dns / opennic / dnscrypt

Serial: 2015111401

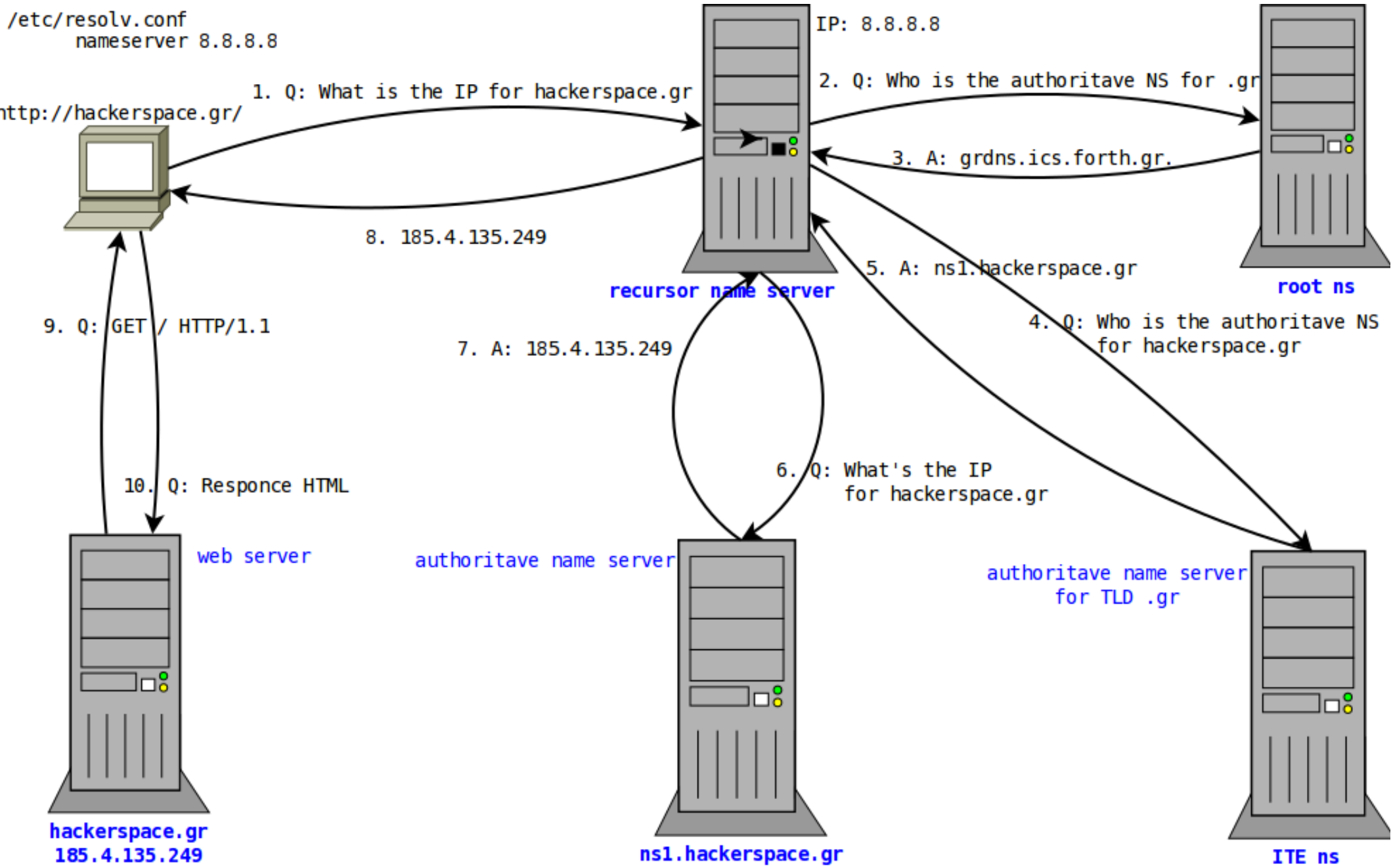
What is DNS

- Domain Name System

- In simple words when you are looking for **hackerspace.gr** you 're looking for the IP of the server that hosts the hackerspace site.

- But how ?

How DNS works



public/open dns

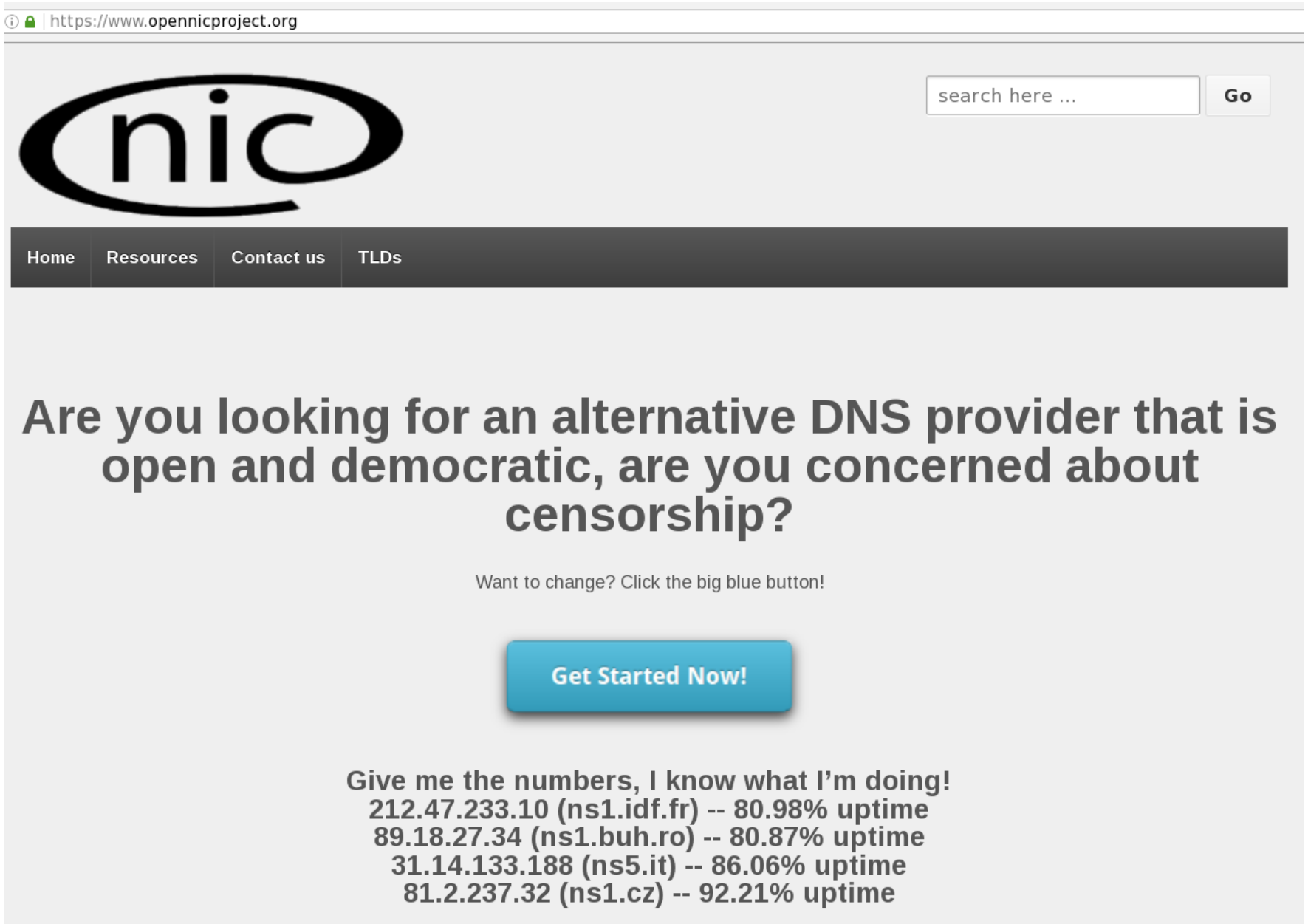
- Goodle dns
  - 8.8.8.8 2001:4860:4860::8888
  - 8.8.4.4 2001:4860:4860::8844
- OpenDNS
  - 208.67.222.222 2620:0:ccc::2
  - 208.67.220.220 2620:0:ccd::2
- norton dns/comodo/dns advantage/dns.watch
- fdn/freeDNS/Verisign

- BUT THEY ALL track what you are watching!!!!

https://www.opennicproject.org/

- OpenNIC is an alternate network information center/alternative DNS root which lists itself as an alternative to ICANN and its registries.
- Total DNS Neutrality
- Have A Say In Your DNS
- Protect Your Privacy
- No More ISP DNS Hijacking
- No Cost (Gratis)
- Freedom From Government Intervention

openic website/wiki



New Top Level Domains

.bbs

.dyn

.free

.fur

.geek

.gopher

.indy

.ing

.micro

.neo

.null

.oss

.oz

.parody

How does opennic work?

1.

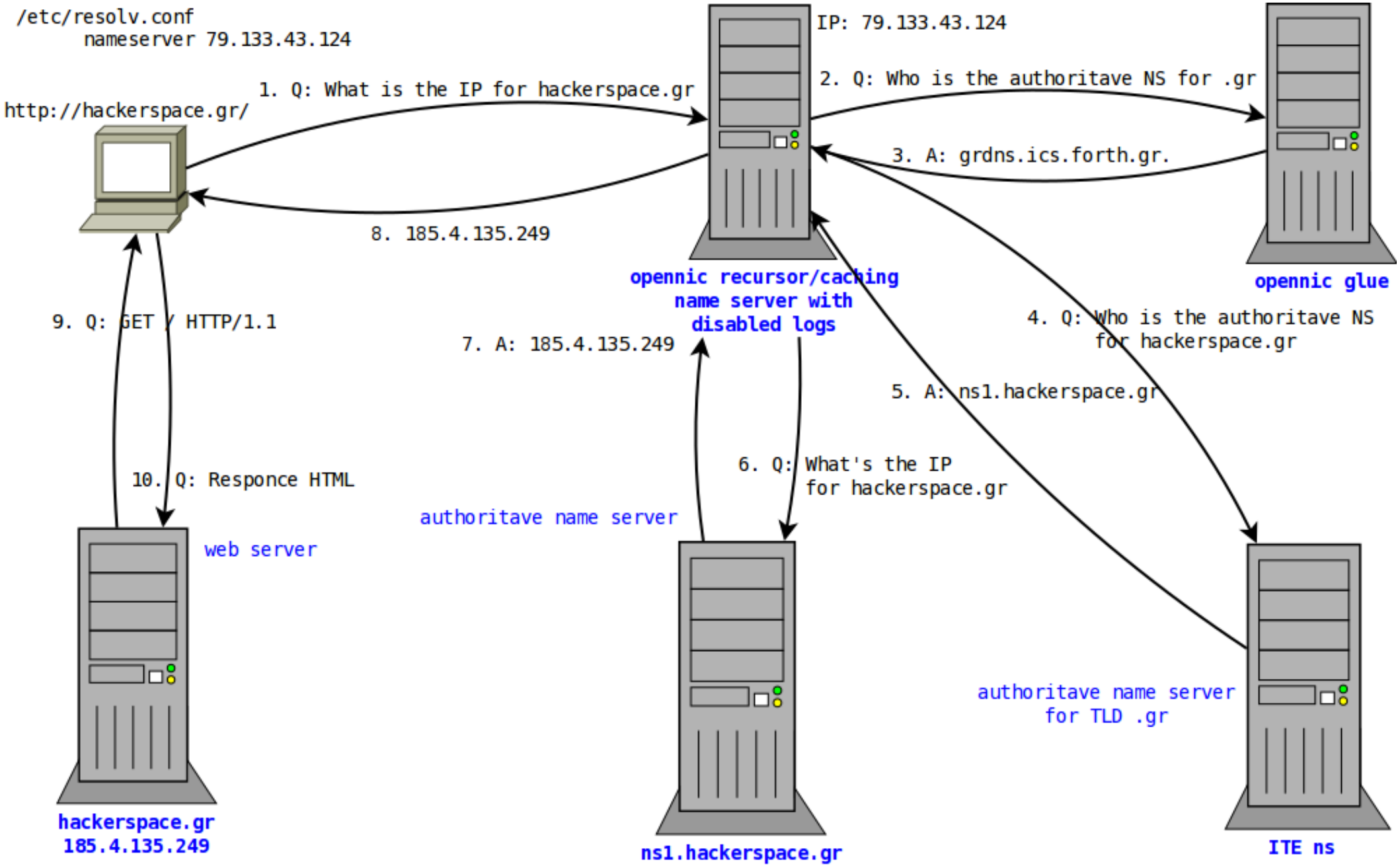
```
.   82796   IN  NS  ns9.opennic.glue.
.   82796   IN  NS  ns3.opennic.glue.
.   82796   IN  NS  ns8.opennic.glue.
.   82796   IN  NS  ns4.opennic.glue.
.   82796   IN  NS  ns10.opennic.glue.
.   82796   IN  NS  ns6.opennic.glue.
.   82796   IN  NS  ns7.opennic.glue.
.   82796   IN  NS  ns2.opennic.glue.
;; Received 174 bytes from 94.242.59.170#53(94.242.59.170) in 126 ms
```

2.

```
gr. 172800  IN  NS  gr-br.ics.forth.gr.
gr. 172800  IN  NS  gr-at.ics.forth.gr.
gr. 172800  IN  NS  estia.ics.forth.gr.
gr. 172800  IN  NS  grdns.ics.forth.gr.
gr. 172800  IN  NS  gr-ix.ics.forth.gr.
gr. 172800  IN  NS  grdns-de.denic.de.
gr. 172800  IN  NS  gr-m.ics.forth.gr.
gr. 86400   IN  DS  35136 7 2
;; Received 734 bytes from 188.226.146.136#53(ns10.opennic.glue) in 70 ms
```

How does opennic work?

```
3.

hackerspace.gr.         10800   IN  NS  ns1.hackerspace.gr.

hackerspace.gr.         10800   IN  NS  ns2.hackerspace.gr.

;; Received 598 bytes from 200.160.7.163#53(gr-br.ics.forth.gr) in 285 ms


4.

hackerspace.gr.         86400   IN  A   185.4.135.249

hackerspace.gr.         86400   IN  NS  ns1.hackerspace.gr.

hackerspace.gr.         86400   IN  NS  ns2.he.net.

hackerspace.gr.         86400   IN  NS  ns3.he.net.

hackerspace.gr.         86400   IN  NS  ns4.he.net.

hackerspace.gr.         86400   IN  NS  ns5.he.net.

;; Received 171 bytes from 185.4.135.249#53(ns1.hackerspace.gr) in 28 ms
```


/etc/resolv.conf
nameserver 79.133.43.124
http://hackerspace.gr/
1. Q: What is the IP for hackerspace.gr
IP: 79.133.43.124
2. Q: Who is the authoritave NS for .gr
3. A: grdns.ics.forth.gr.
8. 185.4.135.249
opennic recursor/caching
name server with
disabled logs
opennic glue
9. Q: GET / HTTP/1.1
7. A: 185.4.135.249
4. Q: Who is the authoritave NS
for hackerspace.gr
5. A: ns1.hackerspace.gr
6. Q: What's the IP
for hackerspace.gr
10. Q: Responce HTML
authoritave name server
web server
authoritave name server
for TLD .gr
hackerspace.gr
185.4.135.249
ns1.hackerspace.gr
ITE ns

Is it secure ?

- Opennic yes/no !
- DNS no !
- Any solutions ?
  - Some, like
    - dnssec/dane for auth-ns
    - dnscrypt for clients
  - Are you going to tell us something?
  - Yes, about dnscrypt !

dnscrypt

- Something to improve DNS security

- Current stable DNSCrypt **client** version: 1.6.0
  - dnscrypt-proxy
- Current stable DNSCrypt **server** version: 0.2.0
  - dnscrypt-wrapper

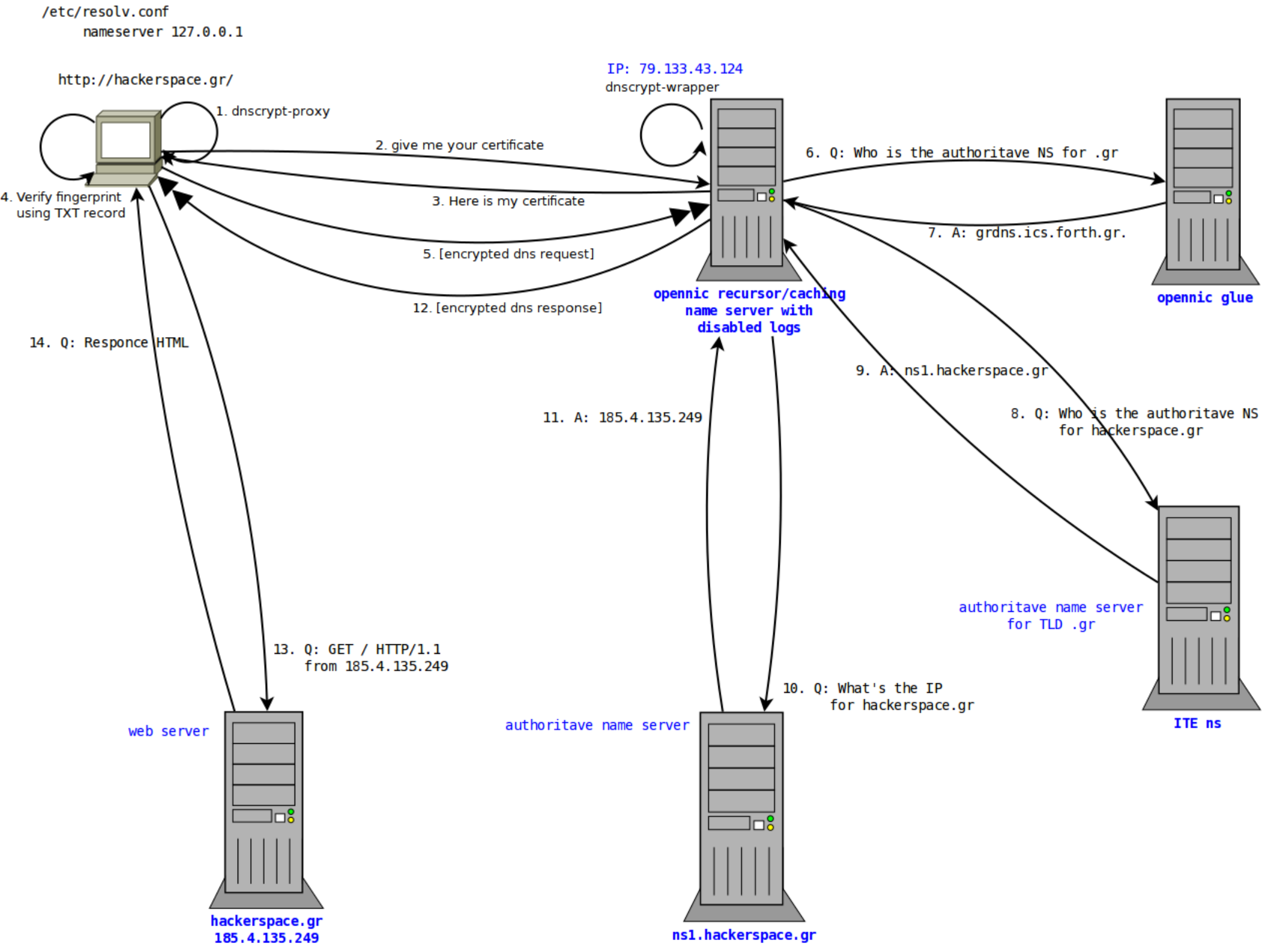
- DNSCrypt is a protocol that authenticates communications between a DNS client and a DNS resolver. It prevents DNS spoofing. It uses cryptographic signatures to verify that responses originate from the chosen DNS resolver and haven't been tampered with.

How does dnscrypt work?

- Certificate Authority - server's keys
- Time-limited service keys (signed-certificate)
- dnscrypt-wrapper (server)
  - Listen Address, eg. 0.0.0.0:5353
  - Remote Address, eg. 127.0.0.1:53
  - Keys, Certs
- 2.dnscrypt-cert.mydomain.tld (txt record) with server's fingerprint

How does dnscrypt work?

- dnscrypt-proxy (client)
- dns wrapper for resolving !
  - Server's IP
  - Server's fingerprint
  - Client verifies fingerprint with txt record
- 127.0.0.1 – localhost dns resolver !!
- can change to dnsmasq or other caching server


/etc/resolv.conf
nameserver 127.0.0.1
http://hackerspace.gr/
IP: 79.133.43.124
dnscrypt-wrapper
1. dnscrypt-proxy
2. give me your certificate
3. Here is my certificate
4. Verify fingerprint using TXT record
5. [encrypted dns request]
6. Q: Who is the authoritave NS for .gr
7. A: grdns.ics.forth.gr.
8. Q: Who is the authoritave NS for hackerspace.gr
9. A: ns1.hackerspace.gr
10. Q: What's the IP for hackerspace.gr
11. A: 185.4.135.249
12. [encrypted dns response]
13. Q: GET / HTTP/1.1 from 185.4.135.249
14. Q: Responce HTML
opennic recursor/caching name server with disabled logs
opennic glue
authoritave name server for TLD .gr
ITE ns
authoritave name server
ns1.hackerspace.gr
web server
hackerspace.gr
185.4.135.249

Questions ?