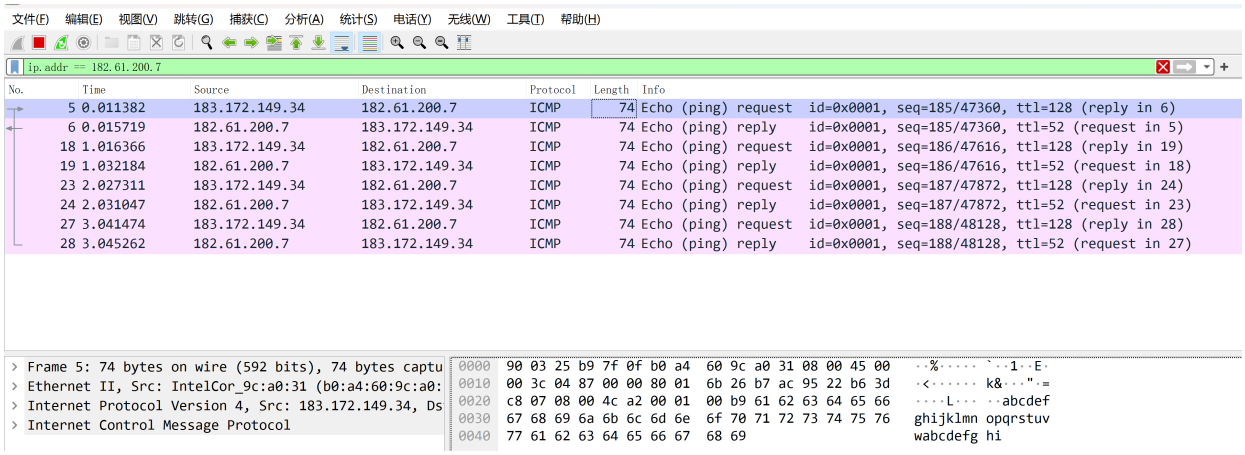
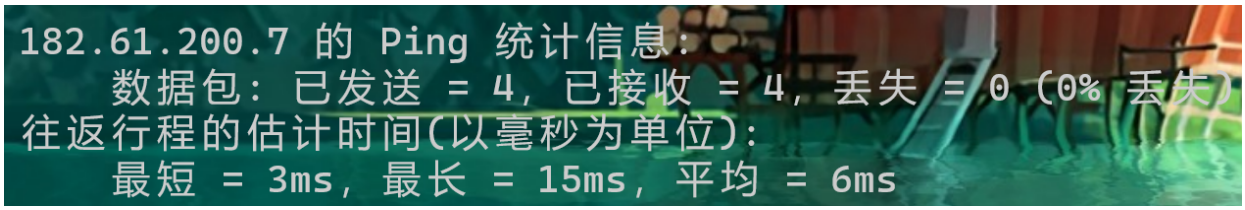
# 网原第一次小实验

## 实验

### 抓包实验 1： 利用 Wireshark 观察 ping 流量

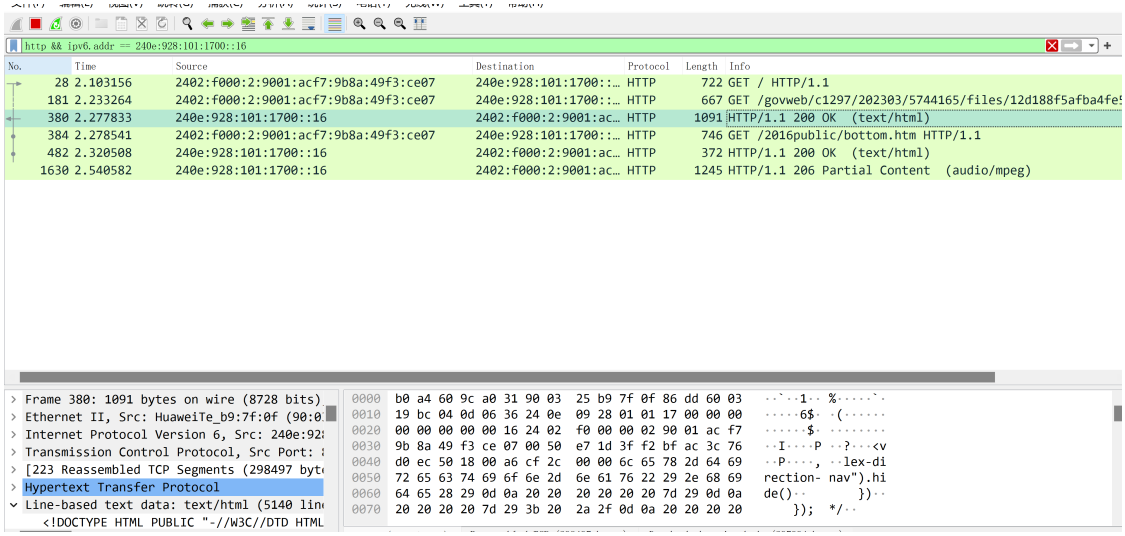
- 回答思考题
    1. ICMP协议
    2. 交互流程由一个request和一个reply构成，交互过程中网卡会记录前后延时并显示在控制台上，此外控制台和Wireshark对于每次交互均返回了一个TTL值，上网了解知道它指示了IP数据包可以经过最大的路由器数量。
- 关键过程截图



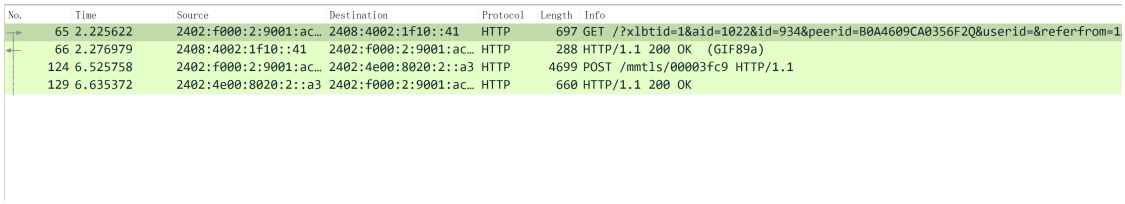

### 抓包实验 2： 利用 Wireshark 观察 http&https 流量

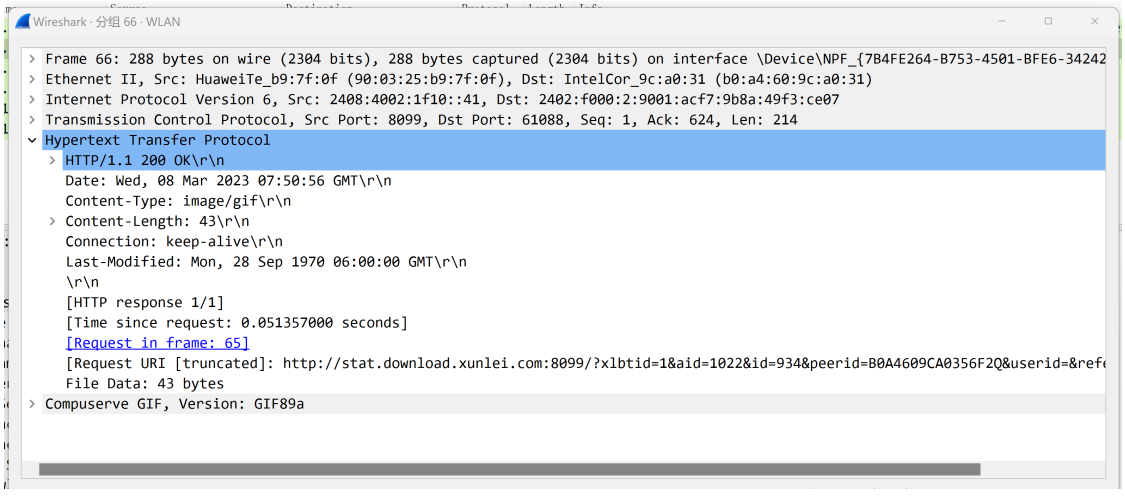
- 回答思考题
    1. 浏览过程中，数据包以http协议返回，其中以可以观察到多组网页源代码，包括网页的各种信息
    2. http协议返回的数据包中并不能直接看到源代码，上网查询后得知是https对网页信息进行了加密
- 关键过程截图
    - 抓取中国政府网过程




```
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/013582404bd78ad3c016b8fffefe6a9a/
  <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="中央政府门户网站,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
```

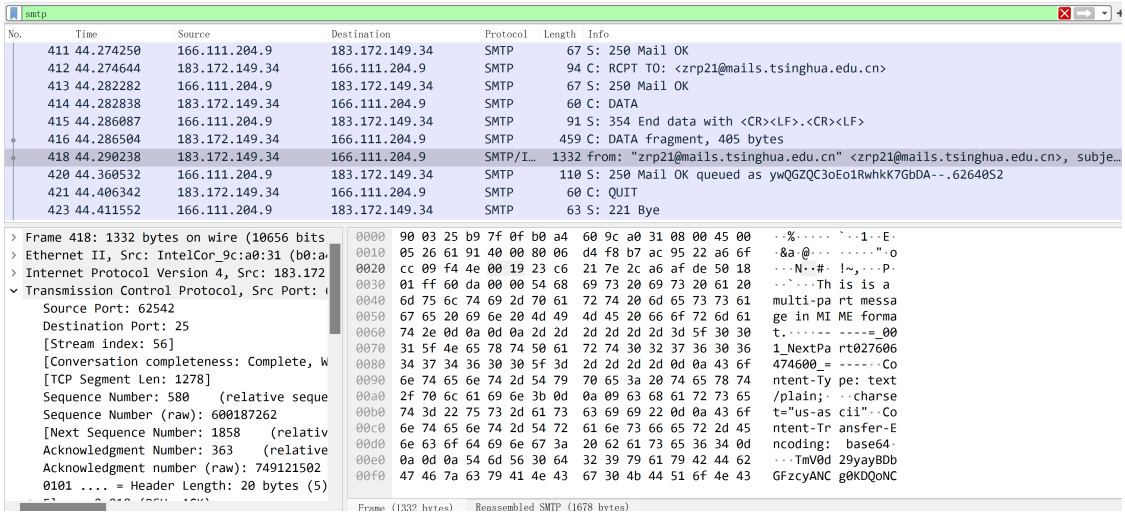
- 抓取清华大学官网过程



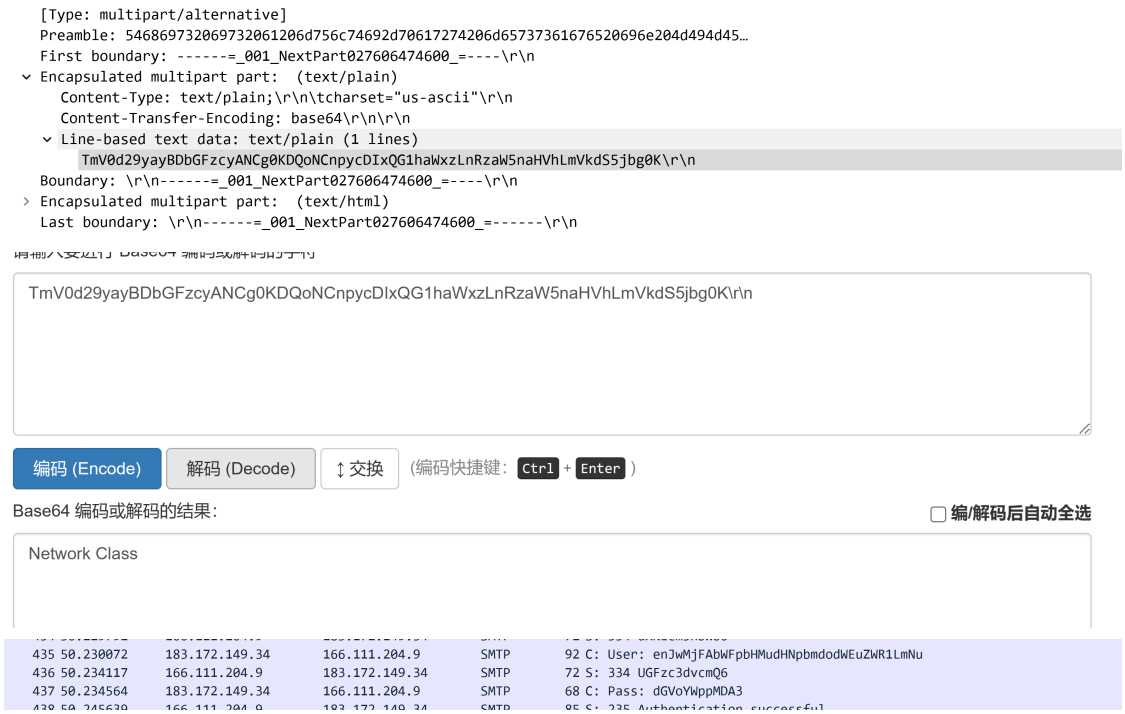



# 抓包实验 3： 利用 Wireshark 观察 SMTP 流量

- 回答思考题
  1. 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
  2. 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

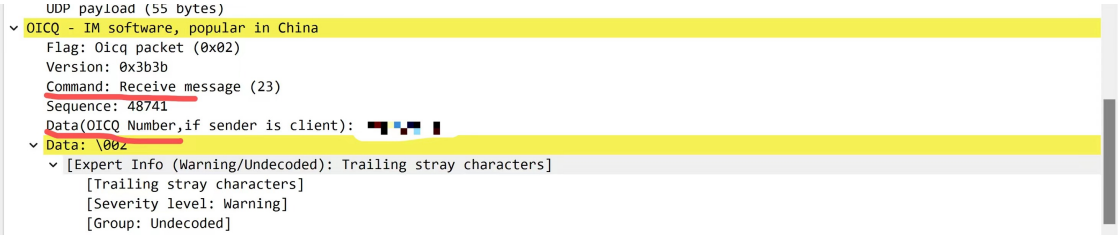



  - 数据包内容中包含的正文信息以及用户名和密码




# 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




# 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。