

# 计算机网络 Lab2

---

## 一、实验目的

---

1. 掌握 Telnet、Netcat、Dig 等网络工具的基本使用方法；
2. 通过逐步模拟 HTTP、SMTP 等常见应用层协议的通信过程，理解应用层协议的工作原理；
3. 观察和分析 DNS 解析过程，体会 DNS 服务在网络连接中的重要性；
4. 培养网络故障排除和调试能力，学会使用工具来诊断和解决网络通信中可能出现的问题。

## 二、实验任务

---

### 1.使用 Telnet 发送 HTTP 请求

**提交内容1：**进行以上操作和获取到的应答的命令行截图，并与直接使用浏览器访问该网页的内容进行对比。

获得的命令行应答中有服务器直接提供的原始 HTTP 响应。包括详细的 HTTP 协议头部信息，如状态码、服务器信息、内容类型（Content-Type）、内容长度（Content-Length）等。除此之外还有未渲染的 HTML 代码，包括，，

等 HTML 标签以及页面中引用的 CSS 和 JavaScript 代码。

而直接使用浏览器访问该网页得到的内容是处理后的可视化界面，包含渲染后的HTML。只能看到最终的呈现内容，所有的网络请求和处理都被隐藏在后台。

```
[09/26/24]seed@VM:~$ telnet www.example.com http
Trying 93.184.215.14...
Connected to www.example.com.
Escape character is '^]'.
GET / HTTP/1.1
Host: www.example.com
```

```
HTTP/1.1 200 OK
Age: 198592
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Fri, 27 Sep 2024 02:55:49 GMT
Etag: "3147526947+gzip+ident"
Expires: Fri, 04 Oct 2024 02:55:49 GMT
Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
Server: ECAcc (sac/2565)
Vary: Accept-Encoding
X-Cache: HIT
Content-Length: 1256
```

```
<!doctype html>
<html>
<head>
  <title>Example Domain</title>

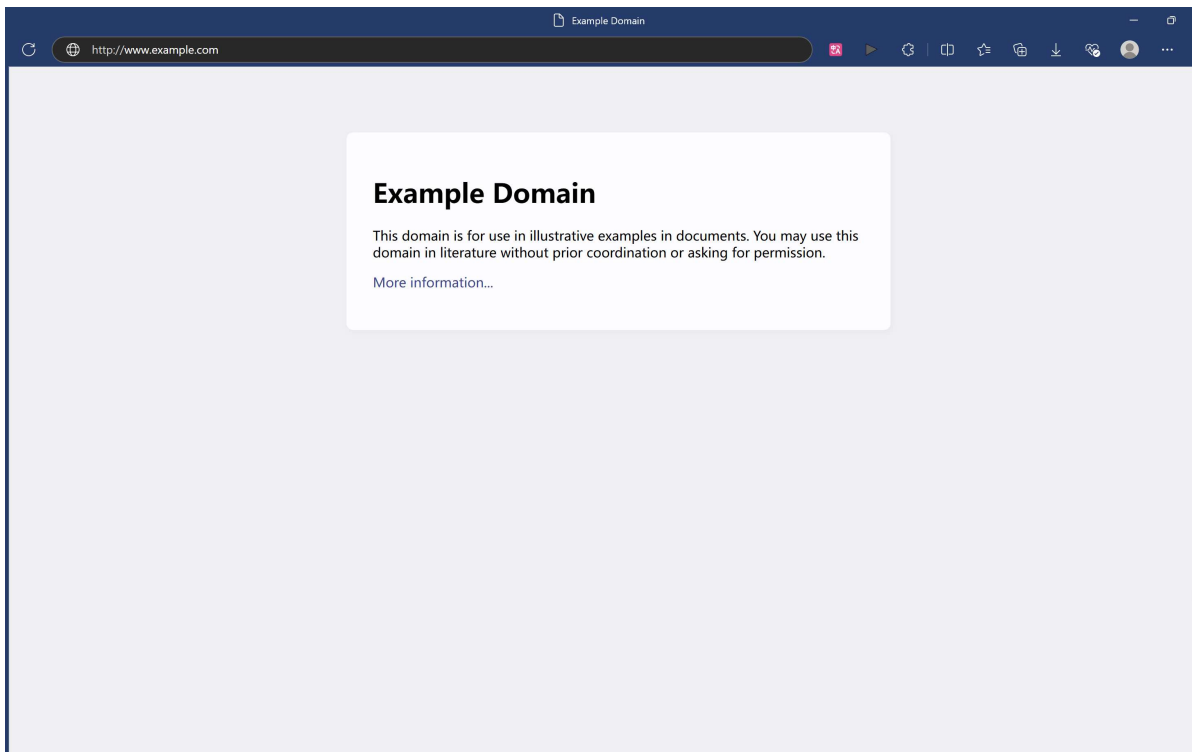
  <meta charset="utf-8" />
  <meta http-equiv="Content-type" content="text/html
; charset=utf-8" />
  <meta name="viewport" content="width=device-width,
initial-scale=1" />
  <style type="text/css">
    body {
      background-color: #f0f0f2;
      margin: 0;
      padding: 0;
      font-family: -apple-system, system-ui, BlinkMa
cSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue"
, Helvetica, Arial, sans-serif;

    }
  }

```

```
div {
  width: 600px;
  margin: 5em auto;
  padding: 2em;
  background-color: #fdfdff;
  border-radius: 0.5em;
  box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
}
a:link, a:visited {
  color: #38488f;
  text-decoration: none;
}
@media (max-width: 700px) {
  div {
    margin: 0 auto;
    width: auto;
  }
}
</style>
</head>
```

```
<body>
<div>
  <h1>Example Domain</h1>
  <p>This domain is for use in illustrative examples
in documents. You may use this
domain in literature without prior coordination or
asking for permission.</p>
  <p><a href="https://www.iana.org/domains/example">
More information...</a></p>
</div>
</body>
</html>
Connection closed by foreign host.
[09/26/24] seed@VM:~$
```



## 2.使用 Telnet 登陆 SMTP 服务器发送邮件

**提交内容2：**使用 telnet 发送邮件的过程截图，以及网页客户端中对方收到的邮件的截图。

```
[09/26/24] seed@VM:~$ telnet smtp.163.com 25
Trying 1.95.20.21...
Connected to smtp163.mail.ntes53.netease.com.
Escape character is '^]'.
220 163.com Anti-spam GT for Coremail System (163com[2
0141201])
helo 163
250 OK
auth login
334 dXNlcm5hbWU6
eWZob3UyMDI0QDE2My5jb20=
334 UGFzc3dvcmQ6
VUJlVQnRHUdZOUGR4eDY0ag==
235 Authentication successful
mail from:<yfhou2024@163.com>
250 Mail OK
rcpt to:<yfhou22@m.fudan.edu.cn>
250 Mail OK
data
354 End data with <CR><LF>.<CR><LF>

354 End data with <CR><LF>.<CR><LF>
subject: Prepare for mail of hyf
from:fake_hyf@163.com
to:fake_yfh@m.fudan.edu.cn

Hello, this email from hyf is to prepare for the lab c
lass this Friday!
.
250 Mail OK queued as gzga-smtp-mta-g3-3,_____wCn75kPK
vZm8LR0Fg--.20283S2 1727408741
quit
221 Bye
Connection closed by foreign host.
[09/26/24] seed@VM:~$
```

Prepare for mail of hyf ☆

发件人: fake\_hyf <fake\_hyf@163.com>  
(由 yfhou2024@163.com 代发)  
时 间: 2024年9月27日(星期五) 中午11:45  
收件人: fake\_yfh <fake\_yfh@m.fudan.edu.cn>

翻译全文 | 图标

Hello, this email from hyf is to prepare for the lab class this Friday!

**提交内容3:** 在发送邮件的过程中, 通过 Wireshark 抓包, 截图并分析 SMTP 发送邮件的过程。

SMTP 发送邮件的过程:

1. **DNS 查询:** 解析 SMTP 服务器的 IP 地址。
2. **TCP 三次握手:** 建立与 SMTP 服务器的连接。Wireshark 抓到的 TCP 报文显示了 SYN、SYN-ACK 和 ACK 包的交换, 表明客户端成功与服务器建立 TCP 连接, 准备传输数据。服务器在连接建立后, 向客户端发送 220 响应, 表示邮件服务已经准备好。



3. **身份认证**: 客户端发送 `HELO` 命令向服务器表明自己的身份, 并请求开始 SMTP 会话。服务器返回 `250 OK`, 表示接收客户端的请求。客户端通过 `AUTH LOGIN` 命令验证发件人的身份来完成 SMTP 身份认证。服务器返回 `235 Authentication successful`, 表示身份验证成功。
4. **邮件传输**: 使用 SMTP 命令传输邮件内容, 包括发件人(`MAIL FROM` 命令)、收件人(`RCPT TO` 命令)、邮件主题 (`SUBJECT` 命令)、邮件正文(`DATA` 命令)等。服务器返回 `250 OK` 表示接受成功
5. **关闭连接**: `.` 占一行表示邮件内容结束。发送 `QUIT` 命令, 终止会话并关闭 TCP 连接。

No.	Time	Source	Destination	Protocol	Length
6	2024-09-26 23:52:39...	202.120.224.26	10.0.2.15	DNS	
7	2024-09-26 23:52:39...	10.0.2.15	1.95.20.21	TCP	
8	2024-09-26 23:52:40...	1.95.20.21	10.0.2.15	TCP	
9	2024-09-26 23:52:40...	10.0.2.15	1.95.20.21	TCP	
10	2024-09-26 23:52:40...	1.95.20.21	10.0.2.15	SMTP	
11	2024-09-26 23:52:40...	10.0.2.15	1.95.20.21	TCP	
12	2024-09-26 23:52:52...	10.0.2.15	1.95.20.21	SMTP	
13	2024-09-26 23:52:52...	1.95.20.21	10.0.2.15	TCP	
14	2024-09-26 23:52:52...	10.0.2.15	1.95.20.21	SMTP/IMF	
15	2024-09-26 23:52:52...	1.95.20.21	10.0.2.15	TCP	
16	2024-09-26 23:52:52...	1.95.20.21	10.0.2.15	SMTP	
17	2024-09-26 23:52:52...	10.0.2.15	1.95.20.21	TCP	
18	2024-09-26 23:52:52...	1.95.20.21	10.0.2.15	SMTP	
19	2024-09-26 23:52:52...	10.0.2.15	1.95.20.21	TCP	
20	2024-09-26 23:52:52...	1.95.20.21	10.0.2.15	SMTP	
21	2024-09-26 23:52:52...	10.0.2.15	1.95.20.21	TCP	
22	2024-09-26 23:52:52...	1.95.20.21	10.0.2.15	SMTP	
23	2024-09-26 23:52:52...	10.0.2.15	1.95.20.21	TCP	
24	2024-09-26 23:52:52...	1.95.20.21	10.0.2.15	SMTP	
25	2024-09-26 23:52:52...	10.0.2.15	1.95.20.21	TCP	
26	2024-09-26 23:52:52...	1.95.20.21	10.0.2.15	SMTP	
27	2024-09-26 23:52:52...	10.0.2.15	1.95.20.21	TCP	
28	2024-09-26 23:53:05...	10.0.2.15	1.95.20.21	SMTP	
29	2024-09-26 23:53:05...	1.95.20.21	10.0.2.15	TCP	
30	2024-09-26 23:53:05...	1.95.20.21	10.0.2.15	SMTP	

Protocol	Length	Info
DNS	164	Standard query response 0x06ed AAAA smtp163.mail.ntes53.netease.com SOA ns1-n...
TCP	74	56202 → 25 [SYN] Seq=1232539326 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=37...
TCP	60	25 → 56202 [SYN, ACK] Seq=213312001 Ack=1232539327 Win=65535 Len=0 MSS=1460
TCP	54	56202 → 25 [ACK] Seq=1232539327 Ack=213312002 Win=64240 Len=0
SMTP	119	S: 220 163.com Anti-spam GT for Coremail System (163com[20141201])
TCP	54	56202 → 25 [ACK] Seq=1232539327 Ack=213312067 Win=64175 Len=0
SMTP	64	C: helo 163
TCP	60	25 → 56202 [ACK] Seq=213312067 Ack=1232539337 Win=65535 Len=0
SMTP/IMF	352	from: fake_hyf@163.com, , Hello, this email from hyf is to prepare for the la...
TCP	60	25 → 56202 [ACK] Seq=213312067 Ack=1232539635 Win=65535 Len=0
SMTP	80	S: 250 OK   334 dXNlcm5hbWU6
TCP	54	56202 → 25 [ACK] Seq=1232539635 Ack=213312093 Win=64149 Len=0
SMTP	72	S: 334 UGFzc3dvcmQ6
TCP	54	56202 → 25 [ACK] Seq=1232539635 Ack=213312111 Win=64131 Len=0
SMTP	85	S: 235 Authentication successful
TCP	54	56202 → 25 [ACK] Seq=1232539635 Ack=213312142 Win=64100 Len=0
SMTP	67	S: 250 Mail OK
TCP	54	56202 → 25 [ACK] Seq=1232539635 Ack=213312155 Win=64087 Len=0
SMTP	104	S: 250 Mail OK   354 End data with <CR><LF>.<CR><LF>
TCP	54	56202 → 25 [ACK] Seq=1232539635 Ack=213312205 Win=64037 Len=0
SMTP	140	S: 250 Mail OK queued as gzga-smtp-mta-g2-1,_____wDn158HLPZmJ6H2Ag--.13215S2 ...
TCP	54	56202 → 25 [ACK] Seq=1232539635 Ack=213312291 Win=64037 Len=0
SMTP	60	C: quit
TCP	60	25 → 56202 [ACK] Seq=213312291 Ack=1232539641 Win=65535 Len=0
SMTP	63	S: 221 Bye

### 3.使用 Telnet 和 Netcat 模拟客户端/服务器模型

**提交内容4：**使用 Telnet 和 Netcat 模拟客户端和服务端进行信息传输的截图。

```
seed@VM: ~  
netcat: getnameinfo: Temporary failure in name resolution  
[09/26/24] seed@VM: ~$ netcat -v -l -p 9090  
netcat: getnameinfo: Temporary failure in name resolution  
[09/26/24] seed@VM: ~$ netcat -v -ln -p 9090  
Listening on 0.0.0.0 9090  
^C  
[09/27/24] seed@VM: ~$ sudo vim /etc/resolv.conf  
[09/27/24] seed@VM: ~$ netcat -v -l -p 9090  
Listening on 0.0.0.0 9090  
Connection received on localhost 45340  
hello,world  
world,hello  
hello,client  
hello,server  
^C  
  
seed@VM: ~  
[09/27/24] seed@VM: ~$ telnet localhost 9090  
Trying 127.0.0.1...  
Connected to localhost.  
Escape character is '^]'.  
hello,world  
world,hello  
hello,client  
hello,server  
Connection closed by foreign host.  
[09/27/24] seed@VM: ~$
```

### 4.使用 Dig 观察 DNS 请求过程

**提交内容5：**观察并分析 DNS 查询过程，判断查询采用的是递归查询还是迭代查询，并说明理由。

查询采用迭代查询。

理由：根据运行dig +trace命令返回的结果，可以看到查询是从根域名服务器（如 d.root-servers.net, f.root-servers.net 等）开始，接着查询 .com 顶级域名服务器（如 a.gtld-servers.net），最后查询 baidu.com 的权威域名服务器（如

ns3.baidu.com) 。可以看出查询过程是逐级进行的，每一级服务器返回下一步要查询的服务器信息。这符合迭代查询逐级向不同的服务器查询的特征

除此之外可以从命令行结果中可以看出客户每次根据上一层服务器提供的信息，继续向下一级服务器发出查询请求，而不是迭代查询中，客户端只需要向一个 DNS 服务器发出请求，由一个服务器完成整个查询过程的模式

```
[09/27/24] seed@VM:~$ dig +trace www.baidu.com

; <<>> DiG 9.16.1-Ubuntu <<>> +trace www.baidu.com
;; global options: +cmd
.                356052  IN      NS      d.root
-servers.net.    356052  IN      NS      e.root
.                356052  IN      NS      f.root
-servers.net.    356052  IN      NS      g.root
.                356052  IN      NS      h.root
-servers.net.    356052  IN      NS      i.root
.                356052  IN      NS      j.root
-servers.net.    356052  IN      NS      k.root
.                356052  IN      NS      l.root
-servers.net.    356052  IN      NS      m.root
.                356052  IN      NS      a.root
-servers.net.    356052  IN      NS      b.root
.                356052  IN      NS      c.root
-servers.net.
;; Received 262 bytes from 127.0.0.53#53(127.0.0.53) in 12 ms
com.            172800  IN      NS      f.gtld
-servers.net.   172800  IN      NS      k.gtld
com.            172800  IN      NS      m.gtld
-servers.net.
```



```

-servers.net.
com. 172800 IN NS a.gtld
-servers.net.
com. 172800 IN NS l.gtld
-servers.net.
com. 172800 IN NS d.gtld
-servers.net.
com. 172800 IN NS e.gtld
-servers.net.
com. 172800 IN NS g.gtld
-servers.net.
com. 172800 IN NS i.gtld
-servers.net.
com. 172800 IN NS h.gtld
-servers.net.
com. 172800 IN NS b.gtld
-servers.net.
com. 172800 IN NS j.gtld
-servers.net.
com. 172800 IN NS c.gtld
-servers.net.
com. 86400 IN DS 19718
13 2 8ACBB0CD28F41250A80A491389424D341522D946B0DA0C029
1F2D3D7 71D7805A
com. 86400 IN RRSIG DS 8 1
86400 20241009170000 20240926160000 20038 . TKmq/jXUI
psnGjxBgIe4bIrXcFkpCre17hcNzvVla43lrCrNe1CVe7ZL 1B136C
iGTIPX8LCH/rKjijfz9IC9okjm05CkopmHYLUsUp9+OHFEJmRc zp2
qq3lNgz6fwhatozJ90sA/xIzGpUfrBhiEJ01HfqnuLLm6co7Y4tr2
xybN9mYHAf5TsHxSmfTYtpQD/i/RrWX2EifoGD0rK60n9PB5wwnRIP
8I nfvu+ue1AHrtliq3BPRHPRosiFdZMASGjto5Upks5YD/xCg+KVU
dT1cw ZA8Zrt+SN/zD2edxnH3d5xYn90jQwzJIrhgVsG8CY2FrGdU7
mQ0cj03K 7WsnWw==
;; Received 1201 bytes from 192.5.5.241#53(f.root-serv
ers.net) in 16 ms

baidu.com. 172800 IN NS ns2.ba

baidu.com. 172800 IN NS ns2.ba
idu.com.
baidu.com. 172800 IN NS ns3.ba
idu.com.
baidu.com. 172800 IN NS ns4.ba
idu.com.
baidu.com. 172800 IN NS ns1.ba
idu.com.
baidu.com. 172800 IN NS ns7.ba
idu.com.
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN NSEC3 1
1 0 - CK0Q3UDG8CEKKAEE7RUKPGCT1DVSSH8LL NS SOA RRSIG D
NSKEY NSEC3PARAM
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN RRSIG N
SEC3 13 2 86400 20241003002550 20240925231550 59354 co
m. xYjdNYr7t+PA8u0z3Zx0T0LSjJN6sbdas8TxWJbNHhjK0SqWwtc
jymJ6 +c77A05p8MkslFDyqcp0d0ZeS0t3Hg==
HPVV1UNKTCF9TD77I2AUR73709T975GH.com. 86400 IN NSEC3 1
1 0 - HPVVP23QU00FP9R0A04URSICJPESK09J NS DS RRSIG

```



```
SEC3 13 2 86400 20241003002550 20240925231550 59354 co
m. xYjdNYr7t+PA8uOz3Zx0T0LSjJN6sbdas8TxWJbNHhjK0SqWwtc
jymJ6 +c77A05p8MkslFDyqcp0d0ZeS0t3Hg==
HPVV1UNKTCF9TD77I2AUR73709T975GH.com. 86400 IN NSEC3 1
1 0 - HPVVP23QU00FP9R0A04URSICJPESK09J NS DS RRSIG
HPVV1UNKTCF9TD77I2AUR73709T975GH.com. 86400 IN RRSIG N
SEC3 13 2 86400 20241002004732 20240924233732 59354 co
m. N0nBU5qYLApgZC/2oocGBdwACu5EhtN5Z2mYd+IKzoe9j2C4rsG
flG7b sP+kyaf9nTJiLbESsXJH0dUXrCSMqA==
;; Received 657 bytes from 192.54.112.30#53(h.gtld-ser
vers.net) in 232 ms

www.baidu.com. 1200 IN CNAME www.a.
shifen.com.
;; Received 100 bytes from 220.181.33.31#53(ns2.baidu.
com) in 28 ms

[09/27/24]seed@VM:~$ █
```

**提交内容6：**在 DNS 查询过程中使用 Wireshark 抓包，任选一对 DNS 请求与应答分组，解释 DNS 报文中各个字段的含义，以及标志 (flag) 字段中各个 flag 位的含义

### DNS报文各字段含义：

**Transaction ID：**每个 DNS 查询的唯一标识符，用于匹配请求和响应。客户端发送查询时生成一个随机 ID，服务器在响应时返回相同的 ID，确保客户端能够识别出这是对应的响应。

**Flags:**包含了一系列的标志位，用来指示该报文的类型以及其他相关的信息。

**Queries：**表示查询的域名和查询类型，客户端请求服务器查找的资源类型（如 A 记录、NS 记录等）

**Answers：**服务器返回的实际查询结果，包括域名的 IP 地址或名称服务器等信息。

**Additional records：**附加信息部分，包含与查询相关的其他信息。

### 标志 (flag) 字段中各个 flag 位的含义：

#### 1. QR (Query/Response) 位

0: 表示这是一个查询 (Query) 。

1: 表示这是一个响应 (Response) 。

## 2. Opcode 位: 表示查询的类型

0: 标准查询。

1: 反向查询。

2: 服务器状态请求

## 3. Authoritative 位: 在响应报文中使用, 表示该响应是否是由权威 DNS 服务器返回.

0: 表示该响应不是权威的

1: 表示该响应是权威的。

## 4. TC (Truncated) 位: 表示报文是否因为长度超过了 UDP 协议的限制而被截断。

0: 表示报文没有被截断。

1: 表示报文被截断, 需要使用 TCP 重新查询以获得完整的报文。

## 5. RD (Recursion Desired) 位: 由客户端在查询报文中设置, 表示客户端是否希望服务器执行递归查询。

0: 不请求递归查询。

1: 请求递归查询。

## 6. RA (Recursion Available) 位: 由服务器在响应报文中设置, 表示该服务器是否支持递归查询。

0: 服务器不支持递归查询。

1: 服务器支持递归查询

## 7. Z 位: 保留位, 在当前的 DNS 协议中未使用, 必须为 0。

**8. Answer authenticated 位：**如果启用了 DNSSEC 并且数据通过认证，服务器将设置此标志，以便客户端知道数据的来源已通过验证。

**9. Non-Authenticated Data 位：**用于表示响应中的数据是否经过 DNSSEC (DNS Security Extensions) 认证。

0：表示返回的数据未经过认证（即未启用 DNSSEC）。

1：表示返回的数据已通过 DNSSEC 认证。

**10. Reply Code (RCODE)：**用于指示 DNS 响应的结果状态代码，代表查询是否成功或遇到了什么问题

0：无错误 (No Error) 。

1：格式错误 (Format Error) ，服务器无法理解该请求。

2：服务器失败 (Server Failure) ，服务器无法处理该请求。

3：名称错误 (Name Error) ，表示查询的域名不存在（权威 DNS 服务器设置此位） 。

4：未实现 (Not Implemented) ，服务器不支持查询的请求类型。

5：拒绝 (Refused) ，服务器拒绝处理该请求。

Destination	Protocol	Length	Info
202.120.224.26	DNS	70	Standard query 0x81c5 NS <Root> OPT
10.0.2.15	DNS	281	Standard query response 0x81c5 NS <Root> NS d.root-
202.120.224.26	DNS	89	Standard query 0x85ae A d.root-servers.net OPT
202.120.224.26	DNS	89	Standard query 0x1833 AAAA d.root-servers.net OPT
10.0.2.15	DNS	117	Standard query response 0x1833 AAAA d.root-servers.
10.0.2.15	DNS	105	Standard query response 0x85ae A d.root-servers.net
202.120.224.26	DNS	89	Standard query 0xf04d A e.root-servers.net OPT
202.120.224.26	DNS	89	Standard query 0xe7f4 AAAA e.root-servers.net OPT
10.0.2.15	DNS	105	Standard query response 0xf04d A e.root-servers.net
10.0.2.15	DNS	117	Standard query response 0xe7f4 AAAA e.root-servers.
202.120.224.26	DNS	89	Standard query 0x1ac2 A f.root-servers.net OPT
202.120.224.26	DNS	89	Standard query 0x873e AAAA f.root-servers.net OPT
10.0.2.15	DNS	105	Standard query response 0x1ac2 A f.root-servers.net
10.0.2.15	DNS	117	Standard query response 0x873e AAAA f.root-servers.
202.120.224.26	DNS	89	Standard query 0x4f97 A g.root-servers.net OPT
202.120.224.26	DNS	89	Standard query 0x3ca2 AAAA g.root-servers.net OPT
10.0.2.15	DNS	105	Standard query response 0x4f97 A g.root-servers.net
10.0.2.15	DNS	117	Standard query response 0x3ca2 AAAA g.root-servers.
202.120.224.26	DNS	89	Standard query 0xf531 A h.root-servers.net OPT
202.120.224.26	DNS	89	Standard query 0x752b AAAA h.root-servers.net OPT
10.0.2.15	DNS	117	Standard query response 0x752b AAAA h.root-servers.
10.0.2.15	DNS	105	Standard query response 0xf531 A h.root-servers.net
202.120.224.26	DNS	89	Standard query 0x6f1d A i.root-servers.net OPT
202.120.224.26	DNS	89	Standard query 0x3889 AAAA i.root-servers.net OPT
10.0.2.15	DNS	117	Standard query response 0x3889 AAAA i.root-servers.

Destination	Protocol	Length	Info
202.120.224.26	DNS	70	Standard query 0x81c5 NS <Root> OPT
10.0.2.15	DNS	281	Standard query response 0x81c5 NS <Root> NS d.ro
<p>Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface enp0s3, id 0</p> <p>Ethernet II, Src: PcsCompu_b5:20:59 (08:00:27:b5:20:59), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)</p> <p>Internet Protocol Version 4, Src: 10.0.2.15, Dst: 202.120.224.26</p> <p>User Datagram Protocol, Src Port: 50979, Dst Port: 53</p> <p><b>Domain Name System (query)</b></p> <p>Transaction ID: 0x81c5</p> <p>Flags: 0x0100 Standard query</p> <p>0... .. = Response: Message is a query</p> <p>.000 0... .. = Opcode: Standard query (0)</p> <p>... ..0... .. = Truncated: Message is not truncated</p> <p>... ..1... .. = Recursion desired: Do query recursively</p> <p>... ..0... .. = Z: reserved (0)</p> <p>... ..0... .. = Non-authenticated data: Unacceptable</p> <p>Questions: 1</p> <p>Answer RRs: 0</p> <p>Authority RRs: 0</p> <p>Additional RRs: 1</p> <p>Queries</p> <p>&gt; &lt;Root&gt;: type NS, class IN</p> <p>Additional records</p> <p>&gt; &lt;Root&gt;: type OPT</p> <p><a href="#">[Response In: 2]</a></p>			

Destination	Protocol	Length	Info
202.120.224.26	DNS	70	Standard query 0x81c5 NS <Root> OPT
10.0.2.15	DNS	281	Standard query response 0x81c5 NS <Root> NS d.ro
<p><b>Domain Name System (response)</b></p> <p>Transaction ID: 0x81c5</p> <p>Flags: 0x8180 Standard query response, No error</p> <p>1... .. = Response: Message is a response</p> <p>.000 0... .. = Opcode: Standard query (0)</p> <p>... ..0... .. = Authoritative: Server is not an authority for domain</p> <p>... ..0... .. = Truncated: Message is not truncated</p> <p>... ..1... .. = Recursion desired: Do query recursively</p> <p>... ..1... .. = Recursion available: Server can do recursive queries</p> <p>... ..0... .. = Z: reserved (0)</p> <p>... ..0... .. = Answer authenticated: Answer/authority portion was not authenticated</p> <p>... ..0... .. = Non-authenticated data: Unacceptable</p> <p>... ..0000... .. = Reply code: No error (0)</p> <p>Questions: 1</p> <p>Answer RRs: 13</p> <p>Authority RRs: 0</p> <p>Additional RRs: 1</p> <p>Queries</p> <p>&gt; &lt;Root&gt;: type NS, class IN</p> <p>Answers</p> <p>&gt; &lt;Root&gt;: type NS, class IN, ns d.root-servers.net</p> <p>&gt; &lt;Root&gt;: type NS, class IN, ns e.root-servers.net</p> <p>&gt; &lt;Root&gt;: type NS, class IN, ns f.root-servers.net</p> <p>&gt; &lt;Root&gt;: type NS, class IN, ns g.root-servers.net</p> <p>&gt; &lt;Root&gt;: type NS, class IN, ns h.root-servers.net</p> <p>&gt; &lt;Root&gt;: type NS, class IN, ns i.root-servers.net</p> <p>&gt; &lt;Root&gt;: type NS, class IN, ns j.root-servers.net</p> <p>&gt; &lt;Root&gt;: type NS, class IN, ns k.root-servers.net</p> <p>&gt; &lt;Root&gt;: type NS, class IN, ns l.root-servers.net</p> <p>&gt; &lt;Root&gt;: type NS, class IN, ns m.root-servers.net</p> <p>&gt; &lt;Root&gt;: type NS, class IN, ns a.root-servers.net</p> <p>&gt; &lt;Root&gt;: type NS, class IN, ns b.root-servers.net</p> <p>&gt; &lt;Root&gt;: type NS, class IN, ns c.root-servers.net</p> <p>Additional records</p> <p>&gt; &lt;Root&gt;: type OPT</p> <p><a href="#">[Request In: 1]</a></p> <p>[Time: 0.012273680 seconds]</p>			