60-367 Assignment 1

Calvin Moras, Ryan Lebeau

104448832 - 104535367

HTTP

1. My browser is running HTTP/1.1, the server is running 1.1 as well.
2. English-US and English (general) are the languages accepted.
3. At the time of testing, my computer's IP address was 10.242.95.164, the server's was 128.119.245.12.
4. The server returned a status code 200, the "OK" message indicating everything went correctly.
5. The date last modified was Thu, 27 Sep 2018 05:59:01 GMT
6. A 520 byte response was sent from the server to the client.
7. No, there were no headers available in the raw data that were not already available in the packet listing window. This makes sense because the raw data simply lists every bit in the packet.
8. No, there is no IF-MODIFIED-SINCE entry.
9. Yes, under line-based text data or at the end of the raw data, the page contents can be read.
10. Yes, there was an IF-MODIFIED-SINCE: Thu, 27 Sep 2018 05:59:01 GMT
11. The server returns status code 302 with response "NOT MODIFIED.", meaning that the packets sent the first time were not replaced with a new copy. In other words, the page was reloaded but the contents were not resent.
12. My browser sent one get request, packet 188.
13. Packet 194 contains the server response.

14. The response code was a 200 “OK” message.
15. 4 Data-containing TCP segments were needed to carry the 4861 http response, packets 190-194.
16. My browser sent 3 get requests. One request to load the page’s html at 128.119.245.12, one request to load the pearson.png to the same IP, and one to load the textbook cover jpg at the same IP as well.
17. After creating a column for a TCP-stream index, I was able to see that the first two get requests were on the same TCP stream, but last request was part of a different. This would tell me the first image and main page html were downloaded in parallel, but the second image was downloaded serially after. Looking at just the two images, this would technically mean they were serial.
18. Initially, when attempting a GET request, the server provides a 401 Unauthorized response.
19. The new HTTP GET request contains a field called Authorization: Basic, with the base-64 value d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=, which translates to wireshark-students:network, the entered username and password.

DNS

1. The IP Address of a specific web server located in Asia is 162.105.131.196
2. The authoritative DNS server address for the Milan Institute is 159.149.10.1
3. The address is 216.109.127.60
4. Both query and response messages are UDP.
5. The query destination port is 53 and the response source port is 53.
6. The query destination ip address is 192.168.0.1 which is my local DNS server.

7. The query is of Recursive type and contains 0 answers.

8. The response contains 3 answers which contain type “A”, class “IN”, and an address “104.20.1.85”.

9. The destination address of the SYN packet corresponds to the DNS address of the website server, listed as an answer in the DNS response.

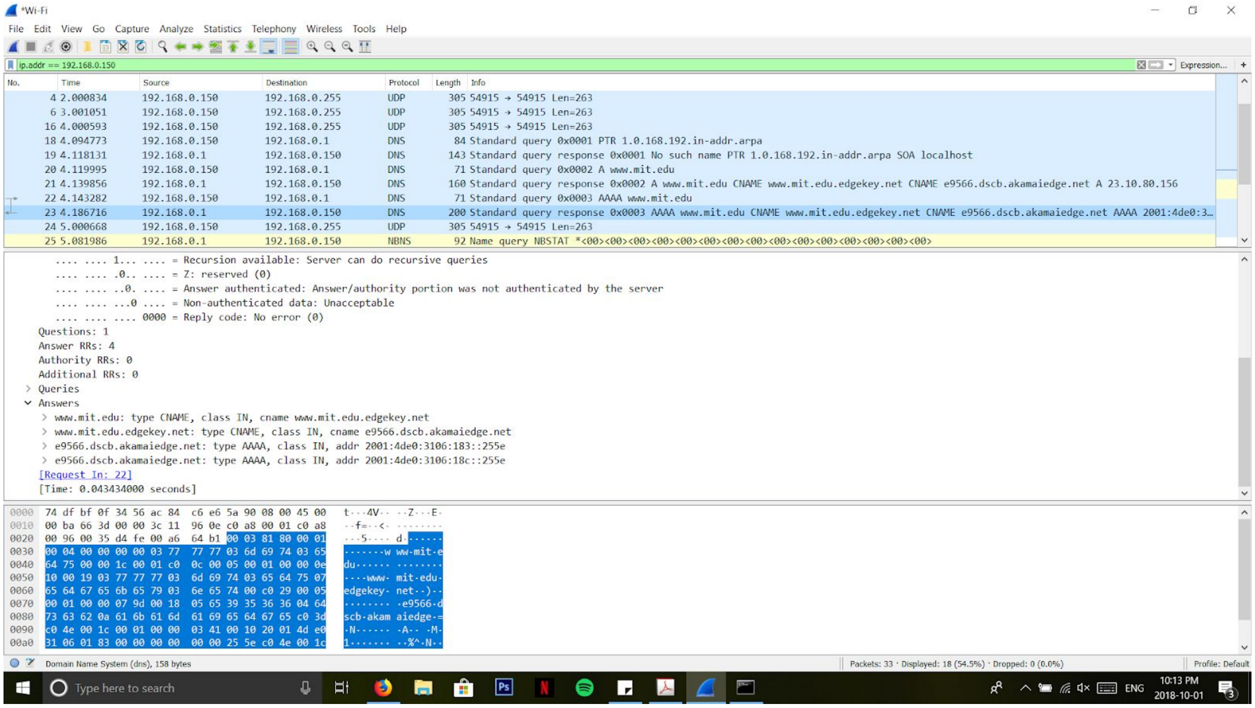
10. No the host does not issue new DNS queries before receiving each image.

11. The destination port of the DNS query is 53, the source port of the DNS response is 53

12. The query is sent to address 192.168.0.1 and yes it is the same as my local DNS server.

13. The query is of type Recursive and contains 0 answers.

14. There are 4 answers within the query response, 2 are of type CNAME and 2 of type AAAA, all are of class IN, the first 2 access a cname and the last 2 access an address.

15. 
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Type here to search
ENG
10:13 PM
2018-10-01

```
ip.addr == 192.168.0.150
```

```
No.  Time      Source         Destination    Protocol Length Info
   4 2.000834  192.168.0.150  192.168.0.255  UDP      305 54915 → 54915 Len=263
   6 3.001051  192.168.0.150  192.168.0.255  UDP      305 54915 → 54915 Len=263
  16 4.000593  192.168.0.150  192.168.0.255  UDP      305 54915 → 54915 Len=263
  18 4.094773  192.168.0.150  192.168.0.1    DNS       84 Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
  19 4.118131  192.168.0.1    192.168.0.150  DNS      143 Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa SOA localhost
  20 4.119995  192.168.0.150  192.168.0.1    DNS       71 Standard query 0x0002 A www.mit.edu
  21 4.139856  192.168.0.1    192.168.0.150  DNS      160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.10.80.156
  22 4.143282  192.168.0.150  192.168.0.1    DNS       71 Standard query 0x0003 AAAA www.mit.edu
  23 4.186716  192.168.0.1    192.168.0.150  DNS      200 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2001:4de0:3…
  24 5.000668  192.168.0.150  192.168.0.255  UDP      305 54915 → 54915 Len=263
  25 5.081986  192.168.0.1    192.168.0.150  NBNS      92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
```

```
        .... .... 1... .... = Recursion available: Server can do recursive queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 4
    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 AAAA, class IN, addr 2001:4de0:3106:183::255e
    > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2001:4de0:3106:18c::255e
    [Request In: 22]
    [Time: 0.043434000 seconds]
```

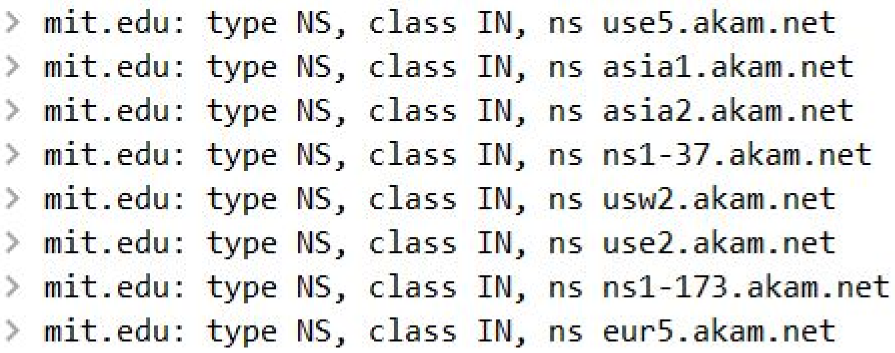
```
0000  74 df bf 0f 34 56 ac 84  c6 e6 5a 90 08 00 45 00   t···4V·· ··Z···E·
0010  00 ba 66 3d 00 00 3c 11  96 0e c0 a8 00 01 c0 a8   ··f=··<· ········
0020  00 96 00 35 d4 fe 00 a6  64 b1 00 03 81 80 00 01   ···5···· d·······
0030  00 04 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 1c 00 01 c0  0c 00 05 00 01 00 00 0e   du······ ········
0050  10 00 19 03 77 77 77 03  6d 69 74 03 65 64 75 07   ····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 07 9d 00 18  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 c0 3d   scb·akam aiedge·=
0090  c0 4e 00 1c 00 01 00 00  03 41 00 10 20 01 4d e0   ·N······ ·A·· ·M·
00a0  31 06 01 83 00 00 00 00  00 00 25 5e c0 4e 00 1c   1······· ··%^·N··
```

```
Domain Name System (dns), 158 bytes    Packets: 33 · Displayed: 18 (54.5%) · Dropped: 0 (0.0%)    Profile: Default
```

16. The query destination address is 192.168.0.1 which is the address of my local DNS server.

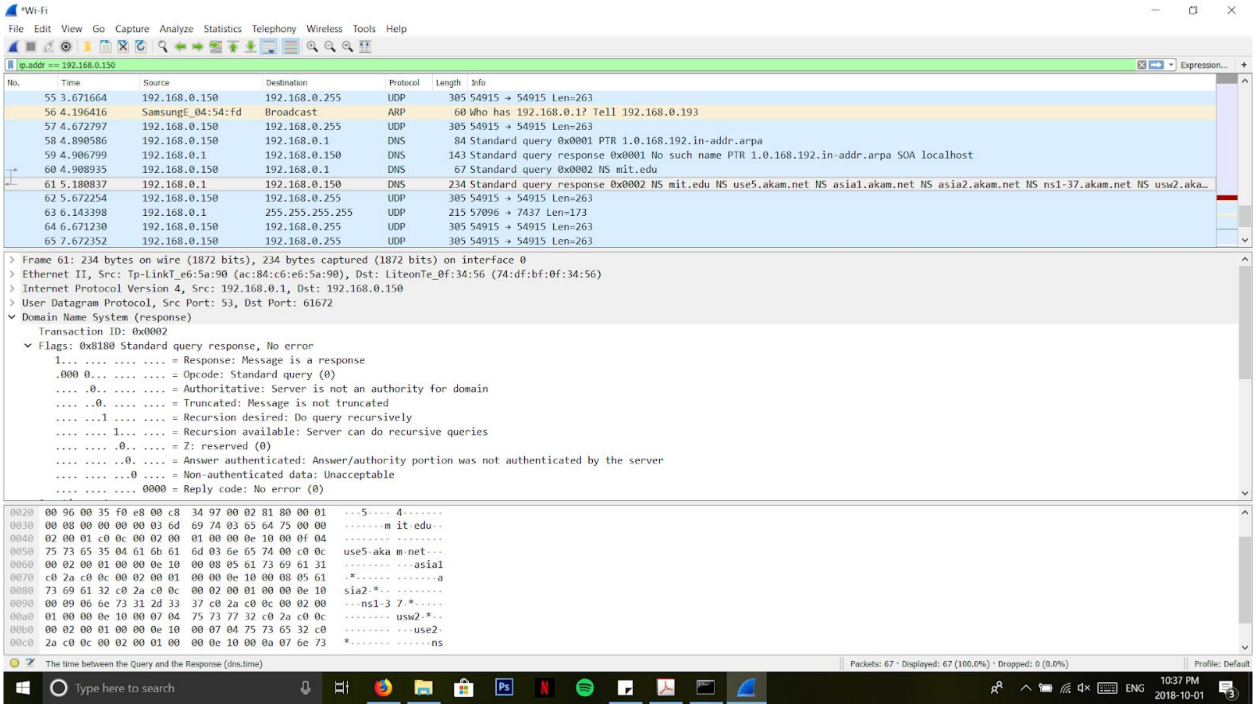
17. The query is Recursive and contains 0 answers.

18. The response provides 8 different nameservers with no IP addresses.



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

19.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Type here to search
ENG
10:37 PM
2018-10-01

```
ip.addr == 192.168.0.150

No.  Time      Source             Destination      Protocol Length Info
  55 3.671664  192.168.0.150      192.168.0.255    UDP         305 54915 → 54915 Len=263
  56 4.196416  SamsungE_04:54:fd  Broadcast        ARP          60 Who has 192.168.0.1? Tell 192.168.0.193
  57 4.672797  192.168.0.150      192.168.0.255    UDP         305 54915 → 54915 Len=263
  58 4.890586  192.168.0.150      192.168.0.1      DNS          84 Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
  59 4.906799  192.168.0.1        192.168.0.150    DNS         143 Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa SOA localhost
  60 4.908935  192.168.0.150      192.168.0.1      DNS          67 Standard query 0x0002 NS mit.edu
  61 5.180837  192.168.0.1        192.168.0.150    DNS         234 Standard query response 0x0002 NS mit.edu NS use5.akam.net NS asia1.akam.net NS asia2.akam.net NS ns1-37.akam.net NS usw2.aka…
  62 5.672254  192.168.0.150      192.168.0.255    UDP         305 54915 → 54915 Len=263
  63 6.143398  192.168.0.1        255.255.255.255  UDP         215 57096 → 7437 Len=173
  64 6.671230  192.168.0.150      192.168.0.255    UDP         305 54915 → 54915 Len=263
  65 7.672352  192.168.0.150      192.168.0.255    UDP         305 54915 → 54915 Len=263
```

```
> Frame 61: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_e6:5a:90 (ac:84:c6:e6:5a:90), Dst: LiteonTe_0f:34:56 (74:df:bf:0f:34:56)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.150
> User Datagram Protocol, Src Port: 53, Dst Port: 61672
v Domain Name System (response)
    Transaction ID: 0x0002
  v Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
```

```
0020  00 96 00 35 f0 e8 00 c8  34 97 00 02 81 80 00 01   ···5···· 4·······
0030  00 08 00 00 00 00 03 6d  69 74 03 65 64 75 00 00   ·······m it·edu··
0040  02 00 01 c0 0c 00 02 00  01 00 00 0e 10 00 0f 04   ········ ········
0050  75 73 65 35 04 61 6b 61  6d 03 6e 65 74 00 c0 0c   use5·aka m·net···
0060  00 02 00 01 00 00 0e 10  00 08 05 61 73 69 61 31   ········ ···asia1
0070  c0 2a c0 0c 00 02 00 01  00 00 0e 10 00 08 05 61   ·*······ ·······a
0080  73 69 61 32 c0 2a c0 0c  00 02 00 01 00 00 0e 10   sia2·*·· ········
0090  00 09 06 6e 73 31 2d 33  37 c0 2a c0 0c 00 02 00   ···ns1-3 7·*·····
00a0  01 00 00 0e 10 00 07 04  75 73 77 32 c0 2a c0 0c   ········ usw2·*··
00b0  00 02 00 01 00 00 0e 10  00 07 04 75 73 65 32 c0   ········ ···use2·
00c0  2a c0 0c 00 02 00 01 00  00 0e 10 00 0a 07 6e 73   *······· ······ns
```

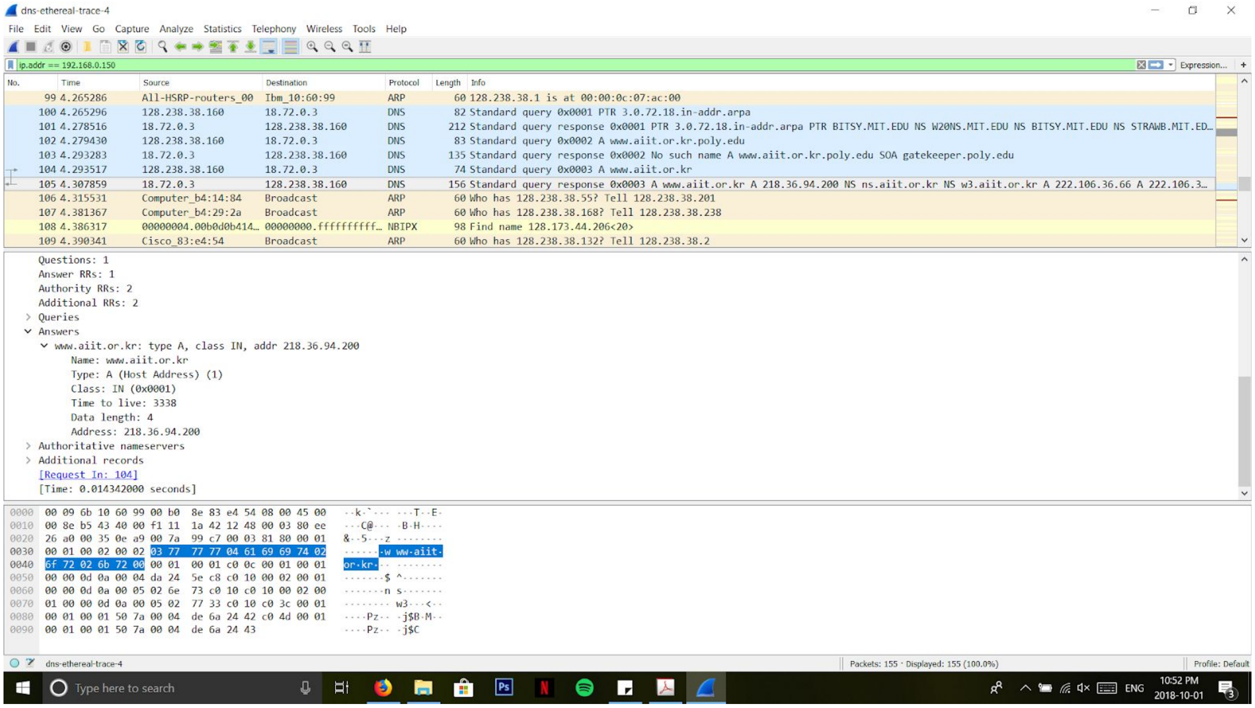
```
The time between the Query and the Response (dns.time)    Packets: 67 · Displayed: 67 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

20. The DNS query is sent to IP address 18.72.0.3 which is the address of bitsy.mit.edu

21. The DNS is of recursive type with 0 answers.

22. There is one answer of type A, class IN, and address 218.36.94.200

23.



```
No.   Time      Source                Destination           Protocol Length Info
   99 4.265286  All-HSRP-routers_00   Ibm_10:60:99          ARP         60 128.238.38.1 is at 00:00:0c:07:ac:00
  100 4.265296  128.238.38.160        18.72.0.3             DNS         82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
  101 4.278516  18.72.0.3             128.238.38.160        DNS        212 Standard query response 0x0001 PTR 3.0.72.18.in-addr.arpa PTR BITSY.MIT.EDU NS W20NS.MIT.EDU NS BITSY.MIT.EDU NS STRAWB.MIT.ED…
  102 4.279430  128.238.38.160        18.72.0.3             DNS         83 Standard query 0x0002 A www.aiit.or.kr.poly.edu
  103 4.293283  18.72.0.3             128.238.38.160        DNS        135 Standard query response 0x0002 No such name A www.aiit.or.kr.poly.edu SOA gatekeeper.poly.edu
  104 4.293517  128.238.38.160        18.72.0.3             DNS         74 Standard query 0x0003 A www.aiit.or.kr
  105 4.307859  18.72.0.3             128.238.38.160        DNS        156 Standard query response 0x0003 A www.aiit.or.kr A 218.36.94.200 NS ns.aiit.or.kr NS w3.aiit.or.kr A 222.106.36.66 A 222.106.3…
  106 4.315531  Computer_b4:14:84     Broadcast             ARP         60 Who has 128.238.38.55? Tell 128.238.38.201
  107 4.381367  Computer_b4:29:2a     Broadcast             ARP         60 Who has 128.238.38.168? Tell 128.238.38.238
  108 4.386317  00000004.00b0d0b414…  00000000.ffffffffff…  NBIPX       98 Find name 128.173.44.206<20>
  109 4.390341  Cisco_83:e4:54        Broadcast             ARP         60 Who has 128.238.38.132? Tell 128.238.38.2
```

```
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  > Queries
  ∨ Answers
    ∨ www.aiit.or.kr: type A, class IN, addr 218.36.94.200
        Name: www.aiit.or.kr
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3338
        Data length: 4
        Address: 218.36.94.200
  > Authoritative nameservers
  > Additional records
    [Request In: 104]
    [Time: 0.014342000 seconds]
```

```
0000  00 09 6b 10 60 99 00 b0  8e 83 e4 54 08 00 45 00   ··k·`··· ···T··E·
0010  00 8e b5 43 40 00 f1 11  1a 42 12 48 00 03 80 ee   ···C@··· ·B·H····
0020  26 a0 00 35 0e a9 00 7a  99 c7 00 03 81 80 00 01   &··5···z ········
0030  00 01 00 02 00 02 03 77  77 77 04 61 69 69 74 02   ·······w ww·aiit·
0040  6f 72 02 6b 72 00 00 01  00 01 c0 0c 00 01 00 01   or·kr··· ········
0050  00 00 0d 0a 00 04 da 24  5e c8 c0 10 00 02 00 01   ·······$ ^·······
0060  00 00 0d 0a 00 05 02 6e  73 c0 10 c0 10 00 02 00   ·······n s·······
0070  01 00 00 0d 0a 00 05 02  77 33 c0 10 c0 3c 00 01   ········ w3···<··
0080  00 01 00 01 50 7a 00 04  de 6a 24 42 c0 4d 00 01   ····Pz·· ·j$B·M··
0090  00 01 00 01 50 7a 00 04  de 6a 24 43              ····Pz·· ·j$C
```