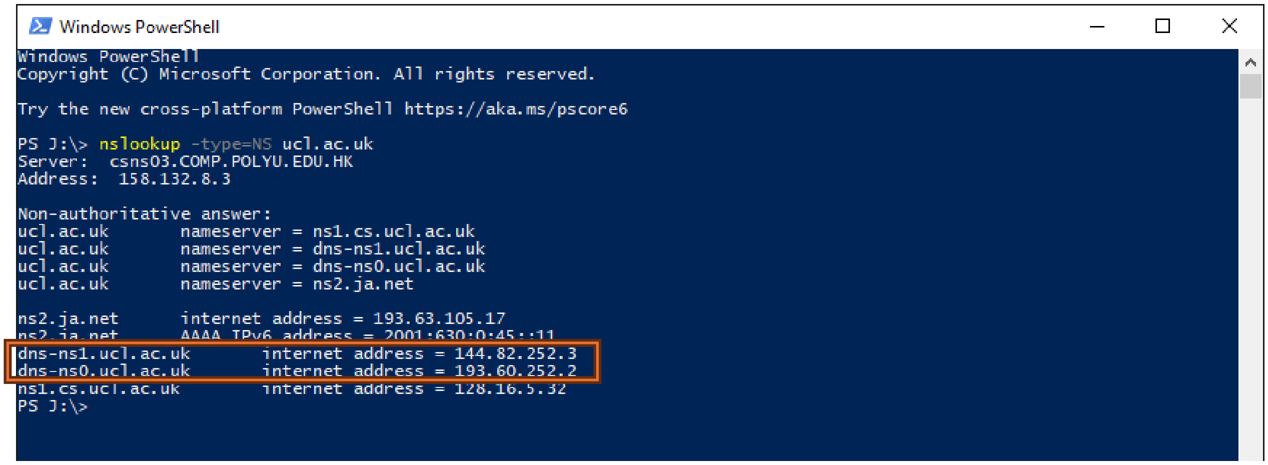
COMP2322 Computer Networking

Lab 3 DNS

Name: HE Yiyang

ID: 22100143D

Mar 1st, 2024



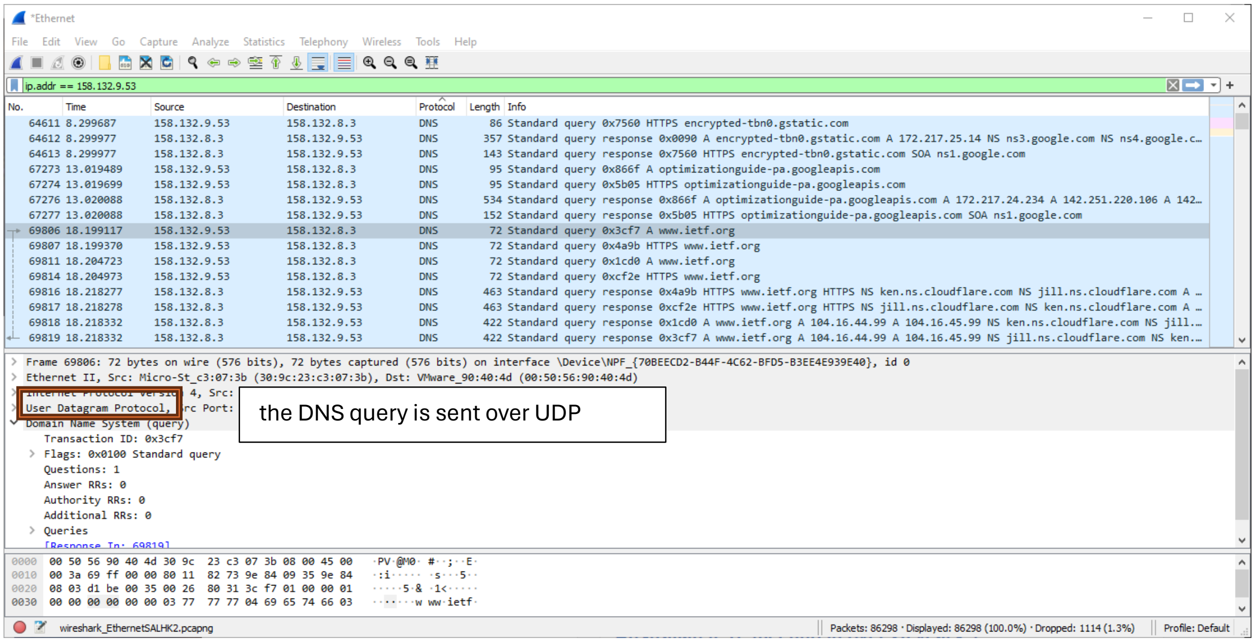
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS J:\> nslookup -type=NS ucl.ac.uk
Server:  csns03.COMP.POLYU.EDU.HK
Address:  158.132.8.3

Non-authoritative answer:
ucl.ac.uk       nameserver = ns1.cs.ucl.ac.uk
ucl.ac.uk       nameserver = dns-ns1.ucl.ac.uk
ucl.ac.uk       nameserver = dns-ns0.ucl.ac.uk
ucl.ac.uk       nameserver = ns2.ja.net

ns2.ja.net      internet address = 193.63.105.17
ns2.ja.net      AAAA IPv6 address = 2001:630:0:45::11
dns-ns1.ucl.ac.uk       internet address = 144.82.252.3
dns-ns0.ucl.ac.uk       internet address = 193.60.252.2
ns1.cs.ucl.ac.uk        internet address = 128.16.5.32
PS J:\>
```

Problem 2 trace file: a nslookup result for a European university's authoritative DNS servers

Problem 2 solution

I look up the UCL (University College London) in UK sever by nslookup and it owns 2 authoritative DNS servers. Their IP address are 144.82.252.3 and 193.60.252.2, respectively.

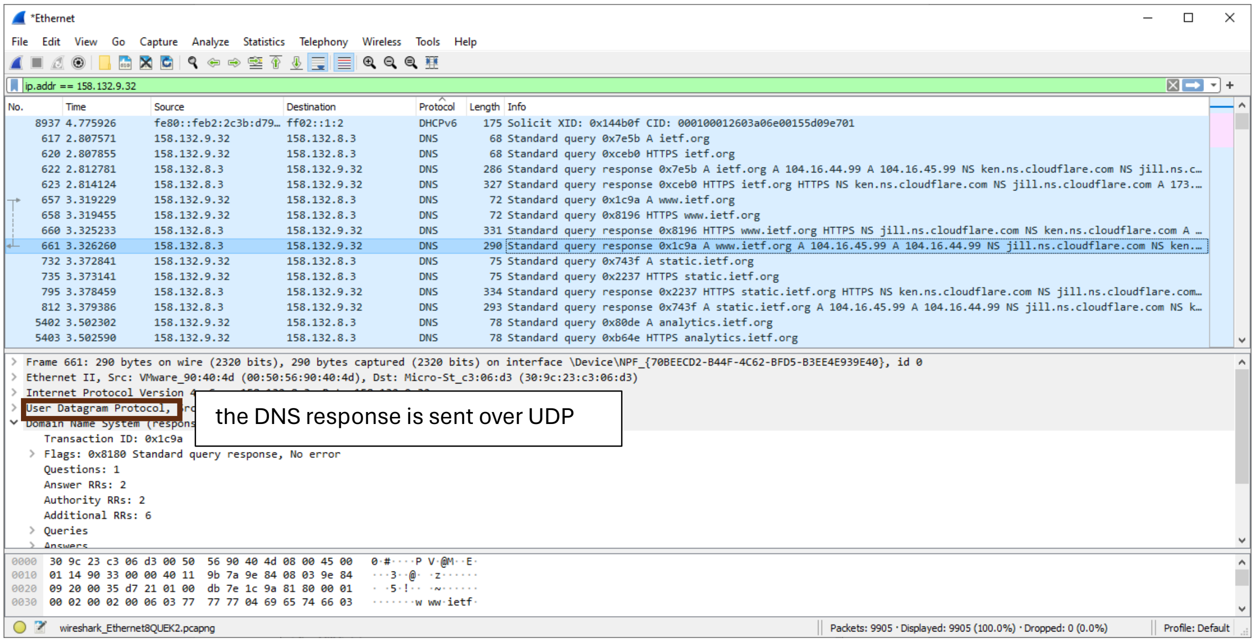
Part 3a:


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 158.132.9.53

No.   Time       Source        Destination   Protocol Length Info
64611 8.299687   158.132.9.53  158.132.8.3   DNS       86 Standard query 0x7560 HTTPS encrypted-tbn0.gstatic.com
64612 8.299977   158.132.8.3   158.132.9.53  DNS      357 Standard query response 0x0090 A encrypted-tbn0.gstatic.com A 172.217.25.14 NS ns3.google.com NS ns4.google.c…
64613 8.299977   158.132.8.3   158.132.9.53  DNS      143 Standard query response 0x7560 HTTPS encrypted-tbn0.gstatic.com SOA ns1.google.com
67273 13.019489  158.132.9.53  158.132.8.3   DNS       95 Standard query 0x866f A optimizationguide-pa.googleapis.com
67274 13.019699  158.132.9.53  158.132.8.3   DNS       95 Standard query 0x5b05 HTTPS optimizationguide-pa.googleapis.com
67276 13.020088  158.132.8.3   158.132.9.53  DNS      534 Standard query response 0x866f A optimizationguide-pa.googleapis.com A 172.217.24.234 A 142.251.220.106 A 142…
67277 13.020088  158.132.8.3   158.132.9.53  DNS      152 Standard query response 0x5b05 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
69806 18.199117  158.132.9.53  158.132.8.3   DNS       72 Standard query 0x3cf7 A www.ietf.org
69807 18.199370  158.132.9.53  158.132.8.3   DNS       72 Standard query 0x4a9b HTTPS www.ietf.org
69811 18.204723  158.132.9.53  158.132.8.3   DNS       72 Standard query 0x1cd0 A www.ietf.org
69814 18.204973  158.132.9.53  158.132.8.3   DNS       72 Standard query 0xcf2e HTTPS www.ietf.org
69816 18.218277  158.132.8.3   158.132.9.53  DNS      463 Standard query response 0x4a9b HTTPS www.ietf.org HTTPS NS ken.ns.cloudflare.com NS jill.ns.cloudflare.com A …
69817 18.218278  158.132.8.3   158.132.9.53  DNS      463 Standard query response 0xcf2e HTTPS www.ietf.org HTTPS NS jill.ns.cloudflare.com NS ken.ns.cloudflare.com A …
69818 18.218332  158.132.8.3   158.132.9.53  DNS      422 Standard query response 0x1cd0 A www.ietf.org A 104.16.44.99 A 104.16.45.99 NS ken.ns.cloudflare.com NS jill.…
69819 18.218332  158.132.8.3   158.132.9.53  DNS      422 Standard query response 0x3cf7 A www.ietf.org A 104.16.44.99 A 104.16.45.99 NS jill.ns.cloudflare.com NS ken.…

> Frame 69806: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{70BEECD2-B44F-4C62-BFD5-B3EE4E939E40}, id 0
> Ethernet II, Src: Micro-St_c3:07:3b (30:9c:23:c3:07:3b), Dst: VMware_90:40:4d (00:50:56:90:40:4d)
> Internet Protocol Version 4, Src:
> User Datagram Protocol, Src Port:
v Domain Name System (query)
    Transaction ID: 0x3cf7
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 69819]

0000  00 50 56 90 40 4d 30 9c  23 c3 07 3b 08 00 45 00   ·PV·@M0· #··;··E·
0010  00 3a 69 ff 00 00 80 11  82 73 9e 84 09 35 9e 84   ·:i····· ·s···5··
0020  08 03 d1 be 00 35 00 26  80 31 3c f7 01 00 00 01   ·····5·& ·1<·····
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf·

wireshark_EthernetSALHK2.pcapng    Packets: 86298 · Displayed: 86298 (100.0%) · Dropped: 1114 (1.3%)    Profile: Default
```

the DNS query is sent over UDP

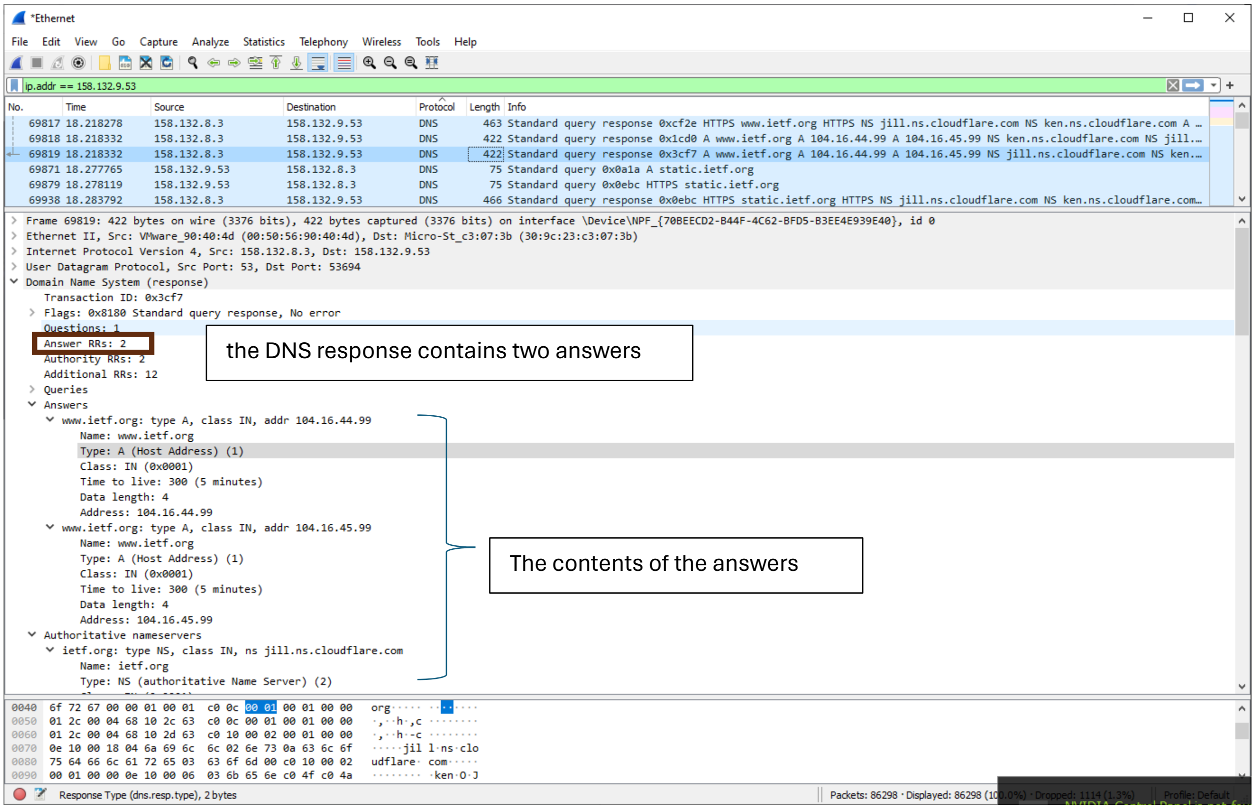
Problem 4 trace file: the DNS query



```
ip.addr == 158.132.9.32

No.   Time      Source                 Destination    Protocol Length Info
 8937 4.775926  fe80::feb2:2c3b:d79…   ff02::1:2      DHCPv6    175 Solicit XID: 0x144b0f CID: 000100012603a06e00155d09e701
  617 2.807571  158.132.9.32           158.132.8.3    DNS        68 Standard query 0x7e5b A ietf.org
  620 2.807855  158.132.9.32           158.132.8.3    DNS        68 Standard query 0xceb0 HTTPS ietf.org
  622 2.812781  158.132.8.3            158.132.9.32   DNS       286 Standard query response 0x7e5b A ietf.org A 104.16.44.99 A 104.16.45.99 NS ken.ns.cloudflare.com NS jill.ns.c…
  623 2.814124  158.132.8.3            158.132.9.32   DNS       327 Standard query response 0xceb0 HTTPS ietf.org HTTPS NS ken.ns.cloudflare.com NS jill.ns.cloudflare.com A 173.…
  657 3.319229  158.132.9.32           158.132.8.3    DNS        72 Standard query 0x1c9a A www.ietf.org
  658 3.319455  158.132.9.32           158.132.8.3    DNS        72 Standard query 0x8196 HTTPS www.ietf.org
  660 3.325233  158.132.8.3            158.132.9.32   DNS       331 Standard query response 0x8196 HTTPS www.ietf.org HTTPS NS jill.ns.cloudflare.com NS ken.ns.cloudflare.com A …
  661 3.326260  158.132.8.3            158.132.9.32   DNS       290 Standard query response 0x1c9a A www.ietf.org A 104.16.45.99 A 104.16.44.99 NS jill.ns.cloudflare.com NS ken.…
  732 3.372841  158.132.9.32           158.132.8.3    DNS        75 Standard query 0x743f A static.ietf.org
  735 3.373141  158.132.9.32           158.132.8.3    DNS        75 Standard query 0x2237 HTTPS static.ietf.org
  795 3.378459  158.132.8.3            158.132.9.32   DNS       334 Standard query response 0x2237 HTTPS static.ietf.org HTTPS NS ken.ns.cloudflare.com NS jill.ns.cloudflare.com…
  812 3.379386  158.132.8.3            158.132.9.32   DNS       293 Standard query response 0x743f A static.ietf.org A 104.16.45.99 A 104.16.44.99 NS jill.ns.cloudflare.com NS k…
 5402 3.502302  158.132.9.32           158.132.8.3    DNS        78 Standard query 0x80de A analytics.ietf.org
 5403 3.502590  158.132.9.32           158.132.8.3    DNS        78 Standard query 0xb64e HTTPS analytics.ietf.org

> Frame 661: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits) on interface \Device\NPF_{70BEECD2-B44F-4C62-BFD5-B3EE4E939E40}, id 0
> Ethernet II, Src: VMware_90:40:4d (00:50:56:90:40:4d), Dst: Micro-St_c3:06:d3 (30:9c:23:c3:06:d3)
> Internet Protocol Version 4
> User Datagram Protocol,
v Domain Name System (respons
    Transaction ID: 0x1c9a
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 2
    Additional RRs: 6
  > Queries
  > Answers

0000  30 9c 23 c3 06 d3 00 50  56 90 40 4d 08 00 45 00   0·#····P V·@M··E·
0010  01 14 90 33 00 00 40 11  9b 7a 9e 84 08 03 9e 84   ···3··@· ·z······
0020  09 20 00 35 d7 21 01 00  db 7e 1c 9a 81 80 00 01   · ·5·!·· ·~······
0030  00 02 00 02 00 06 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf·

wireshark_Ethernet8QUEK2.pcapng   Packets: 9905 · Displayed: 9905 (100.0%) · Dropped: 0 (0.0%)   Profile: Default
```

the DNS response is sent over UDP

Problem 4 trace file: the DNS response



```
ip.addr == 158.132.9.53

No.    Time       Source         Destination    Protocol Length Info
69817 18.218278   158.132.8.3    158.132.9.53   DNS       463 Standard query response 0xcf2e HTTPS www.ietf.org HTTPS NS jill.ns.cloudflare.com NS ken.ns.cloudflare.com A …
69818 18.218332   158.132.8.3    158.132.9.53   DNS       422 Standard query response 0x1cd0 A www.ietf.org A 104.16.44.99 A 104.16.45.99 NS ken.ns.cloudflare.com NS jill.…
69819 18.218332   158.132.8.3    158.132.9.53   DNS       422 Standard query response 0x3cf7 A www.ietf.org A 104.16.44.99 A 104.16.45.99 NS jill.ns.cloudflare.com NS ken.…
69871 18.277765   158.132.9.53   158.132.8.3    DNS        75 Standard query 0x0a1a A static.ietf.org
69879 18.278119   158.132.9.53   158.132.8.3    DNS        75 Standard query 0x0ebc HTTPS static.ietf.org
69938 18.283792   158.132.8.3    158.132.9.53   DNS       466 Standard query response 0x0ebc HTTPS static.ietf.org HTTPS NS jill.ns.cloudflare.com NS ken.ns.cloudflare.com…

> Frame 69819: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface \Device\NPF_{70BEECD2-B44F-4C62-BFD5-B3EE4E939E40}, id 0
> Ethernet II, Src: VMware_90:40:4d (00:50:56:90:40:4d), Dst: Micro-St_c3:07:3b (30:9c:23:c3:07:3b)
> Internet Protocol Version 4, Src: 158.132.8.3, Dst: 158.132.9.53
> User Datagram Protocol, Src Port: 53, Dst Port: 53694
v Domain Name System (response)
    Transaction ID: 0x3cf7
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 2
    Additional RRs: 12
  > Queries
  v Answers
    v www.ietf.org: type A, class IN, addr 104.16.44.99
        Name: www.ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 104.16.44.99
    v www.ietf.org: type A, class IN, addr 104.16.45.99
        Name: www.ietf.org
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 104.16.45.99
  v Authoritative nameservers
    v ietf.org: type NS, class IN, ns jill.ns.cloudflare.com
        Name: ietf.org
        Type: NS (authoritative Name Server) (2)

0040  6f 72 67 00 00 01 00 01  c0 0c 00 01 00 01 00 00   org····· ········
0050  01 2c 00 04 68 10 2c 63  c0 0c 00 01 00 01 00 00   ·,··h·,c ········
0060  01 2c 00 04 68 10 2d 63  c0 10 00 02 00 01 00 00   ·,··h·-c ········
0070  0e 10 00 18 04 6a 69 6c  6c 02 6e 73 0a 63 6c 6f   ·····jil l·ns·clo
0080  75 64 66 6c 61 72 65 03  63 6f 6d 00 c0 10 00 02   udflare· com·····
0090  00 01 00 00 0e 10 00 06  03 6b 65 6e c0 4f c0 4a   ········ ·ken·O·J

Response Type (dns.resp.type), 2 bytes   Packets: 86298 · Displayed: 86298 (100.0%) · Dropped: 1114 (1.3%)   Profile: Default
```

the DNS response contains two answers

The contents of the answers

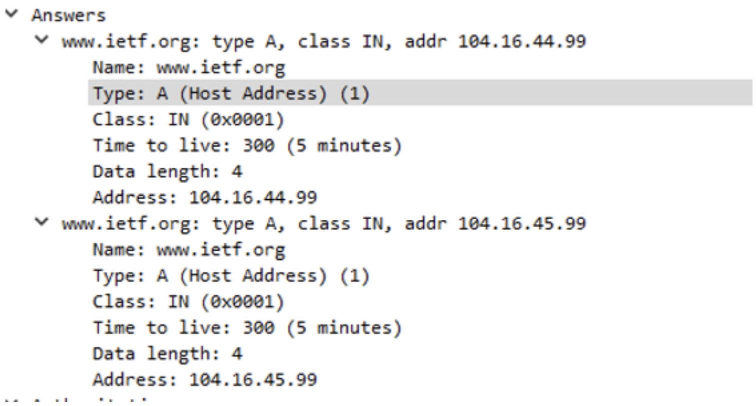
Problem 8 trace file: the DNS response

Problem 4 solution

They are all sent over UDP.

Problem 8 solution

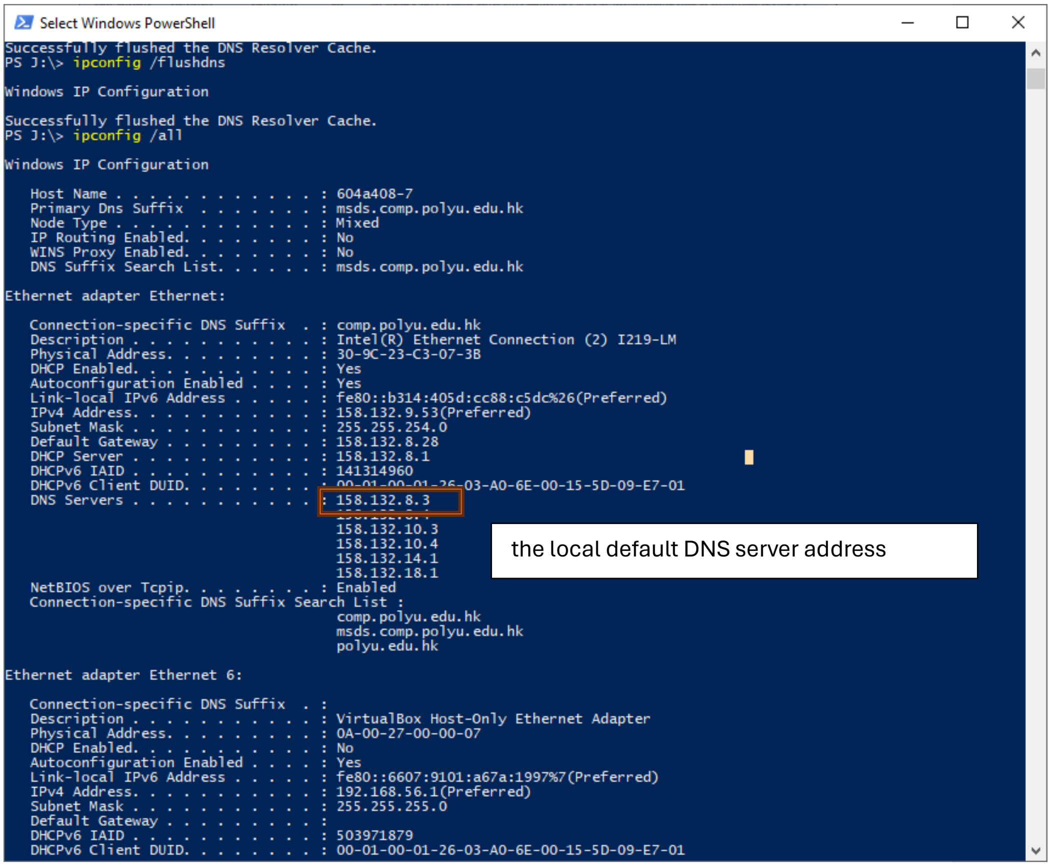
There were 2 answers containing information about the name of the host, the type of address, class, the Time to live, the data length and the IP address.



```
∨ Answers
  ∨ www.ietf.org: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org
      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: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.45.99
```

Problem 8 trace file: the DNS response's answers

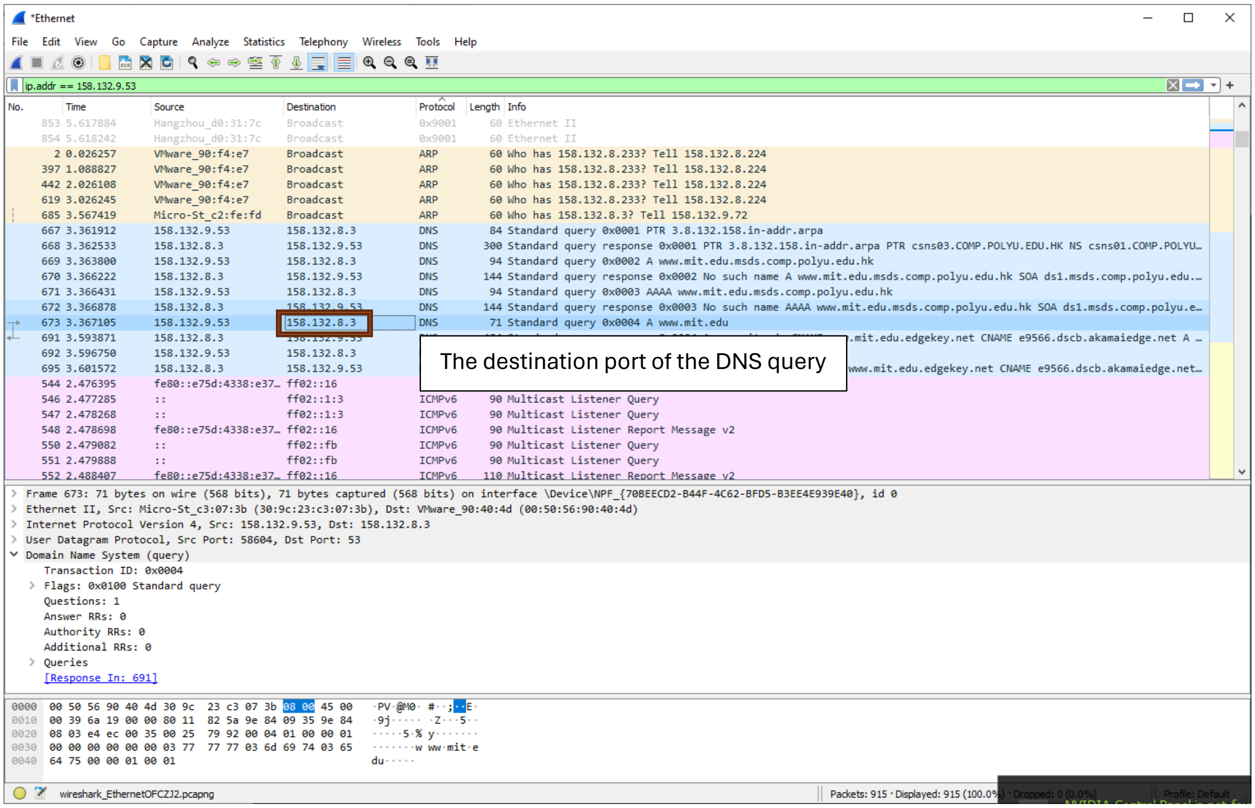
Part 3b:



```
Successfully flushed the DNS Resolver Cache.
PS J:\> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
PS J:\> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : 604a408-7
   Primary Dns Suffix  . . . . . . . : msds.comp.polyu.edu.hk
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : msds.comp.polyu.edu.hk

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : comp.polyu.edu.hk
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (2) I219-LM
   Physical Address. . . . . . . . . : 30-9C-23-C3-07-3B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b314:405d:cc88:c5dc%26(Preferred)
   IPv4 Address. . . . . . . . . . . : 158.132.9.53(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 158.132.8.28
   DHCP Server . . . . . . . . . . . : 158.132.8.1
   DHCPv6 IAID . . . . . . . . . . . : 141314960
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-03-A0-6E-00-15-5D-09-E7-01
   DNS Servers . . . . . . . . . . . : 158.132.8.3
                                       158.132.8.4
                                       158.132.10.3
                                       158.132.10.4
                                       158.132.14.1
                                       158.132.18.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       comp.polyu.edu.hk
                                       msds.comp.polyu.edu.hk
                                       polyu.edu.hk

Ethernet adapter Ethernet 6:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-07
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6607:9101:a67a:1997%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 503971879
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-03-A0-6E-00-15-5D-09-E7-01
```

the local default DNS server address

Problem 12 trace file: the local default DNS address by ipconfig command


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 158.132.9.53

```
No.   Time      Source                Destination    Protocol Length Info
  853 5.617884  Hangzhou_d0:31:7c     Broadcast      0x9001    60 Ethernet II
  854 5.618242  Hangzhou_d0:31:7c     Broadcast      0x9001    60 Ethernet II
    2 0.026257  VMware_90:f4:e7       Broadcast      ARP       60 Who has 158.132.8.233? Tell 158.132.8.224
  397 1.088827  VMware_90:f4:e7       Broadcast      ARP       60 Who has 158.132.8.233? Tell 158.132.8.224
  442 2.026108  VMware_90:f4:e7       Broadcast      ARP       60 Who has 158.132.8.233? Tell 158.132.8.224
  619 3.026245  VMware_90:f4:e7       Broadcast      ARP       60 Who has 158.132.8.233? Tell 158.132.8.224
  685 3.567419  Micro-St_c2:fe:fd     Broadcast      ARP       60 Who has 158.132.8.3? Tell 158.132.9.72
  667 3.361912  158.132.9.53          158.132.8.3    DNS       84 Standard query 0x0001 PTR 3.8.132.158.in-addr.arpa
  668 3.362533  158.132.8.3           158.132.9.53   DNS      300 Standard query response 0x0001 PTR 3.8.132.158.in-addr.arpa PTR csns03.COMP.POLYU.EDU.HK NS csns01.COMP.POLYU…
  669 3.363800  158.132.9.53          158.132.8.3    DNS       94 Standard query 0x0002 A www.mit.edu.msds.comp.polyu.edu.hk
  670 3.366222  158.132.8.3           158.132.9.53   DNS      144 Standard query response 0x0002 No such name A www.mit.edu.msds.comp.polyu.edu.hk SOA ds1.msds.comp.polyu.edu.…
  671 3.366431  158.132.9.53          158.132.8.3    DNS       94 Standard query 0x0003 AAAA www.mit.edu.msds.comp.polyu.edu.hk
  672 3.366878  158.132.8.3           158.132.9.53   DNS      144 Standard query response 0x0003 No such name AAAA www.mit.edu.msds.comp.polyu.edu.hk SOA ds1.msds.comp.polyu.e…
  673 3.367105  158.132.9.53          158.132.8.3    DNS       71 Standard query 0x0004 A www.mit.edu
  691 3.593871  158.132.8.3                                       .mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A …
  692 3.596750  158.132.9.53          158.132.8.3
  695 3.601572  158.132.8.3           158.132.9.53                www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net…
  544 2.476395  fe80::e75d:4338:e37…  ff02::16
  546 2.477285  ::                    ff02::1:3      ICMPv6    90 Multicast Listener Query
  547 2.478268  ::                    ff02::1:3      ICMPv6    90 Multicast Listener Query
  548 2.478698  fe80::e75d:4338:e37…  ff02::16       ICMPv6    90 Multicast Listener Report Message v2
  550 2.479082  ::                    ff02::fb       ICMPv6    90 Multicast Listener Query
  551 2.479888  ::                    ff02::fb       ICMPv6    90 Multicast Listener Query
  552 2.488407  fe80::e75d:4338:e37…  ff02::16       ICMPv6   110 Multicast Listener Report Message v2
```

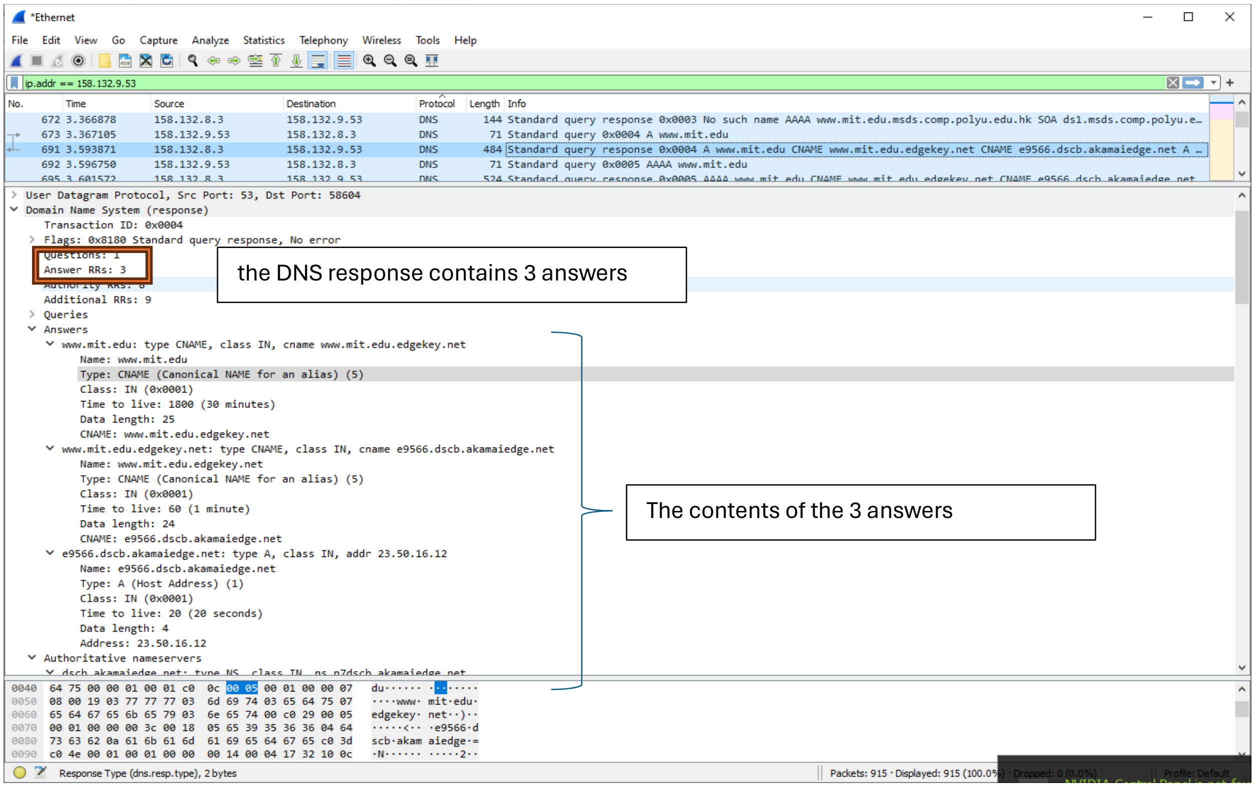
```
> Frame 673: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{70BEECD2-B44F-4C62-BFD5-B3EE4E939E40}, id 0
> Ethernet II, Src: Micro-St_c3:07:3b (30:9c:23:c3:07:3b), Dst: VMware_90:40:4d (00:50:56:90:40:4d)
> Internet Protocol Version 4, Src: 158.132.9.53, Dst: 158.132.8.3
> User Datagram Protocol, Src Port: 58604, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 691]
```

```
0000  00 50 56 90 40 4d 30 9c  23 c3 07 3b 08 00 45 00   ·PV·@M0· #··;··E·
0010  00 39 6a 19 00 00 80 11  82 5a 9e 84 09 35 9e 84   ·9j····· ·Z···5··
0020  08 03 e4 ec 00 35 00 25  79 92 00 04 01 00 00 01   ·····5·% y·······
0030  00 00 00 00 00 00 03 77  77 77 03 6d 69 74 03 65   ·······w ww·mit·e
0040  64 75 00 00 01 00 01                               du·····
```

wireshark_EthernetOFCZJ2.pcapng   Packets: 915 · Displayed: 915 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

The destination port of the DNS query

Problem 12 trace file: DNS query


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 158.132.9.53

```
No.   Time      Source         Destination    Protocol Length Info
  672 3.366878  158.132.8.3    158.132.9.53   DNS      144 Standard query response 0x0003 No such name AAAA www.mit.edu.msds.comp.polyu.edu.hk SOA ds1.msds.comp.polyu.e…
  673 3.367105  158.132.9.53   158.132.8.3    DNS       71 Standard query 0x0004 A www.mit.edu
  691 3.593871  158.132.8.3    158.132.9.53   DNS      484 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A …
  692 3.596750  158.132.9.53   158.132.8.3    DNS       71 Standard query 0x0005 AAAA www.mit.edu
  695 3.601572  158.132.8.3    158.132.9.53   DNS      524 Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net
```

```
> User Datagram Protocol, Src Port: 53, Dst Port: 58604
v Domain Name System (response)
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 8
    Additional RRs: 9
  > Queries
  v Answers
    v 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
    v 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
    v e9566.dscb.akamaiedge.net: type A, class IN, addr 23.50.16.12
        Name: e9566.dscb.akamaiedge.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 4
        Address: 23.50.16.12
  v Authoritative nameservers
    v dscb.akamaiedge.net: type NS, class IN, ns n7dscb.akamaiedge.net
```

```
0040  64 75 00 00 01 00 01 c0  0c 00 05 00 01 00 00 07   du······ ········
0050  08 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 00 3c 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 01 00 01 00 00  00 14 00 04 17 32 10 0c   ·N······ ·····2··
```

Response Type (dns.resp.type), 2 bytes   Packets: 915 · Displayed: 915 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

the DNS response contains 3 answers

The contents of the 3 answers

Problem 14 trace file: the contents of the DNS answers

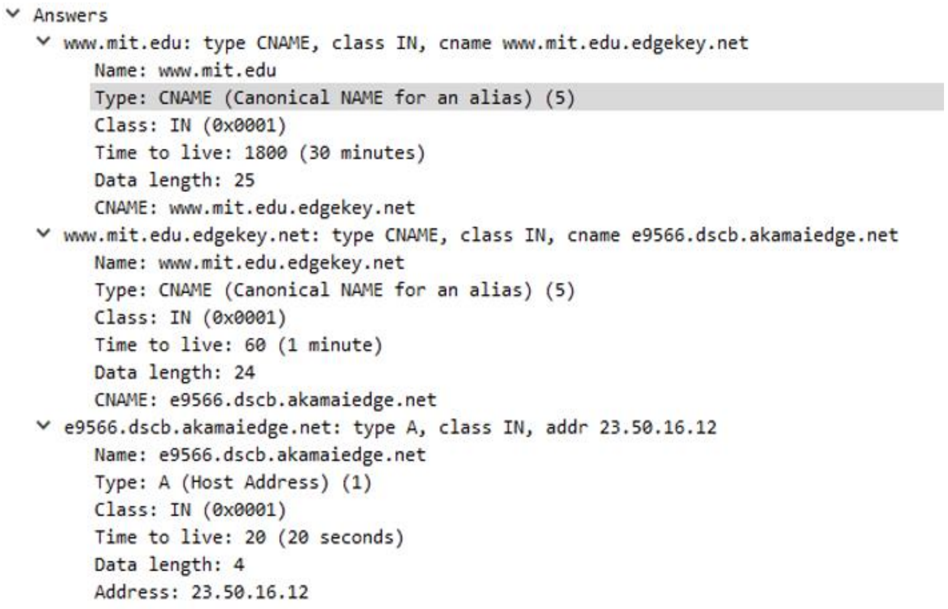
Problem 12 solution

The DNS query is sent to 158.132.8.3;

And the default local DNS server's address could be obtained by the ipconfig /all command, which is also 158.132.8.3. So they are of the same.

Problem 14 solution

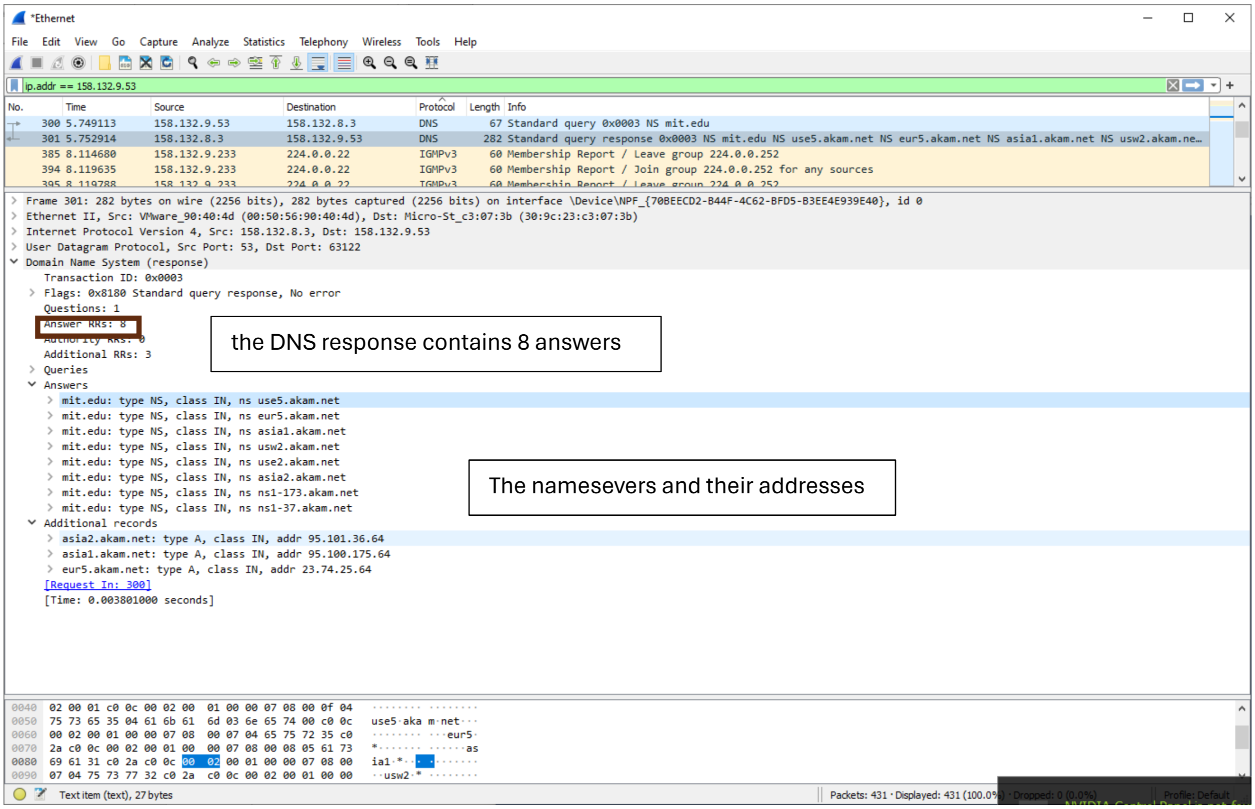
The response DNS message contains one answer containing the name of the host, the type of address, the class, and the IP address.



```
v Answers
  v 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
  v 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
  v e9566.dscb.akamaiedge.net: type A, class IN, addr 23.50.16.12
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 4
      Address: 23.50.16.12
```

Problem 14 trace file: the contents of the DNS answers

Part 3c:


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 158.132.9.53

No.  Time       Source          Destination   Protocol Length Info
 300 5.749113   158.132.9.53    158.132.8.3   DNS       67 Standard query 0x0003 NS mit.edu
 301 5.752914   158.132.8.3     158.132.9.53  DNS      282 Standard query response 0x0003 NS mit.edu NS use5.akam.net NS eur5.akam.net NS asia1.akam.net NS usw2.akam.ne…
 385 8.114680   158.132.9.233   224.0.0.22    IGMPv3    60 Membership Report / Leave group 224.0.0.252
 394 8.119635   158.132.9.233   224.0.0.22    IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
 395 8.119788   158.132.9.233   224.0.0.22    IGMPv3    60 Membership Report / Leave group 224.0.0.252

> Frame 301: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface \Device\NPF_{70BEECD2-B44F-4C62-BFD5-B3EE4E939E40}, id 0
> Ethernet II, Src: VMware_90:40:4d (00:50:56:90:40:4d), Dst: Micro-St_c3:07:3b (30:9c:23:c3:07:3b)
> Internet Protocol Version 4, Src: 158.132.8.3, Dst: 158.132.9.53
> User Datagram Protocol, Src Port: 53, Dst Port: 63122
v Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 3
  > Queries
  v Answers
    > 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 asia1.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 asia2.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
  v Additional records
    > asia2.akam.net: type A, class IN, addr 95.101.36.64
    > asia1.akam.net: type A, class IN, addr 95.100.175.64
    > eur5.akam.net: type A, class IN, addr 23.74.25.64
    [Request In: 300]
    [Time: 0.003801000 seconds]

0040  02 00 01 c0 0c 00 02 00  01 00 00 07 08 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 07 08  00 07 04 65 75 72 35 c0   ········ ···eur5·
0070  2a c0 0c 00 02 00 01 00  00 07 08 00 08 05 61 73   *······· ······as
0080  69 61 31 c0 2a c0 0c 00  02 00 01 00 00 07 08 00   ia1·*··· ········
0090  07 04 75 73 77 32 c0 2a  c0 0c 00 02 00 01 00 00   ··usw2·* ········

Text item (text), 27 bytes    Packets: 431 · Displayed: 431 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

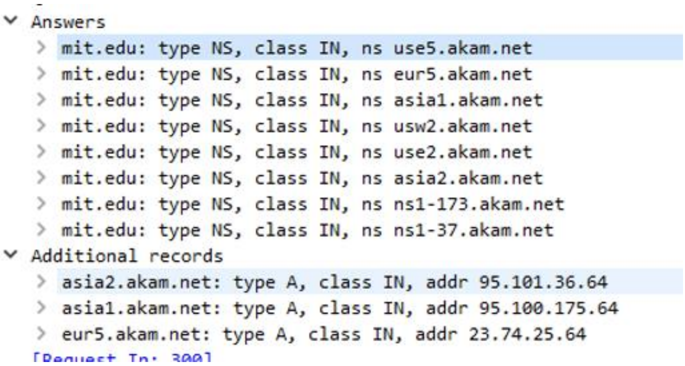
the DNS response contains 8 answers

The namesevers and their addresses

Problem 18 trace file: the answers of the DNS response

Problem 18 solution

The nameservers are use5, eur5, asia1, usw2, asia2, ns1-173, ns1-37. We can find their IP addresses if we in the Additional records field.



```
v Answers
  > 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 asia1.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 asia2.akam.net
  > mit.edu: type NS, class IN, ns ns1-173.akam.net
  > mit.edu: type NS, class IN, ns ns1-37.akam.net
v Additional records
  > asia2.akam.net: type A, class IN, addr 95.101.36.64
  > asia1.akam.net: type A, class IN, addr 95.100.175.64
  > eur5.akam.net: type A, class IN, addr 23.74.25.64
  [Request In: 300]
```

Problem 18 trace file: the answers of the DNS response