DNS实验

林宸昊 PB20000034

1.
```
C:\Users\lenovo>nslookup omofun.tv
服务器:  UnKnown
Address:  192.168.43.1

非权威应答:
名称:    omofun.tv
Address:  154.214.13.29
```

   - IP地址为154.214.13.29（这真的是亚洲网站）。

2.
```
C:\Users\lenovo>nslookup -type=NS cam.ac.uk
服务器:  UnKnown
Address:  192.168.43.1

非权威应答:
cam.ac.uk        nameserver = auth0.dns.cam.ac.uk
cam.ac.uk        nameserver = ns3.mythic-beasts.com
cam.ac.uk        nameserver = dns0.eng.cam.ac.uk
cam.ac.uk        nameserver = dns0.c1.cam.ac.uk
cam.ac.uk        nameserver = ns1.mythic-beasts.com
cam.ac.uk        nameserver = ns2.ic.ac.uk

auth0.dns.cam.ac.uk     internet address = 131.111.8.37
dns0.c1.cam.ac.uk       internet address = 128.232.0.19
ns1.mythic-beasts.com   internet address = 45.33.127.156
dns0.eng.cam.ac.uk      internet address = 129.169.8.8
ns2.ic.ac.uk    internet address = 155.198.142.82
auth0.dns.cam.ac.uk     AAAA IPv6 address = 2001:630:212:8::d:a0
dns0.c1.cam.ac.uk       AAAA IPv6 address = 2a05:b400:110::d:a0
dns0.c1.cam.ac.uk       AAAA IPv6 address = 2001:630:212:200::d:a0
ns1.mythic-beasts.com   AAAA IPv6 address = 2600:3c00:e000:19::1
ns2.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::82
```

   - 所查询为剑桥大学网址。

3.
```
C:\Users\lenovo>nslookup youtube.com auth0.dns.cam.ac.uk
服务器:  auth0.dns.cam.ac.uk
Address:  131.111.8.37

非权威应答:
名称:    youtube.com
Addresses:  2001::c710:9e10
          211.104.160.39
```

   - 使用第一个DNS服务器查询youtube.com的服务器（yahoo怎么试都超时，gmail也超时）。

4.
```
192.168.43.112  192.168.43.1    DNS   72 Standard query 0x56e0 A www.ietf.org
192.168.43.1    192.168.43.112  DNS  149 Standard query response 0x56e0 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
```

   4-10

   - 查询报文：

```
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.43.112
Destination Address: 192.168.43.1
> User Datagram Protocol, Src Port: 51493, Dst Port: 53
```

- 响应报文：

```
Protocol: UDP (17)
Header Checksum: 0x0cf5 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.43.1
Destination Address: 192.168.43.112
> User Datagram Protocol, Src Port: 53, Dst Port: 51493
```

- 由图可看出均使用UDP协议；
- 查询的目标端口和响应的源端口均为53；
- 查询报文发送到IP地址192.168.43.1，通过ipconfig查询得本地DNS服务器IP：

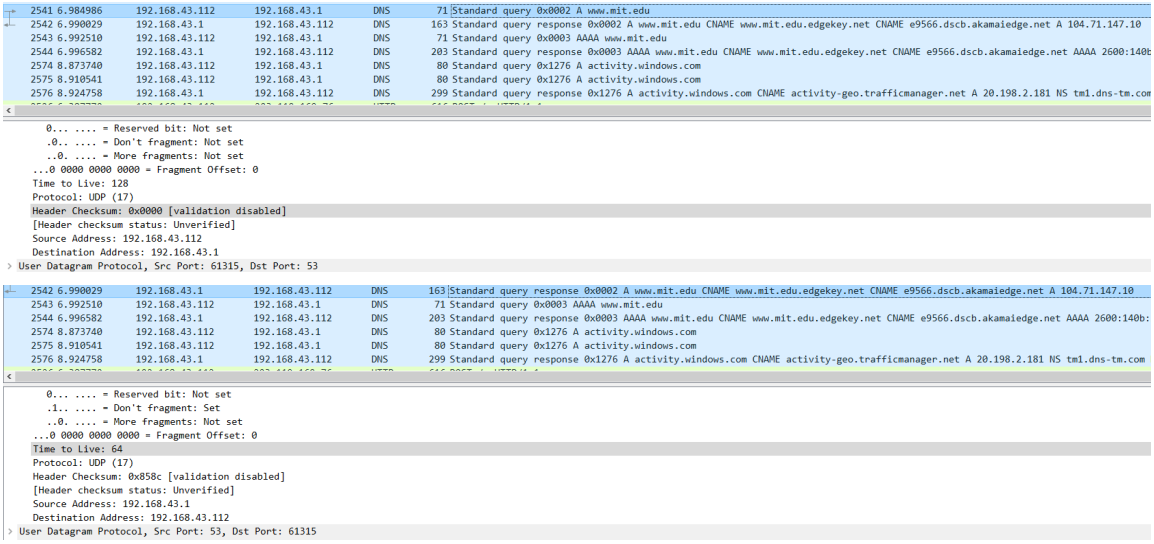
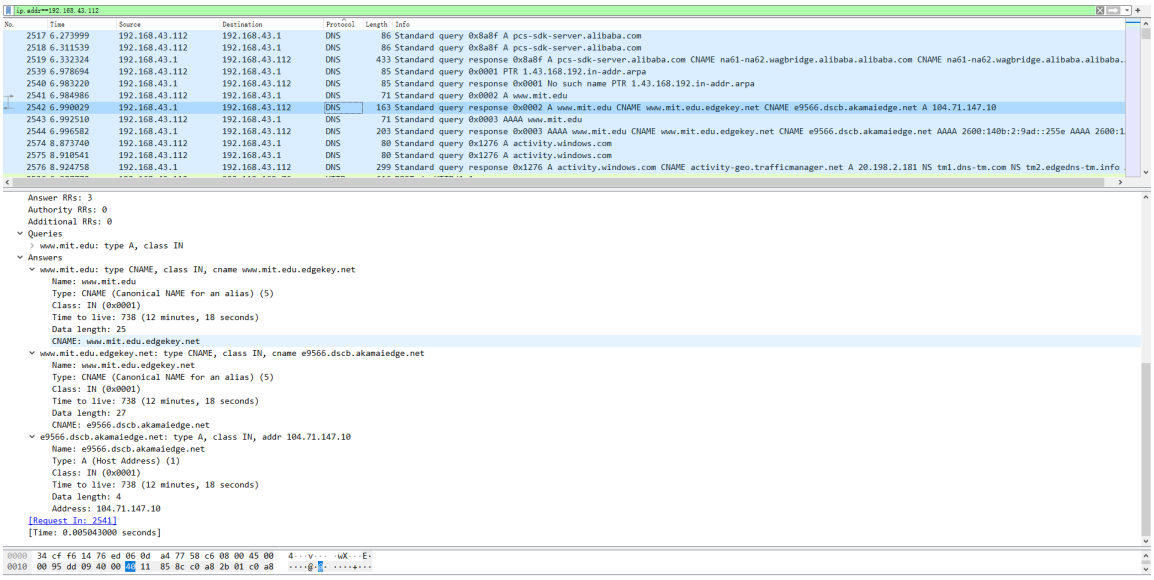
```
DNS 服务器  . . . . . . . . . . . . : 192.168.43.1
```

二者一致；

- ```
  v Domain Name System (query)
      Transaction ID: 0x56e0
    > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    v Queries
      > www.ietf.org: type A, class IN
      [Response In: 35]
  ```

由图可知为Type A，未包含answers；

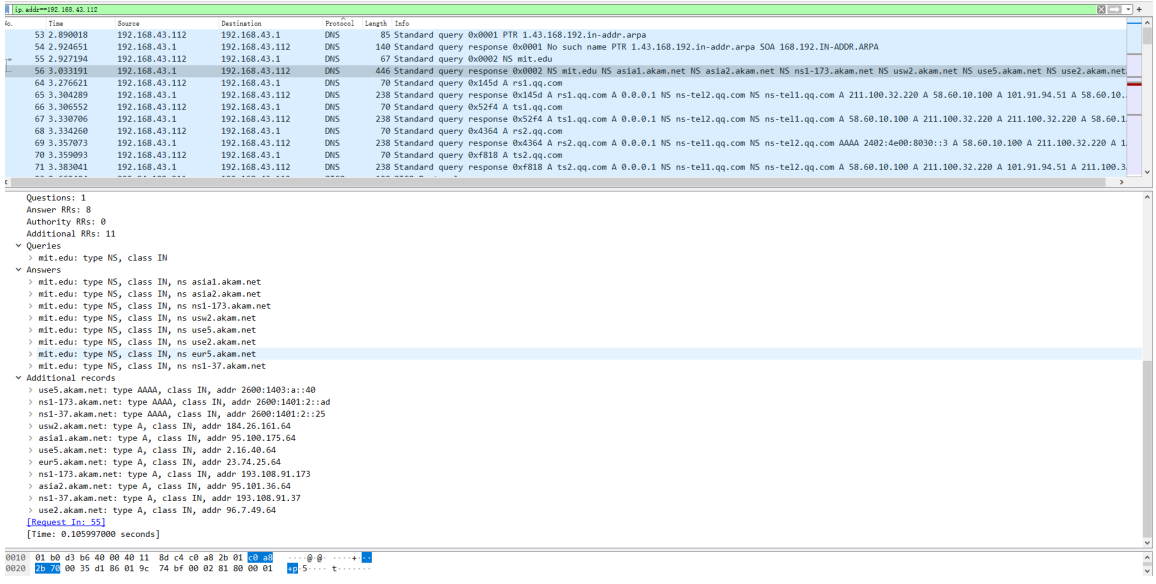
响应报文包含三个answers，具体为：

```
v 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: 834 (13 minutes, 54 seconds)
    Data length: 33
    CNAME: www.ietf.org.cdn.cloudflare.net
v 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: 834 (13 minutes, 54 seconds)
    Data length: 4
    Address: 104.16.45.99
```
```

```
▾ 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: 834 (13 minutes, 54 seconds)
    Data length: 4
    Address: 104.16.44.99
```

- ```
  192.168.43.112    104.16.45.99    TCP    66 13546 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  192.168.43.112    104.16.45.99    TCP    66 13547 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  ```

  与上图中第二张图IP地址相同；
- 没有，仅发出一次DNS查询。

5. 11-23

- 

  ```
  2541 6.984986   192.168.43.112   192.168.43.1     DNS   71 Standard query 0x0002 A www.mit.edu
  2542 6.990029   192.168.43.1     192.168.43.112   DNS  163 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.71.147.10
  2543 6.992510   192.168.43.112   192.168.43.1     DNS   71 Standard query 0x0003 AAAA www.mit.edu
  2544 6.996582   192.168.43.1     192.168.43.112   DNS  203 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2600:140b
  2574 8.873740   192.168.43.112   192.168.43.1     DNS   80 Standard query 0x1276 A activity.windows.com
  2575 8.910541   192.168.43.112   192.168.43.1     DNS   80 Standard query 0x1276 A activity.windows.com
  2576 8.924758   192.168.43.1     192.168.43.112   DNS  299 Standard query response 0x1276 A activity.windows.com CNAME activity-geo.trafficmanager.net A 20.198.2.181 NS tm1.dns-tm.com
  ```

  ```
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.43.112
  Destination Address: 192.168.43.1
  > User Datagram Protocol, Src Port: 61315, Dst Port: 53
  ```

  ```
  2542 6.990029   192.168.43.1     192.168.43.112   DNS  163 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.71.147.10
  2543 6.992510   192.168.43.112   192.168.43.1     DNS   71 Standard query 0x0003 AAAA www.mit.edu
  2544 6.996582   192.168.43.1     192.168.43.112   DNS  203 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2600:140b:
  2574 8.873740   192.168.43.112   192.168.43.1     DNS   80 Standard query 0x1276 A activity.windows.com
  2575 8.910541   192.168.43.112   192.168.43.1     DNS   80 Standard query 0x1276 A activity.windows.com
  2576 8.924758   192.168.43.1     192.168.43.112   DNS  299 Standard query response 0x1276 A activity.windows.com CNAME activity-geo.trafficmanager.net A 20.198.2.181 NS tm1.dns-tm.com
  ```

  ```
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0x858c [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.43.1
  Destination Address: 192.168.43.112
  > User Datagram Protocol, Src Port: 53, Dst Port: 61315
  ```

  如图，二者均为53；
- 查询地址是192.168.43.1，是默认本地DNS服务器地址；
- ```
  Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▾ Queries
    > www.mit.edu: type A, class IN
  ```

  Type A，没有answers；

  响应报文包含如下三个answers：

```
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: 738 (12 minutes, 18 seconds)
    Data length: 25
    CNAME: www.mit.edu.edgekey.net
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: 738 (12 minutes, 18 seconds)
    Data length: 27
    CNAME: e9566.dscb.akamaiedge.net
e9566.dscb.akamaiedge.net: type A, class IN, addr 104.71.147.10
    Name: e9566.dscb.akamaiedge.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 738 (12 minutes, 18 seconds)
    Data length: 4
    Address: 104.71.147.10
```

整体截图如下：




- ```
  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
  ```

```
192.168.43.112      192.168.43.1      DNS      67 Standard query 0x0002 NS mit.edu
```

查询报文发送到192.168.43.1，与本地DNS服务器IP地址相同；

Type NS，不包含answers；

响应报文如下：
```

```
Answer RRs: 8
Authority RRs: 0
Additional RRs: 11
▾ 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 asia2.akam.net
  › mit.edu: type NS, class IN, ns ns1-173.akam.net
  › mit.edu: type NS, class IN, ns usw2.akam.net
  › mit.edu: type NS, class IN, ns use5.akam.net
  › mit.edu: type NS, class IN, ns use2.akam.net
  › mit.edu: type NS, class IN, ns eur5.akam.net
  › mit.edu: type NS, class IN, ns ns1-37.akam.net
▾ Additional records
  › use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
  › ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
  › ns1-37.akam.net: type AAAA, class IN, addr 2600:1401:2::25
  › usw2.akam.net: type A, class IN, addr 184.26.161.64
  › asia1.akam.net: type A, class IN, addr 95.100.175.64
  › use5.akam.net: type A, class IN, addr 2.16.40.64
  › eur5.akam.net: type A, class IN, addr 23.74.25.64
  › ns1-173.akam.net: type A, class IN, addr 193.108.91.173
  › asia2.akam.net: type A, class IN, addr 95.101.36.64
  › ns1-37.akam.net: type A, class IN, addr 193.108.91.37
  › use2.akam.net: type A, class IN, addr 96.7.49.64
```

提供了8个域名服务器，并且均提供了IP地址；

- 整体截图如下：



- 

查询报文发送到96.7.49.64，并非本机DNS服务器地址，而是指定的域名服务器地址；

-

```
Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > mit.edu: type A, class IN
```

Type A，无answers；

响应报文包含一个answers：

```
Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8500 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > mit.edu: type A, class IN
  v Answers
    v mit.edu: type A, class IN, addr 104.86.4.124
        Name: mit.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 4
        Address: 104.86.4.124
```

- 整体截图如下：