浙江大学

本科实验报告

课程名称：	计算机网络基础
姓　　名：	葛现隆
学　　院：	计算机科学与技术学院
系：	计算机系
专　　业：	计算机科学与技术专业
学　　号：	3120102146
指导教师：	陆魁军 陈辉

2015 年 4 月 30 日

浙江大学实验报告

课程名称：计算机网络基础　　实验类型：综合性实验

实验项目名称：使用 Ethereal 分析 Ethernet 帧及高层协议

学生姓名：葛现隆　　专业：计科　　学号：3120102146

同组学生姓名：无　　指导老师：陆魁军

实验地点：曹西软件学院机房　　实验日期：2015 年 4 月 30 日

一、　实验目的和要求：

熟悉掌握 Ethereal 软件的使用,并应用该软件分析 Ethernet 帧以及高级协议，从而能够加深对 TCP/IP 协议栈上的参与通信的网络数据包结构以及通信方式有进一步的了解。

二、　实验内容和原理

1. 安装 windows 下的 Ethereal 及 WinPcap 软件。

2. 捕捉任何主机发出的 Ethernet 802.3 格式的帧（帧的长度字段<=1500）， Ethereal 的 capture filter 的 filter string 设置为：ether[12:2] <= 1500

捕捉任何主机发出的 DIX Ethernet V2（即 Ethernet II）格式的帧（帧的长度字段>1500, 帧的长度字段实际上是类型字段）， Ethereal 的 capture filter 的 filter string 设置为：ether[12:2] > 1500

(1)观察并分析帧结构，802.3 格式的帧的上一层主要是哪些 PDU？是 IP、LLC 还是其它哪种？

(2)观察并分析帧结构，Ethernet II 的帧的上一层主要是哪些 PDU？是 IP、LLC 还是其它哪种？

3. 捕捉并分析局域网上的所有 ethernet broadcast 帧，Ethereal 的 capture filter 的 filter string 设置为：ether broadcast

(1). 观察并分析哪些主机在发广播帧，这些帧的高层协议是什么？**普通穿透 HUB 广播可以穿透交换机 netbios-ns**

(2). 你的 LAN 的共享网段上连接了多少台计算机？1 分钟内有几个广播帧？有否发生广播风暴？

4. 捕捉局域网上的所有 ethernet multicast 帧，Ethereal 的 capture filter 的 filter string 设置为：ether multicast

(1). 观察并分析哪些节点在发 multicast 帧，这些帧的高层协议是什么？ARP

5. 捕捉局域网上主机 10.14.26.53 发出或接受的所有 ARP 包，Ethereal 的 capture filter 的 filter string 设置为：arp host 10.14.26.53.

(1)主机 10.14.26.53 上执行 ”arp –d *” 清楚 arp cache.

(2)在主机 10.14.26.53 上 ping 局域网上的另一主机（例如 10.14.26.54）

(3)观察并分析主机 10.14.26.53 发出或接受的所有 ARP 包，及 arp 包结构。

6. 捕捉局域网上的所有 IP 广播包，Ethereal 的 capture filter 的 filter string 设置为：ip broadcast

(1). 观察并分析哪些节点在发广播包，这些包的高层协议是什么？

7. 捕捉局域网上的所有 IP 组播包，Ethereal 的 capture filter 的 filter string 设置为： ip multicast

(1). 观察并分析哪些节点在发组播包，这些包的高层协议是什么？

8. 捕捉局域网上的所有 icmp 包，Ethereal 的 capture filter 的 filter string 设置为：icmp

(1). 在主机 10.14.26.53 上 ping 局域网上的另一主机（例如 10.14.26.54）。

(2). 观察并分析主机 10.14.26.53 发出或接受的所有 icmp 包，及 icmp 包的类型和结构。

9. 捕捉主机 10.14.26.53 和 www 服务器 www.zju.edu.cn 之间的通信（这里主机 10.14.26.53 可以是自身，也可以是通过普通 HUB（而不是交换机）与本机相连的 LAN 上的其它主机或路由器, IP 地址也不要求一定是 10.14.26.53, 下同），Ethereal 的 capture filter 的 filter string 设置为：host 10.14.26.53 and www.zju.edu.cn

(1)主机 10.14.26.53 用 IE 访问 www 服务器 www.zju.edu.cn。

(2)观察并分析 10.14.26.53 和 www 服务器 www.zju.edu.cn 之间传输的 Ethernet II (即 DIX Ethernet v2) 帧结构，IP 数据报结构，TCP segment 结构，HTTP PDU 结构。

(3)观察并分析 10.14.26.53 和 www 服务器 www.zju.edu.cn 之间建立 TCP 连接时的三次握手过程。

10. 捕捉局域网上主机 10.14.26.53 发出或接受的所有 FTP 包（即 src or dst port＝21），Ethereal 的 capture filter 的 filter string 设置为：

tcp port 21 and host 10.14.26.53

(1). 在主机 10.14.26.53 上用 FTP 客户端软件访问 FTP server。

(2). 观察并分析 10.14.26.53 和 FTP server 之间传输的 Ethernet II (即 DIX Ethernet v2) 帧结构，IP 数据报结构，TCP segment 结构。

(3). 观察并分析 FTP PDU 名称和结构。注意 10.14.26.53 发出的 FTP request PDU 中以 USER 开头、以 PASS 开头的两个 PDU，他们包含了什么信息？对 INTERNET 的 FTP 协议的安全性作出评价。

11. 捕捉局域网上主机 10.14.26.53 发出或接受的所有 POP 包（即 src port 110 or dst port 110），Ethereal 的 capture filter 的 filter string 设置为：

tcp port 110 and host 10.14.26.53

(1). 在主机 10.14.26.53 上用 outlook express 或 foxmail 收取邮件。

(2). 观察并分析 10.14.26.53 和 MAIL server 之间传输的 Ethernet II (即 DIX Ethernet v2) 帧结构，IP 数据报结构，TCP segment 结构。

(3). 观察并分析 POP3 PDU 名称和结构。注意 10.14.26.53 发出的 POP3 request PDU 中以 USER 开头、以 PASS 开头的两个 PDU，他们包含了什么信息？对 INTERNET 的 EMAIL 软件的安全性作出评价。

三、 主要仪器设备

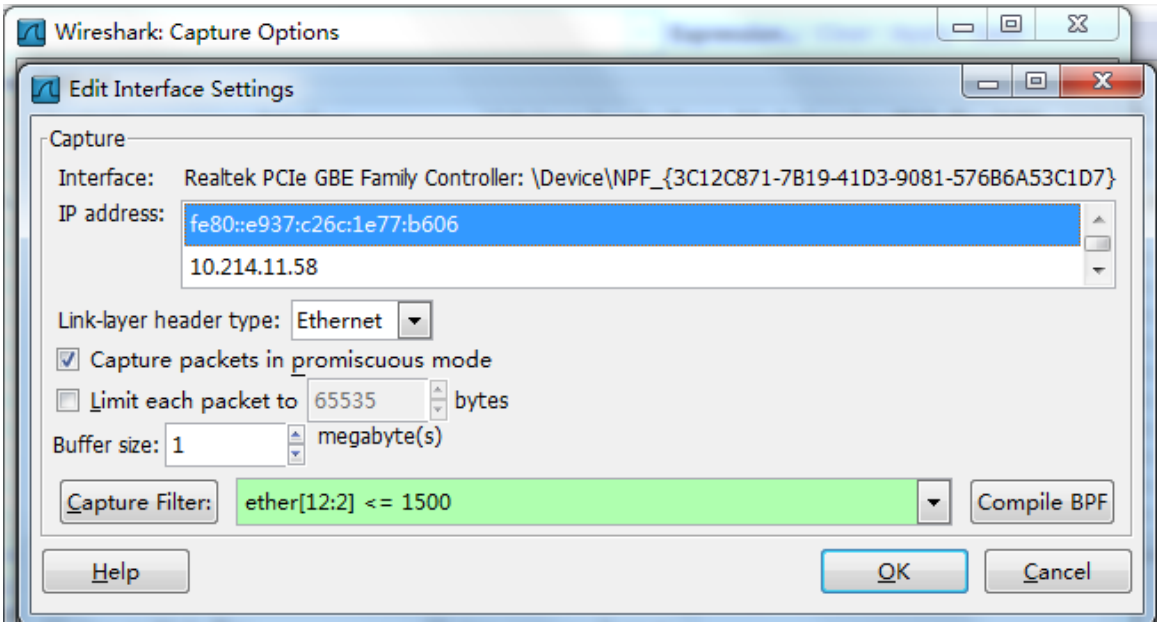
包嗅探及协议分析软件 Ethereal，联网的 PC 机。

四、 操作方法与实验步骤

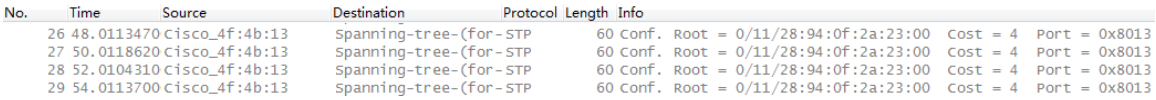
1. 安装 WinPcap

2. Ethernet 802.3 格式的帧

设置

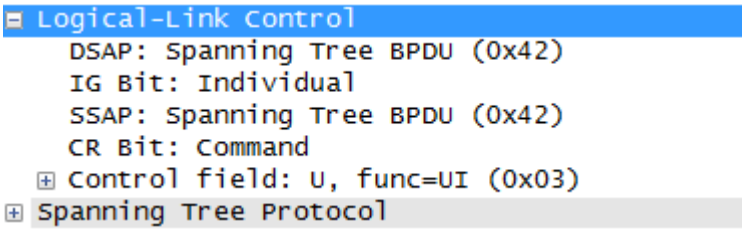


抓包



No.	Time	Source	Destination	Protocol	Length	Info
26	48.0113470	Cisco_4f:4b:13	Spanning-tree-(for-STP		60	Conf. Root = 0/11/28:94:0f:2a:23:00 Cost = 4 Port = 0x8013
27	50.0118620	Cisco_4f:4b:13	Spanning-tree-(for-STP		60	Conf. Root = 0/11/28:94:0f:2a:23:00 Cost = 4 Port = 0x8013
28	52.0104310	Cisco_4f:4b:13	Spanning-tree-(for-STP		60	Conf. Root = 0/11/28:94:0f:2a:23:00 Cost = 4 Port = 0x8013
29	54.0113700	Cisco_4f:4b:13	Spanning-tree-(for-STP		60	Conf. Root = 0/11/28:94:0f:2a:23:00 Cost = 4 Port = 0x8013

由图片分析可知，802.3 格式的帧的上一层主要是 LLC。



Ethernet II 的帧，同样设置判断条件

15	16.7624810	10.214.11.22	224.0.0.252	LLMNR	64	Standard query 0xfcf0 A wpad
16	16.9103890	Cisco_4f:4b:48	e0:3f:49:b4:89:4a	ARP	60	Who has 10.214.11.33? Tell 10.214.11.1
17	16.9184470	fe80::85f9:6cf7:b79	ff02::1:2	DHCPv6	150	Solicit XID: 0x814568 CID: 0001000119a6b09374d02b7a179f
18	16.9655660	10.214.11.22	10.214.11.255	NBNS	92	Name query NB WPAD<00>
19	17.7297040	10.214.11.22	10.214.11.255	NBNS	92	Name query NB WPAD<00>
20	18.2479590	fe80::3c79:c631:23c	ff02::1:2	DHCPv6	150	Solicit XID: 0xa13c71 CID: 0001000119a6a6e874d02b7c5cb2
21	18.2663070	114.112.83.218	10.214.11.58	TCP	60	http > intuitive-edge [FIN, ACK] Seq=1 Ack=1 Win=31 Len=0
22	18.2664300	10.214.11.58	114.112.83.218	TCP	54	intuitive-edge > http [ACK] Seq=1 Ack=2 Win=258 Len=0
23	18.4938760	10.214.11.22	10.214.11.255	NBNS	92	Name query NB WPAD<00>

有 UDP，ARP，TCP，IP 等上层。

IP

```
⊞ Frame 81: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_7a:17:96 (74:d0:2b:7a:17:96), Dst: IPv6mcast_00:00:00:16 (3
⊞ Internet Protocol Version 6, Src: fe80::cdce:b706:2775:2691 (fe80::cdce:b706:2775:2691
⊞ Internet Control Message Protocol v6
```

UDP

```
⊞ Frame 83: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_7a:17:96 (74:d0:2b:7a:17:96), Dst: IPv4mcast_00:00:fc (01:
⊞ Internet Protocol Version 4, Src: 10.214.11.52 (10.214.11.52), Dst: 224.0.0.252 (224.
⊞ User Datagram Protocol, Src Port: 58919 (58919), Dst Port: llmnr (5355)
⊞ Link-local Multicast Name Resolution (query)
```

ARP

```
⊞ Frame 61: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_7a:17:96 (74:d0:2b:7a:17:96), Dst: Broadcast (ff:ff:ff:ff
⊞ Address Resolution Protocol (request)
```

3. Ether broadcast

1) 高层协议有 DHCP, ARP，发送广播包的主机有：

10.214.11.22
10.214.11.59
10.214.11.28
10.214.11.36
10.214.11.1
0.0.0.0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.214.11.22	10.214.11.255	NBNS	92	Name query NB WPAD<00>
2	0.76420500	10.214.11.22	10.214.11.255	NBNS	92	Name query NB WPAD<00>
3	1.52857800	10.214.11.22	10.214.11.255	NBNS	92	Name query NB WPAD<00>
4	32.1911080	10.214.11.59	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xea18f271
5	32.4969720	10.214.11.59	10.214.11.255	NBNS	92	Name query NB WPAD<00>
6	33.2463630	10.214.11.59	10.214.11.255	NBNS	92	Name query NB WPAD<00>
7	33.6642780	0.0.0.0	255.255.255.255	DHCP	348	DHCP Request - Transaction ID 0x2d4c4397
8	33.6650200	10.214.11.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x2d4c4397
9	33.6693000	AsustekC_7e:86:7b	Broadcast	ARP	60	Who has 10.214.11.1? Tell 10.214.11.36
10	33.6914090	AsustekC_7a:10:75	Broadcast	ARP	60	Who has 10.214.11.36? Tell 10.214.11.28
11	33.7238080	AsustekC_7e:86:7b	Broadcast	ARP	60	Who has 10.214.11.36? Tell 0.0.0.0
12	33.9966240	10.214.11.59	10.214.11.255	NBNS	92	Name query NB WPAD<00>
13	34.2307420	AsustekC_7e:86:7b	Broadcast	ARP	60	Who has 10.214.11.1? Tell 10.214.11.36
14	34.2421750	AsustekC_7e:86:7b	Broadcast	ARP	60	Who has 10.214.11.1? Tell 10.214.11.36
15	34.7221410	AsustekC_7e:86:7b	Broadcast	ARP	60	Who has 10.214.11.36? Tell 0.0.0.0
16	34.7261090	AsustekC_7e:86:7b	Broadcast	ARP	60	Who has 10.214.11.1? Tell 10.214.11.36
17	35.7204950	AsustekC_7e:86:7b	Broadcast	ARP	60	Who has 10.214.11.36? Tell 0.0.0.0
18	36.7188680	AsustekC_7e:86:7b	Broadcast	ARP	60	Gratuitous ARP for 10.214.11.36 (Request)
19	36.7256760	AsustekC_7e:86:7b	Broadcast	ARP	60	Who has 10.214.11.1? Tell 10.214.11.36
20	37.0086310	AsustekC_7a:10:75	Broadcast	ARP	60	Who has 10.214.11.1? Tell 10.214.11.28

2) 根据子网掩码可知，最多可连接 254 台计算机，但目前连接了 4 台计算机；10 秒内共有数据包 38 个，其中广播包 14 个；无广播风暴。

4. Ethernet multicast

发送的节点有：

7.24.12.1(路由网关)
7.24.12.104
7.24.12.100
222.205.49.40
222.205.49.170
10.111.230.54
222.205.47.8
222.205.46.60
222.205..46.188
……
高层协议有 SSDP, IGMPv2, MDNS, UDP, LLMNR, NBNS, WSP。

1	0.00000000	7.24.12.1	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
2	0.01631400	7.24.12.1	239.255.255.250	SSDP	334	NOTIFY * HTTP/1.1
3	0.03319200	7.24.12.1	239.255.255.250	SSDP	388	NOTIFY * HTTP/1.1
4	0.04978200	7.24.12.1	239.255.255.250	SSDP	380	NOTIFY * HTTP/1.1
5	0.06678800	7.24.12.1	239.255.255.250	SSDP	310	NOTIFY * HTTP/1.1
6	0.08307400	7.24.12.1	239.255.255.250	SSDP	352	NOTIFY * HTTP/1.1
7	0.09979400	7.24.12.1	239.255.255.250	SSDP	384	NOTIFY * HTTP/1.1
8	0.11646800	7.24.12.1	239.255.255.250	SSDP	330	NOTIFY * HTTP/1.1
9	0.13301900	7.24.12.1	239.255.255.250	SSDP	382	NOTIFY * HTTP/1.1
10	0.14982700	7.24.12.1	239.255.255.250	SSDP	376	NOTIFY * HTTP/1.1
11	11.0327770	7.24.12.1	224.0.0.1	IGMPv2	60	Membership Query, general
12	14.4176660	7.24.12.104	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
13	15.5846990	222.205.49.40	224.0.0.251	MDNS	139	Standard query 0x0000 PTR _sleep-proxy.
14	16.2705900	7.24.12.100	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
15	18.6941330	222.205.49.40	224.0.0.251	MDNS	438	Standard query response 0x0000 TXT, cac
16	19.9996210	7.24.12.1	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
17	20.0159330	7.24.12.1	239.255.255.250	SSDP	334	NOTIFY * HTTP/1.1
18	20.0327310	7.24.12.1	239.255.255.250	SSDP	388	NOTIFY * HTTP/1.1
19	20.0493630	7.24.12.1	239.255.255.250	SSDP	380	NOTIFY * HTTP/1.1

5. Arp host 7.24.12.100

1) 删除 arp(管理员身份)

```
C:\Windows\system32>arp -d *

C:\Windows\system32>
```

2) 删除后

	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.1? Tell 7.24.12.100
2	0.00080000	Tp-LinkT_28:ea:f2	HewlettP_1d:40:21	ARP	60	7.24.12.1 is at bc:d1:77:28:ea:f2
3	53.6023060	HewlettP_1d:40:21	Tp-LinkT_28:ea:f2	ARP	42	Who has 7.24.12.1? Tell 7.24.12.100
4	53.6031020	Tp-LinkT_28:ea:f2	HewlettP_1d:40:21	ARP	60	7.24.12.1 is at bc:d1:77:28:ea:f2
5	63.8203710	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.1? Tell 7.24.12.100
6	63.8211530	Tp-LinkT_28:ea:f2	HewlettP_1d:40:21	ARP	60	7.24.12.1 is at bc:d1:77:28:ea:f2

3) Ping 7.24.12.101(不存在)

7	83.5630280	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.101? Tell 7.24.12.100
8	84.1026560	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.101? Tell 7.24.12.100
9	85.1026830	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.101? Tell 7.24.12.100
10	86.1028780	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.101? Tell 7.24.12.100
11	87.1017900	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.101? Tell 7.24.12.100
12	88.1018310	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.101? Tell 7.24.12.100
13	89.1037500	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.101? Tell 7.24.12.100
14	90.1019160	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.101? Tell 7.24.12.100
15	91.1019640	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.101? Tell 7.24.12.100
16	92.1034500	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.101? Tell 7.24.12.100
17	93.1020550	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.101? Tell 7.24.12.100
18	94.1020780	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.101? Tell 7.24.12.100

4) Ping 7.24.12.103（存在）

28	123.110327	HewlettP_1d:40:21	Broadcast	ARP	42	Who has 7.24.12.1? Tell 7.24.12.100
29	123.111118	Tp-LinkT_28:ea:f2	HewlettP_1d:40:21	ARP	60	7.24.12.1 is at bc:d1:77:28:ea:f2
30	149.101527	HewlettP_1d:40:21	Tp-LinkT_28:ea:f2	ARP	42	Who has 7.24.12.1? Tell 7.24.12.100
31	149.102325	Tp-LinkT_28:ea:f2	HewlettP_1d:40:21	ARP	60	7.24.12.1 is at bc:d1:77:28:ea:f2
32	206.601057	HewlettP_1d:40:21	Tp-LinkT_28:ea:f2	ARP	42	Who has 7.24.12.1? Tell 7.24.12.100
33	206.601867	Tp-LinkT_28:ea:f2	HewlettP_1d:40:21	ARP	60	7.24.12.1 is at bc:d1:77:28:ea:f2
34	323.599226	HewlettP_1d:40:21	Tp-LinkT_28:ea:f2	ARP	42	Who has 7.24.12.1? Tell 7.24.12.100
35	323.600038	Tp-LinkT_28:ea:f2	HewlettP_1d:40:21	ARP	60	7.24.12.1 is at bc:d1:77:28:ea:f2
36	399.098556	HewlettP_1d:40:21	Tp-LinkT_28:ea:f2	ARP	42	Who has 7.24.12.1? Tell 7.24.12.100
37	399.099372	Tp-LinkT_28:ea:f2	HewlettP_1d:40:21	ARP	60	7.24.12.1 is at bc:d1:77:28:ea:f2

6. Ip broadcast，使用 mac(7.24.12.106) ping 主机(7.24.12.100)，获得以下数据包，source 标记为 0.0.0.0，Ethernet 中数据为 mac 物理地址，包括于 bootstrap protocol；

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	0.0.0.0	255.255.255.255	BOOTP	232	Boot Request from a4:5e:60:ba:3e:1f (Apple_ba:3e:1f)
2	4.10169100	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe0f33b5a
3	12.9335640	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe0f33b5a
4	21.3706640	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe0f33b5a
5	22.9711860	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xe0f33b5a

7. Ip multicast,顶层协议包括 MDNS, SSDP, IGMPv2，发送节点有：

169.254.56.221
222.205.47.54
222.205.47.37
222.205.49.152
7.24.12.1
7.24.12.102
7.24.12.104
7.24.12.106

39	33.8548720	222.205.47.54	224.0.0.251	MDNS	534	Standard query response 0x0000 PTR, cache flush My Computer-2.local PTR,
40	41.5996590	222.205.47.54	224.0.0.251	MDNS	166	Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question PTR _ap
41	49.4945170	7.24.12.1	239.255.255.250	SSDP	316	NOTIFY * HTTP/1.1
42	49.5112830	7.24.12.1	239.255.255.250	SSDP	334	NOTIFY * HTTP/1.1
43	49.5275430	7.24.12.1	239.255.255.250	SSDP	388	NOTIFY * HTTP/1.1
44	49.5445650	7.24.12.1	239.255.255.250	SSDP	380	NOTIFY * HTTP/1.1
45	49.5610430	7.24.12.1	239.255.255.250	SSDP	310	NOTIFY * HTTP/1.1
46	49.5775460	7.24.12.1	239.255.255.250	SSDP	352	NOTIFY * HTTP/1.1
47	49.5943250	7.24.12.1	239.255.255.250	SSDP	384	NOTIFY * HTTP/1.1
48	49.6112550	7.24.12.1	239.255.255.250	SSDP	330	NOTIFY * HTTP/1.1
49	49.6276610	7.24.12.1	239.255.255.250	SSDP	382	NOTIFY * HTTP/1.1
50	49.6443270	7.24.12.1	239.255.255.250	SSDP	376	NOTIFY * HTTP/1.1
51	55.7440360	7.24.12.1	224.0.0.1	IGMPv2	60	Membership Query, general
52	56.1782750	7.24.12.105	239.255.255.250	IGMPv2	60	Membership Report group 239.255.255.250
53	59.1492200	7.24.12.104	224.0.0.251	MDNS	126	Standard query response 0x0000 TXT
54	59.9598460	7.24.12.104	224.0.0.251	MDNS	126	Standard query response 0x0000 TXT
55	60.5599170	7.24.12.102	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
56	61.5933860	7.24.12.106	224.0.0.251	MDNS	183	Standard query 0x0000 PTR _raop._tcp.local, "QM" question PTR _airplay._

8. Icmp

1) 主机 10.214.11.41

```
C:\Users\cszju>ping 10.214.11.39 -t

正在 Ping 10.214.11.39 具有 32 字节的数据:
来自 10.214.11.39 的回复: 字节=32 时间<1ms TTL=128
来自 10.214.11.39 的回复: 字节=32 时间<1ms TTL=128
来自 10.214.11.39 的回复: 字节=32 时间<1ms TTL=128
来自 10.214.11.39 的回复: 字节=32 时间<1ms TTL=128
来自 10.214.11.39 的回复: 字节=32 时间<1ms TTL=128
来自 10.214.11.39 的回复: 字节=32 时间<1ms TTL=128
```

2) 由图可知，icmp 类型有 icmp 和 icmpv6，其中，icmp 主要 echo 了 ping 的信息（request、reply）；icmpv6 信息较多，有 Router solicitation、neighbor solicitation、neighbor advertisement、multicast listener report

message 等；IP 协议后紧跟 ICMP 协议，并用 ICMP 协议说明了 ping 信息；

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.214.11.92	10.255.255.255	NBNS	92	Name query NB WPAD<00>
2	0.25984400	10.214.11.92	10.255.255.255	NBNS	92	Name query NB API.BING.COM<00>
3	0.26693300	fe80::f1f6:c60c:c4d	ff02::1:2	DHCPv6	150	Solicit XID: 0xa61308 CID: 0001000119a6a6d374d02b7c5c4a
4	0.27850600	Cisco_4f:4b:13	Spanning-tree-(for-	STP	60	Conf. Root = 0/11/28:94:0f:2a:23:00 Cost = 4 Port = 0x8013
5	0.30454200	10.214.11.41	10.214.11.39	ICMP	74	Echo (ping) request id=0x0001, seq=1160/34820, ttl=128
6	0.30505600	10.214.11.39	10.214.11.41	ICMP	74	Echo (ping) reply id=0x0001, seq=1160/34820, ttl=128
7	0.47506400	10.214.11.11	10.214.11.255	NBNS	92	Name query NB WPAD<00>
8	0.52096700	10.214.11.92	10.255.255.255	NBNS	92	Name query NB ARMMF.ADOBE.COM<00>
9	0.54717700	10.214.11.44	10.214.11.255	NBNS	92	Name query NB WPAD<00>
10	0.74980700	10.214.11.92	10.255.255.255	NBNS	92	Name query NB WPAD<00>
11	0.77867000	10.214.11.41	218.108.29.249	ICMP	74	Echo (ping) request id=0x0001, seq=1161/35076, ttl=64
12	0.78089100	218.108.29.249	10.214.11.41	ICMP	74	Echo (ping) reply id=0x0001, seq=1161/35076, ttl=253
13	0.81476400	fe80::c025:8653:86b	ff02::2	ICMPv6	70	Router Solicitation from 74:d0:2b:7a:1a:ce
14	1.01038000	10.214.11.92	10.255.255.255	NBNS	92	Name query NB API.BING.COM<00>
15	1.23318600	AsustekC_7c:5c:4a	Broadcast	ARP	60	Who has 10.214.11.44? Tell 10.214.11.43
16	1.27091200	10.214.11.92	10.255.255.255	NBNS	92	Name query NB ARMMF.ADOBE.COM<00>
17	1.29715000	10.214.11.44	10.214.11.255	NBNS	92	Name query NB WPAD<00>
18	1.30762700	10.214.11.41	10.214.11.39	ICMP	74	Echo (ping) request id=0x0001, seq=1162/35332, ttl=128
19	1.30820800	10.214.11.39	10.214.11.41	ICMP	74	Echo (ping) reply id=0x0001, seq=1162/35332, ttl=128

```
⊞ Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_7c:5c:b2 (74:d0:2b:7c:5c:b2), Dst: AsustekC_7c:5c:d7 (74:d0:2b:7c:5c:d7)
⊞ Internet Protocol Version 4, Src: 10.214.11.41 (10.214.11.41), Dst: 10.214.11.39 (10.214.11.39)
⊞ Internet Control Message Protocol
```

```
⊞ Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_7c:5c:b2 (74:d0:2b:7c:5c:b2), Dst: AsustekC_7c:5c:d7 (74:d0:2b:7c:5c:d7)
⊟ Internet Protocol Version 4, Src: 10.214.11.41 (10.214.11.41), Dst: 10.214.11.39 (10.214.11.39)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transp
    Total Length: 60
    Identification: 0x7f48 (32584)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x0000 [incorrect, should be 0x8f7d (may be caused by "IP checksum offload"?)]
    Source: 10.214.11.41 (10.214.11.41)
    Destination: 10.214.11.39 (10.214.11.39)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x48d3 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 1160 (0x0488)
    Sequence number (LE): 34820 (0x8804)
    [Response In: 6]
  ⊞ Data (32 bytes)
```

9. Host 10.214.11.41 and www.zju.edu.cn

   1) Ethernet II 帧结构，包含了源 mac 和目标 mac，以及数据包类型 ip;

```
⊟ Ethernet II, Src: AsustekC_7c:5c:b2 (74:d0:2b:7c:5c:b2), Dst: Cisco_4f:4b:48 (00:11:21:4f:4b:48)
  ⊞ Destination: Cisco_4f:4b:48 (00:11:21:4f:4b:48)
  ⊞ Source: AsustekC_7c:5c:b2 (74:d0:2b:7c:5c:b2)
    Type: IP (0x0800)
```

   2) IP 数据报结构，包含版本 4，头长 20bytes，总长等信息；

```
⊟ Internet Protocol Version 4, Src: 10.214.11.41 (10.214.11.41), Dst: 10.203.5.199 (10.203.5.199)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 78
    Identification: 0x2fac (12204)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  ⊞ Header checksum: 0x0000 [incorrect, should be 0xa462 (may be caused by "IP checksum offload"?)]
    Source: 10.214.11.41 (10.214.11.41)
    Destination: 10.203.5.199 (10.203.5.199)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

3) TCP segment 结构，包含源端口号、目标端口号、headerlength 等信息；

```
⊟ Transmission Control Protocol, Src Port: vsat-control (1880), Dst Port: http (80), Seq: 0, Len: 0
    Source port: vsat-control (1880)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 0    (relative sequence number)
    Header length: 32 bytes
  ⊞ Flags: 0x002 (SYN)
    Window size value: 8192
    [Calculated window size: 8192]
  ⊞ Checksum: 0x2ccc [validation disabled]
  ⊞ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
```

10. FTP

1) 在 cmd 中输入 ftp 10.214.47.70 访问 ftp 服务器，捕获一下数据包

176	14.1383880	10.214.11.41	10.214.47.70	TCP	66 tcoflashagent > ftp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
177	14.1393170	10.214.47.70	10.214.11.41	TCP	66 ftp > tcoflashagent [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256
178	14.1394290	10.214.11.41	10.214.47.70	TCP	54 tcoflashagent > ftp [ACK] Seq=1 Ack=1 Win=8192 Len=0
179	14.1405960	10.214.47.70	10.214.11.41	FTP	103 Response: 220 Serv-U FTP Server v6.4 for WinSock ready...
180	14.1603100	10.214.11.41	218.108.29.249	ICMP	74 Echo (ping) request id=0x0001, seq=3731/37646, ttl=64
181	14.1673370	218.108.29.249	10.214.11.41	ICMP	74 Echo (ping) reply id=0x0001, seq=3731/37646, ttl=253
182	14.3447890	10.214.11.41	10.214.47.70	TCP	54 tcoflashagent > ftp [ACK] Seq=1 Ack=50 Win=8143 Len=0

2) 首先发送目标端口类型为 ftp，Flag 为 SYN 的 tcp 协议

```
Transmission Control Protocol, Src Port: tcoflashagent (1975), Dst Port: ftp (21), Seq: 0, Len: 0
  Source port: tcoflashagent (1975)
  Destination port: ftp (21)
  [Stream index: 0]
  Sequence number: 0    (relative sequence number)
  Header length: 32 bytes
⊞ Flags: 0x002 (SYN)
  Window size value: 8192
  [Calculated window size: 8192]
⊞ Checksum: 0x5041 [validation disabled]
⊞ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
```

3) 之后接受 TCP 数据包（Flags：ACK），又发送 TCP 数据包，完成 3 次握手协议；

```
⊞ Frame 178: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_7c:5c:b2 (74:d0:2b:7c:5c:b2), Dst: Cisco_4f:4b:48 (00:11:21:4f:4b:48)
⊞ Internet Protocol Version 4, Src: 10.214.11.41 (10.214.11.41), Dst: 10.214.47.70 (10.214.47.70)
⊟ Transmission Control Protocol, Src Port: tcoflashagent (1975), Dst Port: ftp (21), Seq: 1, Ack: 1, Len: 0
    Source port: tcoflashagent (1975)
    Destination port: ftp (21)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x010 (ACK)
    Window size value: 8192
    [Calculated window size: 8192]
    [Window size scaling factor: 1]
  ⊞ Checksum: 0x5035 [validation disabled]
  ⊞ [SEQ/ACK analysis]
```

4) 之后服务器端发送 DNS 和 UDP 数据包，要求输入密码

232	18.5242990	10.214.11.41	10.10.0.21	DNS	78 Standard query 0x0db6 A hub5pnc.sandai.net
233	18.5252360	10.10.0.21	10.214.11.41	DNS	253 Standard query response 0x0db6 A 114.80.189
234	18.5256840	10.214.11.41	114.80.189.3	UDP	92 Source port: 61919 Destination port: irdmi

5) 主机发送用户名，并收到回应

290	25.5840840	10.214.11.41	10.214.47.70	FTP	69 Request: USER lkj.down
291	25.5886170	10.214.47.70	10.214.11.41	FTP	90 Response: 331 User name okay, need password.
292	25.6039010	10.214.11.48	10.214.11.255	NBNS	92 Name query NB WPAD<00>
293	25.8077400	10.214.11.41	10.214.47.70	TCP	54 tcoflashagent > ftp [ACK] Seq=16 Ack=86 Win=8107 Len=0

```
⊞ Frame 290: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_7c:5c:b2 (74:d0:2b:7c:5c:b2), Dst: Cisco_4f:4b:48 (00:11:21:4f:4b:48)
⊞ Internet Protocol Version 4, Src: 10.214.11.41 (10.214.11.41), Dst: 10.214.47.70 (10.214.47.70)
⊞ Transmission Control Protocol, Src Port: tcoflashagent (1975), Dst Port: ftp (21), Seq: 1, Ack: 50, Len: 15
⊟ File Transfer Protocol (FTP)
  ⊟ USER lkj.down\r\n
      Request command: USER
      Request arg: lkj.down
```

6) 主机端发送密码，并收到回应

326	28.8724740	10.214.11.41	10.214.47.70	FTP	69 Request: PASS lkj.down
327	28.8735810	10.214.47.70	10.214.11.41	FTP	84 Response: 230 User logged in, proceed.
328	29.0871770	10.214.11.41	10.214.47.70	TCP	54 tcoflashagent > ftp [ACK] Seq=31 Ack=116 Win=8077 Len=0

```
⊞ Frame 326: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_7c:5c:b2 (74:d0:2b:7c:5c:b2), Dst: Cisco_4f:4b:48 (00:11:21:4f:4b:48)
⊞ Internet Protocol Version 4, Src: 10.214.11.41 (10.214.11.41), Dst: 10.214.47.70 (10.214.47.70)
⊞ Transmission Control Protocol, Src Port: tcoflashagent (1975), Dst Port: ftp (21), Seq: 16, Ack: 86, Len: 15
⊟ File Transfer Protocol (FTP)
  ⊟ PASS lkj.down\r\n
      Request command: PASS
      Request arg: lkj.down
```

11. POP

1) 使用 Foxmail，自动配置 SMTP，POP3

2) 以 gyxl259@163.com 向 elegabriel@163.com 发送简短邮件

发件人： gyxl259
收件人： elegabriel
日期： 2015年6月4日 19:43:58
主题： hello

hello

2015-06-04

gyxl259

3) 首先进行 TCP 三次握手

374	41.7546320	10.214.11.41	220.181.12.16	TCP	62 pktcable-cops > smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
376	41.8351860	10.214.11.51	224.0.0.252	LLMNR	66 Standard query 0xf7d8 A isatap
377	41.8578050	220.181.12.16	10.214.11.41	TCP	62 smtp > pktcable-cops [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 s
378	41.8578530	10.214.11.41	220.181.12.16	TCP	54 pktcable-cops > smtp [ACK] Seq=1 Ack=1 Win=64860 Len=0

4) 以 TCP Simple Mail Transfer 协议发送 HELO cszju-PC

382	41.9692130	10.214.11.41	220.181.12.16	SMTP	69 C: HELO cszju-PC
383	42.0699950	220.181.12.16	10.214.11.41	TCP	60 smtp > pktcable-cops [ACK] Seq=66 Ack=16 Win=5840 Len=0
384	42.0699970	220.181.12.16	10.214.11.41	SMTP	62 S: 250 OK

```
⊞ Frame 382: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0
⊞ Ethernet II, Src: AsustekC_7c:5c:b2 (74:d0:2b:7c:5c:b2), Dst: Cisco_4f:4b:48 (00:11:21:4f:4b:48)
⊞ Internet Protocol Version 4, Src: 10.214.11.41 (10.214.11.41), Dst: 220.181.12.16 (220.181.12.16)
⊞ Transmission Control Protocol, Src Port: pktcable-cops (2126), Dst Port: smtp (25), Seq: 1, Ack: 66, Len: 15
⊟ Simple Mail Transfer Protocol
  ⊟ Command Line: HELO cszju-PC\r\n
      Command: HELO
      Request parameter: cszju-PC
```

5) 说明发送人，自动登陆，数据传输，收件方，数据；

385	42.0811470	10.214.11.41	220.181.12.16	SMTP	84 C: MAIL FROM: <gyxl259@163.com>
386	42.0927420	10.214.11.45	10.214.11.255	NBNS	92 Name query NB WPAD<00>
387	42.1361350	10.214.11.51	10.214.11.255	NBNS	92 Name query NB ISATAP<00>
388	42.1866640	220.181.12.16	10.214.11.41	SMTP	137 S: 553 authentication is required,smtp12,EMCowEAJqmkPOnBVbZEwBg--.49261S2 1433418255
389	42.1869700	10.214.11.41	220.181.12.16	TCP	54 pktcable-cops > smtp [RST, ACK] Seq=46 Ack=157 Win=0 Len=0
390	42.1936650	10.214.11.41	220.181.12.16	TCP	66 index-pc-wb > smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
391	42.2248160	10.214.11.48	10.214.11.255	NBNS	92 Name query NB WPAD<00>
392	42.2927320	220.181.12.16	10.214.11.41	TCP	66 smtp > index-pc-wb [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1 WS=128
393	42.2928630	10.214.11.41	220.181.12.16	TCP	54 index-pc-wb > smtp [ACK] Seq=1 Ack=1 Win=66240 Len=0
394	42.4135250	220.181.12.16	10.214.11.41	SMTP	119 S: 220 163.com Anti-spam GT for Coremail System (163com[20141201])
395	42.4165460	10.214.11.41	220.181.12.16	SMTP	69 C: EHLO cszju-PC
396	42.5178510	220.181.12.16	10.214.11.41	TCP	60 smtp > index-pc-wb [ACK] Seq=66 Ack=16 Win=5888 Len=0
397	42.5184940	220.181.12.16	10.214.11.41	SMTP	239 S: 250-mail | 250-PIPELINING | 250-AUTH LOGIN PLAIN | 250-AUTH=LOGIN PLAIN | 250-coremail
398	42.5194080	10.214.11.41	220.181.12.16	SMTP	66 C: AUTH LOGIN
399	42.6666380	10.214.11.41	218.108.29.249	ICMP	74 Echo (ping) request id=0x0001, seq=4677/17682, ttl=64
400	42.6765860	218.108.29.249	10.214.11.41	ICMP	74 Echo (ping) reply id=0x0001, seq=4677/17682, ttl=253
401	42.8312600	10.214.11.41	220.181.12.16	SMTP	66 [TCP Retransmission] C: AUTH LOGIN
403	42.8695240	10.214.11.45	224.0.0.252	LLMNR	64 Standard query 0x1cfb A wpad
404	42.8856880	10.214.11.51	10.214.11.255	NBNS	92 Name query NB ISATAP<00>
405	42.9383320	220.181.12.16	10.214.11.41	TCP	66 [TCP Previous segment not captured] smtp > index-pc-wb [ACK] Seq=269 Ack=28 Win=5888 Len=
406	42.9530160	220.181.12.16	10.214.11.41	SMTP	72 [TCP Retransmission] S: 334 dXN!cm5hbWU6
407	42.9539100	10.214.11.41	220.181.12.16	SMTP	68 C: Z3l4bDIIOQ==
409	42.9664000	10.214.11.45	224.0.0.252	LLMNR	64 Standard query 0x1cfb A wpad
410	42.9893850	10.214.11.48	10.214.11.255	NBNS	92 Name query NB WPAD<00>
411	43.0552400	220.181.12.16	10.214.11.41	TCP	60 smtp > index-pc-wb [ACK] Seq=269 Ack=42 Win=5888 Len=0
412	43.0552420	220.181.12.16	10.214.11.41	SMTP	72 S: 334 UGFzc3dvcmQ6
413	43.0556340	10.214.11.41	220.181.12.16	SMTP	72 C: Z3l4bDcyNTI0MTI=
414	43.1694170	10.214.11.45	10.214.11.255	NBNS	92 Name query NB WPAD<00>
415	43.2059800	220.181.12.16	10.214.11.41	TCP	60 smtp > index-pc-wb [ACK] Seq=287 Ack=60 Win=5888 Len=0
416	43.2199640	220.181.12.16	10.214.11.41	SMTP	85 S: 235 Authentication successful
417	43.2250070	10.214.11.41	220.181.12.16	SMTP	84 C: MAIL FROM: <gyxl259@163.com>
418	43.6357930	10.214.11.51	10.214.11.255	NBNS	92 Name query NB ISATAP<00>
419	43.6496840	220.181.12.16	10.214.11.41	SMTP	67 S: 250 Mail OK
420	43.6528480	10.214.11.41	220.181.12.16	SMTP	85 C: RCPT TO: <elegabriel@163.com>
421	43.6731630	10.214.11.41	218.108.29.249	ICMP	74 Echo (ping) request id=0x0001, seq=4678/17938, ttl=64
422	43.6785350	218.108.29.249	10.214.11.41	ICMP	74 Echo (ping) reply id=0x0001, seq=4678/17938, ttl=253
423	43.7645690	220.181.12.16	10.214.11.41	SMTP	67 S: 250 Mail OK
424	43.7659590	10.214.11.41	220.181.12.16	SMTP	60 C: Data
426	43.7887430	10.214.11.48	224.0.0.252	LLMNR	64 Standard query 0x7bb4 A wpad
427	43.8094700	10.214.11.53	255.255.255.255	DHCP	342 DHCP Inform - Transaction ID 0x20a65944
429	43.8194850	10.214.11.53	224.0.0.252	LLMNR	64 Standard query 0xad26 A wpad
430	43.8771840	220.181.12.16	10.214.11.41	SMTP	91 S: 354 End data with <CR><LF>.<CR><LF>
431	43.8802390	10.214.11.41	220.181.12.16	SMTP	369 C: DATA fragment, 315 bytes
433	43.8940720	10.214.11.48	224.0.0.252	LLMNR	64 Standard query 0x7bb4 A wpad
435	43.9334720	10.214.11.45	10.214.11.255	NBNS	92 Name query NB WPAD<00>
436	43.9334920	10.214.11.53	224.0.0.252	LLMNR	64 Standard query 0xad26 A wpad
438	43.9478390	10.214.11.53	224.0.0.252	LLMNR	64 Standard query 0x3b27 A wpad
439	44.0265270	220.181.12.16	10.214.11.41	TCP	60 smtp > index-pc-wb [ACK] Seq=381 Ack=442 Win=6912 Len=0
440	44.0265810	10.214.11.41	220.181.12.16	IMF	1252 from: "gyxl259" <gyxl259@163.com>, subject: hello,

6) Data fragment 内部包含了信件的绝大部分信息；

```
44 61 74 65 3a 20 54 68 75 2c   @Q....Da te: Thu,
20 32 30 31 35 20 31 39 3a 34    4 Jun 2 015 19:4
30 38 30 30 0d 0a 46 72 6f 6d   4:00 +08 00..From
6c 32 35 39 22 20 3c 67 79 78   : "gyxl2 59" <gyx
36 33 2e 63 6f 6d 3e 0d 0a 54   l259@163 .com>..T
67 61 62 72 69 65 6c 20 3c 65   o: elega briel <e
69 65 6c 40 31 36 33 2e 63 6f   legabrie l@163.co
62 6a 65 63 74 3a 20 68 65 6c   m>..Subj ect: hel
73 73 61 67 65 2d 49 44 3a 20   lo..Mess age-ID:
36 30 34 31 39 34 33 35 38 37   <2015060 41943587
40 31 36 33 2e 63 6f 6d 3e 0d   952246@1 63.com>.
6c 65 72 3a 20 46 6f 78 6d 61   .X-maile r: Foxma
39 2c 20 32 30 31 2c 20 31 36   il 6, 9,  201, 16
0a 4d 69 6d 65 2d 56 65 72 73    [cn]..M ime-Vers
2e 30 0d 0a 43 6f 6e 74 65 6e   ion: 1.0 ..Conten
3a 20 6d 75 6c 74 69 70 61 72   t-Type:  multipar
72 6e 61 74 69 76 65 3b 0d 0a   t/altern ative;..
61 72 79 3d 22 3d 3d 3d 3d 3d   .boundar y="=====
61 67 6f 6e 37 34 36 34 38 32   003_Drag on746482
5f 3d 3d 3d 3d 3d 22 0d 0a 0d   647541_= ====".....
```

7) Quit

447	44.1759880	10.214.11.41	220.181.12.16	SMTP	60 C: QUIT
448	44.2478900	10.214.11.53	10.214.11.255	NBNS	92 Name query NB WPAD<00>
449	44.2862170	220.181.12.16	10.214.11.41	SMTP	63 S: 221 Bye
450	44.2863930	10.214.11.41	220.181.12.16	TCP	54 index-pc-wb > smtp [RST, ACK] Seq=1646 Ack=464 Win=0 Len=0
451	44.4037100	10.214.11.41	114.80.189.3	UDP	92 Source port: 50343 Destination port: irdmi

8) 接受邮件(此时回寝室继续做实验，主机 IP 7.24.12.100，发送方 18868104399@163.com，接受方为 elegabriel@163.com，foxmail，Foxmail 中使用的邮箱是 elegabriel@163.com)

9) TCP 握手

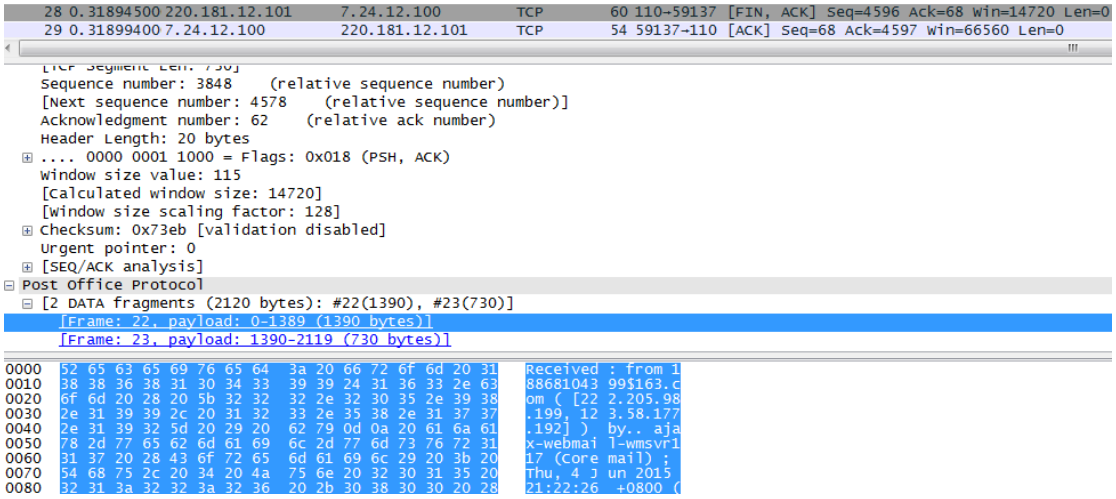
1	0.00000000	7.24.12.100	220.181.12.101	TCP	66 59137→110 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.02546800	220.181.12.101	7.24.12.100	TCP	66 110→59137 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1390 SACK_PERM=1
3	0.02553300	7.24.12.100	220.181.12.101	TCP	54 59137→110 [ACK] Seq=1 Ack=1 Win=66560 Len=0

10) 确认账号密码（明文存储）

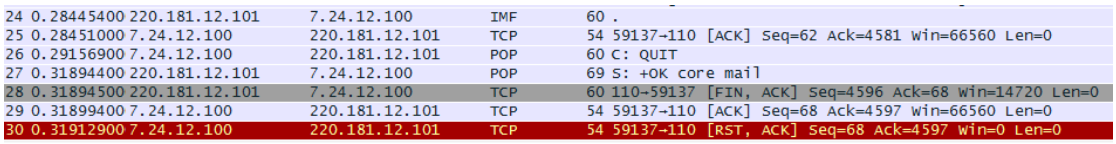
4	0.05051800	220.181.12.101	7.24.12.100	POP	141 S: +OK Welcome to coremail Mail Pop3 Server (163coms[726cd87d72d896a1ac393507346040fas])
5	0.05200000	7.24.12.100	220.181.12.101	POP	71 C: USER elegabriel
6	0.07666700	220.181.12.101	7.24.12.100	TCP	60 110→59137 [ACK] Seq=88 Ack=18 Win=14720 Len=0
7	0.07750100	220.181.12.101	7.24.12.100	POP	69 S: +OK core mail
8	0.07856700	7.24.12.100	220.181.12.101	POP	71 C: PASS [redacted]
9	0.15024300	220.181.12.101	7.24.12.100	TCP	60 110→59137 [ACK] Seq=103 Ack=35 Win=14720 Len=0
10	0.15986700	220.181.12.101	7.24.12.100	POP	92 S: +OK 62 message(s) [16103752 byte(s)]

11) 接收到来自 18868104399@163.com 的邮件

11	0.16190000	7.24.12.100	220.181.12.101	POP	60 C: STAT
12	0.18644800	220.181.12.101	7.24.12.100	TCP	60 110→59137 [ACK] Seq=141 Ack=41 Win=14720 Len=0
13	0.18722300	220.181.12.101	7.24.12.100	POP	71 S: +OK 62 16103752
14	0.18840300	7.24.12.100	220.181.12.101	POP	60 C: UIDL
15	0.21562700	220.181.12.101	7.24.12.100	POP	1444 S: +OK 62 16103752
16	0.21645200	220.181.12.101	7.24.12.100	IMF	349 biVB4LQVUL3UWLDWAASC , 53 1tbiDhIMQVEANEzx-QAAsO , 54 1tbiDhIMQVEANEzx-QABs1 , 55 1tbiDhIMQVEANEzx-QACs2
17	0.21663000	7.24.12.100	220.181.12.101	TCP	54 59137→110 [ACK] Seq=47 Ack=1843 Win=66560 Len=0
18	0.22052700	7.24.12.100	220.181.12.101	POP	60 C: LIST
19	0.25005000	220.181.12.101	7.24.12.100	POP	652 S: +OK 62 16103752
20	0.25604900	7.24.12.100	220.181.12.101	POP	63 C: RETR 62
21	0.28350300	220.181.12.101	7.24.12.100	POP	71 S: +OK 2120 octets
22	0.28445000	220.181.12.101	7.24.12.100	POP	1444 S: DATA fragment, 1390 bytes
23	0.28445200	220.181.12.101	7.24.12.100	IMF	784 from: gxl <18868104399@163.com>, subject: return hello, (text/plain) (text/html)



12) Quit



五、 实验数据记录和处理

具体数据见实验第四部分；

六、 实验结果与分析

具体实验结果见第四部分；

七、 讨论、心得

本实验内容较多，耗时较长，同时需要对各种协议有较好的理解，对于 Wireshark 也需要能较好的使用；

通过本次实验，一方面熟悉并掌握了 Wireshark 的基本使用，能过通过 Wireshark 对于网络数据包进行分析，另一方面也进一步，更加具体地了解了各协议数据包的结构以及通讯方式。