华东师范大学数据科学与工程学院实验报告

课程名称：计算机网络原理与编程	**年级：**2021	**上机实践成绩：**
指导教师：张召	**姓名：**温兆和	**学号：**10205501432
上机实践名称： 利用 WireShark 抓包		**上机实践日期：**2022.03.25
上机实践编号：04 05	**组号：**001-432	**上机实践时间：**13：00

一、 **实验目的**

WireShark 软件熟悉

二、 **实验任务**

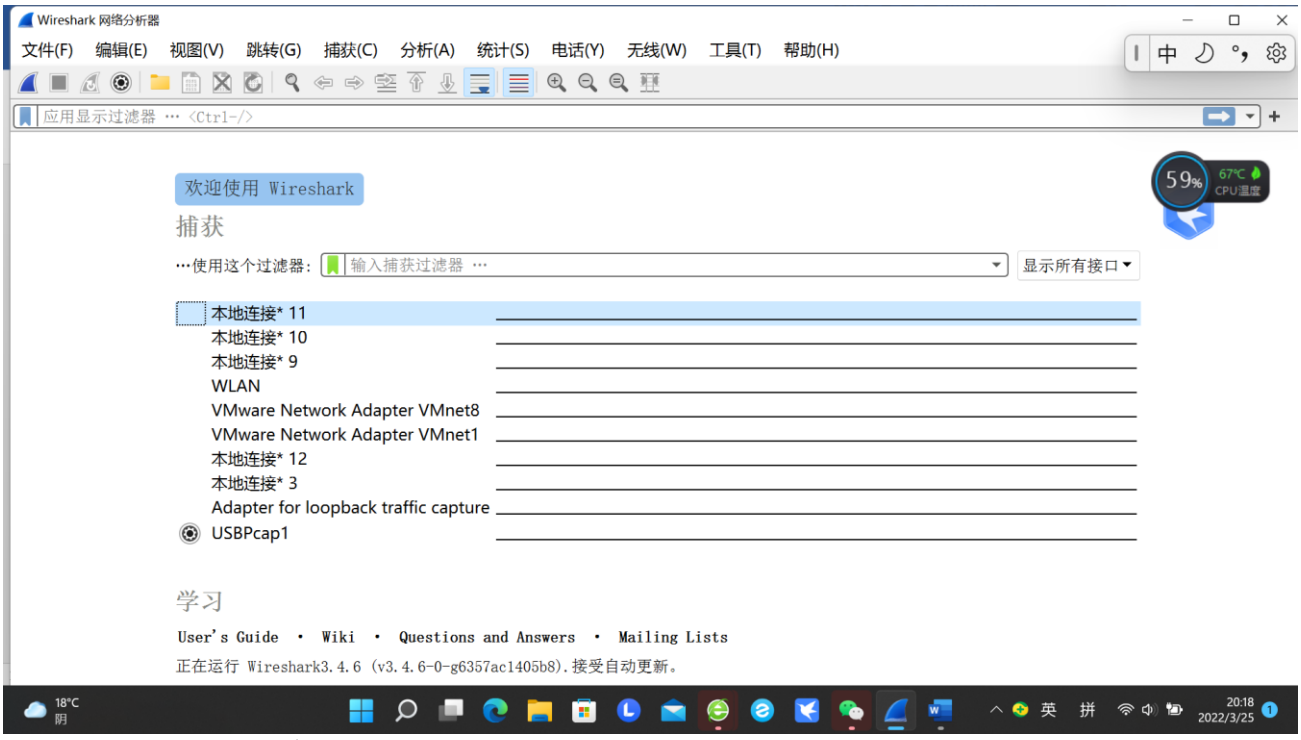
网络包抓取

三、 **使用环境**

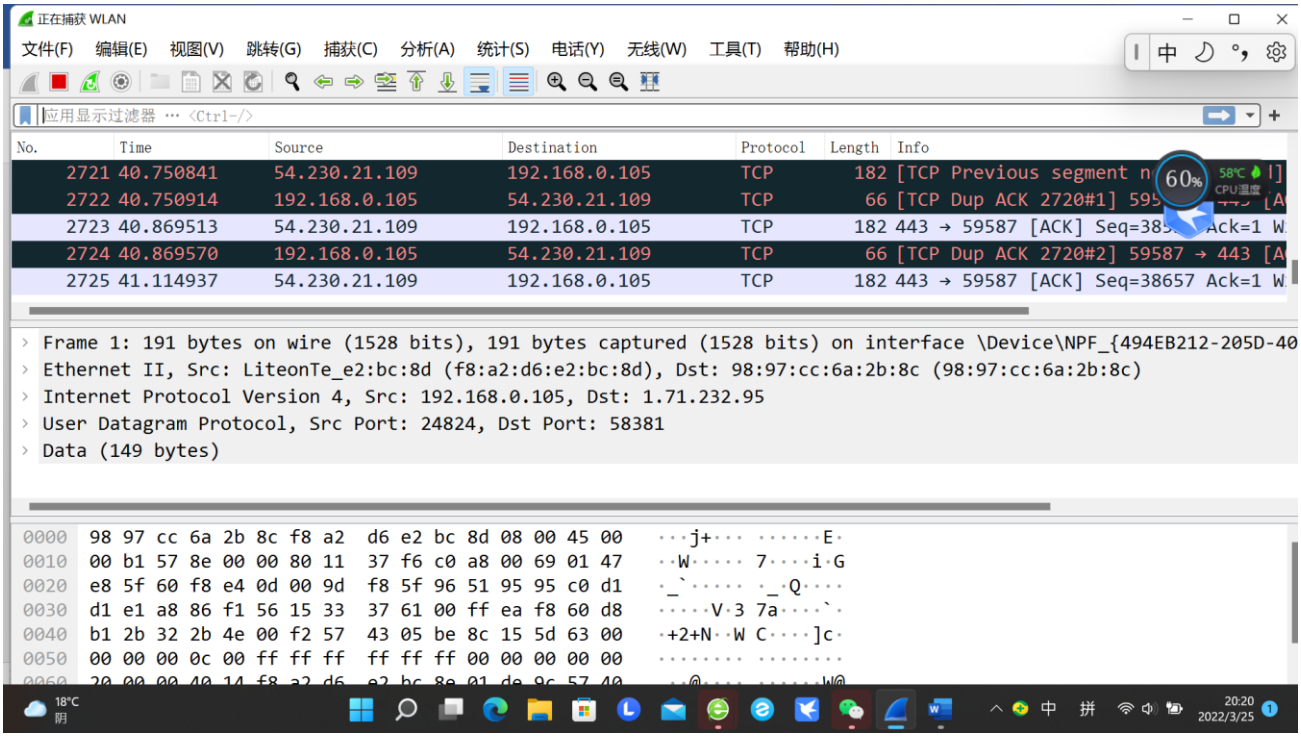
WireShark

四、 **实验过程**

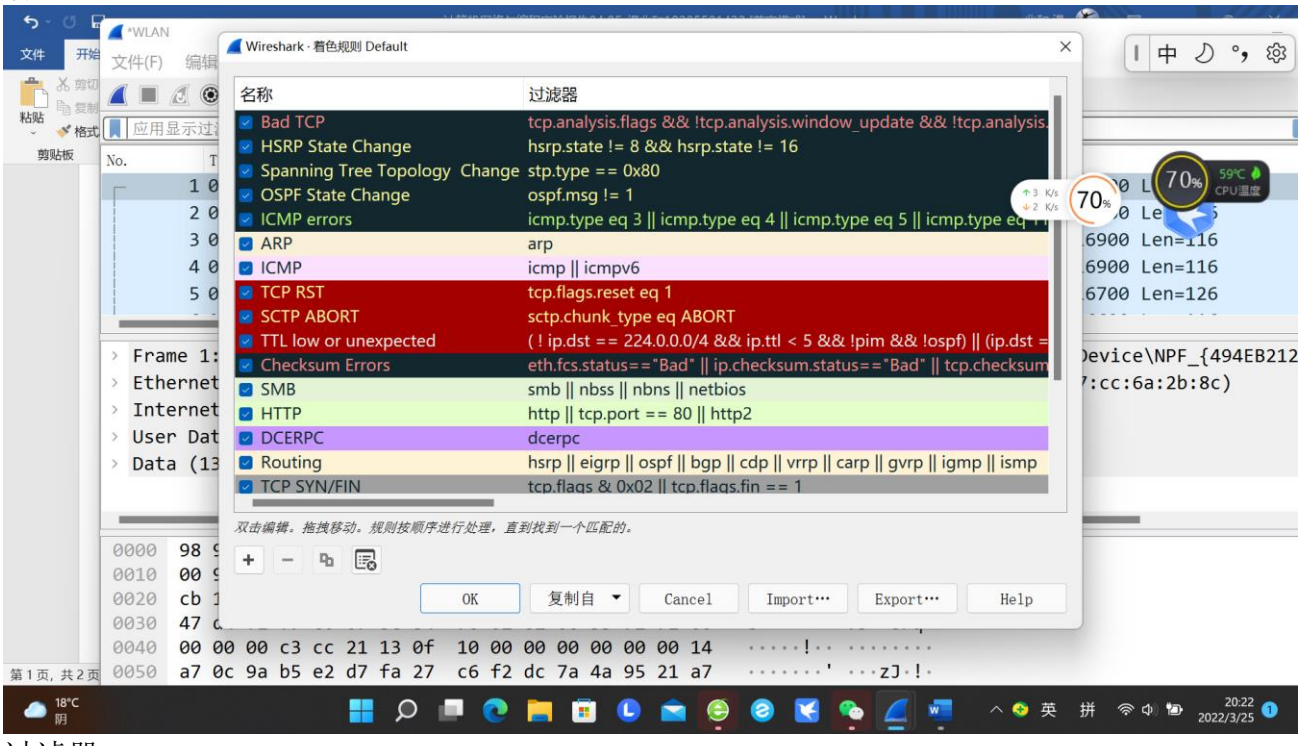
4.1 WireShark 安装



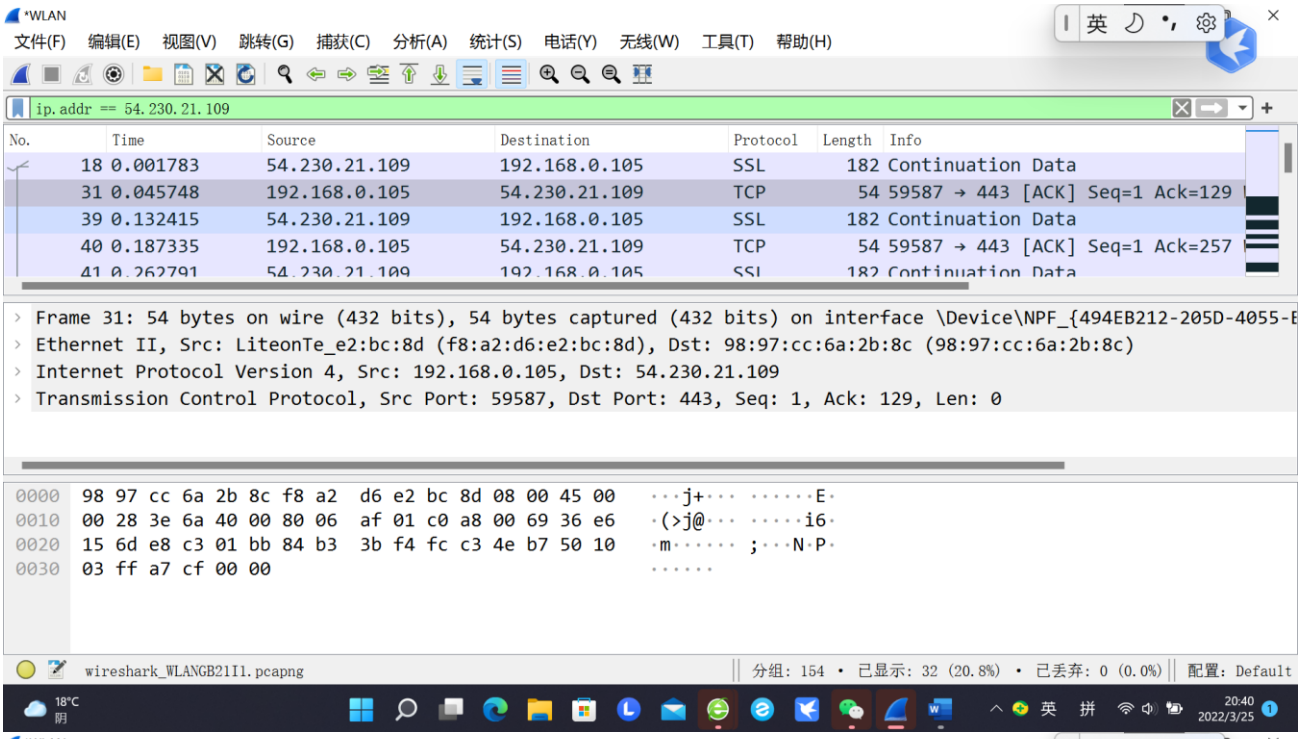
4.2 网络包抓取（网卡：WLAN）

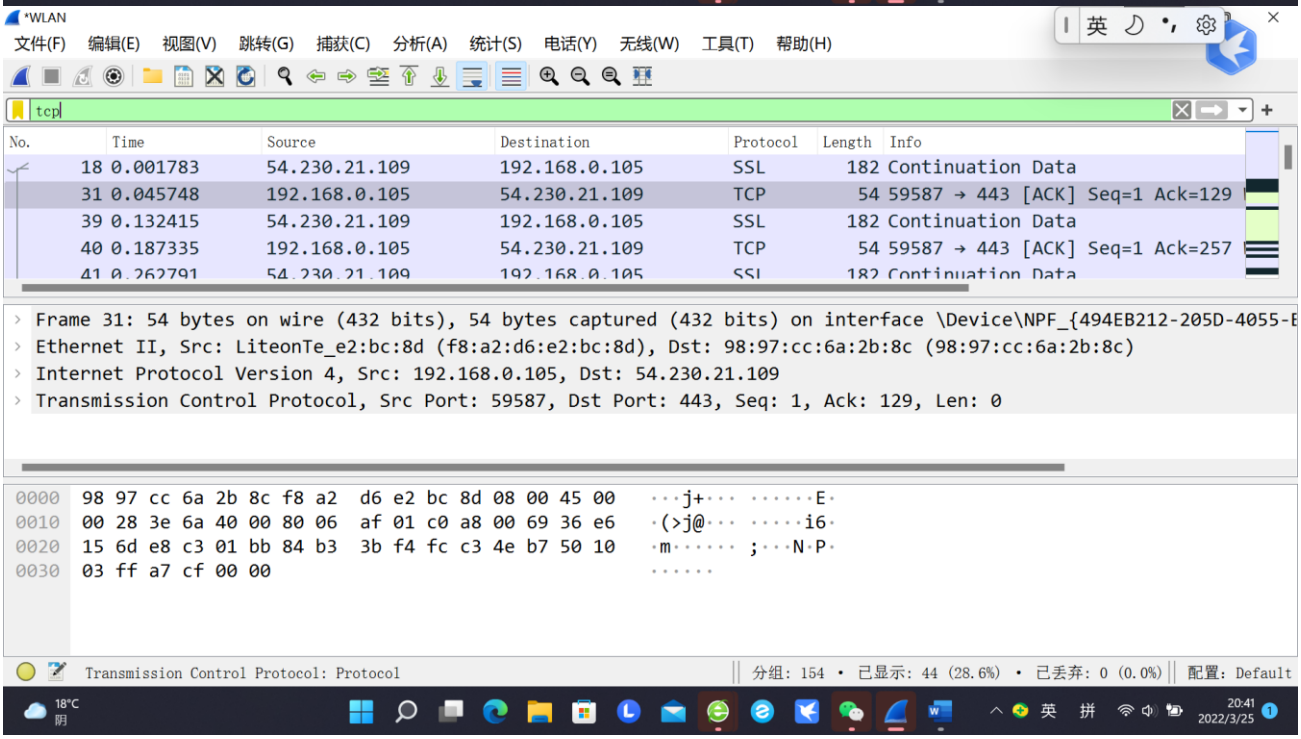

正在捕获 WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
No. Time Source Destination Protocol Length Info
2721 40.750841 54.230.21.109 192.168.0.105 TCP 182 [TCP Previous segment n
2722 40.750914 192.168.0.105 54.230.21.109 TCP 66 [TCP Dup ACK 2720#1]
2723 40.869513 54.230.21.109 192.168.0.105 TCP 182 443 → 59587 [ACK] Seq=385
2724 40.869570 192.168.0.105 54.230.21.109 TCP 66 [TCP Dup ACK 2720#2] 59587 → 443
2725 41.114937 54.230.21.109 192.168.0.105 TCP 182 443 → 59587 [ACK] Seq=38657 Ack=1 W
Frame 1: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface \Device\NPF_{494EB212-205D-40
Ethernet II, Src: LiteonTe_e2:bc:8d (f8:a2:d6:e2:bc:8d), Dst: 98:97:cc:6a:2b:8c (98:97:cc:6a:2b:8c)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 1.71.232.95
User Datagram Protocol, Src Port: 24824, Dst Port: 58381
Data (149 bytes)
0000 98 97 cc 6a 2b 8c f8 a2 d6 e2 bc 8d 08 00 45 00
0010 00 b1 57 8e 00 00 80 11 37 f6 c0 a8 00 69 01 47
0020 e8 5f 60 f8 e4 0d 00 9d f8 5f 96 51 95 95 c0 d1
0030 d1 e1 a8 86 f1 56 15 33 37 61 00 ff ea f8 60 d8
0040 b1 2b 32 2b 4e 00 f2 57 43 05 be 8c 15 5d 63 00

着色规则：


Wireshark · 着色规则 Default
名称 过滤器
Bad TCP tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.
HSRP State Change hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change stp.type == 0x80
OSPF State Change ospf.msg != 1
ICMP errors icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq
ARP arp
ICMP icmp || icmpv6
TCP RST tcp.flags.reset eq 1
SCTP ABORT sctp.chunk_type eq ABORT
TTL low or unexpected (! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst =
Checksum Errors eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum
SMB smb || nbss || nbns || netbios
HTTP http || tcp.port == 80 || http2
DCERPC dcerpc
Routing hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN tcp.flags & 0x02 || tcp.flags.fin == 1
双击编辑。拖拽移动。规则按顺序进行处理，直到找到一个匹配的。
OK 复制自 Cancel Import··· Export··· Help

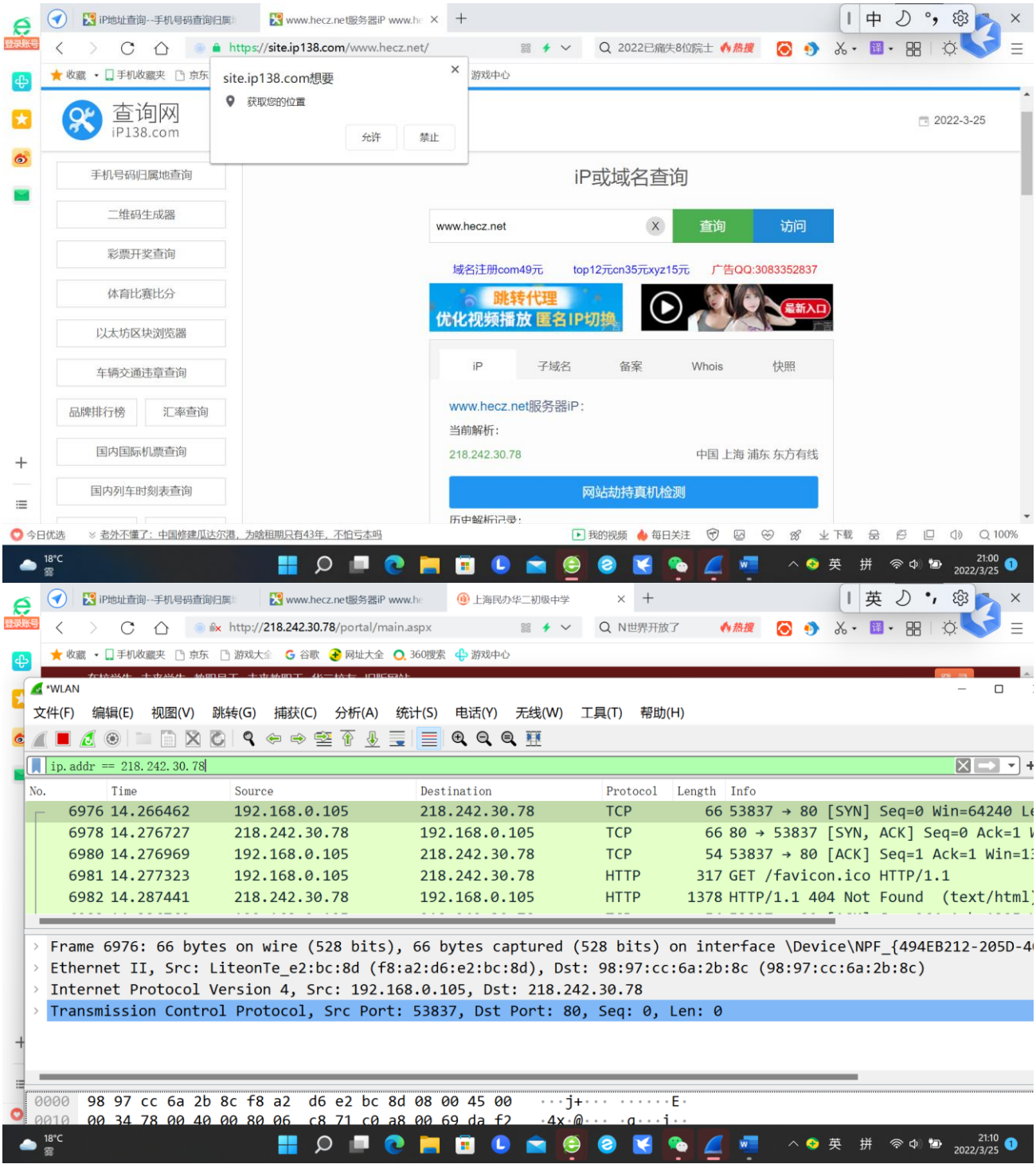
过滤器：



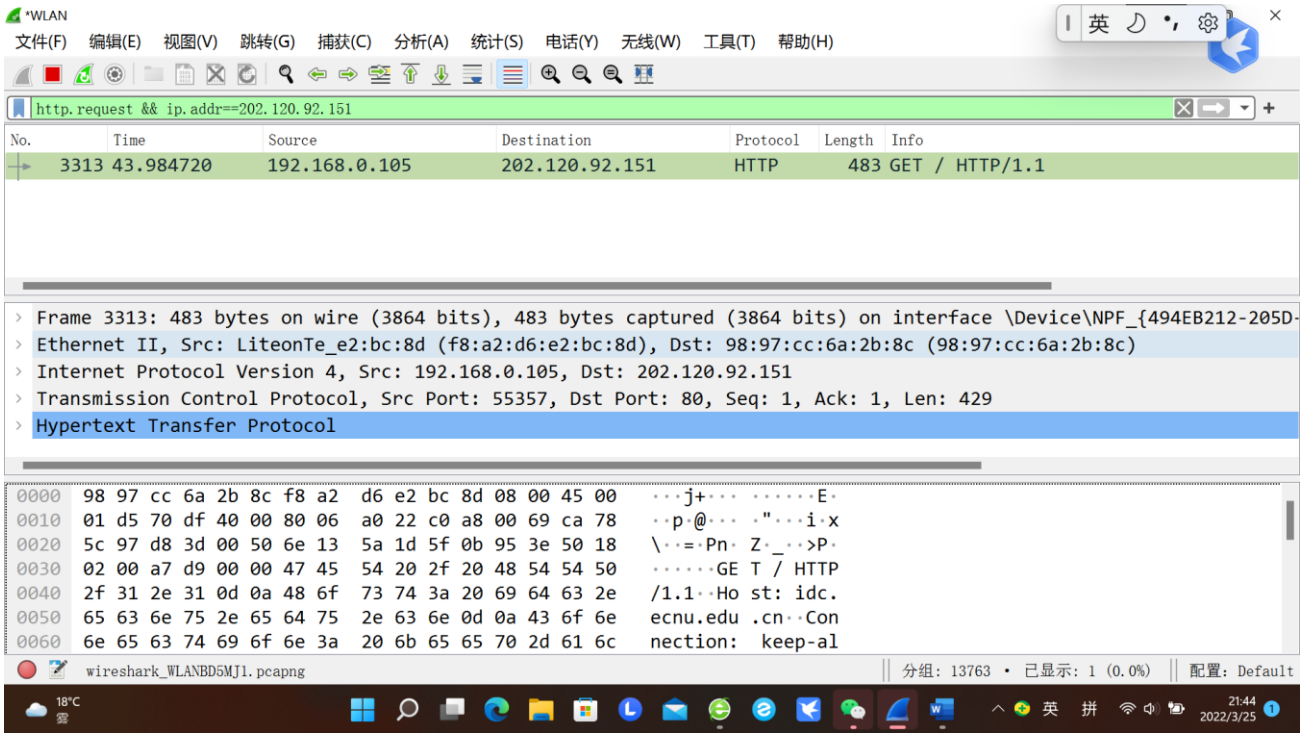


3.3 WireShark 抓包获取网站登录信息

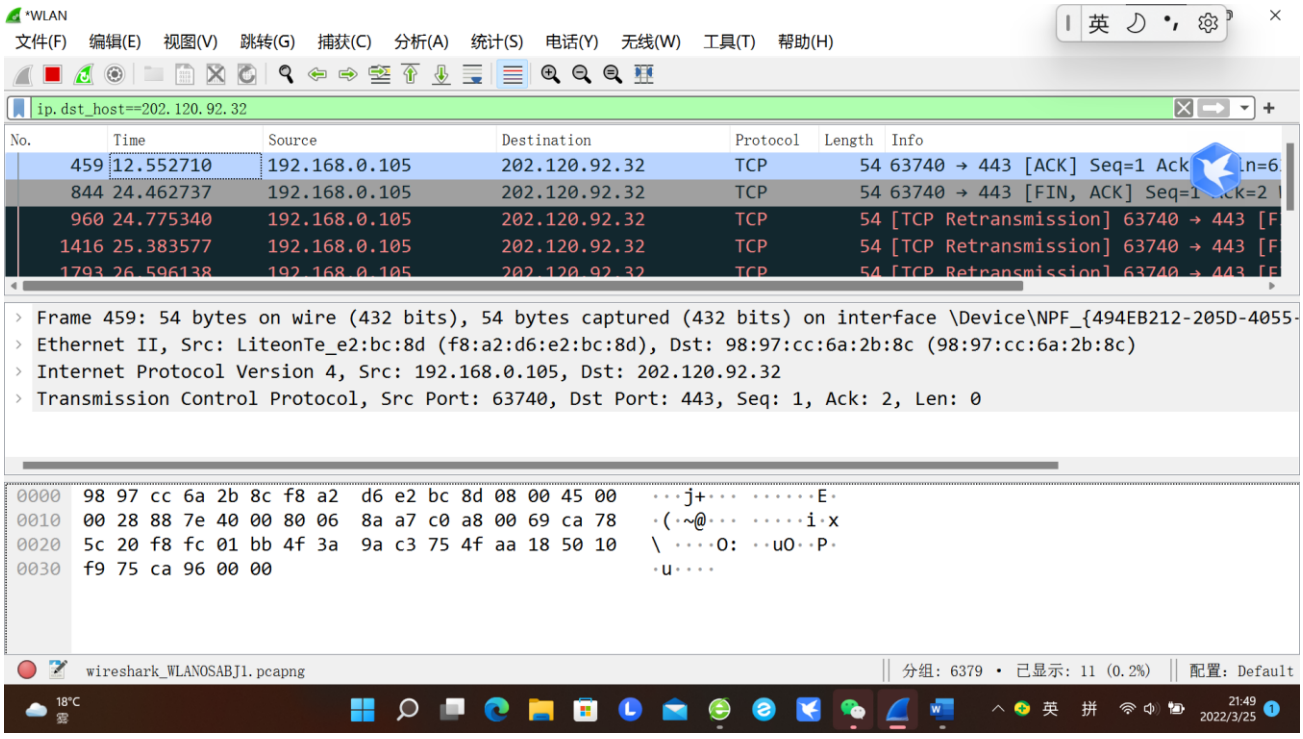
明文：


site.ip138.com想要
获取您的位置
允许
禁止
查询网
iP138.com
iP或域名查询
www.hecz.net
查询
访问
www.hecz.net服务器iP:
当前解析:
218.242.30.78
中国 上海 浦东 东方有线
网站劫持真机检测
*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
ip.addr == 218.242.30.78
No. Time Source Destination Protocol Length Info
6976 14.266462 192.168.0.105 218.242.30.78 TCP 66 53837 → 80 [SYN] Seq=0 Win=64240
6978 14.276727 218.242.30.78 192.168.0.105 TCP 66 80 → 53837 [SYN, ACK] Seq=0 Ack=1
6980 14.276969 192.168.0.105 218.242.30.78 TCP 54 53837 → 80 [ACK] Seq=1 Ack=1 Win=1
6981 14.277323 192.168.0.105 218.242.30.78 HTTP 317 GET /favicon.ico HTTP/1.1
6982 14.287441 218.242.30.78 192.168.0.105 HTTP 1378 HTTP/1.1 404 Not Found (text/html
Frame 6976: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{494EB212-205D-4
Ethernet II, Src: LiteonTe_e2:bc:8d (f8:a2:d6:e2:bc:8d), Dst: 98:97:cc:6a:2b:8c (98:97:cc:6a:2b:8c)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 218.242.30.78
Transmission Control Protocol, Src Port: 53837, Dst Port: 80, Seq: 0, Len: 0
0000 98 97 cc 6a 2b 8c f8 a2 d6 e2 bc 8d 08 00 45 00
0010 00 34 78 00 40 00 80 06 c8 71 c0 a8 00 69 da f2

明文：



密文：



五、总结

通过本次实验，我安装了 WireShark 并初步熟悉了它的使用方法，为以后的实验和课程项目打下了基础。