network-top to down

实验一：

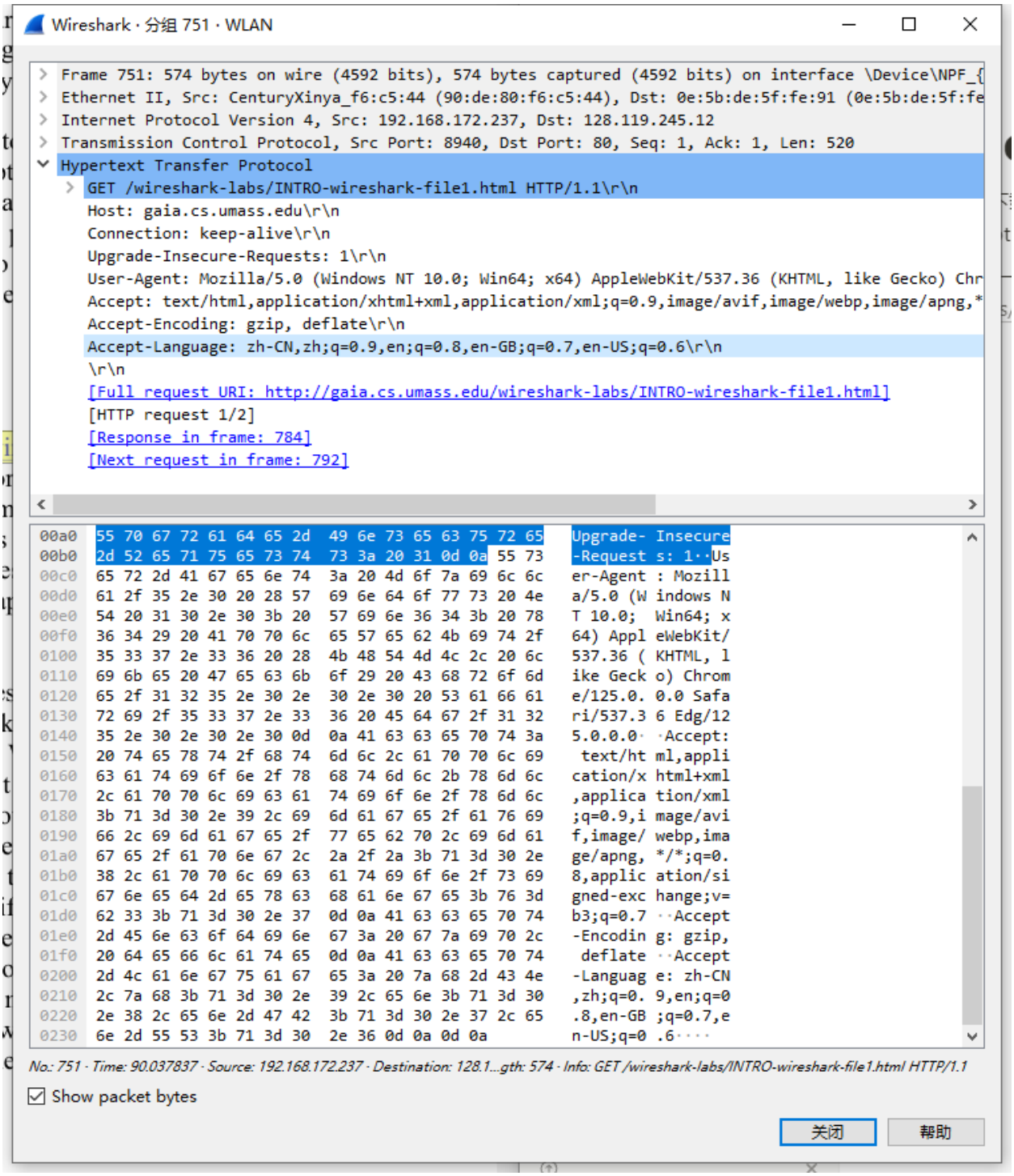
下载wireshark 它是一个数据包嗅探器 实际上是由一个数据包capture和数据包analyse library 组成

第一个实验去抓取访问http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html这个网站时发送接受的数据包

ps：我尝试了好几次都不成功，都未能抓取到该packet

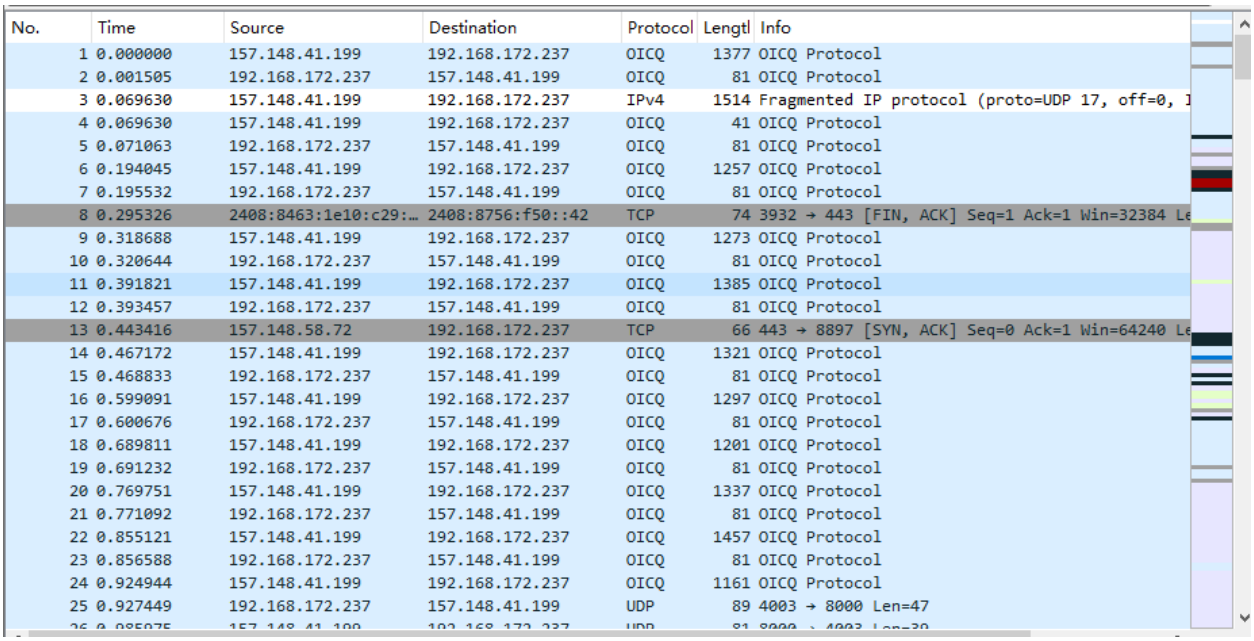
1：不要开代理，因为我一直挂着机场的原因，只能看到抓取到一个发往机场的数据包

2：要分浏览器，我关闭代理之后还未成功？因为我使用的是Google，连发送出去的packet都抓不到！后面使用edge成功



problem：

1.列出未过滤的协议栏中出现的3个不同的协议上面步骤 7 中的数据包列表窗口。



No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000	157.148.41.199	192.168.172.237	OICQ	1377	OICQ Protocol
2	0.001505	192.168.172.237	157.148.41.199	OICQ	81	OICQ Protocol
3	0.069630	157.148.41.199	192.168.172.237	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, I
4	0.069630	157.148.41.199	192.168.172.237	OICQ	41	OICQ Protocol
5	0.071063	192.168.172.237	157.148.41.199	OICQ	81	OICQ Protocol
6	0.194045	157.148.41.199	192.168.172.237	OICQ	1257	OICQ Protocol
7	0.195532	192.168.172.237	157.148.41.199	OICQ	81	OICQ Protocol
8	0.295326	2408:8463:1e10:c29:…	2408:8756:f50::42	TCP	74	3932 → 443 [FIN, ACK] Seq=1 Ack=1 Win=32384 Le
9	0.318688	157.148.41.199	192.168.172.237	OICQ	1273	OICQ Protocol
10	0.320644	192.168.172.237	157.148.41.199	OICQ	81	OICQ Protocol
11	0.391821	157.148.41.199	192.168.172.237	OICQ	1385	OICQ Protocol
12	0.393457	192.168.172.237	157.148.41.199	OICQ	81	OICQ Protocol
13	0.443416	157.148.58.72	192.168.172.237	TCP	66	443 → 8897 [SYN, ACK] Seq=0 Ack=1 Win=64240 Le
14	0.467172	157.148.41.199	192.168.172.237	OICQ	1321	OICQ Protocol
15	0.468833	192.168.172.237	157.148.41.199	OICQ	81	OICQ Protocol
16	0.599091	157.148.41.199	192.168.172.237	OICQ	1297	OICQ Protocol
17	0.600676	192.168.172.237	157.148.41.199	OICQ	81	OICQ Protocol
18	0.689811	157.148.41.199	192.168.172.237	OICQ	1201	OICQ Protocol
19	0.691232	192.168.172.237	157.148.41.199	OICQ	81	OICQ Protocol
20	0.769751	157.148.41.199	192.168.172.237	OICQ	1337	OICQ Protocol
21	0.771092	192.168.172.237	157.148.41.199	OICQ	81	OICQ Protocol
22	0.855121	157.148.41.199	192.168.172.237	OICQ	1457	OICQ Protocol
23	0.856588	192.168.172.237	157.148.41.199	OICQ	81	OICQ Protocol
24	0.924944	157.148.41.199	192.168.172.237	OICQ	1161	OICQ Protocol
25	0.927449	192.168.172.237	157.148.41.199	UDP	89	4003 → 8000 Len=47

2、从发送HTTP GET报文到HTTP报文返回需要多长时间
OK 收到回复了吗？（默认情况下，数据包中时间列的值
列表窗口是自 Wireshark 跟踪开始以来的时间量（以秒为单位）。
要以一天中的时间格式显示“时间”字段，请选择“Wireshark 视图”拉动
向下菜单，然后选择时间显示格式，然后选择当天时间。）

```
23:52:32.425118
23:52:32.756178
```

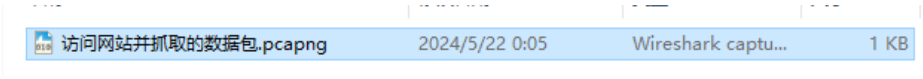
3. gaia.cs.umass.edu 的互联网地址是什么（也称为 www-
net.cs.umass.edu）？ 您计算机的互联网地址是什么？

```
Source Address: 192.168.172.237
Destination Address: 128.119.245.12
```

```
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
```

4. 打印上面问题 2 中提到的两条 HTTP 消息（GET 和 OK）。 到
为此，请从 Wireshark 文件命令菜单中选择打印，然后选择

“仅选定的数据包”和“按显示打印”单选按钮，然后单击
好的



实验二：