DNS TUNNELING

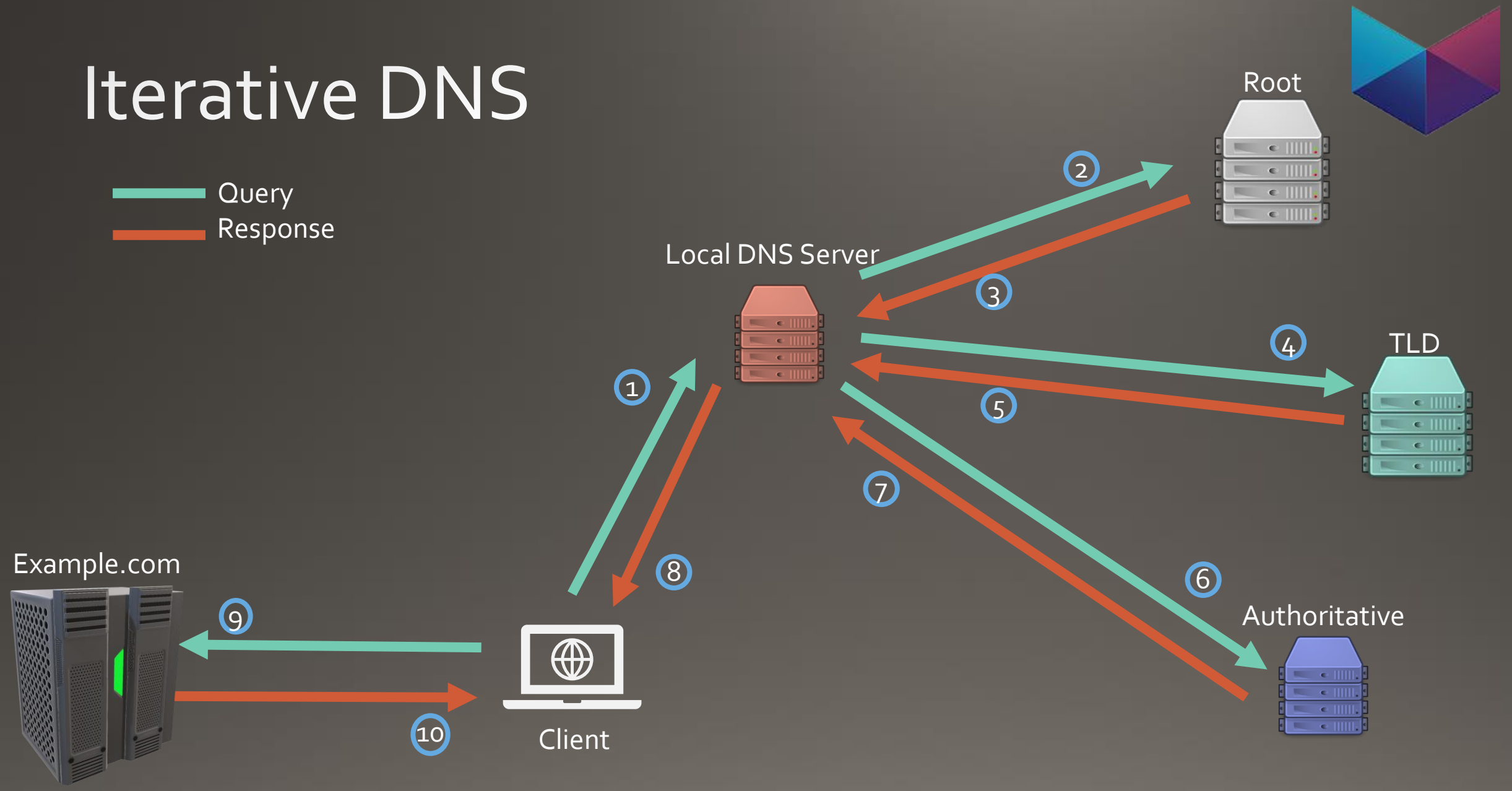
Shachar Markovich & Naor Shimon Maman

Today:

- What is DNS
- DNS Tunneling:
  - What is it
  - Why we need it?
  - The Idea
  - Who it is work
  - Our Implementation
- Demonstration & Code

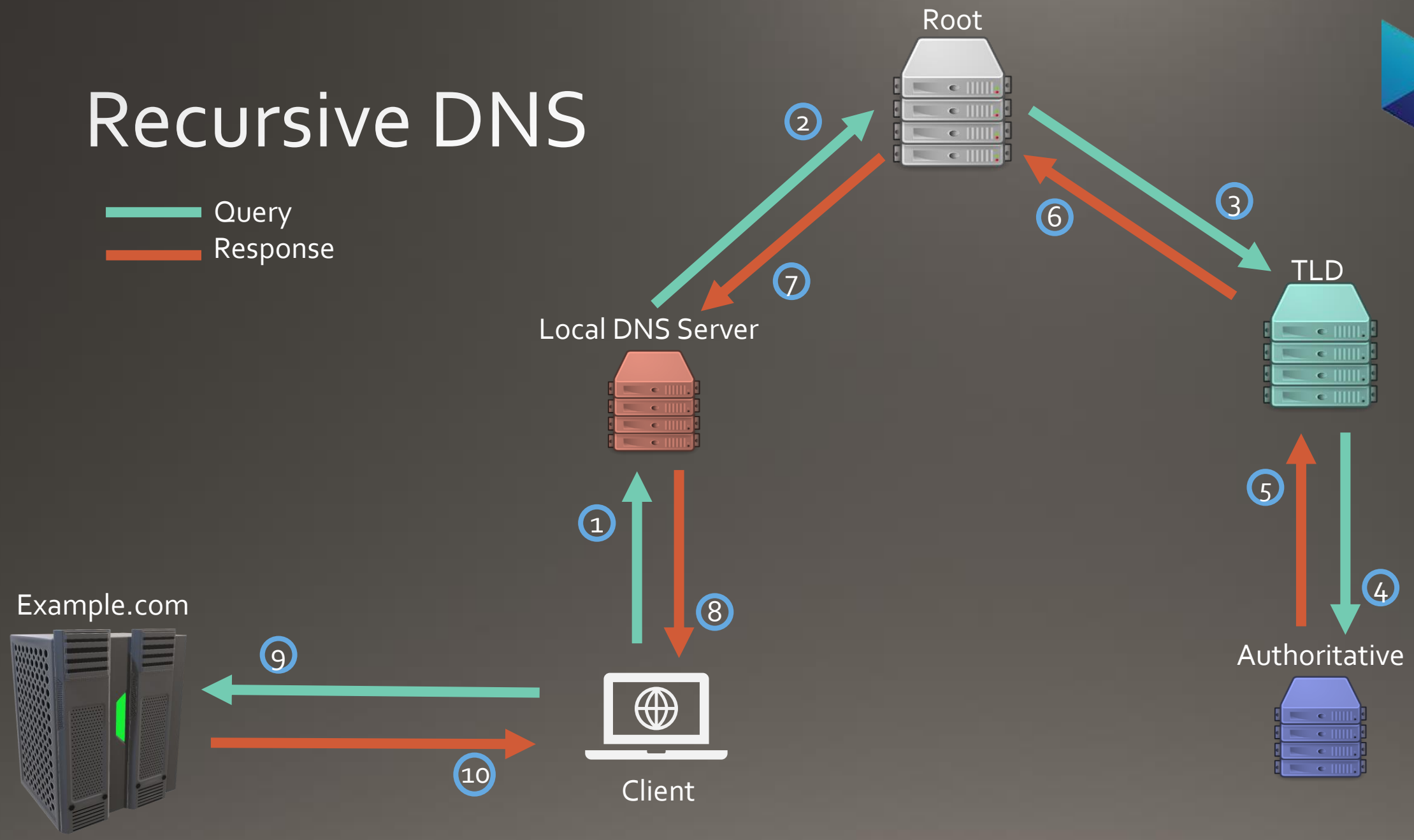
What is DNS ?

Iterative DNS



Shachar Markovich & Naor Shimon Maman

Recursive DNS



Shachar Markovich & Naor Shimon Maman

DNS Reco es

RR Type	
A	R
AAAA	R
CNAME	**R**
MX	R
NS	R

that domain

C:\Windows\system32\cmd.exe

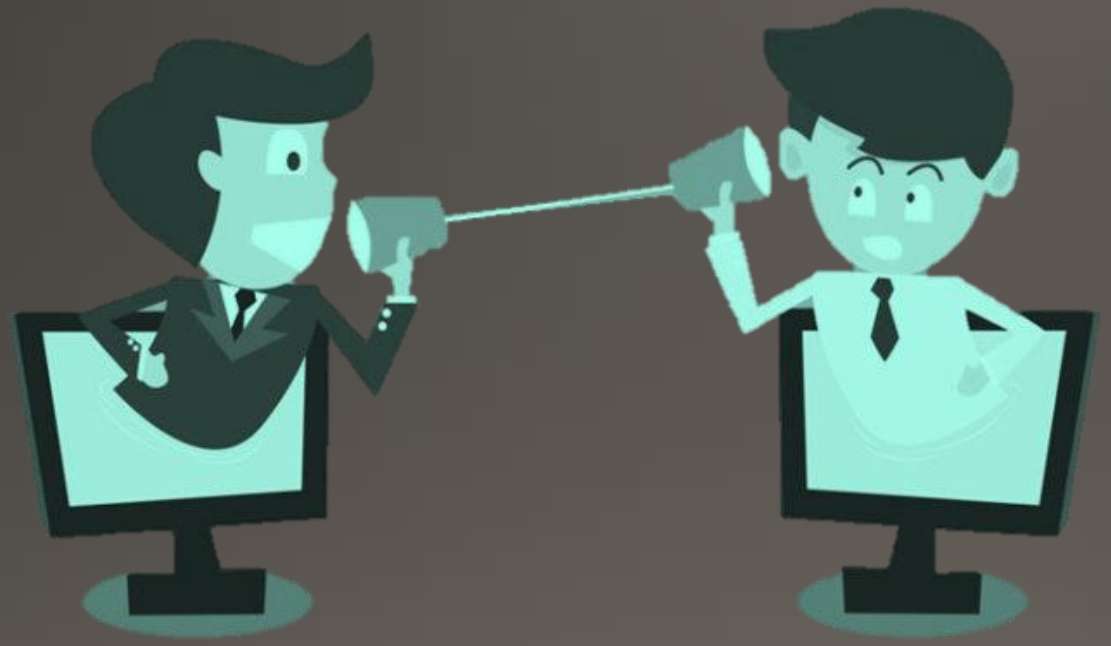
```
C:\>nslookup www.cnn.com
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    turner-tls.map.fastly.net
Addresses:  2a04:4e42:400::323
          2a04:4e42:200::323
          2a04:4e42:600::323
          2a04:4e42::323
          151.101.129.67
          151.101.65.67
          151.101.193.67
          151.101.1.67
Aliases:  www.cnn.com
```

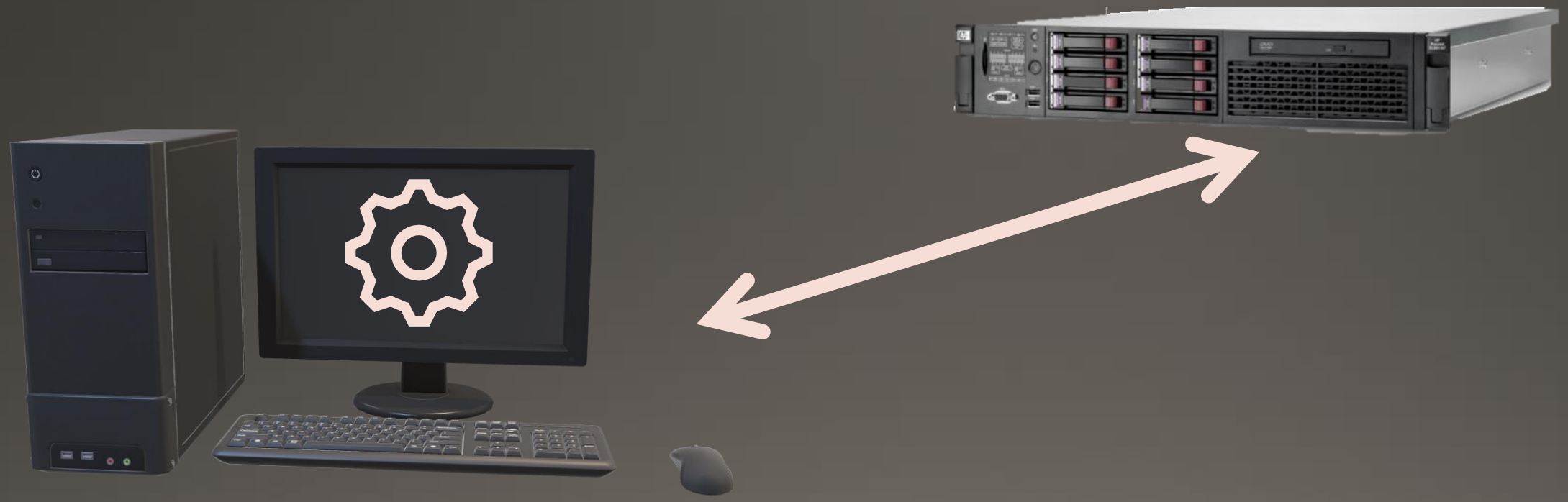
How can we manipulate DNS?

Shachar Markovich & Naor Shimon Maman

DNS Tunneling – Why?



DNS Tunneling – Why?



DNS Tunneling – Why?

DNS Tunneling – The Idea

- Script in Client Side
- An Authoritative DNS server
- A domain: **resh.gimel**

- Domain is limited to 255 characters (!)

  Slice_of_msg.resh.gimel.

- Stateless protocol

DNS Tunneling – Our Scenario

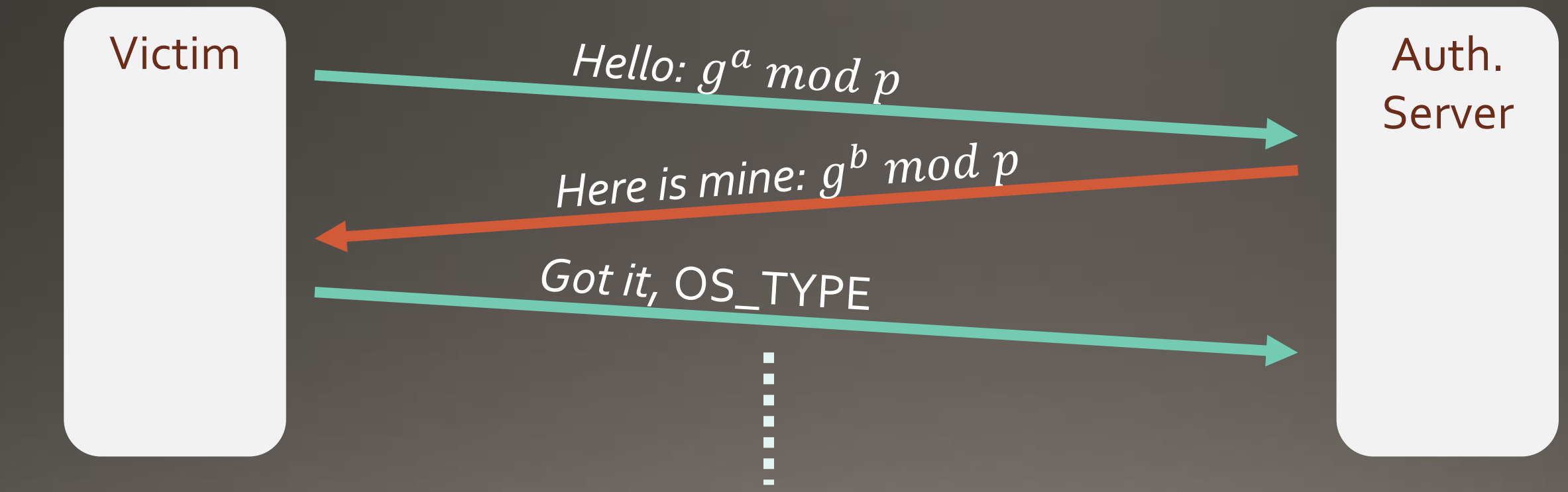
Who it is work

```
"/home/kali/Desktop/auto DNS/venv/bin/python" "/home/kali/Desktop/auto DNS/main.py"
[!] waiting for victim to connect...
[!] victim connected. ID: 38jdpk3w   OS type: Linux
Enter command to send to '38jdpk3w': route
[!] Got from victim:

    Kernel IP routing table
    Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
    default         10.0.2.1        0.0.0.0         UG    0      0        0 eth0
    10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

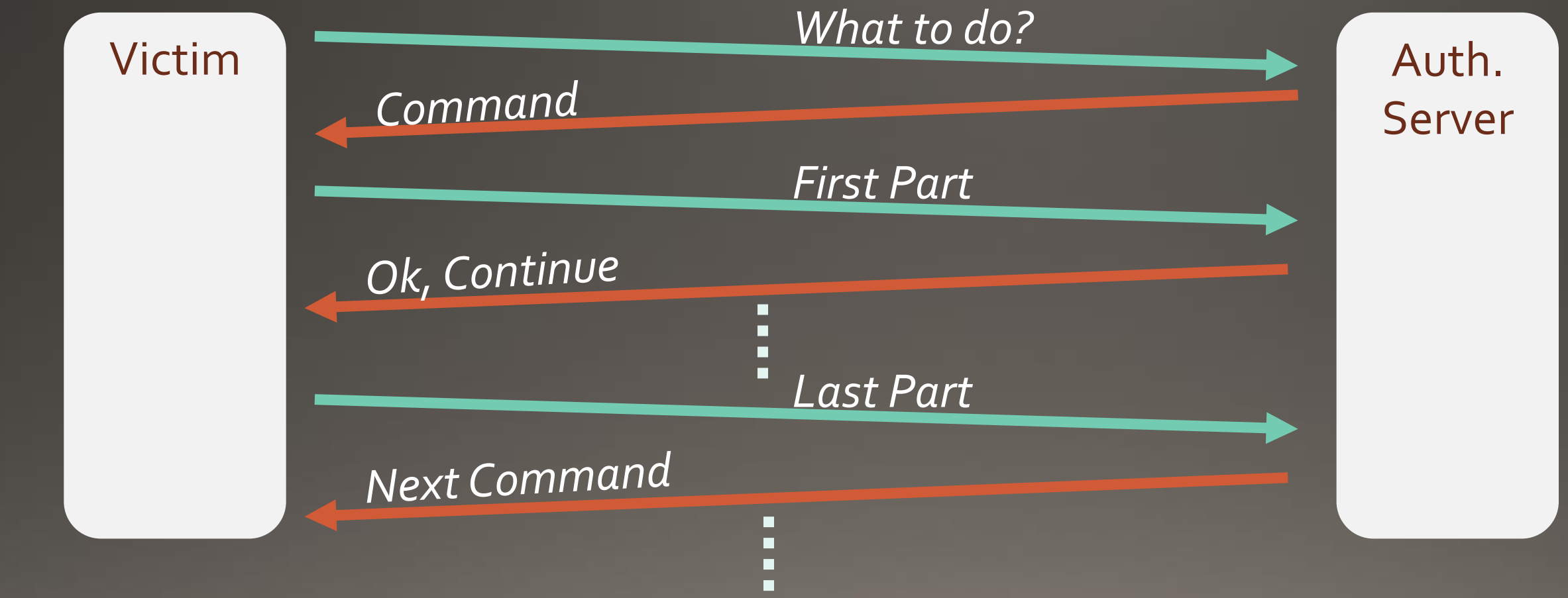
DNS Tunneling – How?

Diffie Hellman Key Exchanging



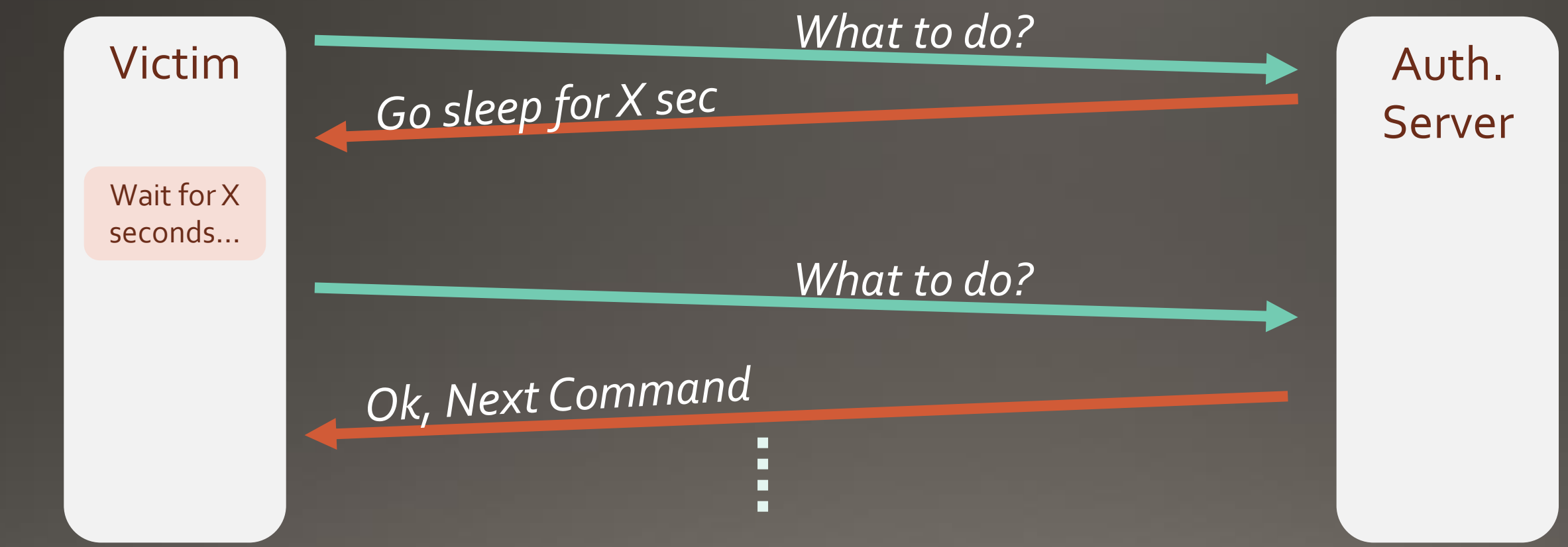
DNS Tunneling – How?

Sending Data



DNS Tunneling – How?

Go sleep



DNS Tunneling – Our Scenario

Configuration

+

+

DNS Tunneling – Our Scenario

Implementation

1 Diffie Hellman Key Exchange

2 Encrypting

The client data with AES

3 Encoding

The encrypted data to Base32

4 Sending

The data in DNS request to DNS Resolver

5 Forwarding

The request to Auth. server

6 Processing

Decode & decrypt the data in the request and process it

7 Response

With a fit DNS response - contains the next command to preform

Shachar Markovich & Naor Shimon Maman

DNS Tunneling – Our Protocol

In every message:

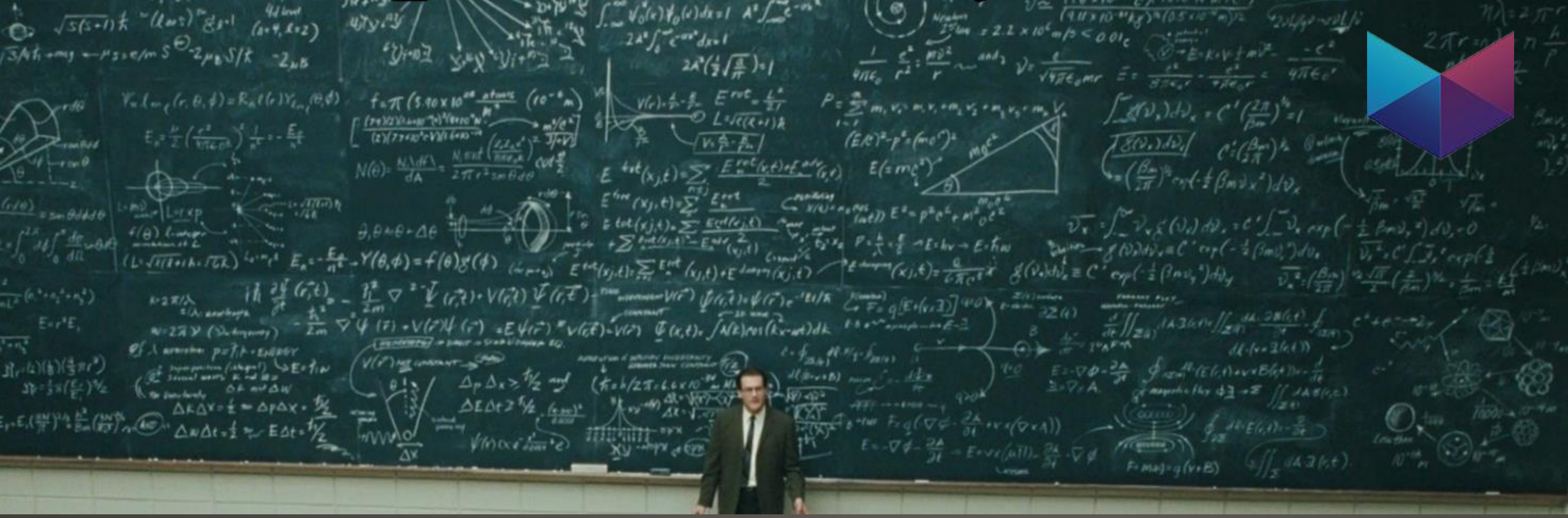
identify_number.base32(code).part of base32(AES(data)).resh.gimel.

Allowed codes messages:

Code	Meaning
10x	D.H. Key exchange
20x	Command & answer
30x	Sleep
40x	Error & Retransmission

שימושים

- עמידה בזמנים
- למה בחרנו את כל מה שבחרנו
- לא לשכוח לשלוח שאלות
- לברר כמה תווים במפתח הציבורי וכמה במפתח ההצפנה הסימטרי ולמה



Questions?

Shachar Markovich & Naor Shimon Maman

Thank You!

Shachar Markovich & Naor Shimon Maman