACK] Seq=54
739	66.141227	50.63.125.1	Scottsdale, US, A...	192.168.22.94		80 → 49161 [ACK] Seq=54

Packet Details (Frame 740):

- Frame 740: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
- Ethernet II, Src: Cisco_ec:1b:a9 (00:07:50:ec:1b:a9), Dst: Dell_c3:3a:1b (00:1e:c9:c3:3a:1b)
- Internet Protocol Version 4, Src: 50.63.125.1, Dst: 192.168.22.94
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 1500
 - Identification: 0xabff (44031)
 - Flags: 0x4000, Don't fragment
 - Time to live: 49
 - Protocol: TCP (6)
 - Header checksum: 0x11d6 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 50.63.125.1
 - Destination: 192.168.22.94
 - [Source GeoIP: Scottsdale, US, ASN 26496, GoDaddy.com, LLC]
 - [Source GeoIP City: Scottsdale]

2.过滤端口

例子:

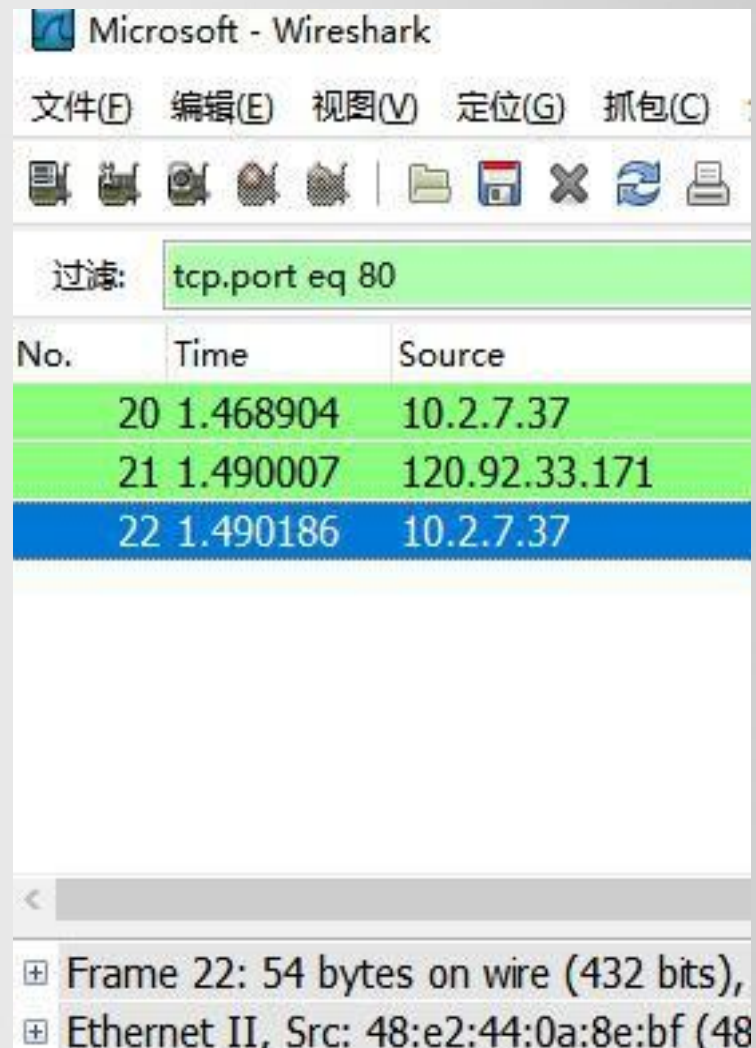
`tcp.port eq 80` // 不管端口是来源的还是目标的都显示

`tcp.dstport == 80` // 只显tcp协议的目标端口80

`tcp.srcport == 80` // 只显tcp协议的来源端口80

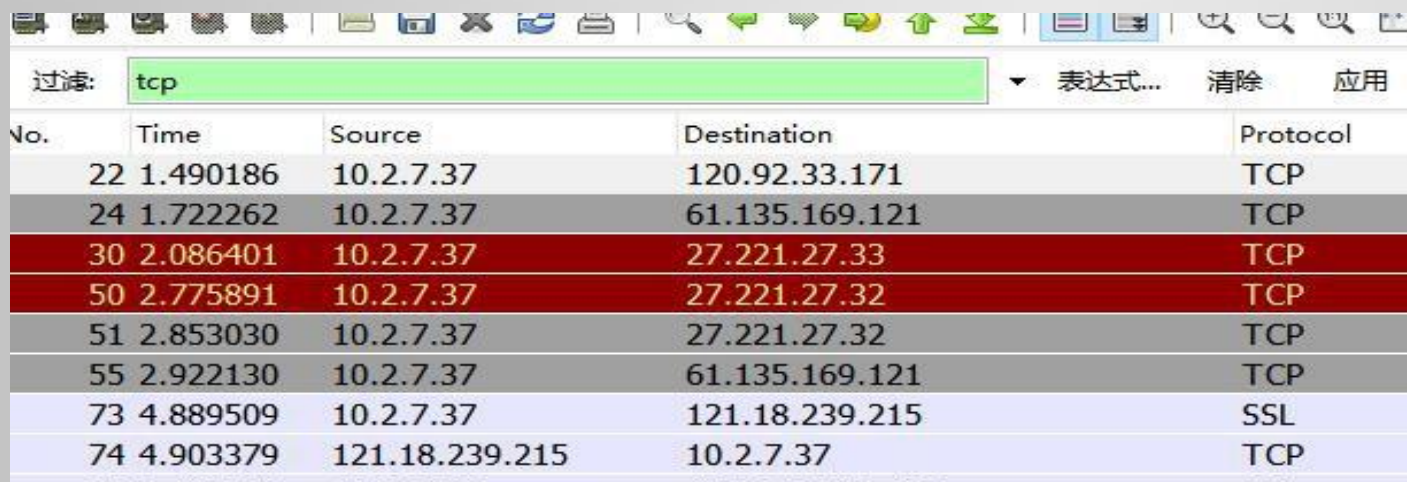
过滤端口范围

`tcp.port >= 1 and tcp.port <= 80`



3.过滤协议

例子:tcp udp arp



The image shows the Wireshark network protocol analyzer interface. The top toolbar contains various icons for file operations, network analysis, and display. Below the toolbar, the 'Filter' field is set to 'tcp', and the 'Expression' field is empty. The packet list table below shows several packets, with the first two (No. 22 and 24) filtered out (grayed out) and the subsequent three (No. 30, 50, and 51) highlighted in red, indicating they match the filter. The table has five columns: No., Time, Source, Destination, and Protocol.

No.	Time	Source	Destination	Protocol
22	1.490186	10.2.7.37	120.92.33.171	TCP
24	1.722262	10.2.7.37	61.135.169.121	TCP
30	2.086401	10.2.7.37	27.221.27.33	TCP
50	2.775891	10.2.7.37	27.221.27.32	TCP
51	2.853030	10.2.7.37	27.221.27.32	TCP
55	2.922130	10.2.7.37	61.135.169.121	TCP
73	4.889509	10.2.7.37	121.18.239.215	SSL
74	4.903379	121.18.239.215	10.2.7.37	TCP

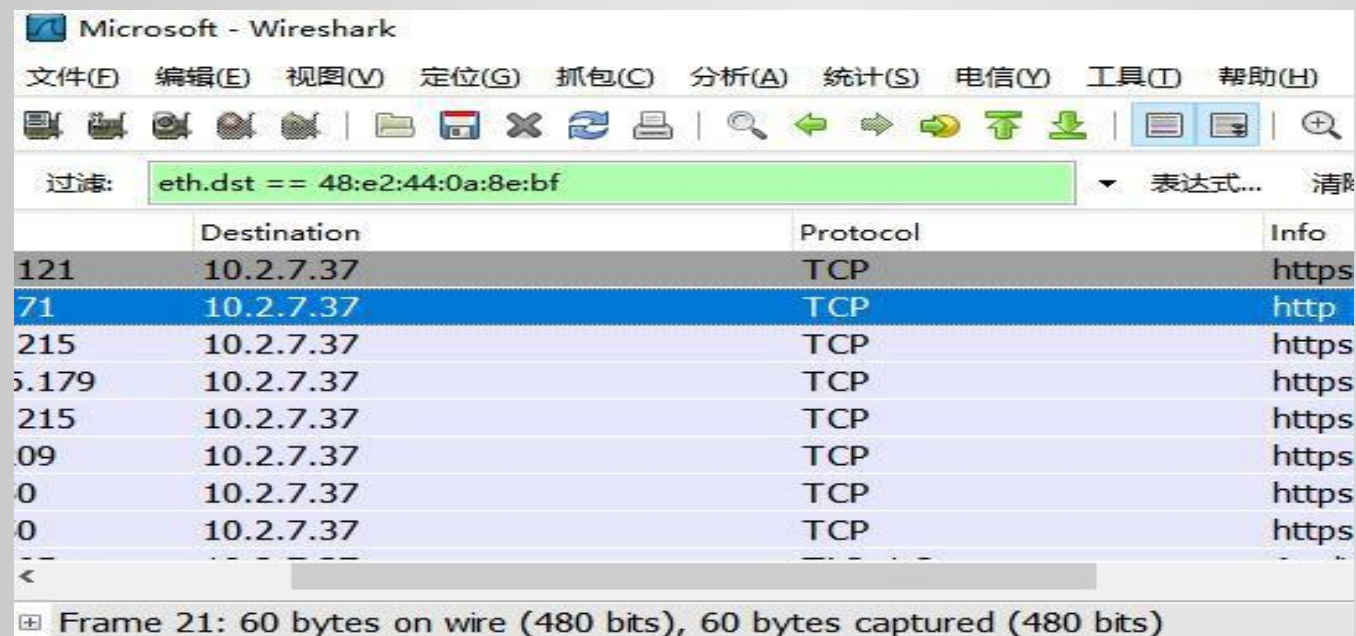
Wireshark过滤方式

过滤MAC

以太网头过滤

eth.dst == A0:00:00:04:C5:84 // 过滤目标mac eth.src eq A0:00:00:04:C5:84 // 过滤来源mac

eth.addr eq A0:00:00:04:C5:84 // 过滤来源MAC和目标MAC都等于A0:00:00:04:C5:84的



5.包长度过滤

例子:

udp.length == 26 这个长度是指udp本身固定长度8加上udp下面那块数据包之和
tcp.len >= 7 指的是ip数据包(tcp下面那块数据),不包括tcp本身

6.http模式过滤

例子:

http.request.method == "GET" http.request.method == "POST" http.request.uri == "/img/logo-edu.gif" http contains "GET"
http contains "HTTP/1."