

# DNS 实验报告

PB20111689 蓝俊玮

## nslookup

1. 在 WSL2 终端运行 `nslookup www.ustc.edu.cn` 后会得到一个 IP 地址为 **202.38.64.246**

```
ljwt13@LAPTOP-LAN:~$ nslookup www.ustc.edu.cn
Server:      172.24.192.1
Address:     172.24.192.1#53

Non-authoritative answer:
Name:   www.ustc.edu.cn
Address: 202.38.64.246
Name:   www.ustc.edu.cn
Address: 2001:da8:d800:642::246

ljwt13@LAPTOP-LAN:~$
```

2. 我选取的是英国的牛津大学，在终端运行 `nslookup -type=NS ox.ac.uk` 后，共返回了 **7** 个权威域名服务器名

```
ljwt13@LAPTOP-LAN:~$ nslookup -type=NS ox.ac.uk
Server:      172.24.192.1
Address:     172.24.192.1#53

Non-authoritative answer:
ox.ac.uk      nameserver = dns0.ox.ac.uk.
ox.ac.uk      nameserver = auth6.dns.ox.ac.uk.
ox.ac.uk      nameserver = dns2.ox.ac.uk.
ox.ac.uk      nameserver = dns1.ox.ac.uk.
ox.ac.uk      nameserver = auth4.dns.ox.ac.uk.
ox.ac.uk      nameserver = ns2.ja.net.
ox.ac.uk      nameserver = auth5.dns.ox.ac.uk.

Authoritative answers can be found from:

ljwt13@LAPTOP-LAN:~$
```

3. (这里因为我的 WSL2 访问一直被拒绝，所以在这里我使用了学校的 vlab 进行操作) 在终端运行 `nslookup mail.yahoo.com dns0.ox.ac.uk` 可以返回得到的 IP 地址有 **69.147.80.15** 和 **69.147.80.12**

```
ljwt13@LAPTOP-LAN:~$ nslookup mail.yahoo.com dns0.ox.ac.uk
Server:      dns0.ox.ac.uk
Address:     129.67.1.190#53

Non-authoritative answer:
mail.yahoo.com canonical name = edge.gycpi.b.yahoodns.net.
Name:   edge.gycpi.b.yahoodns.net
Address: 69.147.80.15
Name:   edge.gycpi.b.yahoodns.net
Address: 69.147.80.12
Name:   edge.gycpi.b.yahoodns.net
Address: 2406:2000:a8:800::e7
Name:   edge.gycpi.b.yahoodns.net
Address: 2406:2000:a8:800::e6

ljwt13@VM3103-Lan13:/home/ubuntu/desktop#
```

## ipconfig

## Tracing DNS with Wireshark

#### 4. DNS 的查询报文和响应报文采用的都是 UDP 的方式运输

No.	Time	Source	Destination	Protocol	Length	Info
19	4.986132	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x8b08 A www.ietf.org
20	4.986839	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x55db AAAA www.ietf.org
26	5.223499	202.38.64.56	114.214.176.129	DNS	149	Standard query response 0x8b08 A www.ietf.org
30	5.983208	114.214.176.129	202.38.64.17	DNS	72	Standard query 0x55db AAAA www.ietf.org
31	6.145173	202.38.64.17	114.214.176.129	DNS	173	Standard query response 0x55db AAAA www.ietf.org
34	6.162580	114.214.176.129	202.38.64.56	DNS	94	Standard query 0xee7a A nav-edge.smartscreen.microsoft.com
35	6.166017	202.38.64.56	114.214.176.129	DNS	237	Standard query response 0xee7a A nav-edge.smartscreen.microsoft.com
289	7.528947	202.38.64.56	114.214.176.129	DNS	173	Standard query response 0x55db AAAA www.ietf.org
328	7.572090	114.214.176.129	202.38.64.56	DNS	78	Standard query 0x4278 A analytics.ietf.org
329	7.572388	114.214.176.129	202.38.64.56	DNS	78	Standard query 0x17ef AAAA analytics.ietf.org

> Frame 19: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF\_{78348DFD-6104-46FF-8000-000000000000} (0.0.0.0)

> Ethernet II, Src: LiteonTe\_17:ac:48 (80:30:49:17:ac:48), Dst: Hangzhou\_91:72:e2 (5c:dd:70:91:72:e2)

> Internet Protocol Version 4, Src: 114.214.176.129, Dst: 202.38.64.56

> User Datagram Protocol, Src Port: 63875, Dst Port: 53

Source Port: 63875

Destination Port: 53

Length: 38

Checksum: 0x2ae5 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

> [Timestamps]

UDP payload (30 bytes)

> Domain Name System (query)

No.	Time	Source	Destination	Protocol	Length	Info
19	4.986132	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x8b08 A www.ietf.org
20	4.986839	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x55db AAAA www.ietf.org
26	5.223499	202.38.64.56	114.214.176.129	DNS	149	Standard query response 0x8b08 A www.ietf.org
30	5.983208	114.214.176.129	202.38.64.17	DNS	72	Standard query 0x55db AAAA www.ietf.org
31	6.145173	202.38.64.17	114.214.176.129	DNS	173	Standard query response 0x55db AAAA www.ietf.org
34	6.162580	114.214.176.129	202.38.64.56	DNS	94	Standard query 0xee7a A nav-edge.smartscreen.microsoft.com
35	6.166017	202.38.64.56	114.214.176.129	DNS	237	Standard query response 0xee7a A nav-edge.smartscreen.microsoft.com
289	7.528947	202.38.64.56	114.214.176.129	DNS	173	Standard query response 0x55db AAAA www.ietf.org
328	7.572090	114.214.176.129	202.38.64.56	DNS	78	Standard query 0x4278 A analytics.ietf.org
329	7.572388	114.214.176.129	202.38.64.56	DNS	78	Standard query 0x17ef AAAA analytics.ietf.org

> Frame 26: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF\_{78348DFD-6104-46FF-8000-000000000000} (0.0.0.0)

> Ethernet II, Src: Hangzhou\_91:72:e2 (5c:dd:70:91:72:e2), Dst: LiteonTe\_17:ac:48 (80:30:49:17:ac:48)

> Internet Protocol Version 4, Src: 202.38.64.56, Dst: 114.214.176.129

> User Datagram Protocol, Src Port: 53, Dst Port: 63875

Source Port: 53

Destination Port: 63875

Length: 115

Checksum: 0xd691 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

> [Timestamps]

UDP payload (107 bytes)

> Domain Name System (response)

#### 5. DNS 查询报文的目标端口是 53，而响应报文的源端口也是 53

No.	Time	Source	Destination	Protocol	Length	Info
19	4.986132	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x8b08 A www.ietf.org
20	4.986839	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x55db AAAA www.ietf.org
26	5.223499	202.38.64.56	114.214.176.129	DNS	149	Standard query response 0x8b08 A www.ietf.org
30	5.983208	114.214.176.129	202.38.64.17	DNS	72	Standard query 0x55db AAAA www.ietf.org
31	6.145173	202.38.64.17	114.214.176.129	DNS	173	Standard query response 0x55db AAAA www.ietf.org
34	6.162580	114.214.176.129	202.38.64.56	DNS	94	Standard query 0xee7a A nav-edge.smartscreen.microsoft.com
35	6.166017	202.38.64.56	114.214.176.129	DNS	237	Standard query response 0xee7a A nav-edge.smartscreen.microsoft.com
289	7.528947	202.38.64.56	114.214.176.129	DNS	173	Standard query response 0x55db AAAA www.ietf.org
328	7.572090	114.214.176.129	202.38.64.56	DNS	78	Standard query 0x4278 A analytics.ietf.org
329	7.572388	114.214.176.129	202.38.64.56	DNS	78	Standard query 0x17ef AAAA analytics.ietf.org

> Frame 19: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF\_{78348DFD-6104-46FF-8000-000000000000} (0.0.0.0)

> Ethernet II, Src: LiteonTe\_17:ac:48 (80:30:49:17:ac:48), Dst: Hangzhou\_91:72:e2 (5c:dd:70:91:72:e2)

> Internet Protocol Version 4, Src: 114.214.176.129, Dst: 202.38.64.56

> User Datagram Protocol, Src Port: 63875, Dst Port: 53

Source Port: 63875

Destination Port: 53

Length: 38

Checksum: 0x2ae5 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

> [Timestamps]

UDP payload (30 bytes)

> Domain Name System (query)

No.	Time	Source	Destination	Protocol	Length	Info
19	4.986132	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x8b08 A www.ietf.org
20	4.986839	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x55db AAAA www.ietf.org
26	5.223499	202.38.64.56	114.214.176.129	DNS	149	Standard query response 0x8b08 A www.ietf.org
30	5.983208	114.214.176.129	202.38.64.17	DNS	72	Standard query 0x55db AAAA www.ietf.org
31	6.145173	202.38.64.17	114.214.176.129	DNS	173	Standard query response 0x55db AAAA www.ietf.org
34	6.162580	114.214.176.129	202.38.64.56	DNS	94	Standard query 0xee7a A nav-edge.smart
35	6.166017	202.38.64.56	114.214.176.129	DNS	237	Standard query response 0xee7a A nav-edge.smart
289	7.528947	202.38.64.56	114.214.176.129	DNS	173	Standard query response 0x55db AAAA www.ietf.org
328	7.572090	114.214.176.129	202.38.64.56	DNS	78	Standard query 0x4278 A analytics.ietf.org
329	7.572388	114.214.176.129	202.38.64.56	DNS	78	Standard query 0x17ef AAAA analytics.ietf.org

> Frame 26: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF\_{78348DFD-...}

> Ethernet II, Src: Hangzhou\_91:72:e2 (5c:dd:70:91:72:e2), Dst: LiteonTe\_17:ac:48 (80:30:49:17:ac:48)

> Internet Protocol Version 4, Src: 202.38.64.56, Dst: 114.214.176.129

> User Datagram Protocol, Src Port: 53, Dst Port: 63875

Source Port: 53

Destination Port: 63875

Length: 115

Checksum: 0xd691 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

> [Timestamps]

UDP payload (107 bytes)

> Domain Name System (response)

6. DNS 查询报文的目标 IP 地址是 **202.38.64.56**，与本地 DNS 服务器的 IP 地址是相等的

No.	Time	Source	Destination	Protocol	Length	Info
19	4.986132	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x8b08 A www.ietf.org
20	4.986839	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x55db AAAA www.ietf.org
26	5.223499	202.38.64.56	114.214.176.129	DNS	149	Standard query response 0x8b08 A www.ietf.org
30	5.983208	114.214.176.129	202.38.64.17	DNS	72	Standard query 0x55db AAAA www.ietf.org
31	6.145173	202.38.64.17	114.214.176.129	DNS	173	Standard query response 0x55db AAAA www.ietf.org
34	6.162580	114.214.176.129	202.38.64.56	DNS	94	Standard query 0xee7a A nav-edge.smart
35	6.166017	202.38.64.56	114.214.176.129	DNS	237	Standard query response 0xee7a A nav-edge.smart
289	7.528947	202.38.64.56	114.214.176.129	DNS	173	Standard query response 0x55db AAAA www.ietf.org
328	7.572090	114.214.176.129	202.38.64.56	DNS	78	Standard query 0x4278 A analytics.ietf.org
329	7.572388	114.214.176.129	202.38.64.56	DNS	78	Standard query 0x17ef AAAA analytics.ietf.org

> Frame 19: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF\_{78348DFD-6104-...}

> Ethernet II, Src: LiteonTe\_17:ac:48 (80:30:49:17:ac:48), Dst: Hangzhou\_91:72:e2 (5c:dd:70:91:72:e2)

> Internet Protocol Version 4, Src: 114.214.176.129, Dst: 202.38.64.56

> User Datagram Protocol, Src Port: 63875, Dst Port: 53

> Domain Name System (query)

```

无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . : uisc.edu.cn
   描述 . . . . . : Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
   物理地址 . . . . . : 80-30-49-17-AC-48
   DHCP 已启用 . . . . . : 是
   自动配置已启用 . . . . . : 是
   IPv6 地址 . . . . . : 2001:da8:d800:189:8826:41fd:7398:1b4b(首选)
   临时 IPv6 地址 . . . . . : 2001:da8:d800:189:6509:2523:a41f:e73f(首选)
   本地链接 IPv6 地址 . . . . . : fe80::8826:41fd:7398:1b4b%11(首选)
   IPv4 地址 . . . . . : 114.214.176.129(首选)
   子网掩码 . . . . . : 255.255.240.0
   获得租约的时间 . . . . . : 2022年9月26日 19:03:26
   租约过期的时间 . . . . . : 2022年9月26日 20:33:28
   默认网关 . . . . . : fe80::5edd:70ff:fe91:72e2%11
   . . . . . : 114.214.191.254
   DHCP 服务器 . . . . . : 202.38.64.17
   DHCPv6 IAID . . . . . : 109064265
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2A-4A-1B-6D-80-30-49-17-AC-3F
   DNS 服务器 . . . . . : 202.38.64.56
   . . . . . : 202.38.64.17
   TCP/IP 上的 NetBIOS . . . . . : 已启用
  
```

7. DNS 查询报文的类型 Type 是 A，没有任何 answers，因为其标志了响应报文在第 26 个分组中

No.	Time	Source	Destination	Protocol	Length	Info
19	4.986132	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x8b08 A www.ietf.org
20	4.986839	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x55db AAAA www.ietf.org
26	5.223499	202.38.64.56	114.214.176.129	DNS	149	Standard query response 0x8b08 A www.ietf.org
30	5.983208	114.214.176.129	202.38.64.17	DNS	72	Standard query 0x55db AAAA www.ietf.org
31	6.145173	202.38.64.17	114.214.176.129	DNS	173	Standard query response 0x55db AAAA www.ietf.org
34	6.162580	114.214.176.129	202.38.64.56	DNS	94	Standard query 0xee7a A nav-edge.smart
35	6.166017	202.38.64.56	114.214.176.129	DNS	237	Standard query response 0xee7a A nav-edge.smart
289	7.528947	202.38.64.56	114.214.176.129	DNS	173	Standard query response 0x55db AAAA www.ietf.org
328	7.572090	114.214.176.129	202.38.64.56	DNS	78	Standard query 0x4278 A analytics.ietf.org
329	7.572388	114.214.176.129	202.38.64.56	DNS	78	Standard query 0x17ef AAAA analytics.ietf.org

> User Datagram Protocol, Src Port: 63875, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x8b08

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

> www.ietf.org: type A, class IN

Name: www.ietf.org

[Name Length: 12]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

[Response In: 26]

8. 这一个 DNS 响应报文中 有 3 个 `answers`。第一个 `answer` 中的 `type` 是 CNAME，包含了 [www.ietf.org](http://www.ietf.org) 的规范主机名；第二个和第三个 `answer` 的 `type` 都是 A，包含了该规范主机名对应的 IP 地址。

dns						
No.	Time	Source	Destination	Protocol	Length	Info
19	4.986132	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x8b08 A www.ietf.org
20	4.986839	114.214.176.129	202.38.64.56	DNS	72	Standard query 0x55db AAAA www.ietf.org
26	5.223499	202.38.64.56	114.214.176.129	DNS	149	Standard query response 0x8b08 A www.ietf.org
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: 176 (2 minutes, 56 seconds)						
Data length: 33						
CNAME: www.ietf.org.cdn.cloudflare.net						
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						
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						
[Request In: 19]						
[Time: 0.237367000 seconds]						

9. 在后续发送的 TCP SYN 分组中，TCP SYN 分组的目标 IP 地址与 DNS 响应报文所返回 IP 地址是**有**关联的

tcp						
No.	Time	Source	Destination	Protocol	Length	Info
43	6.282510	2606:4700::6810:2c63	2001:da8:d800:189:6...	TCP	74	80 → 49352 [ACK] Seq=1 Ack=468 Win=65536 Len=0
44	6.300920	2606:4700::6810:2c63	2001:da8:d800:189:6...	HTTP	377	HTTP/1.1 301 Moved Permanently
45	6.305646	2001:da8:d800:189:6...	2606:4700::6810:2c63	TCP	86	49356 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 W
46	6.319971	114.214.176.129	20.212.97.243	TCP	66	49359 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
47	6.336813	20.212.97.243	114.214.176.129	TCP	1514	443 → 49355 [ACK] Seq=1 Ack=518 Win=525056 Len=146
48	6.336813	20.212.97.243	114.214.176.129	TCP	1514	443 → 49355 [ACK] Seq=1461 Ack=518 Win=525056 Len=0
49	6.336999	114.214.176.129	20.212.97.243	TCP	54	49355 → 443 [ACK] Seq=518 Ack=2921 Win=66048 Len=0
50	6.346528	2001:da8:d800:189:6...	2606:4700::6810:2c63	TCP	74	49352 → 80 [ACK] Seq=468 Ack=304 Win=66304 Len=0
51	6.455330	20.212.97.243	114.214.176.129	TCP	66	443 → 49359 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
52	6.455618	114.214.176.129	20.212.97.243	TCP	54	49359 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
53	6.462622	114.214.176.129	104.16.45.99	TCP	66	49360 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS
54	6.477312	114.214.176.129	20.212.97.243	TCP	54	Client Hello
> Frame 53: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{783480FD-6104-46FE-923D-EF}						
> Ethernet II, Src: LiteonTe_17:ac:48 (80:30:49:17:ac:48), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)						
> Internet Protocol Version 4, Src: 114.214.176.129, Dst: 104.16.45.99						
0100 ... = Version: 4						
... 0101 = Header Length: 20 bytes (5)						
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 52						
Identification: 0x86b2 (34482)						
> Flags: 0x40, Don't fragment						
... 0 0000 0000 0000 = Fragment Offset: 0						
Time to Live: 128						
Protocol: TCP (6)						
Header Checksum: 0xbb46 [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 114.214.176.129						
Destination Address: 104.16.45.99						

10. 没有，在检索每个图片时，并没有发送新的 DNS 请求（除去无关的 smartscreen 请求以及与 IPv4 对应的 `type` 为 AAAA 的 DNS IPv6 请求）

No.	Time	Source	Destination	Protocol	Length	Info
23	5.065416	2600:140e:6::17ca:2...	2001:da8:d800:189:6...	TLSv1.2	98	Application Data
24	5.065416	2600:140e:6::17ca:2...	2001:da8:d800:189:6...	TCP	74	443 → 65007 [FIN, ACK] Seq=25 Ack=3 Win=501 Len=0
25	5.065558	2001:da8:d800:189:6...	2600:140e:6::17ca:2...	TCP	74	65007 → 443 [RST, ACK] Seq=3 Ack=25 Win=0 Len=0
26	5.223499	202.38.64.56	114.214.176.129	DNS	149	Standard query response 0x8b08 A www.ietf.org CNAME www.ietf.org.cdn.cl
27	5.311099	114.214.176.129	40.126.35.86	TCP	54	[TCP Retransmission] 65014 → 443 [FIN, ACK] Seq=2 Ack=1 Win=258 Len=0
28	5.919272	114.214.176.129	40.126.35.86	TCP	54	[TCP Retransmission] 65014 → 443 [FIN, ACK] Seq=2 Ack=1 Win=258 Len=0
29	5.978551	2001:da8:d800:189:11	ff02::1:ffbd:6caa	ICMPv6	86	Neighbor Solicitation for 2001:da8:d800:189:e547:ed91:febd:6caa from 5c
30	5.983208	114.214.176.129	202.38.64.17	TCP	72	Standard query 0x55db AAAA www.ietf.org
31	6.145173	202.38.64.17	114.214.176.129	DNS	173	Standard query response 0x55db AAAA www.ietf.org CNAME www.ietf.org.cdn
32	6.146563	2001:da8:d800:189:6...	2606:4700::6810:2c63	TCP	86	49351 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
33	6.148454	2001:da8:d800:189:6...	2606:4700::6810:2c63	TCP	86	49352 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
34	6.162580	114.214.176.129	202.38.64.56	TCP	94	Standard query 0xee7a A nav-edge.smartscreen.microsoft.com
35	6.166017	202.38.64.56	114.214.176.129	DNS	237	Standard query response 0xee7a A nav-edge.smartscreen.microsoft.com CNA
36	6.168176	114.214.176.129	20.212.97.243	TCP	66	49355 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
37	6.216070	2606:4700::6810:2c63	2001:da8:d800:189:6...	TCP	86	80 → 49352 [SYN, ACK] Seq=0 Ack=1 Win=65280 Len=0 MSS=1360 SACK_PERM=1
38	6.216238	2001:da8:d800:189:6...	2606:4700::6810:2c63	TCP	74	49352 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
39	6.216879	2001:da8:d800:189:6...	2606:4700::6810:2c63	HTTP	541	GET / HTTP/1.1
40	6.244937	20.212.97.243	114.214.176.129	TCP	66	443 → 49355 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK
41	6.245140	114.214.176.129	20.212.97.243	TCP	54	49355 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
42	6.264117	114.214.176.129	20.212.97.243	TLSv1.2	571	Client Hello
43	6.282510	2606:4700::6810:2c63	2001:da8:d800:189:6...	TCP	74	80 → 49352 [ACK] Seq=1 Ack=468 Win=65536 Len=0
44	6.300920	2606:4700::6810:2c63	2001:da8:d800:189:6...	HTTP	377	HTTP/1.1 301 Moved Permanently

nslookup [www.mit.edu](http://www.mit.edu)

11. DNS 查询报文的目标端口是 **53**，而 DNS 响应报文的目标端口也是 **53**

No.	Time	Source	Destination	Protocol	Length	Info
33	16.504...	114.214.176.129	120.92.107.7	TCP	55	50072 → 443 [ACK] Seq=1 Ack=1 Win=512
34	16.526...	120.92.107.7	114.214.176.129	TCP	66	443 → 50072 [ACK] Seq=1 Ack=2 Win=66
35	16.616...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=4
37	17.713...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=5
38	18.635...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=6
40	19.656...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=7
41	20.683...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=8
42	20.780...	114.214.176.129	202.38.64.56	DNS	85	Standard query 0x0001 PTR 56.64.38.20
43	20.790...	202.38.64.56	114.214.176.129	DNS	138	Standard query response 0x0001 PTR 56
44	20.795...	114.214.176.129	202.38.64.56	DNS	71	Standard query 0x0002 A www.mit.edu
45	21.092...	202.38.64.56	114.214.176.129	DNS	163	Standard query response 0x0002 A www.i

> Frame 44: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF\_{78348DFD-6104}

> Ethernet II, Src: LiteonTe\_17:ac:48 (80:30:49:17:ac:48), Dst: Hangzhou\_91:72:e2 (5c:dd:70:91:72:e2)

> Internet Protocol Version 4, Src: 114.214.176.129, Dst: 202.38.64.56

> User Datagram Protocol, Src Port: 61521, Dst Port: 53

Source Port: 61521

Destination Port: 53

Length: 37

Checksum: 0x8eb9 [unverified]

[Checksum Status: Unverified]

[Stream index: 2]

> [Timestamps]

UDP payload (29 bytes)

> Domain Name System (query)

No.	Time	Source	Destination	Protocol	Length	Info
33	16.504...	114.214.176.129	120.92.107.7	TCP	55	50072 → 443 [ACK] Seq=1 Ack=1 Win=512
34	16.526...	120.92.107.7	114.214.176.129	TCP	66	443 → 50072 [ACK] Seq=1 Ack=2 Win=66
35	16.616...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=4
37	17.713...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=5
38	18.635...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=6
40	19.656...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=7
41	20.683...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=8
42	20.780...	114.214.176.129	202.38.64.56	DNS	85	Standard query 0x0001 PTR 56.64.38.20
43	20.790...	202.38.64.56	114.214.176.129	DNS	138	Standard query response 0x0001 PTR 56
44	20.795...	114.214.176.129	202.38.64.56	DNS	71	Standard query 0x0002 A www.mit.edu
45	21.092...	202.38.64.56	114.214.176.129	DNS	163	Standard query response 0x0002 A www.i

> Frame 45: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface \Device\NPF\_{78348DFD-6104}

> Ethernet II, Src: Hangzhou\_91:72:e2 (5c:dd:70:91:72:e2), Dst: LiteonTe\_17:ac:48 (80:30:49:17:ac:48)

> Internet Protocol Version 4, Src: 202.38.64.56, Dst: 114.214.176.129

> User Datagram Protocol, Src Port: 53, Dst Port: 61521

Source Port: 53

Destination Port: 61521

Length: 129

Checksum: 0xc8e1 [unverified]

[Checksum Status: Unverified]

[Stream index: 2]

> [Timestamps]

UDP payload (121 bytes)

> Domain Name System (response)

12. DNS 查询报文发送的目标 IP 地址是 **202.38.64.56**，是我本地默认的 DNS 服务器的 IP 地址



ip.addr == 114.214.176.129						
No.	Time	Source	Destination	Protocol	Length	Info
33	16.504...	114.214.176.129	120.92.107.7	TCP	55	50072 → 443 [ACK] Seq=1 Ack=1 Win=512
34	16.526...	120.92.107.7	114.214.176.129	TCP	66	443 → 50072 [ACK] Seq=1 Ack=2 Win=66 Len=0
35	16.616...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=4/
37	17.713...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=5/
38	18.635...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=6/
40	19.656...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=7/
41	20.683...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=8/
42	20.780...	114.214.176.129	202.38.64.56	DNS	85	Standard query 0x0001 PTR 56.64.38.202
43	20.790...	202.38.64.56	114.214.176.129	DNS	138	Standard query response 0x0001 PTR 56.
44	20.795...	114.214.176.129	202.38.64.56	DNS	71	Standard query 0x0002 A www.mit.edu
45	21.092...	202.38.64.56	114.214.176.129	DNS	163	Standard query response 0x0002 A www.m

> Frame 44: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF\_{78348DFD-6104-  
 > Ethernet II, Src: LiteonTe\_17:ac:48 (80:30:49:17:ac:48), Dst: Hangzhou\_91:72:e2 (5c:dd:70:91:72:e2)  
 > Internet Protocol Version 4, Src: 114.214.176.129, Dst: 202.38.64.56  
 > User Datagram Protocol, Src Port: 61521, Dst Port: 53  
 > Domain Name System (query)

13. DNS 查询报文的 Type 类型是 A，没有任何 answers，因为其标志了响应报文在第 45 个分组中

ip.addr == 114.214.176.129						
No.	Time	Source	Destination	Protocol	Length	Info
33	16.504...	114.214.176.129	120.92.107.7	TCP	55	50072 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1
34	16.526...	120.92.107.7	114.214.176.129	TCP	66	443 → 50072 [ACK] Seq=1 Ack=2 Win=66 Len=0
35	16.616...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=4/1024,
37	17.713...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=5/1280,
38	18.635...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=6/1536,
40	19.656...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=7/1792,
41	20.683...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=8/2048,
42	20.780...	114.214.176.129	202.38.64.56	DNS	85	Standard query 0x0001 PTR 56.64.38.202.in-a
43	20.790...	202.38.64.56	114.214.176.129	DNS	138	Standard query response 0x0001 PTR 56.64.38
44	20.795...	114.214.176.129	202.38.64.56	DNS	71	Standard query 0x0002 A www.mit.edu
45	21.092...	202.38.64.56	114.214.176.129	DNS	163	Standard query response 0x0002 A www.mit.ed

> Domain Name System (query)  
 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  
 Name: www.mit.edu  
 [Name Length: 11]  
 [Label Count: 3]  
 Type: A (Host Address) (1)  
 Class: IN (0x0001)  
 [Response In: 45]

14. DNS 响应报文中存在 3 个 answers。第一个 answer 的 Type 是 CNAME，包含了 [www.mit.edu](http://www.mit.edu) 的规范主机名；第二个 answer 的 Type 也是 CNAME，包含了 [www.mit.edu.edgekey.net](http://www.mit.edu.edgekey.net) 的规范主机名；第三个 answer 的 Type 是 A，包含了该规范主机名的 IP 地址

ip.addr == 114.214.176.129						
No.	Time	Source	Destination	Protocol	Length	Info
33	16.504...	114.214.176.129	120.92.107.7	TCP	55	50072 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP s
34	16.526...	120.92.107.7	114.214.176.129	TCP	66	443 → 50072 [ACK] Seq=1 Ack=2 Win=66 Len=0 SLE=1 S
35	16.616...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=4/1024, ttl=48
37	17.713...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=5/1280, ttl=48
38	18.635...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=6/1536, ttl=48
40	19.656...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=7/1792, ttl=48
41	20.683...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=8/2048, ttl=48
42	20.780...	114.214.176.129	202.38.64.56	DNS	85	Standard query 0x0001 PTR 56.64.38.202.in-addr.arp
43	20.790...	202.38.64.56	114.214.176.129	DNS	138	Standard query response 0x0001 PTR 56.64.38.202.in
44	20.795...	114.214.176.129	202.38.64.56	DNS	71	Standard query 0x0002 A www.mit.edu
45	21.092...	202.38.64.56	114.214.176.129	DNS	163	Standard query response 0x0002 A www.mit.edu CNAME

> User Datagram Protocol, Src Port: 53, Dst Port: 61521  
 > Domain Name System (response)  
 Transaction ID: 0x0002  
 > Flags: 0x8180 Standard query response, No error  
 Questions: 1  
 Answer RRs: 3  
 Authority RRs: 0  
 Additional RRs: 0  
 > Queries  
 > Answers  
 > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net  
 > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net  
 > e9566.dscb.akamaiedge.net: type A, class IN, addr 104.84.170.92  
 [Request In: 44]  
 [Time: 0.297245000 seconds]

15.

*WLAN						
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)						
ip.addr == 114.214.176.129						
No.	Time	Source	Destination	Protocol	Length	Info
33	16.504...	114.214.176.129	120.92.107.7	TCP	55	50072 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
34	16.526...	120.92.107.7	114.214.176.129	TCP	66	443 → 50072 [ACK] Seq=1 Ack=2 Win=66 Len=0 SLE=1 SRE=2
35	16.616...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=4/1024, ttl=48 (no response found!)
37	17.713...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=5/1280, ttl=48 (no response found!)
38	18.635...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=6/1536, ttl=48 (no response found!)
40	19.656...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=7/1792, ttl=48 (no response found!)
41	20.683...	121.89.58.3	114.214.176.129	ICMP	98	Echo (ping) request id=0x0004, seq=8/2048, ttl=48 (no response found!)
42	20.780...	114.214.176.129	202.38.64.56	DNS	85	Standard query 0x0001 PTR 56.64.38.202.in-addr.arpa
43	20.790...	202.38.64.56	114.214.176.129	DNS	138	Standard query response 0x0001 PTR 56.64.38.202.in-addr.arpa PTR mx.ustc.edu.cn
44	20.795...	114.214.176.129	202.38.64.56	DNS	71	Standard query 0x0002 A www.mit.edu
45	21.092...	202.38.64.56	114.214.176.129	DNS	163	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME
> User Datagram Protocol, Src Port: 53, Dst Port: 61521						
Domain Name System (response)						
Transaction ID: 0x0002						
> Flags: 0x8180 Standard query response, No error						
Questions: 1						
Answer RRs: 3						
Authority RRs: 0						
Additional RRs: 0						
> Queries						
Answers						
> www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net						
> www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net						
> e9566.dscb.akamaiedge.net: type A, class IN, addr 104.84.170.92						
[Request In: 44]						
[Time: 0.297245000 seconds]						
0020	b0 81 00 35 f0 51 00 81	c8 e1 00 02 81 80	00 01	...	5	Q...
0030	00 03 00 00 00 00 03 77	77 77 03 6d 69 74 03 65		...	...	...
0040	64 75 00 00 01 00 01 c0	0c 00 05 00 01 00 00 02		...	...	...
0050	58 00 19 03 77 77 77 03	6d 69 74 03 65 64 75 07		X...	www.	mit.edu
0060	65 64 67 65 6b 65 79 03	6e 65 74 00 c0 29 00 05		...	edgekey.	net...
0070	00 01 00 00 00 03 c0 01 b	05 65 39 35 36 36 04 64		...	e9566.d	
0080	73 63 62 0a 61 6b 61 6d	61 69 65 64 67 65 03 6e		...	scb.akam	aiedge.n
0090	65 74 00 c0 4e 00 01 00	01 00 00 00 14 00 04 68		et...	N...	...
00a0	54 aa 5c			T...		

nslookup -type=NS mit.edu

16. DNS 查询报文的目标 IP 地址是 202.38.64.56，是我本地默认的 DNS 服务器的 IP 地址

ip.addr == 114.214.232.98						
No.	Time	Source	Destination	Protocol	Length	Info
19	1.061441	114.214.232.98	117.18.237.29	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 58227 → 80 [SYN]
22	3.064322	114.214.232.98	117.18.237.29	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 58227 → 80 [SYN]
23	4.055776	114.214.232.98	202.38.64.56	DNS	85	Standard query 0x0001 PTR 56.64.38.202.in-addr.arpa
24	4.061148	202.38.64.56	114.214.232.98	DNS	138	Standard query response 0x0001 PTR 56.64.38.202.in-addr.arpa PT
25	4.064663	114.214.232.98	202.38.64.56	DNS	79	Standard query 0x0002 NS mit.edu.ustc.edu.cn
26	4.068395	202.38.64.56	114.214.232.98	DNS	135	Standard query response 0x0002 No such name NS mit.edu.ustc.edu
27	4.068952	114.214.232.98	202.38.64.56	DNS	74	Standard query 0x0003 NS mit.edu.edu.cn
28	4.071861	202.38.64.56	114.214.232.98	DNS	141	Standard query response 0x0003 No such name NS mit.edu.edu.cn S
29	4.072305	114.214.232.98	202.38.64.56	DNS	67	Standard query 0x0004 NS mit.edu
30	4.076588	202.38.64.56	114.214.232.98	DNS	234	Standard query response 0x0004 NS mit.edu NS use5.akam.net NS n
31	5.246737	114.214.232.98	106.15.45.19	TCP	54	58155 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
32	5.262155	106.15.45.19	114.214.232.98	TCP	60	443 → 58155 [FIN, ACK] Seq=1 Ack=2 Win=245 Len=0
33	5.262322	114.214.232.98	106.15.45.19	TCP	54	58155 → 443 [ACK] Seq=2 Ack=2 Win=513 Len=0
> Frame 23: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{78348DFD-6104-46FE-923D-EF83B9D90DB2},						
> Ethernet II, Src: LiteonTe_17:ac:d8 (80:30:49:17:ac:d8), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)						
> Internet Protocol Version 4, Src: 114.214.232.98, Dst: 202.38.64.56						
> User Datagram Protocol, Src Port: 60313, Dst Port: 53						
> Domain Name System (query)						

17. DNS 查询报文的 Type 类型是 NS，没有任何 answers，因为其标志了响应报文在第 30 个分组中

ip.addr == 114.214.232.98						
No.	Time	Source	Destination	Protocol	Length	Info
19	1.061441	114.214.232.98	117.18.237.29	TCP	66	[TCP Retransmission] [TCP Port number
22	3.064322	114.214.232.98	117.18.237.29	TCP	66	[TCP Retransmission] [TCP Port number
23	4.055776	114.214.232.98	202.38.64.56	DNS	85	Standard query 0x0001 PTR 56.64.38.202
24	4.061148	202.38.64.56	114.214.232.98	DNS	138	Standard query response 0x0001 PTR 56.64.38.202
25	4.064663	114.214.232.98	202.38.64.56	DNS	79	Standard query 0x0002 NS mit.edu.ustc
26	4.068395	202.38.64.56	114.214.232.98	DNS	135	Standard query response 0x0002 No such
27	4.068952	114.214.232.98	202.38.64.56	DNS	74	Standard query 0x0003 NS mit.edu.edu.
28	4.071861	202.38.64.56	114.214.232.98	DNS	141	Standard query response 0x0003 No such
29	4.072305	114.214.232.98	202.38.64.56	DNS	67	Standard query 0x0004 NS mit.edu
30	4.076588	202.38.64.56	114.214.232.98	DNS	234	Standard query response 0x0004 NS mit.edu
31	5.246737	114.214.232.98	106.15.45.19	TCP	54	58155 → 443 [FIN, ACK] Seq=1 Ack=1 Wi
32	5.262155	106.15.45.19	114.214.232.98	TCP	60	443 → 58155 [FIN, ACK] Seq=1 Ack=2 Wi
33	5.262322	114.214.232.98	106.15.45.19	TCP	54	58155 → 443 [ACK] Seq=2 Ack=2 Win=513

Transaction ID: 0x0004

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

- mit.edu: type NS, class IN
  - Name: mit.edu
  - [Name Length: 7]
  - [Label Count: 2]
  - Type: NS (authoritative Name Server) (2)
  - Class: IN (0x0001)

[Response In: 30]

18. 响应报文一共提供了 8 个域名服务器，**没有在响应报文中提供 IP 地址**

ip.addr == 114.214.232.98						
No.	Time	Source	Destination	Protocol	Length	Info
19	1.061441	114.214.232.98	117.18.237.29	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5822
22	3.064322	114.214.232.98	117.18.237.29	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5822
23	4.055776	114.214.232.98	202.38.64.56	DNS	85	Standard query 0x0001 PTR 56.64.38.202.in-addr.arpa
24	4.061148	202.38.64.56	114.214.232.98	DNS	138	Standard query response 0x0001 PTR 56.64.38.202.in-addr.arpa
25	4.064663	114.214.232.98	202.38.64.56	DNS	79	Standard query 0x0002 NS mit.edu.ustc.edu.cn
26	4.068395	202.38.64.56	114.214.232.98	DNS	135	Standard query response 0x0002 No such name NS mit.edu.edu.cn
27	4.068952	114.214.232.98	202.38.64.56	DNS	74	Standard query 0x0003 NS mit.edu.edu.cn
28	4.071861	202.38.64.56	114.214.232.98	DNS	141	Standard query response 0x0003 No such name NS mit.edu.edu.cn
29	4.072305	114.214.232.98	202.38.64.56	DNS	67	Standard query 0x0004 NS mit.edu
30	4.076588	202.38.64.56	114.214.232.98	DNS	234	Standard query response 0x0004 NS mit.edu NS use5.akam.net NS ns1-173.akam.net NS eur5.akam.net NS usw2.akam.net NS asia1.akam.net NS asia2.akam.net
31	5.246737	114.214.232.98	106.15.45.19	TCP	54	58155 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
32	5.262155	106.15.45.19	114.214.232.98	TCP	60	443 → 58155 [FIN, ACK] Seq=1 Ack=2 Win=245 Len=0
33	5.262322	114.214.232.98	106.15.45.19	TCP	54	58155 → 443 [ACK] Seq=2 Ack=2 Win=513 Len=0

[Label Count: 2]

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Answers

- mit.edu: type NS, class IN, ns use5.akam.net
- mit.edu: type NS, class IN, ns ns1-173.akam.net
- mit.edu: type NS, class IN, ns eur5.akam.net
- mit.edu: type NS, class IN, ns usw2.akam.net
- 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 ns1-37.akam.net
- mit.edu: type NS, class IN, ns use2.akam.net

[Request In: 29]

[Time: 0.004283000 seconds]

19.

ip.addr == 114.214.232.98						
No.	Time	Source	Destination	Protocol	Length	Info
27	4.068952	114.214.232.98	202.38.64.56	DNS	74	Standard query 0x0003 NS mit.edu.edu.cn
28	4.071861	202.38.64.56	114.214.232.98	DNS	141	Standard query response 0x0003 No such name NS mit.edu.edu.cn SOA dns.edu.cn
29	4.072305	114.214.232.98	202.38.64.56	DNS	67	Standard query 0x0004 NS mit.edu
30	4.076588	202.38.64.56	114.214.232.98	DNS	234	Standard query response 0x0004 NS mit.edu NS use5.akam.net NS ns1-173.akam.net NS eur5.akam.net NS usw2.akam.net NS asia1.akam.net NS asia2.akam.net
31	5.246737	114.214.232.98	106.15.45.19	TCP	54	58155 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
32	5.262155	106.15.45.19	114.214.232.98	TCP	60	443 → 58155 [FIN, ACK] Seq=1 Ack=2 Win=245 Len=0
33	5.262322	114.214.232.98	106.15.45.19	TCP	54	58155 → 443 [ACK] Seq=2 Ack=2 Win=513 Len=0

Flags: 0x0100 Standard query response, No error

Questions: 1

Answer RRs: 8

Authority RRs: 0

Additional RRs: 0

Queries

- mit.edu: type NS, class IN
  - Name: mit.edu
  - [Name Length: 7]
  - [Label Count: 2]
  - Type: NS (authoritative Name Server) (2)
  - Class: IN (0x0001)

Answers

- mit.edu: type NS, class IN, ns use5.akam.net
  - Name: mit.edu
  - Type: NS (authoritative Name Server) (2)
  - Class: IN (0x0001)
  - Time to live: 43 (43 seconds)
  - Data length: 15
  - Name Server: use5.akam.net

0030 00 00 00 00 00 03 6d 69 74 03 65 64 75 00 00 .....m it.edu  
0040 00 01 c0 00 02 00 01 00 00 00 2b 00 0f 04 .....use5.aka m:net  
0050 75 73 65 35 04 61 6b 61 6d 03 6e 65 74 00 c0 0c .....ns1-1  
0060 00 02 00 01 00 00 2b 00 0a 07 6e 73 31 2d 31 .....73-  
0070 37 33 c0 2a c0 0c 00 02 00 01 00 00 00 2b 00 07 .....eur5-  
0080 04 65 75 72 35 c0 2a c0 0c 00 02 00 01 00 00 00 .....+usw2-  
0090 2b 00 07 04 75 73 77 32 c0 2a c0 0c 00 02 00 01 .....+asia1-  
00a0 00 00 0b 00 08 05 61 73 69 61 31 c0 2a c0 0c .....+asia2  
00b0 00 02 00 01 00 00 0b 00 00 05 61 73 69 61 32

Number of additional records in packet (dns.count.add\_rr): 2 byte(s)

分组: 575 · 已显示: 514 (89.4%) · 已过滤: 0 (0.0%) 配置: Default



nslookup [www.aiit.or.kr](http://www.aiit.or.kr) mx.ustc.edu.cn

20. DNS 查询报文的目标 IP 地址是 **2001:da8:d800::56**，这个 IP 地址不是我本地默认 DNS 的地址，这个 IP 地址是与 ustc 服务器相关的 IP 地址

dns						
No.	Time	Source	Destination	Protocol	Length	Info
292	25.616...	114.214.232.98	202.38.64.56	DNS	74	Standard query 0x2961 A mx.ustc.edu.cn
293	25.616...	114.214.232.98	202.38.64.56	DNS	74	Standard query 0xe6c0 AAAA mx.ustc.edu.cn
297	25.622...	202.38.64.56	114.214.232.98	DNS	90	Standard query response 0x2961 A mx.ustc.edu.cn
298	25.622...	202.38.64.56	114.214.232.98	DNS	102	Standard query response 0xe6c0 AAAA mx.ustc.edu.cn
299	25.626...	2001:da8:d800:189:a...	2001:da8:d800::56	DNS	152	Standard query 0x0001 PTR 6.5.0.0.0.0.0.0
300	25.629...	2001:da8:d800::56	2001:da8:d800:189:a...	DNS	242	Standard query response 0x0001 No such name
301	25.632...	2001:da8:d800:189:a...	2001:da8:d800::56	DNS	94	Standard query 0x0002 A www.aiit.or.kr
302	25.639...	2001:da8:d800::56	2001:da8:d800:189:a...	DNS	110	Standard query response 0x0002 A www.aiit.or.kr
303	25.646...	2001:da8:d800:189:a...	2001:da8:d800::56	DNS	94	Standard query 0x0003 AAAA www.aiit.or.kr
304	25.651...	2001:da8:d800::56	2001:da8:d800:189:a...	DNS	148	Standard query response 0x0003 AAAA www.aiit.or.kr

> Frame 301: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF\_{78348DFD-6104-4}

> Ethernet II, Src: LiteonTe\_17:ac:d8 (80:30:49:17:ac:d8), Dst: Hangzhou\_91:72:e2 (5c:dd:70:91:72:e2)

> Internet Protocol Version 6, Src: 2001:da8:d800:189:a4a0:8fc0:c612:1c0a, Dst: 2001:da8:d800::56

> 0110 .... = Version: 6

> .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)

> .... 1100 0001 1011 0100 1100 = Flow Label: 0xc1b4c

> Payload Length: 40

> Next Header: UDP (17)

> Hop Limit: 64

> Source Address: 2001:da8:d800:189:a4a0:8fc0:c612:1c0a

> Destination Address: 2001:da8:d800::56

> User Datagram Protocol, Src Port: 60638, Dst Port: 53

> Domain Name System (query)

21. DNS 查询报文的类型 Type 是 A，没有任何 answers，因为其标志了响应报文在第 302 个分组中

dns						
No.	Time	Source	Destination	Protocol	Length	Info
292	25.616...	114.214.232.98	202.38.64.56	DNS	74	Standard query 0x2961 A mx.ustc.edu.cn
293	25.616...	114.214.232.98	202.38.64.56	DNS	74	Standard query 0xe6c0 AAAA mx.ustc.edu.cn
297	25.622...	202.38.64.56	114.214.232.98	DNS	90	Standard query response 0x2961 A mx.ustc.edu.cn
298	25.622...	202.38.64.56	114.214.232.98	DNS	102	Standard query response 0xe6c0 AAAA mx.ustc.edu.cn
299	25.626...	2001:da8:d800:189:a...	2001:da8:d800::56	DNS	152	Standard query 0x0001 PTR 6.5.0.0.0.0.0.0
300	25.629...	2001:da8:d800::56	2001:da8:d800:189:a...	DNS	242	Standard query response 0x0001 No such name
301	25.632...	2001:da8:d800:189:a...	2001:da8:d800::56	DNS	94	Standard query 0x0002 A www.aiit.or.kr
302	25.639...	2001:da8:d800::56	2001:da8:d800:189:a...	DNS	110	Standard query response 0x0002 A www.aiit.or.kr
303	25.646...	2001:da8:d800:189:a...	2001:da8:d800::56	DNS	94	Standard query 0x0003 AAAA www.aiit.or.kr
304	25.651...	2001:da8:d800::56	2001:da8:d800:189:a...	DNS	148	Standard query response 0x0003 AAAA www.aiit.or.kr

Transaction ID: 0x0002

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

> www.aiit.or.kr: type A, class IN

> Name: www.aiit.or.kr

> [Name Length: 14]

> [Label Count: 4]

> Type: A (Host Address) (1)

> Class: IN (0x0001)

> [Response In: 302]

22. DNS 响应报文中只有 1 个 answers。其包含了 [www.aiit.or.kr](http://www.aiit.or.kr) 的 IP 地址

[illegible]

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

- Queries

▼ Answers

✓ www.aiit.or.kr: type A, class IN, addr 58.229.6.225

Name: `www.aiit.or.kr`

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 125 (2 minutes, 5 seconds)

Data length: 4

Address: 58.229.6.225

[Request In: 301]

```
[Time: 0.006905000 seconds]
```

[illegible]