山东大学 计算机 学院

计算机网络 课程实验报告

学号：202400130240	姓名： 贾宗翰	班级： 24.6
实验题目：Wireshark Lab:DNS v8.1		
实验学时：2h	实验日期： 2025.9.16	
实验目的： 了解 DNS		
硬件环境： 联想拯救者		
软件环境：wireshark，终端		

实验步骤与内容：

1. nslookup

```
C:\Users\jiazonghan>nslookup www.iitb.ac.in
服务器:  UnKnown
Address:  192.168.254.245

非权威应答:
名称:    www.iitb.ac.in
Address:  103.21.124.133
```

2. The DNS cache on your computer

清空缓存：

```
C:\Users\jiazonghan>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。
```

3. Tracing DNS with Wireshark

获取 ipv4：

```
以太网适配器 以太网：

   连接特定的 DNS 后缀 . . . . . :
   IPv6 地址 . . . . . . . . . . . . : 2001:250:5800:1000::825
   本地链接 IPv6 地址. . . . . . . . : fe80::7fcc:56ca:eda9:7395%12
   IPv4 地址 . . . . . . . . . . . . : 101.76.243.171
   子网掩码 . . . . . . . . . . . . : 255.255.240.0
   默认网关. . . . . . . . . . . . . : fe80::2aa2:4bff:fef6:12a0%12
                                       101.76.255.254
```

ip.addr == 101.76.243.171

No.	Time	Source	Destination	Protoco	Lengt	Info
3	0.191212	101.76.243.171	223.5.5.5	TCP	66	57928 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
4	0.191212	101.76.243.171	223.5.5.5	TCP	66	57929 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5	0.201099	223.5.5.5	101.76.243.171	TCP	66	443 → 57929 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 SACK_PERM
6	0.201145	223.5.5.5	101.76.243.171	TCP	66	443 → 57928 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 SACK_PERM
7	0.201184	101.76.243.171	223.5.5.5	TCP	54	57929 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
8	0.201234	101.76.243.171	223.5.5.5	TCP	54	57928 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
9	0.201271	101.76.243.171	223.5.5.5	TCP	54	57929 → 443 [FIN, ACK] Seq=1 Ack=1 Win=262656 Len=0
10	0.201397	101.76.243.171	223.5.5.5	TCP	54	57928 → 443 [FIN, ACK] Seq=1 Ack=1 Win=262656 Len=0
11	0.211321	223.5.5.5	101.76.243.171	TCP	60	443 → 57928 [FIN, ACK] Seq=1 Ack=2 Win=43008 Len=0
12	0.211383	101.76.243.171	223.5.5.5	TCP	54	57928 → 443 [ACK] Seq=2 Ack=2 Win=262656 Len=0
13	0.211900	223.5.5.5	101.76.243.171	TCP	60	443 → 57929 [ACK] Seq=1 Ack=2 Win=43008 Len=0
14	0.212422	223.5.5.5	101.76.243.171	TCP	60	443 → 57929 [FIN, ACK] Seq=1 Ack=2 Win=43008 Len=0
15	0.212437	101.76.243.171	223.5.5.5	TCP	54	57929 → 443 [ACK] Seq=2 Ack=2 Win=262656 Len=0
17	1.036607	101.76.243.171	120.220.73.7	TCP	55	57131 → 443 [ACK] Seq=1 Ack=1 Win=1022 Len=1
18	1.050132	120.220.73.7	101.76.243.171	TCP	66	443 → 57131 [ACK] Seq=1 Ack=2 Win=165 Len=0 SLE=1 SRE=2
20	1.566166	101.76.243.171	60.204.2.4	TCP	55	56969 → 443 [ACK] Seq=1 Ack=1 Win=1022 Len=1
21	1.601180	60.204.2.4	101.76.243.171	TCP	66	443 → 56969 [ACK] Seq=1 Ack=2 Win=2171 Len=0 SLE=1 SRE=2
22	1.677429	101.76.243.171	8.8.8.8	DNS	78	Standard query 0x69ec A cloudflare-dns.com
23	1.677429	101.76.243.171	223.6.6.6	DNS	78	Standard query 0x5b05 AAAA cloudflare-dns.com
24	1.677429	101.76.243.171	223.6.6.6	DNS	78	Standard query 0x69ec A cloudflare-dns.com
25	1.677429	101.76.243.171	8.8.8.8	DNS	78	Standard query 0x5b05 AAAA cloudflare-dns.com
28	2.577858	101.76.243.171	14.152.34.130	TLSv1.2	165	Application Data
29	2.632659	14.152.34.130	101.76.243.171	TCP	60	20067 → 57919 [ACK] Seq=1 Ack=112 Win=11 Len=0
30	2.841610	14.152.34.130	101.76.243.171	TLSv1.2	154	Application Data
31	2.893389	101.76.243.171	14.152.34.130	TCP	54	57919 → 20067 [ACK] Seq=112 Ack=101 Win=1025 Len=0

结论分析与体会：

1. 答题：IP：103.21.124.133
2. 服务器的 ip 是 192.168.254.245
3. 非权威服务器
4. 可以看到名称：dns1.iitb.ac.in。执行操作：nslookup dns1.iitb.ac.in 就可以得到对应的 ip：

```
C:\Users\jiazonghan>nslookup www.iitb.ac.in
服务器:  UnKnown
Address:  192.168.254.245

非权威应答:
名称:    www.iitb.ac.in
Address:  103.21.124.133
```

5. 按照 dns 查询，定位到第一个：

21	1.601180	60.204.2.4	101.76.243.171	TCP	66 443 → 56969 [ACK] Seq=1 Ack=2 Win=2171 Len=0 SLE=1 SRE=2
22	1.677429	101.76.243.171	8.8.8.8	DNS	78 Standard query 0x69ec A cloudflare-dns.com
23	1.677429	101.76.243.171	223.6.6.6	DNS	78 Standard query 0x5b05 AAAA cloudflare-dns.com
24	1.677429	101.76.243.171	223.6.6.6	DNS	78 Standard query 0x69ec A cloudflare-dns.com
25	1.677429	101.76.243.171	8.8.8.8	DNS	78 Standard query 0x5b05 AAAA cloudflare-dns.com
28	2.577858	101.76.243.171	14.152.34.130	TLSv1.2	165 Application Data

编号是 22

```
> Frame 22: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{8D0CDAB8-A5C2-4E9C-B7A3-93AF29DBEEF2},
> Ethernet II, Src: LCFCElectron_cb:90:63 (c4:c6:e6:cb:90:63), Dst: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)
> Internet Protocol Version 4, Src: 101.76.243.171, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 50464, Dst Port: 53
> Domain Name System (query)
```

可见是 UDP

6. 定位到对应的数据包编号：

```
Frame 1954: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{8D0CDAB8-A5C2-4E9C-B7A3-93AF29DBEEF2}
Ethernet II, Src: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0), Dst: LCFCElectron_cb:90:63 (c4:c6:e6:cb:90:63)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 101.76.243.171
User Datagram Protocol, Src Port: 53, Dst Port: 55795
```

7.

```
Frame 1926: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{8D0CDAB8-A5C2-4E9C-B7A3-93AF29DBEEF
Ethernet II, Src: LCFCElectron_cb:90:63 (c4:c6:e6:cb:90:63), Dst: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)
Internet Protocol Version 4, Src: 101.76.243.171, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 55795, Dst Port: 53
Domain Name System (query)
```

可见，目的端口是 53，source 是 55795

8. 从上文分析得知，发送的 ip 地址是 223.5.5.5

9. 观察 query：

```
v Domain Name System (response)
    Transaction ID: 0xfa9e
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
```

发现一个问题，一个答案

10. 观察 response

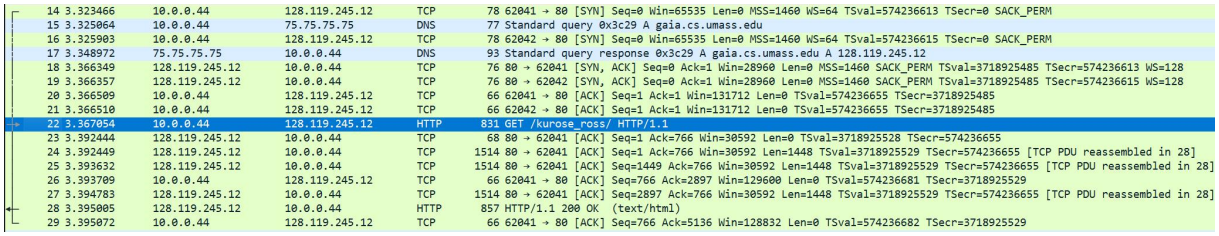
```
v Domain Name System (response)
    Transaction ID: 0x9742
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  > Queries
```

1 个答案，0 个问题

11.

No.	Time	Source	Destination	Protocol	Length	Info
22	3.367054	10.0.0.44	128.119.245.12	HTTP	831	GET /kurose_ross/ HTTP/1.1
28	3.395005	128.119.245.12	10.0.0.44	HTTP	857	HTTP/1.1 200 OK (text/html)
205	3.570142	10.0.0.44	128.119.245.12	HTTP	817	GET /kurose_ross/header_graphic_book_8E_2.jpg HTTP/1.1
516	3.670350	128.119.245.12	10.0.0.44	HTTP	454	HTTP/1.1 200 OK (JPEG JFIF image)
520	3.673776	10.0.0.44	128.119.245.12	HTTP	788	GET /favicon.ico HTTP/1.1
524	3.692288	128.119.245.12	10.0.0.44	HTTP	550	HTTP/1.1 404 Not Found (text/html)

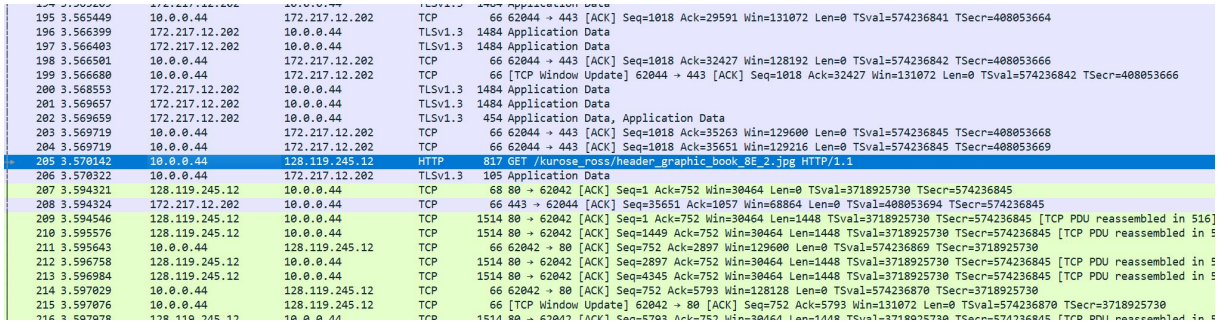
发现初始 get 编号是 22，



14	3.323466	10.0.0.44	128.119.245.12	TCP	78 62041 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=574236613 TSecr=0 SACK_PERM
15	3.325064	10.0.0.44	75.75.75.75	DNS	77 Standard query 0x3c29 A gaia.cs.umass.edu
16	3.325903	10.0.0.44	128.119.245.12	TCP	78 62042 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=574236615 TSecr=0 SACK_PERM
17	3.348972	75.75.75.75	10.0.0.44	DNS	93 Standard query response 0x3c29 A gaia.cs.umass.edu A 128.119.245.12
18	3.366349	128.119.245.12	10.0.0.44	TCP	76 80 → 62041 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=3718925485 TSecr=574236613 WS=128
19	3.366357	128.119.245.12	10.0.0.44	TCP	76 80 → 62042 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=3718925485 TSecr=574236615 WS=128
20	3.366509	10.0.0.44	128.119.245.12	TCP	66 62041 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=574236655 TSecr=3718925485
21	3.366510	10.0.0.44	128.119.245.12	TCP	66 62042 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=574236655 TSecr=3718925485
22	3.367054	10.0.0.44	128.119.245.12	HTTP	831 GET /kurose_ross/ HTTP/1.1
23	3.392444	128.119.245.12	10.0.0.44	TCP	68 80 → 62041 [ACK] Seq=1 Ack=766 Win=30592 Len=0 TSval=3718925528 TSecr=574236655
24	3.392449	128.119.245.12	10.0.0.44	TCP	1514 80 → 62041 [ACK] Seq=1 Ack=766 Win=30592 Len=1448 TSval=3718925529 TSecr=574236655 [TCP PDU reassembled in 28]
25	3.393632	128.119.245.12	10.0.0.44	TCP	1514 80 → 62041 [ACK] Seq=1449 Ack=766 Win=30592 Len=1448 TSval=3718925529 TSecr=574236655 [TCP PDU reassembled in 28]
26	3.393709	10.0.0.44	128.119.245.12	TCP	66 62041 → 80 [ACK] Seq=766 Ack=2897 Win=129600 Len=0 TSval=574236681 TSecr=3718925529
27	3.394783	128.119.245.12	10.0.0.44	TCP	1514 80 → 62041 [ACK] Seq=2897 Ack=766 Win=30592 Len=1448 TSval=3718925529 TSecr=574236655 [TCP PDU reassembled in 28]
28	3.395005	128.119.245.12	10.0.0.44	HTTP	857 HTTP/1.1 200 OK (text/html)
29	3.395072	10.0.0.44	128.119.245.12	TCP	66 62041 → 80 [ACK] Seq=766 Ack=5136 Win=128832 Len=0 TSval=574236682 TSecr=3718925529

发现初始 DNS 数据包编号是 15.收到的 DNS 编号是 17

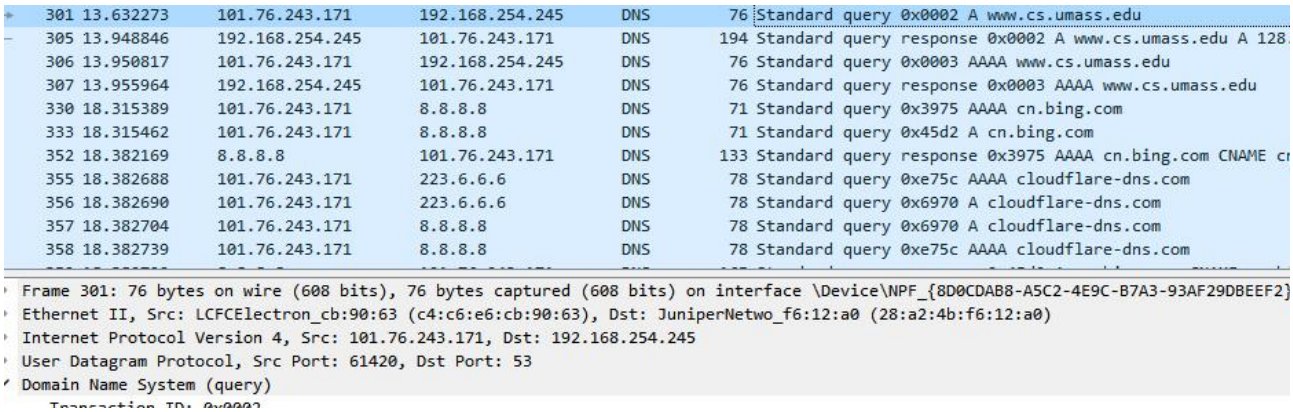
第二次 http：



195	3.565449	10.0.0.44	172.217.12.202	TCP	66 62044 → 443 [ACK] Seq=1018 Ack=29591 Win=131072 Len=0 TSval=574236841 TSecr=408053664
196	3.566399	172.217.12.202	10.0.0.44	TLSv1.3	1484 Application Data
197	3.566403	172.217.12.202	10.0.0.44	TLSv1.3	1484 Application Data
198	3.566501	10.0.0.44	172.217.12.202	TCP	66 62044 → 443 [ACK] Seq=1018 Ack=32427 Win=128192 Len=0 TSval=574236842 TSecr=408053666
199	3.566680	10.0.0.44	172.217.12.202	TCP	66 [TCP Window Update] 62044 → 443 [ACK] Seq=1018 Ack=32427 Win=131072 Len=0 TSval=574236842 TSecr=408053666
200	3.568553	172.217.12.202	10.0.0.44	TLSv1.3	1484 Application Data
201	3.569657	172.217.12.202	10.0.0.44	TLSv1.3	1484 Application Data
202	3.569659	172.217.12.202	10.0.0.44	TLSv1.3	454 Application Data, Application Data
203	3.569719	10.0.0.44	172.217.12.202	TCP	66 62044 → 443 [ACK] Seq=1018 Ack=35263 Win=129600 Len=0 TSval=574236845 TSecr=408053668
204	3.569719	10.0.0.44	172.217.12.202	TCP	66 62044 → 443 [ACK] Seq=1018 Ack=35651 Win=129216 Len=0 TSval=574236845 TSecr=408053669
205	3.570142	10.0.0.44	128.119.245.12	HTTP	817 GET /kurose_ross/header_graphic_book_8E_2.jpg HTTP/1.1
206	3.570322	10.0.0.44	172.217.12.202	TLSv1.3	105 Application Data
207	3.594321	128.119.245.12	10.0.0.44	TCP	68 80 → 62042 [ACK] Seq=1 Ack=752 Win=30464 Len=0 TSval=3718925730 TSecr=574236845
208	3.594324	172.217.12.202	10.0.0.44	TCP	66 443 → 62044 [ACK] Seq=35651 Ack=1057 Win=68864 Len=0 TSval=408053694 TSecr=574236845
209	3.594546	128.119.245.12	10.0.0.44	TCP	1514 80 → 62042 [ACK] Seq=1 Ack=752 Win=30464 Len=1448 TSval=3718925730 TSecr=574236845 [TCP PDU reassembled in 516]
210	3.595576	128.119.245.12	10.0.0.44	TCP	1514 80 → 62042 [ACK] Seq=1449 Ack=752 Win=30464 Len=1448 TSval=3718925730 TSecr=574236845 [TCP PDU reassembled in 5
211	3.595643	10.0.0.44	128.119.245.12	TCP	66 62042 → 80 [ACK] Seq=752 Ack=2897 Win=129600 Len=0 TSval=574236869 TSecr=3718925730
212	3.596758	128.119.245.12	10.0.0.44	TCP	1514 80 → 62042 [ACK] Seq=2897 Ack=752 Win=30464 Len=1448 TSval=3718925730 TSecr=574236845 [TCP PDU reassembled in 5
213	3.596984	128.119.245.12	10.0.0.44	TCP	1514 80 → 62042 [ACK] Seq=4345 Ack=752 Win=30464 Len=1448 TSval=3718925730 TSecr=574236845 [TCP PDU reassembled in 5
214	3.597029	10.0.0.44	128.119.245.12	TCP	66 62042 → 80 [ACK] Seq=752 Ack=5793 Win=128128 Len=0 TSval=574236870 TSecr=3718925730
215	3.597076	10.0.0.44	128.119.245.12	TCP	66 [TCP Window Update] 62042 → 80 [ACK] Seq=752 Ack=5793 Win=131072 Len=0 TSval=574236870 TSecr=3718925730

没有发现相应的 DNS 数据包，推测是因为 DNS 缓存，没有再次发送 DNS 查询

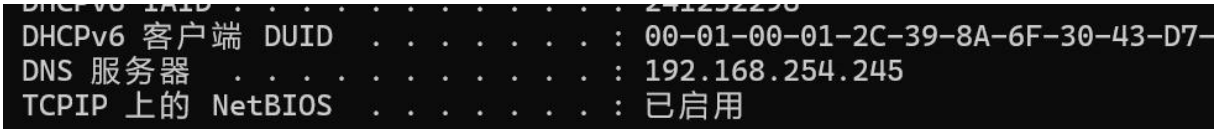
12.



301	13.632273	101.76.243.171	192.168.254.245	DNS	76 Standard query 0x0002 A www.cs.umass.edu
305	13.948846	192.168.254.245	101.76.243.171	DNS	194 Standard query response 0x0002 A www.cs.umass.edu A 128
306	13.950817	101.76.243.171	192.168.254.245	DNS	76 Standard query 0x0003 AAAA www.cs.umass.edu
307	13.955964	192.168.254.245	101.76.243.171	DNS	76 Standard query response 0x0003 AAAA www.cs.umass.edu
330	18.315389	101.76.243.171	8.8.8.8	DNS	71 Standard query 0x3975 AAAA cn.bing.com
333	18.315462	101.76.243.171	8.8.8.8	DNS	71 Standard query 0x45d2 A cn.bing.com
352	18.382169	8.8.8.8	101.76.243.171	DNS	133 Standard query response 0x3975 AAAA cn.bing.com CNAME cr
355	18.382688	101.76.243.171	223.6.6.6	DNS	78 Standard query 0xe75c AAAA cloudflare-dns.com
356	18.382690	101.76.243.171	223.6.6.6	DNS	78 Standard query 0x6970 A cloudflare-dns.com
357	18.382704	101.76.243.171	8.8.8.8	DNS	78 Standard query 0x6970 A cloudflare-dns.com
358	18.382739	101.76.243.171	8.8.8.8	DNS	78 Standard query 0xe75c AAAA cloudflare-dns.com

```
Frame 301: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{8D0CDAB8-A5C2-4E9C-B7A3-93AF29DBEEF2}
Ethernet II, Src: LCFCElectron_cb:90:63 (c4:c6:e6:cb:90:63), Dst: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)
Internet Protocol Version 4, Src: 101.76.243.171, Dst: 192.168.254.245
User Datagram Protocol, Src Port: 61420, Dst Port: 53
Domain Name System (query)
```

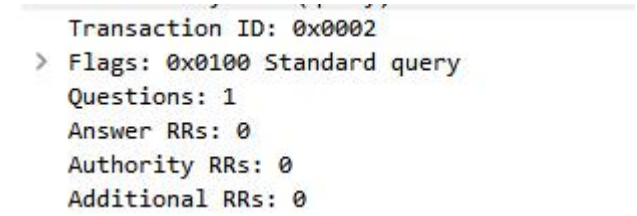
分析可得目的端口 53，源端口 61420

13. 

```
DHCPv6 客户端 DUID  . . . . . : 00-01-00-01-2C-39-8A-6F-30-43-D7-
DNS 服务器  . . . . . : 192.168.254.245
TCPIP 上的 NetBIOS  . . . . . : 已启用
```

发送地址：192.168.254.245

14.类型 typeA,查询消息没有包含答案



```
Transaction ID: 0x0002
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
```

15.1 个问题，1 个答案

```
Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
```

16.

192.168.254.245	101.76.243.171	DNS	123	Standard query response 0x0001 No such name PTR 245.2
101.76.243.171	192.168.254.245	DNS	76	Standard query 0x0002 A www.cs.umass.edu
192.168.254.245	101.76.243.171	DNS	194	Standard query response 0x0002 A www.cs.umass.edu A 1
101.76.243.171	192.168.254.245	DNS	76	Standard query 0x0003 AAAA www.cs.umass.edu
192.168.254.245	101.76.243.171	DNS	76	Standard query response 0x0003 AAAA www.cs.umass.edu

发现和前面的地址是一样的，也就是本地的默认地址。

17. 一个问题，没有答案：

```
Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

18. 一个问题，三个答案

```
Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 3
```