WireShark 实验-DNS

专业班级： 信息安全智息技术班　　**学号：** 21307130076　　**姓名：** 杨乙

【实验目的】

探索 DNS 协议

【实验结果】

分析操作，回答问题。

1.运行 nslookup 以获取任意一个亚洲 Web 服务器的 IP 地址。该服务器的 IP 地址是什么？

如图，IP 地址为 2408:8719:64:1f:8000::3 和 119.188.208.2
（一个域名可解析到多个 IP 地址，以实现 DNS 的负载均衡以及线路的智能选择）

2.运行 nslookup 来确定一个欧洲的大学（例如 berklee.edu）的权威 DNS 服务器

```
C:\Users\杨乙>nslookup -type=NS berklee.edu
服务器:  ns.fudan.edu.cn
Address:  202.120.224.26

非权威应答:
berklee.edu     nameserver = ns2.berklee.edu
berklee.edu     nameserver = ns3.p21.dynect.net
berklee.edu     nameserver = ns4.p21.dynect.net
berklee.edu     nameserver = ns1.p21.dynect.net
berklee.edu     nameserver = ns2.p21.dynect.net

ns1.p21.dynect.net      internet address = 108.59.161.21
ns1.p21.dynect.net      AAAA IPv6 address = 2600:2000:2210::21
ns2.p21.dynect.net      internet address = 108.59.162.21
ns2.p21.dynect.net      AAAA IPv6 address = 2600:2000:2220::21
ns2.berklee.edu internet address = 192.136.22.11
```

如图，berklee.edu 的权威 DNS 服务器有：

ns2.berklee.edu

ns3.p21.dynect.net

ns4.p21.dynect.net

ns1.p21.dynect.net

ns2.p21.dynect.net

（响应来自某个服务器的缓存）

3.运行 nslookup，是否可以使用问题 2 中一个已获得的 DNS 服务器，来查询 Yahoo!邮箱的邮件服务器(mail.yahoo.com)。若不行，是否可使用其它方法获得它的 IP 地址是什么？

无法查询。会出现如下几种问题：

（1）请求超时

```
C:\Users\杨乙>nslookup mail.yahoo.com ns1.p21.dynect.net
DNS request timed out.
    timeout was 2 seconds.
服务器:  UnKnown
Address:  108.59.161.21

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** 请求 UnKnown 超时
```

（2）未显示 IP 地址

```
C:\Users\杨乙>nslookup mail.yahoo.com ns4.p21.dynect.net
服务器:  ns4.p21.dynect.net
Address:  108.59.164.21

名称:    mail.yahoo.com
Served by:
- orans.null.bet

          mail.yahoo.com
```

（3）Query refused

```
C:\Users\杨乙>nslookup mail.yahoo.com ns2.berklee.edu
服务器:  ns2.berklee.edu
Address:  192.136.22.11

*** ns2.berklee.edu 找不到 mail.yahoo.com: Query refused
```

其它获得它的 IP 地址的方法：使用本地的 DNS 服务器查询

```
C:\Users\杨乙>nslookup mail.yahoo.com
服务器:  UnKnown
Address:  192.168.167.183

非权威应答:
名称:    edge.gycpi.b.yahoodns.net
Addresses:  2001:4998:64:800::6000
          2001:4998:64:800::6001
          69.147.80.12
          69.147.80.15
Aliases:  mail.yahoo.com
```

查询到的 IP 地址见上图

4. 找到 DNS 查询和响应消息。它们是否通过 UDP 或 TCP 发送？

```
Protocol: TCP (6)
```

如上图，通过 TCP 发送

5. DNS 查询消息的目标端口是什么？ DNS 响应消息的源端口是什么？

```
Transmission Control Protocol, Src Port: 53581, Dst Port: 53, Seq: 3, Ack: 1, Len: 28
    Source Port: 53581
    Destination Port: 53
    [Stream index: 4]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 28]
    Sequence Number: 3    (relative sequence number)
    Sequence Number (raw): 2122834194
    [Next Sequence Number: 31    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 4148944484
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 1029
    [Calculated window size: 263424]
    [Window size scaling factor: 256]
    Checksum: 0xbccf [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (28 bytes)
    [PDU Size: 30]
    TCP segment data (28 bytes)
> [2 Reassembled TCP Segments (30 bytes): #56(2), #57(28)]
> Domain Name System (query)
```

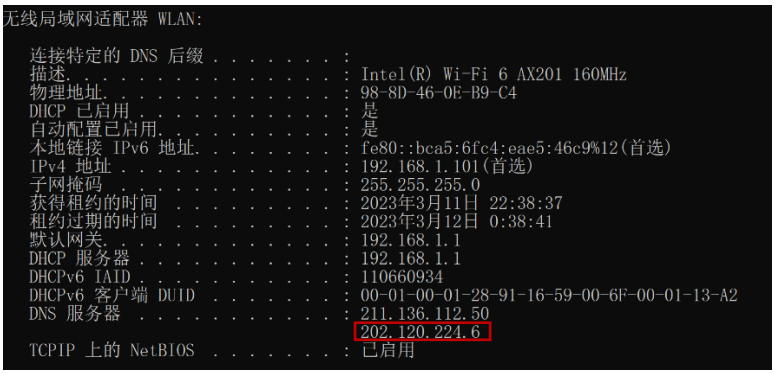
```
Transmission Control Protocol, Src Port: 53, Dst Port: 53581, Seq: 1, Ack: 31, Len: 428
    Source Port: 53
    Destination Port: 53581
    [Stream index: 4]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 428]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4148944484
    [Next Sequence Number: 429    (relative sequence number)]
    Acknowledgment Number: 31    (relative ack number)
    Acknowledgment number (raw): 2122834222
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 227
    [Calculated window size: 29056]
    [Window size scaling factor: 128]
    Checksum: 0xc117 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (428 bytes)
    [PDU Size: 428]
> Domain Name System (response)
```

如图，DNS 查询消息的目标端口和 DNS 响应消息的源端口都是 53

6. DNS 查询消息发送到哪个 IP 地址？使用 ipconfig 来确定本地 DNS 服务器的 IP 地址。这两个 IP 地址是否相同？

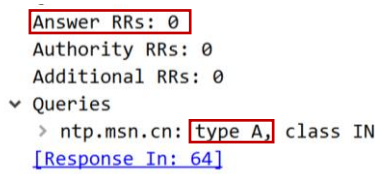
```
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 202.120.224.6
```

发送到 202.120.224.6



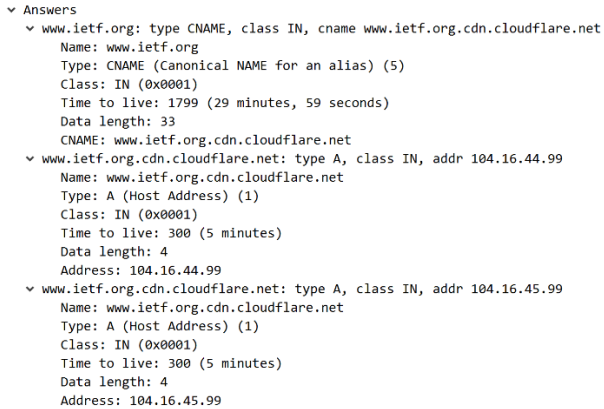
如图，这两个 IP 地址相同

7. 检查 DNS 查询消息。DNS 查询是什么"Type"的？查询消息是否包含任何"answers"？



如图，Type 是 A，查询消息不包含任何 answers

8. 检查 DNS 响应消息。提供了多少个"answers"？这些答案具体包含什么？



包含 3 个 answers，这些答案包含了 Name，Type，Value（位于最后一行，没有显式出现），TTL，Class，Data length 这些字段。其中 Name 和 Value 的值取决于 Type：当 Type = A

时，Name 是主机名，Value 是主机名对应的 IP 地址；当 Type = CNAME 时，Value 是别名为 Name 的主机对应的规范主机名。Class 是地址类型，通常为互联网地址，值为 1；Data length 是资源数据的长度；TTL 是记录生存时间，决定资源记录应当从缓存中删除的时间

9. 考虑从您主机发送的后续 TCP SYN 数据包。SYN 数据包的目的 IP 地址是否与 DNS 响应消息中提供的任何 IP 地址相对应？

SYN 数据包的目的 IP 地址：104.16.44.99

```
Source Address: 192.168.1.104
Destination Address: 104.16.44.99
```

与 DNS 响应消息提供的第二条 answers 的主机名对应的 IP 地址相对应：

```
Answers
  www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1799 (29 minutes, 59 seconds)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.44.99
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.45.99
```

当两台计算机在 TCP 连接上进行会话时，连接一定会首先被初始化。完成这项任务的包叫作 SYN。一个 SYN 包表明另一台计算机已经做好了会话的准备，两者之间连接建立。上述信息说明此计算机（192.168.1.104）与某台 DNS 服务器（104.16.44.99）建立了连接

10. 这个网页包含一些图片。在获取每个图片前，您的主机是否都发出了新的 DNS 查询？

没有。查看捕获的数据包，只发出了两个 DNS 查询，并收到了两个 DNS 响应，因此获取每个图片前主机不一定发起新的 DNS 查询

5075	20.692729	192.168.1.104	202.120.224.6	DNS	96 Standard query 0x75d2 HTTPS www.ietf.org
5076	20.692761	192.168.1.104	202.120.224.6	TCP	68 56662 → 53 [PSH, ACK] Seq=1 Ack=1 Win=263424 Len=2 TSval=307130435 TSecr=435049455 [TCP segment o
5077	20.692774	192.168.1.104	202.120.224.6	DNS	96 Standard query 0x2881 A www.ietf.org
5078	20.695114	202.120.224.6	192.168.1.104	TCP	66 53 → 56663 [ACK] Seq=1 Ack=3 Win=29056 Len=0 TSval=435049457 TSecr=307130435
5079	20.695861	202.120.224.6	192.168.1.104	TCP	66 53 → 56662 [ACK] Seq=1 Ack=3 Win=29056 Len=0 TSval=435049457 TSecr=307130435
5080	20.695861	202.120.224.6	192.168.1.104	TCP	66 53 → 56663 [ACK] Seq=1 Ack=33 Win=29056 Len=0 TSval=435049457 TSecr=307130435
5081	20.695861	202.120.224.6	192.168.1.104	TCP	66 53 → 56662 [ACK] Seq=1 Ack=33 Win=29056 Len=0 TSval=435049457 TSecr=307130435
5082	20.695861	202.120.224.6	192.168.1.104	DNS	532 Standard query response 0x75d2 HTTPS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net HTTPS NS
5083	20.695861	202.120.224.6	192.168.1.104	DNS	485 Standard query response 0x2881 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.9

（观察到第一个 DNS 查询类型为 HTTPS，查阅资料知，HTTPS rr 用于在不受信任的通道上分发，以提高安全性）

（以下实验中我的主机 IP 地址切换为 192.168.167.246）

11. DNS 查询消息的目标端口是什么？ DNS 响应消息的源端口是什么？

都是 53 号端口

```
User Datagram Protocol, Src Port: 64322, Dst Port: 53
    Source Port: 64322
    Destination Port: 53
    Length: 37
    Checksum: 0xd135 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (29 bytes)
```

```
User Datagram Protocol, Src Port: 53, Dst Port: 64323
    Source Port: 53
    Destination Port: 64323
    Length: 166
    Checksum: 0xfea3 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (158 bytes)
```

12. DNS 查询消息的目标 IP 地址是什么？这是你的默认本地 DNS 服务器的 IP 地址吗？

DNS 查询消息的目标 IP 地址：

```
19 2.401558    192.168.167.246    192.168.167.183    DNS    71 Standard query 0x0002 A www.mit.edu
```

我的默认本地 DNS 服务器的 IP 地址（二者相同）：

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   物理地址. . . . . . . . . . . . . : 98-8D-46-0E-B9-C4
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . . : 2409:891f:5b86:7a5:c72:1271:1b02:cdfb(首选)
   临时 IPv6 地址. . . . . . . . . . : 2409:891f:5b86:7a5:c9fc:2915:c02c:cea3(首选)
   本地链接 IPv6 地址. . . . . . . . : fe80::bca5:6fc4:eae5:46c9%12(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.167.246(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2023年3月12日 11:20:44
   租约过期的时间  . . . . . . . . . : 2023年3月12日 12:20:42
   默认网关. . . . . . . . . . . . . : fe80::349e:14ff:fef8:1479%12
                                       192.168.167.183
   DHCP 服务器 . . . . . . . . . . . : 192.168.167.183
   DHCPv6 IAID . . . . . . . . . . . : 110660934
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-28-91-16-59-00-6F-00-01-13-A2
   DNS 服务器  . . . . . . . . . . . : 192.168.167.183
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

13. 检查 DNS 查询消息。DNS 查询是什么"Type"的？查询消息是否包含任何"answers"？

```
> Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
v Queries
  > www.mit.edu: type A, class IN
  [Response In: 20]
```

DNS 查询 Type = A，查询消息不包含任何 answers

14. 检查 DNS 响应消息。提供了多少个"answers"？这些答案包含什么？

```
v Answers
  v www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  v www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 60 (1 minute)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  v e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1417:e800:185::255e
      Name: e9566.dscb.akamaiedge.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 30 (30 seconds)
      Data length: 16
      AAAA Address: 2600:1417:e800:185::255e
  v e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1417:e800:188::255e
      Name: e9566.dscb.akamaiedge.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 30 (30 seconds)
      Data length: 16
      AAAA Address: 2600:1417:e800:188::255e
```

DNS 响应消息提供了 4 个"answers"，这些答案包含了 Name，Type，Value（位于最后一行，没有显式出现），TTL，Class，Data length 这些字段。其中 Name 和 Value 的值取决于 Type：当 Type = AAAA 时，Name 是主机名，Value 是主机名对应的 IP 地址(AAAA 记录是用来将域名解析到 IPv6 地址的 DNS 记录)；当 Type = CNAME 时，Value 是别名为 Name 的主机对应的规范主机名。Class 是地址类型，通常为互联网地址，值为 1；Data length 是资源数据的长度；TTL 是记录生存时间，决定资源记录应当从缓存中删除的时间

15. DNS 查询消息发送到的 IP 地址是什么？这是您的默认本地 DNS 服务器的 IP 地址吗？

```
202 11.037394    192.168.167.246    192.168.167.183    DNS    67 Standard query 0x0002 NS mit.edu
```

DNS 查询消息发送到的 IP 地址是 192.168.167.183，是默认本地 DNS 服务器的 IP 地址

16. 检查 DNS 查询消息。DNS 查询是什么"Type"的？查询消息是否包含任何"answers"？

```
▾ Domain Name System (query)
    Transaction ID: 0x0002
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ mit.edu: type NS, class IN
    [Response In: 203]
```

DNS 查询 Type = NS，没有包含任何"answers"

17. 检查 DNS 响应消息。响应消息提供的 MIT 域名服务器是什么？此响应消息还提供了 MIT 域名服务器的 IP 地址吗？

```
▾ Queries
  ▸ mit.edu: type NS, class IN
▾ Answers
  ▸ mit.edu: type NS, class IN, ns asia1.akam.net
  ▸ mit.edu: type NS, class IN, ns eur5.akam.net
  ▸ mit.edu: type NS, class IN, ns use5.akam.net
  ▸ mit.edu: type NS, class IN, ns ns1-37.akam.net
  ▸ mit.edu: type NS, class IN, ns use2.akam.net
  ▸ mit.edu: type NS, class IN, ns usw2.akam.net
  ▸ mit.edu: type NS, class IN, ns asia2.akam.net
  ▸ mit.edu: type NS, class IN, ns ns1-173.akam.net
  [Request In: 202]
  [Time: 0.063408000 seconds]
```

响应消息提供的 MIT 域名服务器如上。没有提供 MIT 域名服务器的 IP 地址