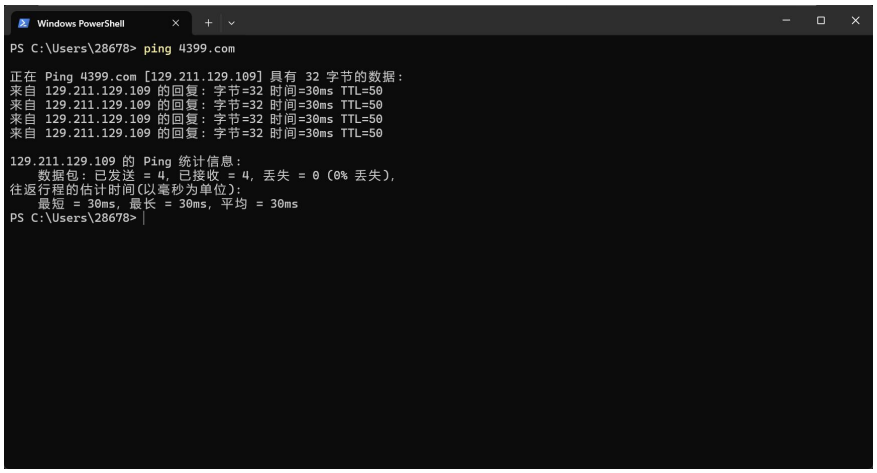
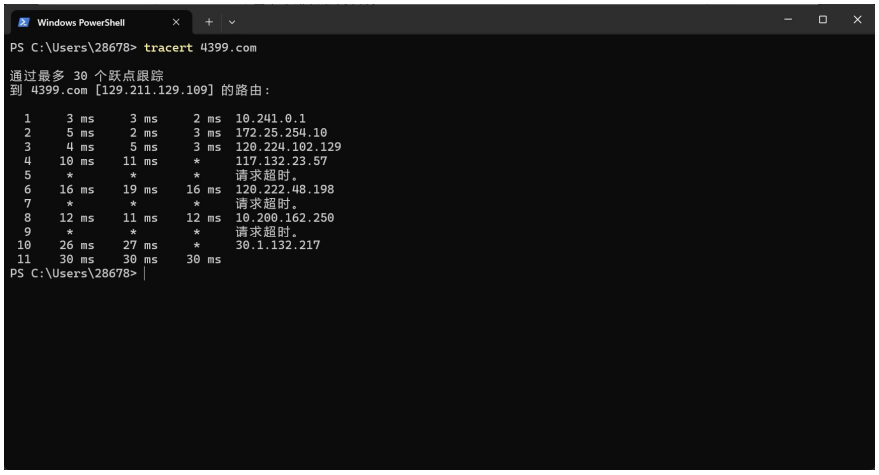
计算机网络与通信实验报告（一）

学　号	姓　名	班　级	报告日期
2022211939	杨涛	22211106	2024/10/10
实验内容	**网络常用命令的使用及 DNS 层次查询、SMTP 协议分析**		
实验目的	1、掌握网络常用命令的使用； 2、利用网络常用命令对网络中常见现象进行分析判断。 3、了解和掌握 DNS 层次结构，利用 NSLOOKUP 命令对 DNS 层次结构进行访问； 4、了解电子邮件系统发送及接受处理过程，对 SMTP 协议进行分析； 5、掌握捕包软件 ethereal 的使用，了解网络协议实体间进行交互以及报文交换的情况；		
实验预备知识	1、掌握 DNS 基本构成原理及三层结构。 2、电子邮件系统的构成，包含在发送方、接收方进行邮件传递涉及的各种协议及协议构成，区分 SMTP 协议与邮件消息格式的异同点。 3、了解常用捕包软件。捕包软件不但可以分析数据包的流向，也可以对数据包的内容进行监听，可以观察 TCP/IP 协议族中应用层、传输层、网络层、数据链路层和有关网络安全的各种协议的活动。		
实验过程描述	**一、网络常用命令的使用** **1. 掌握 PING 命令的基本使用方法（包括参数的使用），对网络常见故障利用命令进行分析判断。**		



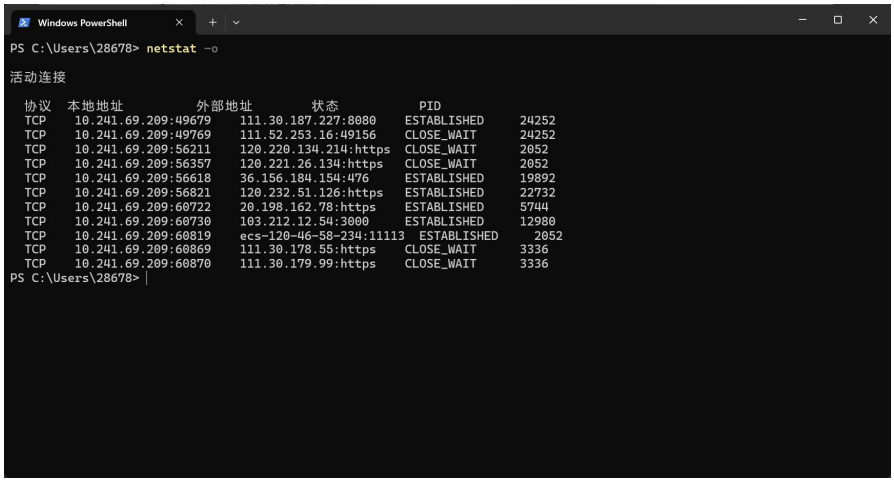
2.用 Tracert 命令用来显示数据包到达目标主机所经过的路径，并显示到达每个节点的时间，分析网络延时产生的原因。



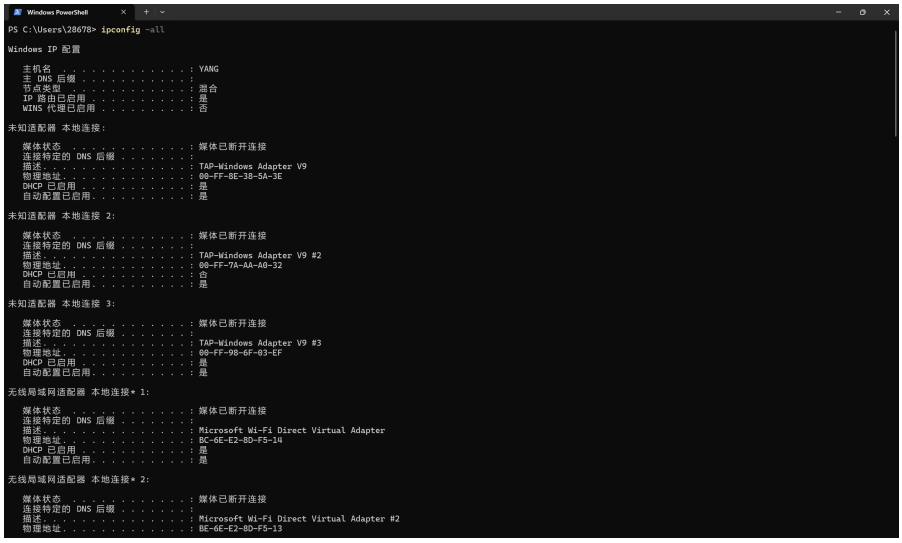
原因：

网络延迟的原因包括物理距离、网络拥塞、路由器性能不足、数据包丢失导致的重传，以及不同网络协议的效率差异。这些因素共同影响数据包在传输过程中所需的时间，从而造成延迟。

3.利用 Netstat 命令了解网络的整体使用情况。显示当前正在活动的网络连接的详细信息，例如显示网络连接、路由表和网络接口信息，统计目前总共有哪些网络连接正在运行。



4.利用 IPCONFIG 命令显示所有当前的 TCP/IP 网络配置值、刷新动态主机配置协议 (DHCP) 和域名系统 (DNS) 设置。 使用不带参数的 IPCONFIG 显示所有适配器的 IP 地址、子网掩码、默认网关。



5.利用 ARP 确定对应 IP 地址的网卡物理地址。查看本地计算机或另一台计算机的 ARP 高速缓存中的当前内容。

```
Windows PowerShell
PS C:\Users\28678> arp -a

接口: 192.168.33.1 --- 0x8
  Internet 地址         物理地址              类型
  192.168.33.254        00-50-56-e9-6f-f1     动态
  192.168.33.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     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

接口: 192.168.192.228 --- 0xa
  Internet 地址         物理地址              类型
  25.255.255.254        2a-00-41-ad-b5-5b     静态
  192.168.192.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     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

接口: 192.168.88.1 --- 0xf
  Internet 地址         物理地址              类型
  192.168.88.135        00-0c-29-3e-6f-4f     动态
  192.168.88.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     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

接口: 10.241.69.209 --- 0x17
  Internet 地址         物理地址              类型
  10.241.0.1            58-69-6c-a6-8f-09     动态
  10.241.255.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     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
PS C:\Users\28678>
```

二、DNS 层次查询、SMTP 协议分析

（1）.DNS 层次查询

1. 查找 13 个根名称服务器的 IP 地址

```
PS C:\Users\28678\Desktop> nslookup a.root-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    a.root-servers.net
Addresses:  2001:503:ba3e::2:30
          198.41.0.4

PS C:\Users\28678\Desktop> nslookup b.root-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    b.root-servers.net
Addresses:  2801:1b8:10::b
          170.247.170.2

PS C:\Users\28678\Desktop> nslookup c.root-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    c.root-servers.net
Addresses:  2001:500:2::c
          192.33.4.12

PS C:\Users\28678\Desktop> nslookup d.root-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    d.root-servers.net
Addresses:  2001:500:2d::d
          199.7.91.13

PS C:\Users\28678\Desktop> nslookup e.root-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    e.root-servers.net
Addresses:  2001:500:a8::e
          192.203.230.10

PS C:\Users\28678\Desktop> nslookup f.root-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    f.root-servers.net
Addresses:  2001:500:2f::f
          192.5.5.241

PS C:\Users\28678\Desktop> nslookup g.root-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    g.root-servers.net
Addresses:  2001:500:12::d0d
          192.112.36.4

PS C:\Users\28678\Desktop> nslookup h.root-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    h.root-servers.net
Addresses:  2001:500:1::53
          198.97.190.53

PS C:\Users\28678\Desktop> nslookup i.root-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    i.root-servers.net
Addresses:  2001:7fe::53
          192.36.148.17

PS C:\Users\28678\Desktop> nslookup j.root-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    j.root-servers.net
Addresses:  2001:503:c27::2:30
          192.58.128.30
```

```
PS C:\Users\28678\Desktop> nslookup k.root-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    k.root-servers.net
Addresses:  2001:7fd::1
          193.0.14.129

PS C:\Users\28678\Desktop> nslookup l.root-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    l.root-servers.net
Addresses:  2001:500:9f::42
          199.7.83.42

PS C:\Users\28678\Desktop> nslookup m.root-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    m.root-servers.net
Addresses:  2001:dc3::35
          202.12.27.33
```

2. 选择一个根名称服务器进行逐级 NDS 解析

选择的根名称服务器：a.root-servers.net

2.1 查询根名称服务器的 NS 记录

```
PS C:\Users\28678\Desktop> nslookup -qt=NS example.com a.root-servers.ne
in-addr.arpa    nameserver = f.in-addr-servers.arpa
in-addr.arpa    nameserver = b.in-addr-servers.arpa
in-addr.arpa    nameserver = d.in-addr-servers.arpa
in-addr.arpa    nameserver = a.in-addr-servers.arpa
in-addr.arpa    nameserver = c.in-addr-servers.arpa
in-addr.arpa    nameserver = e.in-addr-servers.arpa
f.in-addr-servers.arpa  internet address = 193.0.9.1
f.in-addr-servers.arpa  AAAA IPv6 address = 2001:67c:e0::1
b.in-addr-servers.arpa  internet address = 199.253.183.183
b.in-addr-servers.arpa  AAAA IPv6 address = 2001:500:87::87
d.in-addr-servers.arpa  internet address = 200.10.60.53
d.in-addr-servers.arpa  AAAA IPv6 address = 2001:13c7:7010::53
a.in-addr-servers.arpa  internet address = 199.180.182.53
a.in-addr-servers.arpa  AAAA IPv6 address = 2620:37:e000::53
c.in-addr-servers.arpa  internet address = 196.216.169.10
c.in-addr-servers.arpa  AAAA IPv6 address = 2001:43f8:110::10
e.in-addr-servers.arpa  internet address = 203.119.86.101
e.in-addr-servers.arpa  AAAA IPv6 address = 2001:dd8:6::101
服务器:  UnKnown
Address:  198.41.0.4

com     nameserver = l.gtld-servers.net
com     nameserver = j.gtld-servers.net
com     nameserver = h.gtld-servers.net
com     nameserver = d.gtld-servers.net
com     nameserver = b.gtld-servers.net
com     nameserver = f.gtld-servers.net
com     nameserver = k.gtld-servers.net
com     nameserver = m.gtld-servers.net
com     nameserver = i.gtld-servers.net
com     nameserver = g.gtld-servers.net
com     nameserver = a.gtld-servers.net
com     nameserver = c.gtld-servers.net
com     nameserver = e.gtld-servers.net
```

```
l.gtld-servers.net      internet address = 192.41.162.30
l.gtld-servers.net      AAAA IPv6 address = 2001:500:d937::30
j.gtld-servers.net      internet address = 192.48.79.30
j.gtld-servers.net      AAAA IPv6 address = 2001:502:7094::30
h.gtld-servers.net      internet address = 192.54.112.30
h.gtld-servers.net      AAAA IPv6 address = 2001:502:8cc::30
d.gtld-servers.net      internet address = 192.31.80.30
d.gtld-servers.net      AAAA IPv6 address = 2001:500:856e::30
b.gtld-servers.net      internet address = 192.33.14.30
b.gtld-servers.net      AAAA IPv6 address = 2001:503:231d::2:3
f.gtld-servers.net      internet address = 192.35.51.30
f.gtld-servers.net      AAAA IPv6 address = 2001:503:d414::30
k.gtld-servers.net      internet address = 192.52.178.30
k.gtld-servers.net      AAAA IPv6 address = 2001:503:d2d::30
m.gtld-servers.net      internet address = 192.55.83.30
m.gtld-servers.net      AAAA IPv6 address = 2001:501:b1f9::30
i.gtld-servers.net      internet address = 192.43.172.30
i.gtld-servers.net      AAAA IPv6 address = 2001:503:39c1::30
g.gtld-servers.net      internet address = 192.42.93.30
g.gtld-servers.net      AAAA IPv6 address = 2001:503:eea3::30
a.gtld-servers.net      internet address = 192.5.6.30
a.gtld-servers.net      AAAA IPv6 address = 2001:503:a83e::2:3
c.gtld-servers.net      internet address = 192.26.92.30
c.gtld-servers.net      AAAA IPv6 address = 2001:503:83eb::30
e.gtld-servers.net      internet address = 192.12.94.30
e.gtld-servers.net      AAAA IPv6 address = 2001:502:1ca1::30
```

2.2 查询顶级域名称服务器的 NS 记录

选择的顶级域名称服务器：l.gtld-servers.net

```
PS C:\Users\28678\Desktop> nslookup -qt=NS example.com l.gtld-servers.ne
(root)  nameserver = f.root-servers.net
(root)  nameserver = g.root-servers.net
(root)  nameserver = h.root-servers.net
(root)  nameserver = i.root-servers.net
(root)  nameserver = j.root-servers.net
(root)  nameserver = k.root-servers.net
(root)  nameserver = l.root-servers.net
(root)  nameserver = m.root-servers.net
(root)  nameserver = a.root-servers.net
(root)  nameserver = b.root-servers.net
(root)  nameserver = c.root-servers.net
(root)  nameserver = d.root-servers.net
(root)  nameserver = e.root-servers.net
服务器:  UnKnown
Address:  192.41.162.30

example.com     nameserver = a.iana-servers.net
example.com     nameserver = b.iana-servers.net
```

2.3 查询权威名称服务器的 A 记录

选择的权威名称服务器：a.iana-servers.net

```
PS C:\Users\28678\Desktop> nslookup -qt=A a.iana-servers.net
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    a.iana-servers.net
Address:  199.43.135.53
```

3. 在本地名称服务器上手动逐级进行 NDS 解析

3.1 查询根名称服务器的 NS 记录

```
PS C:\Users\28678\Desktop> nslookup -qt=NS example.com
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
example.com     nameserver = a.iana-servers.net
example.com     nameserver = b.iana-servers.net
PS C:\Users\28678\Desktop>
```

3.2 查询顶级域名称服务器的 NS 记录

```
PS C:\Users\28678\Desktop> nslookup -qt=NS com
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
com     nameserver = k.gtld-servers.net
com     nameserver = j.gtld-servers.net
com     nameserver = h.gtld-servers.net
com     nameserver = e.gtld-servers.net
com     nameserver = i.gtld-servers.net
com     nameserver = f.gtld-servers.net
com     nameserver = g.gtld-servers.net
com     nameserver = d.gtld-servers.net
com     nameserver = l.gtld-servers.net
com     nameserver = b.gtld-servers.net
com     nameserver = a.gtld-servers.net
com     nameserver = m.gtld-servers.net
com     nameserver = c.gtld-servers.net
```

3.3 查询权威名称服务器的 A 记录

```
PS C:\Users\28678\Desktop> nslookup -qt=A www.example.com
服务器:  UnKnown
Address:  192.168.86.75

非权威应答:
名称:    www.example.com
Address:  93.184.215.14
```

（2）.利用 TELNET 进行 SMTP 的邮件发送。

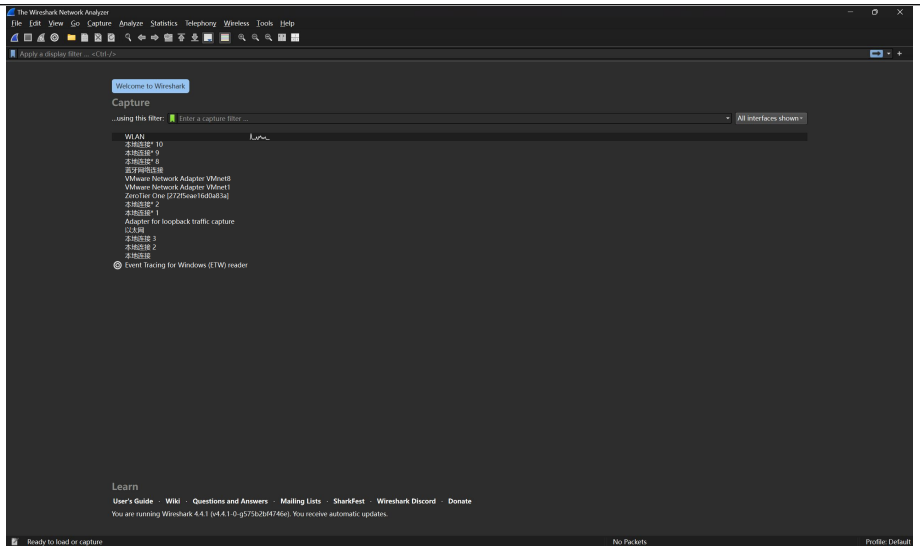
```
HELO mycomputer
250 OK
AUTH LOGIN
334 dXNlcm5hbWU6
MTg2MzYzMDYyNTBAMTYzLmNvbQ==
334 UGFzc3dvcmQ6
U1pxZ0NKRVB1QkJiUGloOQ==
235 Authentication successful
MAIL FROM:<18636306250@163.com>
250 Mail OK
RCPT TO:<2867868802@qq.com>
250 Mail OK
DATA
354 End data with <CR><LF>.<CR><LF>
FROM: <18636306250@163.com>
TO: <2867868802@qq.com>
SUBJECT: HELLO SMTP

Hello, this is a test email!
.
250 Mail OK queued as gzga-smtp-mtada-g0-0,_____wDXr0Hf3hxnliISBg--.32497S9 1729945391
QUIT
221 Bye
```

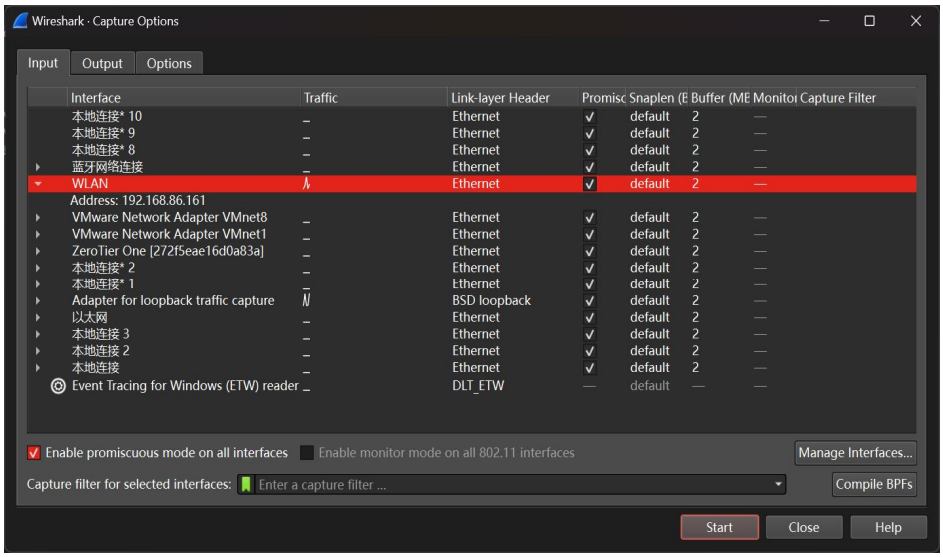
三、熟练掌握抓包软件 ethereal。

1. 熟练掌握抓包软件 ethereal。

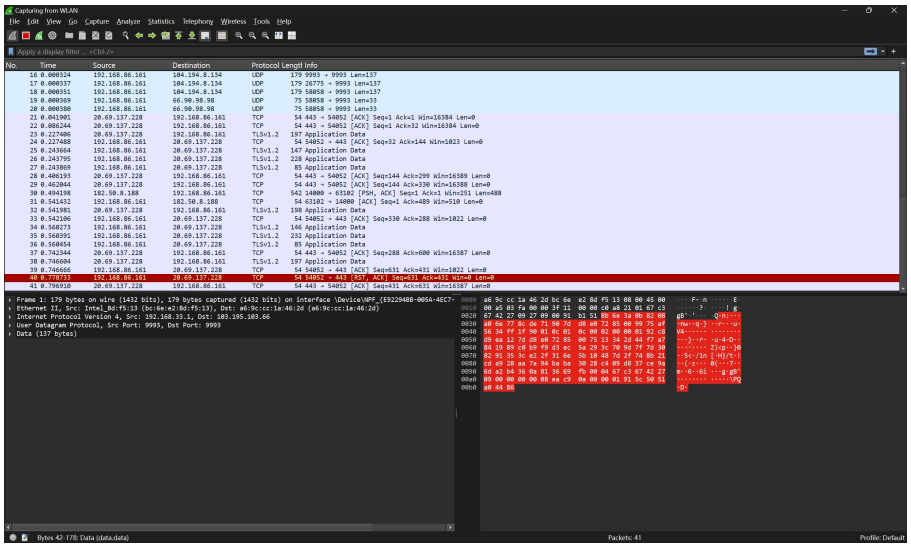
过程：1) Ethereal 主页面



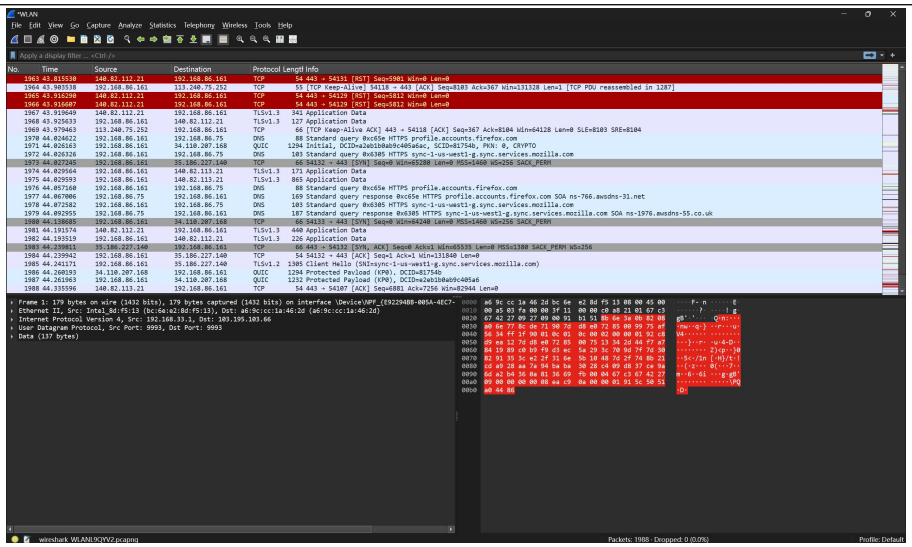
2) 设置所需捕获的网络接口



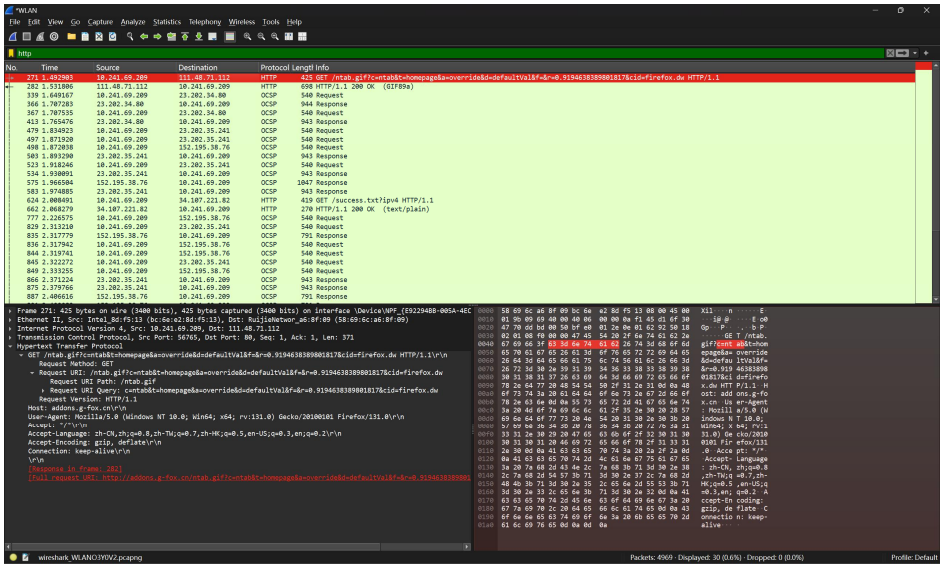
3) 开始分组俘获(捕获中)



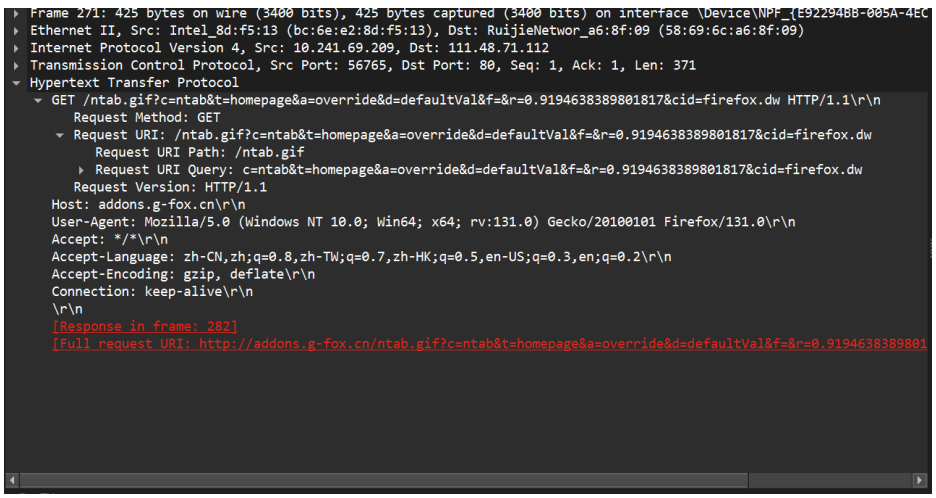
4) 结束分组俘获并查看俘获结果



5) 筛选 HTTP 报文



6) 查看报文



7) 退出 Ethereal

2. 问题：

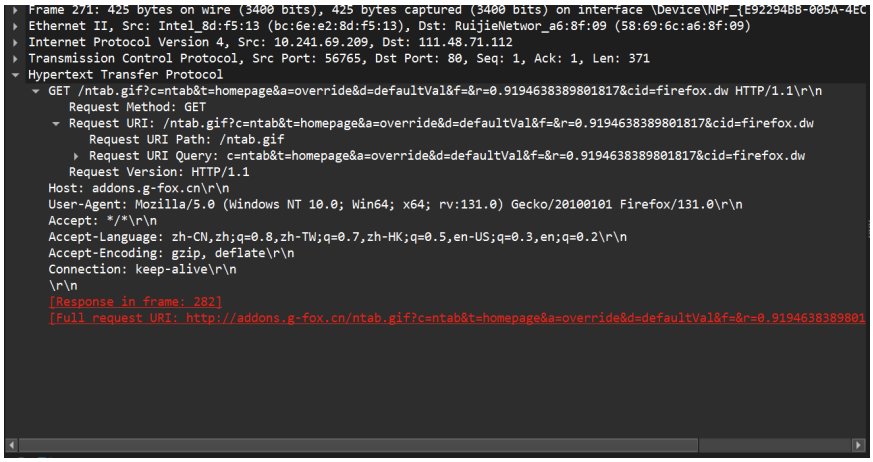
1)分组捕获中出现的所有协议类型:ARP、BROWSER、CLASSIC-STUN、DHCP、DNS、DTLS、HTTP、ICMP、ICMPv6、IGMPv2、IGMPv3、IPv4、LLMNR、MDNS、NBNS、OICQ、QUIC、SSDP、SSL、TCP、TLSv1.2、TLSv1.3、UDP。

2)本次分组捕获中，从发出 HTTP GET 报文到接收到 HTTP OK 响应报文共需要 0.038903 秒。

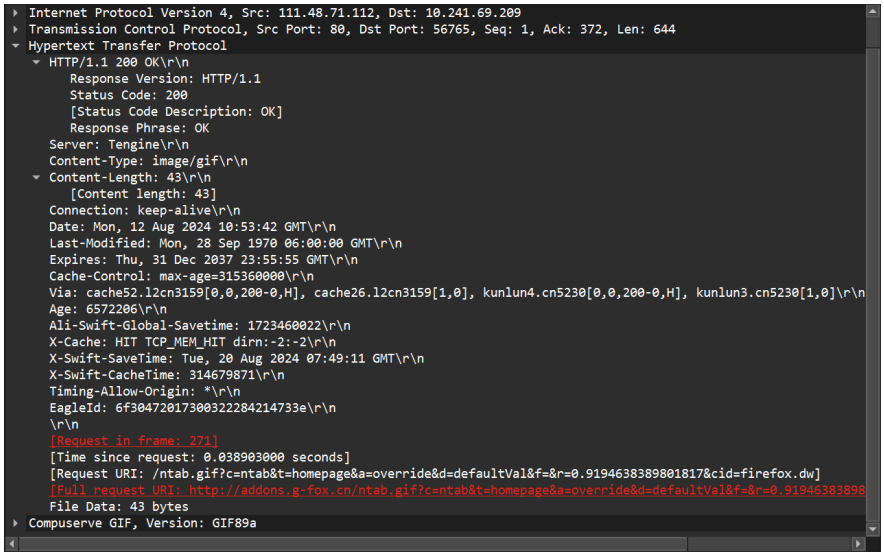
3)本机 IP 地址为：10.241.69.209

4)访问的主页所在服务器 IP 地址为：111.48.71.112

5)HTTP 报文头部行信息 1：



6)HTTP 报文头部行信息 2：



实验结果	实验一：主要围绕网络常用命令的使用、DNS 层次查询和 SMTP 协议分析进行。通过 Windows 的命令行进入，掌握了如 PING、Tracert、Netstat、IPCONFIG 和 ARP 等命令的基本用法。PING 用于测试网络连接状况，能够判断故障可能出现在网线或配置上；Tracert 显示数据包的传输路径和延迟信息，帮助分析网络延时的原因；Netstat 提供当前活动网络连接的详细信息，便于监控网络使用情况；

	IPCONFIG 显示 TCP/IP 配置，刷新 DHCP 和 DNS 设置；而 ARP 则用于确定 IP 地址对应的 MAC 地址。实验通过现场讲解和实践，结合分析总结了在网络故障排查中的应用。 实验二：在 DNS 层次查询中，利用 NSLOOKUP 命令深入理解 DNS 的三层结构，通过逐级解析域名获取相关信息。此外，SMTP 协议的分析通过 TELNET 进行邮件发送，学习了邮件的格式和发送过程，同时观察协议交互。 实验三：最后，使用抓包软件 Ethereal 监测和分析网络协议的工作过程，捕获 HTTP 报文，理解了协议间的交互细节。
实验当中问题及解决方法	1. Nslookup 指令常出现超时现象，在使用 Nslookup 进行域名解析时，时常会遇到超时的情况，这通常是由于指定的 DNS 服务器未响应造成的。为了解决这个问题，可以尝试更改尝试访问的 DNS 服务器，例如从默认的本地 DNS 切换到其他公共 DNS 服务，如 Google 的 8.8.8.8 或 Cloudflare 的 1.1.1.1。通过不断调整，直到找到一个能够成功访问的服务器。 2. 登录电子邮件系统提示密码错误，在尝试登录电子邮件系统时，若提示密码错误，可以先检查输入是否正确。如果确认无误，则可能是因为使用的密码格式不符合要求。此时，可以前往 163 电子邮件官网，使用提供的 POP3 专用密码生成功能，生成一个新的专用密码。生成后，需要将其进行 Base64 编码，这样便能够成功登录 SMTP 服务器进行邮件发送。 3. Ethereal 进行分组俘获后，报文过多。在使用 Ethereal（现在称为 Wireshark）进行网络数据包捕获时，可能会发现抓取到的报文数量庞大，导致分析困难。为了解决这一问题，可以先关闭设备上多余的应用程序，以减少这些程序对网络的占用。接着，可以获取目标网站的 IP 地址，在 Ethereal 的过滤器中设置针对该 IP 地址的过滤规则，这样就可以筛选出所有与目标 IP 进行通信的报文，方便后续的分析和处理。

成绩（教师打分）	优秀	良好	及格	不及格