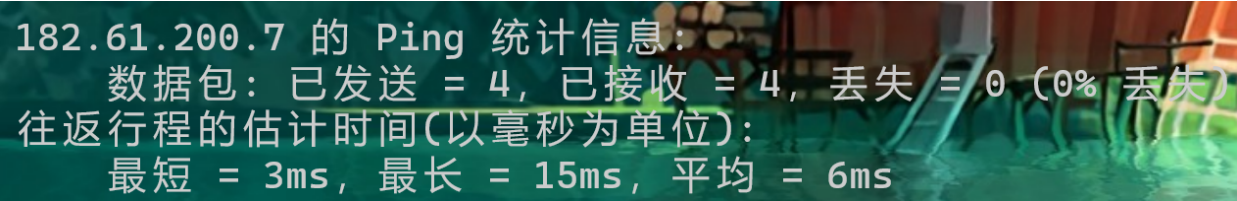
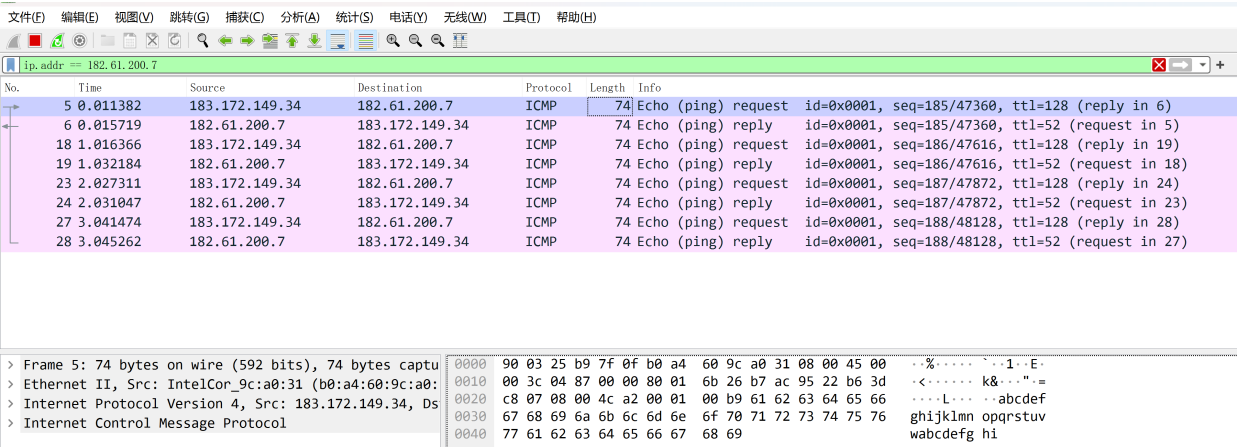


网原第一次小实验

实验

抓包实验 1： 利用 Wireshark 观察 ping 流量

- 回答思考题
 - ICMP协议
 - 交互流程由一个request和一个reply构成，交互过程中网卡会记录前后延时并显示在控制台上，此外控制台和Wireshark对于每次交互均返回了一个TTL值，上网了解知道它指示了IP数据包可以经过最大的路由器数量。
- 关键过程截图



抓包实验 2： 利用 Wireshark 观察 http&https 流量

- 回答思考题
 - 浏览过程中，数据包以http协议返回，其中以可以观察到多组网页源代码，包括网页的各种信息
 - http协议返回的数据包中并不能直接看到源代码，上网查询后得知是https对网页信息进行了加密
- 关键过程截图
 - 抓取中国政府网过程

No.	Time	Source	Destination	Protocol	Length	Info
28	2.103156	2402:f000:2:9001:acf7:9b8a:49f3:ce07	240e:928:101:1700::16	HTTP	722	GET / HTTP/1.1
181	2.233264	2402:f000:2:9001:acf7:9b8a:49f3:ce07	240e:928:101:1700::16	HTTP	667	GET /govweb/c1297/202303/5744165/files/12d188f5afba4fe...
380	2.277833	240e:928:101:1700::16	2402:f000:2:9001:ac...	HTTP	1091	HTTP/1.1 200 OK (text/html)
384	2.278541	2402:f000:2:9001:acf7:9b8a:49f3:ce07	240e:928:101:1700::16	HTTP	746	GET /2016public/bottom.htm HTTP/1.1
482	2.320508	240e:928:101:1700::16	2402:f000:2:9001:ac...	HTTP	372	HTTP/1.1 200 OK (text/html)
1630	2.540582	240e:928:101:1700::16	2402:f000:2:9001:ac...	HTTP	1245	HTTP/1.1 206 Partial Content (audio/mpeg)

> Frame 380: 1091 bytes on wire (8728 bits)	0000	b0 a4 60 9c a0 31 90 03	25 b9 7f 0f 86 dd 60 03	--...1-- %.....
> Ethernet II, Src: HuaweiTe_b9:7f:0f (90:03:25:b9:7f:0f), Dst: IntelCor_9c:a0:31 (b0:a4:60:9c:a0:31)	0010	19 bc 04 0d 06 36 24 0e	09 28 01 01 17 00 00 006\$.-(.....
> Internet Protocol Version 6, Src: 240e:928:101:1700::16, Dst: 2402:f000:2:9001:ac...	0020	00 00 00 00 00 16 24 02	f0 00 00 02 90 01 ac f7\$.
> Transmission Control Protocol, Src Port: 8089, Dst Port: 61088	0030	9b 8a 49 f3 ce 07 00 50	e7 1d 3f f2 bf ac 3c 76	--I....P --?....<v
> [223 Reassembled TCP Segments (298497 bytes) ...]	0040	d0 ec 50 18 00 a6 cf 2c	00 00 6c 65 78 2d 64 69	--P...., ..lex-di
> Hypertext Transfer Protocol	0050	72 65 63 74 69 6f 6e 2d	6e 61 76 22 29 2e 68 69	rection- nav").hi
> Line-based text data: text/html (5140 lines)	0060	64 65 28 29 0d 0a 20 20	20 20 20 20 7d 29 0d 0a	de()-..}};..
> <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">\r\n	0070	20 20 20 20 7d 29 3b 20	2a 2f 0d 0a 20 20 20 20	}); /*/..

```

Line-based text data: text/html (5140 lines)
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">\r\n
<html>\r\n
[truncated]<head><script id="allmobilize" charset="utf-8" src="//ysp.www.gov.cn/013582404bd78ad3c016b8ffffefe6a9a/
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">\r\n
<link href="//www.gov.cn/govweb/xhtml/favicon.ico" rel="shortcut icon" type="image/x-icon">\r\n
<title>中国政府网_中央人民政府门户网站</title>\r\n
<meta name="others" content="页面生成时间 2023-03-03 19:55:13" />\r\n
<meta http-equiv="X-UA-Compatible" content="IE=8" />\r\n
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">\r\n
  <meta name="renderer" content="webkit">\r\n
  <meta name="viewport" content="width=1100" />\r\n
[truncated]<meta name="keywords" content="中央门户网站,中国政府网,国务院,总理,李克强,政府,GOV,我向总理说句话,双
[truncated]<meta name="description" content="中国政府网由国务院办公厅主办, 中国政府网运行中心负责运行维护,是国务院和国务
  <meta name="lanmu" content="中国政府网2016版首页">\r\n
<meta name="filepath" content="/index.htm">\r\n
<META name="catalog" content="2016govs">\r\n

```

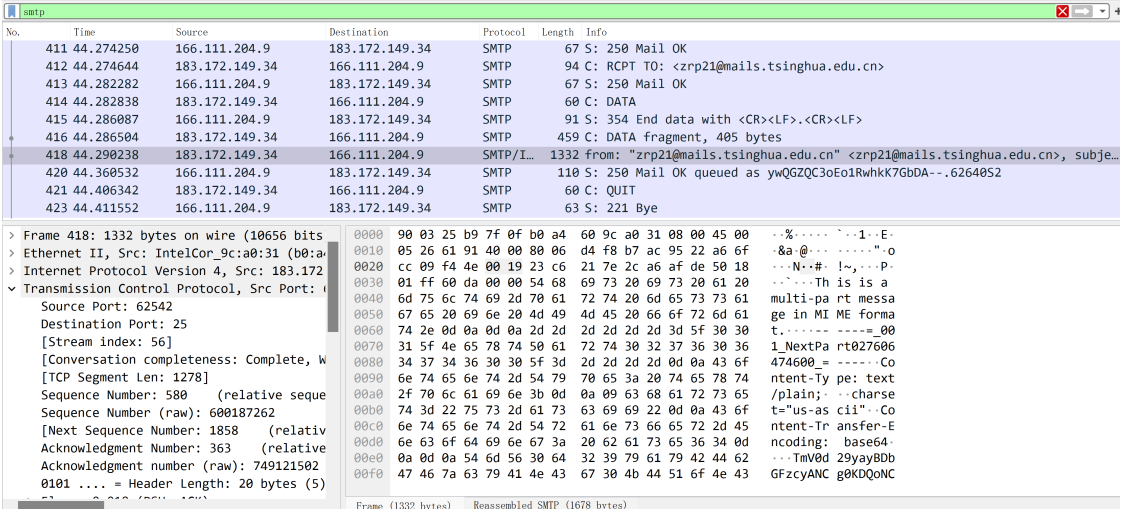
○ 抓取清华大学官网过程

No.	Time	Source	Destination	Protocol	Length	Info
65	2.225622	2402:f000:2:9001:ac...	2408:4002:1f10::41	HTTP	697	GET /?xlbtid=1&aid=1022&id=934&peerid=B0A4609CA0356F2Q&userid=&referfrom=1
66	2.276979	2408:4002:1f10::41	2402:f000:2:9001:ac...	HTTP	288	HTTP/1.1 200 OK (GIF89a)
124	6.525758	2402:f000:2:9001:ac...	2402:4e00:8020:2::a3	HTTP	4699	POST /mmtls/00003fc9 HTTP/1.1
129	6.635372	2402:4e00:8020:2::a3	2402:f000:2:9001:ac...	HTTP	660	HTTP/1.1 200 OK

> Frame 66: 288 bytes on wire (2304 bits), 288 bytes captured (2304 bits) on interface \Device\NPF_{7B4FE264-B753-4501-BFE6-34242}
> Ethernet II, Src: HuaweiTe_b9:7f:0f (90:03:25:b9:7f:0f), Dst: IntelCor_9c:a0:31 (b0:a4:60:9c:a0:31)
> Internet Protocol Version 6, Src: 2408:4002:1f10::41, Dst: 2402:f000:2:9001:acf7:9b8a:49f3:ce07
> Transmission Control Protocol, Src Port: 8089, Dst Port: 61088, Seq: 1, Ack: 624, Len: 214
> Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Date: Wed, 08 Mar 2023 07:50:56 GMT\r\n
Content-Type: image/gif\r\n
Content-Length: 43\r\n
Connection: keep-alive\r\n
Last-Modified: Mon, 28 Sep 1970 06:00:00 GMT\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.051357000 seconds]
[Request in frame: 65]
[Request URI [truncated]: http://stat.download.xunlei.com:8089/?xlbtid=1&aid=1022&id=934&peerid=B0A4609CA0356F2Q&userid=&refe
File Data: 43 bytes
> Compuserve GIF, Version: GIF89a

抓包实验 3： 利用 Wireshark 观察 SMTP 流量

- 回答思考题
 - 删除ssl选项后，在抓取的smtp协议数据包中可看到邮件内容部分，通过base64解码后可以看到具体内容
 - 发送邮件的过程中还对用户名和密码进行了确认，因此在数据包中也可以看到User和Pass字样，通过base64解码后可以获得具体的内容。由此看出，ssl协议加密技术对于保护网络通信过程中的数据安全十分重要，不采取任何加密措施直接明文传输的方式容易导致信息泄露等安全问题。
- 关键过程截图
 - 抓取到的smtp协议数据包



- 数据包内容中包含的正文信息以及用户名和密码

[Type: multipart/alternative]
Preamble: 546869732069732061206d756c74692d70617274206d65737361676520696e204d494d45...
First boundary: -----_001_NextPart027606474600_-----\r\n

Encapsulated multipart part: (text/plain)
Content-Type: text/plain;\r\n\tcharset="us-ascii"\r\nContent-Transfer-Encoding: base64\r\n\r\n

Line-based text data: text/plain (1 lines)
TmV0d29yayBDbGFzcyANCg0KDQoNCnpycDIxQG1haWxzLnRzaW5naHVhLmVkdS5jbG0K\r\n

Boundary: \r\n-----_001_NextPart027606474600_-----\r\n

Encapsulated multipart part: (text/html)
Last boundary: \r\n-----_001_NextPart027606474600_-----\r\n

网络流量捕获结果

TmV0d29yayBDbGFzcyANCg0KDQoNCnpycDIxQG1haWxzLnRzaW5naHVhLmVkdS5jbG0K\r\n

编码 (Encode)

解码 (Decode)

↑ 交换

(编码快捷键: Ctrl + Enter)

Base64 编码或解码的结果:

☐ 编/解码后自动全选

Network Class

435 50.230072 183.172.149.34 166.111.204.9 SMTP 92 C: User: enJwMjFABWfPbHMudHNpmdodWUeUZR1LnNu

436 50.234117 166.111.204.9 183.172.149.34 SMTP 72 S: 334 UGFzc3dvcmQ6

437 50.234564 183.172.149.34 166.111.204.9 SMTP 68 C: Pass: dGVoYwppMDA3

438 50.245630 166.111.204.9 183.172.149.34 SMTP 95 S: 235 Authentication successful

请输入要进行 Base64 编码或解码的字符

enJwMjFAbWFpbHMudHNpbmdodWEuZWVR1LmNu
dGV0YWppMDA3

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码结果

☐ 编/解码后自动全选

抓包实验 4： 利用 Wireshark 观察 QQ 流量（选做）

- 回答思考题
 - qq在应用层通过OICQ协议传输数据，在传输层通过UDP协议传输数据。
 - 在数据包中可以观察到用户信息（QQ账号）和操作类型等信息，
- 关键过程截图
 - 获取用户信息，操作类型

```
UDP payload (55 bytes)
▼ OICQ - IM software, popular in China
  Flag: 01cq packet (0x02)
  Version: 0x3b3b
  Command: Receive message (23)
  Sequence: 48741
  Data(OICQ Number,if sender is client): [REDACTED]
  Data: \00z
  ▼ [Expert Info (Warning/Undecoded): Trailing stray characters]
    [Trailing stray characters]
    [Severity level: Warning]
    [Group: Undecoded]
```

简述题

1. Ping (ICMP协议)

ping 是一种用来测试网络可达性的网络层协议。ping返回ip地址，说明ICMP的数据包会被封装在IP数据包中。而IP 数据包则被封装在数据链路层的帧中（如 Ethernet 帧等），使用ATM或FDDI协议。最后在物理层使用Rj45，802.3等协议封装传输。

2. HTTP协议

HTTP协议是应用层协议，直观理解是网页是可以看到的应用。实验中，HTTP相应和请求均以TCP协议形式传输，说明HTTP数据包被TCP协议封装，又被IP协议封装，最后数据包被数据链路层用ATM或FDDI协议封装。最后在物理层使用Rj45，802.3等协议封装传输。

3. 邮件协议

邮件也是应用层协议。实验中SMTP响应时能观察到伴随的TCP相应，说明SMTP数据包封装在TCP中，又封装在IP协议中，在链路层用ATM或FDDI协议封装。最后在物理层使用Rj45，802.3等协议封装传输。