附录A：Wireshark 教程

一、Wireshark简介

Wireshark是一个非常强大的开源网络协议分析工具，具有以下特点和功能：

1. **实时抓包和分析：** Wireshark能够实时捕获网络分组，以人类可读的方式展示，并提供详细的分析和解析功能，帮助用户了解网络流量和协议交互情况。
2. **多平台支持：** Wireshark可在Windows、Mac和Linux/Unix等多个操作系统平台上运行，为不同用户提供了方便的网络分析工具。
3. **强大的过滤功能：** Wireshark提供了丰富的过滤器功能，用户可以根据需要过滤出特定协议、IP地址、端口等信息，以便更好地分析和查看网络分组。
4. **协议支持广泛：** Wireshark支持众多网络协议的解析和展示，包括常见的TCP、UDP、IP、HTTP等协议，使用户能够深入分析各种网络通信情况。
5. **分组重组和导出：** Wireshark可以帮助用户重组分组流，还可以将捕获的分组导出为不同格式，方便用户进行进一步的分析和存档。

Wireshark仅仅监视网络状况，但不会处理网络事务，也不能检测和防止网络入侵或攻击。

二、下载与安装

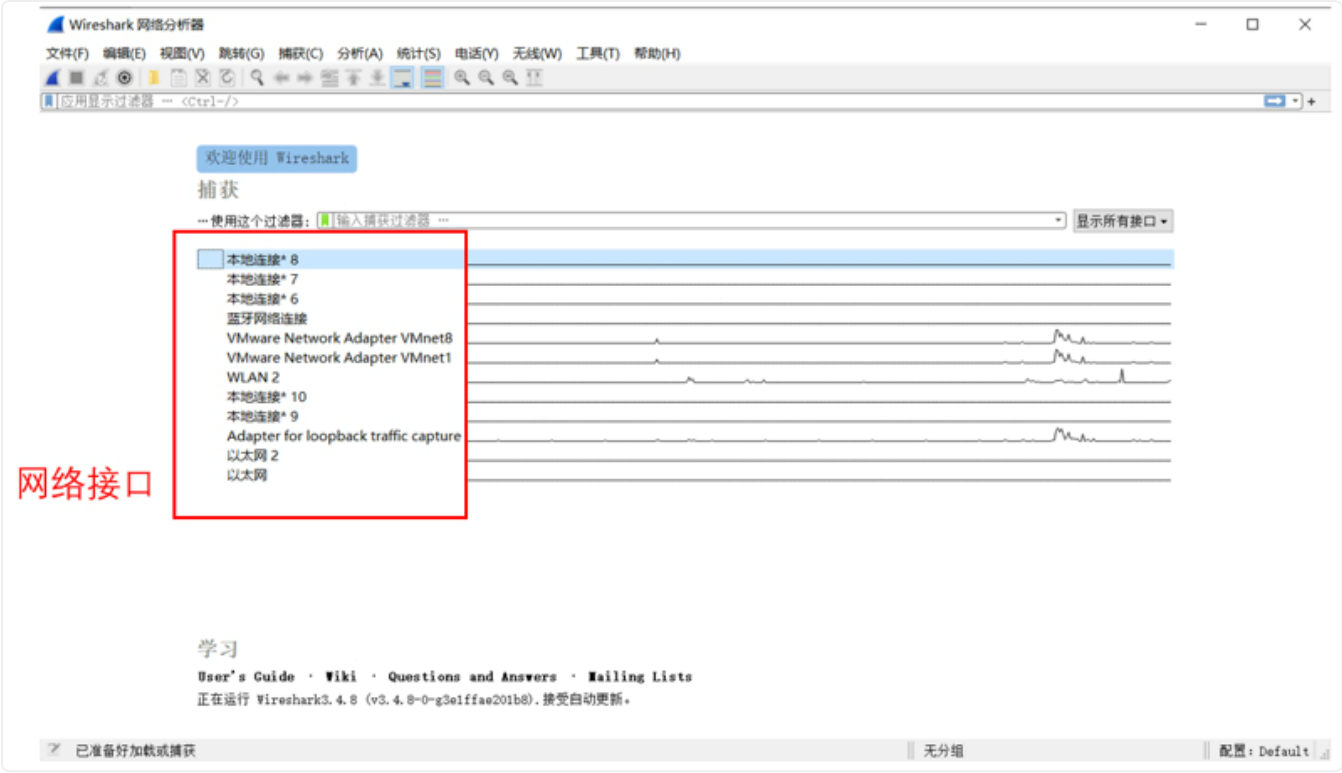
下载网址：https://www.wireshark.org/#download

选择符合本机环境的版本，按默认选项安装即可。

三、使用

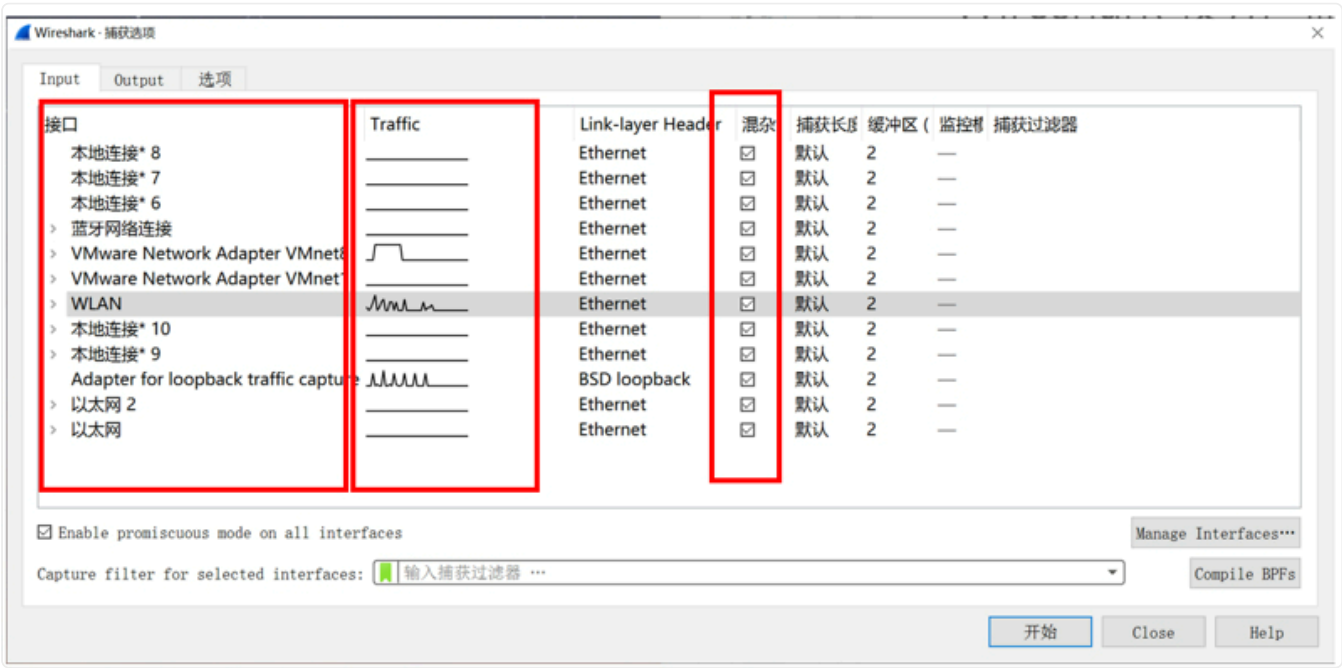
3.1 捕获分组

Wireshark的首页如下图所示。中间列出了当前计算机上可用的一系列网络接口，右侧的波形图显示网络流量的实时情况。在捕获流量时需要选择一个接口，我们实验中常用**WLAN**或**WLAN2**。



Wireshark首页

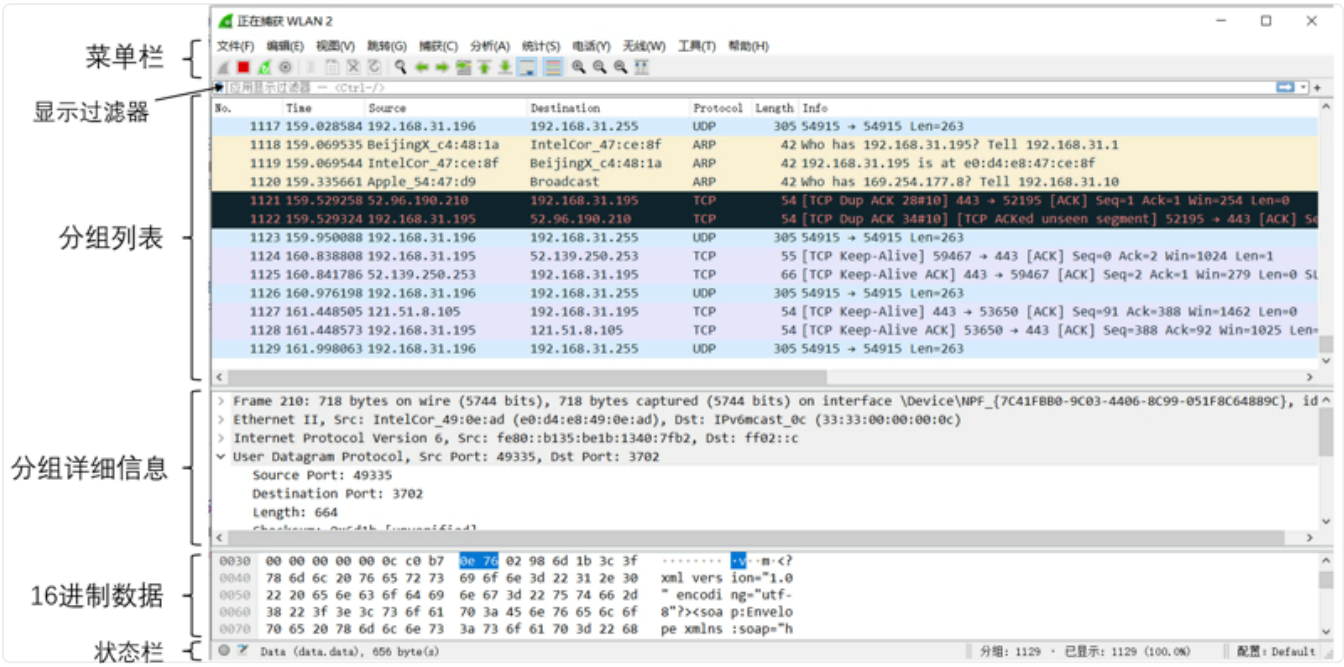
点击上方菜单栏的“捕获-选项”，可以打开以下窗口，请确认所有接口都打开了混杂模式（尽管wireshark默认设置一般已经选择混杂模式）。混杂模式意味着，wireshark会捕获经过本机的所有分组，因此可以对网络流量进行全面分析；而不打开此模式时wireshark只会捕获目的地是本机的分组。



捕获选项

选择好网络接口，点击左上角的蓝色鲨鱼鳍，或菜单栏的“捕获-开始”，即可开始捕获分组，点击红色方块可停止捕获。捕获分组后的页面如下图所示，分组列表中的每一行即代表一个捕获

到的分组，点击任意分组，下方将显示该分组的详细信息。拖动区域边缘，可以调整每个区域的大小。双击分组，可以为分组详细信息打开一个独立的窗口。



捕获结果页面

在菜单栏“文件”中，可选择“导出”、“打印”部分或全部分组。导出的格式可以选择pcap、txt、csv、json等，其中pcap、pcapng等格式是网络流量的默认格式，可以用wireshark再次打开，效果与捕获到的分组相同。打印则一般以便于人类阅读的格式输出，例如pdf。

3.2 过滤器

Wireshark能在短时间内捕获海量分组，为了快速找到关注的分组，我们需要使用过滤器。过滤器分为以下两种：

捕获过滤器：在开始捕获分组前在捕获选项底端设置，可以只捕获符合条件的分组。

捕获过滤器的表达式语法如下图：

Protocol	Direction	Host(s)	Value	Logical Operations	Other expression
tcp	dst	10.1.1.1	80	and	tcp dst 10.2.2.2 3128

捕获过滤器表达式语法

以下是一些捕获过滤器的表达式示例：

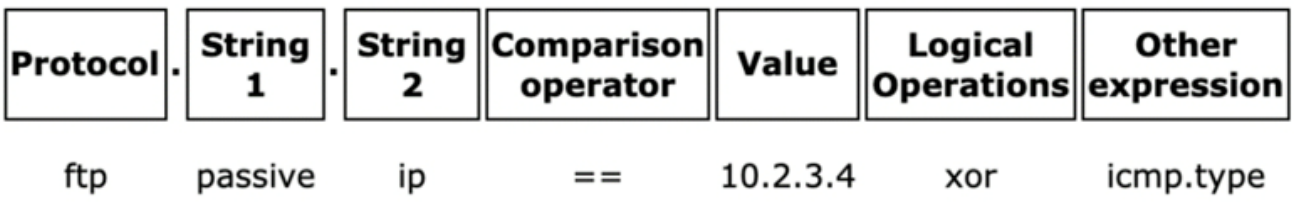
- `tcp src port 443` 抓取TCP源端口为443的分组
-

- `ip dst host 10.1.1.1` 抓取目的IP地址为10.1.1.1的分组
- `src portrange 2000-2500` 抓取源端口号在2000至2500范围内的分组
- `not icmp` 抓取除ICMP协议以外的分组

更多细节可查询wireshark捕获过滤器官方文档。

显示过滤器：在结果页面顶端设置，可以只显示符合条件的分组。

显示过滤器的表达式语法如下图：



显示过滤器表达式语法

以下是一些显示过滤器的表达式示例：

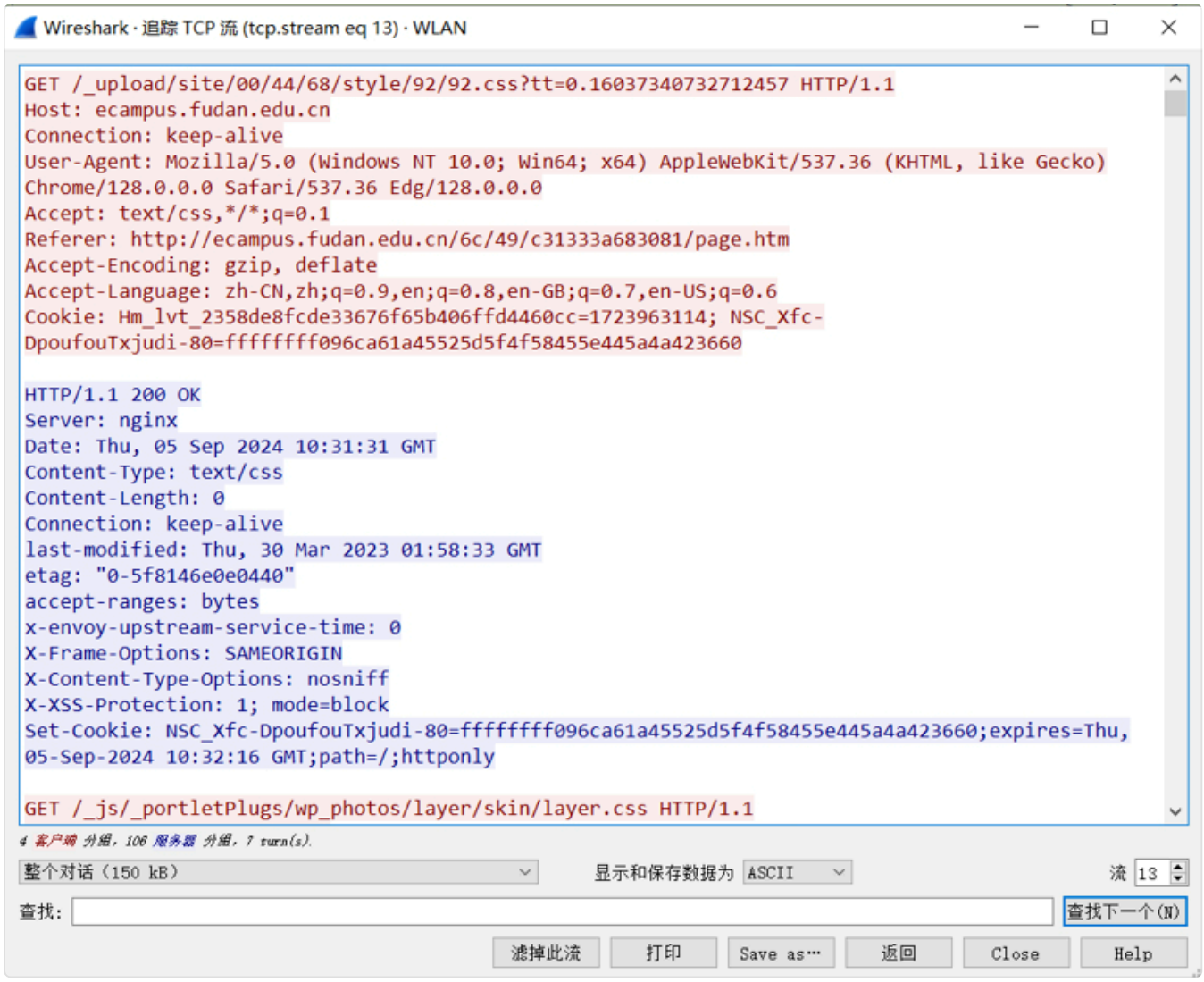
- `tcp` 只显示TCP协议的分组
- `ip.dst == 202.120.224.82` 显示目的IP地址为202.120.224.82的分组
- `eth.type == 0x0806` 显示以太网协议号为0x0806的协议（ARP协议）

更多细节可查询wireshark显示过滤器官方文档。

3.3 结果分析

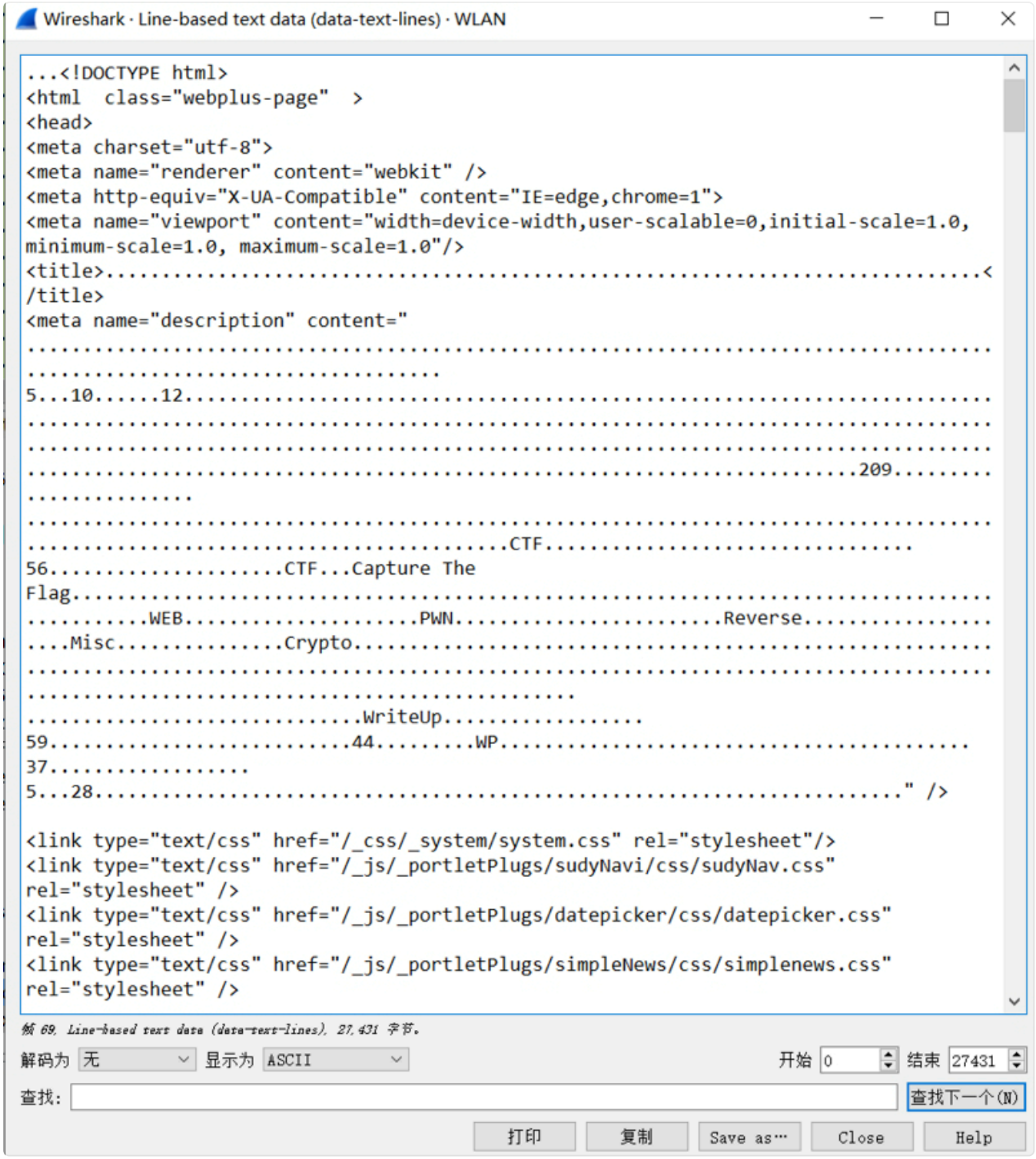
点击菜单栏“**统计-捕获文件属性**”，可以了解此次捕获到的分组的一些统计信息。

点击一个分组，右键“追踪流-TCP流”或在菜单栏点击“**分析-追踪流**-TCP流”，这将打开一个新窗口，包含这个流中的所有数据，可以看到数据是如何在源地址和目的地址之间传输的，以及数据的实际内容。同时，上方的显示过滤器也会自动调整为只显示这个流的分组。



追踪流

选择一个有实际内容的HTTP分组（Info往往为 HTTP/1.1 200 OK + css/png/javascript等文件类型），在分组详细信息最下方找到分组内容（与Info中描述的类型相同），右键“显示分组字节”或点击后在菜单栏点击“**分析-显示分组字节**”，将打开一个新窗口，包含分组详细内容。



显示分组字节

Wireshark的更多功能，欢迎同学们自己探索，也可阅读wireshark官网的教程。

Previous
Lab 1: 使用Wireshark观察分组

Next
常见问题