Leaving Traces Online

Using DNSCrypt

Irfan Kanat

Department of Digitization
Copenhagen Business School

May 24, 2021

2021-05-24

Leaving Traces Online
Using DNSCrypt

Irfan Kanat

Department of Digitization
Copenhagen Business School

May 24, 2021

This work is licensed under a Creative Commons Attribution 4.0 International License.

In this module we will talk about what kind of traces we leave going about our daily lives and how to minimize this.

What is Domain Name System (DNS)

STATE OF NEBRASKA - WAN SERVICE 2200 N 33rd St 402-477-0352

STATE OFFICES

Information & Capitol Switchboard 402-471-2311

Abstracters Board Of Examiners
1200 N Ste 404 68508 402-471-2383

Accountability And Disclosure Commission Nebraska
Capitol Bldg 68508 402-471-2522

Administrative Services Department Of
Director's Office State Capitol 68509 402-471-2331
Accounting Division 68509 402-471-2581
Budget Division

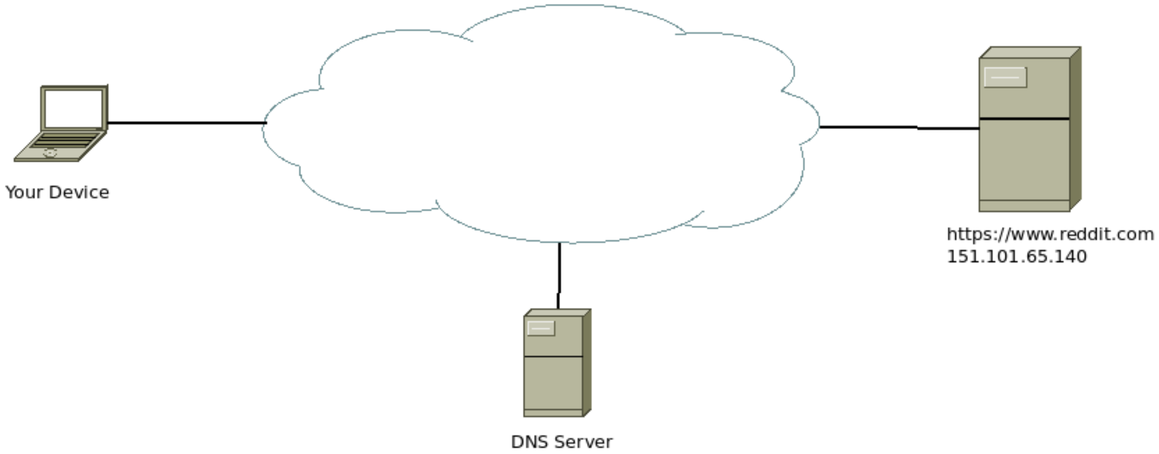
402-471-4420
402-475-9588
402-435-5107
402-328-0802
402-475-5749

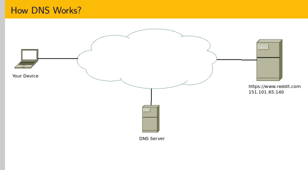
Diagnostic & Evaluation Cen
Federal Surplus Property
Lincoln Correctional Center
Lincoln District Parole Office
Nebraska State Penitentiary
Parole Administration
Adult Parole
Folsom & W Prospector Pl 68
Building #1
Residential Treatment Center
Court Of Appeals
Credit Union 330 S 16th 68508
Crime Commission 301 Centennial Mall
Crime Victim's Reparations Board
301 Centennial Mall S 68509
Drivers License Testing See Motor Vehicle
Deaf & Hard Of Hearing Commission
Economic Development Dept Of
301 Centennial Mall S 68509
Education Department Of
301 Centennial Mall S 68509
Curriculum
Data Services
Disability Determinations
Early Childhood

Anytime a piece software on your device tries to connect to a URL, the URL needs to be converted to an address that computer scan understand. This is done through a shared service called Domain Name System.

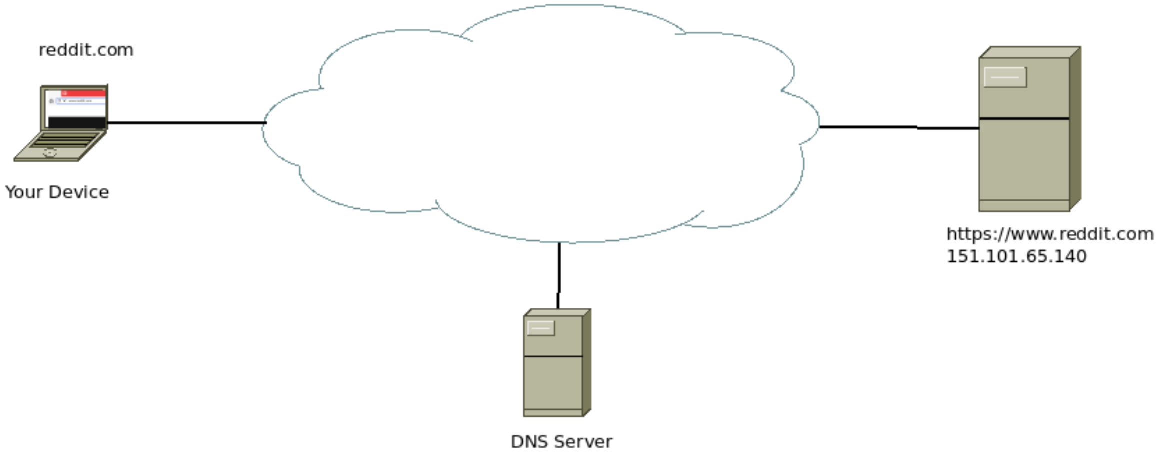
Think of this as the phone books. In the old days before DNS servers and Internet, when you wanted to call your friend you would look up their name on a phone book.

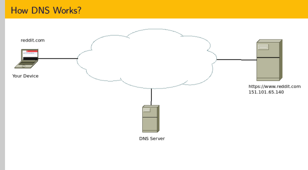
How DNS Works?



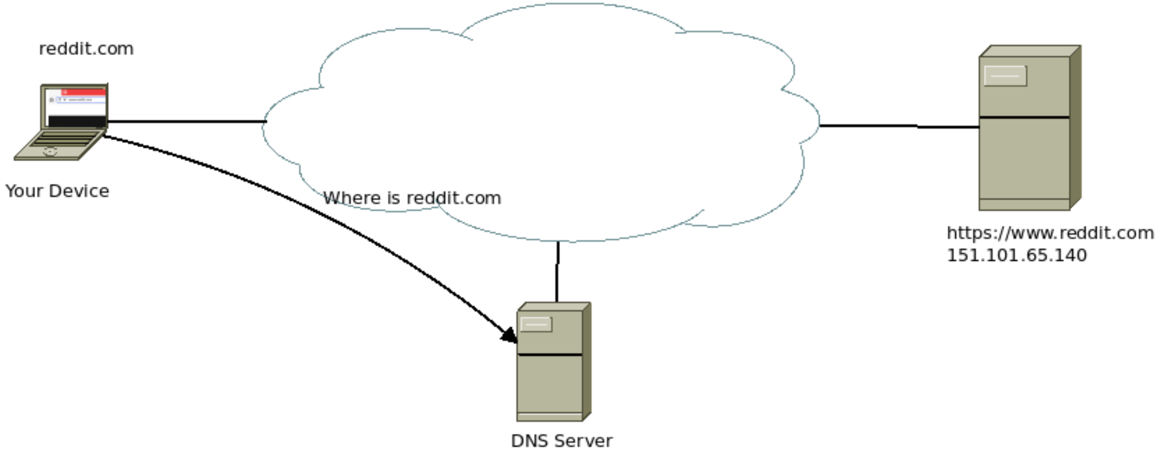


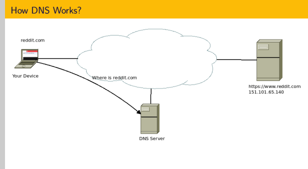
How DNS Works?



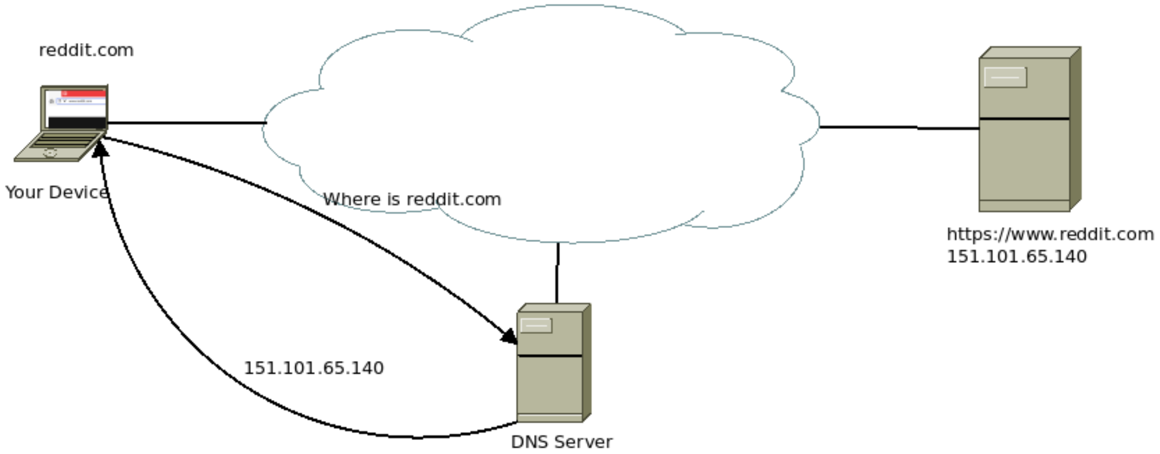


How DNS Works?





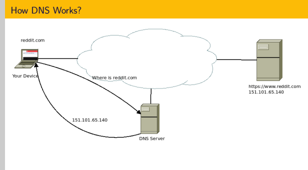
How DNS Works?



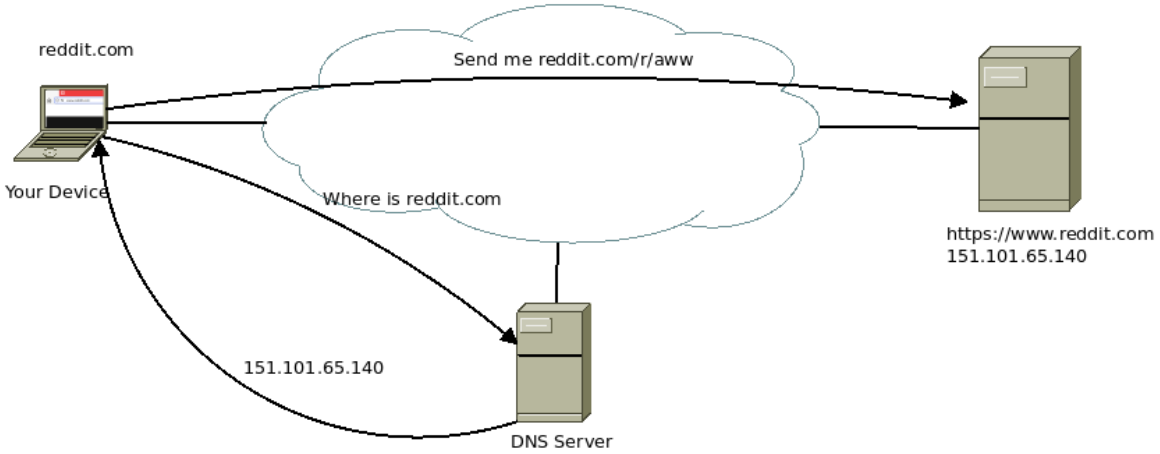
Leaving Traces Online

2021-05-24

└How DNS Works?



How DNS Works?



reddit.com

Send me reddit.com/r/aww

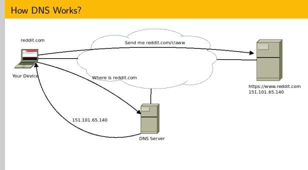
Your Device

Where is reddit.com

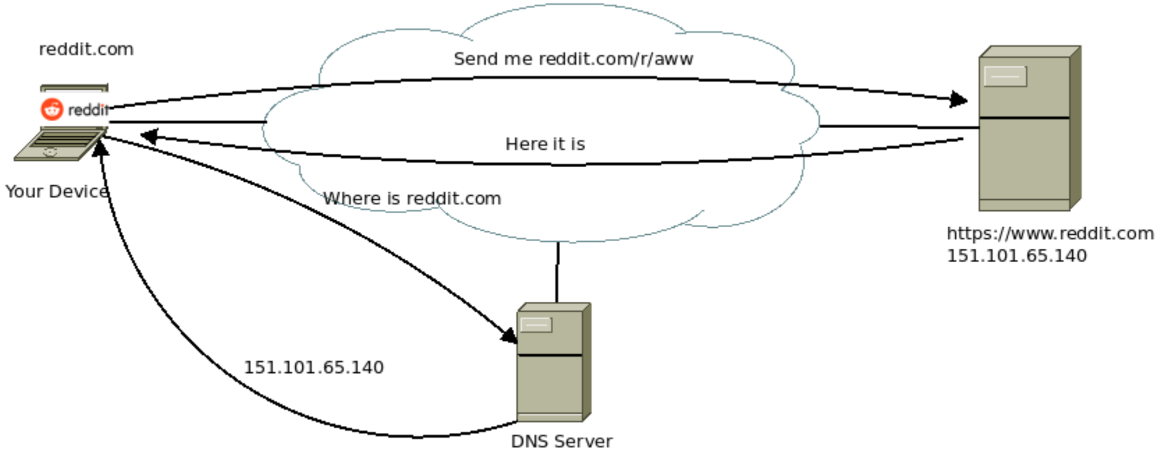
https://www.reddit.com
151.101.65.140

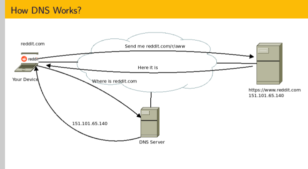
151.101.65.140

DNS Server



How DNS Works?



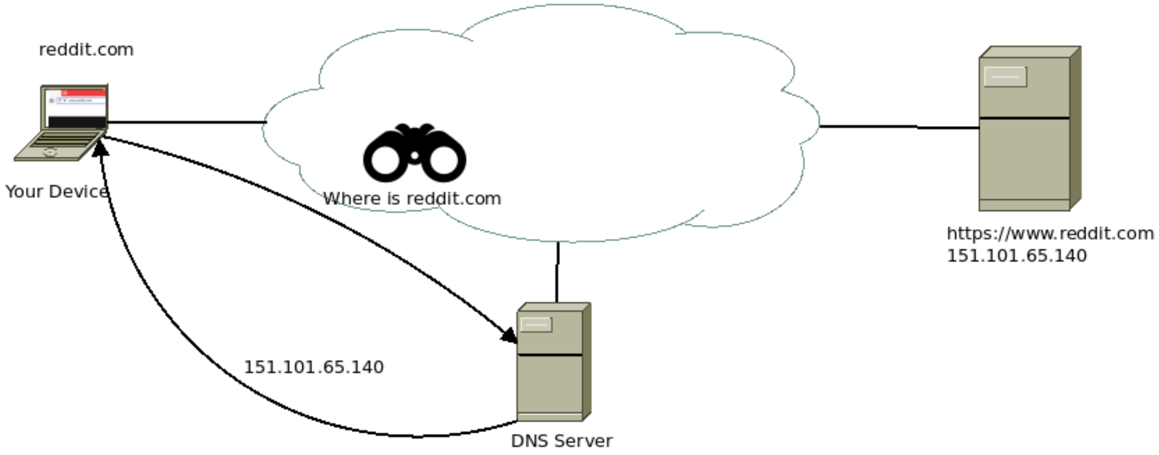

How DNS Works?

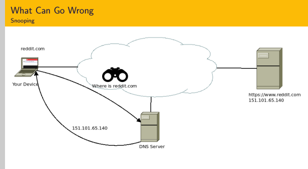
Almost all software running on your computer needs to make use of the DNS service. Your operating system looking for updates, your browser finding web sites, your cloud file storage syncronizing files... They all will have to use DNS service to look up IP addresses through DNS. How it works is this way:

1. A request is made with a URL (such as reddit.com).
2. Your computer asks the DNS server for the IP address matching the URL.
3. DNS server respons with the IP address.
4. Your computer then rends the request to the correct server.
5. Server responds.

What Can Go Wrong

Snooping

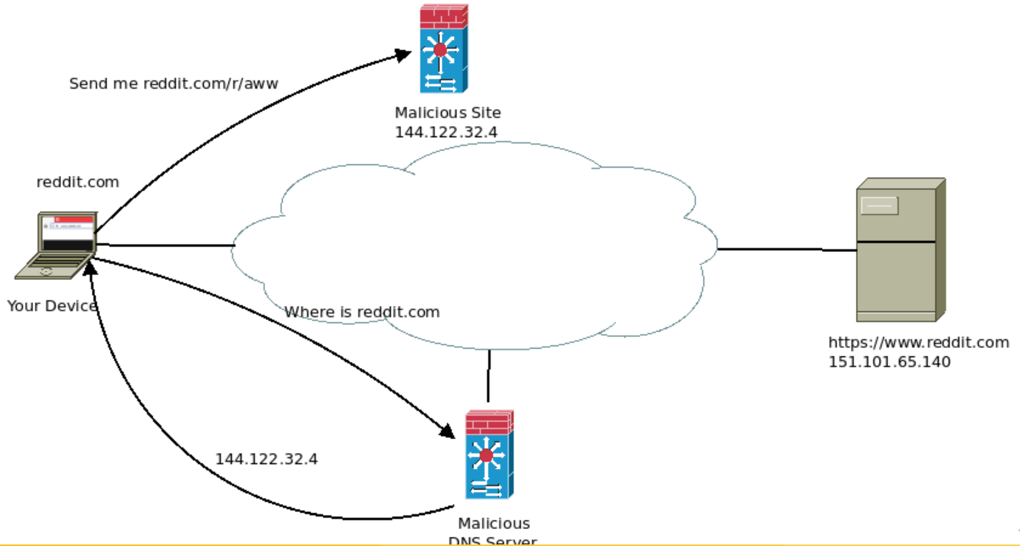


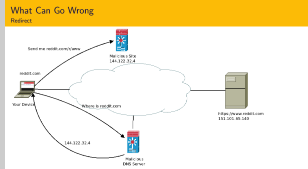


Standard DNS queries are not encrypted. Meaning anyone observing your traffic can easily figure out what you are interested in just by inspecting your DNS querries.

What Can Go Wrong

Redirect



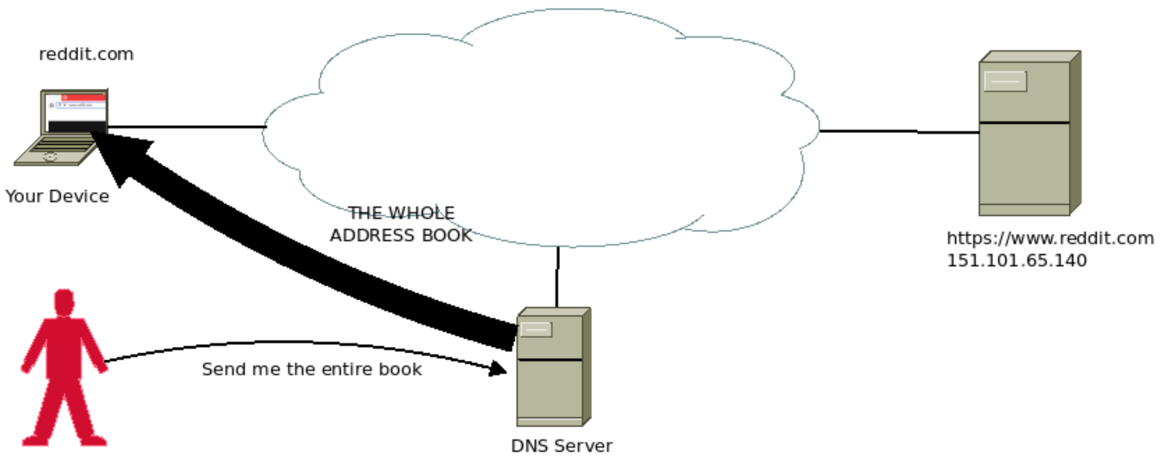


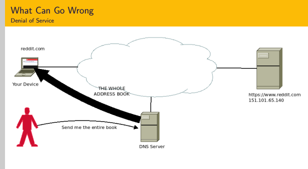
The DNS also does not have authentication mechanisms.
So if the DNS operator acts maliciously, or if someone impersonates your DNS operator, they can redirect you to the wrong addresses.
As an example of this: When you try to reach piracy web sites, the DNS servers redirect you to alternative addresses.

Although not malicious, they redirect you to a site you did not intend to visit.

What Can Go Wrong

Denial of Service





A common type of attack is called a Denial of Service (DOS) attack. The goal here is to send traffic to the victim to cause a sort of "traffic jam".

A single attacker is limited by the amount of traffic they can send. If an attacker could multiply the size of the traffic they generate, they can increase the impact of their DOS attack.

A DNS server can serve as that multiplier. The attacker, pretending (IP Spoofing) to be the victim can make fake requests to DNS servers, asking them for the entire DNS registry (which can be sizable). Therefore using the DNS servers to DOS the victim.

DNSCrypt

Authentication

Encryption

DNSCrypt

Authentication

Encryption

Enter DNSCrypt, an enhancement of the classical DNS protocol.

DNSCrypt supports authentication, thus malicious parties can not impersonate DNS servers.

All DNS traffic sent this way is also encrypted. Thus not subject to Snooping.