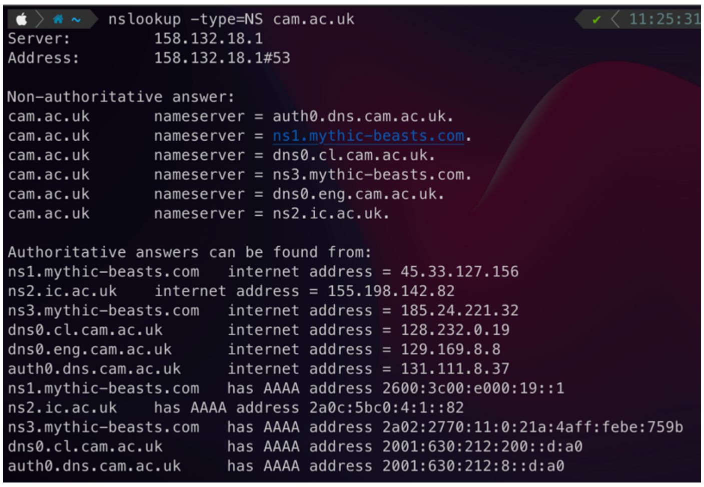
# Lab 3 DNS

# Lab Report

Guanlin Jiang (21093962D)

**Q2:** Run nslookup to determine the authoritative DNS servers for a university in Europe.

**Answer:** I look a university in Europe.

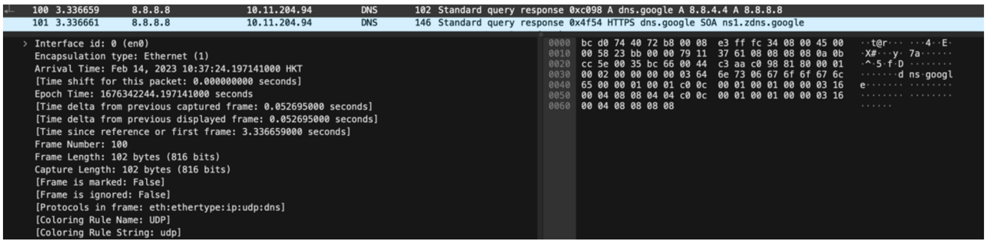


```
~ nslookup -type=NS cam.ac.uk                                  ✓ 11:25:31
Server:         158.132.18.1
Address:        158.132.18.1#53

Non-authoritative answer:
cam.ac.uk       nameserver = auth0.dns.cam.ac.uk.
cam.ac.uk       nameserver = ns1.mythic-beasts.com.
cam.ac.uk       nameserver = dns0.cl.cam.ac.uk.
cam.ac.uk       nameserver = ns3.mythic-beasts.com.
cam.ac.uk       nameserver = dns0.eng.cam.ac.uk.
cam.ac.uk       nameserver = ns2.ic.ac.uk.

Authoritative answers can be found from:
ns1.mythic-beasts.com   internet address = 45.33.127.156
ns2.ic.ac.uk    internet address = 155.198.142.82
ns3.mythic-beasts.com   internet address = 185.24.221.32
dns0.cl.cam.ac.uk       internet address = 128.232.0.19
dns0.eng.cam.ac.uk      internet address = 129.169.8.8
auth0.dns.cam.ac.uk     internet address = 131.111.8.37
ns1.mythic-beasts.com   has AAAA address 2600:3c00:e000:19::1
ns2.ic.ac.uk    has AAAA address 2a0c:5bc0:4:1::82
ns3.mythic-beasts.com   has AAAA address 2a02:2770:11:0:21a:4aff:febe:759b
dns0.cl.cam.ac.uk       has AAAA address 2001:630:212:200::d:a0
auth0.dns.cam.ac.uk     has AAAA address 2001:630:212:8::d:a0
```

**Q4:** Locate the DNS query and response messages. Are then sent over UDP or TCP?

**Answer:**

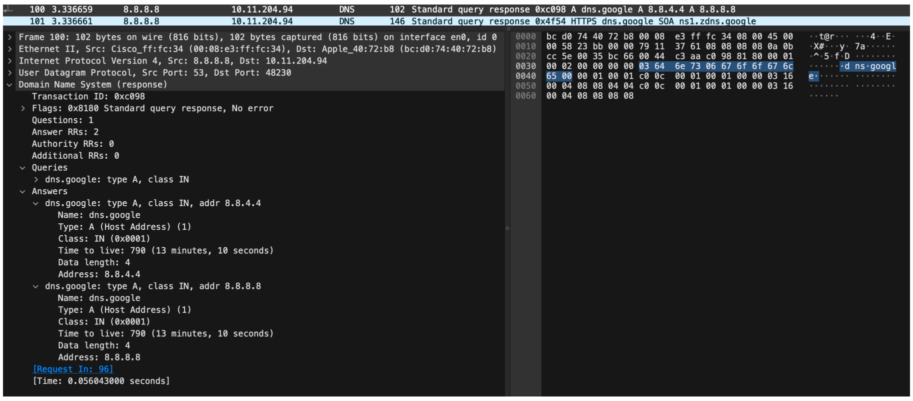
They send UDP.



```
100 3.336659   8.8.8.8   10.11.204.94   DNS   102 Standard query response 0xc098 A dns.google A 8.8.4.4 A 8.8.8.8
101 3.336661   8.8.8.8   10.11.204.94   DNS   146 Standard query response 0x4f54 HTTPS dns.google SOA ns1.zdns.google

> Interface id: 0 (en0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 14, 2023 10:37:24.197141000 HKT
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1676342244.197141000 seconds
  [Time delta from previous captured frame: 0.052695000 seconds]
  [Time delta from previous displayed frame: 0.052695000 seconds]
  [Time since reference or first frame: 3.336659000 seconds]
  Frame Number: 100
  Frame Length: 102 bytes (816 bits)
  Capture Length: 102 bytes (816 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:dns]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]

0000  bc d0 74 40 72 b8 00 08  e3 ff fc 34 08 00 45 00   ··t@r···  ···4··E·
0010  00 58 23 bb 00 00 79 11  37 61 08 08 08 08 0a 0b   ·X#···y·  7a······
0020  cc 5e 00 35 bc 66 00 44  c3 aa c0 98 81 80 00 01   ·^·5·f·D  ········
0030  00 02 00 00 00 00 03 64  6e 73 06 67 6f 6f 67 6c   ·······d  ns·googl
0040  65 00 00 01 00 01 c0 0c  00 01 00 01 00 00 03 16   e·······  ········
0050  00 04 08 08 04 04 c0 0c  00 01 00 01 00 00 03 16   ········  ········
0060  00 04 08 08 08 08                                  ······
```

**Q8:** Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

**Answer:**
2 “answers” are provided, the answer contain the name of the host, the type of address, class, the Time to Live, the data length and the IP address.

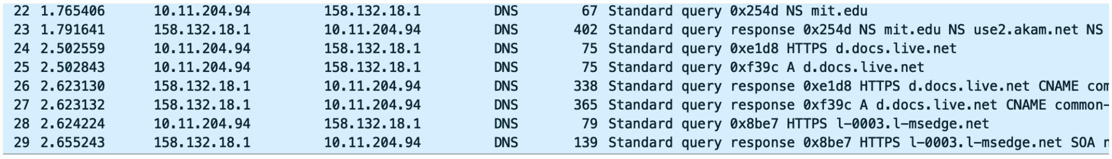


```
  100 3.336659    8.8.8.8        10.11.204.94     DNS     102 Standard query response 0xc098 A dns.google A 8.8.4.4 A 8.8.8.8
  101 3.336661    8.8.8.8        10.11.204.94     DNS     146 Standard query response 0x4f54 HTTPS dns.google SOA ns1.zdns.google
> Frame 100: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface en0, id 0
> Ethernet II, Src: Cisco_ff:fc:34 (00:08:e3:ff:fc:34), Dst: Apple_40:72:b8 (bc:d0:74:40:72:b8)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.11.204.94
> User Datagram Protocol, Src Port: 53, Dst Port: 48230
v Domain Name System (response)
    Transaction ID: 0xc098
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > dns.google: type A, class IN
  v Answers
    v dns.google: type A, class IN, addr 8.8.4.4
        Name: dns.google
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 790 (13 minutes, 10 seconds)
        Data length: 4
        Address: 8.8.4.4
    v dns.google: type A, class IN, addr 8.8.8.8
        Name: dns.google
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 790 (13 minutes, 10 seconds)
        Data length: 4
        Address: 8.8.8.8
    [Request In: 96]
    [Time: 0.056043000 seconds]

0000  bc d0 74 40 72 b8 00 08  e3 ff fc 34 08 00 45 00   ··t@r···  ···4··E·
0010  00 58 23 bb 00 00 79 11  37 61 08 08 08 08 0a 0b   ·X#···y·  7a······
0020  cc 5e 00 35 bc 66 00 44  c3 aa c0 98 81 80 00 01   ·^·5·f·D  ········
0030  00 02 00 00 00 00 03 64  6e 73 06 67 6f 6f 67 6c   ·······d  ns·googl
0040  65 00 00 01 00 01 c0 0c  00 01 00 01 00 00 03 16   e·······  ········
0050  00 04 08 08 04 04 c0 0c  00 01 00 01 00 00 03 16   ········  ········
0060  00 04 08 08 08 08                                  ······
```

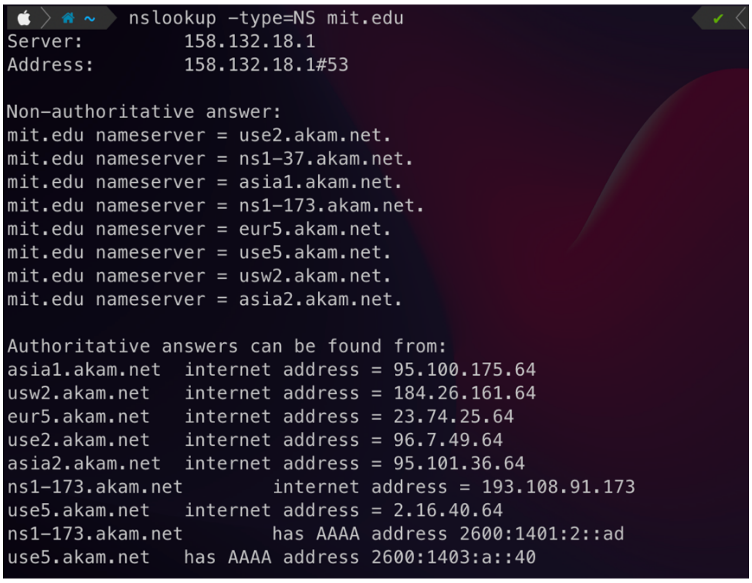
**Q12:** To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

**Answer:**

The IP address sent is 10.11.204.94, not the default local DNS server.



```
 22 1.765406    10.11.204.94    158.132.18.1    DNS    67 Standard query 0x254d NS mit.edu
 23 1.791641    158.132.18.1    10.11.204.94    DNS   402 Standard query response 0x254d NS mit.edu NS use2.akam.net NS
 24 2.502559    10.11.204.94    158.132.18.1    DNS    75 Standard query 0xe1d8 HTTPS d.docs.live.net
 25 2.502843    10.11.204.94    158.132.18.1    DNS    75 Standard query 0xf39c A d.docs.live.net
 26 2.623130    158.132.18.1    10.11.204.94    DNS   338 Standard query response 0xe1d8 HTTPS d.docs.live.net CNAME com
 27 2.623132    158.132.18.1    10.11.204.94    DNS   365 Standard query response 0xf39c A d.docs.live.net CNAME common-
 28 2.624224    10.11.204.94    158.132.18.1    DNS    79 Standard query 0x8be7 HTTPS l-0003.l-msedge.net
 29 2.655243    158.132.18.1    10.11.204.94    DNS   139 Standard query response 0x8be7 HTTPS l-0003.l-msedge.net SOA r
```

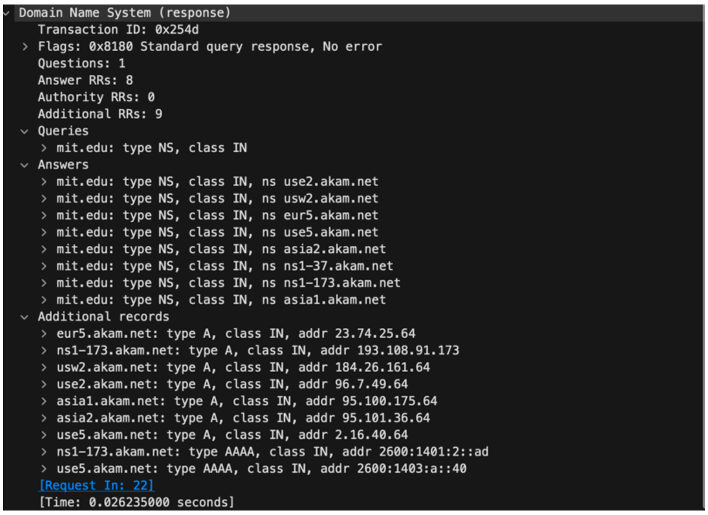


```
nslookup -type=NS mit.edu
Server:         158.132.18.1
Address:        158.132.18.1#53

Non-authoritative answer:
mit.edu nameserver = use2.akam.net.
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = ns1-173.akam.net.
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = asia2.akam.net.

Authoritative answers can be found from:
asia1.akam.net  internet address = 95.100.175.64
usw2.akam.net   internet address = 184.26.161.64
eur5.akam.net   internet address = 23.74.25.64
use2.akam.net   internet address = 96.7.49.64
asia2.akam.net  internet address = 95.101.36.64
ns1-173.akam.net        internet address = 193.108.91.173
use5.akam.net   internet address = 2.16.40.64
ns1-173.akam.net        has AAAA address 2600:1401:2::ad
use5.akam.net   has AAAA address 2600:1403:a::40
```

**Q14:** Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

**Answer:**

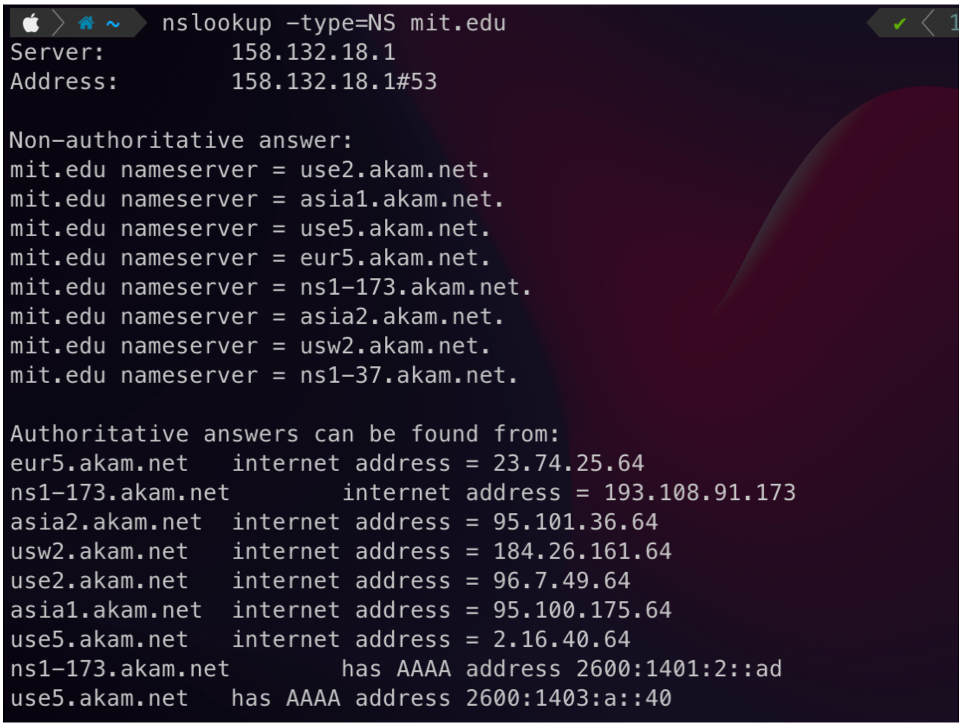
9 responses messages, the response DNS message contains one answer containing the name of the host, the type of address, the class, and the IP address.



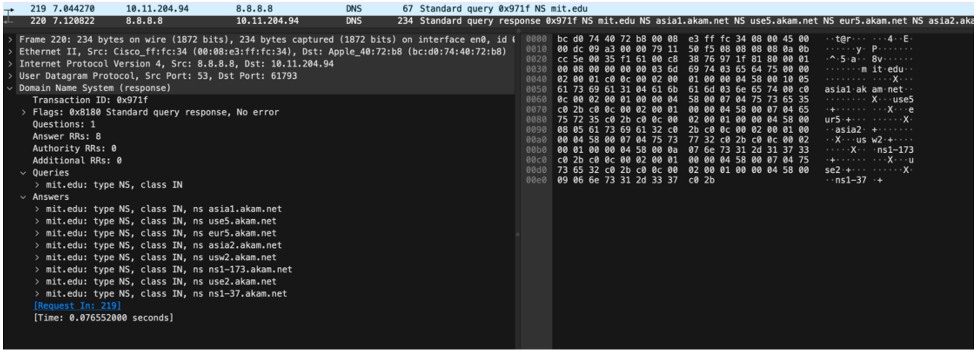
```
⌄ Domain Name System (response)
    Transaction ID: 0x254d
  › Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 9
  ⌄ Queries
    › mit.edu: type NS, class IN
  ⌄ Answers
    › mit.edu: type NS, class IN, ns use2.akam.net
    › mit.edu: type NS, class IN, ns usw2.akam.net
    › mit.edu: type NS, class IN, ns eur5.akam.net
    › mit.edu: type NS, class IN, ns use5.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 ns1-173.akam.net
    › mit.edu: type NS, class IN, ns asia1.akam.net
  ⌄ Additional records
    › eur5.akam.net: type A, class IN, addr 23.74.25.64
    › ns1-173.akam.net: type A, class IN, addr 193.108.91.173
    › usw2.akam.net: type A, class IN, addr 184.26.161.64
    › use2.akam.net: type A, class IN, addr 96.7.49.64
    › asia1.akam.net: type A, class IN, addr 95.100.175.64
    › asia2.akam.net: type A, class IN, addr 95.101.36.64
    › use5.akam.net: type A, class IN, addr 2.16.40.64
    › ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad
    › use5.akam.net: type AAAA, class IN, addr 2600:1403:a::40
    [Request In: 22]
    [Time: 0.026235000 seconds]
```

**Q18:** Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

**Answer:**
Nameserver are asia1.akam.net, use5.akam.net, eur5.akam.net, asia2.akam.net., usw2.akam.net, ns1-173.akam.net, use2.akam.net, ns1-37.akam.net. Also ip address from MIT nameserver in below.



```
 nslookup -type=NS mit.edu
Server:         158.132.18.1
Address:        158.132.18.1#53

Non-authoritative answer:
mit.edu nameserver = use2.akam.net.
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = ns1-173.akam.net.
mit.edu nameserver = asia2.akam.net.
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = ns1-37.akam.net.

Authoritative answers can be found from:
eur5.akam.net   internet address = 23.74.25.64
ns1-173.akam.net        internet address = 193.108.91.173
asia2.akam.net  internet address = 95.101.36.64
usw2.akam.net   internet address = 184.26.161.64
use2.akam.net   internet address = 96.7.49.64
asia1.akam.net  internet address = 95.100.175.64
use5.akam.net   internet address = 2.16.40.64
ns1-173.akam.net        has AAAA address 2600:1401:2::ad
use5.akam.net   has AAAA address 2600:1403:a::40
```



```
    219 7.044270     10.11.204.94       8.8.8.8            DNS      67 Standard query 0x971f NS mit.edu
    220 7.120822     8.8.8.8            10.11.204.94       DNS     234 Standard query response 0x971f NS mit.edu NS asia1.akam.net NS use5.akam.net NS eur5.akam.net NS asia2.aka
```

```
> Frame 220: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface en0, id (
> Ethernet II, Src: Cisco_ff:fc:34 (00:08:e3:ff:fc:34), Dst: Apple_40:72:b8 (bc:d0:74:40:72:b8)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.11.204.94
> User Datagram Protocol, Src Port: 53, Dst Port: 61793
v Domain Name System (response)
    Transaction ID: 0x971f
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > mit.edu: type NS, class IN
  v Answers
    > mit.edu: type NS, class IN, ns asia1.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    [Request In: 219]
    [Time: 0.076552000 seconds]
```

```
0000  bc d0 74 40 72 b8 00 08  e3 ff fc 34 08 00 45 00   ··t@r··· ···4··E·
0010  00 dc 09 a3 00 00 79 11  50 f5 08 08 08 08 0a 0b   ······y· P·······
0020  cc 5e 00 35 f1 61 00 c8  38 76 97 1f 81 80 00 01   ·^·5·a·· 8v······
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 04 58 00 10 05   ········ ····X···
0050  61 73 69 61 31 04 61 6b  61 6d 03 6e 65 74 00 c0   asia1·ak am·net··
0060  0c 00 02 00 01 00 00 04  58 00 07 04 75 73 65 35   ········ X···use5
0070  c0 2b c0 0c 00 02 00 01  00 00 04 58 00 07 04 65   ·+······ ···X···e
0080  75 72 35 c0 2b c0 0c 00  02 00 01 00 00 04 58 00   ur5·+··· ······X·
0090  08 05 61 73 69 61 32 c0  2b c0 0c 00 02 00 01 00   ··asia2· +·······
00a0  00 04 58 00 07 04 75 73  77 32 c0 2b c0 0c 00 02   ··X···us w2·+····
00b0  00 01 00 00 04 58 00 0a  07 6e 73 31 2d 31 37 33   ·····X·· ·ns1-173
00c0  c0 2b c0 0c 00 02 00 01  00 00 04 58 00 07 04 75   ·+······ ···X···u
00d0  73 65 32 c0 2b c0 0c 00  02 00 01 00 00 04 58 00   se2·+··· ······X·
00e0  09 06 6e 73 31 2d 33 37  c0 2b                     ··ns1-37 ·+
```