实验三

Wireshark Lab: DNS

阅读实验文档并进行操作。

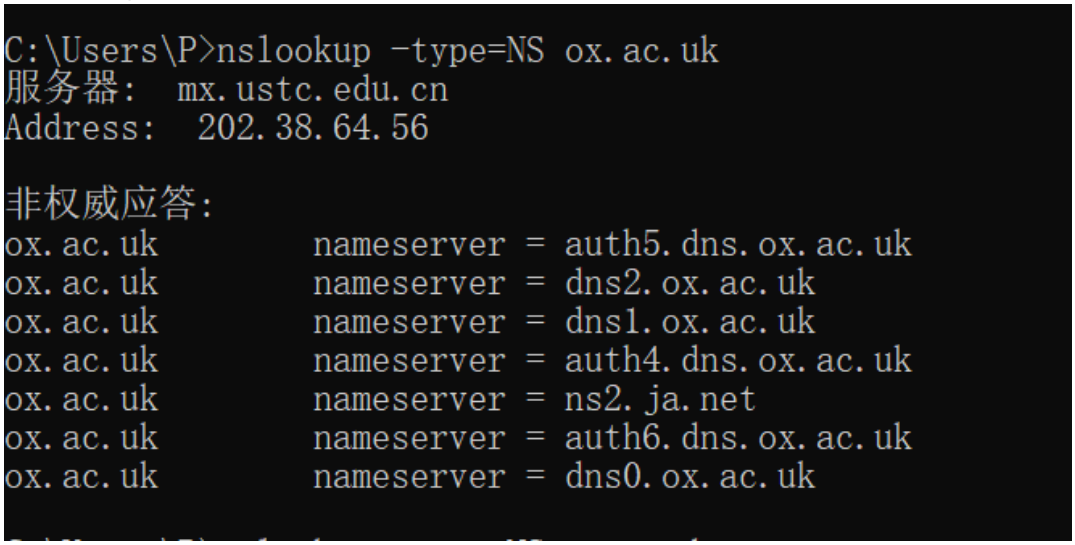
1. **nslookup**

   阅读文档，熟悉nslookup的各个操作，并以此完成1，2，3题

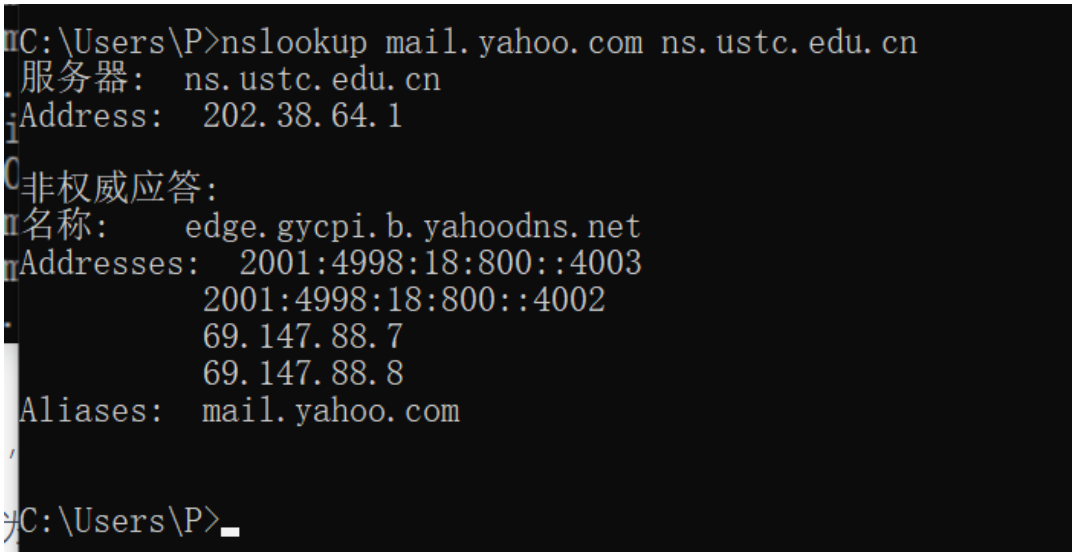
   1. 用nslookup访问科大的web，IP地址为202.38.64.246

   2. 用nslookup确定一个欧洲大学的权威服务器

   3. 利用2的一个DNS服务器查询Yahoo邮箱的邮件服务器，尝试了一下上面的DNS都不行，似乎是被墙了，但是尝试使用科大的DNS成功查询



2. **ipconfig**

   阅读实验文档，熟悉ipconfig

```
C:\Users\P>ipconfig/all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : DESKTOP-CX
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型  . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否
   DNS 后缀搜索列表  . . . . . . . . : ustc.edu.cn

以太网适配器 以太网:

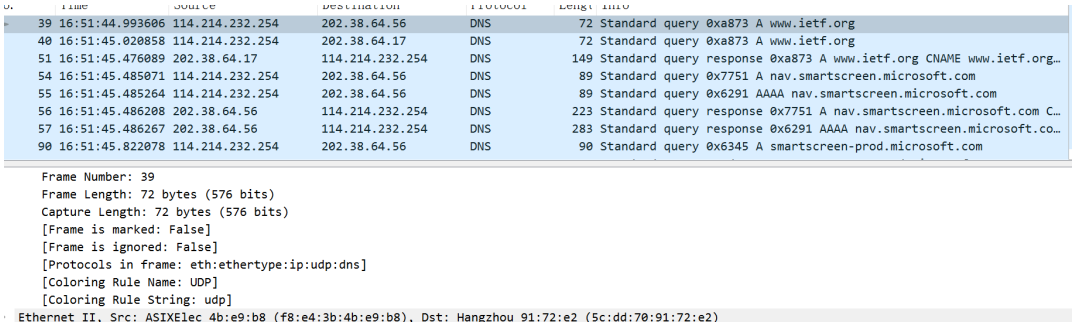
   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . : ustc.edu.cn
   描述. . . . . . . . . . . . . . . : Realtek PCIe FE Family Controller
   物理地址. . . . . . . . . . . . . : E4-54-E8-00-9B-5D
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

以太网适配器 以太网 2:

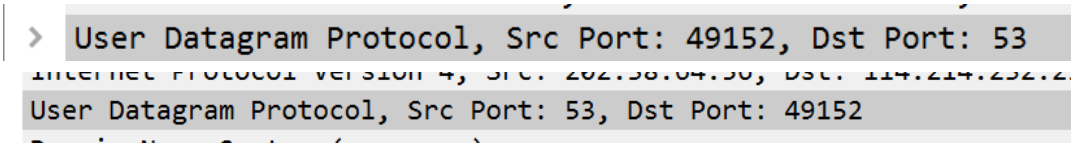
   连接特定的 DNS 后缀 . . . . . . . : ustc.edu.cn
   描述. . . . . . . . . . . . . . . : ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter
   物理地址. . . . . . . . . . . . . : F8-E4-3B-4B-E9-B8
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . . : 2001:da8:d800:523:25a6:ff11:7b52:98a1(首选)
   临时 IPv6 地址. . . . . . . . . . : 2001:da8:d800:523:60fa:a356:6e08:7361(首选)
   本地链接 IPv6 地址. . . . . . . . : fe80::25a6:ff11:7b52:98a1%3(首选)
   IPv4 地址 . . . . . . . . . . . . : 114.214.232.254(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.252.0
   获得租约的时间  . . . . . . . . . : 2021年9月24日 11:54:50
   租约过期的时间  . . . . . . . . . : 2021年9月24日 17:25:58
   默认网关. . . . . . . . . . . . . : 114.214.235.254
   DHCP 服务器 . . . . . . . . . . . : 202.38.64.17
   DHCPv6 IAID . . . . . . . . . . . : 905503803
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-28-C7-2C-42-E4-54-E8-00-9B-5D
   DNS 服务器  . . . . . . . . . . . : 202.38.64.56
                                       202.38.64.17
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

3. **Tracing DNS with Wireshark**

   按照操作清除缓存，打开Wireshark进行捕获，捕获后的结果有点多，干扰较大，回答问题。

4. 

   根据捕获内容，是使用UDP发送

5. 

   都是53端口

6. 查询消息发送到202.38.64.56

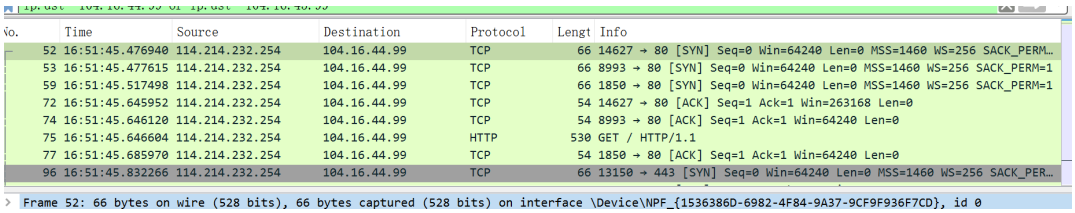
   正是本地DNS服务器地址

7. type是A，Answer RRs：0，查询消息不包含任何answer

8.

```
Queries
Answers
    www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
[Request In: 39]
```

回复3条，回复是类型，主机别名，以及两个ip地址

9. 

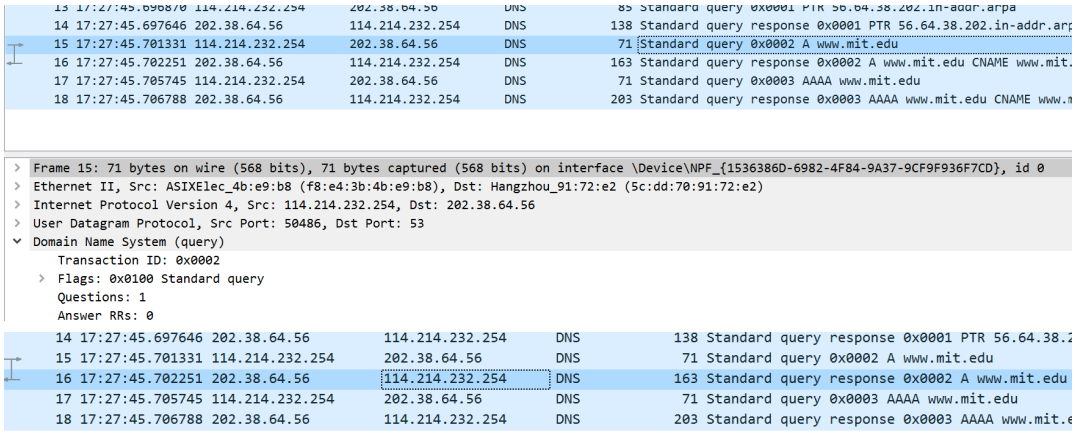
No.	Time	Source	Destination	Protocol	Length	Info
52	16:51:45.476940	114.214.232.254	104.16.44.99	TCP	66	14627 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM…
53	16:51:45.477615	114.214.232.254	104.16.44.99	TCP	66	8993 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
59	16:51:45.517498	114.214.232.254	104.16.44.99	TCP	66	1850 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
72	16:51:45.645952	114.214.232.254	104.16.44.99	TCP	54	14627 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
74	16:51:45.646120	114.214.232.254	104.16.44.99	TCP	54	8993 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
75	16:51:45.646604	114.214.232.254	104.16.44.99	HTTP	530	GET / HTTP/1.1
77	16:51:45.685970	114.214.232.254	104.16.44.99	TCP	54	1850 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
96	16:51:45.832266	114.214.232.254	104.16.44.99	TCP	66	13150 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER…

```
Frame 52: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{1536386D-6982-4F84-9A37-9CF9F936F7CD}, id 0
```

是对应的

10. 并没有，本地的DNS已经缓存了，不需要再查询了

使用nslookup，查询www.mit.edu，回答问题

11. 

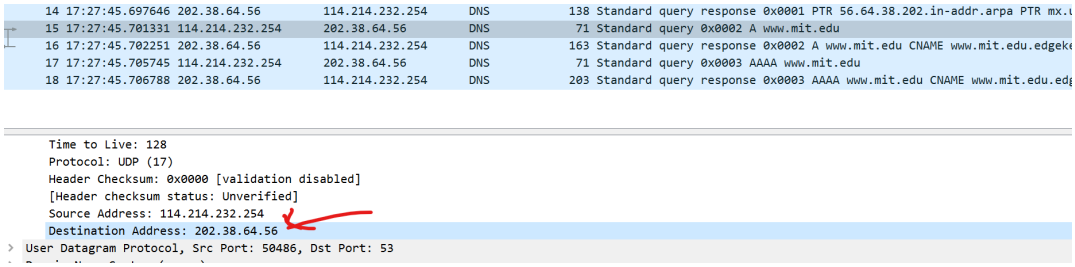
14	17:27:45.697646	202.38.64.56	114.214.232.254	DNS	138 Standard query response 0x0001 PTR 56.64.38.202.in-addr.arp
15	17:27:45.701331	114.214.232.254	202.38.64.56	DNS	71 Standard query 0x0002 A www.mit.edu
16	17:27:45.702251	202.38.64.56	114.214.232.254	DNS	163 Standard query response 0x0002 A www.mit.edu CNAME www.mit.
17	17:27:45.705745	114.214.232.254	202.38.64.56	DNS	71 Standard query 0x0003 AAAA www.mit.edu
18	17:27:45.706788	202.38.64.56	114.214.232.254	DNS	203 Standard query response 0x0003 AAAA www.mit.edu CNAME www.m

```
Frame 15: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{1536386D-6982-4F84-9A37-9CF9F936F7CD}, id 0
Ethernet II, Src: ASIXElec_4b:e9:b8 (f8:e4:3b:4b:e9:b8), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
Internet Protocol Version 4, Src: 114.214.232.254, Dst: 202.38.64.56
User Datagram Protocol, Src Port: 50486, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0x0002
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
```

14	17:27:45.697646	202.38.64.56	114.214.232.254	DNS	138 Standard query response 0x0001 PTR 56.64.38.2
15	17:27:45.701331	114.214.232.254	202.38.64.56	DNS	71 Standard query 0x0002 A www.mit.edu
16	17:27:45.702251	202.38.64.56	114.214.232.254	DNS	163 Standard query response 0x0002 A www.mit.edu
17	17:27:45.705745	114.214.232.254	202.38.64.56	DNS	71 Standard query 0x0003 AAAA www.mit.edu
18	17:27:45.706788	202.38.64.56	114.214.232.254	DNS	203 Standard query response 0x0003 AAAA www.mit.e

```
Frame 16: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface \Device\NPF_{1536386D-6982-4F84-9A37-9CF9F
Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: ASIXElec_4b:e9:b8 (f8:e4:3b:4b:e9:b8)
Internet Protocol Version 4, Src: 202.38.64.56, Dst: 114.214.232.254
User Datagram Protocol, Src Port: 53, Dst Port: 50486
Domain Name System (response)
    Transaction ID: 0x0002
    Flags: 0x8180 Standard query response, No error
    Questions: 1
```

都是53端口

12. 

14	17:27:45.697646	202.38.64.56	114.214.232.254	DNS	138 Standard query response 0x0001 PTR 56.64.38.202.in-addr.arpa PTR mx.
15	17:27:45.701331	114.214.232.254	202.38.64.56	DNS	71 Standard query 0x0002 A www.mit.edu
16	17:27:45.702251	202.38.64.56	114.214.232.254	DNS	163 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgeke
17	17:27:45.705745	114.214.232.254	202.38.64.56	DNS	71 Standard query 0x0003 AAAA www.mit.edu
18	17:27:45.706788	202.38.64.56	114.214.232.254	DNS	203 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edg

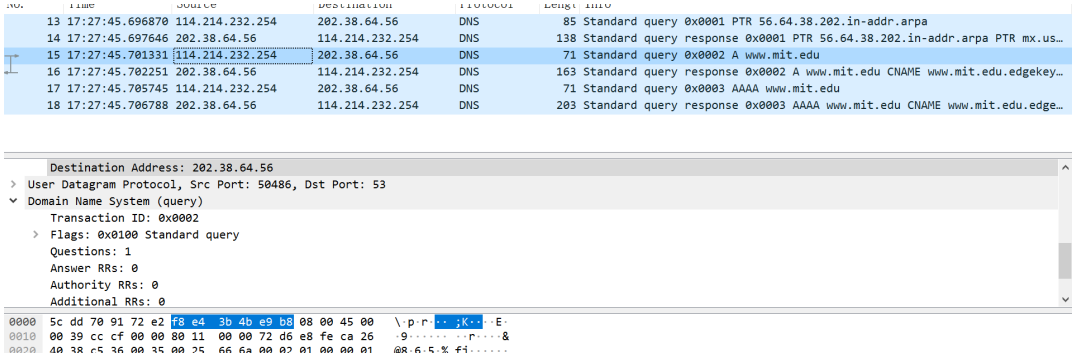
```
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.232.254
    Destination Address: 202.38.64.56
User Datagram Protocol, Src Port: 50486, Dst Port: 53
```

IP地址202.38.64.56，是本地DNS地址

13. type为A，查询信息没有任何answer
14. ```
    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 104.106.56.136
    [Request In: 15]
    [Time: 0.000920000 seconds]
    ```

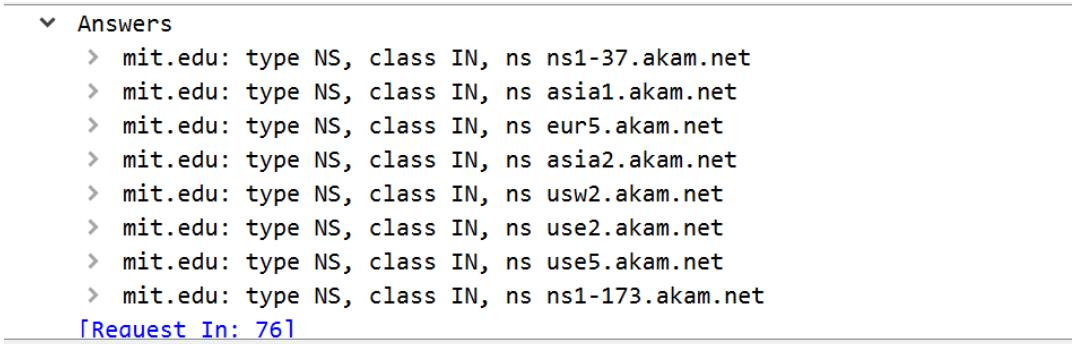
    3个回复，包含两个主机别名和一个IP地址

15.
    ```

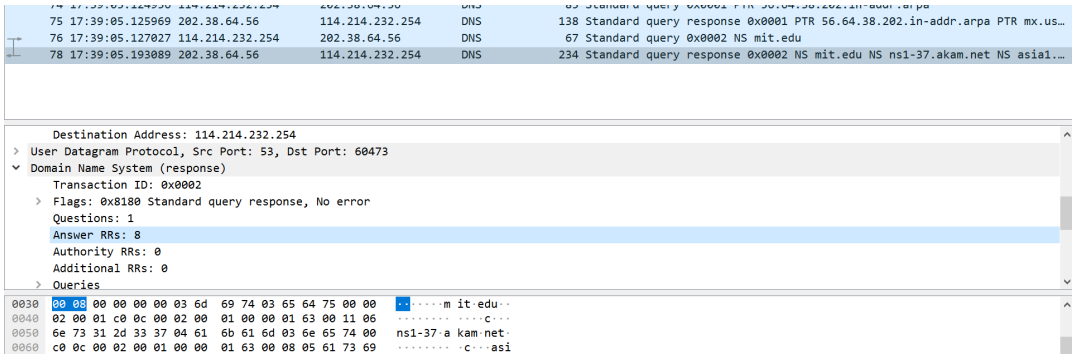


更换指令重复实验，回答问题

16. IP地址202.38.64.56，是本地服务器DNS地址
17. type是NS，Answer RRs：0，没有任何answer
18. 域名服务器



没有提供IP地址

19. 

更改指令后重复操作，回答问题

20. 地址是18.0.72.3，不是本地默认DNS服务器地址，这是mit的bitsy.mit.edu的IP地址
21. type是A，Answer RRs：0，没有回复
22. DNS查询失败，从23的截图中看出wireshark中并没有回复，所以answer应该是0

23.

```
C:\Users\P>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
服务器:  UnKnown
Address:  18.0.72.3

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
```

```
 16 17:54:24.664518 202.38.64.56     114.214.232.254 DNS 138 Standard query response 0xc7f9 AAAA bitsy.mit.edu SOA use2.
 19 17:54:24.666689 114.214.232.254  18.0.72.3       DNS  82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
 49 17:54:26.678450 114.214.232.254  18.0.72.3       DNS  74 Standard query 0x0002 A www.aiit.or.kr
 71 17:54:28.690001 114.214.232.254  18.0.72.3       DNS  74 Standard query 0x0003 AAAA www.aiit.or.kr
114 17:54:30.707738 114.214.232.254  18.0.72.3       DNS  74 Standard query 0x0004 A www.aiit.or.kr
484 17:54:32.719810 114.214.232.254  18.0.72.3       DNS  74 Standard query 0x0005 AAAA www.aiit.or.kr
```

```
    Destination Address: 18.0.72.3
> User Datagram Protocol, Src Port: 65150, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
```

```
0000  5c dd 70 91 72 e2 f8 e4  3b 4b e9 b8 08 00 45 00   \·p·r··· ;K····E·
0010  00 3c 74 53 00 00 80 11  00 00 72 d6 e8 fe 12 00   ·<tS···· ··r·····
0020  48 03 fe 7e 00 35 00 28  b6 11 00 02 01 00 00 01   H··~·5·( ········
0030  00 00 00 00 00 00 03 77  77 77 04 61 69 69 74 02   ·······w ww·aiit·
0040  6f 72 02 6b 72 00 00 01  00 01                     or·kr··· ··
```