使用 Kali 进行 Wireshark 数据包捕获与分析

实验目的：

通过使用 Wireshark 工具捕获并分析网络数据包，学习常见网络协议的工作原理，理解网络流量中可能隐藏的安全隐患。

实验步骤：

1. 准备工作：

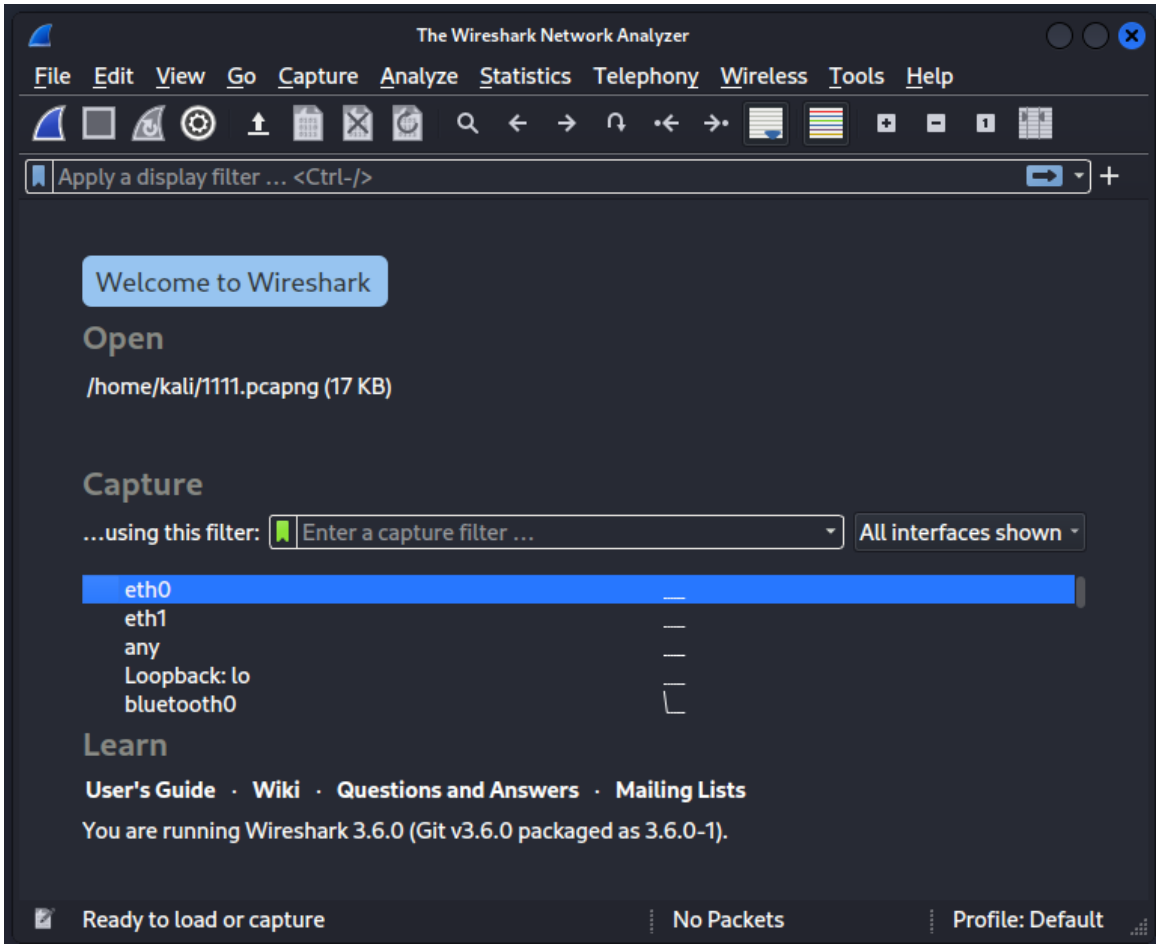
在 Kali Linux 上确保 Wireshark 已安装。

2. 启动 Wireshark：

打开 Wireshark，可以在 Kali 菜单中找到 Wireshark，或者通过终端输入以下命令启动：

```
wireshark &
```

```
┌──(kali㉿kali)-[~]
└─$ wireshark &
[1] 17046
```



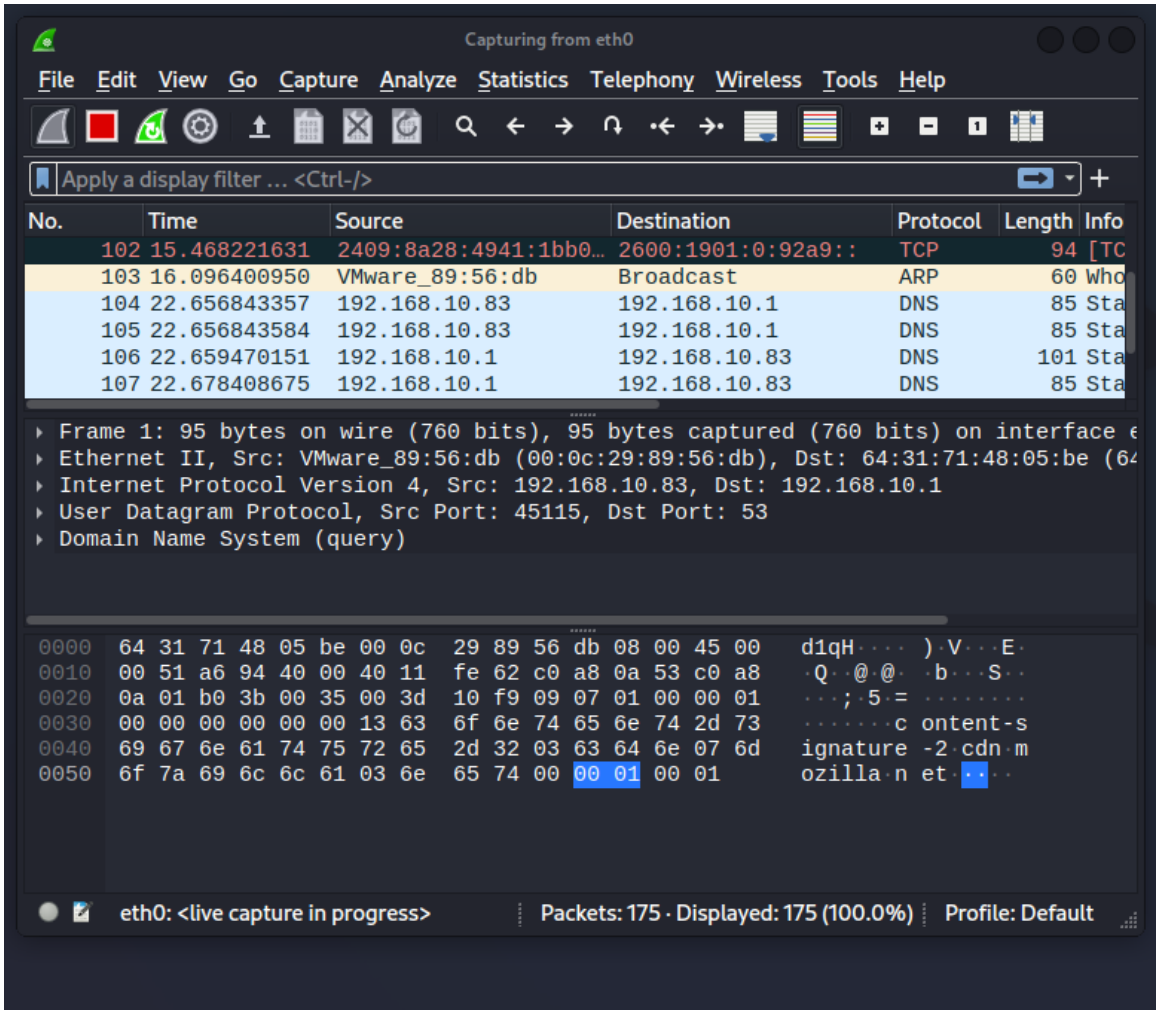
启动 Wireshark 后，选择需要监控的网络接口（例如，eth0 或 wlan0），点击“Start”按钮开始捕获数据包。

3. 捕获数据包：

选择正确的网络接口后，Wireshark 开始实时捕获网络流量。可以让它捕获几分钟的数据包，也可以执行一些网络活动（如浏览网页、发送请求）以生成流量。

捕获过程中，Wireshark 会以列表的形式显示所有数据包，包含时间戳、源 IP、目标 IP、协议类型等。

截图一：



4. 停止捕获：

捕获足够数据包后，点击“Stop”按钮停止捕获。

5. 数据包分析：

使用过滤器来查看特定类型的数据包。查看以下三种类型的数据包，截图并分析

- 查看 ARP 数据包： arp

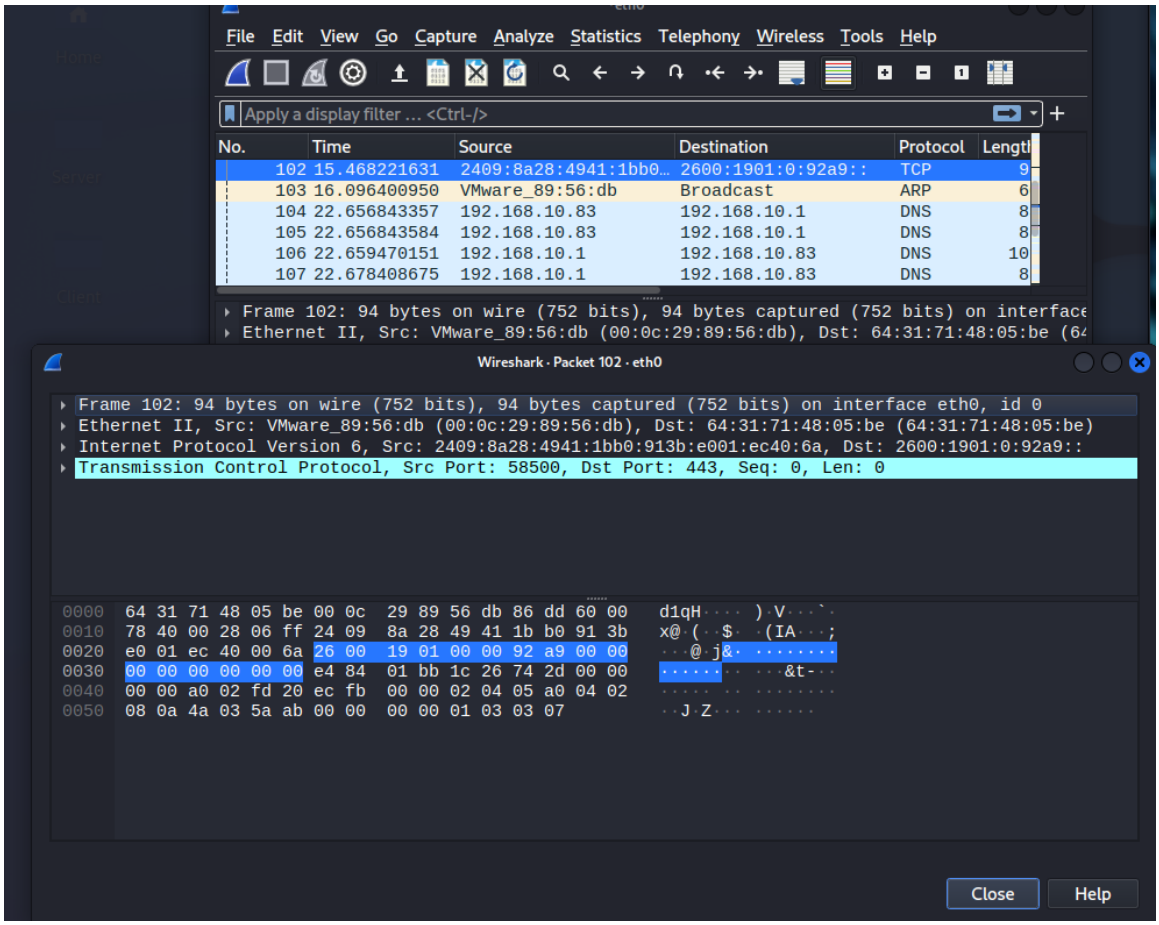
- 查看 TCP 数据包： tcp

- 查看 DNS 请求： dns

选中一个特定数据包，查看其详细信息。Wireshark 会将该数据包的协议层结构分解，包括以太网头、IP 头、传输层协议（TCP/UDP）等。

示例：

1.TCP



1.Ethernet II 层（以太网层）

- **源 MAC 地址**: 00:0c:29:89:56:db

- **目的 MAC 地址**: 64:31:71:48:05:be

2. Internet Protocol Version 6 (IPv6) 层

- **源 IP 地址**: 2409:8a28:4941:1bb0:913b:e001:ec40:6a

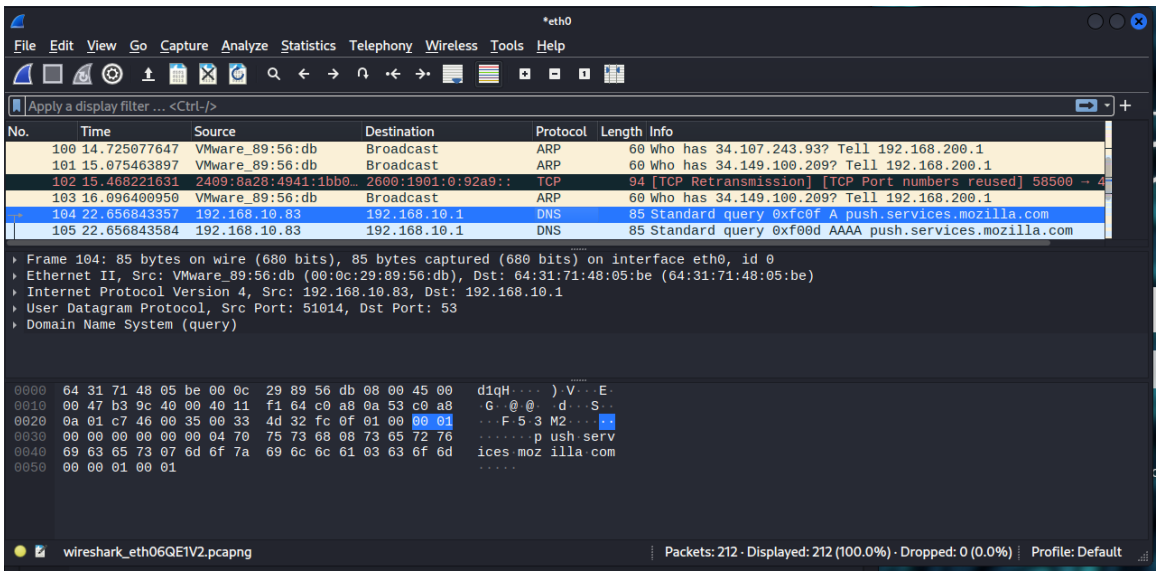
- **目的 IP 地址**: 2600:1901:0:92a9::

3. Transmission Control Protocol (TCP) 层

- **源端口**: 58500

- 目的端口: 443
- **序列号 (Seq)**: 0

2.DNS



1. Ethernet II 层（以太网层）

- **源 MAC 地址**: 00:0c:29:89:56:db

- **目的 MAC 地址**: 64:31:71:48:05:be

2. Internet Protocol Version 4 (IPv4) 层

- **源 IP 地址**: 192.168.10.83
- **目的 IP 地址**: 192.168.10.1

3. User Datagram Protocol (UDP) 层

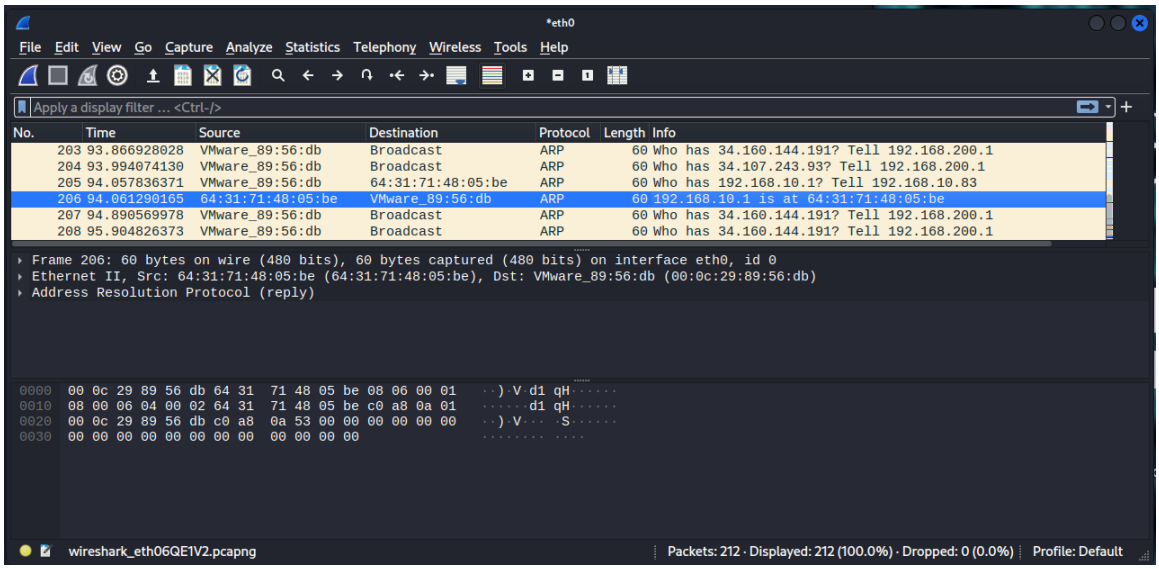
- **源端口**: 51014

- **目的端口**: 53

4. Domain Name System (DNS) 查询层

- **查询内容**: push.services.mozilla.com

3.ARP



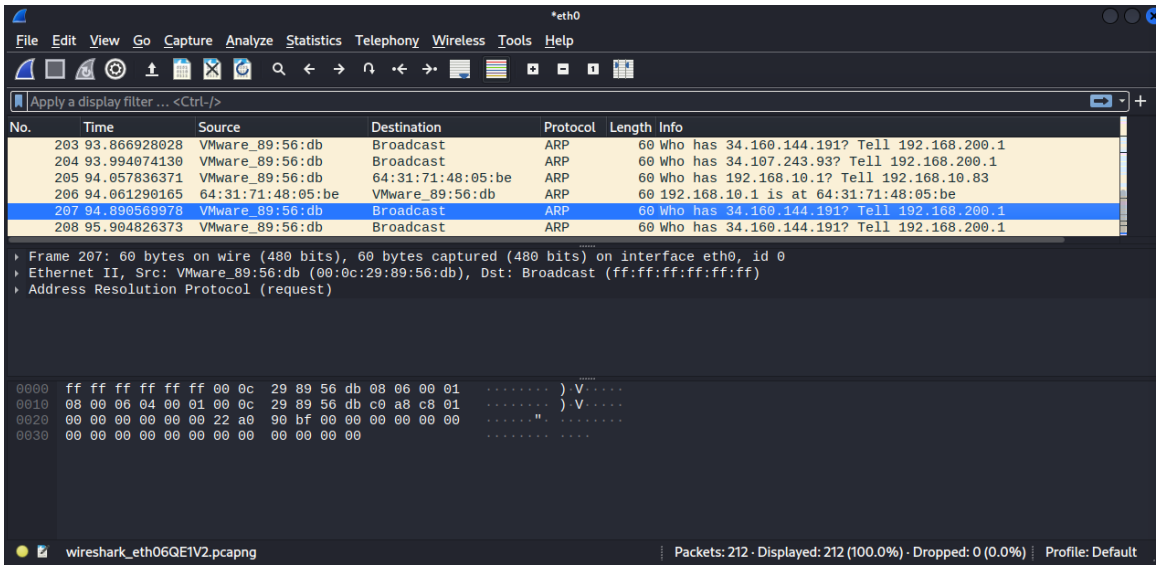
1. Ethernet II 层（以太网层）

- **源 MAC 地址**: 64:31:71:48:05:be

- **目的 MAC 地址**: 00:0c:29:89:56:db

2. Address Resolution Protocol (ARP)

- **操作类型**: 回复 (Reply)
- **发送端 MAC 地址**: 64:31:71:48:05:be
  这是 IP 地址 192.168.10.1 对应的 MAC 地址。
- **发送端 IP 地址**: 192.168.10.1
  这是本地网络中的默认网关（路由器）的 IP 地址。
- **目标 MAC 地址**: 00:0c:29:89:56:db
  这是虚拟机的 MAC 地址。
- **目标 IP 地址**: 192.168.10.83
  这是虚拟机的 IP 地址。



1. Ethernet II 层（以太网层）

- **源 MAC 地址**: 00:0c:29:89:56:db

- **目的 MAC 地址**: ff:ff:ff:ff:ff:ff (广播)
  这是一个广播地址，表示该 ARP 请求被发送到网络中的所有设备。

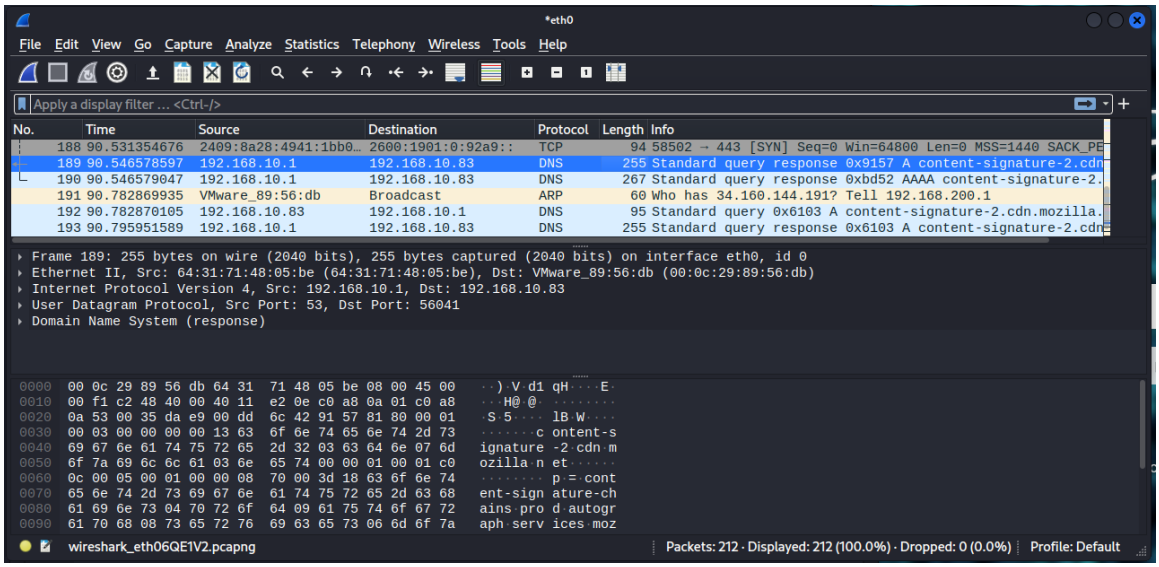
2. Address Resolution Protocol (ARP)

- **操作类型**: 请求 (Request)

- **发送端 MAC 地址**: 00:0c:29:89:56:db
  这是请求发送方的 MAC 地址（虚拟机的 MAC 地址）。

- **发送端 IP 地址**: 192.168.200.1
  这是发送端的 IP 地址。

- **目标 IP 地址**: 34.160.144.191
  该 ARP 请求目标是 34.160.144.191，请求方希望通过 ARP 获取此 IP 地址对应的 MAC 地址。

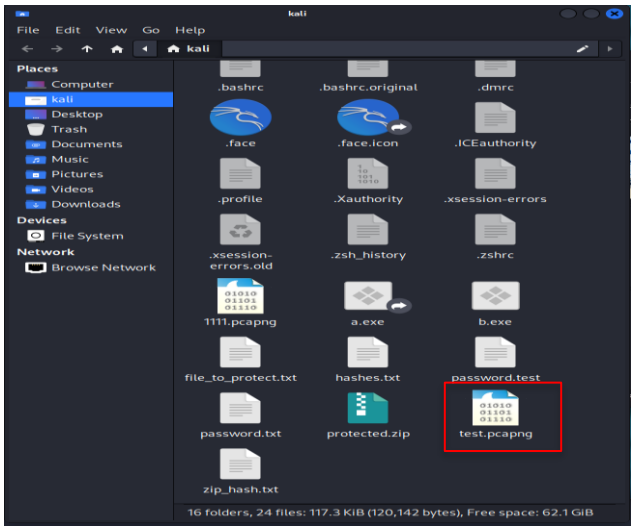


6. 保存捕获的数据：

在 Wireshark 中可以将捕获的数据包保存为.pcap 文件，方便后续分析或报告使用：

File -> Save As -> 保存为.pcap 文件

截图保存结果



实验知识点：

- 网络数据包的捕获与分析原理
- 常见网络协议（TCP/IP, HTTP, DNS）的工作机制
- 通过 Wireshark 了解网络流量中潜在的安全问题