Understanding the Privacy Implications of ECS

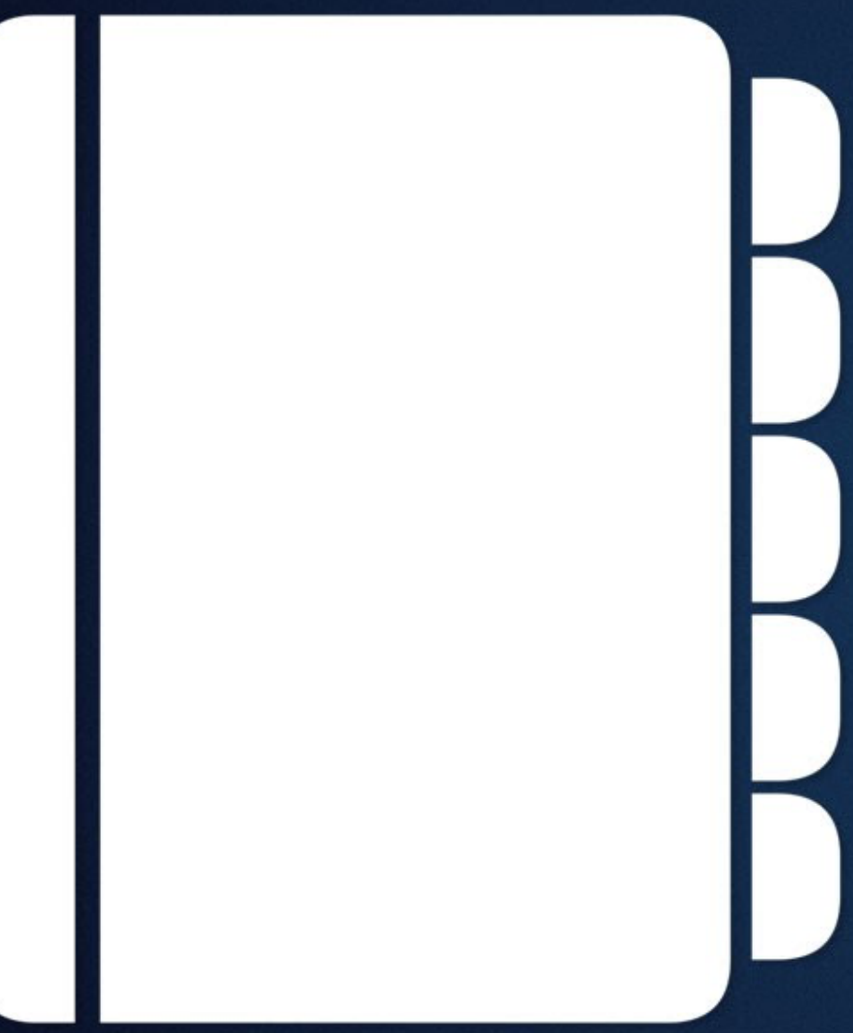
Panagiotis Kintis, Yacin Nadji, David Dagon, Michael Farrell, and Manos Antonakakis

Outline

- Introduction
- Domain Name System
- EDNS Client Subnet
- Surveillance
- Selective DNS Cache Poisoning
- Remedies

Introduction

- Some more data added into a DNS packet
- Recursives share information about the client with the authorities
- Potential new attacks appear
- Not possible to avoid the implications



Domain Name System

The Domain Name System

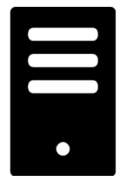
Client

Recursive
DNS Server

root

.com

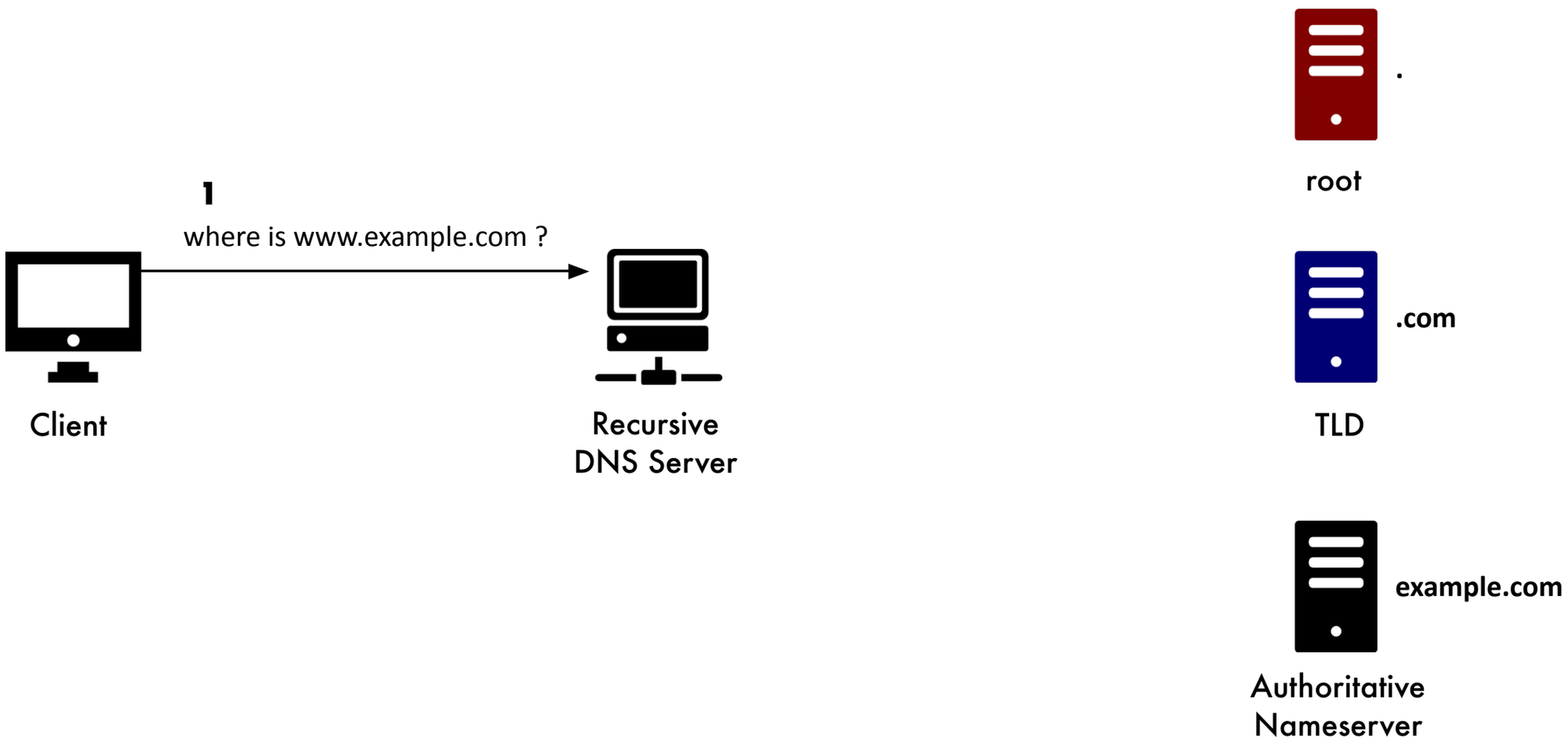
TLD



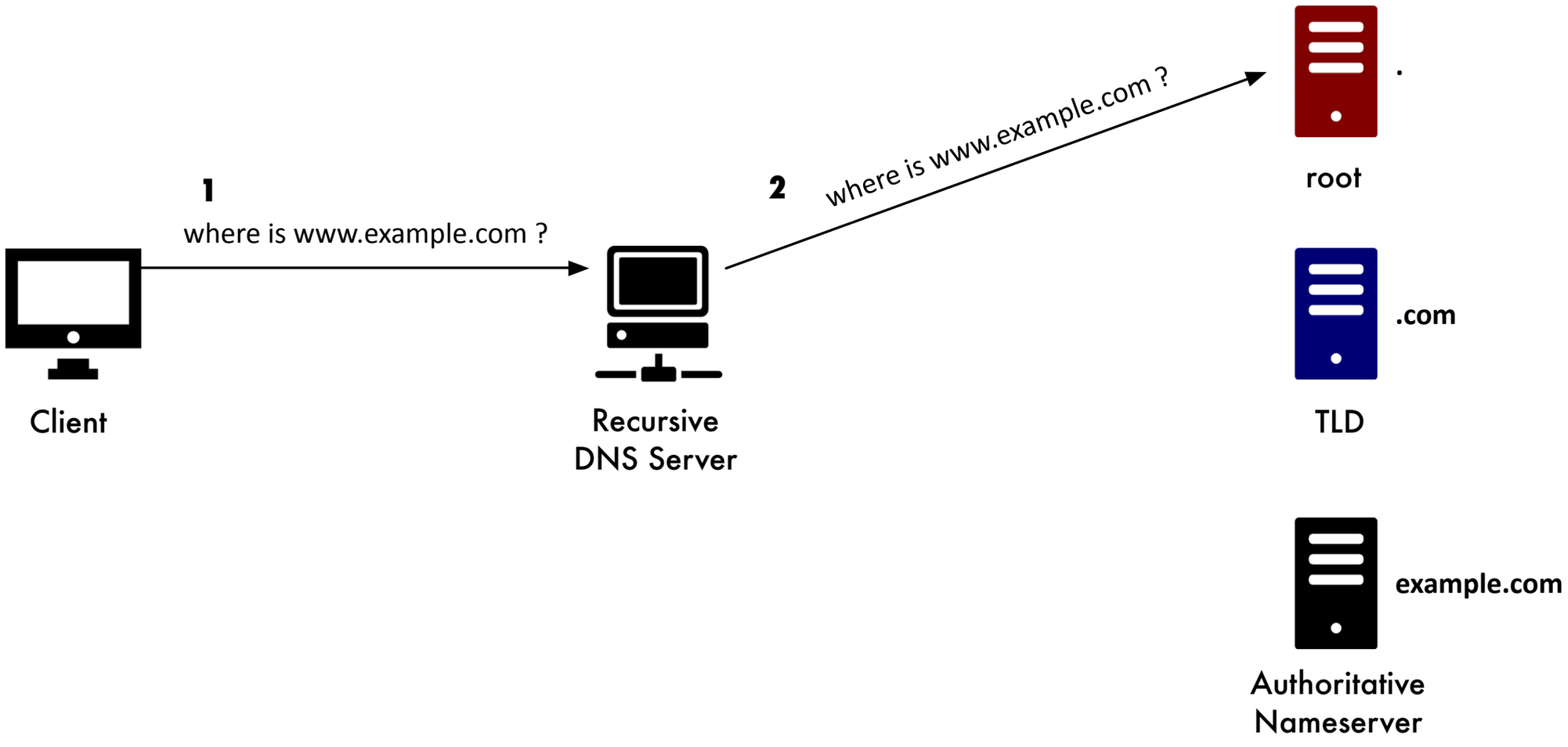
example.com

Authoritative
Nameserver

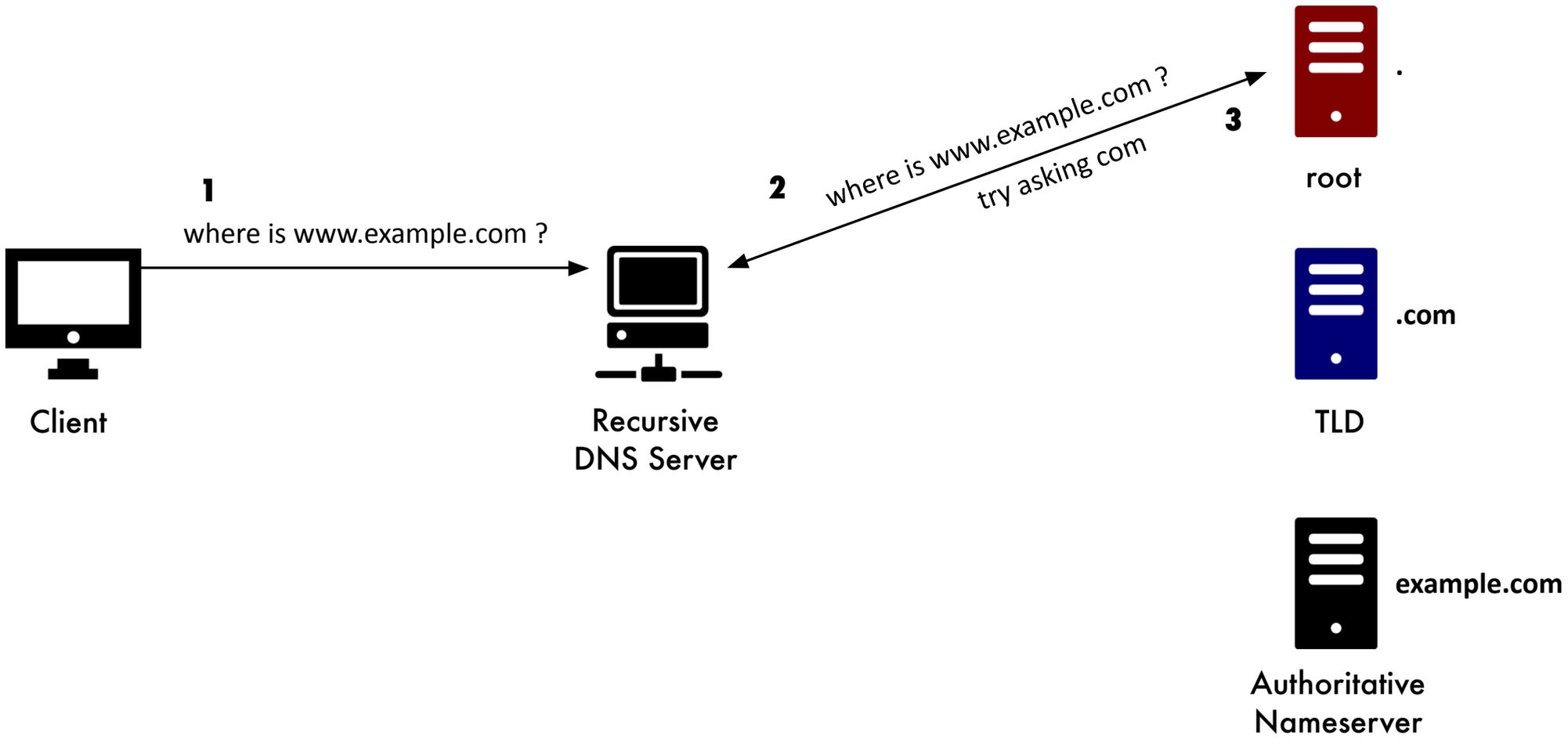
The Domain Name System



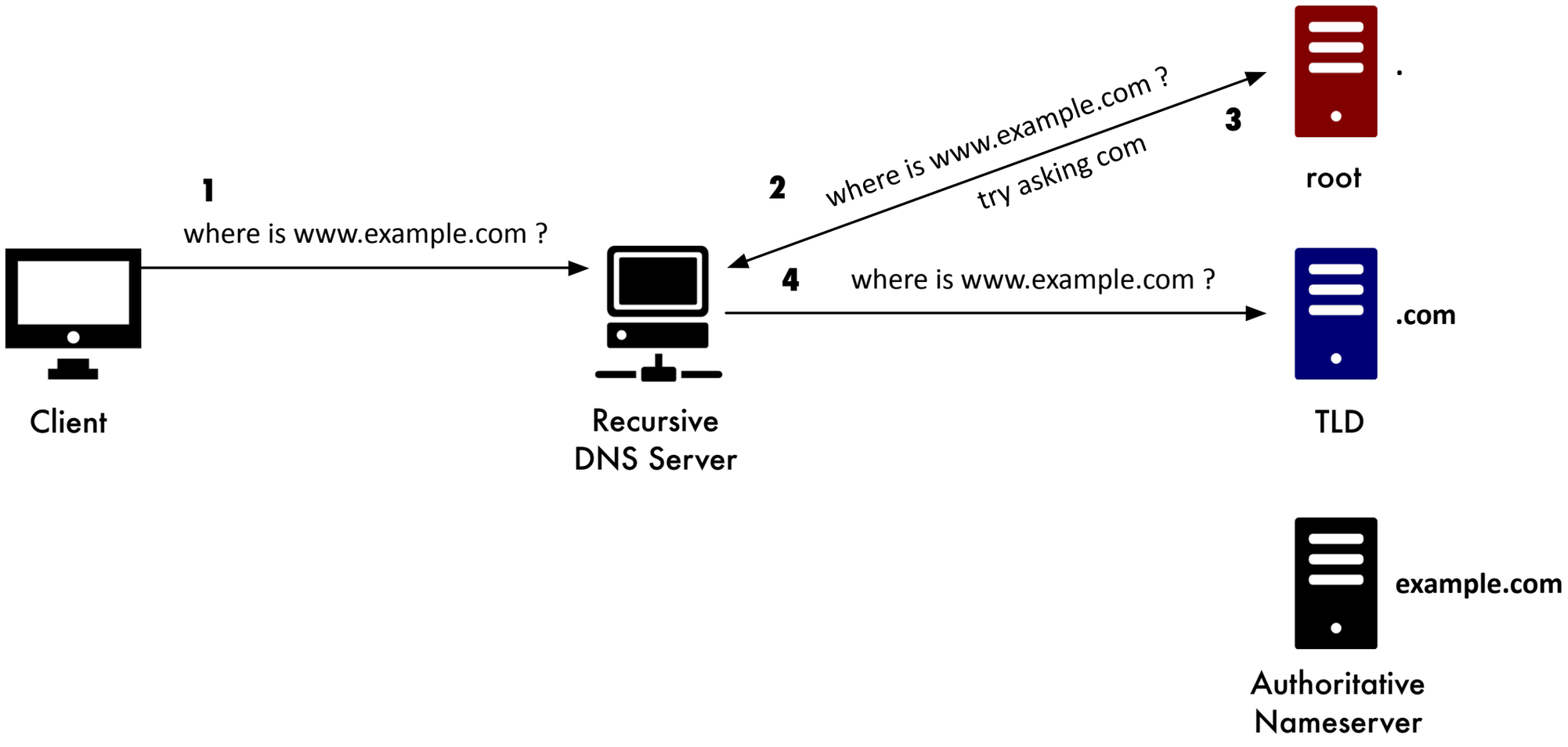
The Domain Name System



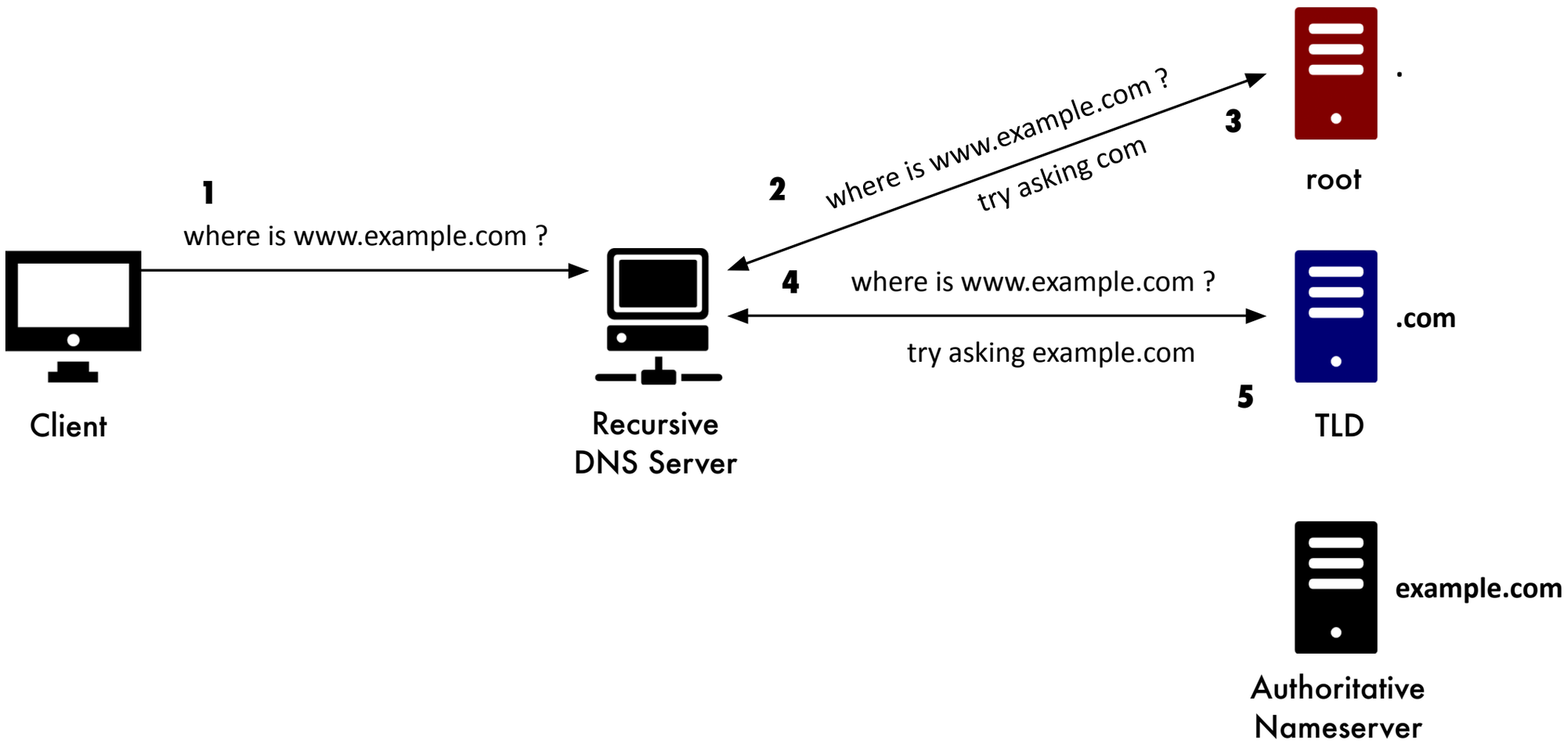
The Domain Name System



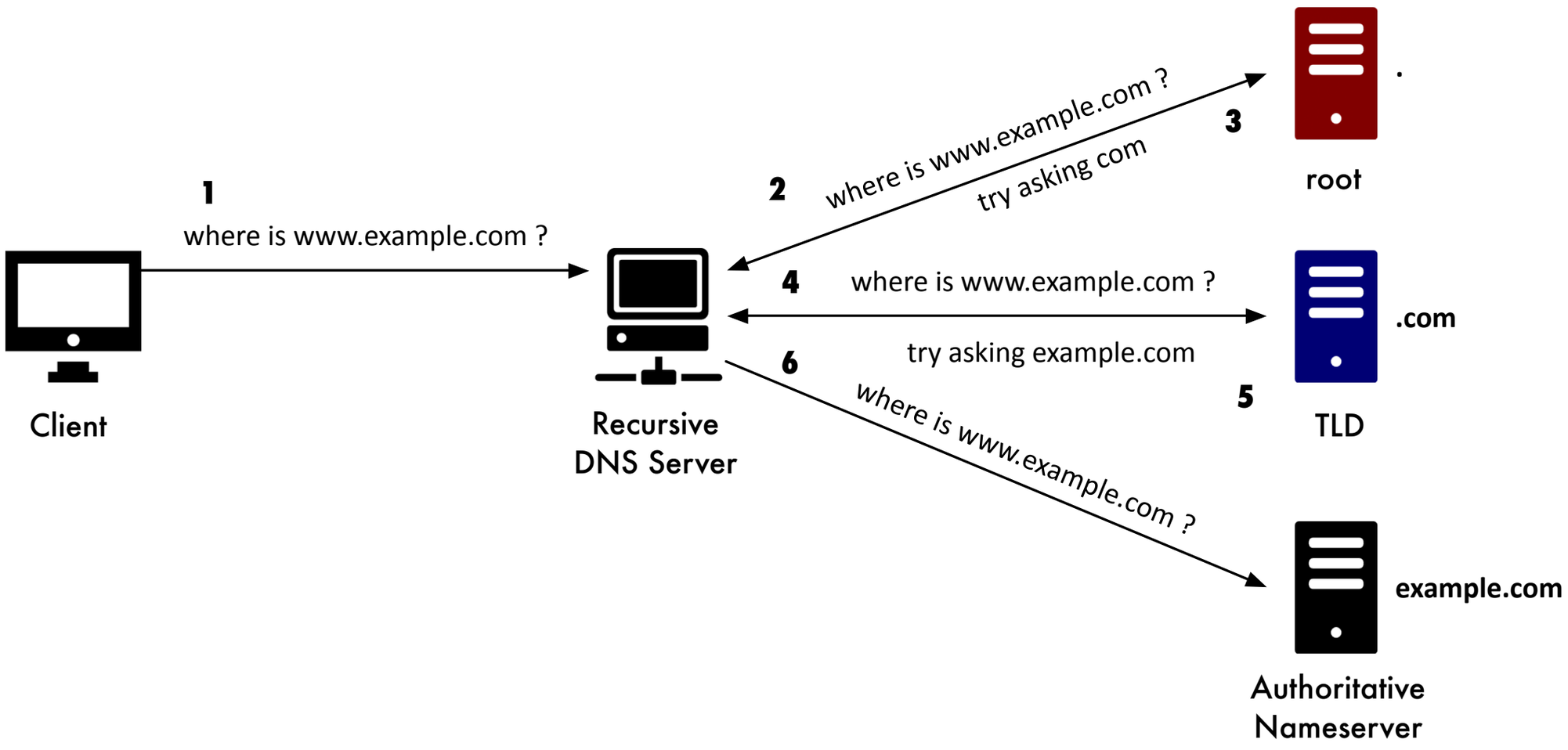
The Domain Name System



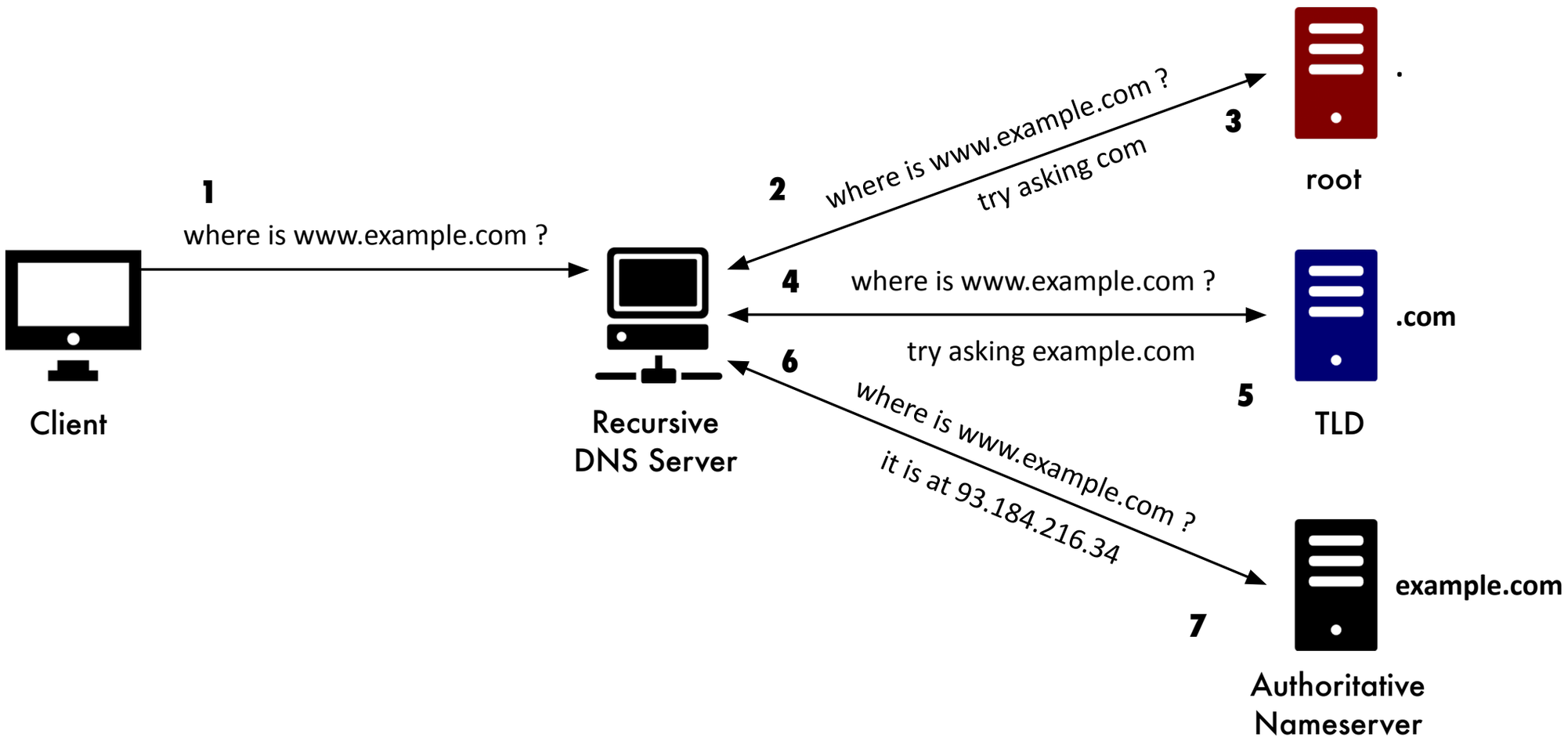
The Domain Name System



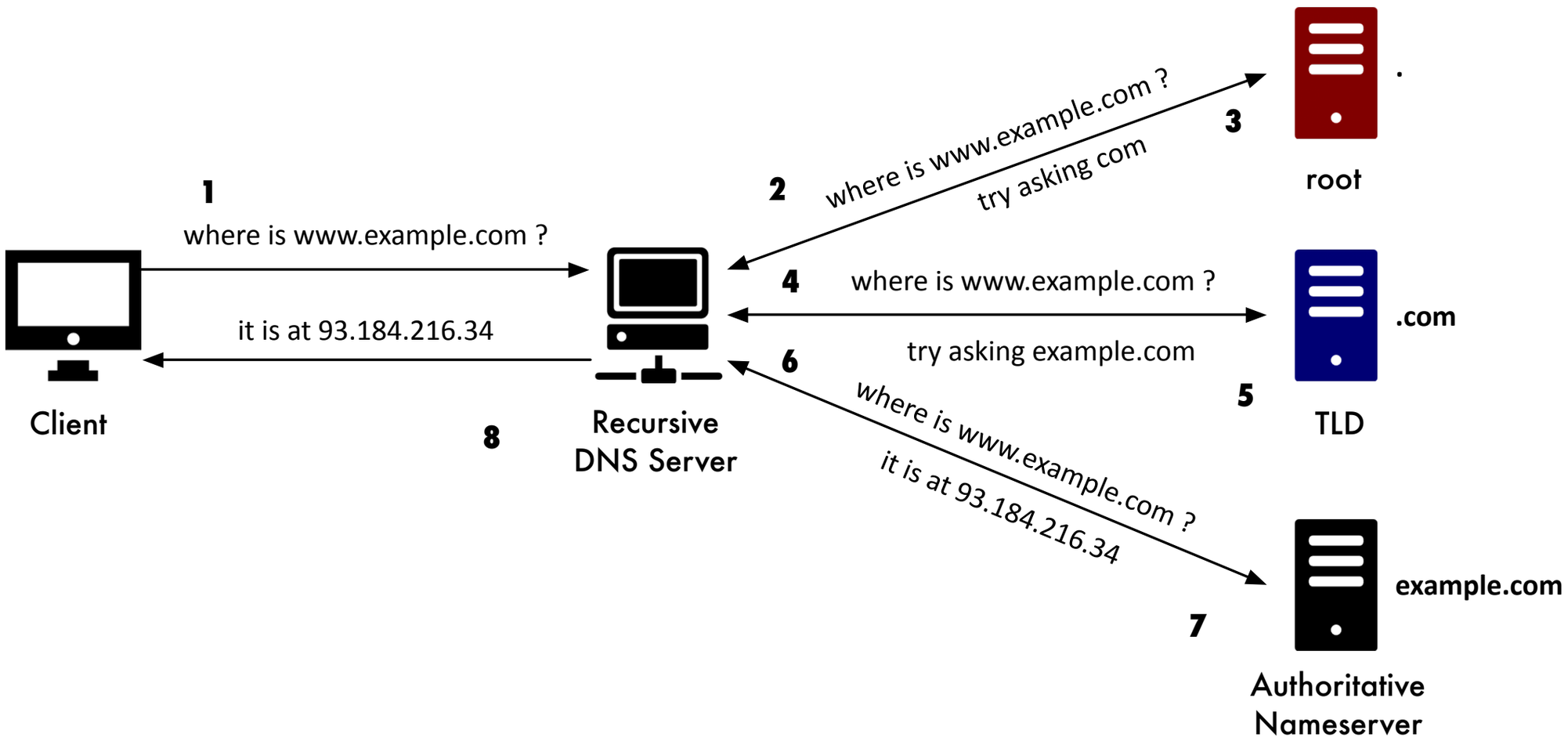
The Domain Name System



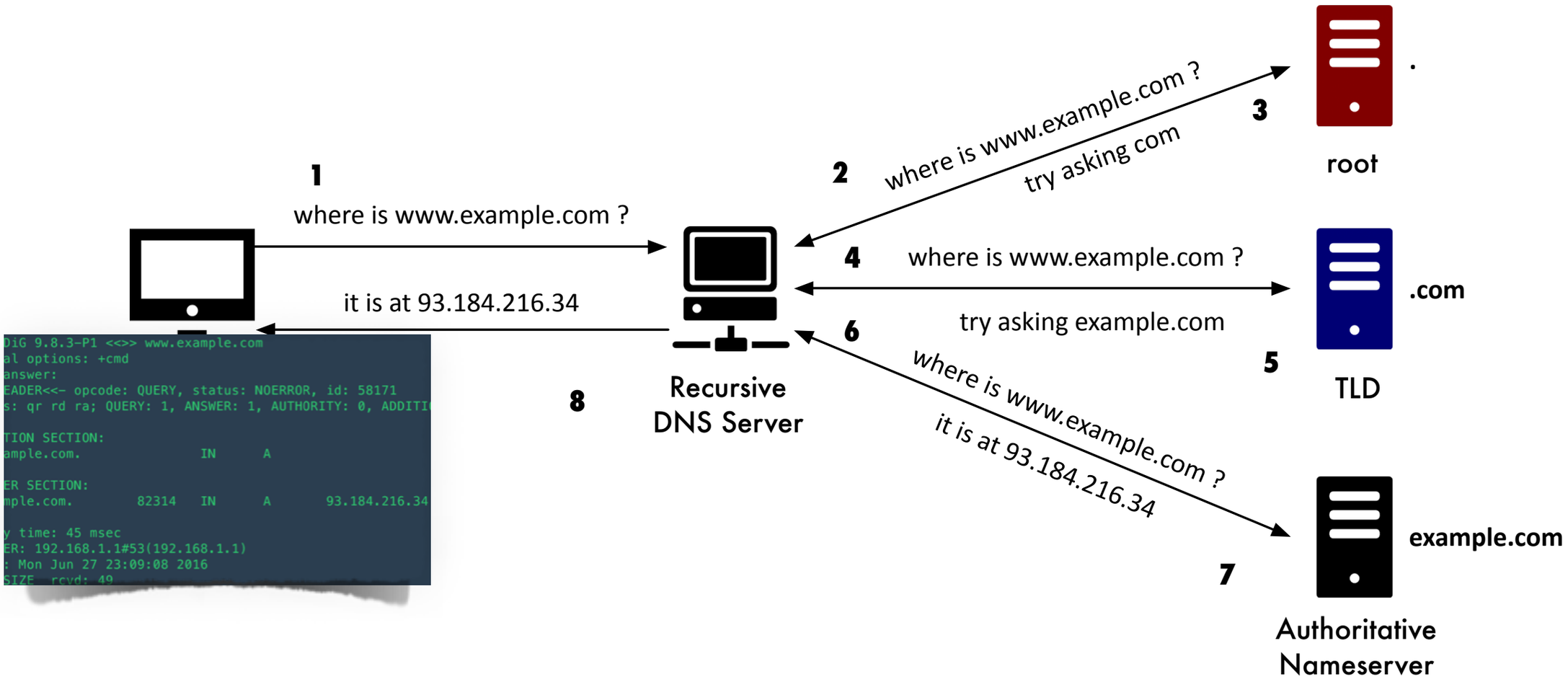
The Domain Name System



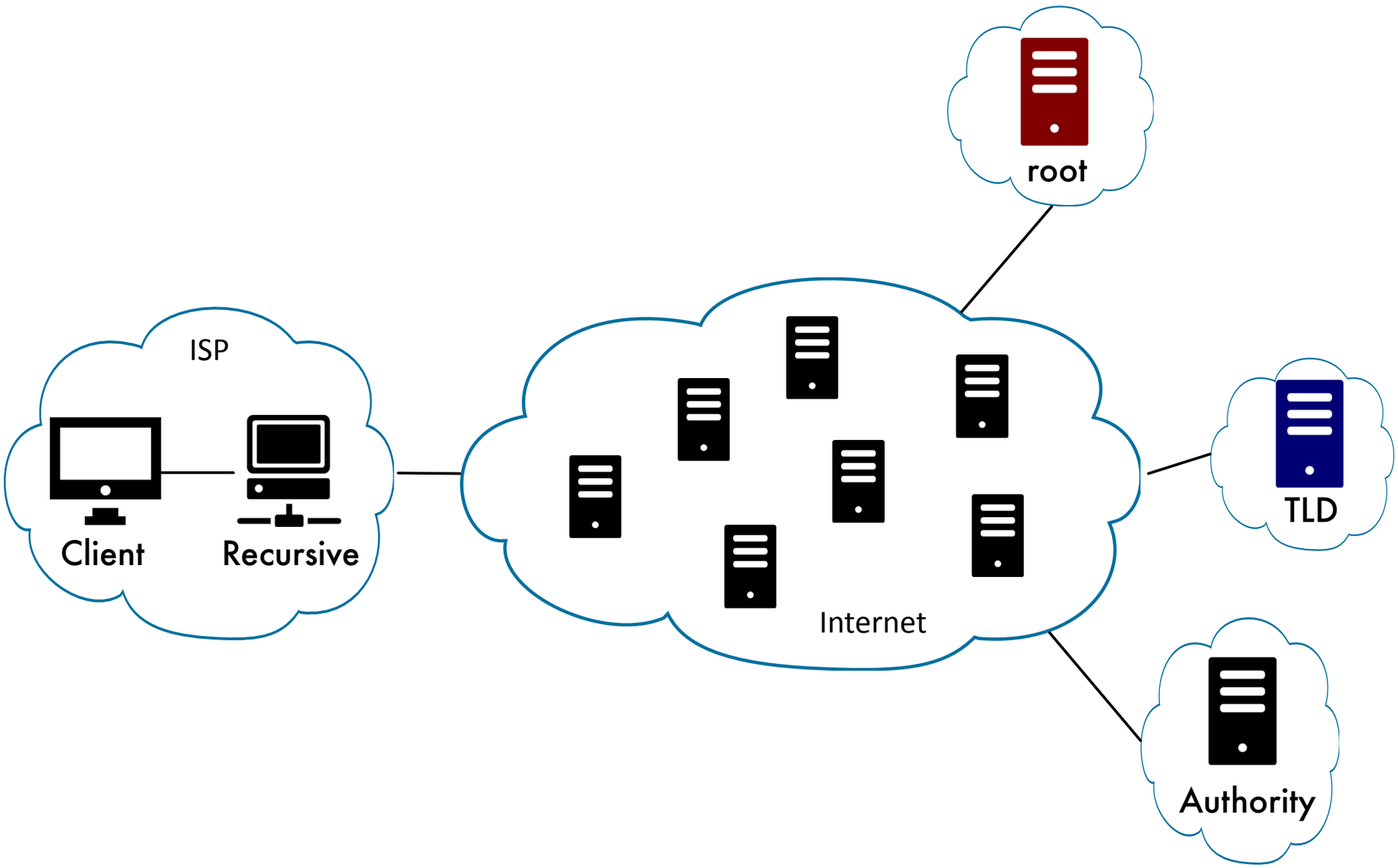
The Domain Name System



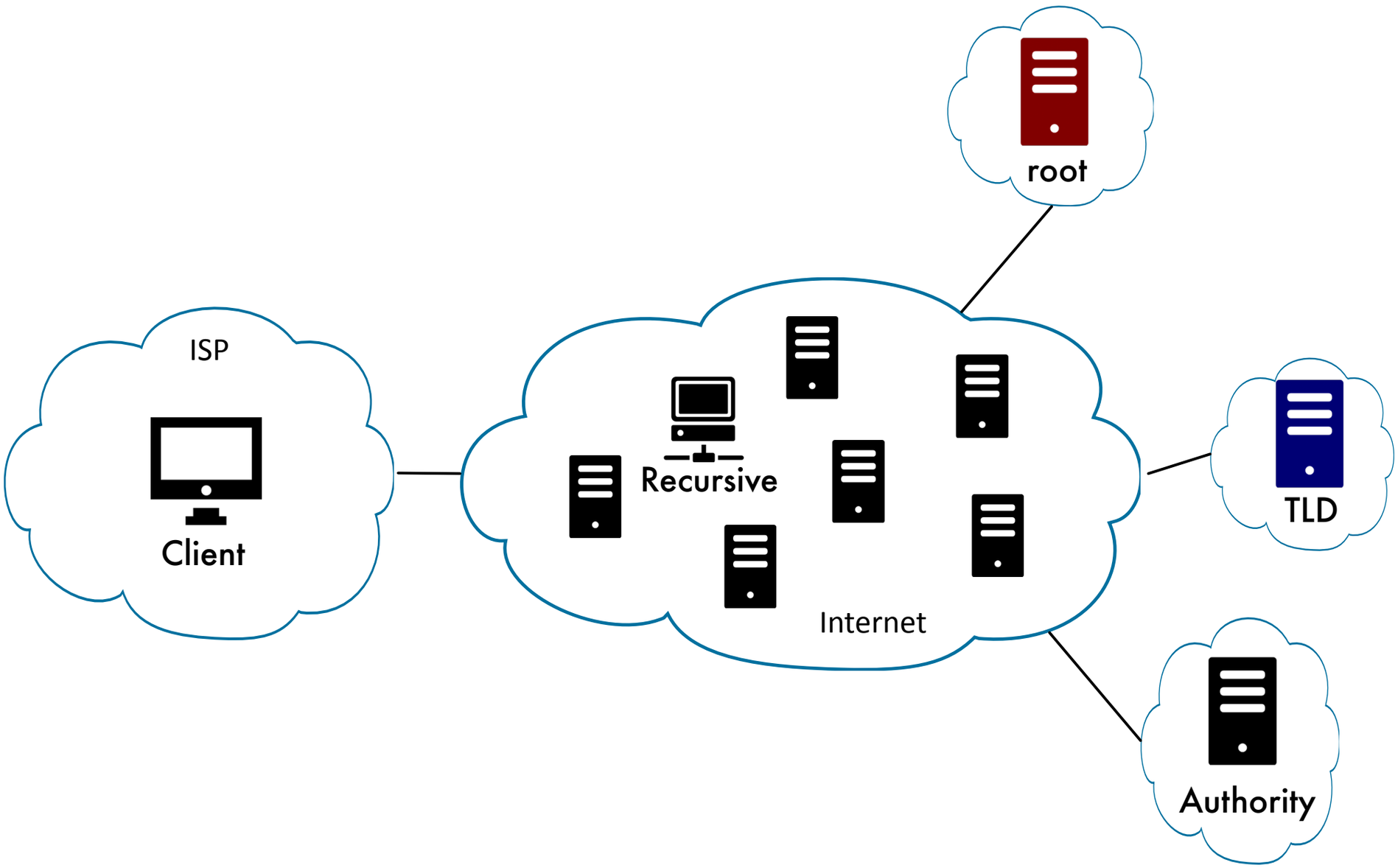
The Domain Name System

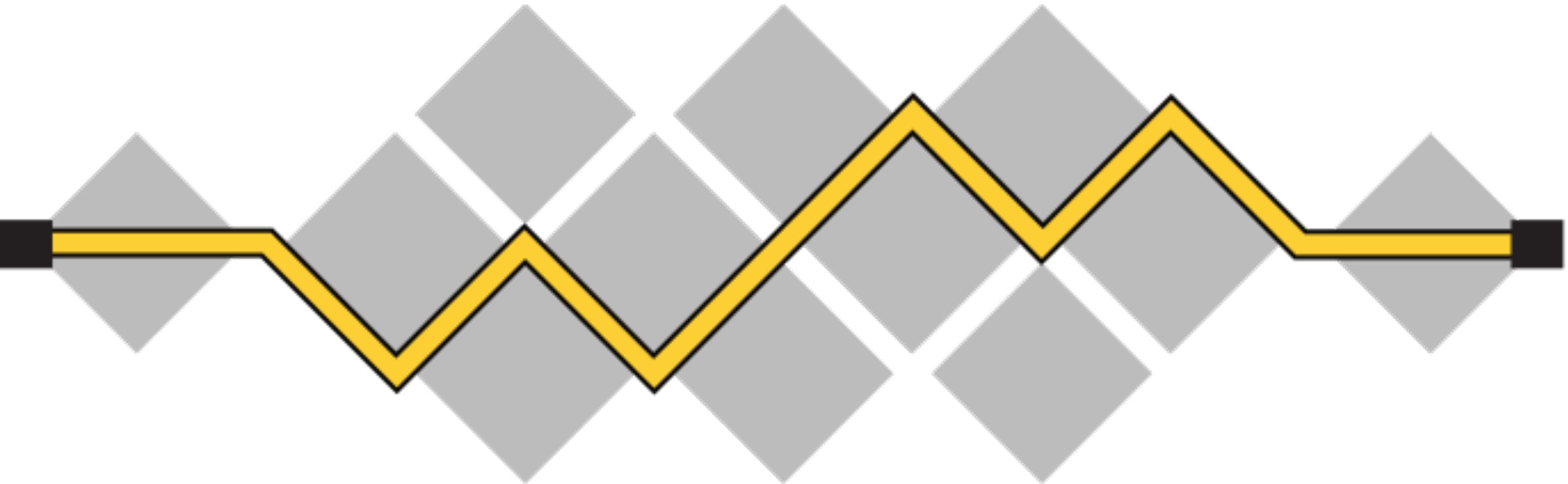


Slightly Larger



Operationally Slightly Different





IETF®

Domain Resolution

Domain Resolution

195.251.97.20 (GR)

Recursive

ns1.google.com.

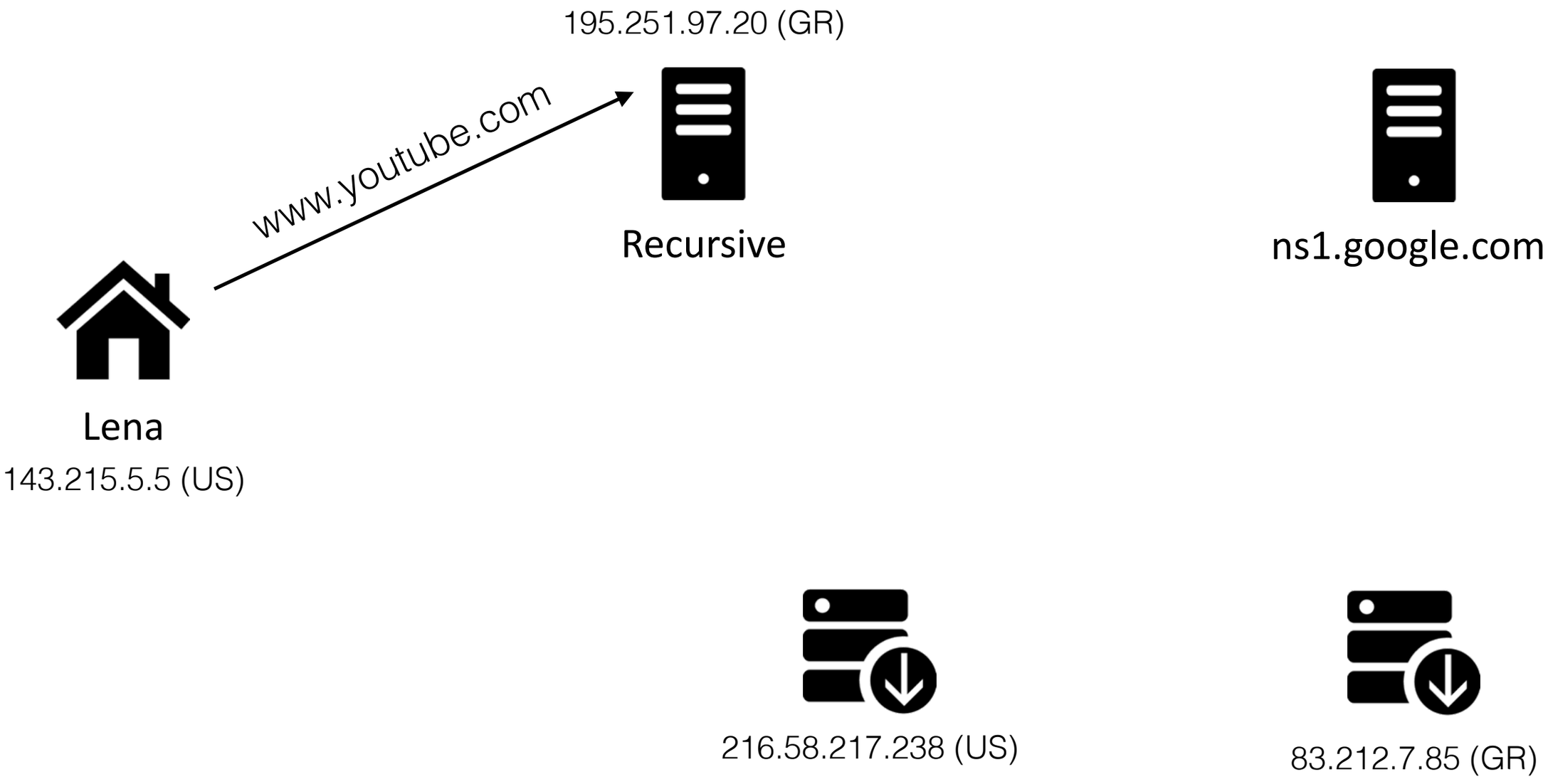
Lena

143.215.5.5 (US)

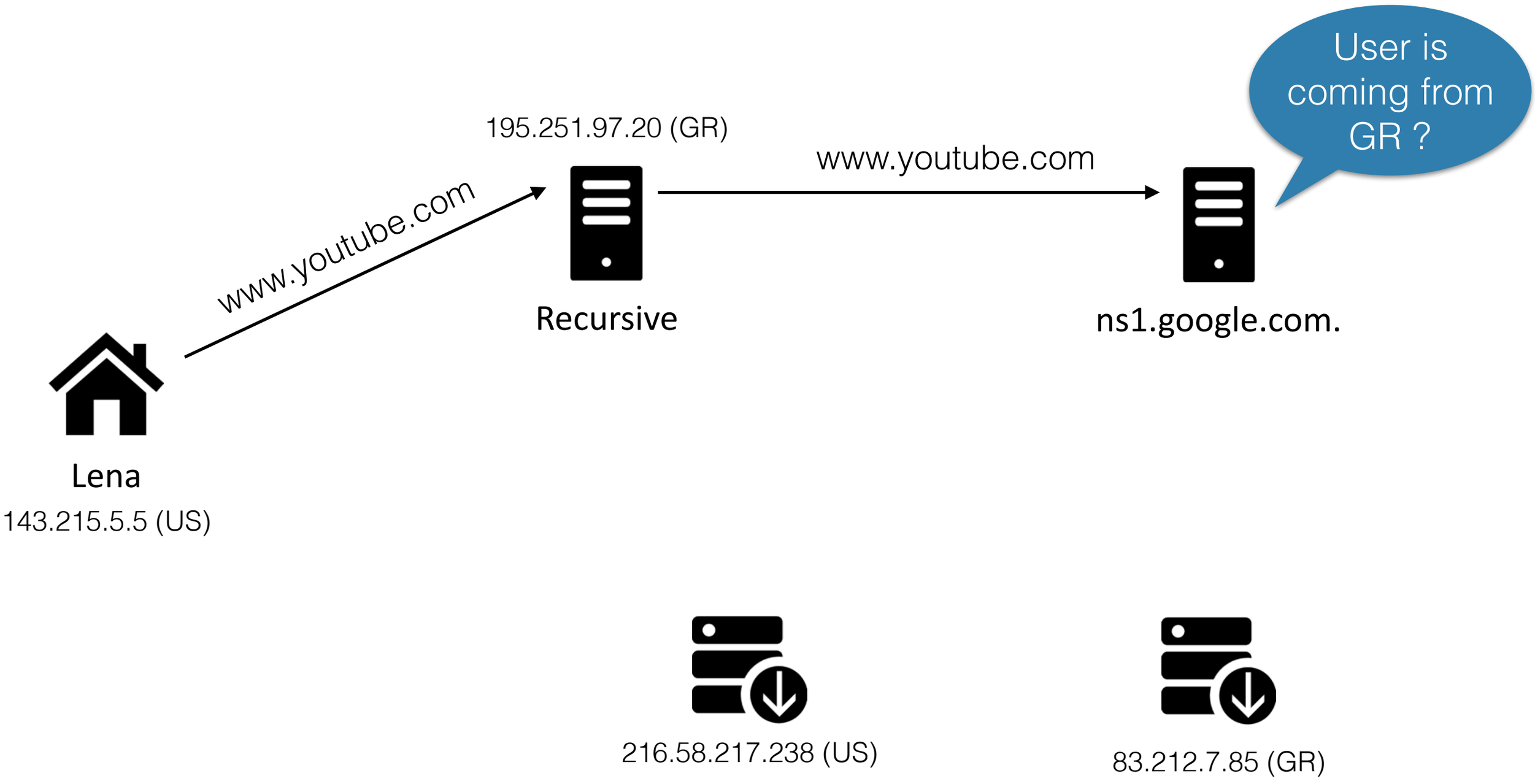
216.58.217.238 (US)

83.212.7.85 (GR)

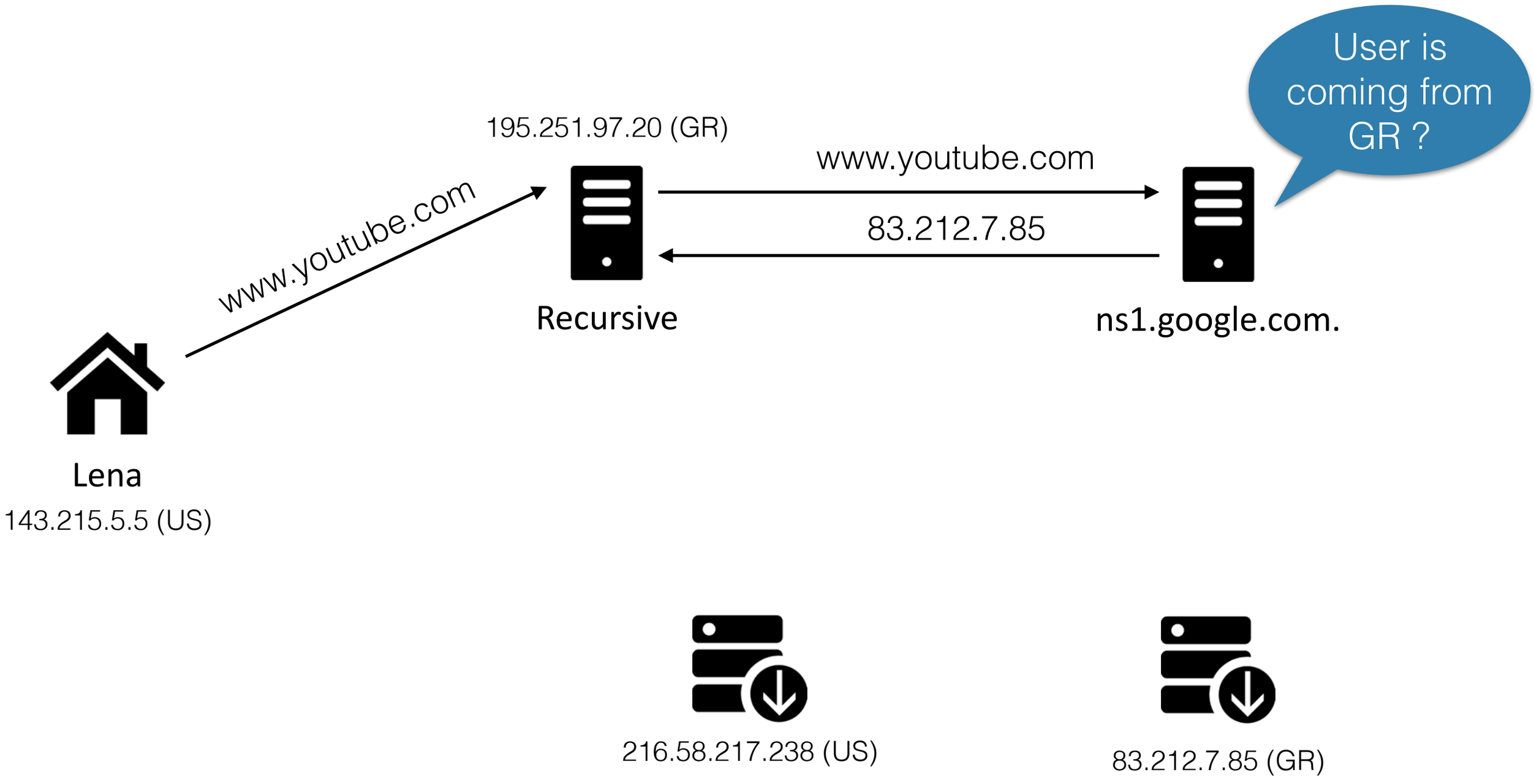
Domain Resolution



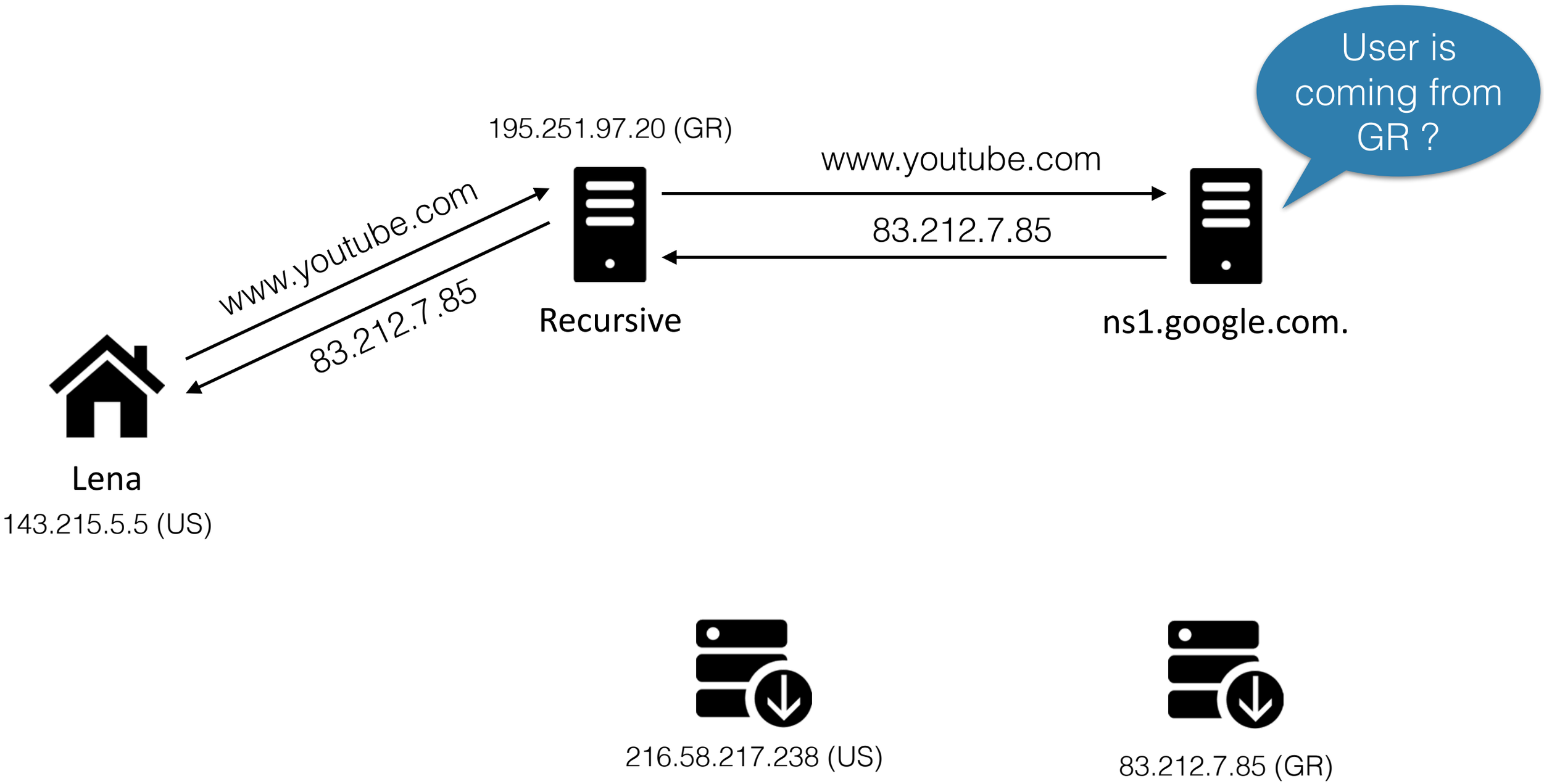
Domain Resolution



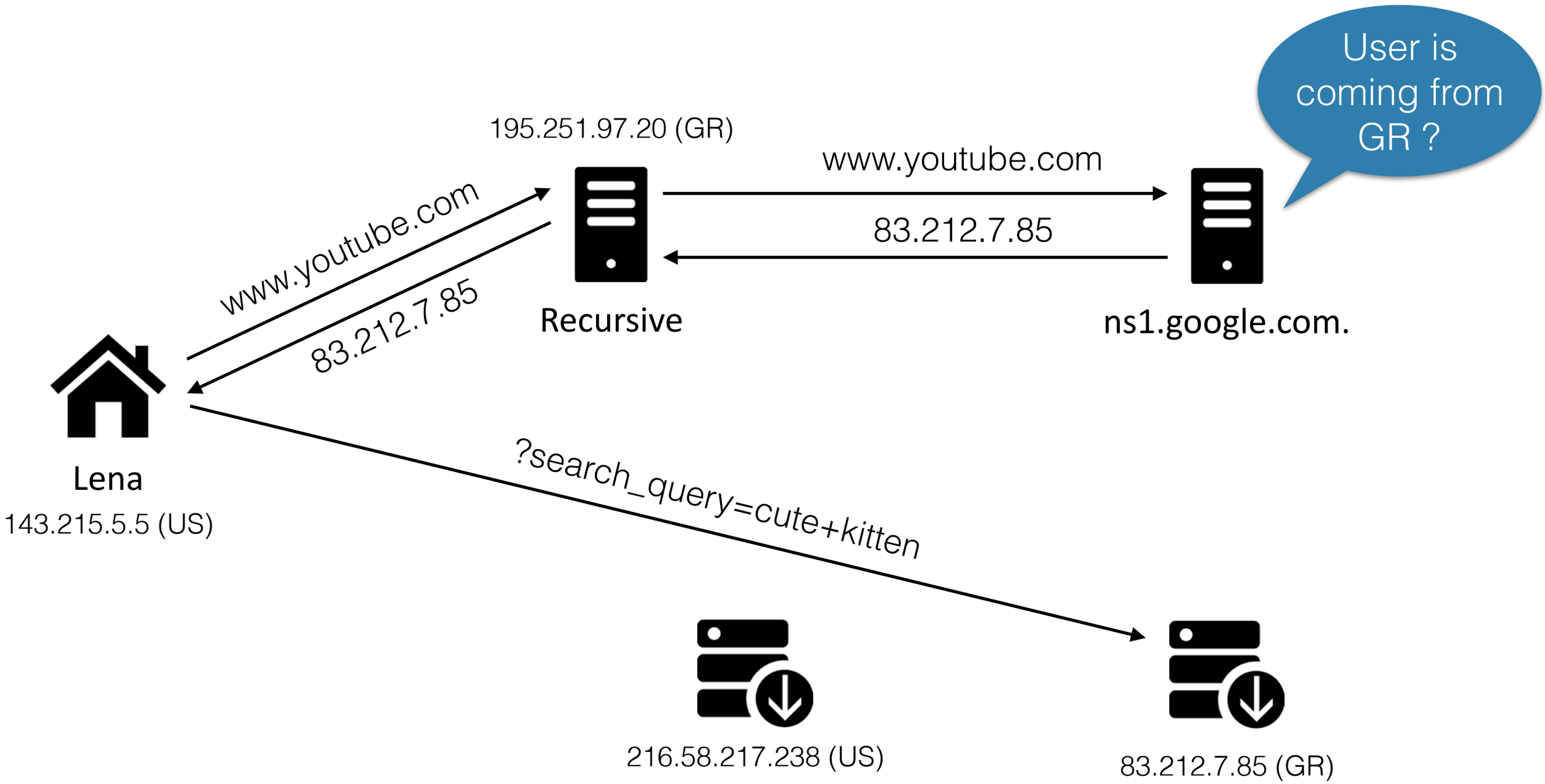
Domain Resolution



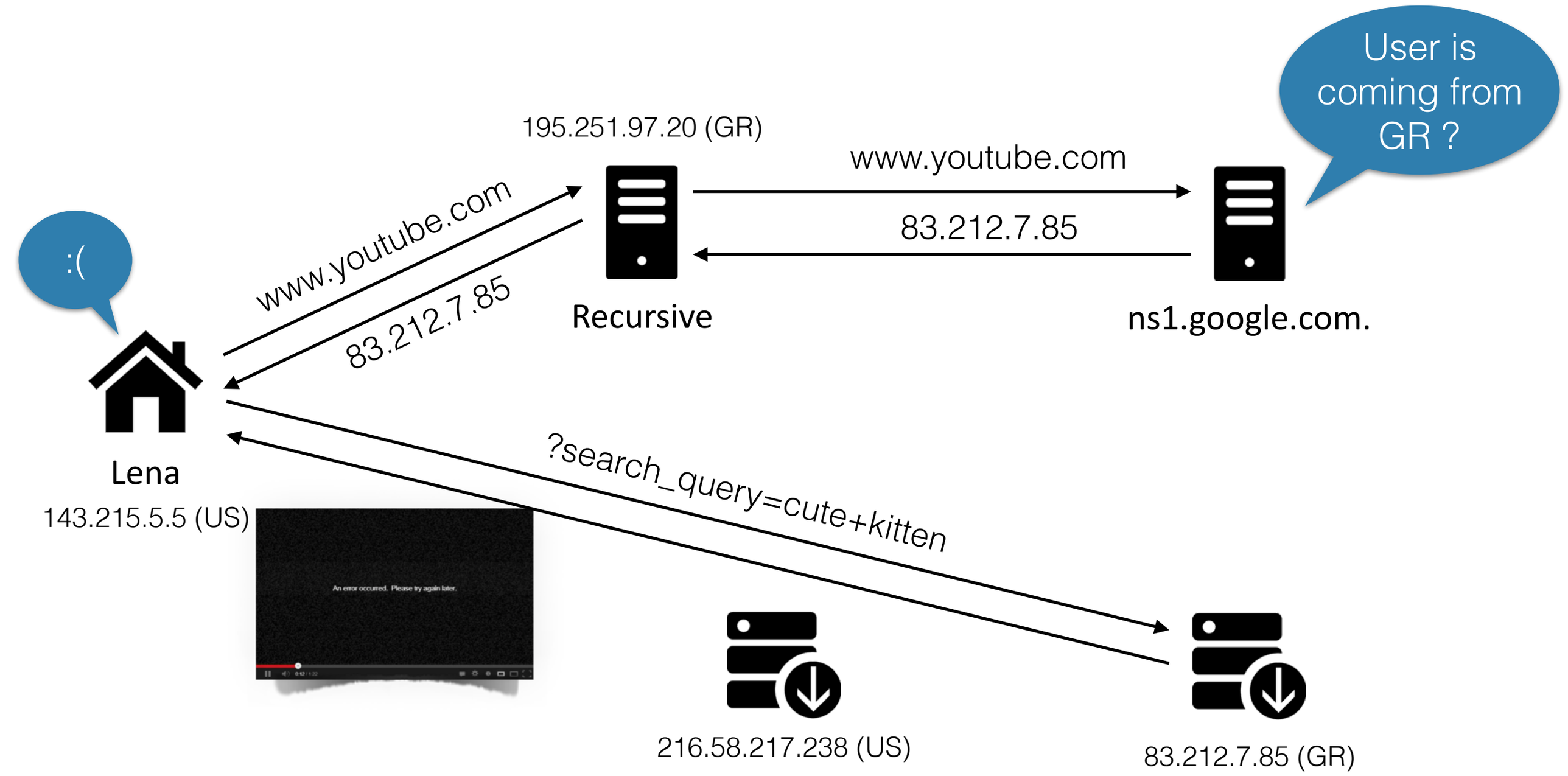
Domain Resolution



Domain Resolution



Domain Resolution



ECS Enabled Request

ECS Enabled Request

195.251.97.20 (GR)

Recursive

ns1.google.com.

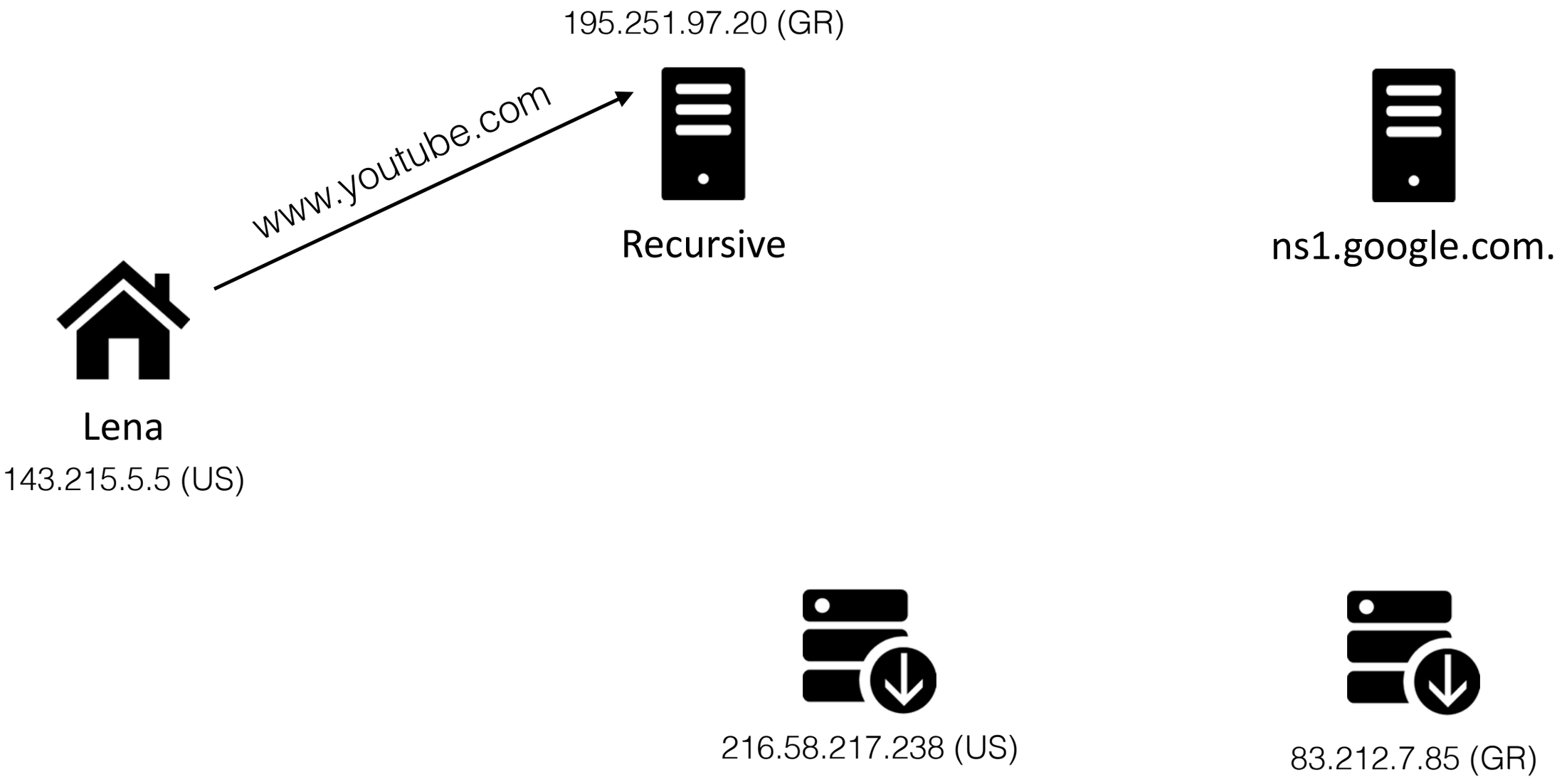
Lena

143.215.5.5 (US)

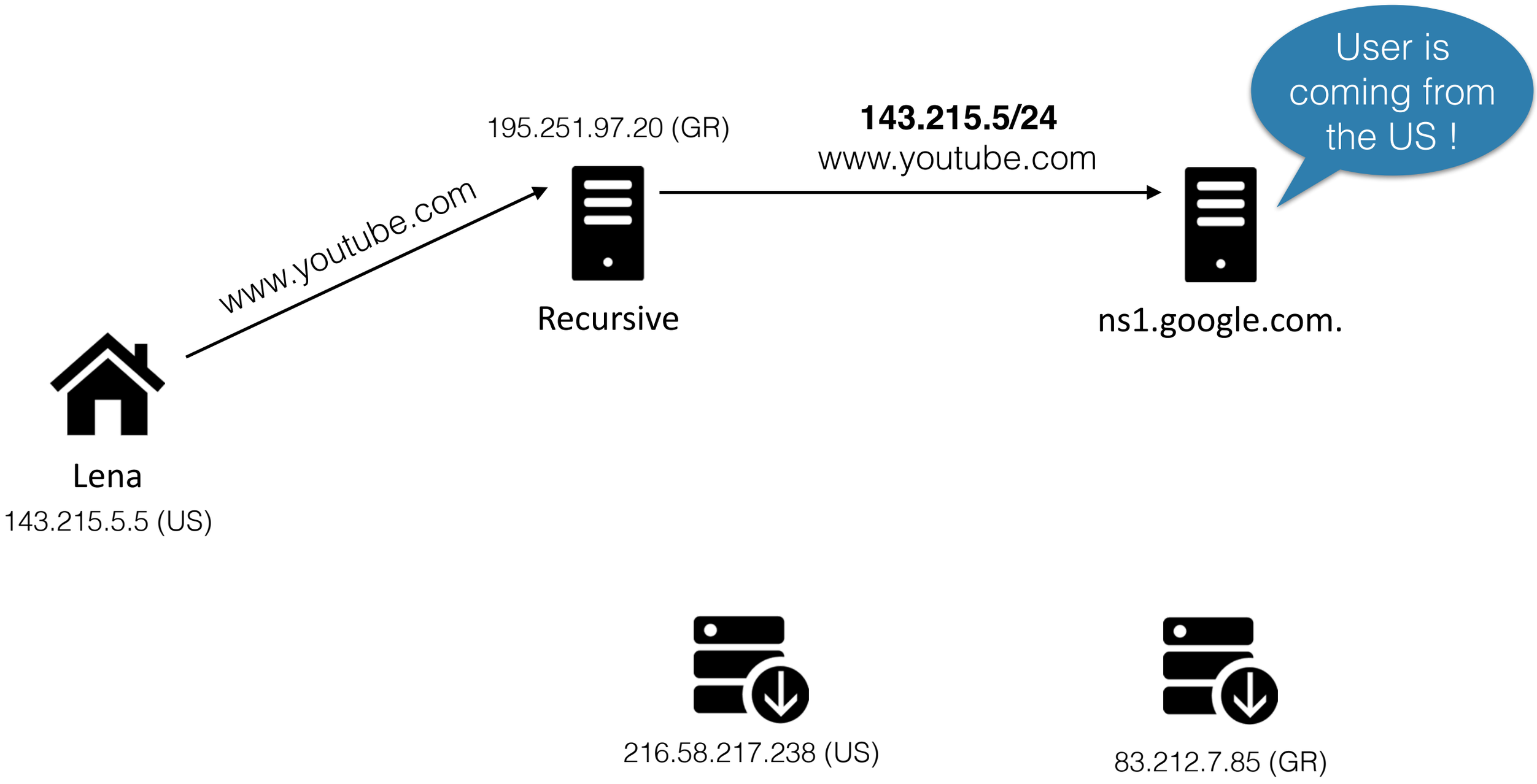
216.58.217.238 (US)

83.212.7.85 (GR)

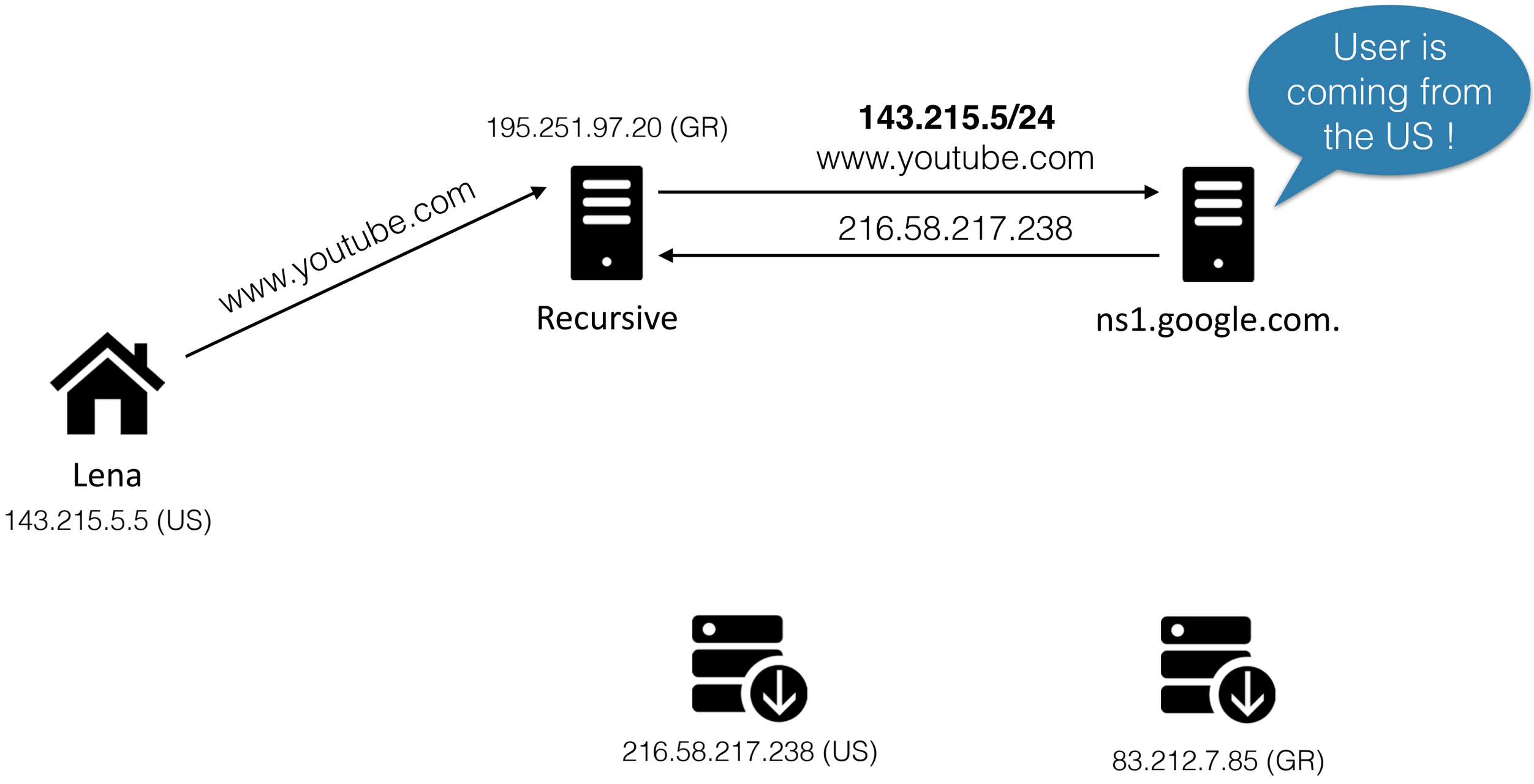
ECS Enabled Request



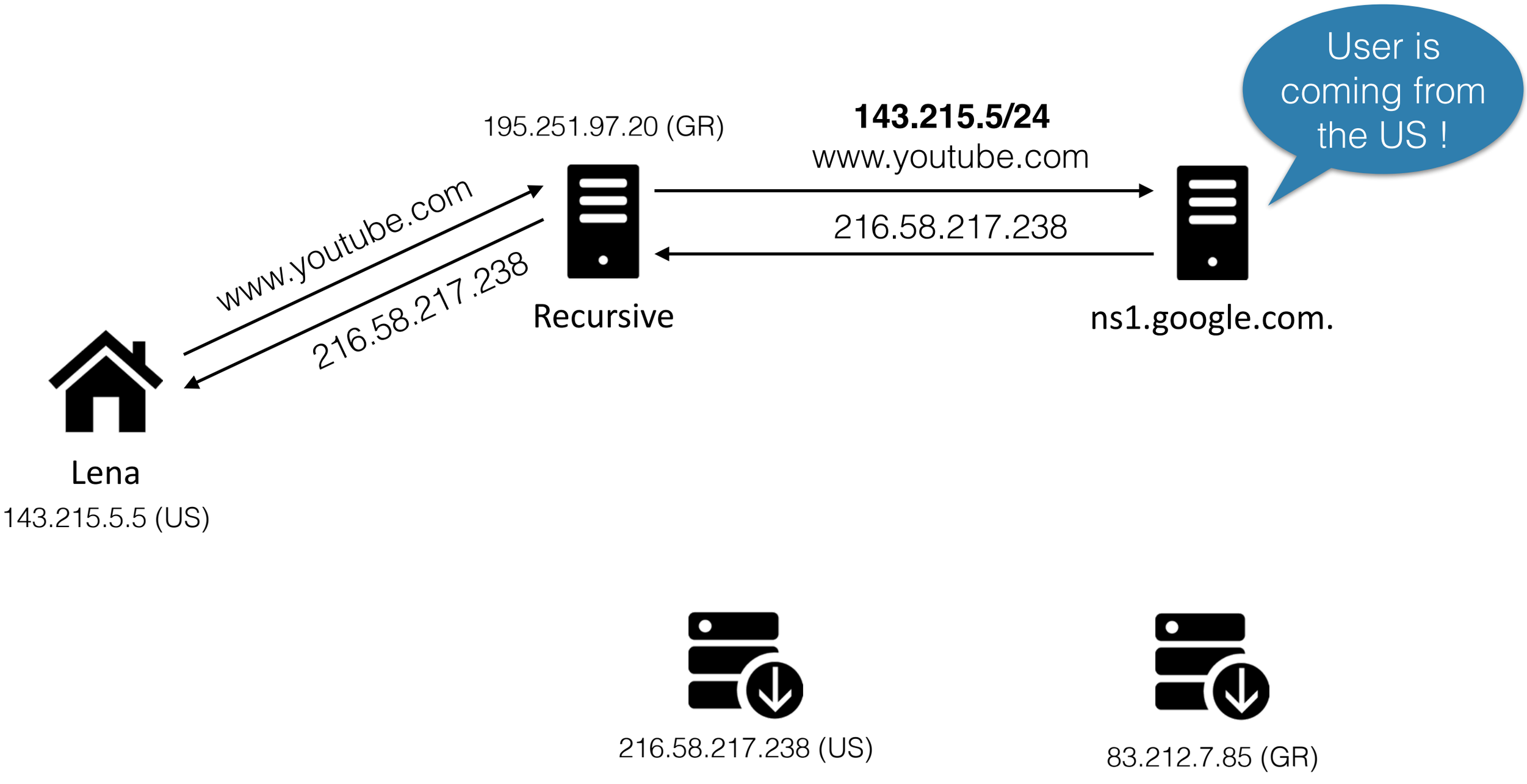
ECS Enabled Request



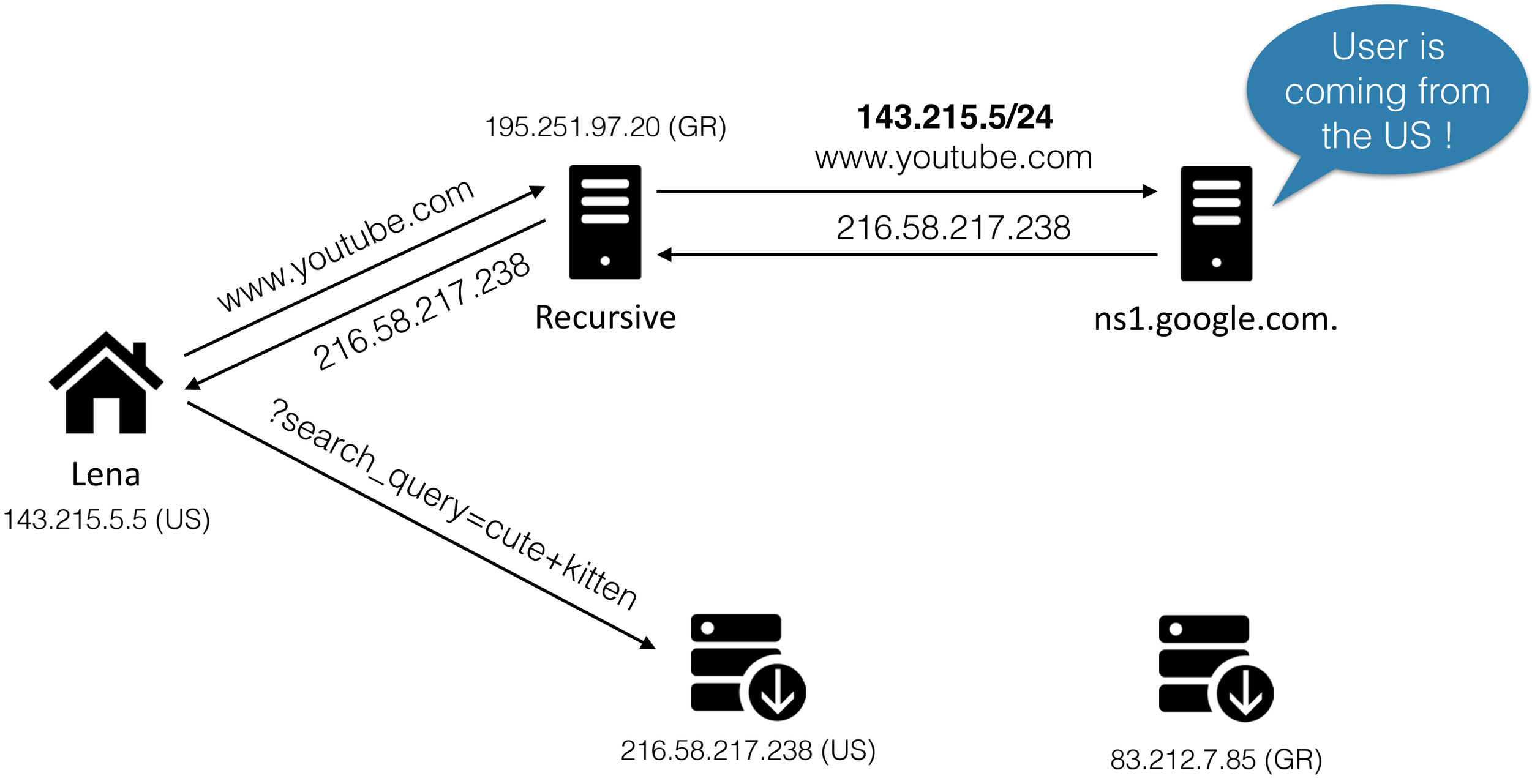
ECS Enabled Request



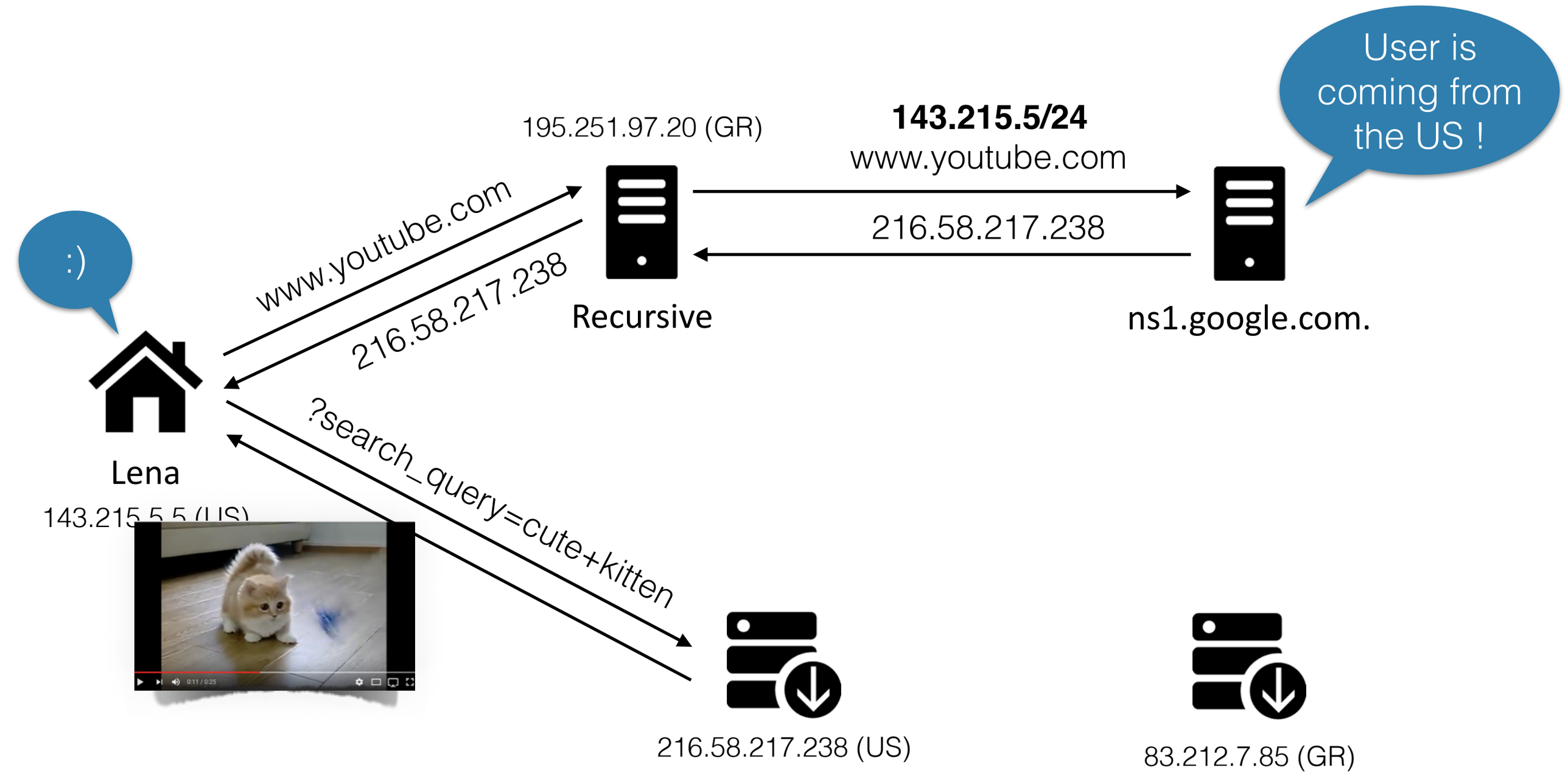
ECS Enabled Request

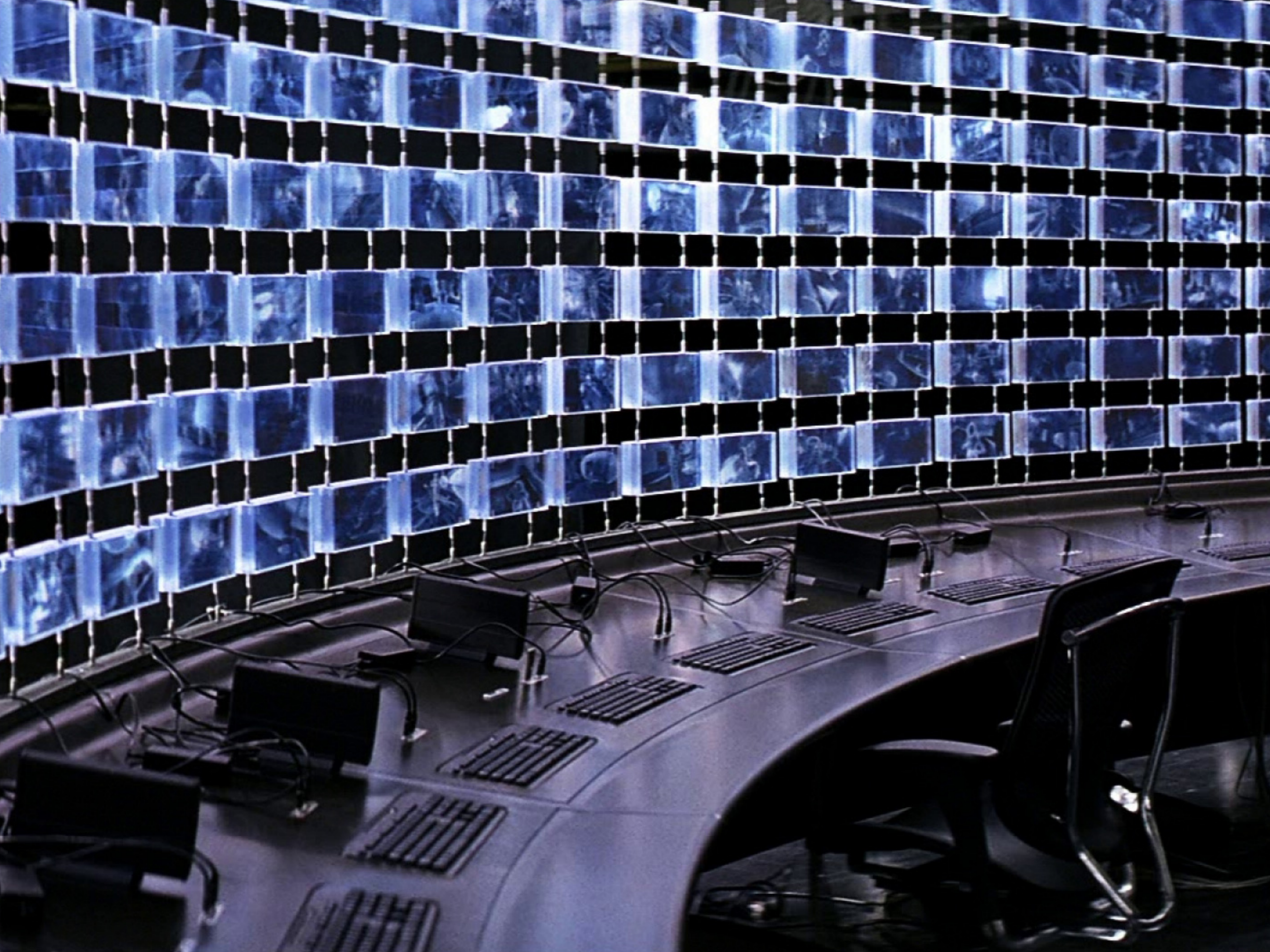


ECS Enabled Request



ECS Enabled Request





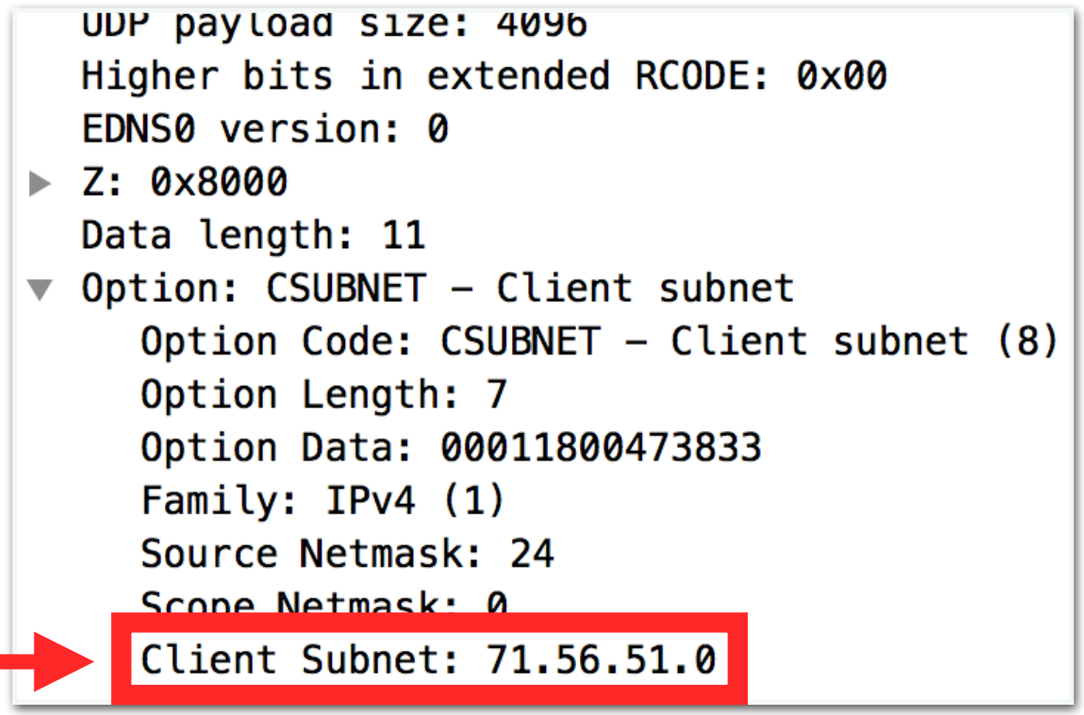
EDNS Client Subnet Payload

- The EDNS0 part of a DNS packet includes 5 fields
  - Option Code
  - IP Family
  - Scope Netmask
  - Source Netmask
  - *Client Subnet*

```
UDP payload size: 4096
Higher bits in extended RCODE: 0x00
EDNS0 version: 0
▶ Z: 0x8000
Data length: 11
▼ Option: CSUBNET – Client subnet
    Option Code: CSUBNET – Client subnet (8)
    Option Length: 7
    Option Data: 00011800473833
    Family: IPv4 (1)
    Source Netmask: 24
    Scope Netmask: 0
    Client Subnet: 71.56.51.0
```

EDNS Client Subnet Payload

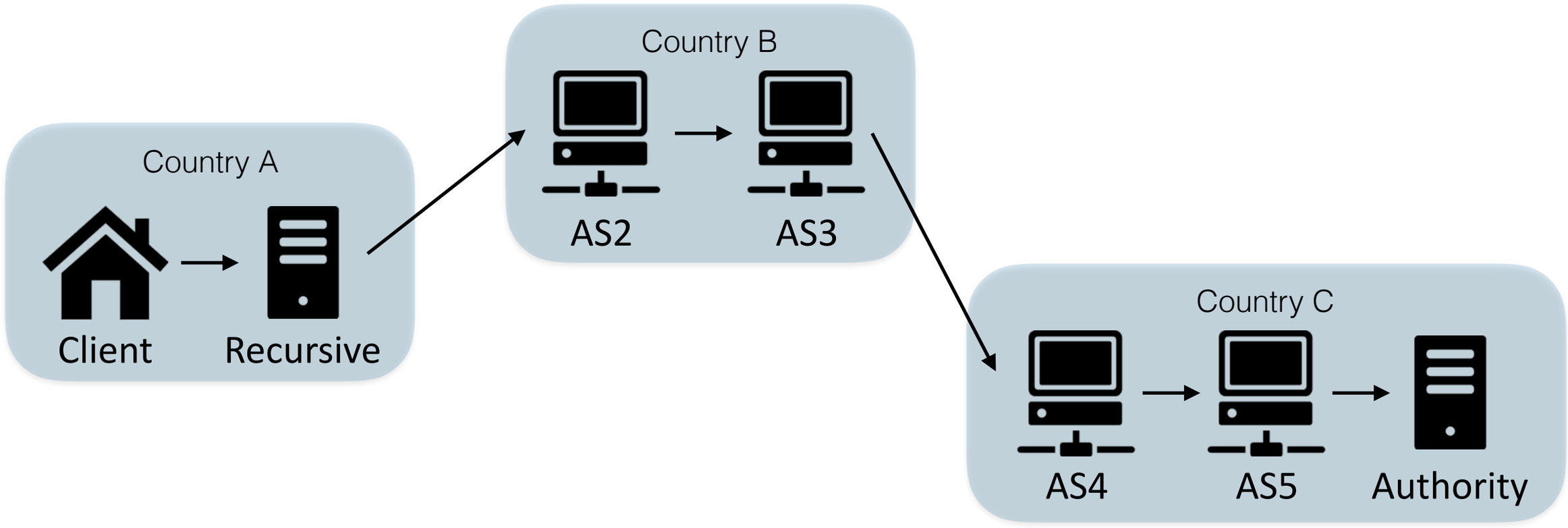
- The EDNS0 part of a DNS packet includes 5 fields
  - Option Code
  - IP Family
  - Scope Netmask
  - Source Netmask
  - *Client Subnet*



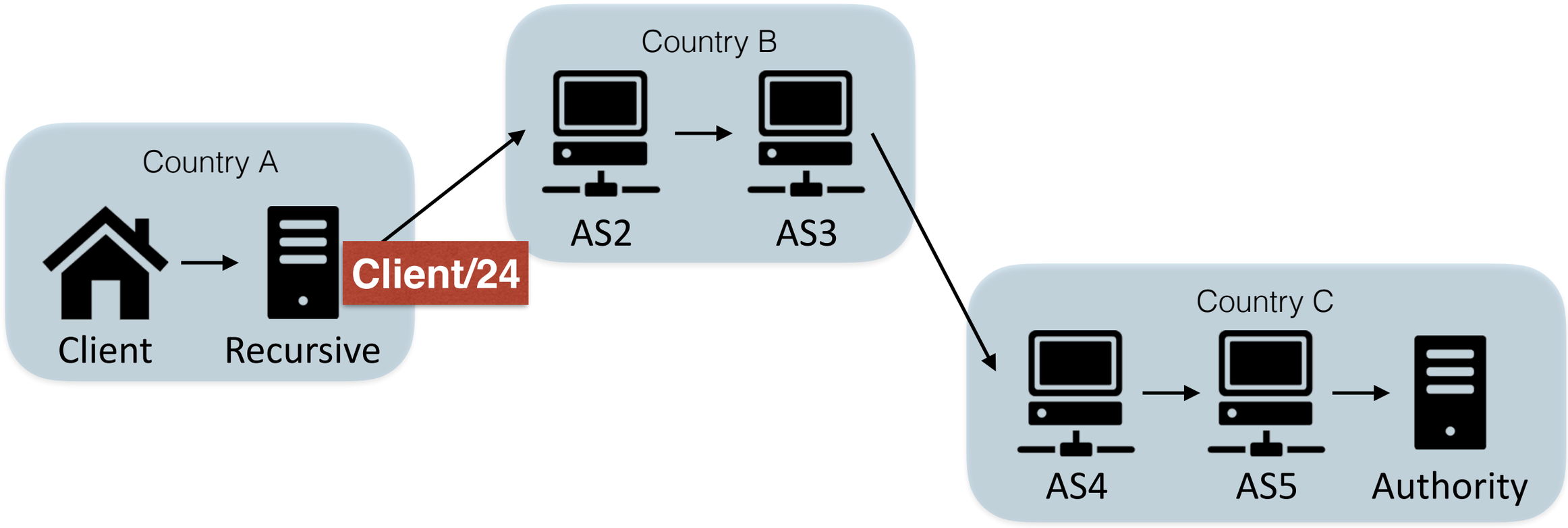
Surveillance Options

- DNS is really easy to monitor
  - Recall the Great Firewall of China
  - Recall the Twitter block in Turkey
  - Recall Turkey BGP hijack of 8.8.8.8, 208.67.222.222, 4.2.2.2
- The Class-C (/24) of a network is visible on-path
- Any Autonomous System between the recursive and the authority can monitor client requests
- A regime can see the clients resolving domains hosted within its country

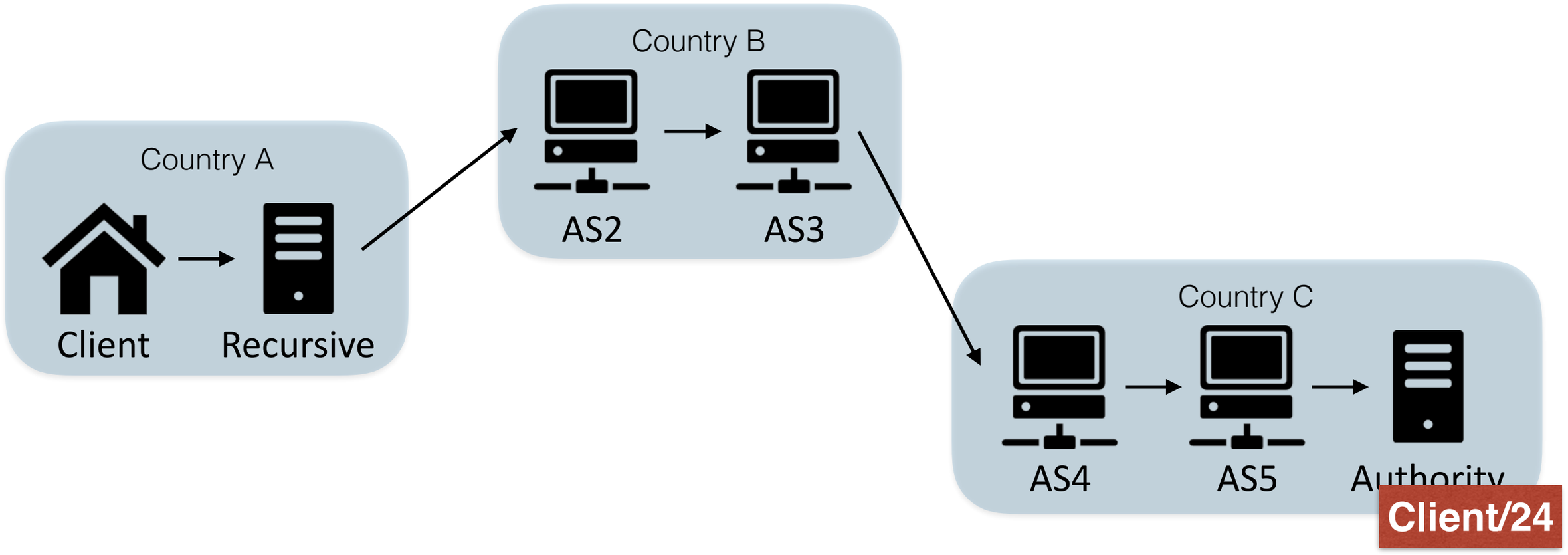
Surveilling DNS Traffic



Surveilling DNS Traffic



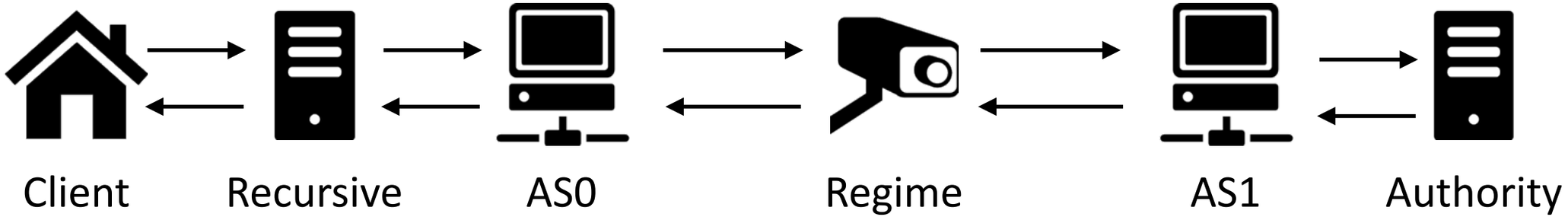
Surveilling DNS Traffic



Selective Cache Poisoning

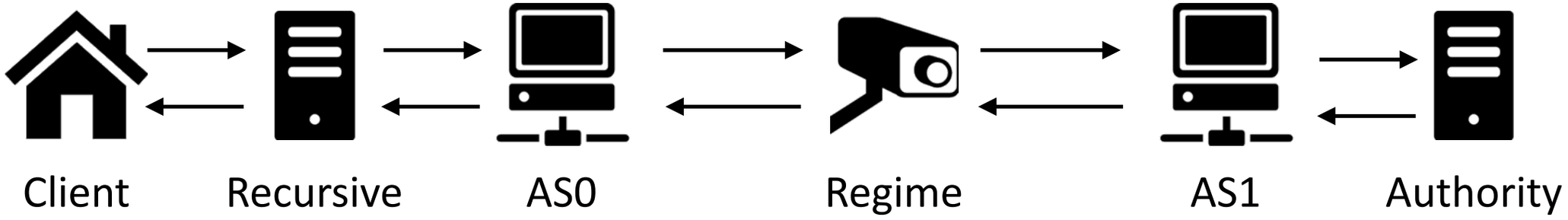
- Select a specific prefix to target
- Wait for requests from that prefix to appear
- Alter packets for the target clients only
- Remember that DNS is very easy to monitor

The Attack

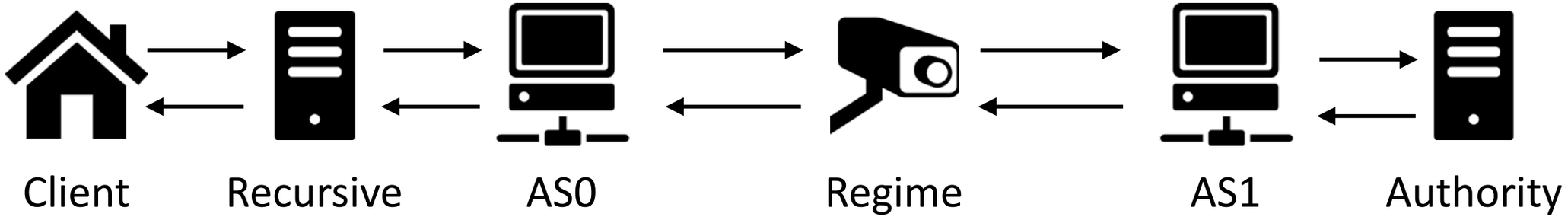


The Attack

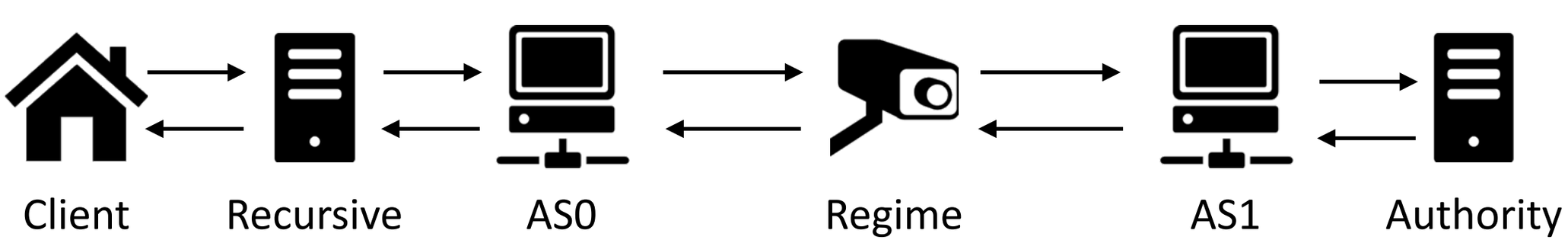
Any/24



The Attack



The Attack



tinyurl.com/cache-poisoning

Poisoning Consequences

- Cyber warfare
- Obtain visibility beyond a global recursive
- Do not affect any other user around the world
- Maybe now Turkey would not need to BGP hijack!

Targeted Attack

85.90.227.23

Lena

Web Server Nameserver

Global
Recursive

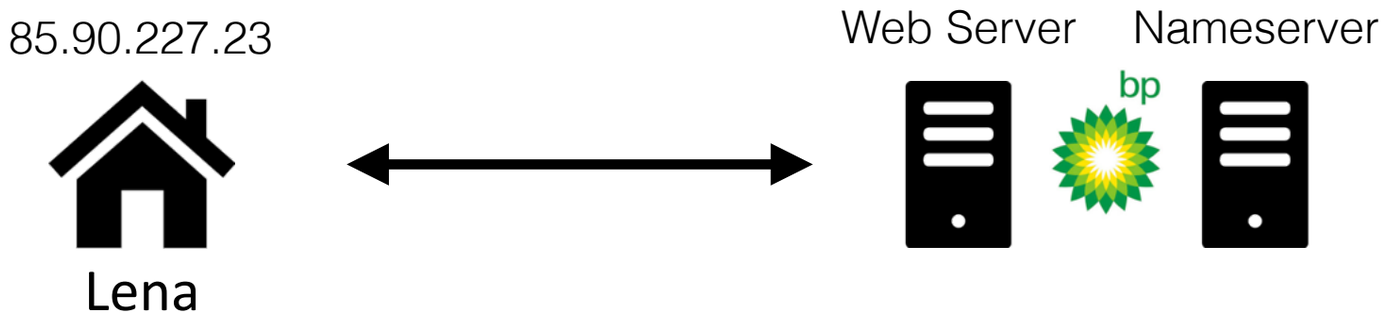
Attacker

195.251.97.20

Alice

Malicious
Host

Targeted Attack



Global
Recursive

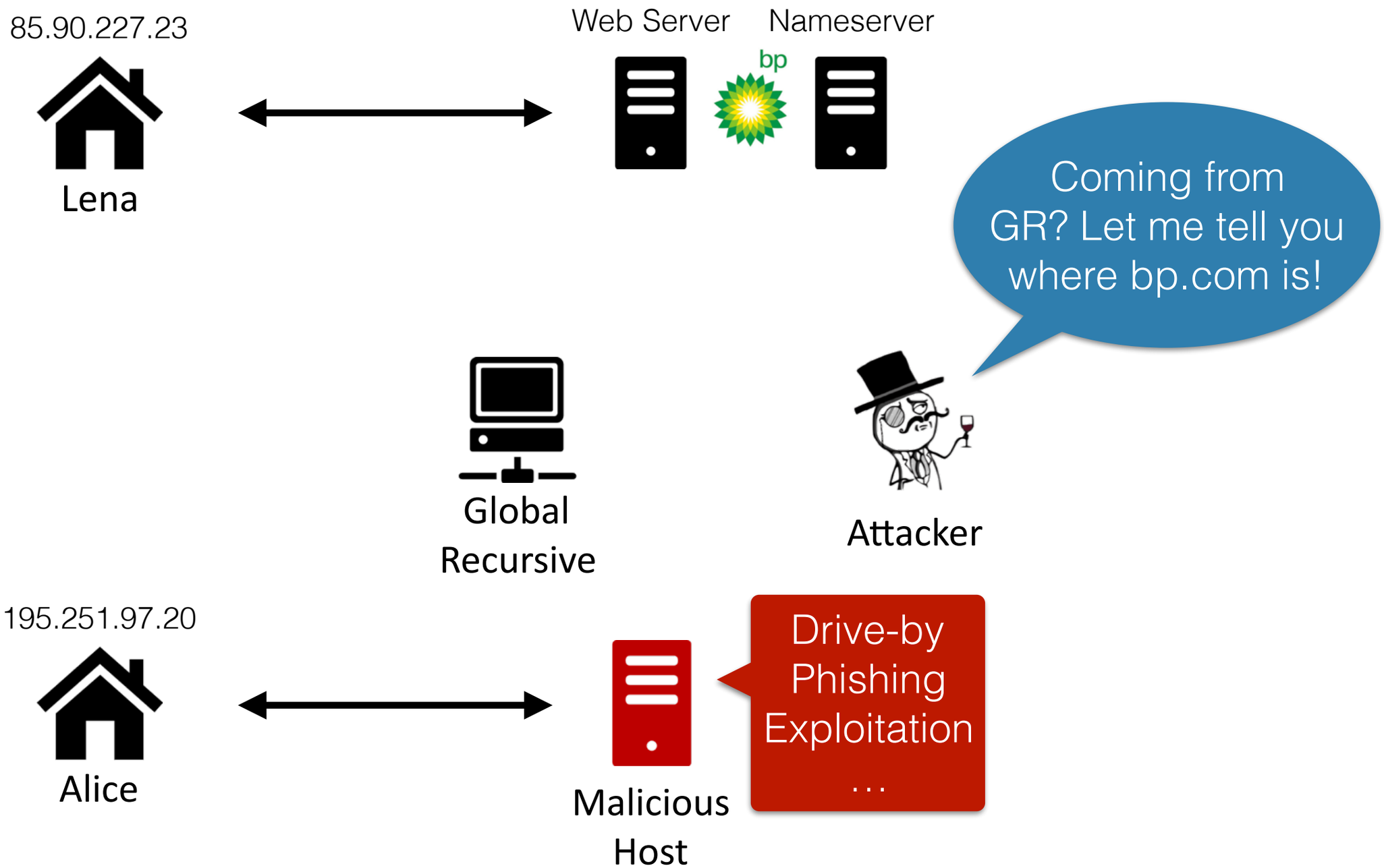
Attacker

195.251.97.20

Alice

Malicious
Host

Targeted Attack



Email Redirection

85.90.227.23

Lena

mail@lena.com

public@mx.com

Global
Recursive

mail@bob.com

195.251.97.20

Alice

mail@alice.com

public@mx.com

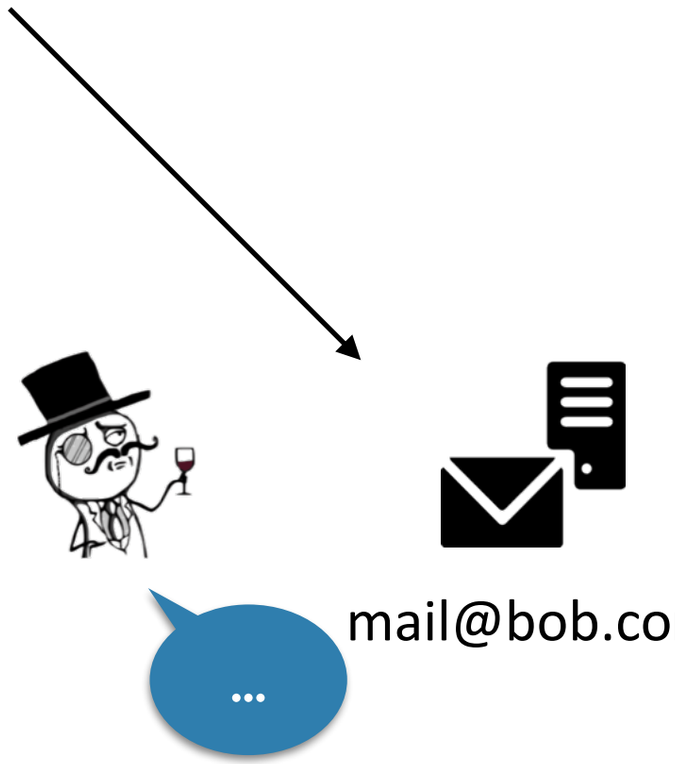
Email Redirection

85.90.227.23

Lena

mail@lena.com

public@mx.com



Global
Recursive

mail@bob.com

195.251.97.20

Alice

mail@alice.com

public@mx.com

Email Redirection

85.90.227.23

Lena

mail@lena.com

public@mx.com

Global Recursive

mail@bob.com

195.251.97.20

Alice

mail@alice.com

public@mx.com

NS Takeover

85.90.227.23

Lena

TLD

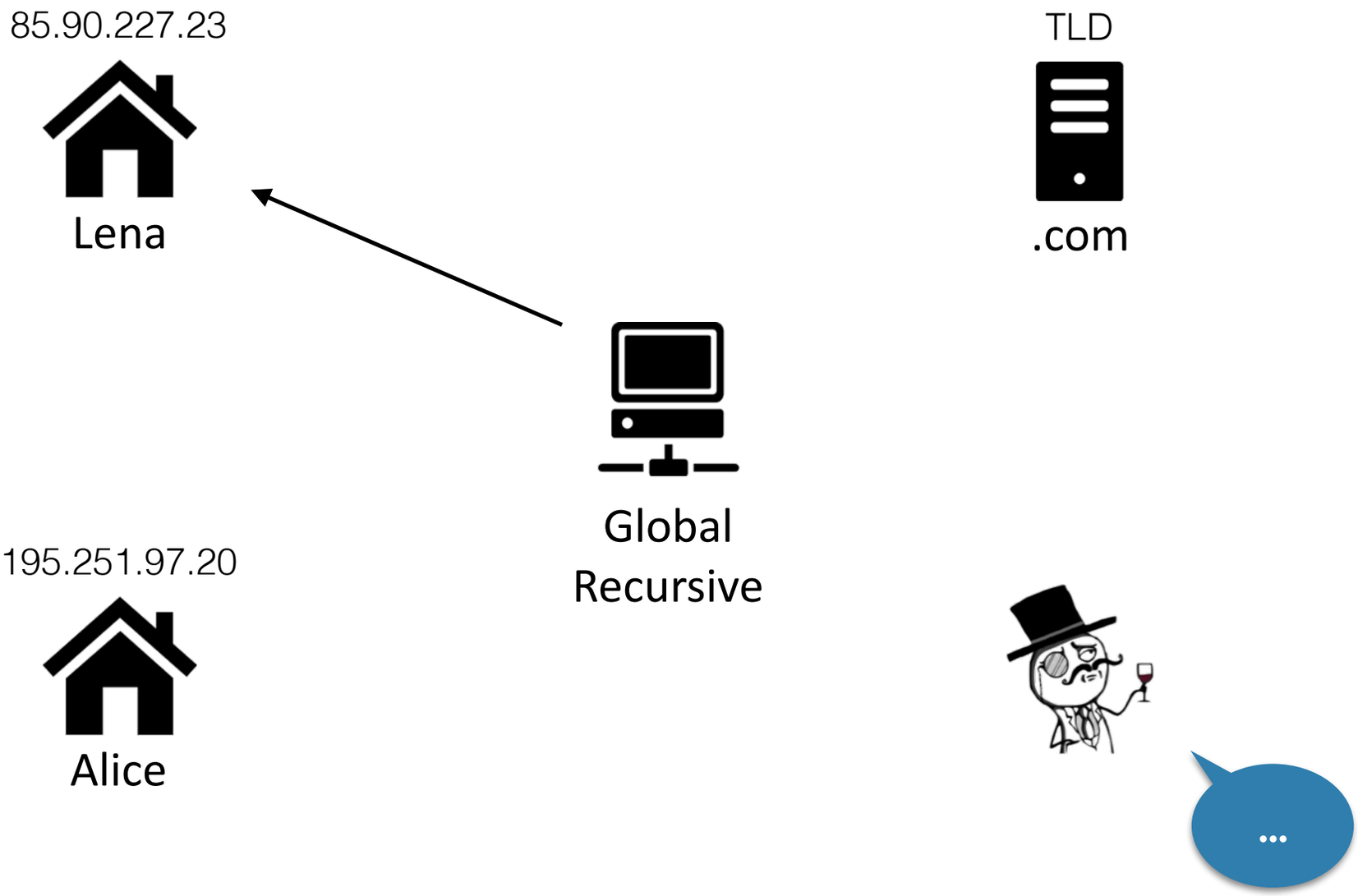
.com

Global
Recursive

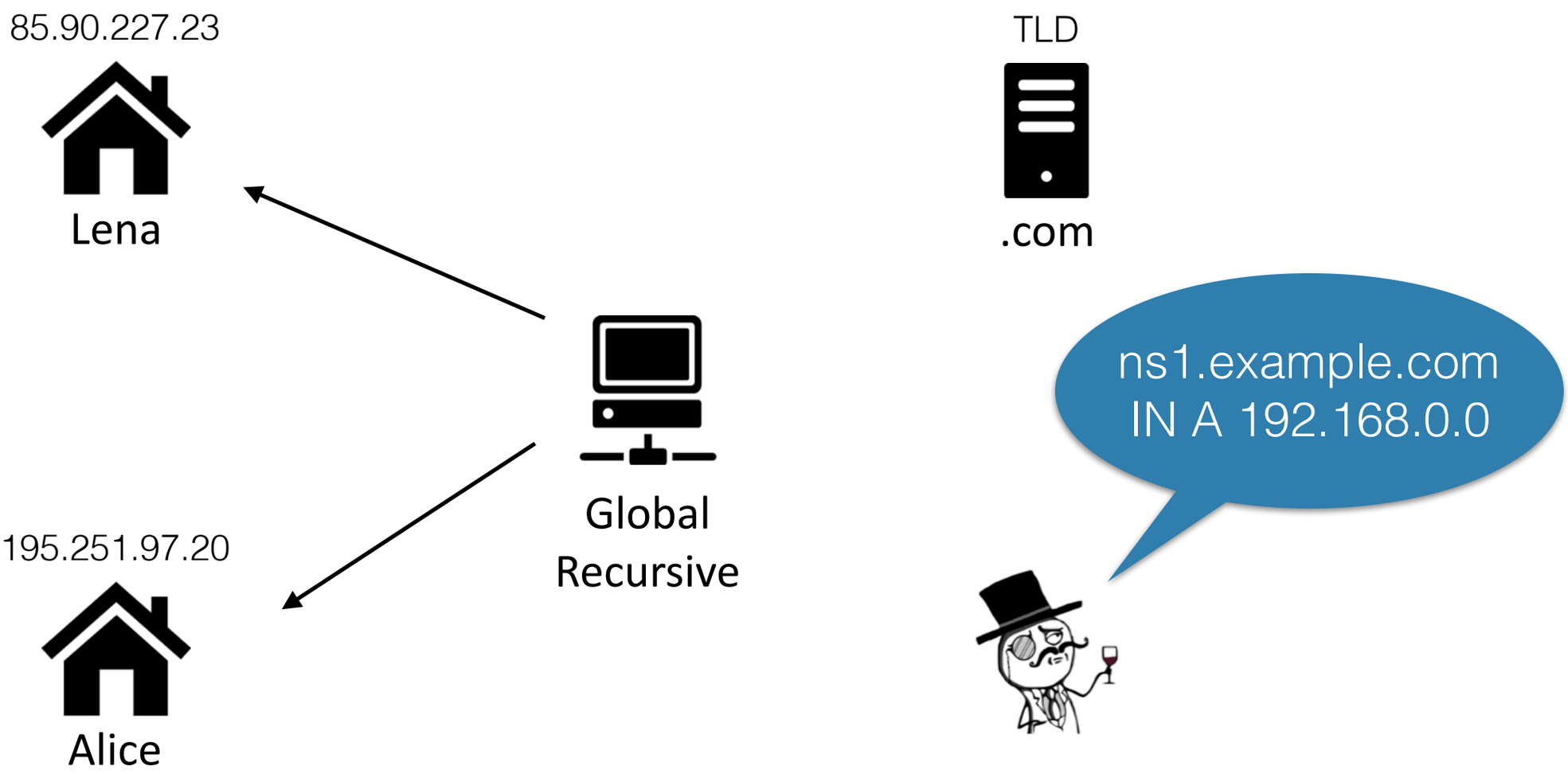
195.251.97.20

Alice

NS Takeover



NS Takeover


85.90.227.23
Lena
TLD
.com
ns1.example.com
IN A 192.168.0.0
Global
Recursive
195.251.97.20
Alice


formation
privacy

Remedies

- RFC 7871 specifies a way to opt out of the protocol
- The client needs to submit an ECS enabled request
- The recursive must respect existing ECS payload
- The Source Netmask needs to be set to 0 bits
- The Client Subnet needs to be set to 0.0.0.0
- **Six years later** - **no tools available** to do so

Unbound Forwarder

- Install an experimental (!) version of Unbound
- Configure to enable ECS
- Set the netmask to be shared equal to zero
- Configure to forward DNS requests to the original recursive server

ECS in a Nutshell

- Is being widely adopted around the world
- Helps users enjoy “a faster internet”
- Allows bandwidth usage minimization
- Opens the door to new attacks
- Reduces users’ privacy online
- Does not allow the user to opt out

“Finally, we recommend that others avoid techniques that may introduce additional metadata in future [DNS] work, as it may damage user trust.”

–RFC 7871 Client Subnet in DNS Queries