**实验二、网络嗅探取证及入侵检测**

**一、实验目的**

通过网络嗅探软件（WireShark）了解网络数据的获取方法，理解网络取证及入侵检测的原理理解硬盘存储原理和结构以及硬盘数据恢复的原理。

**二、实验内容**

1.安装WireShark软件

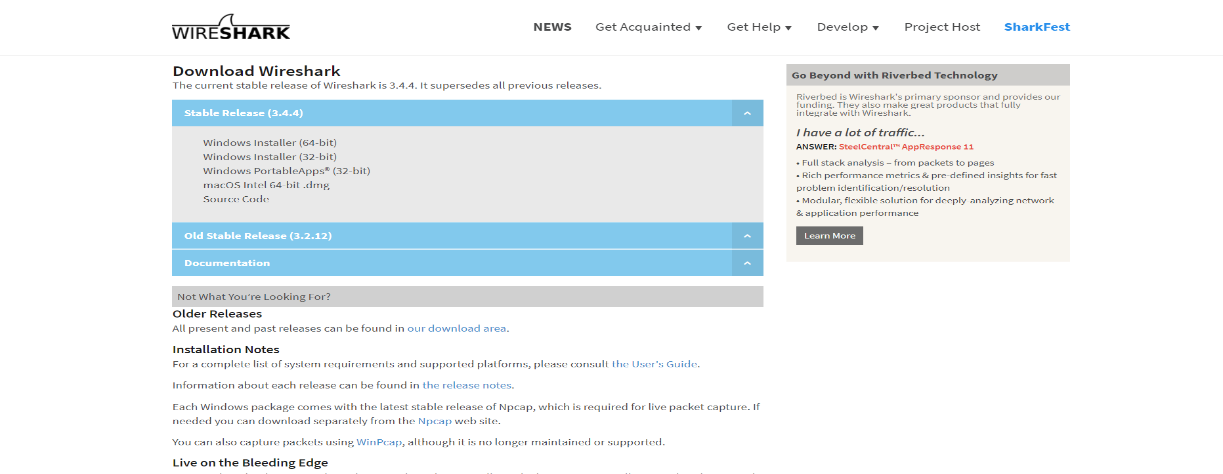
2.了解WireShark的基本使用

3.通过WireShark对网络进行监听

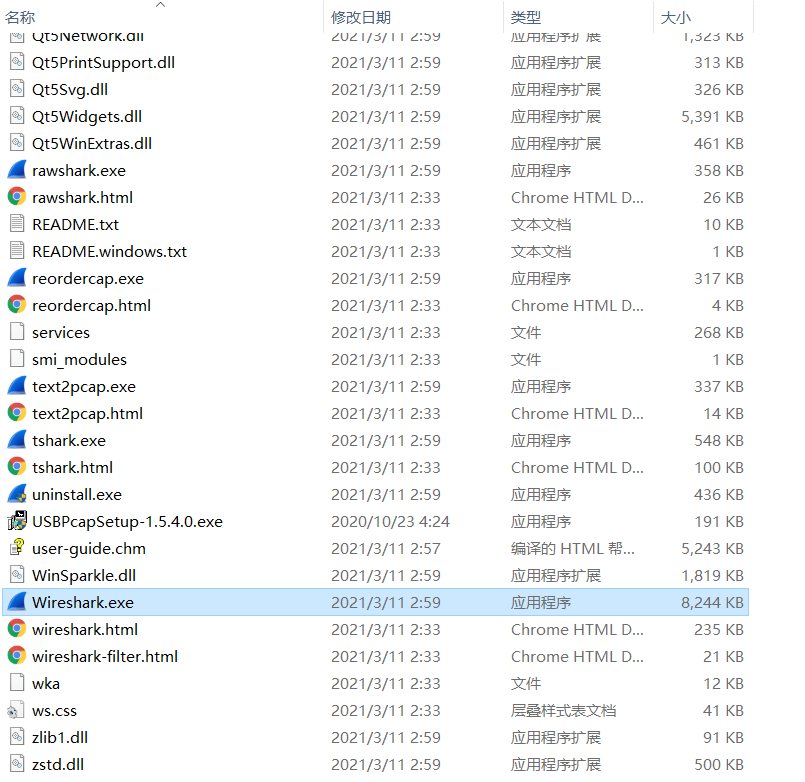
**三、实验步骤**

**1.安装WireShark软件(windows 10)**

(1)打开WireShark官网,根据机型选择下载,此处选择64bit



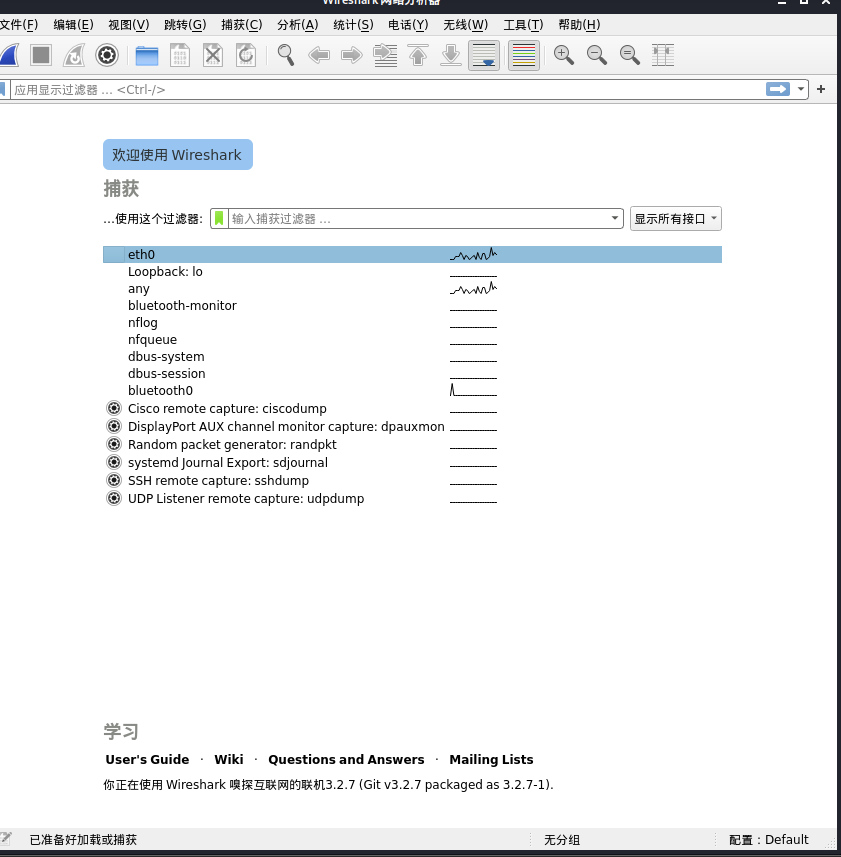
(2)安装软件



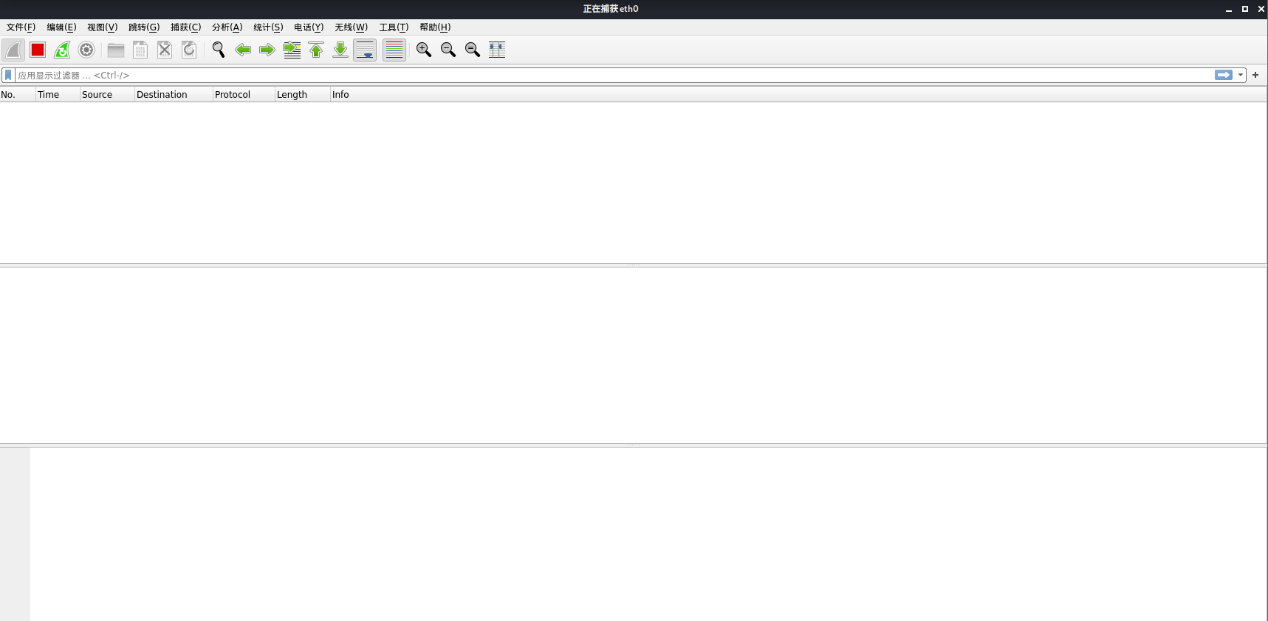
**2.了解WireShark的基本使用(使用VM kali )**

(1)选择网卡设备eth0

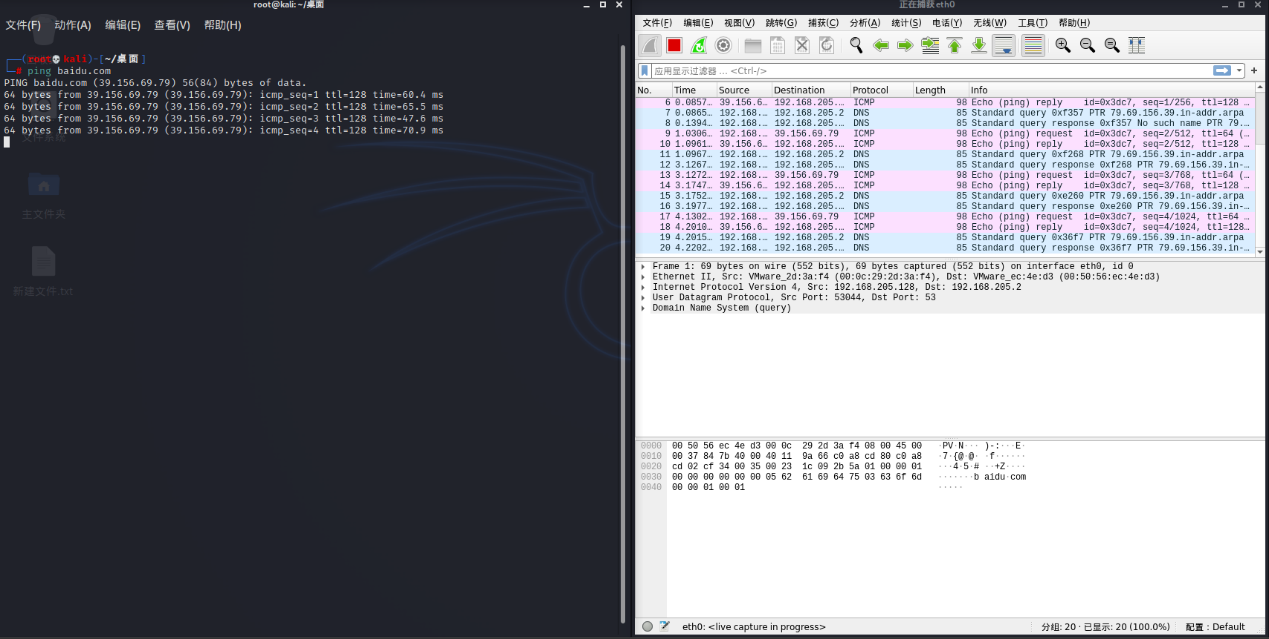
右方曲线图可观察出对应网卡网络流量情况:



无数据接收时:



ping baidu.com :



(2)通过过滤器过滤协议,端口 :

常见协议:tcp,udp,arp,icmp,http,smtp,dns,ip,ssl,bootp等;

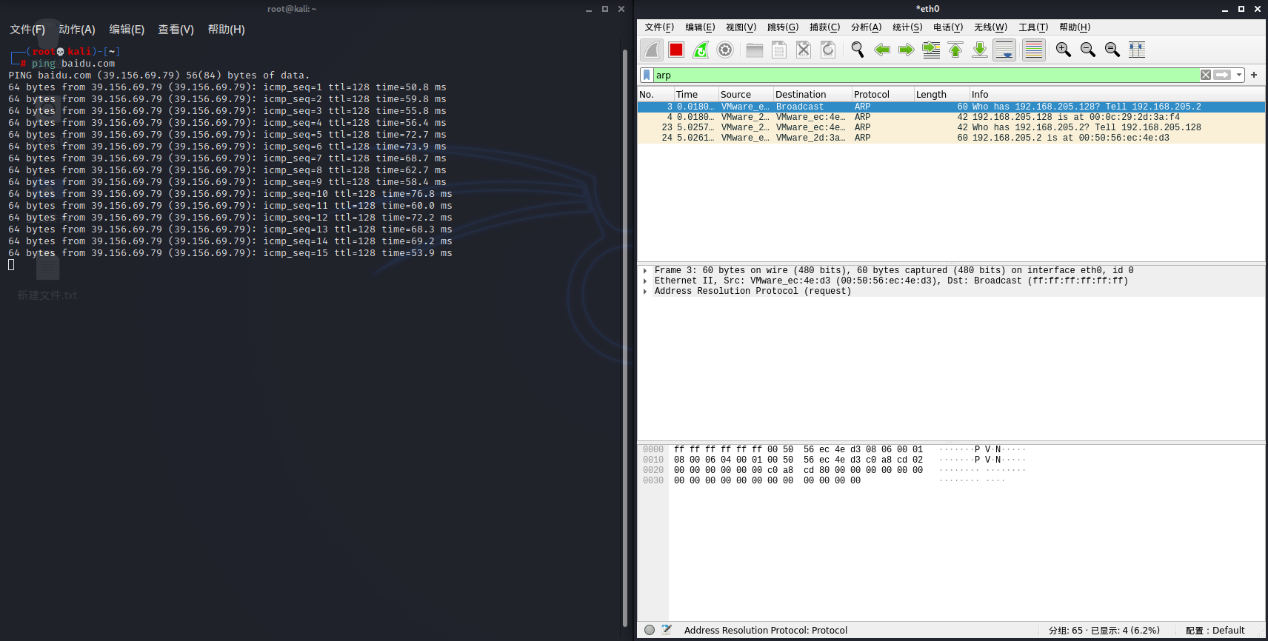
过滤端口:(以tcp为例)

tcp.port eq 80 显示源端口和目的端口为80的报文

tcp.dstport == 80 显示目的端口为80的报文

tcp.srcport == 80 显示来源端口为80的报文

tcp.port >=1 and tcp.port <=80 过滤1->80端口

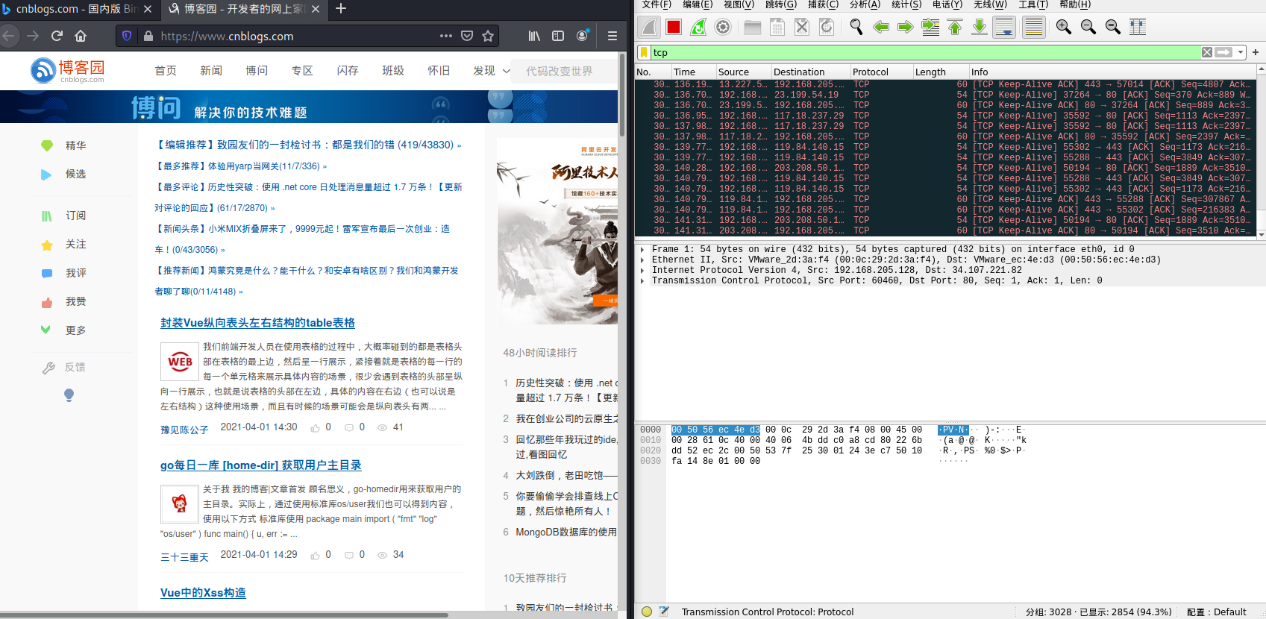


(3)点击相应报文即可查看详情

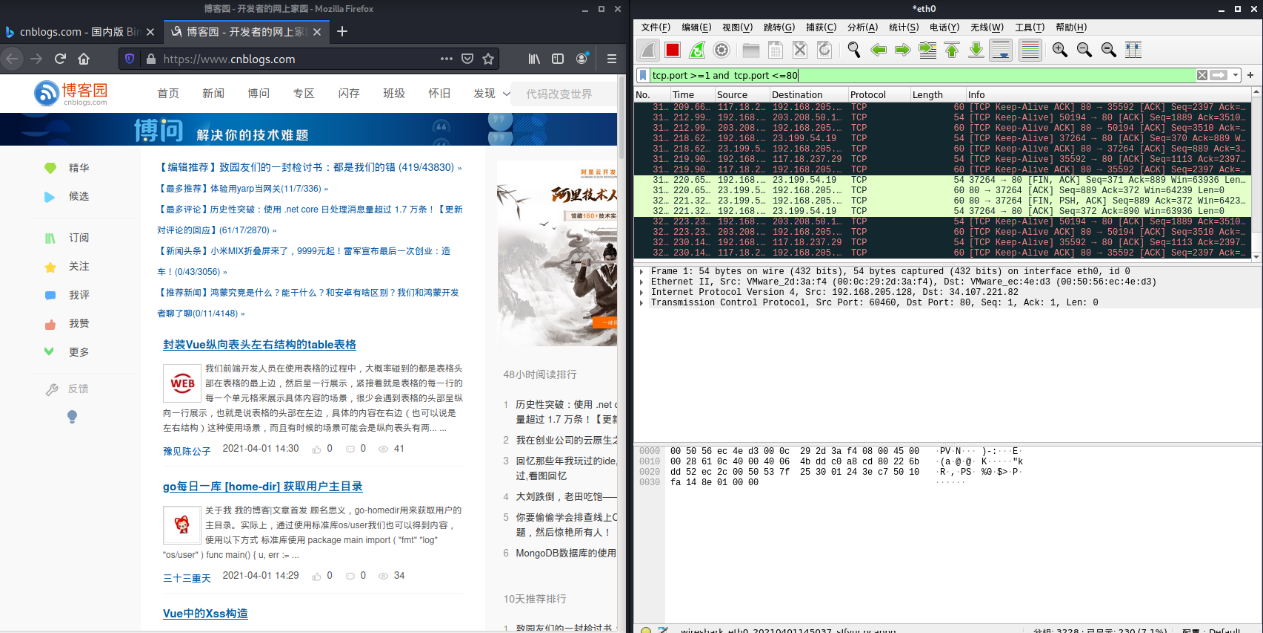
**3. 通过WireShark对网络进行监听**

浏览 cnblogs.com 时 :

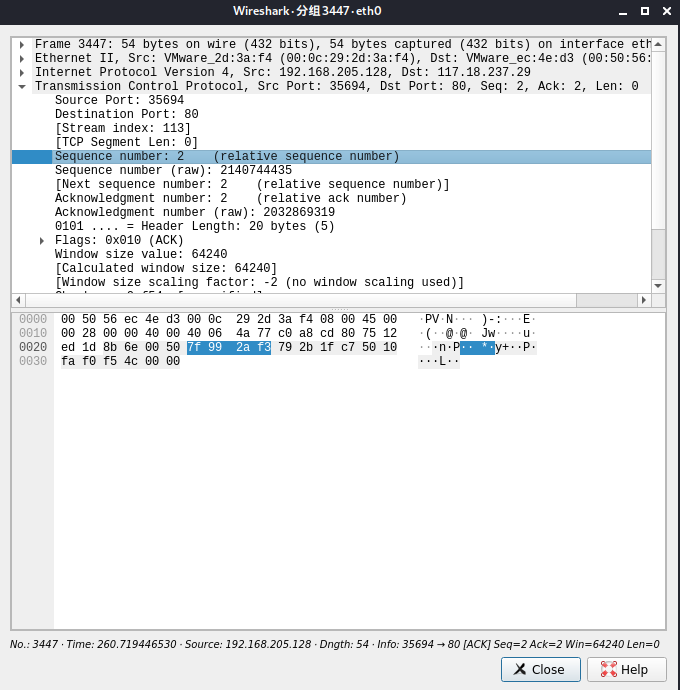
过滤tcp 协议包:



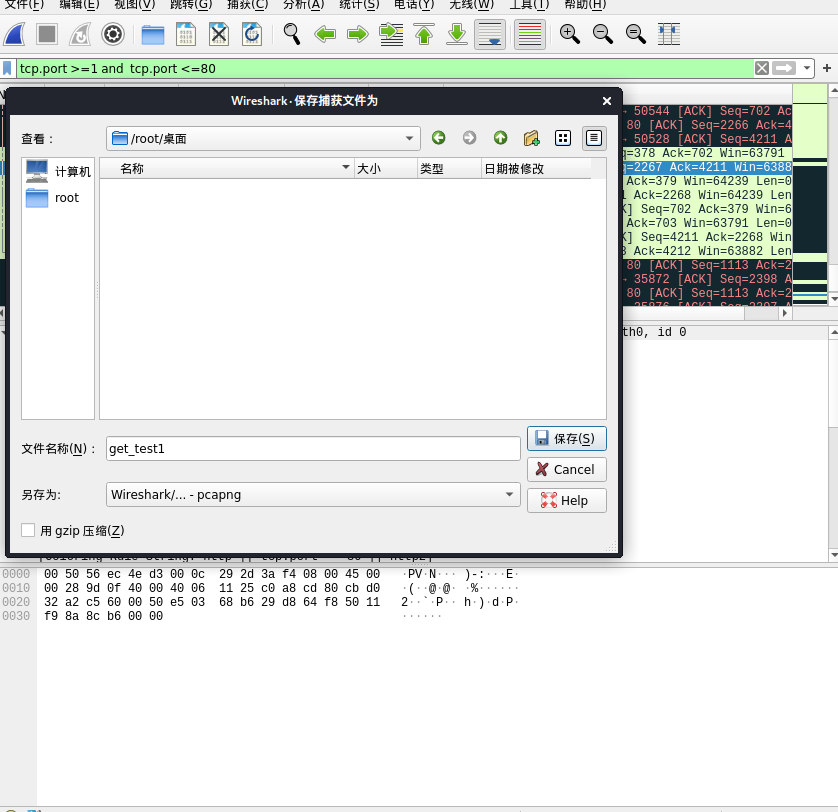
过滤端口范围:



点击筛选出的tcp报文,查看详细信息:



保存抓取的数据包以便分析:



**四、实验结果**

1.成功安装WireShark软件;

2.学会了使用WireShark;

3.成功使用WireShark过滤出报文并进行抓包保存。

**五、写出本次实验的实验心得**

1.学会了使用网络嗅探软件（WireShark）了解网络数据的获取方法;

2.通过抓包理解了网络取证及入侵检测的原理;

3.了解了不同网络协议,学会了更多计算机网络知识;

4.体会到进行实际实验操作对于计算机学习的重要性;

5.体会到维护计算机数据安全的重要性;

6.在计算机专业学习过程中要扎实基础,深刻了解背后原理,勤加实践。