Internet Technology
Recitation Section 03

Negin Dehghanchaleshtori

Computer Science Department

Spring 2022

Internet Access

- IP Address
    192.168.1.100

- Netmask
    255.255.255.0

- Gateway to reach the router
    192.168.1.1

- DNS1
    8.8.8.8

- DNS2 (Backup)
    8.8.4.4

DNS (Domain Name System)

Translate hostnames to IP address
Reason → a lot more easier

Google.com
Amazon.com

142.251.32.46

DNS Client

- Runs in Background

- http, ftp, telnet, smtp

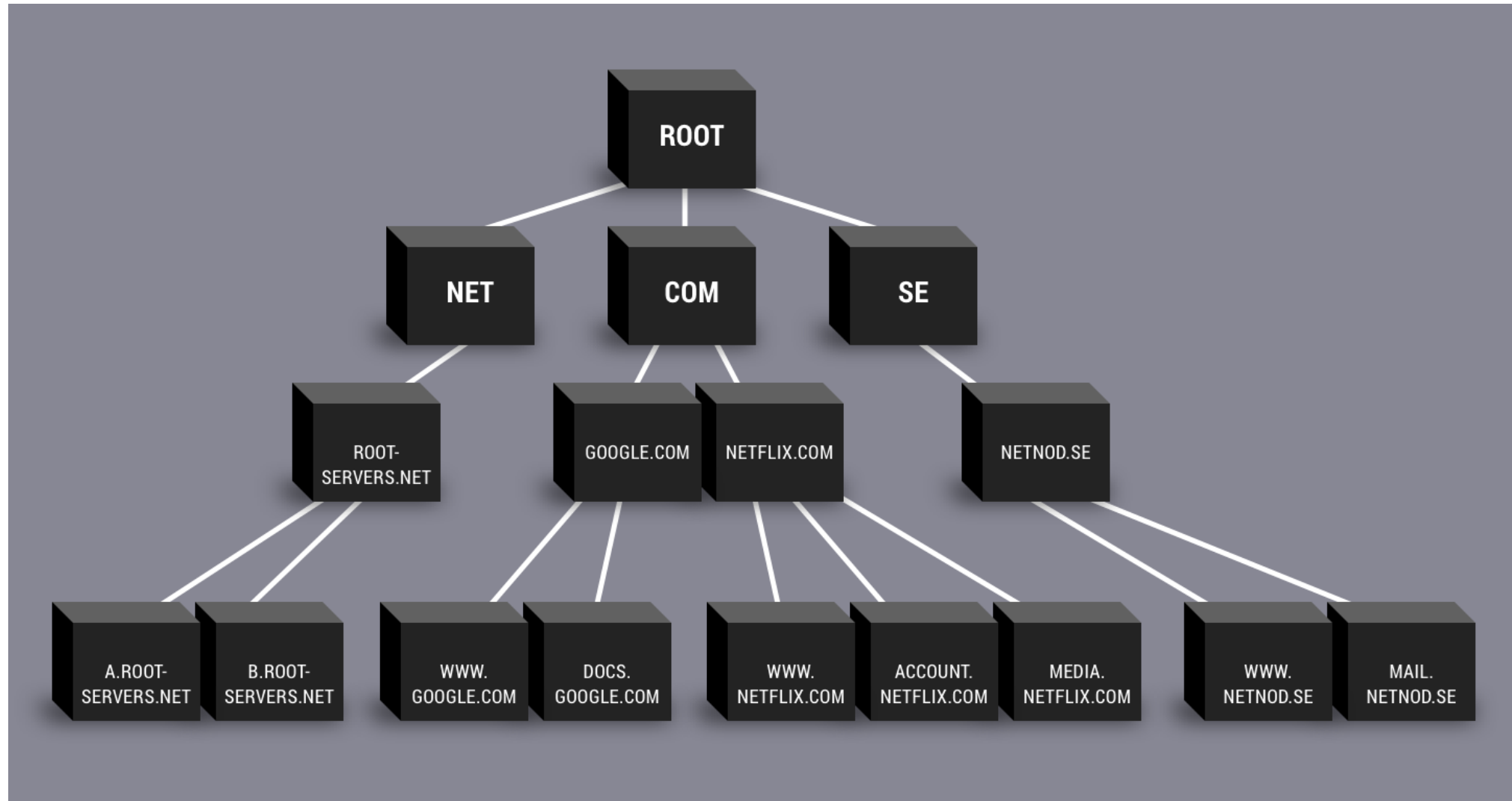   http protocol request the client go and get resolution

- Application layer protocol

- UDP port 53 for transport

Hierarchy of DNS Servers

Use distributed database

Distribute the load

Hierarchy of DNS Servers

DNS Concepts

- The namespace needs to be made hierarchical to be able to scale.

  The idea is to name objects based on location (within country, set of organizations, set of companies, etc)

  unit within that location (company within set of company, etc)

  object within unit (name of person in company)

DNS Queries

- Address
  Need the IP address

  hostname= google.com
  Ip address= 216.58.217.36

- Canonical name (actual name of the host)
  Need the actual hostname

  alias= www.google.com
  Canonical name= google.com

DNS Queries

- Mailserver
  You need the IP address of the mail server

  hostname= google.com
  Canonical name= aspmx.l.google.com

- Nameserver
  You need the IP address of the name server

  hostname= google.com
  Canonical name= ns1.google.com

DNS record

(name, value, type, TTL)

- Type
  A
  CNAME (canonical name)
  MX (mail server)
  NS (name server)
  AAAA (IPv6 address of a host)

  PTR (reverse lookup)
      hostname of an IP address

DNS Name Resolution

DNS server created a hierarchical namespace

- Root (.)
- Top Level Domain (.edu, .gov, .ca)
- Second Level Domain (pbcc, google, military)
- Local DNS Server (ISP, no zone, caching)
- Local DNS Forwarder (local network, no zone, just forward request)

Top Level Domain Server

- Any changes to the DNS domain must made here

- Read/Write copy of DNS Database

Second Level Domain Server

- Server as backup for TLD servers

- Used for load balancing

- Read only copy of DNS Database

Local DNS Server

- Cache name resolution queries

- Network traffic significantly reduced

DNS Client request → Local DNS Server (forwarder)

→ ISP DNS Server (Resolver)

→ Root DNS Server

←

→ TLD DNS Server

←

→ SLD DNS Server

ISP DNS Server ←

Local DNS Server ←

DNS Client Reply ←
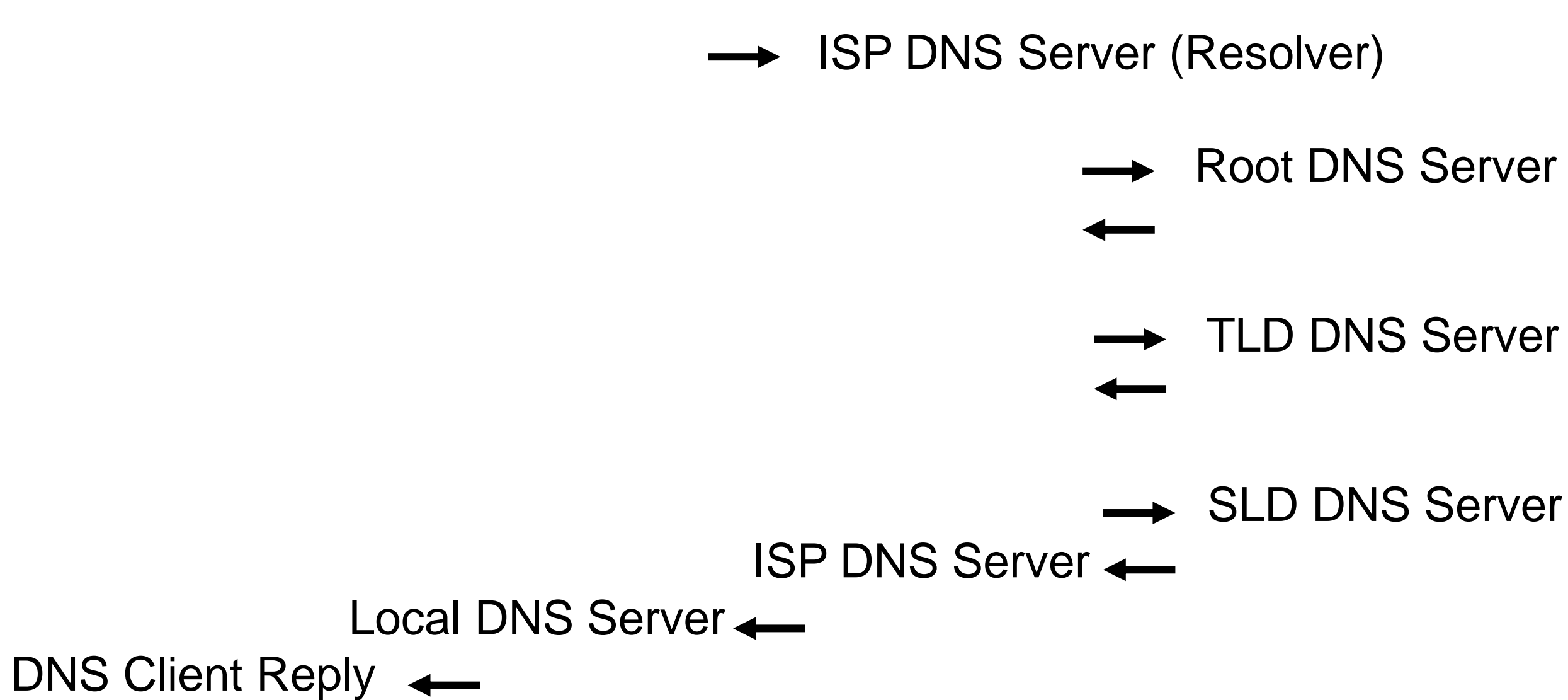
Accessing Web Page

Type www.google.com

What will happen?

Accessing Web Page

Your PC sends a resolution request to its configured DNS Server, typically at your ISP.

Your PC

ISP "Recursive" DNS server
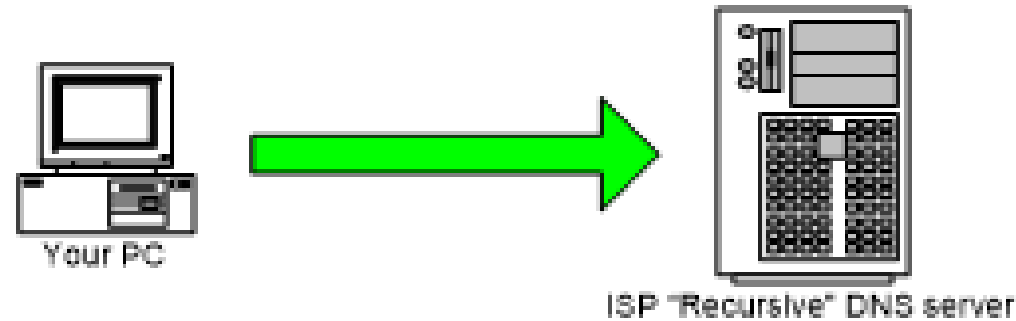
Tell me the Address of
"www.google.com"

Accessing Web Page

Your ISPs recursive name server starts by asking one of the root servers predefined in its "hints" file.

Tell me the Address of "www.google.com"

ISP "Recursive" DNS server

Root Servers
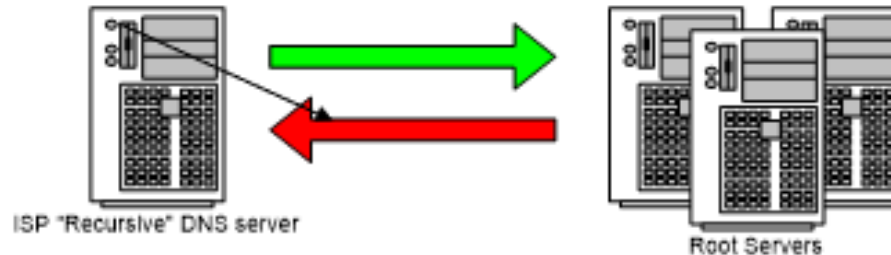
I don't know the address but I know who's authoritative for the "com" domain ask them

Accessing Web Page

Your ISPs recursive name server then asks one of the "com" name servers as directed.

Tell me the Address of "www.google.com"

ISP "Recursive" DNS server

"com" DNS servers
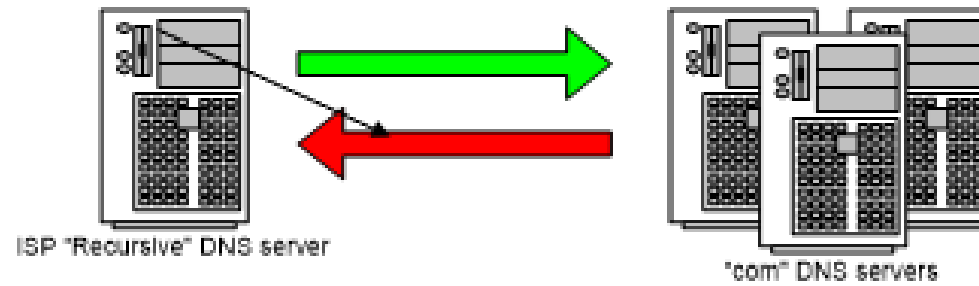
I don't know the address but I know who's authoritative for the "google.com" domain ask them

Accessing Web Page

Your ISPs recursive name server then asks one of the "google.com" name servers as directed

Tell me the Address of "www.google.com"

ISP "Recursive" DNS server

google.com DNS server
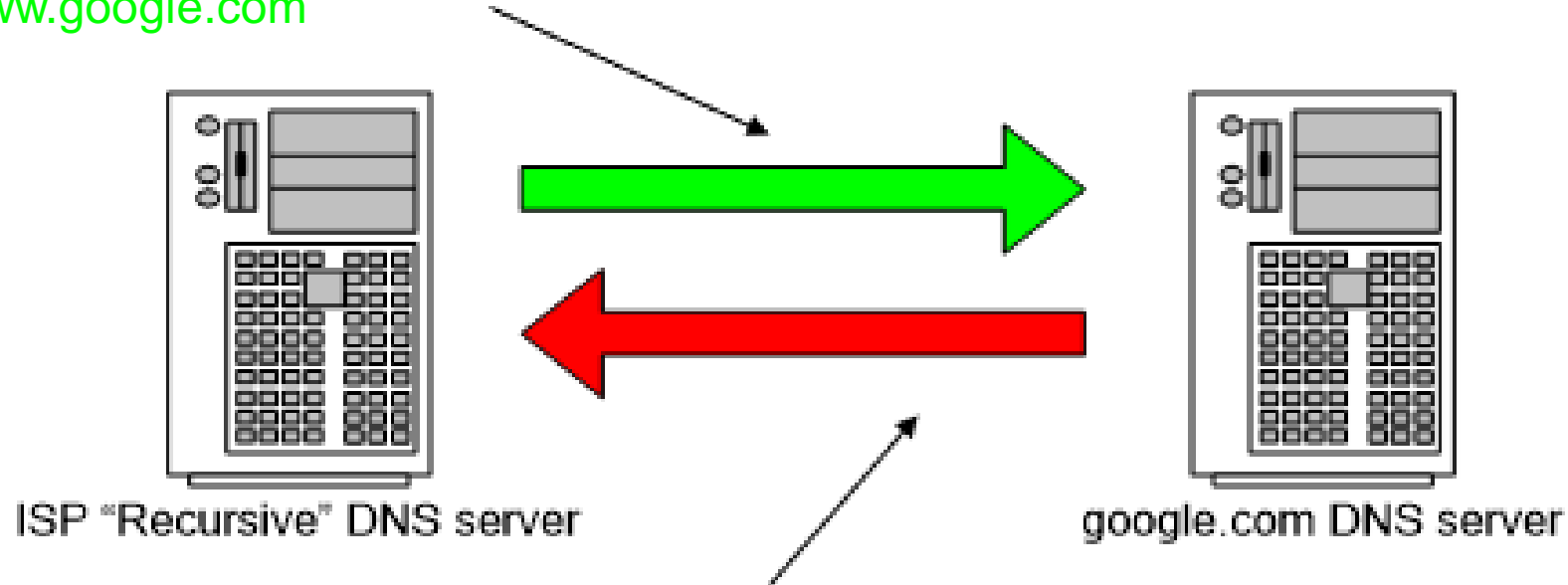
The Address of www.google.com is 216.239.53.99

Accessing Web Page

ISP DNS server then send the answer back to your PC.
The DNS server will "remember" the answer for a period of time

Your PC

ISP "Recursive" DNS server
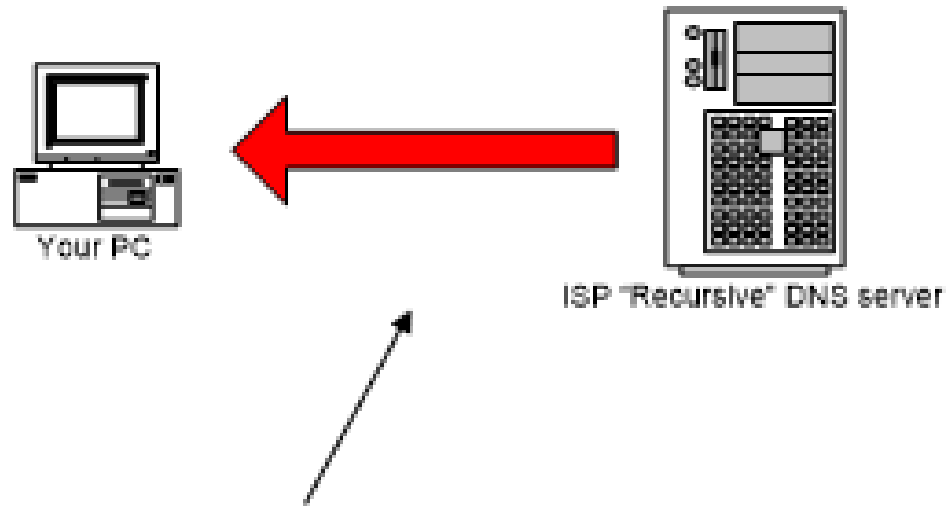
The Address of www.google.com is
216.239.53.99

Accessing Web Page

Your PC can then make the actual HTTP request to the web server
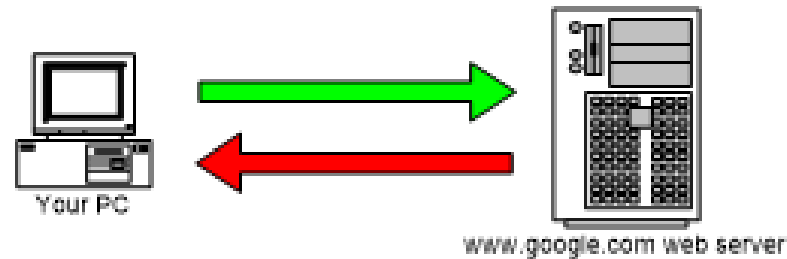
Summary
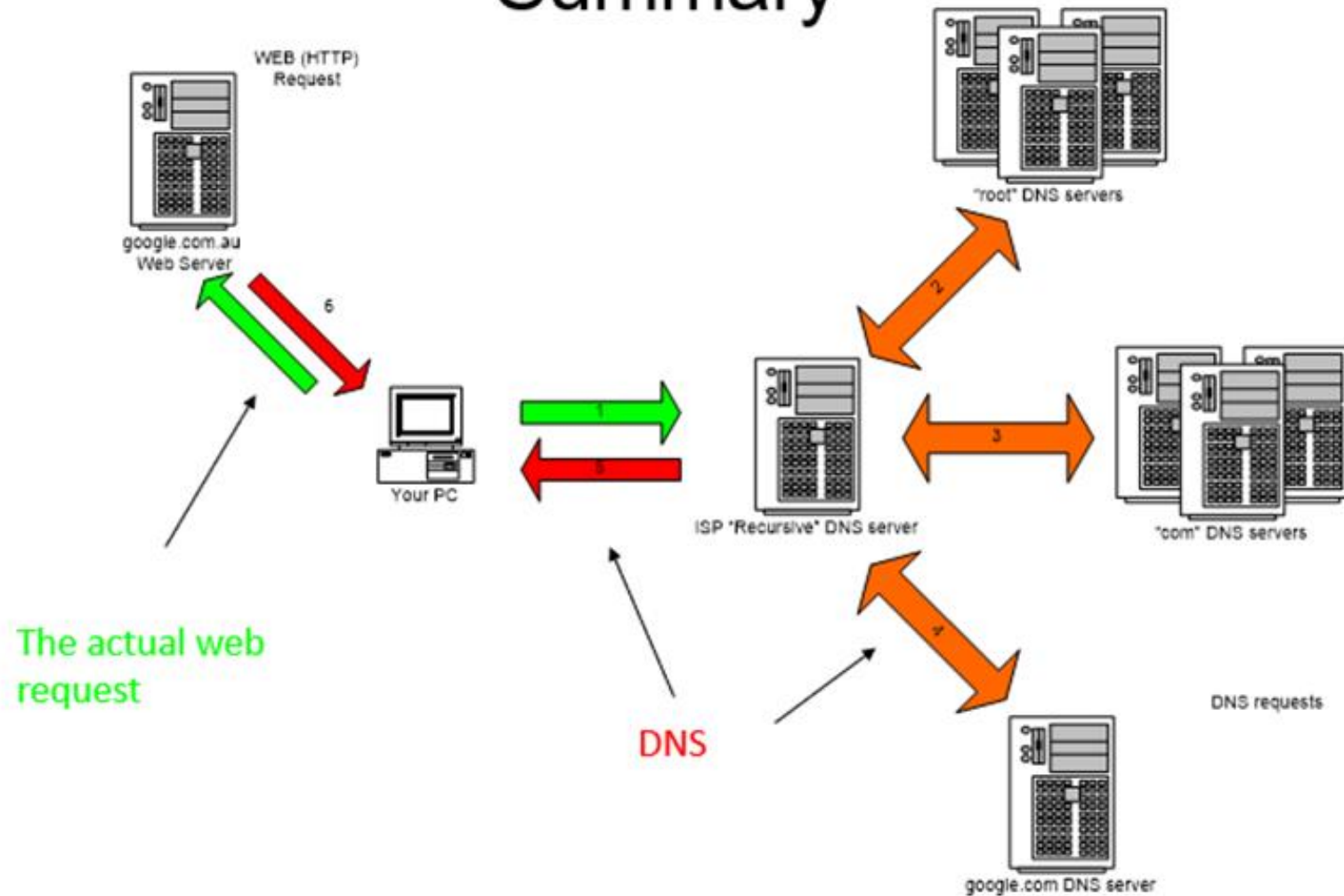
Sending Email

- DNS is not just used in HTTP protocol (web pages)

- DNS is involved in almost every protocol in use on the internet.

How DNS facilitates the transfer of electronic mail

Your PC sends the e-mail to its configured outbound mail server.
A DNS request similar to the previous example is required to find the address of the mail server.

Your PC

Outbound Mail (SMTP) Server
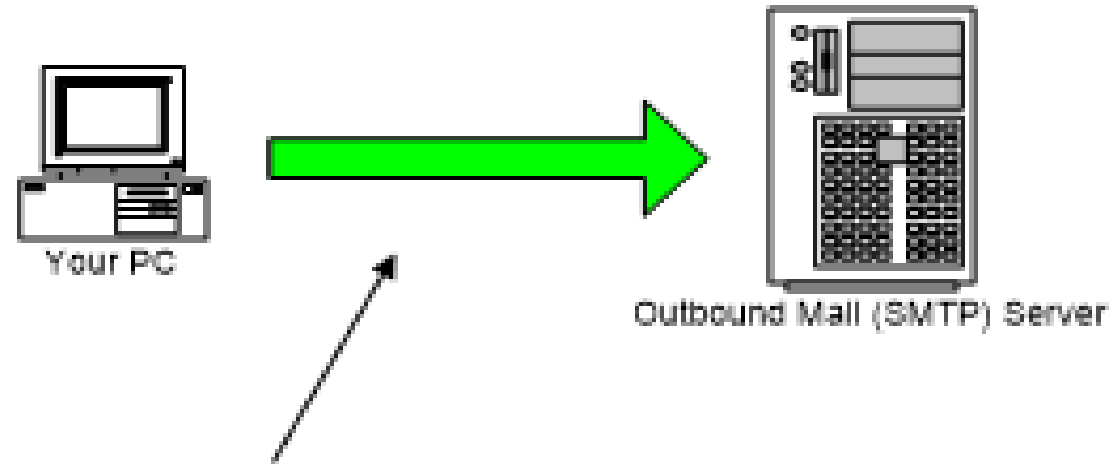
Please send this message to
"someone@example.com"

How DNS facilitates the transfer of electronic mail

Your mail server follows the same intensive process to find the authoritative servers for "example.com".

Tell me the name servers for "example.com"

Outbound Mail server

DNS servers
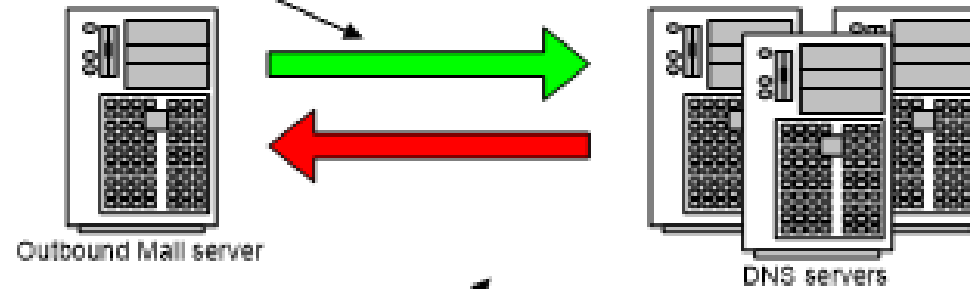
Here are the name servers for "example.com"

How DNS facilitates the transfer of electronic mail

Ask the "example.com" name server for the list of "Mail eXchangers (MX) for that domain.

Tell me the MX's for "example.com"

Outbound Mail Server

example.com DNS server
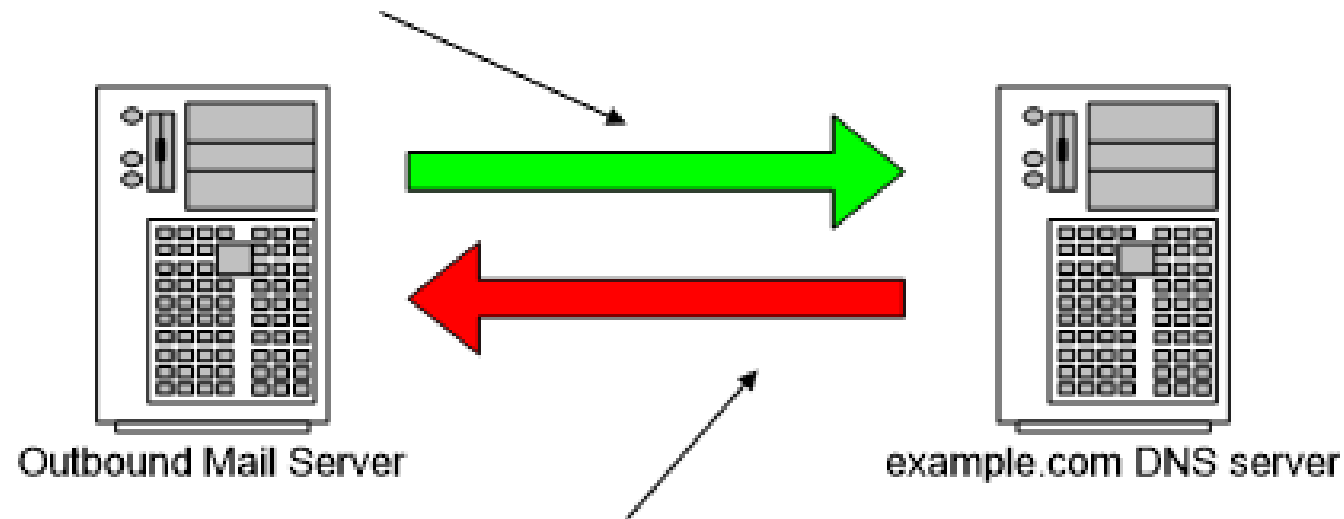
The MXs are mx10.example.com and mx20.backmail.com

How DNS facilitates the transfer of electronic mail

Select a Mail server and deliver the mail.

Here is some mail for the "example.com" domain

Outbound Mail Server

example.com Mail server
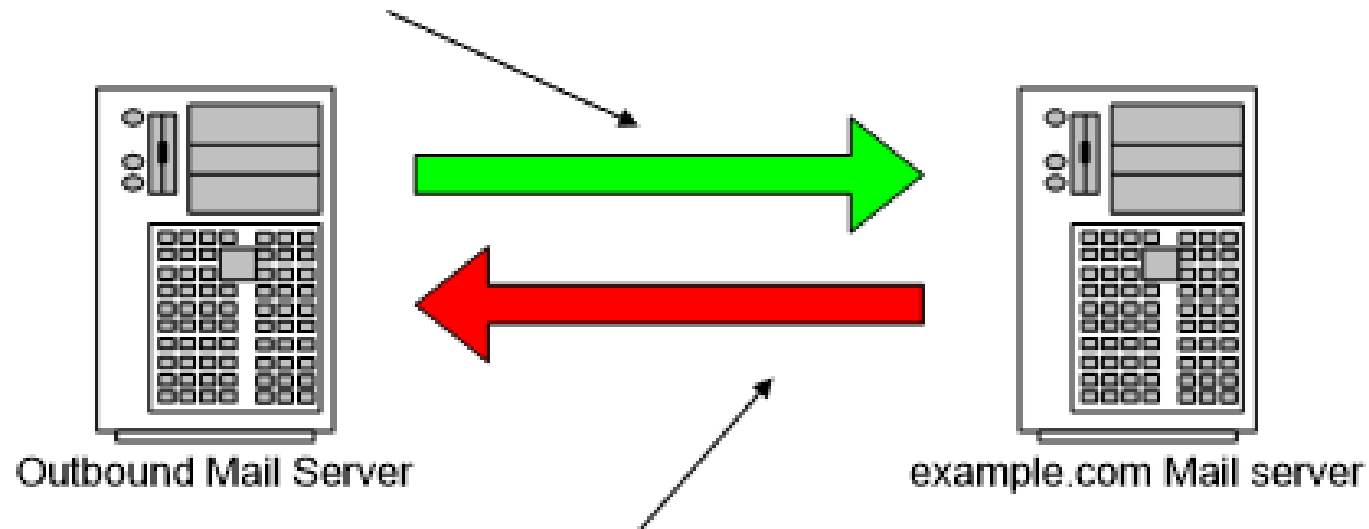
Mail accepted for delivery

DNS Features

Scalability

- No limit to the size of the database
  One server has over 20,000,000 names

- No limit to the number of queries
  24,000 queries per second handled easily

- Queries distributed among masters, slaves, and caches

DNS Features

Reliability

- Data is replicated
  Data from master is copied to multiple slaves

- Clients can query

- Clients will typically query local caches

- DNS protocols can use either UDP or TCP
  If UDP, DNS protocol handles retransmission, sequencing, etc.

DNS Features

Dynamicity

- Database can be updated dynamically
  Add/delete/modify of any record

- Modification of the master database triggers replication
  Only master can be dynamically updated

DNS Protocol

DNS protocol : query and reply messages, both with same message format.

- msg header:
    identification: 16 bit #
    for query, reply to query uses same #

•flags:

    query or reply
    recursion desired
    recursion available
    reply is authoritative

DNS Protocol

identification	flags
number of questions	number of answer RRs
number of authority RRs	number of additional RRs

12 bytes

questions (variable number of questions)
answers (variable number of resource records)
authority (variable number of resource records)
additional information (variable number of resource records)

dns

No.	Time	Source	Destination	Protocol	Length	Info
7	2.400440	192.168.142.203	192.168.142.13	DNS	89	Standard query 0xb44c A pagead2.googlesyndication.com
9	2.452837	192.168.142.13	192.168.142.203	DNS	105	Standard query response 0xb44c A pagead2.googlesyndication.com A 142.250.65.194
54	3.479244	192.168.142.203	192.168.142.13	DNS	74	Standard query 0x0202 A px.moatads.com
55	3.534418	192.168.142.13	192.168.142.203	DNS	170	Standard query response 0x0202 A px.moatads.com CNAME wildcard.moatads.com.edgekey.net
168	4.701024	192.168.142.203	192.168.142.13	DNS	77	Standard query 0x311f A fonts.gstatic.com
171	4.752818	192.168.142.13	192.168.142.203	DNS	129	Standard query response 0x311f A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 1
1026	8.892912	192.168.142.203	192.168.142.13	DNS	87	Standard query 0x9d5e A 3.client-channel.google.com
1097	8.985403	192.168.142.13	192.168.142.203	DNS	103	Standard query response 0x9d5e A 3.client-channel.google.com A 74.125.142.189
2312	25.335254	192.168.142.203	192.168.142.13	DNS	70	Standard query 0xb4bf A google.com
2314	25.394215	192.168.142.13	192.168.142.203	DNS	86	Standard query response 0xb4bf A google.com A 142.251.32.46
2323	25.429952	192.168.142.203	192.168.142.13	DNS	91	Standard query 0x6865 A signaler-pa.clients6.google.com
2324	25.466261	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0x6865 A signaler-pa.clients6.google.com A 142.251.46.170
3146	26.899337	192.168.142.203	192.168.142.13	DNS	91	Standard query 0xb47f A content-autofill.googleapis.com
3157	26.969205	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0xb47f A content-autofill.googleapis.com A 142.251.46.170
3291	27.231413	192.168.142.203	192.168.142.13	DNS	80	Standard query 0x74be A adservice.google.com

> Frame 2312: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{1F09A365-29BF-49E4-A85B-917644423F59}, id 0
> Ethernet II, Src: IntelCor_8d:4e:01 (20:16:b9:8d:4e:01), Dst: 42:4e:bd:f7:0e:77 (42:4e:bd:f7:0e:77)
> Internet Protocol Version 4, Src: 192.168.142.203, Dst: 192.168.142.13
> User Datagram Protocol, Src Port: 65218, Dst Port: 53
> Domain Name System (query)

```
0000   42 4e bd f7 0e 77 20 16   b9 8d 4e 01 08 00 45 00   BN···w· ··N···E·
0010   00 38 37 38 00 00 80 11   00 00 c0 a8 8e cb c0 a8   ·878···· ········
0020   8e 0d fe c2 00 35 00 24   9e 5f b4 bf 01 00 00 01   ·····5·$ ·_······
0030   00 00 00 00 00 00 06 67   6f 6f 67 6c 65 03 63 6f   ·······g oogle·co
0040   6d 00 00 01 00 01                                   m·····
```

Domain Name System (dns), 28 bytes   Packets: 3442 · Displayed: 16 (0.5%) · Dropped: 0 (0.0%)   Profile: Default

File　Edit　View　Go　Capture　Analyze　Statistics　Telephony　Wireless　Tools　Help

`dns`

No.	Time	Source	Destination	Protocol	Length	Info
7	2.400440	192.168.142.203	192.168.142.13	DNS	89	Standard query 0xb44c A pagead2.googlesyndication.com
9	2.452837	192.168.142.13	192.168.142.203	DNS	105	Standard query response 0xb44c A pagead2.googlesyndication.com A 142.250.65.194
54	3.479244	192.168.142.203	192.168.142.13	DNS	74	Standard query 0x0202 A px.moatads.com
55	3.534418	192.168.142.13	192.168.142.203	DNS	170	Standard query response 0x0202 A px.moatads.com CNAME wildcard.moatads.com.edgekey.net
168	4.701024	192.168.142.203	192.168.142.13	DNS	77	Standard query 0x311f A fonts.gstatic.com
171	4.752818	192.168.142.13	192.168.142.203	DNS	129	Standard query response 0x311f A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 1
1026	8.892912	192.168.142.203	192.168.142.13	DNS	87	Standard query 0x9d5e A 3.client-channel.google.com
1097	8.985403	192.168.142.13	192.168.142.203	DNS	103	Standard query response 0x9d5e A 3.client-channel.google.com A 74.125.142.189
2312	25.335254	192.168.142.203	192.168.142.13	DNS	70	Standard query 0xb4bf A google.com
2314	25.394215	192.168.142.13	192.168.142.203	DNS	86	Standard query response 0xb4bf A google.com A 142.251.32.46
2323	25.429952	192.168.142.203	192.168.142.13	DNS	91	Standard query 0x6865 A signaler-pa.clients6.google.com
2324	25.466261	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0x6865 A signaler-pa.clients6.google.com A 142.251.46.170
3146	26.899337	192.168.142.203	192.168.142.13	DNS	91	Standard query 0xb47f A content-autofill.googleapis.com
3157	26.969205	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0xb47f A content-autofill.googleapis.com A 142.251.46.170
3291	27.231413	192.168.142.203	192.168.142.13	DNS	80	Standard query 0x74be A adservice.google.com

> Frame 2312: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{1F09A365-29BF-49E4-A85B-917644423F59}, id 0
> Ethernet II, Src: IntelCor_8d:4e:01 (20:16:b9:8d:4e:01), Dst: 42:4e:bd:f7:0e:77 (42:4e:bd:f7:0e:77)
> Internet Protocol Version 4, Src: 192.168.142.203, Dst: 192.168.142.13
> User Datagram Protocol, Src Port: 65218, Dst Port: 53
∨ Domain Name System (query)
　　Transaction ID: 0xb4bf
　> Flags: 0x0100 Standard query
　　Questions: 1
　　Answer RRs: 0
　　Authority RRs: 0
　　Additional RRs: 0
　> Queries
　　[Response In: 2314]

```
0000   42 4e bd f7 0e 77 20 16   b9 8d 4e 01 08 00 45 00   BN···w · ··N···E·
0010   00 38 37 38 00 00 80 11   00 00 c0 a8 8e cb c0 a8   ·878···· ········
0020   8e 0d fe c2 00 35 00 24   9e 5f b4 bf 01 00 00 01   ·····5·$ ·_······
0030   00 00 00 00 00 00 06 67   6f 6f 67 6c 65 03 63 6f   ·······g oogle·co
0040   6d 00 00 01 00 01                                   m·····
```

○ Domain Name System (dns), 28 bytes　　　　　　　　Packets: 3442 · Displayed: 16 (0.5%) · Dropped: 0 (0.0%)　　Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
7	2.400440	192.168.142.203	192.168.142.13	DNS	89	Standard query 0xb44c A pagead2.googlesyndication.com
9	2.452837	192.168.142.13	192.168.142.203	DNS	105	Standard query response 0xb44c A pagead2.googlesyndication.com A 142.250.65.194
54	3.479244	192.168.142.203	192.168.142.13	DNS	74	Standard query 0x0202 A px.moatads.com
55	3.534418	192.168.142.13	192.168.142.203	DNS	170	Standard query response 0x0202 A px.moatads.com CNAME wildcard.moatads.com.edgekey.net
168	4.701024	192.168.142.203	192.168.142.13	DNS	77	Standard query 0x311f A fonts.gstatic.com
171	4.752818	192.168.142.13	192.168.142.203	DNS	129	Standard query response 0x311f A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 1
1026	8.892912	192.168.142.203	192.168.142.13	DNS	87	Standard query 0x9d5e A 3.client-channel.google.com
1097	8.985403	192.168.142.13	192.168.142.203	DNS	103	Standard query response 0x9d5e A 3.client-channel.google.com A 74.125.142.189
2312	25.335254	192.168.142.203	192.168.142.13	DNS	70	Standard query 0xb4bf A google.com
2314	25.394215	192.168.142.13	192.168.142.203	DNS	86	Standard query response 0xb4bf A google.com A 142.251.32.46
2323	25.429952	192.168.142.203	192.168.142.13	DNS	91	Standard query 0x6865 A signaler-pa.clients6.google.com
2324	25.466261	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0x6865 A signaler-pa.clients6.google.com A 142.251.46.170
3146	26.899337	192.168.142.203	192.168.142.13	DNS	91	Standard query 0xb47f A content-autofill.googleapis.com
3157	26.969205	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0xb47f A content-autofill.googleapis.com A 142.251.46.170
3291	27.231413	192.168.142.203	192.168.142.13	DNS	80	Standard query 0x74be A adservice.google.com

> Frame 2312: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{1F09A365-29BF-49E4-A85B-917644423F59}, id 0
> Ethernet II, Src: IntelCor_8d:4e:01 (20:16:b9:8d:4e:01), Dst: 42:4e:bd:f7:0e:77 (42:4e:bd:f7:0e:77)
> Internet Protocol Version 4, Src: 192.168.142.203, Dst: 192.168.142.13
> User Datagram Protocol, Src Port: 65218, Dst Port: 53
∨ Domain Name System (query)
    Transaction ID: 0xb4bf
   > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
   ∨ Queries
     > google.com: type A, class IN
     [Response In: 2314]

```
0000   42 4e bd f7 0e 77 20 16  b9 8d 4e 01 08 00 45 00   BN...w . ..N..E.
0010   00 38 37 38 00 00 80 11  00 00 c0 a8 8e cb c0 a8   .878.... ........
0020   8e 0d fe c2 00 35 00 24  9e 5f b4 bf 01 00 00 01   .....5.$ ._......
0030   00 00 00 00 00 00 06 67  6f 6f 67 6c 65 03 63 6f   .......g oogle.co
0040   6d 00 00 01 00 01                                  m.....
```

Domain Name System (dns), 28 bytes   Packets: 3442 · Displayed: 16 (0.5%) · Dropped: 0 (0.0%)   Profile: Default

dns

No.	Time	Source	Destination	Protocol	Length	Info
7	2.400440	192.168.142.203	192.168.142.13	DNS	89	Standard query 0xb44c A pagead2.googlesyndication.com
9	2.452837	192.168.142.13	192.168.142.203	DNS	105	Standard query response 0xb44c A pagead2.googlesyndication.com A 142.250.65.194
54	3.479244	192.168.142.203	192.168.142.13	DNS	74	Standard query 0x0202 A px.moatads.com
55	3.534418	192.168.142.13	192.168.142.203	DNS	170	Standard query response 0x0202 A px.moatads.com CNAME wildcard.moatads.com.edgekey.net
168	4.701024	192.168.142.203	192.168.142.13	DNS	77	Standard query 0x311f A fonts.gstatic.com
171	4.752818	192.168.142.13	192.168.142.203	DNS	129	Standard query response 0x311f A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 1
1026	8.892912	192.168.142.203	192.168.142.13	DNS	87	Standard query 0x9d5e A 3.client-channel.google.com
1097	8.985403	192.168.142.13	192.168.142.203	DNS	103	Standard query response 0x9d5e A 3.client-channel.google.com A 74.125.142.189
2312	25.335254	192.168.142.203	192.168.142.13	DNS	70	Standard query 0xb4bf A google.com
2314	25.394215	192.168.142.13	192.168.142.203	DNS	86	Standard query response 0xb4bf A google.com A 142.251.32.46
2323	25.429952	192.168.142.203	192.168.142.13	DNS	91	Standard query 0x6865 A signaler-pa.clients6.google.com
2324	25.466261	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0x6865 A signaler-pa.clients6.google.com A 142.251.46.170
3146	26.899337	192.168.142.203	192.168.142.13	DNS	91	Standard query 0xb47f A content-autofill.googleapis.com
3157	26.969205	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0xb47f A content-autofill.googleapis.com A 142.251.46.170
3291	27.231413	192.168.142.203	192.168.142.13	DNS	80	Standard query 0x74be A adservice.google.com

```
> User Datagram Protocol, Src Port: 65218, Dst Port: 53
∨ Domain Name System (query)
      Transaction ID: 0xb4bf
   > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
   ∨ Queries
      ∨ google.com: type A, class IN
            Name: google.com
            [Name Length: 10]
            [Label Count: 2]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
      [Response In: 2314]
```

```
0000   42 4e bd f7 0e 77 20 16   b9 8d 4e 01 08 00 45 00   BN···w · ··N···E·
0010   00 38 37 38 00 00 80 11   00 00 c0 a8 8e cb c0 a8   ·878···· ········
0020   8e 0d fe c2 00 35 00 24   9e 5f b4 bf 01 00 00 01   ·····5·$ ·_······
0030   00 00 00 00 00 00 06 67   6f 6f 67 6c 65 03 63 6f   ·······g oogle·co
0040   6d 00 00 01 00 01                                    m·····
```

Domain Name System: Protocol   Packets: 3442 · Displayed: 16 (0.5%) · Dropped: 0 (0.0%)   Profile: Default

File   Edit   View   Go   Capture   Analyze   Statistics   Telephony   Wireless   Tools   Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
7	2.400440	192.168.142.203	192.168.142.13	DNS	89	Standard query 0xb44c A pagead2.googlesyndication.com
9	2.452837	192.168.142.13	192.168.142.203	DNS	105	Standard query response 0xb44c A pagead2.googlesyndication.com A 142.250.65.194
54	3.479244	192.168.142.203	192.168.142.13	DNS	74	Standard query 0x0202 A px.moatads.com
55	3.534418	192.168.142.13	192.168.142.203	DNS	170	Standard query response 0x0202 A px.moatads.com CNAME wildcard.moatads.com.edgekey.net
168	4.701024	192.168.142.203	192.168.142.13	DNS	77	Standard query 0x311f A fonts.gstatic.com
171	4.752818	192.168.142.13	192.168.142.203	DNS	129	Standard query response 0x311f A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 1
1026	8.892912	192.168.142.203	192.168.142.13	DNS	87	Standard query 0x9d5e A 3.client-channel.google.com
1097	8.985403	192.168.142.13	192.168.142.203	DNS	103	Standard query response 0x9d5e A 3.client-channel.google.com A 74.125.142.189
2312	25.335254	192.168.142.203	192.168.142.13	DNS	70	Standard query 0xb4bf A google.com
2314	25.394215	192.168.142.13	192.168.142.203	DNS	86	Standard query response 0xb4bf A google.com A 142.251.32.46
2323	25.429952	192.168.142.203	192.168.142.13	DNS	91	Standard query 0x6865 A signaler-pa.clients6.google.com
2324	25.466261	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0x6865 A signaler-pa.clients6.google.com A 142.251.46.170
3146	26.899337	192.168.142.203	192.168.142.13	DNS	91	Standard query 0xb47f A content-autofill.googleapis.com
3157	26.969205	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0xb47f A content-autofill.googleapis.com A 142.251.46.170
3291	27.231413	192.168.142.203	192.168.142.13	DNS	80	Standard query 0x74be A adservice.google.com

> Frame 2314: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{1F09A365-29BF-49E4-A85B-917644423F59}, id 0
> Ethernet II, Src: 42:4e:bd:f7:0e:77 (42:4e:bd:f7:0e:77), Dst: IntelCor_8d:4e:01 (20:16:b9:8d:4e:01)
> Internet Protocol Version 4, Src: 192.168.142.13, Dst: 192.168.142.203
> User Datagram Protocol, Src Port: 53, Dst Port: 65218
> Domain Name System (response)

```
0000   20 16 b9 8d 4e 01 42 4e   bd f7 0e 77 08 00 45 00    ···N·BN ···w··E·
0010   00 48 68 53 40 00 40 11   34 28 c0 a8 8e 0d c0 a8    ·HhS@·@· 4(······
0020   8e cb 00 35 fe c2 00 34   a9 bb b4 bf 81 80 00 01    ···5···4 ········
0030   00 01 00 00 00 00 06 67   6f 6f 67 6c 65 03 63 6f    ·······g oogle·co
0040   6d 00 00 01 00 01 c0 0c   00 01 00 01 00 00 00 72    m······· ·······r
0050   00 04 8e fb 20 2e                                     ···· .
```

Domain Name System: Protocol   Packets: 3442 · Displayed: 16 (0.5%) · Dropped: 0 (0.0%)   Profile: Default

File   Edit   View   Go   Capture   Analyze   Statistics   Telephony   Wireless   Tools   Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
7	2.400440	192.168.142.203	192.168.142.13	DNS	89	Standard query 0xb44c A pagead2.googlesyndication.com
9	2.452837	192.168.142.13	192.168.142.203	DNS	105	Standard query response 0xb44c A pagead2.googlesyndication.com A 142.250.65.194
54	3.479244	192.168.142.203	192.168.142.13	DNS	74	Standard query 0x0202 A px.moatads.com
55	3.534418	192.168.142.13	192.168.142.203	DNS	170	Standard query response 0x0202 A px.moatads.com CNAME wildcard.moatads.com.edgekey.net
168	4.701024	192.168.142.203	192.168.142.13	DNS	77	Standard query 0x311f A fonts.gstatic.com
171	4.752818	192.168.142.13	192.168.142.203	DNS	129	Standard query response 0x311f A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 1
1026	8.892912	192.168.142.203	192.168.142.13	DNS	87	Standard query 0x9d5e A 3.client-channel.google.com
1097	8.985403	192.168.142.13	192.168.142.203	DNS	103	Standard query response 0x9d5e A 3.client-channel.google.com A 74.125.142.189
2312	25.335254	192.168.142.203	192.168.142.13	DNS	70	Standard query 0xb4bf A google.com
2314	25.394215	192.168.142.13	192.168.142.203	DNS	86	Standard query response 0xb4bf A google.com A 142.251.32.46
2323	25.429952	192.168.142.203	192.168.142.13	DNS	91	Standard query 0x6865 A signaler-pa.clients6.google.com
2324	25.466261	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0x6865 A signaler-pa.clients6.google.com A 142.251.46.170
3146	26.899337	192.168.142.203	192.168.142.13	DNS	91	Standard query 0xb47f A content-autofill.googleapis.com
3157	26.969205	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0xb47f A content-autofill.googleapis.com A 142.251.46.170
3291	27.231413	192.168.142.203	192.168.142.13	DNS	80	Standard query 0x74be A adservice.google.com

> Frame 2314: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{1F09A365-29BF-49E4-A85B-917644423F59}, id 0
> Ethernet II, Src: 42:4e:bd:f7:0e:77 (42:4e:bd:f7:0e:77), Dst: IntelCor_8d:4e:01 (20:16:b9:8d:4e:01)
> Internet Protocol Version 4, Src: 192.168.142.13, Dst: 192.168.142.203
> User Datagram Protocol, Src Port: 53, Dst Port: 65218
∨ Domain Name System (response)
    Transaction ID: 0xb4bf
    > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    ∨ Queries
      > google.com: type A, class IN
    > Answers
      [Request In: 2312]
      [Time: 0.058961000 seconds]

```
0000   20 16 b9 8d 4e 01 42 4e   bd f7 0e 77 08 00 45 00   ···N·BN ···w··E·
0010   00 48 68 53 40 00 40 11   34 28 c0 a8 8e 0d c0 a8   ·HhS@·@· 4(······
0020   8e cb 00 35 fe c2 00 34   a9 bb b4 bf 81 80 00 01   ···5···4 ········
0030   00 01 00 00 00 00 06 67   6f 6f 67 6c 65 03 63 6f   ·······g oogle·co
0040   6d 00 00 01 00 01 c0 0c   00 01 00 01 00 00 00 72   m······· ·······r
0050   00 04 8e fb 20 2e                                   ···· .
```

Domain Name System (dns), 44 bytes   Packets: 3442 · Displayed: 16 (0.5%) · Dropped: 0 (0.0%)   Profile: Default

File   Edit   View   Go   Capture   Analyze   Statistics   Telephony   Wireless   Tools   Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
7	2.400440	192.168.142.203	192.168.142.13	DNS	89	Standard query 0xb44c A pagead2.googlesyndication.com
9	2.452837	192.168.142.13	192.168.142.203	DNS	105	Standard query response 0xb44c A pagead2.googlesyndication.com A 142.250.65.194
54	3.479244	192.168.142.203	192.168.142.13	DNS	74	Standard query 0x0202 A px.moatads.com
55	3.534418	192.168.142.13	192.168.142.203	DNS	170	Standard query response 0x0202 A px.moatads.com CNAME wildcard.moatads.com.edgekey.net
168	4.701024	192.168.142.203	192.168.142.13	DNS	77	Standard query 0x311f A fonts.gstatic.com
171	4.752818	192.168.142.13	192.168.142.203	DNS	129	Standard query response 0x311f A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 1
1026	8.892912	192.168.142.203	192.168.142.13	DNS	87	Standard query 0x9d5e A 3.client-channel.google.com
1097	8.985403	192.168.142.13	192.168.142.203	DNS	103	Standard query response 0x9d5e A 3.client-channel.google.com A 74.125.142.189
2312	25.335254	192.168.142.203	192.168.142.13	DNS	70	Standard query 0xb4bf A google.com
2314	25.394215	192.168.142.13	192.168.142.203	DNS	86	Standard query response 0xb4bf A google.com A 142.251.32.46
2323	25.429952	192.168.142.203	192.168.142.13	DNS	91	Standard query 0x6865 A signaler-pa.clients6.google.com
2324	25.466261	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0x6865 A signaler-pa.clients6.google.com A 142.251.46.170
3146	26.899337	192.168.142.203	192.168.142.13	DNS	91	Standard query 0xb47f A content-autofill.googleapis.com
3157	26.969205	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0xb47f A content-autofill.googleapis.com A 142.251.46.170
3291	27.231413	192.168.142.203	192.168.142.13	DNS	80	Standard query 0x74be A adservice.google.com

```
  Transaction ID: 0xb4bf
> Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
v Queries
    v google.com: type A, class IN
        Name: google.com
        [Name Length: 10]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
> Answers
  [Request In: 2312]
  [Time: 0.058961000 seconds]
```

```
0000  20 16 b9 8d 4e 01 42 4e  bd f7 0e 77 08 00 45 00    · · ·N·BN ···w··E·
0010  00 48 68 53 40 00 40 11  34 28 c0 a8 8e 0d c0 a8    ·HhS@·@· 4(······
0020  8e cb 00 35 fe c2 00 34  a9 bb b4 bf 81 80 00 01    ···5···4 ········
0030  00 01 00 00 00 00 06 67  6f 6f 67 6c 65 03 63 6f    ·······g oogle·co
0040  6d 00 00 01 00 01 c0 0c  00 01 00 01 00 00 00 72    m······· ·······r
0050  00 04 8e fb 20 2e                                   ···· ·
```

Domain Name System (dns), 44 bytes   Packets: 3442 · Displayed: 16 (0.5%) · Dropped: 0 (0.0%)   Profile: Default

File   Edit   View   Go   Capture   Analyze   Statistics   Telephony   Wireless   Tools   Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
7	2.400440	192.168.142.203	192.168.142.13	DNS	89	Standard query 0xb44c A pagead2.googlesyndication.com
9	2.452837	192.168.142.13	192.168.142.203	DNS	105	Standard query response 0xb44c A pagead2.googlesyndication.com A 142.250.65.194
54	3.479244	192.168.142.203	192.168.142.13	DNS	74	Standard query 0x0202 A px.moatads.com
55	3.534418	192.168.142.13	192.168.142.203	DNS	170	Standard query response 0x0202 A px.moatads.com CNAME wildcard.moatads.com.edgekey.net
168	4.701024	192.168.142.203	192.168.142.13	DNS	77	Standard query 0x311f A fonts.gstatic.com
171	4.752818	192.168.142.13	192.168.142.203	DNS	129	Standard query response 0x311f A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 1
1026	8.892912	192.168.142.203	192.168.142.13	DNS	87	Standard query 0x9d5e A 3.client-channel.google.com
1097	8.985403	192.168.142.13	192.168.142.203	DNS	103	Standard query response 0x9d5e A 3.client-channel.google.com A 74.125.142.189
2312	25.335254	192.168.142.203	192.168.142.13	DNS	70	Standard query 0xb4bf A google.com
2314	25.394215	192.168.142.13	192.168.142.203	DNS	86	Standard query response 0xb4bf A google.com A 142.251.32.46
2323	25.429952	192.168.142.203	192.168.142.13	DNS	91	Standard query 0x6865 A signaler-pa.clients6.google.com
2324	25.466261	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0x6865 A signaler-pa.clients6.google.com A 142.251.46.170
3146	26.899337	192.168.142.203	192.168.142.13	DNS	91	Standard query 0xb47f A content-autofill.googleapis.com
3157	26.969205	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0xb47f A content-autofill.googleapis.com A 142.251.46.170
3291	27.231413	192.168.142.203	192.168.142.13	DNS	80	Standard query 0x74be A adservice.google.com

```
∨ google.com: type A, class IN
      Name: google.com
      [Name Length: 10]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
∨ Answers
   ∨ google.com: type A, class IN, addr 142.251.32.46
      Name: google.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 114 (1 minute, 54 seconds)
      Data length: 4
      Address: 142.251.32.46
   [Request In: 2312]
   [Time: 0.058961000 seconds]
```

```
0000   20 16 b9 8d 4e 01 42 4e   bd f7 0e 77 08 00 45 00    ···N·BN ···w··E·
0010   00 48 68 53 40 00 40 11   34 28 c0 a8 8e 0d c0 a8    ·HhS@·@· 4(······
0020   8e cb 00 35 fe c2 00 34   a9 bb b4 bf 81 80 00 01    ···5···4 ········
0030   00 01 00 00 00 00 06 67   6f 6f 67 6c 65 03 63 6f    ·······g oogle·co
0040   6d 00 00 01 00 01 c0 0c   00 01 00 01 00 00 00 72    m······· ·······r
0050   00 04 8e fb 20 2e                                     ···· ·
```

Text item (text), 16 bytes   Packets: 3442 · Displayed: 16 (0.5%) · Dropped: 0 (0.0%)   Profile: Default

File   Edit   View   Go   Capture   Analyze   Statistics   Telephony   Wireless   Tools   Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
29	5.637331	192.168.142.203	192.168.142.13	DNS	86	Standard query 0x2e54 A encrypted-tbn0.gstatic.com
31	5.687659	192.168.142.13	192.168.142.203	DNS	102	Standard query response 0x2e54 A encrypted-tbn0.gstatic.com A 216.58.194.206
113	14.266239	192.168.142.203	192.168.142.13	DNS	72	Standard query 0x2441 A facebook.com
114	14.436156	192.168.142.13	192.168.142.203	DNS	88	Standard query response 0x2441 A facebook.com A 157.240.2.35
149	14.746646	192.168.142.203	192.168.142.13	DNS	76	Standard query 0x86dd A www.facebook.com
151	14.870290	192.168.142.13	192.168.142.203	DNS	121	Standard query response 0x86dd A www.facebook.com CNAME star-mini.c10r.facebook.com A
170	15.320209	192.168.142.203	192.168.142.13	DNS	79	Standard query 0x2200 A static.xx.fbcdn.net
200	15.609788	192.168.142.13	192.168.142.203	DNS	118	Standard query response 0x2200 A static.xx.fbcdn.net CNAME scontent.xx.fbcdn.net A 157
541	16.083687	192.168.142.203	192.168.142.13	DNS	88	Standard query 0xf11e A scontent-lga3-2.xx.fbcdn.net
682	16.237058	192.168.142.13	192.168.142.203	DNS	104	Standard query response 0xf11e A scontent-lga3-2.xx.fbcdn.net A 157.240.241.1
2254	17.095550	192.168.142.203	192.168.142.13	DNS	81	Standard query 0x67a7 A scontent.xx.fbcdn.net
2329	17.109140	192.168.142.13	192.168.142.203	DNS	97	Standard query response 0x67a7 A scontent.xx.fbcdn.net A 157.240.2.25
2338	17.146569	192.168.142.203	192.168.142.13	DNS	91	Standard query 0xbed8 A content-autofill.googleapis.com
2377	17.180356	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0xbed8 A content-autofill.googleapis.com A 142.251.46.170
2509	17.233702	192.168.142.203	192.168.142.13	DNS	82	Standard query 0x5939 A edge-chat.facebook.com

> Frame 149: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{1F09A365-29BF-49E4-A85B-917644423F59}, id 0
> Ethernet II, Src: IntelCor_8d:4e:01 (20:16:b9:8d:4e:01), Dst: 42:4e:bd:f7:0e:77 (42:4e:bd:f7:0e:77)
> Internet Protocol Version 4, Src: 192.168.142.203, Dst: 192.168.142.13
> User Datagram Protocol, Src Port: 65228, Dst Port: 53
∨ Domain Name System (query)
      Transaction ID: 0x86dd
   > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
   ∨ Queries
      > www.facebook.com: type A, class IN
      [Response In: 151]

```
0000   42 4e bd f7 0e 77 20 16  b9 8d 4e 01 08 00 45 00   BN···w · ··N···E·
0010   00 3e 37 c1 00 00 80 11  00 00 c0 a8 8e cb c0 a8   ·>7····· ········
0020   8e 0d fe cc 00 35 00 2a  9e 65 86 dd 01 00 00 01   ·····5·* ·e······
0030   00 00 00 00 00 00 03 77  77 77 08 66 61 63 65 62   ·······w ww·faceb
0040   6f 6f 6b 03 63 6f 6d 00  00 01 00 01               ook·com· ····
```

Domain Name System: Protocol   Packets: 4525 · Displayed: 24 (0.5%) · Dropped: 0 (0.0%)   Profile: Default

File   Edit   View   Go   Capture   Analyze   Statistics   Telephony   Wireless   Tools   Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
29	5.637331	192.168.142.203	192.168.142.13	DNS	86	Standard query 0x2e54 A encrypted-tbn0.gstatic.com
31	5.687659	192.168.142.13	192.168.142.203	DNS	102	Standard query response 0x2e54 A encrypted-tbn0.gstatic.com A 216.58.194.206
113	14.266239	192.168.142.203	192.168.142.13	DNS	72	Standard query 0x2441 A facebook.com
114	14.436156	192.168.142.13	192.168.142.203	DNS	88	Standard query response 0x2441 A facebook.com A 157.240.2.35
149	14.746646	192.168.142.203	192.168.142.13	DNS	76	Standard query 0x86dd A www.facebook.com
151	14.870290	192.168.142.13	192.168.142.203	DNS	121	Standard query response 0x86dd A www.facebook.com CNAME star-mini.c10r.facebook.com A
170	15.320209	192.168.142.203	192.168.142.13	DNS	79	Standard query 0x2200 A static.xx.fbcdn.net
200	15.609788	192.168.142.13	192.168.142.203	DNS	118	Standard query response 0x2200 A static.xx.fbcdn.net CNAME scontent.xx.fbcdn.net A 157
541	16.083687	192.168.142.203	192.168.142.13	DNS	88	Standard query 0xf11e A scontent-lga3-2.xx.fbcdn.net
682	16.237058	192.168.142.13	192.168.142.203	DNS	104	Standard query response 0xf11e A scontent-lga3-2.xx.fbcdn.net A 157.240.241.1
2254	17.095550	192.168.142.203	192.168.142.13	DNS	81	Standard query 0x67a7 A scontent.xx.fbcdn.net
2329	17.109140	192.168.142.13	192.168.142.203	DNS	97	Standard query response 0x67a7 A scontent.xx.fbcdn.net A 157.240.2.25
2338	17.146569	192.168.142.203	192.168.142.13	DNS	91	Standard query 0xbed8 A content-autofill.googleapis.com
2377	17.180356	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0xbed8 A content-autofill.googleapis.com A 142.251.46.170
2509	17.233702	192.168.142.203	192.168.142.13	DNS	82	Standard query 0x5939 A edge-chat.facebook.com

```
> Internet Protocol Version 4, Src: 192.168.142.13, Dst: 192.168.142.203
> User Datagram Protocol, Src Port: 53, Dst Port: 65228
v Domain Name System (response)
     Transaction ID: 0x86dd
   > Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 2
     Authority RRs: 0
     Additional RRs: 0
   v Queries
       > www.facebook.com: type A, class IN
   v Answers
       > www.facebook.com: type CNAME, class IN, cname star-mini.c10r.facebook.com
       > star-mini.c10r.facebook.com: type A, class IN, addr 157.240.2.35
     [Request In: 149]
     [Time: 0.123644000 seconds]
```

```
0000   20 16 b9 8d 4e 01 42 4e  bd f7 0e 77 08 00 45 00    ··-N·BN ···w··E·
0010   00 6b b1 b7 40 00 40 11  ea a0 c0 a8 8e 0d c0 a8    ·k··@·@· ········
0020   8e cb 00 35 fe cc 00 57  ad b6 86 dd 81 80 00 01    ···5···W ········
0030   00 02 00 00 00 00 03 77  77 77 08 66 61 63 65 62    ·······w ww·faceb
0040   6f 6f 6b 03 63 6f 6d 00  00 01 00 01 c0 0c 00 05    ook·com· ········
0050   00 01 00 00 04 51 00 11  09 73 74 61 72 2d 6d 69    ·····Q·· ·star-mi
```

Domain Name System: Protocol   Packets: 4525 · Displayed: 24 (0.5%) · Dropped: 0 (0.0%)   Profile: Default

File   Edit   View   Go   Capture   Analyze   Statistics   Telephony   Wireless   Tools   Help

`dns`

No.	Time	Source	Destination	Protocol	Length	Info
29	5.637331	192.168.142.203	192.168.142.13	DNS	86	Standard query 0x2e54 A encrypted-tbn0.gstatic.com
31	5.687659	192.168.142.13	192.168.142.203	DNS	102	Standard query response 0x2e54 A encrypted-tbn0.gstatic.com A 216.58.194.206
113	14.266239	192.168.142.203	192.168.142.13	DNS	72	Standard query 0x2441 A facebook.com
114	14.436156	192.168.142.13	192.168.142.203	DNS	88	Standard query response 0x2441 A facebook.com A 157.240.2.35
149	14.746646	192.168.142.203	192.168.142.13	DNS	76	Standard query 0x86dd A www.facebook.com
151	14.870290	192.168.142.13	192.168.142.203	DNS	121	Standard query response 0x86dd A www.facebook.com CNAME star-mini.c10r.facebook.com A
170	15.320209	192.168.142.203	192.168.142.13	DNS	79	Standard query 0x2200 A static.xx.fbcdn.net
200	15.609788	192.168.142.13	192.168.142.203	DNS	118	Standard query response 0x2200 A static.xx.fbcdn.net CNAME scontent.xx.fbcdn.net A 157
541	16.083687	192.168.142.203	192.168.142.13	DNS	88	Standard query 0xf11e A scontent-lga3-2.xx.fbcdn.net
682	16.237058	192.168.142.13	192.168.142.203	DNS	104	Standard query response 0xf11e A scontent-lga3-2.xx.fbcdn.net A 157.240.241.1
2254	17.095550	192.168.142.203	192.168.142.13	DNS	81	Standard query 0x67a7 A scontent.xx.fbcdn.net
2329	17.109140	192.168.142.13	192.168.142.203	DNS	97	Standard query response 0x67a7 A scontent.xx.fbcdn.net A 157.240.2.25
2338	17.146569	192.168.142.203	192.168.142.13	DNS	91	Standard query 0xbed8 A content-autofill.googleapis.com
2377	17.180356	192.168.142.13	192.168.142.203	DNS	107	Standard query response 0xbed8 A content-autofill.googleapis.com A 142.251.46.170
2509	17.233702	192.168.142.203	192.168.142.13	DNS	82	Standard query 0x5939 A edge-chat.facebook.com

```
  www.facebook.com: type CNAME, class IN, cname star-mini.c10r.facebook.com
      Name: www.facebook.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1105 (18 minutes, 25 seconds)
      Data length: 17
      CNAME: star-mini.c10r.facebook.com
  star-mini.c10r.facebook.com: type A, class IN, addr 157.240.2.35
      Name: star-mini.c10r.facebook.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 38 (38 seconds)
      Data length: 4
      Address: 157.240.2.35
  [Request In: 149]
  [Time: 0.123644000 seconds]
```

```
0000  20 16 b9 8d 4e 01 42 4e  bd f7 0e 77 08 00 45 00    ··N·BN ···w··E·
0010  00 6b b1 b7 40 00 40 11  ea a0 c0 a8 8e 0d c0 a8    ·k··@·@· ········
0020  8e cb 00 35 fe cc 00 57  ad b6 86 dd 81 80 00 01    ···5···W ········
0030  00 02 00 00 00 00 03 77  77 77 08 66 61 63 65 62    ·······w ww·faceb
0040  6f 6f 6b 03 63 6f 6d 00  00 01 00 01 c0 0c 00 05    ook·com· ········
0050  00 01 00 00 04 51 00 11  09 73 74 61 72 2d 6d 69    ·····Q·· ·star-mi
```

Domain Name System: Protocol   Packets: 4525 · Displayed: 24 (0.5%) · Dropped: 0 (0.0%)   Profile: Default

nslookup


```
Command Prompt                                                  —    □    ✕

Microsoft Windows [Version 10.0.19042.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Asman>nslookup google.com
Server:  UnKnown
Address:  192.168.142.13

Non-authoritative answer:
Name:    google.com
Addresses:  2607:f8b0:4005:80e::200e
          142.251.46.238


C:\Users\Asman>
```

nslookup


```
Command Prompt - nslookup                                    —  ☐  ✕

Microsoft Windows [Version 10.0.19042.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Asman>nslookup google.com
Server:  UnKnown
Address:  192.168.142.13

Non-authoritative answer:
Name:    google.com
Addresses:  2607:f8b0:4005:80e::200e
          142.251.46.238


C:\Users\Asman>nslookup
Default Server:  UnKnown
Address:  192.168.142.13

> set type=ns
> google.com
Server:  UnKnown
Address:  192.168.142.13

Non-authoritative answer:
google.com        nameserver = ns3.google.com
google.com        nameserver = ns4.google.com
google.com        nameserver = ns2.google.com
google.com        nameserver = ns1.google.com
>
```
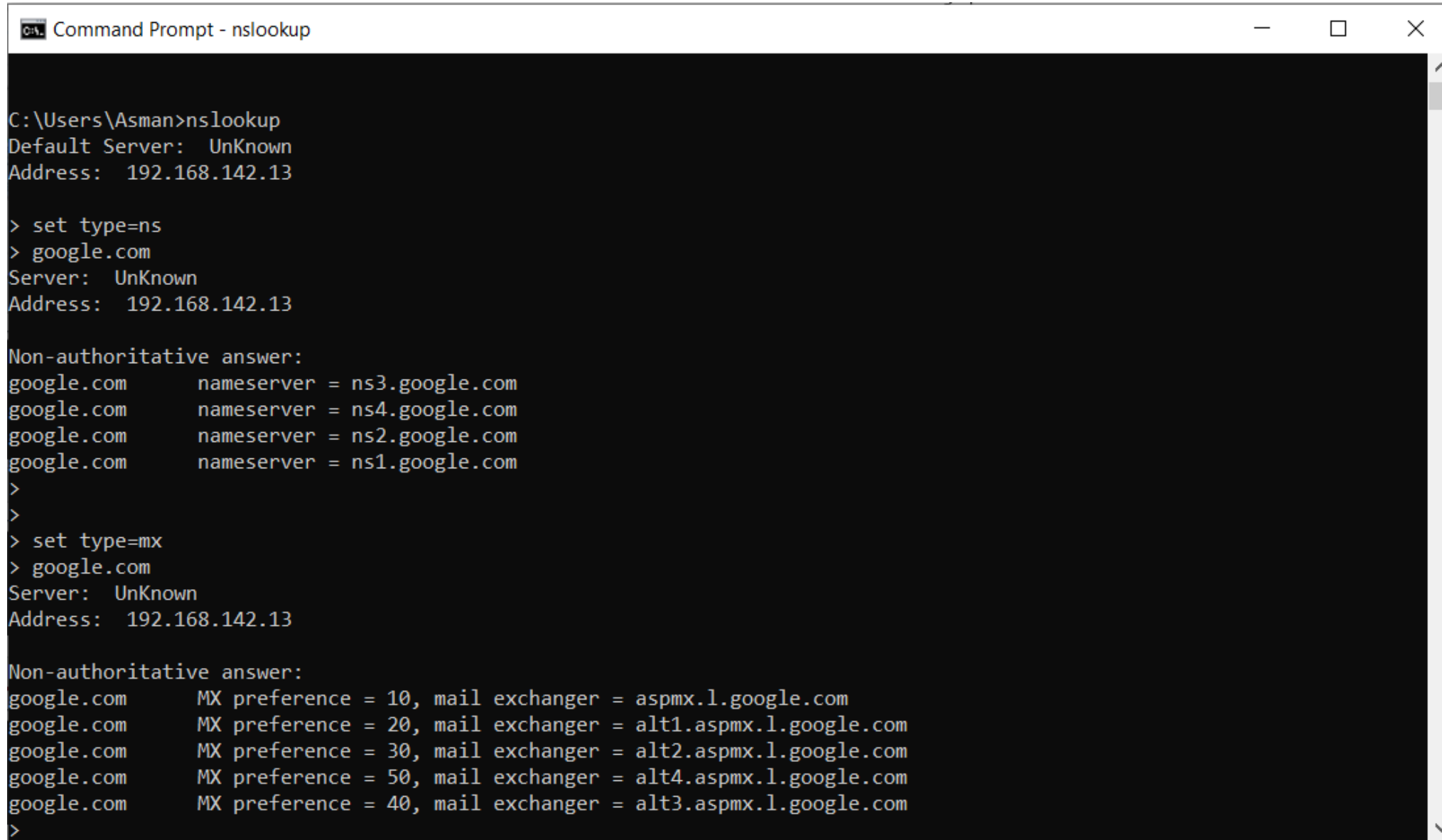
nslookup