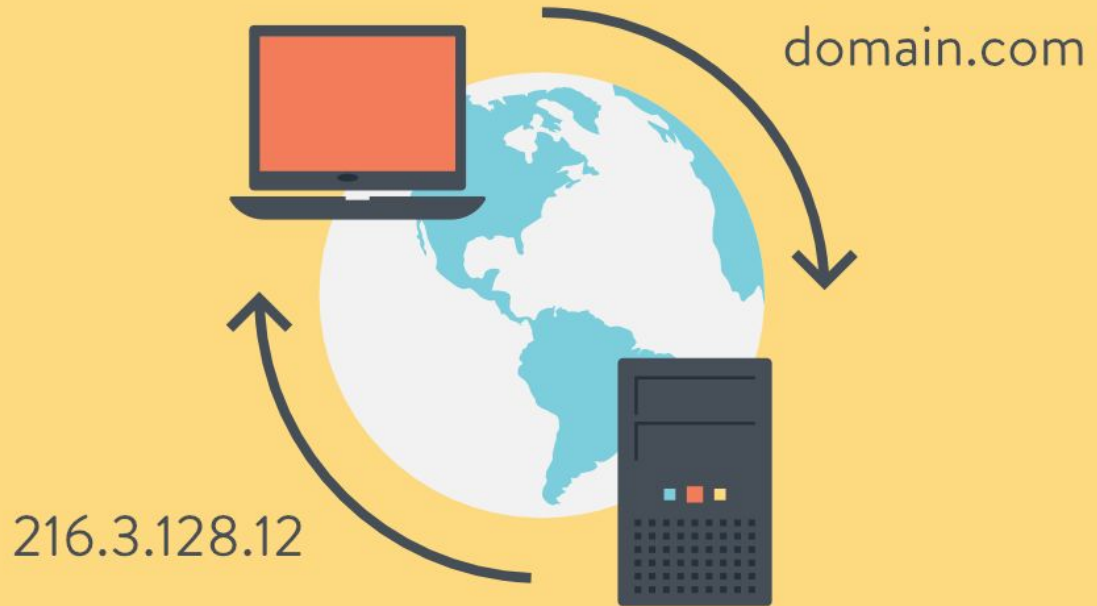# Introduction to DNS Spoofing
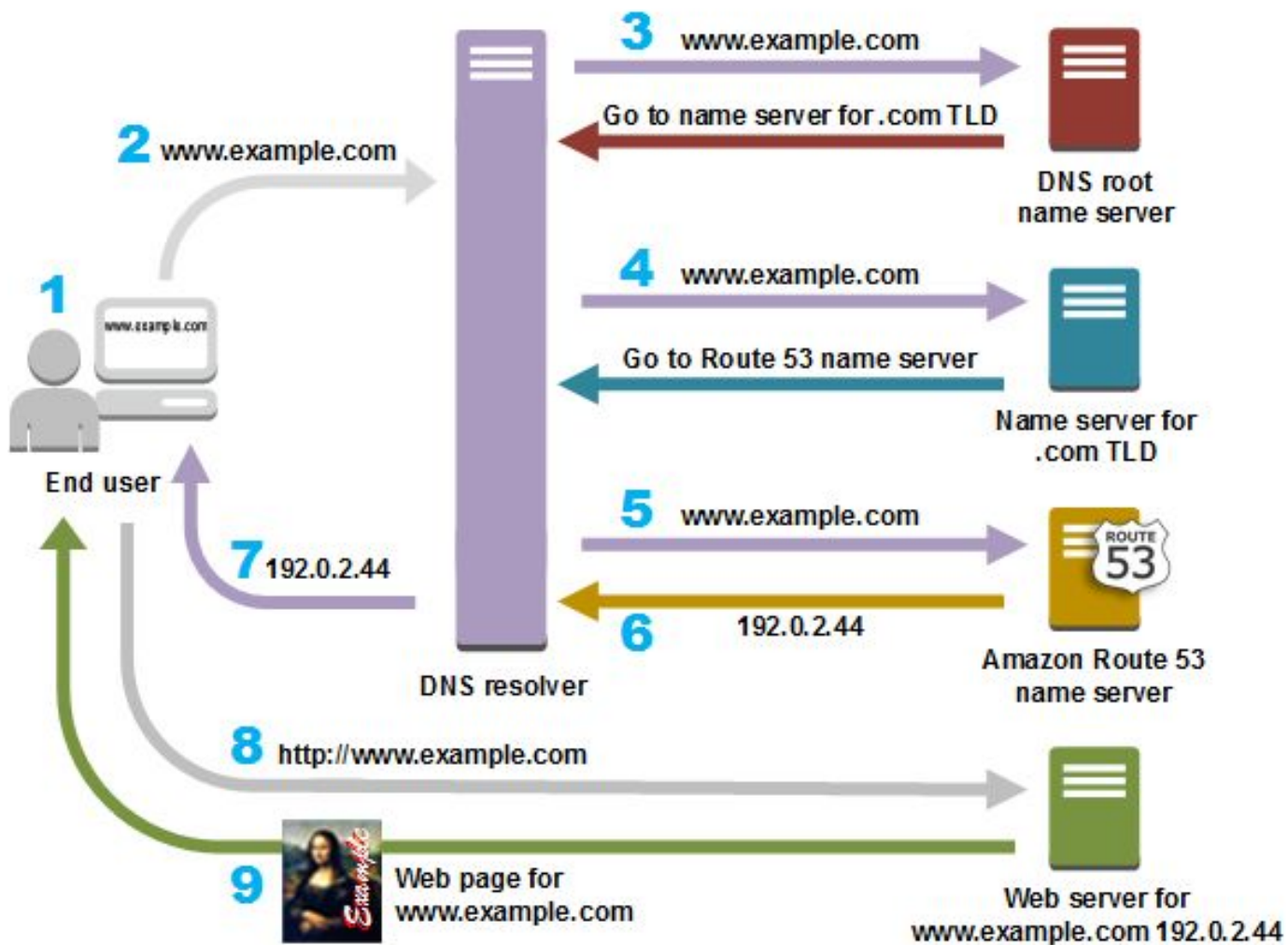
Yadhu Krishna M

What is DNS ?

- Stands for Domain Name System

- Directory of names that match with IP addresses

- Phonebook of the internet

domain.com

216.3.128.12

1 End user

2 www.example.com

3 www.example.com

Go to name server for .com TLD

DNS root name server

4 www.example.com

Go to Route 53 name server

Name server for .com TLD

5 www.example.com

6 192.0.2.44

Amazon Route 53 name server

7 192.0.2.44

DNS resolver

8 http://www.example.com

Web server for www.example.com 192.0.2.44
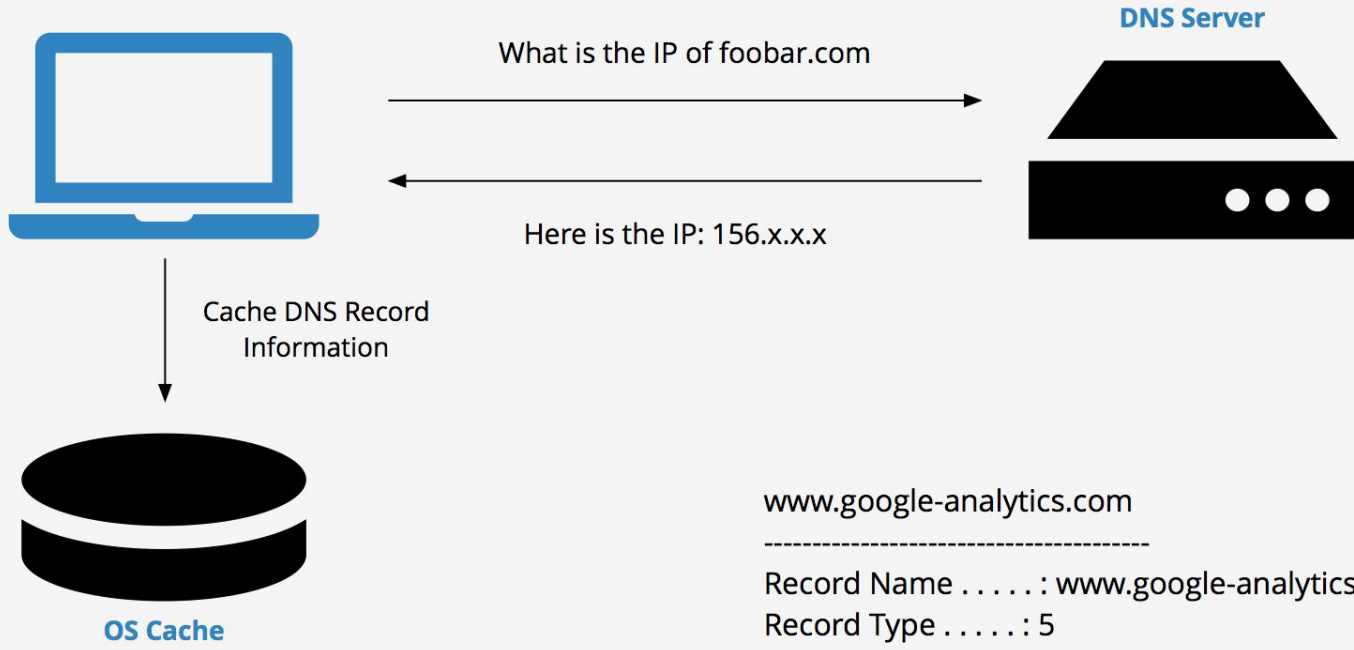
9 Web page for www.example.com

What is DNS Caching?

DNS cache refers to the temporary storage of information about previous DNS lookups on a machine's OS or web browser.

Why DNS Caching?

- Avoid having to complete an entire DNS lookup
- Reduced network traffic
- Improved performance

DNS Server

What is the IP of foobar.com

Here is the IP: 156.x.x.x

Cache DNS Record
Information

OS Cache

DNS Cache

www.google-analytics.com

Record Name . . . . . : www.google-analytics.com
Record Type . . . . . : 5
Time To Live . . . . : 104
Data Length . . . . . : 4
Section . . . . : Answer
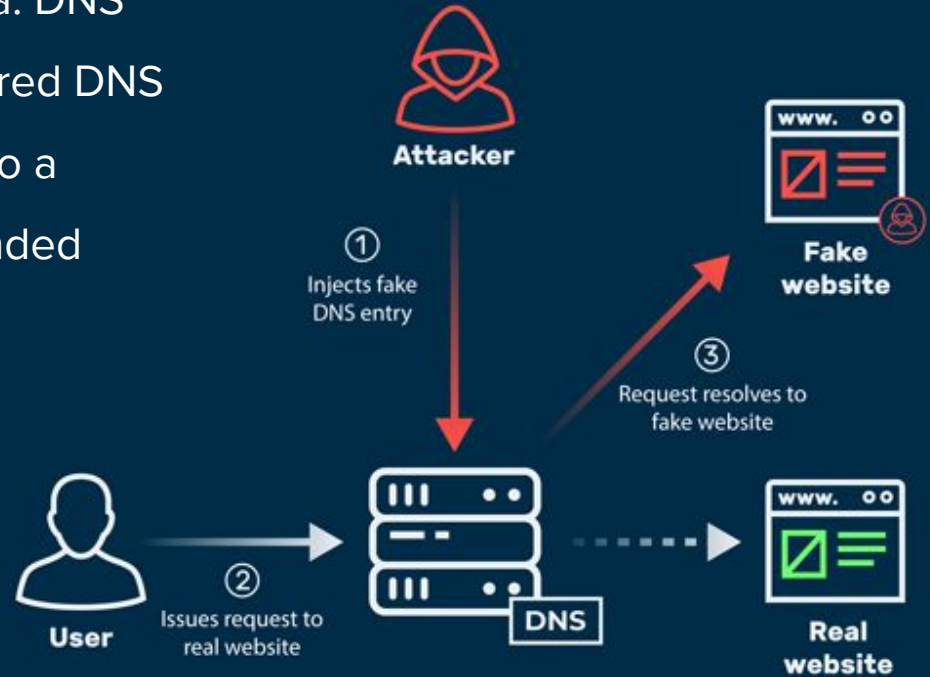CNAME Record . . . . : www-google-analytics.l.google.com

DNS Spoofing

Domain Name Server (DNS) spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.

Attacker

① Injects fake DNS entry

③ Request resolves to fake website

Fake website

User

② Issues request to real website

DNS

Real website

Methods for DNS Spoofing

Most common methods:

- Man-in-the-middle duping

- DNS server hijack

- DNS cache poisoning via spam

Impacts of DNS Spoofing.

- Data theft : Attackers steal sensitive information such as login credentials.

- Malware Injection : Injection viruses, or worms into victim's machine.

- Censorship: Block victims from accessing certain websites.

- Launch distributed Denial-of-Service attack.

- Block security updates to fully impersonate victim's device.

Preventing DNS Spoofing

- DNS spoofing detection tools

- Domain name system security extensions (DNSSEC)

- Using End-to-end encryption

- Never click on unrecognized links

- Regularly scan computer for malware

- Frequently flush DNS cache to solve poisoning

- Using Virtual Private Network (VPN)

Thank you !

Yadhu Krishna M

References.

1. https://www.businessinsider.in/tech/how-to/what-is-a-dns-server-how-domain-name-system-servers-connect-you-to-the-internet/articleshow/81022842.cms
2. https://www.liquidweb.com/kb/how-to-demystify-the-dns-process/
3. https://www.keycdn.com/support/dns-cache
4. https://www.kaspersky.co.in/resource-center/definitions/dns