Matthew Irvine

1001401200

DNS

#1

Name: kamatera.com

Addresses: 2606:4700:3033::6815:1a6b

2606:4700:3032::ac43:87e0

104.21.26.107

172.67.135.224

#2

C:\Users\keepc>nslookup -type=NS cam.ac.uk

Server: dsldevice6.attlocal.net

Address: 2600:1700:580:70e0::1

Non-authoritative answer:

cam.ac.uk nameserver = dns0.cl.cam.ac.uk

cam.ac.uk nameserver = ns1.mythic-beasts.com

cam.ac.uk nameserver = ns2.ic.ac.uk

cam.ac.uk nameserver = dns0.eng.cam.ac.uk

cam.ac.uk nameserver = ns3.mythic-beasts.com

cam.ac.uk nameserver = auth0.dns.cam.ac.uk

#3

Non-authoritative answer:

Name: edge.gycpi.b.yahoodns.net

Addresses: 2001:4998:20:800::1001

2001:4998:20:800::1000

69.147.86.12

69.147.86.11

Aliases: mail.yahoo.com

#4

TCP

28	23:24:04.629337	192.168.1.130	192.168.1.254	DNS	72 Standard query 0xd825 A www.ietf.org
29	23:24:04.663281	192.168.1.254	192.168.1.130	DNS	149 Standard query response 0xd825 A www.ietf.org CNAME www.ietf.org.cdn.clo
426	23:24:05.253679	162.159.136.234	192.168.1.130	TLSv1.2	101 Application Data
427	23:24:05.293450	192.168.1.130	162.159.136.234	TCP	54 49657 → 443 [ACK] Seq=1 Ack=48 Win=63194 Len=0
436	23:24:05.715782	162.159.136.234	192.168.1.130	TLSv1.2	100 Application Data
437	23:24:05.755771	192.168.1.130	162.159.136.234	TCP	54 49657 → 443 [ACK] Seq=1 Ack=94 Win=63148 Len=0
787	23:24:06.908022	162.159.136.234	192.168.1.130	TLSv1.2	143 Application Data
788	23:24:06.948859	192.168.1.130	162.159.136.234	TCP	54 49657 → 443 [ACK] Seq=1 Ack=183 Win=63059 Len=0
790	23:24:07.436416	162.159.136.234	192.168.1.130	TLSv1.2	229 Application Data
791	23:24:07.476587	192.168.1.130	162.159.136.234	TCP	54 49657 → 443 [ACK] Seq=1 Ack=358 Win=64400 Len=0

#5

Dest Port: 53

Src Port: 59948

#6

Dst Address: 192.168.1.254

Local DNS: 192.168.1.254

So, yes, they are the same:

```
Default Gateway . . . . . . . . . : fe80::8a96:4eff:fe2f:b9d0%28
                                    192.168.1.254
```

#7 and #8

Type A query, it does contain answers.

Answers:

```
www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
   Name: www.ietf.org
   Type: CNAME (Canonical NAME for an alias) (5)
   Class: IN (0x0001)
   Time to live: 1800 (30 minutes)
   Data length: 33
   CNAME: www.ietf.org.cdn.cloudflare.net
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
   Name: www.ietf.org.cdn.cloudflare.net
   Type: A (Host Address) (1)
   Class: IN (0x0001)
   Time to live: 300 (5 minutes)
   Data length: 4
   Address: 104.16.44.99
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
   Name: www.ietf.org.cdn.cloudflare.net
   Type: A (Host Address) (1)
   Class: IN (0x0001)
   Time to live: 300 (5 minutes)
   Data length: 4
   Address: 104.16.45.99
```

#9

No, the destination address does not look like any of these answers.

```
C:\Users\keepc>nslookup ietf.org
Server:  dsldevice6.attlocal.net
Address:  2600:1700:580:70e0::1

Non-authoritative answer:
Name:    ietf.org
Addresses:  2001:1900:3001:11::2c
          4.31.198.44
```

IP: 4.31.198.44 or 2001:1900:3001:11::2c

2600:1700:580:70e0:d142:d…	2001:1900:3001:11::2c	TCP	90	65369 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM=1 TSval=4
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TCP	90	443 → 65369 [SYN, ACK] Seq=0 Ack=1 Win=26960 Len=0 MSS=1360 SACK_PER
2600:1700:580:70e0:d142:d…	2001:1900:3001:11::2c	TCP	86	65369 → 443 [ACK] Seq=1 Ack=1 Win=64800 Len=0 TSval=49020571 TSecr=2
2600:1700:580:70e0:d142:d…	2001:1900:3001:11::2c	TLSv1.2	605	Client Hello
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TCP	86	443 → 65369 [ACK] Seq=1 Ack=520 Win=27872 Len=0 TSval=2055014397 TSe
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TLSv1.2	242	Server Hello, Change Cipher Spec, Encrypted Handshake Message
2600:1700:580:70e0:d142:d…	2001:1900:3001:11::2c	TLSv1.2	137	Change Cipher Spec, Encrypted Handshake Message
2600:1700:580:70e0:d142:d…	2001:1900:3001:11::2c	TLSv1.2	585	Application Data
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TCP	86	443 → 65369 [ACK] Seq=157 Ack=1070 Win=28944 Len=0 TSval=2055014447
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TLSv1.2	2942	Application Data
2600:1700:580:70e0:d142:d…	2001:1900:3001:11::2c	TCP	86	65369 → 443 [ACK] Seq=1070 Ack=3013 Win=64704 Len=0 TSval=49020679 T
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TCP	5798	443 → 65369 [ACK] Seq=3013 Ack=1070 Win=28944 Len=5712 TSval=2055014
2600:1700:580:70e0:d142:d…	2001:1900:3001:11::2c	TCP	86	65369 → 443 [ACK] Seq=1070 Ack=8725 Win=64704 Len=0 TSval=49020680 T
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TLSv1.2	2942	Application Data [TCP segment of a reassembled PDU]
2600:1700:580:70e0:d142:d…	2001:1900:3001:11::2c	TCP	86	65369 → 443 [ACK] Seq=1070 Ack=11581 Win=64704 Len=0 TSval=49020680
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TCP	2942	443 → 65369 [ACK] Seq=11581 Ack=1070 Win=28944 Len=2856 TSval=205501
2600:1700:580:70e0:d142:d…	2001:1900:3001:11::2c	TCP	86	65369 → 443 [ACK] Seq=1070 Ack=14437 Win=64704 Len=0 TSval=49020680
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TCP	1514	443 → 65369 [ACK] Seq=14437 Ack=1070 Win=28944 Len=1428 TSval=205501
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
2600:1700:580:70e0:d142:d…	2001:1900:3001:11::2c	TCP	86	65369 → 443 [ACK] Seq=1070 Ack=17293 Win=64704 Len=0 TSval=49020725
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TCP	1514	443 → 65369 [ACK] Seq=17293 Ack=1070 Win=28944 Len=1428 TSval=205501
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TCP	1514	443 → 65369 [ACK] Seq=18721 Ack=1070 Win=28944 Len=1428 TSval=205501
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TLSv1.2	4370	Application Data [TCP segment of a reassembled PDU]
2001:1900:3001:11::2c	2600:1700:580:70e0:d142:d…	TLSv1.2	106	Application Data

Found the second address however, it does not match any from the DNS answer.

#10

Yes, the host does issue new DNS queries.

567	23:40:09.853805	2600:1700:580:70e0:d142:d…	2600:1700:580:70e0::1	DNS	92 Standard query 0x9f9b A www.ietf.org
568	23:40:09.854526	2600:1700:580:70e0:d142:d…	2600:1700:580:70e0::1	DNS	92 Standard query 0x2c0a AAAA www.ietf.org
569	23:40:09.889827	2600:1700:580:70e0::1	2600:1700:580:70e0:d142:d…	DNS	169 Standard query response 0x9f9b A www.ietf.org CNAME www.ietf.org.cdn.clou…
570	23:40:09.919446	2600:1700:580:70e0::1	2600:1700:580:70e0:d142:d…	DNS	193 Standard query response 0x2c0a AAAA www.ietf.org CNAME www.ietf.org.cdn.c…
767	23:40:10.194347	2600:1700:580:70e0:d142:d…	2600:1700:580:70e0::1	DNS	98 Standard query 0x8ac3 A analytics.ietf.org
768	23:40:10.194517	2600:1700:580:70e0:d142:d…	2600:1700:580:70e0::1	DNS	98 Standard query 0x79ac AAAA analytics.ietf.org
890	23:40:10.235214	2600:1700:580:70e0::1	2600:1700:580:70e0:d142:d…	DNS	114 Standard query response 0x8ac3 A analytics.ietf.org A 4.31.198.44
893	23:40:10.236736	2600:1700:580:70e0::1	2600:1700:580:70e0:d142:d…	DNS	126 Standard query response 0x79ac AAAA analytics.ietf.org AAAA 2001:1900:300…

#11

Dst port: 53

Src port: 56970

#12

Destination Address: 2600:1700:580:70e0::1

It is the IP address of my DNS

#13 and #14

Type A DNS Query and it has answers:

```
Answers
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1800 (30 minutes)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 60 (1 minute)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type CNAME, class IN, cname user-att-99-150-144-0.e9566.dscb.akamaiedge.net
      Name: e9566.dscb.akamaiedge.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1 (1 second)
      Data length: 24
      CNAME: user-att-99-150-144-0.e9566.dscb.akamaiedge.net
  user-att-99-150-144-0.e9566.dscb.akamaiedge.net: type A, class IN, addr 23.67.238.142
      Name: user-att-99-150-144-0.e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 4
      Address: 23.67.238.142
```

#16

Destination Address: 2600:1700:580:70e0::1

Not my local DNS

#17 and #18 and #19

Type NS, has Answers:

```
Answers
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1648 (27 minutes, 28 seconds)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 60 (1 minute)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type CNAME, class IN, cname user-att-99-150-144-0.e9566.dscb.akamaiedge.net
      Name: e9566.dscb.akamaiedge.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1 (1 second)
      Data length: 24
      CNAME: user-att-99-150-144-0.e9566.dscb.akamaiedge.net
Authoritative nameservers
  dscb.akamaiedge.net: type SOA, class IN, mname n0dscb.akamaiedge.net
      Name: dscb.akamaiedge.net
      Type: SOA (Start Of a zone of Authority) (6)
      Class: IN (0x0001)
      Time to live: 1000 (16 minutes, 40 seconds)
      Data length: 52
      Primary name server: n0dscb.akamaiedge.net
      Responsible authority's mailbox: hostmaster.akamai.com
      Serial Number: 1617339190
      Refresh Interval: 1000 (16 minutes, 40 seconds)
      Retry Interval: 1000 (16 minutes, 40 seconds)
      Expire limit: 1000 (16 minutes, 40 seconds)
      Minimum TTL: 1800 (30 minutes)
```

#20

Destination Address: 2600:1700:580:70e0::1

Not my local DNS, bitsy.mit.edu address instead.

#21 and #22 and #23

Type A, Answer:

```
bitsy.mit.edu: type A, class IN, addr 18.0.72.3
  Name: bitsy.mit.edu
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 104 (1 minute, 44 seconds)
  Data length: 4
  Address: 18.0.72.3
```