此次试验产生的文件记录



查看本机的ip、mac，网关的ip、mac。

2016-11-11 14:42:16

Microsoft Windows [版本 6.1.7601]

版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ipconfig -all

Windows IP 配置

主机名 . . . . . . . . . . . . . : PC-063

主 DNS 后缀 . . . . . . . . . . . :

节点类型 . . . . . . . . . . . . : 混合

IP 路由已启用 . . . . . . . . . . : 否

WINS 代理已启用 . . . . . . . . . : 否

以太网适配器 本地连接:

连接特定的 DNS 后缀 . . . . . . . :

描述. . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller

物理地址. . . . . . . . . . . . . : B8-AE-ED-F7-D7-AF

DHCP 已启用 . . . . . . . . . . . : 否

自动配置已启用. . . . . . . . . . : 是

本地链接 IPv6 地址. . . . . . . . : fe80::18c7:c47d:77e0:6731%10(首选)

IPv4 地址 . . . . . . . . . . . . : 202.202.243.73(首选)

子网掩码 . . . . . . . . . . . . : 255.255.255.128

默认网关. . . . . . . . . . . . . : 202.202.243.1

DHCPv6 IAID . . . . . . . . . . . : 246984429

DHCPv6 客户端 DUID . . . . . . . : 00-01-00-01-1E-72-CF-90-B8-AE-ED-F7-CF-1B

DNS 服务器 . . . . . . . . . . . : 202.202.240.33

TCPIP 上的 NetBIOS . . . . . . . : 已启用

隧道适配器 isatap.{5BCD5D49-4309-4EAB-9278-31B726C3427A}:

媒体状态 . . . . . . . . . . . . : 媒体已断开

连接特定的 DNS 后缀 . . . . . . . :

描述. . . . . . . . . . . . . . . : Microsoft ISATAP Adapter

物理地址. . . . . . . . . . . . . : 00-00-00-00-00-00-00-E0

DHCP 已启用 . . . . . . . . . . . : 否

自动配置已启用. . . . . . . . . . : 是

隧道适配器 6TO4 Adapter:

连接特定的 DNS 后缀 . . . . . . . :

描述. . . . . . . . . . . . . . . : Microsoft 6to4 Adapter

物理地址. . . . . . . . . . . . . : 00-00-00-00-00-00-00-E0

DHCP 已启用 . . . . . . . . . . . : 否

自动配置已启用. . . . . . . . . . : 是

IPv6 地址 . . . . . . . . . . . . : 2002:caca:f349::caca:f349(首选)

默认网关. . . . . . . . . . . . . : 2002:c058:6301::c058:6301

DNS 服务器 . . . . . . . . . . . : 202.202.240.33

TCPIP 上的 NetBIOS . . . . . . . : 已禁用

C:\Users\Administrator>arp -a

接口: 202.202.243.73 --- 0xa

Internet 地址 物理地址 类型

202.202.243.1 00-1a-a9-0e-c0-d7 动态

202.202.243.2 00-25-64-fd-32-ba 动态

202.202.243.33 c0-3f-d5-5e-2c-1f 动态

202.202.243.37 c0-3f-d5-5e-2c-16 动态

202.202.243.38 c0-3f-d5-5e-2a-ba 动态

202.202.243.39 c0-3f-d5-5e-2a-94 动态

202.202.243.44 c0-3f-d5-5e-01-c0 动态

202.202.243.62 c8-9c-dc-a3-f7-97 动态

202.202.243.74 b8-ae-ed-f7-d4-8d 动态

202.202.243.127 ff-ff-ff-ff-ff-ff 静态

224.0.0.22 01-00-5e-00-00-16 静态

224.0.0.252 01-00-5e-00-00-fc 静态

228.192.90.222 01-00-5e-40-5a-de 静态

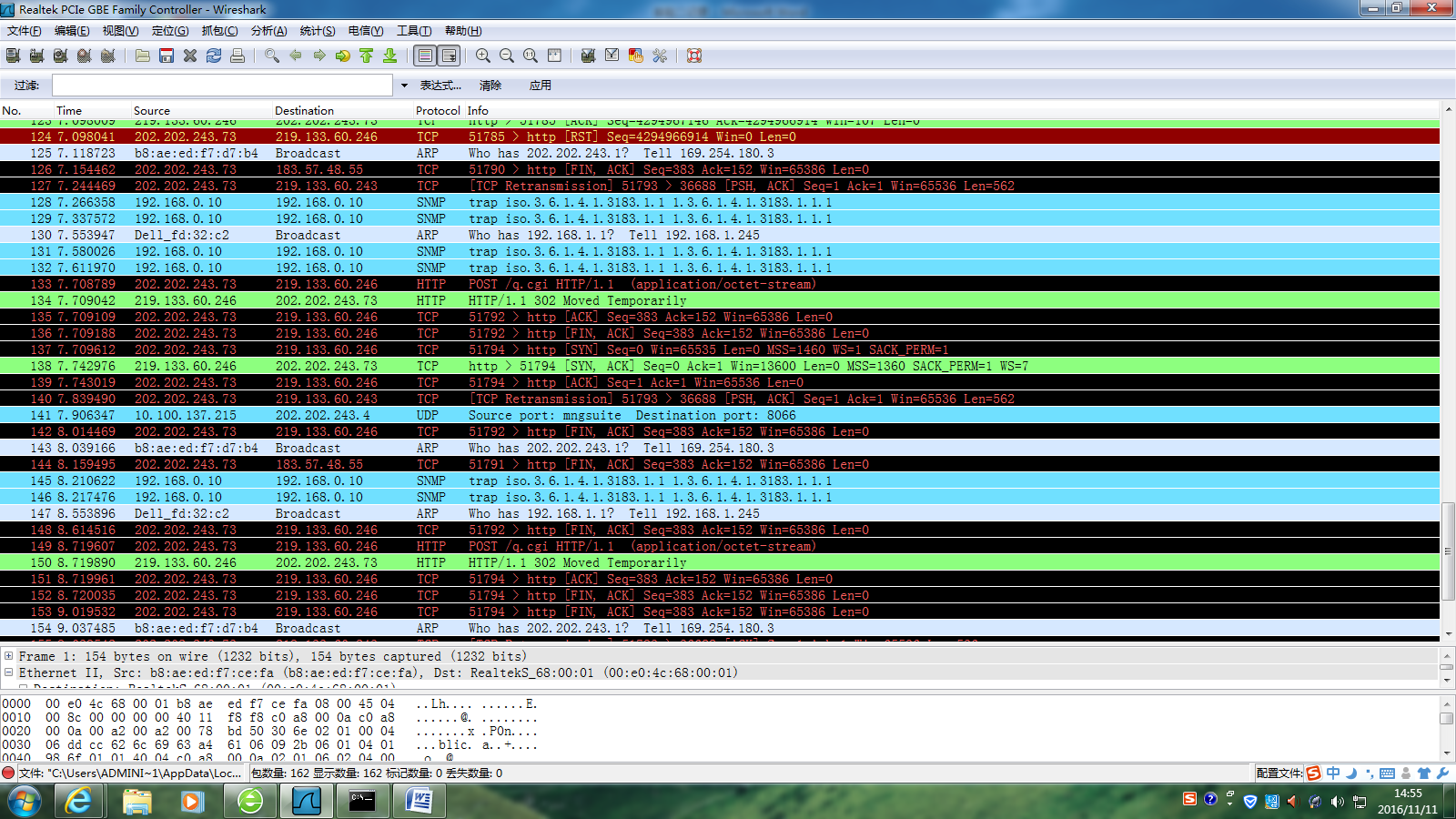
239.192.152.143 01-00-5e-40-98-8f 静态

239.255.255.250 01-00-5e-7f-ff-fa 静态

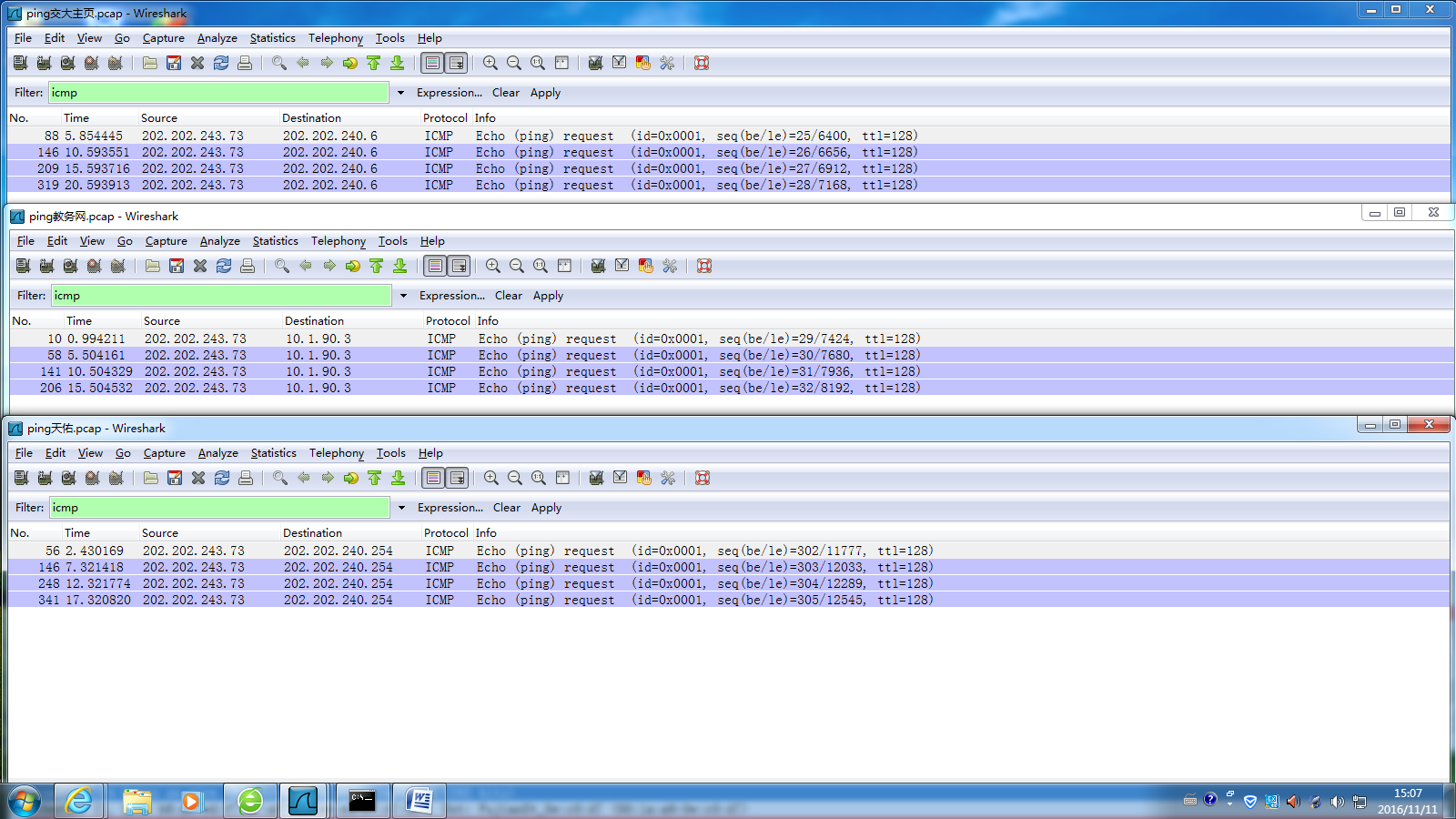
255.255.255.255 ff-ff-ff-ff-ff-ff 静态

C:\Users\Administrator>

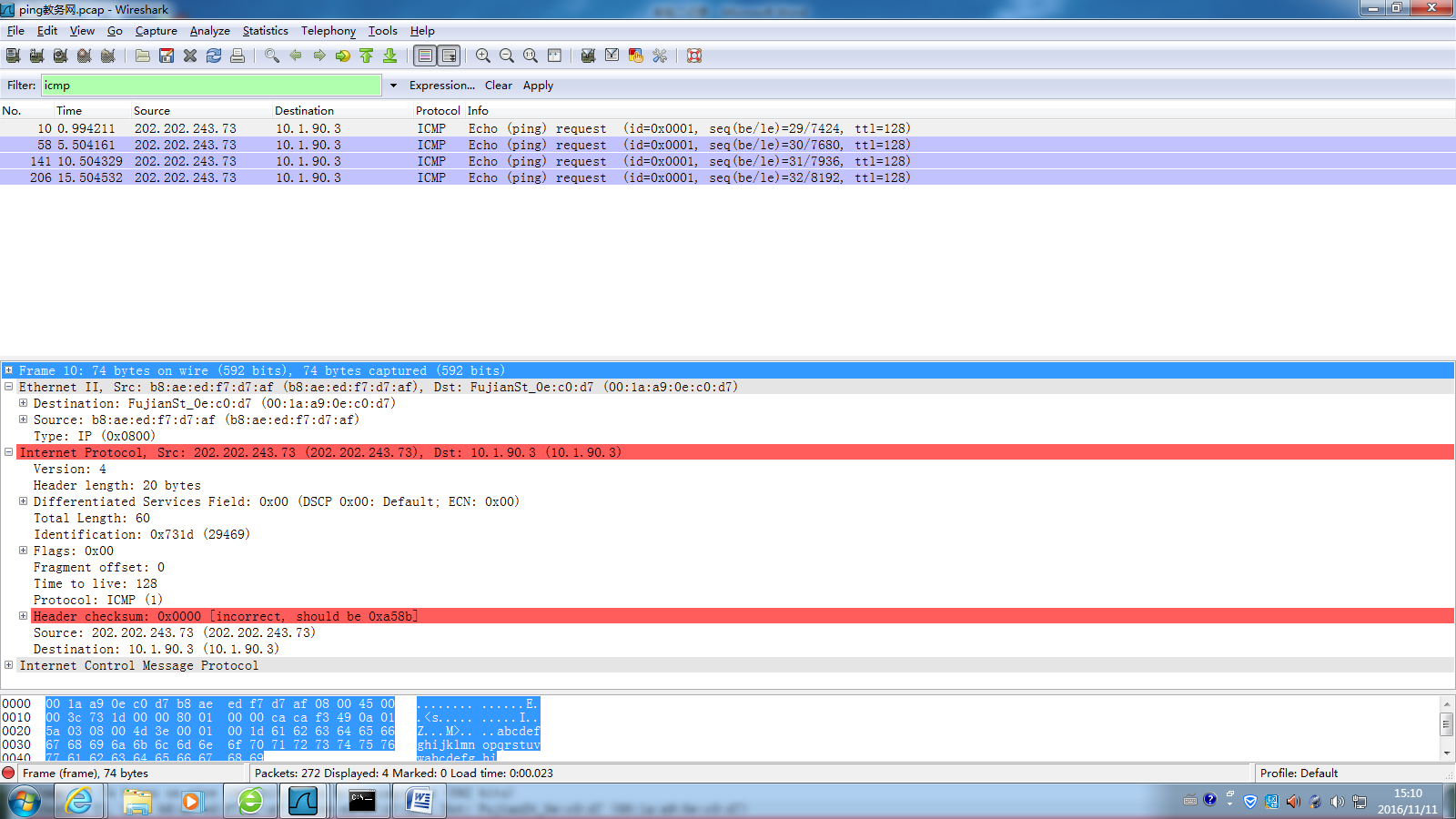
每次都会抓到大量的死包，严重的影响了我查看，所以必须根据协议过滤，对ping采用icmp过滤



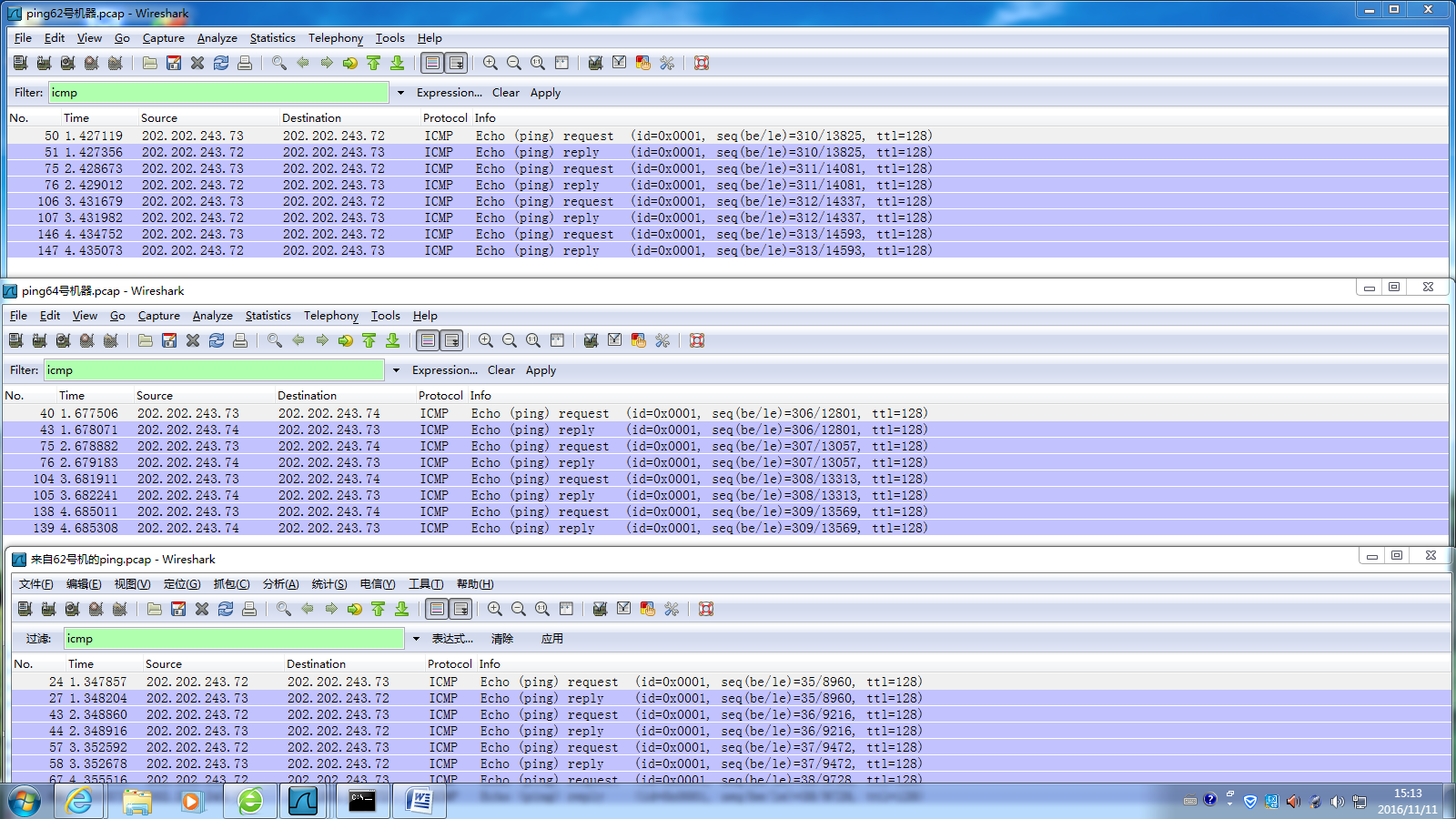
ping交大主页、教务网、天佑抓包记录



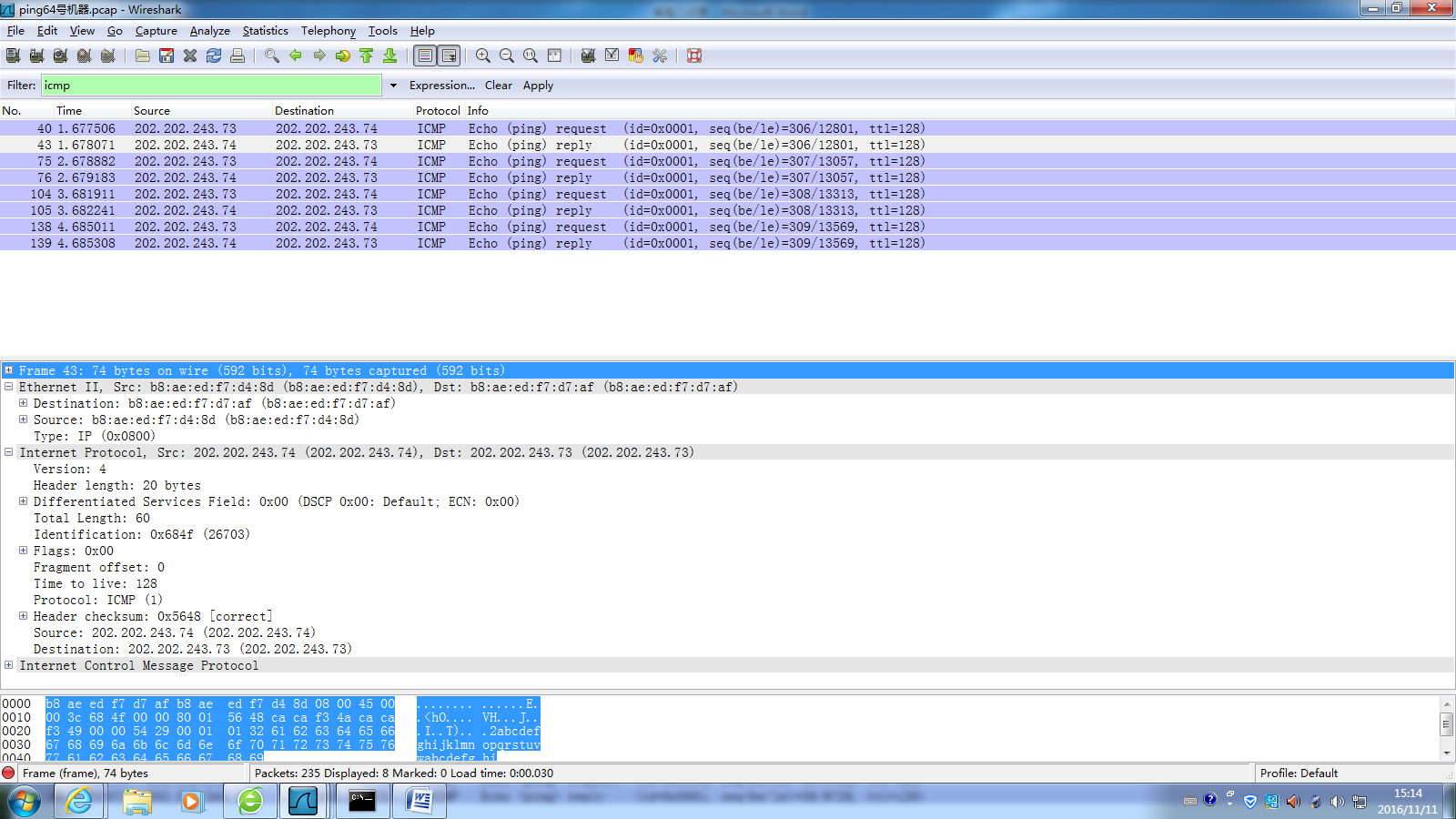
ping的结果相同，下面列出ping教务网的记录



Ping62、64号机器和来自62号机器的ping抓包记录



列出ping64号机器的记录



用Wireshark查看你访问旁边计算机的帧，发出帧的目的MAC地址以及返回帧的源MAC地址是什么？

目的：b8:ae:ed:f7:d4:8d (64号机) b8:ae:ed:f7:d4:f2

源：b8:ae:ed:f7:d7:af (本机)

目的：b8:ae:ed:f7:d4:f2 (62号机)

源：b8:ae:ed:f7:d7:af (本机)

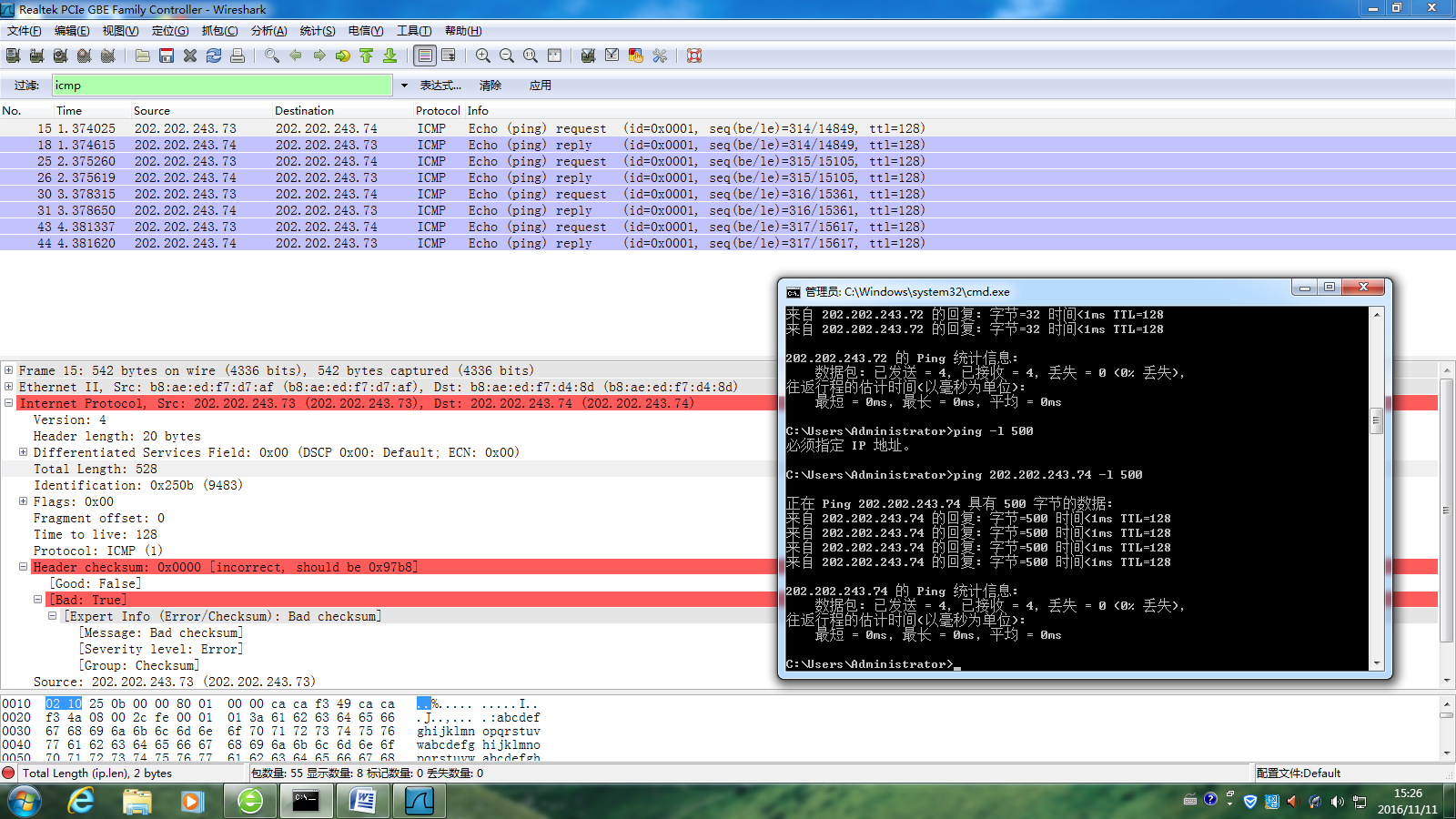
用Wireshark查看你访问天佑和教务网站的帧，发出帧的目的MAC地址以及返回帧的源MAC地址是什么，为什么？

目的：00:1a:a9:0e:c0:d7 (网关)我猜着应该是在通信子网外的传输，都交给网关去做。

源：b8:ae:ed:f7:d7:af (本机)

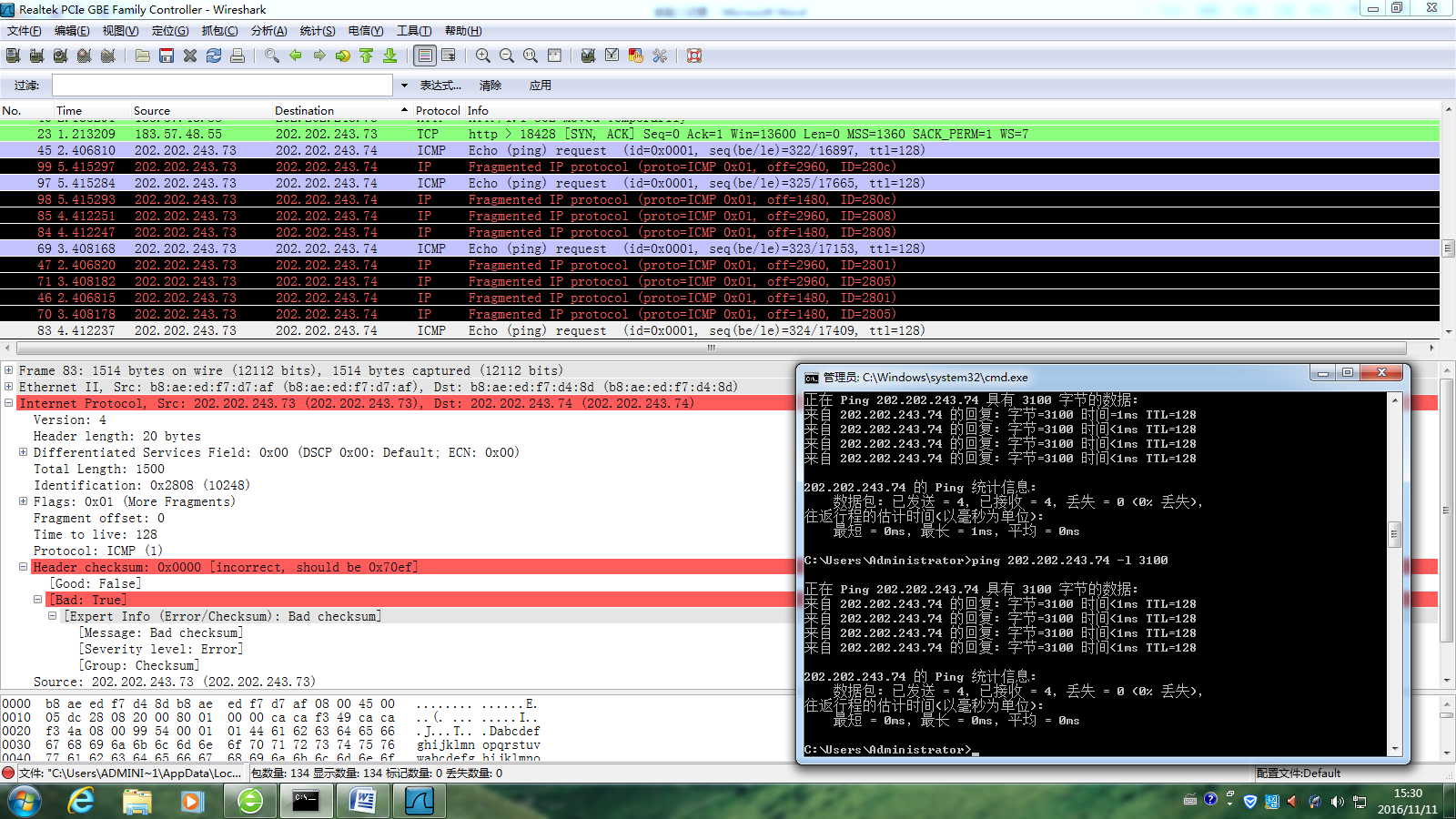
进行Ping命令各种选项的运行，对-l参数进行Wireshark分析，了解IP包的分段。

ping 202.202.243.74 -l 500------------------------------- Total Length: 528



ping 202.202.243.74 -l 3100------------------------------- Total Length: 1500、168

有坏包。



-------------下机---------------2016-11-11 15:31:14