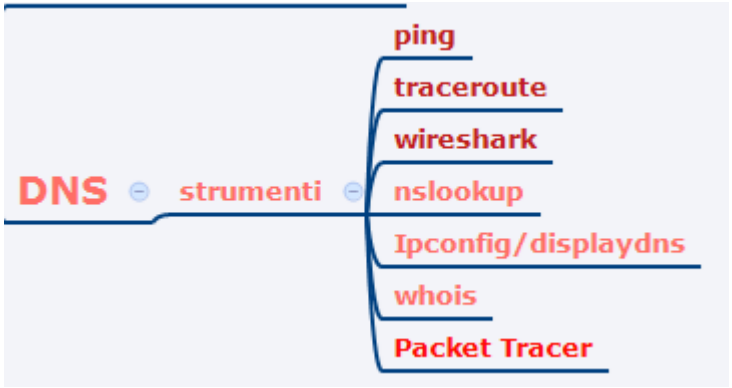
DNS: i concetti chiave



Obiettivi:

- Imparare i concetti chiave del DNS.
- Introdurre le utility che si usano in generale nel troubleshooting (le prime sei).
- Esplorare i concetti chiave tramite le utility – *esercitazione 1.*
- Imparare a utilizzare Wireshark sull'esempio del sito yandex.ru avente 4 indirizzi IPv4 (e 1 indirizzo IPv6) – *esercitazione 2.*

  Per eseguire questo esercizio,

  impostare il filtro Wireshark al «DNS»,
  lanciare contemporaneamente nslookup e Wireshark,
  esplorare i vari campi del frame, individuando i concetti chiave.

DNS ROOT SERVERS

Nome host	Indirizzo IP	Gestore
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

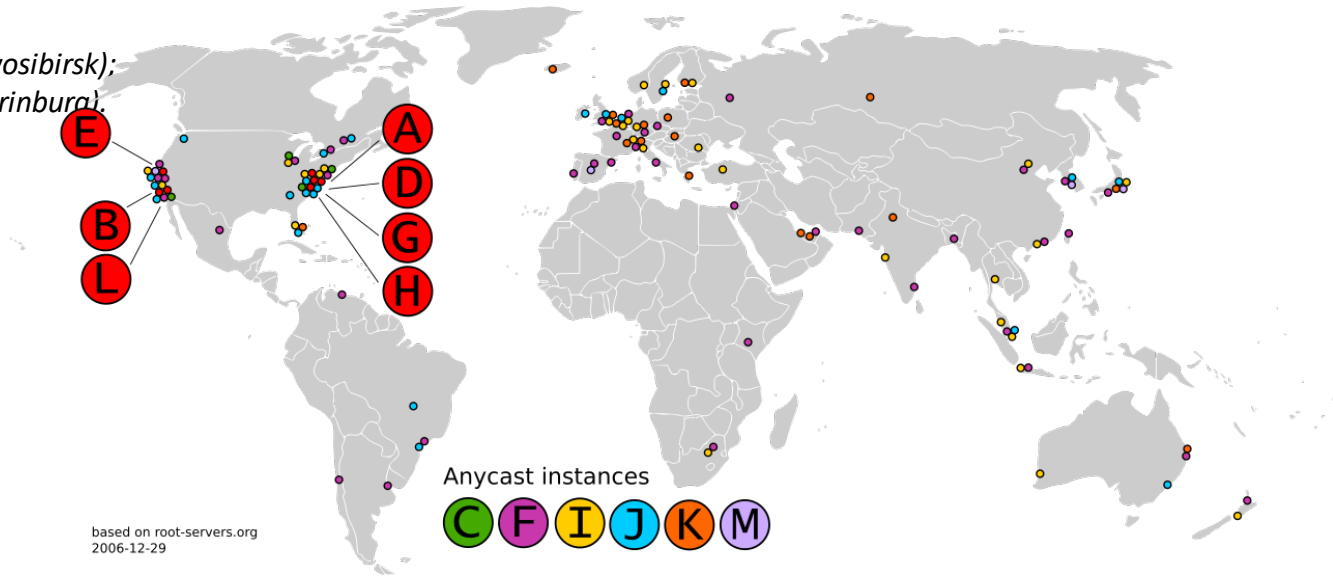
As of 2018-07-09, the root server system consists of 929 instances operated by the 12 independent root server operators. The 13 root name servers are operated by 12 independent organisations.

Le macchine C, F, I, J, K, L e M sono presenti in più luoghi ed in diversi continenti, usando annunci anycast per fornire un servizio decentralizzato.

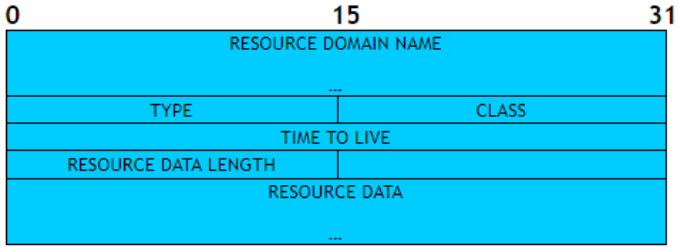
DNS ROOT SERVERS

Ogni server sulla Rete deve essere univocamente raggiungibile (per semplicità: 1 server = 1 indirizzo IP), è stato applicato un metodo (ANYCAST) che consente di spostare l'univocità dal livello globale della Rete a solo parti di essa: in altre parole sono state creati dei "replicanti" dei singoli root name server (stesso nome, stesso indirizzo IP, stesso gestore) e posizionati in punti diversi di Internet, garantendone la visibilità e la raggiungibilità solo ad una porzione ristretta della Rete.

Al 22.05.2018 , in Russia ci sono 11 repliche dei root-server DNS:
f.root (Mosca, 2);
i.root (San-Pietroburgo);
j.root (Mosca, San-Pietroburgo);
k.root (Mosca, San-Pietroburgo, Novosibirsk);
l.root (Mosca, Rostov-sul-Don, Ekaterinburg).



DNS: i concetti chiave



DOMINIO: un nome univoco nel DNS

Registrar: una società che può fornire nomi di dominio Internet e verificare se il domi net richiesto è disponibile, consentendo all'utente di acquistarlo.

SOTTODOMINIO

RESOURSE RECORD, RR

ZONE: Una zona DNS viene usata per ospitare i record DNS per un particolare dominio . Esempio: alfa.com può contenere diversi record come mail.alfa.com, www.alfa.com

DELEGARE

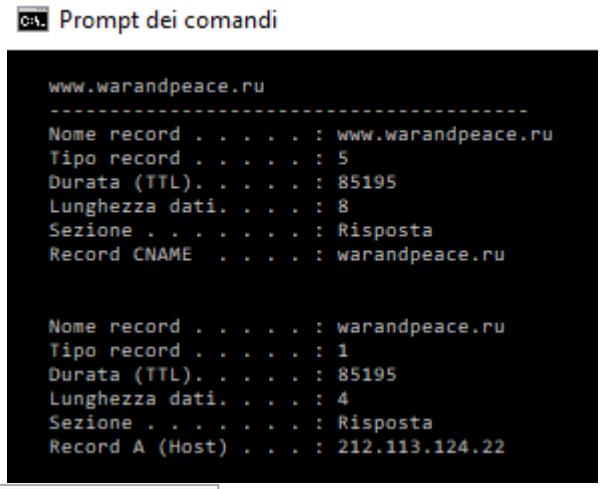
DNS-SERVER : sw di gestione DNS

DNS-client (RESOLVER): una biblioteca o un sw per lavorare con DNS

AUTHORITATIVE: un indicatore di dislocamento della zona sul server DNS.

Le risposte del server DNS possono essere di due tipi:
-autoritative (il server dichiara che risponde per la zona) o
-non-A (il server elabora la richiesta ma ritorna la risposta degli altri server)

DNS-QUERY: ricorsivo o non-ricorsivo



CNAME	5	RFC 1035	**record di nome canonico**	Permette di collegare un nome DNS ad un altro
A	1	RFC 1035	**record di indirizzo**	restituisce un indirizzo IPv4 a 32 bit, normalmente utilizzato per collegare un nome host al suo indirizzo IP.

Esercitazioni in laboratorio 1

nslookup

Prompt dei comandi

```
C:\Users\Natasha>nslookup yoox.it
Server:  cns-c.libero.it
Address:  193.70.152.15

Risposta da un server non autorevole:
Nome:    yoox.it
Address:  54.72.108.69


C:\Users\Natasha>nslookup  -type=A  www.yoox.it
Server:  cns-c.libero.it
Address:  193.70.152.15

Risposta da un server non autorevole:
Nome:    rdr.yservices.net
Address:  54.72.108.69
Aliases:  www.yoox.it
          yoox.rdr.yservices.net
```

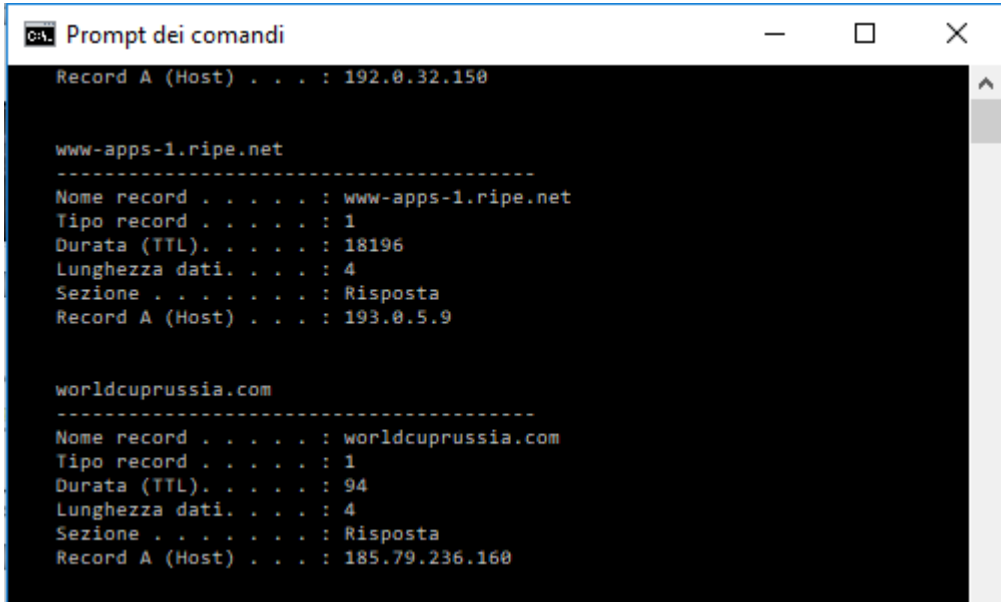
Solo per gli IP versione 4:
nslookup -type=A www.yoox.it
-type=**AAAA** gli IP ver.6
-type=**MX** per server email
-type=**NS** quali server rispondono per la zona yandex.ru
Reversive query , reverse lookup

Prompt dei comandi

```
C:\Users\Natasha>nslookup -type=NS yandex.ru
Server:  cns-c.libero.it
Address:  193.70.152.15

Risposta da un server non autorevole:
yandex.ru       nameserver = ns9.z5h64q92x9.net
yandex.ru       nameserver = ns1.yandex.ru
yandex.ru       nameserver = ns2.yandex.ru

C:\Users\Natasha>
```

Esercitazioni in laboratorio 1

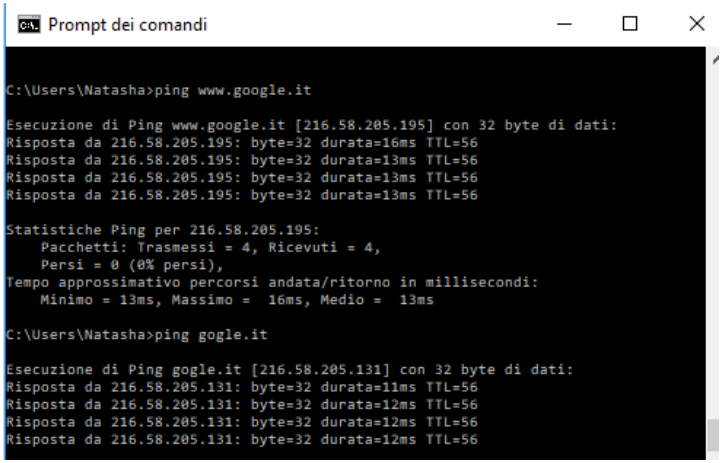
Ipconfig/displaydns



Visualizza la cashe DNS locale (le ultime risposte a DNS Standard query avviate da qualche applicazione), ovvero i record dei database locali del DNS. Notare il campo TTL in secondi.

Ping

Nel caso del malfunzionamento della rete pubblica addebitato al DNS (DNS irragiungibile o malfunzionante, errata configurazione del protocollo, etc)
Si può fare un semplice test con l'utility **ping**:



Esercitazioni in laboratorio 1

whois

whois DOMAINS HOSTING WEBSITES TRADE

Lookup Tools
- WHOIS Lookup
- DNS Lookup
- RBL Lookup
- Traceroute
- IP Lookup
- API/Bulk Data Access

IP Lookup

Discover who controls an IP address

IP lookup is a browser based network diagnostic tool, used for discovering the IP geolocation and contact data for the people responsible for the address being queried.

To perform a IP lookup on a domain name, you just type directly into the IP lookup search box

tracert

PROVE con TRACERT e PING

Prima visualizziamo i parametri disponibili per le due utility (tracert e ping). Quelli da utilizzare adesso sono evidenziati in giallo:
per tracert non vogliamo la risoluzione degli indirizzi, visualizzeremo l'elenco degli "hop" (router);
per ping andiamo ad aumentare il TTL progressivamente da 1 a 3 (*da continuare*) e analizziamo la corrispondenza: 1– il pacchetto arriverà solo al primo router (confrontare gli IP), 2– a router etc.

Digitare **cmd** e poi **>tracert /?**

Sintassi: tracert [-d] [-h max_salti] [-j elenco-host] [-w timeout]
[-R] [-S indorig] [-4] [-6] nome_destinazione

Opzioni:
-d Non risolve gli indirizzi in nome host.
-h max_salti Numero massimo di punti di passaggio per ricercare la destinazione.
-j elenco-host Instradamento libero lungo l'elenco host (solo IPv4).
-w timeout Timeout in millisecondi per ogni risposta.
-R Traccia percorso andata e ritorno (solo IPv6).
-S indorig Indirizzo di origine da utilizzare (solo IPv6).
-4 Impone l'uso di IPv4.
-6 Impone l'uso di IPv6.

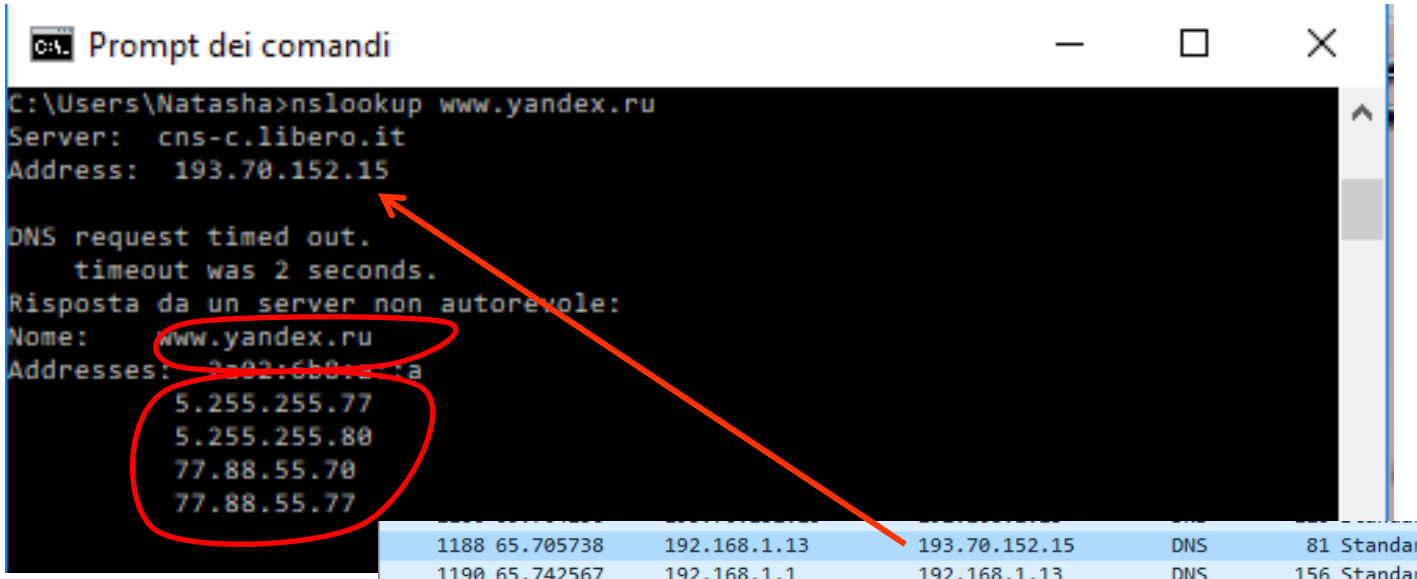
>ping /?

Prompt dei comandi

```
C:\Users\Natasha>tracert regione.veneto.it

Traccia instradamento verso regione.veneto.it [89.17.161.3]
su un massimo di 30 punti di passaggio:

  1     3 ms     2 ms     2 ms  vodafone.station [192.168.1.1]
  2    12 ms    10 ms    10 ms  net-2-42-78-1.cust.vodafonedsl.it [2.42.78.1]
  3    14 ms    13 ms    13 ms  10.176.27.245
  4    14 ms    13 ms    14 ms  10.176.4.182
  5    15 ms    13 ms    13 ms  10.176.8.6
  6    14 ms    13 ms    13 ms  93-63-100-46.ip27.fastwebnet.it [93.63.100.46]
  7     *        *        *     Richiesta scaduta.
  8     *        *        *     Richiesta scaduta.
  9    21 ms    19 ms    18 ms  93-54-36-25.ip127.fastwebnet.it [93.54.36.25]
 10    19 ms    17 ms    18 ms  89-96-234-51.ip14.fastwebnet.it [89.96.234.51]
 11    20 ms    20 ms    18 ms  89.17.162.4
 12    20 ms    19 ms    20 ms  ns03.regione.veneto.it [89.17.161.3]

Traccia completata.
```

Esercitazioni in laboratorio 2

Wireshark



1188	65.705738	192.168.1.13	193.70.152.15	DNS	81 Standard query 0x0002 A www.yandex.ru.station
1190	65.742567	192.168.1.1	192.168.1.13	DNS	156 Standard query response 0x0002 No such name A w
1224	67.707897	192.168.1.13	193.70.152.15	DNS	81 Standard query 0x0003 AAAA www.yandex.ru.statio
1232	67.992604	193.70.152.15	192.168.1.13	DNS	156 Standard query response 0x0003 No such name AAA
1233	67.993912	192.168.1.13	193.70.152.15	DNS	73 Standard query 0x0004 A www.yandex.ru
1234	67.996128	193.70.152.15	192.168.1.13	DNS	137 Standard query response 0x0004 A www.yandex.ru
1235	68.015399	192.168.1.13	193.70.152.15	DNS	73 Standard query 0x0005 AAAA www.yandex.ru
1236	68.016956	193.70.152.15	192.168.1.13	DNS	101 Standard query response 0x0005 AAAA www.yandex.

```
> Frame 1188: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
> Ethernet II, Src: HonHaiPr_b9:fb:d1 (90:00:4e:b9:fb:d1), Dst: e4:8f:34:87:4f:84 (e4:8f:34:87:4f:84)
> Internet Protocol Version 4, Src: 192.168.1.13, Dst: 193.70.152.15
> User Datagram Protocol, Src Port: 56627, Dst Port: 53
> Domain Name System (query)
```

```
0000  e4 8f 34 87 4f 84 90 00  4e b9 fb d1 08 00 45 00   ..4.O... N.....E.
0010  00 43 75 ce 00 00 80 11  a9 d0 c0 a8 01 0d c1 46   .Cu..... .......F
0020  98 0f dd 33 00 35 00 2f  72 b9 00 02 01 00 00 01   ...3.5./ r.......
0030  00 00 00 00 00 00 03 77  77 77 06 79 61 6e 64 65   .......w ww.yande
0040  78 02 72 75 07 73 74 61  74 69 6f 6e 00 00 01 00   x.ru.sta tion....
0050  01                                                .
```

Esercitazioni in laboratorio 2

Wireshark

```
User Datagram Protocol, Src Port: 56627, Dst Port: 53
    Source Port: 56627
    Destination Port: 53
    Length: 47
    Checksum: 0x72b9 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 8]
Domain Name System (query)
```

Source port 56627 assegnato al cliente dal SO

Pacchetto DNS,
ID transazione 2
I flag: query
query standard

Richiesta del funz. server DNS nella modalità ricorsiva

Un campo con query
Risposte dai server autoritativi e dei record aggiuntivi non ci sono

```
Domain Name System (query)
    Transaction ID: 0x0002
  Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    > www.yandex.ru.station: type A, class IN
```

L'unica query

```
  Queries
    www.yandex.ru.station: type A, class IN
        Name: www.yandex.ru.station
        [Name Length: 21]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Tipo record A, dal PC
Classe IN = Internet,
è l'unica classe utilizzata in DNS

Esercitazioni in laboratorio 2

La risposta del server

L'unica query

Wireshark

```
1188 65.705738   192.168.1.13    193.70.152.15   DNS   81 Standard query 0x0002 A www.yandex.ru.station
1190 65.742567   192.168.1.1     192.168.1.13    DNS   156 Standard query response 0x0002 No such name A www.yandex.ru.station SOA a.root-servers.net
```

```
> Frame 1190: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) on interface 0
> Ethernet II, Src: e4:8f:34:87:4f:84 (e4:8f:34:87:4f:84), Dst: HonHaiPr_b9:fb:d1 (90:00:4e:b9:fb:d1)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.13
v User Datagram Protocol, Src Port: 53, Dst Port: 60562
```

```
v User Datagram Protocol, Src Port: 53, Dst Port: 60562
    Source Port: 53
    Destination Port: 60562
    Length: 122
    Checksum: 0x19da [unverified]
    [Checksum Status: Unverified]
    [Stream index: 9]
v Domain Name System (response)
```

Source port 53
Des. Port 60562 assegnato dal SO

```
v Domain Name System (response)
    Transaction ID: 0x0002
  v Flags: 0x8183 Standard query response, No such name
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: A
      .... .... ...0 .... = Non-authenticated data
      .... .... .... 0011 = Reply code: No such na
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  v Queries
    v Queries
      v www.yandex.ru.station: type A, class IN
          Name: www.yandex.ru.station
          [Name Length: 21]
          [Label Count: 4]
          Type: A (Host Address) (1)
          Class: IN (0x0001)
    v Authoritative nameservers
      > <Root>: type SOA, class IN, mname a.root-servers.net
```

Pacchetto DNS, ID transazione 2, lo stesso
flag: è una risposta query standard

Il server ha eseguito la query nella modalità ricorsiva

Un campo con query
1 Risposta dai server autoritativi e
0 record aggiuntivi

Esercitazioni in laboratorio 2

Wireshark

Le info su un server autoritativo

```
Authoritative nameservers
  <Root>: type SOA, class IN, mname a.root-servers.net
    Name: <Root>
    Type: SOA (Start Of a zone of Authority) (6)
    Class: IN (0x0001)
    Time to live: 10800
    Data length: 64
    Primary name server: a.root-servers.net
    Responsible authority's mailbox: nstld.verisign-grs.com
    Serial Number: 2018070902
    Refresh Interval: 1800 (30 minutes)
    Retry Interval: 900 (15 minutes)
    Expire limit: 604800 (7 days)
    Minimum TTL: 86400 (1 day)
```

```
1234 67.996128   193.70.152.15   192.168.1.13   DNS   137 Standard query response 0x0004 A www.yandex.ru A 5.255.255.77 A 5.255.255.80 A 77.88.55.70 A 77.88.55.77
1235 68.015399   192.168.1.13    193.70.152.15  DNS    73 Standard query 0x0005 AAAA www.yandex.ru
```

```
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 4
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.yandex.ru: type A, class IN
      Name: www.yandex.ru
      [Name Length: 13]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  Answers
    www.yandex.ru: type A, class IN, addr 5.255.255.77
    www.yandex.ru: type A, class IN, addr 5.255.255.80
    www.yandex.ru: type A, class IN, addr 77.88.55.70
    www.yandex.ru: type A, class IN, addr 77.88.55.77
```

```
Risposta da un server non autorevole:
Nome:    www.yandex.ru
Addresses:  2a02:6b8:a::a
          5.255.255.77
          5.255.255.80
          77.88.55.70
          77.88.55.77
```