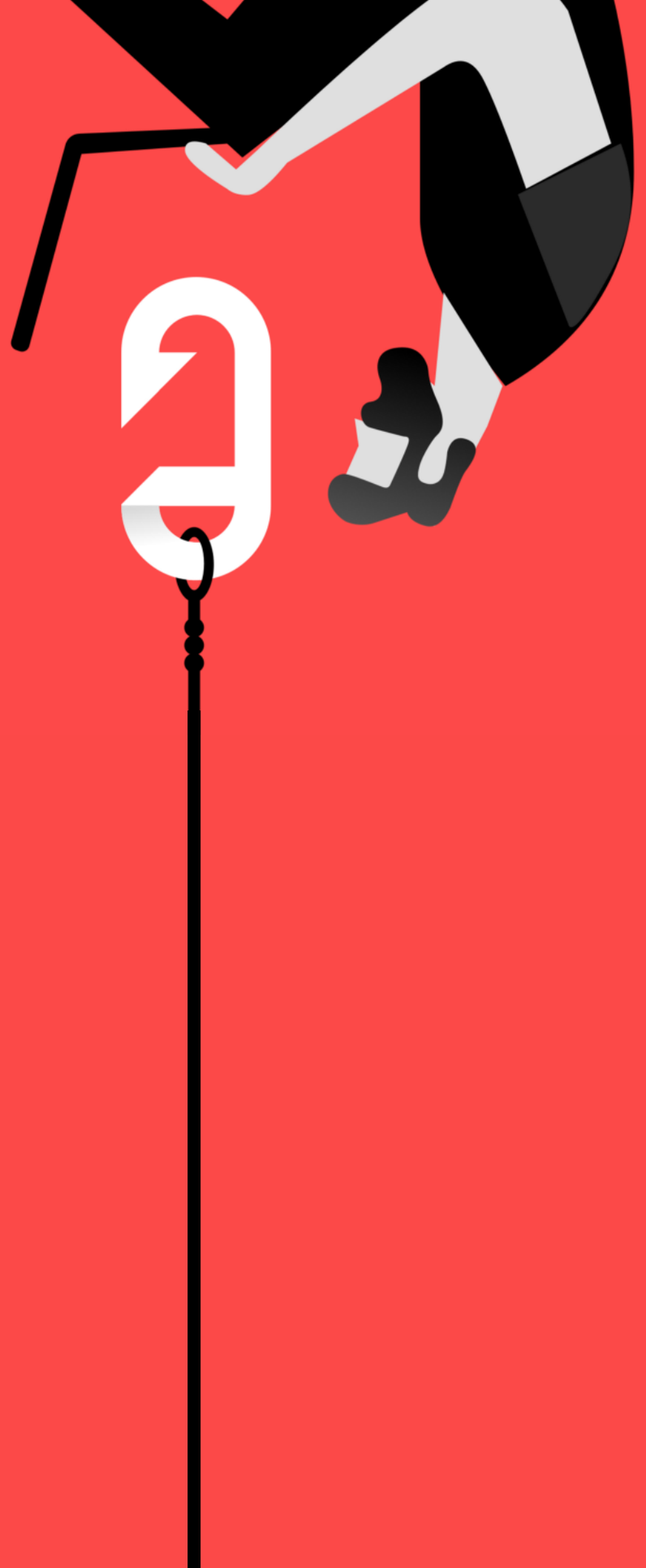
# PHISHING


Sahar Rajabi

Mohammad Ghaffarifar

Ziba Omidvar

Sadegh Hayeri




Sign in

with your Google Account

Email or phone

Forgot email?

Not your computer? Use Private Browsing windows to sign in. Learn more

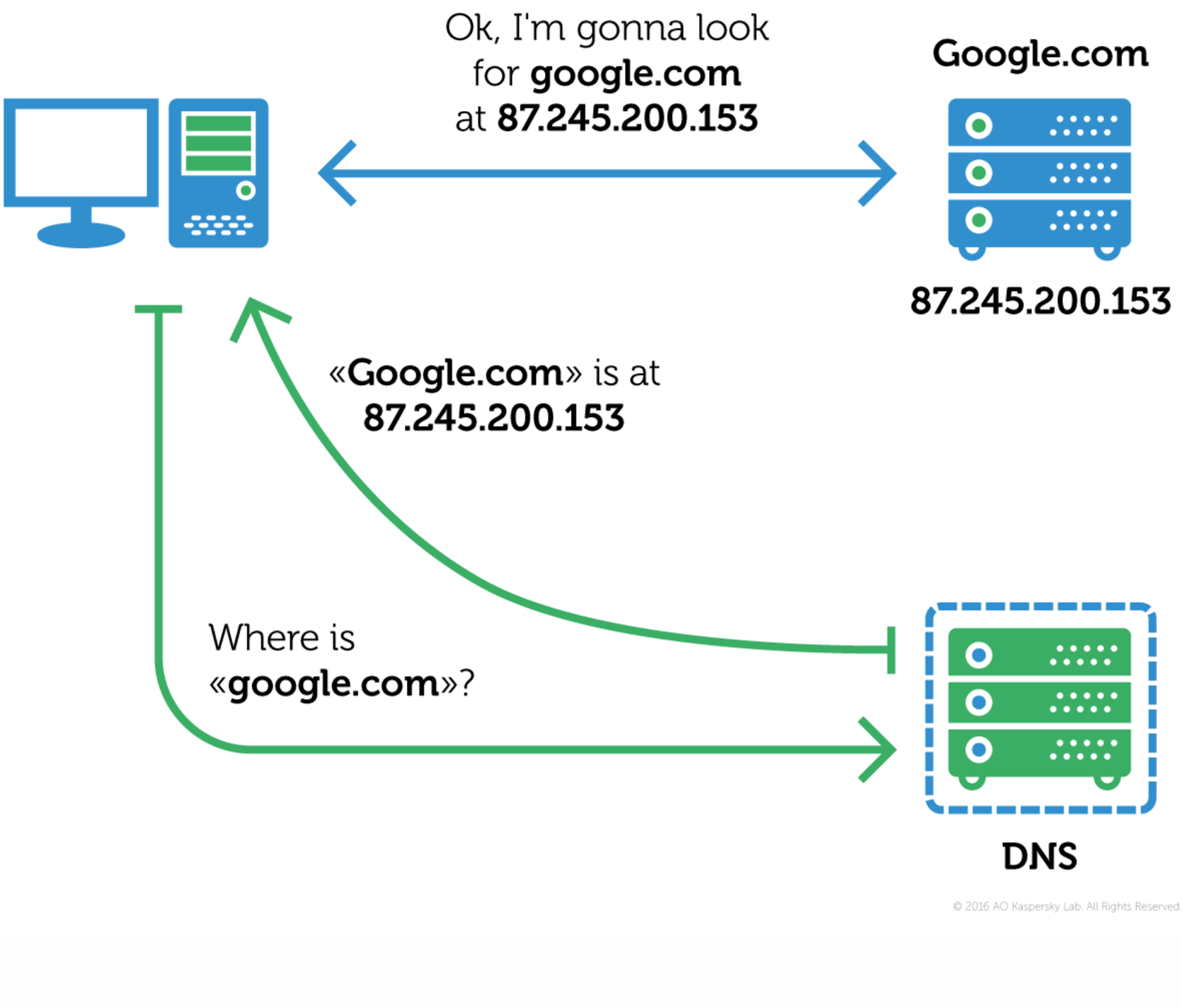
Create account

Next

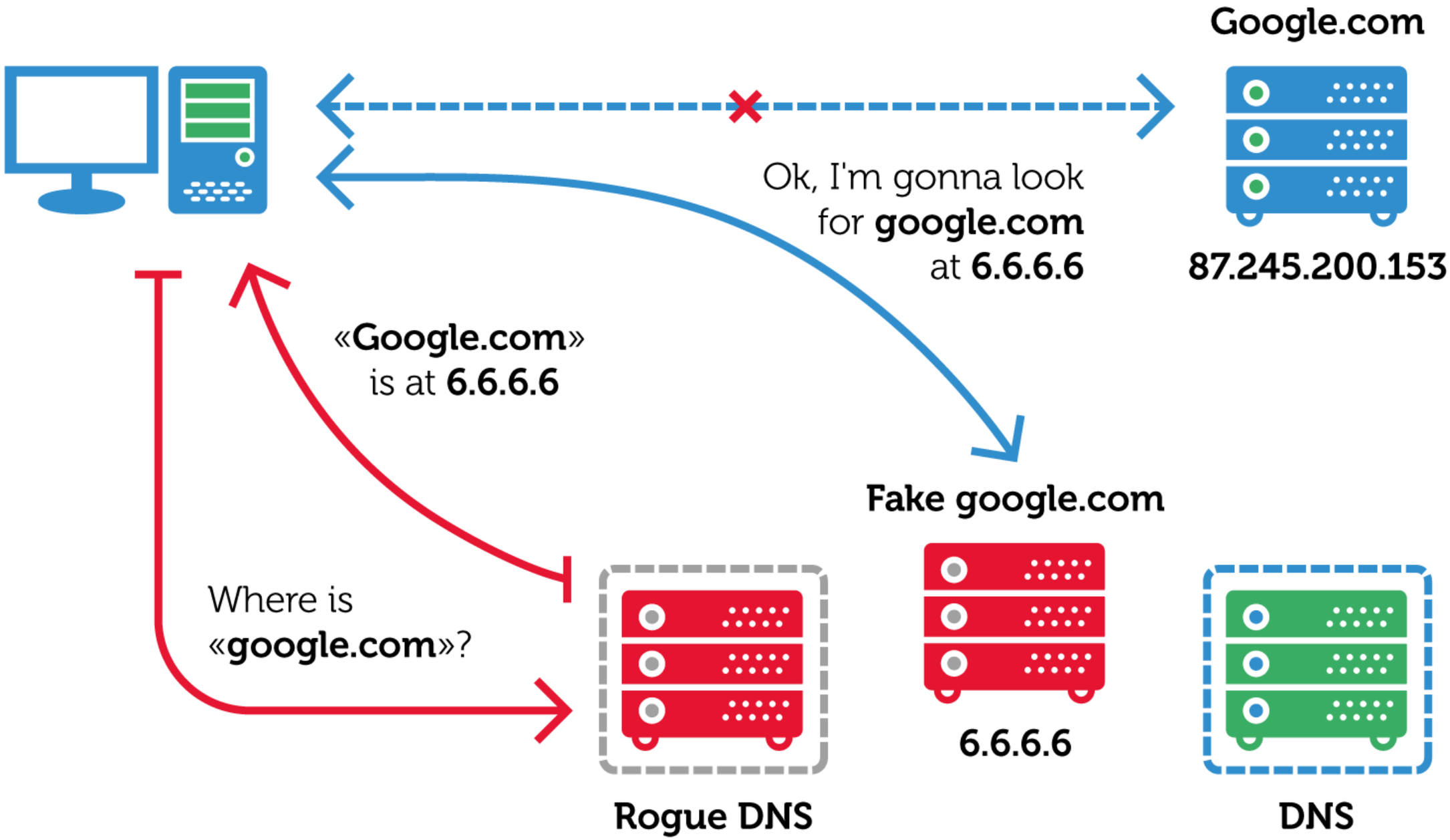
English (United States)

Help Privacy Terms

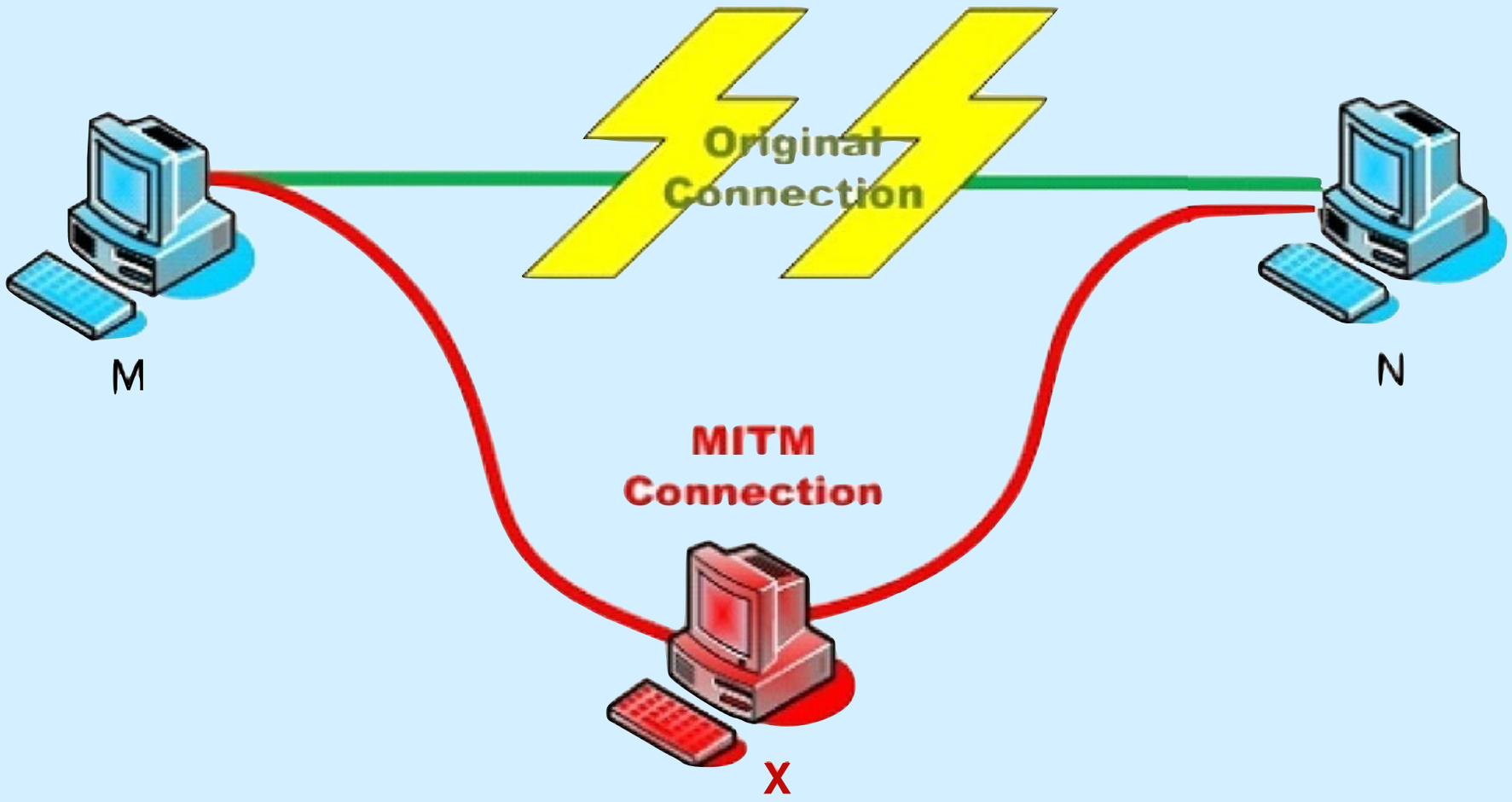
# DNS



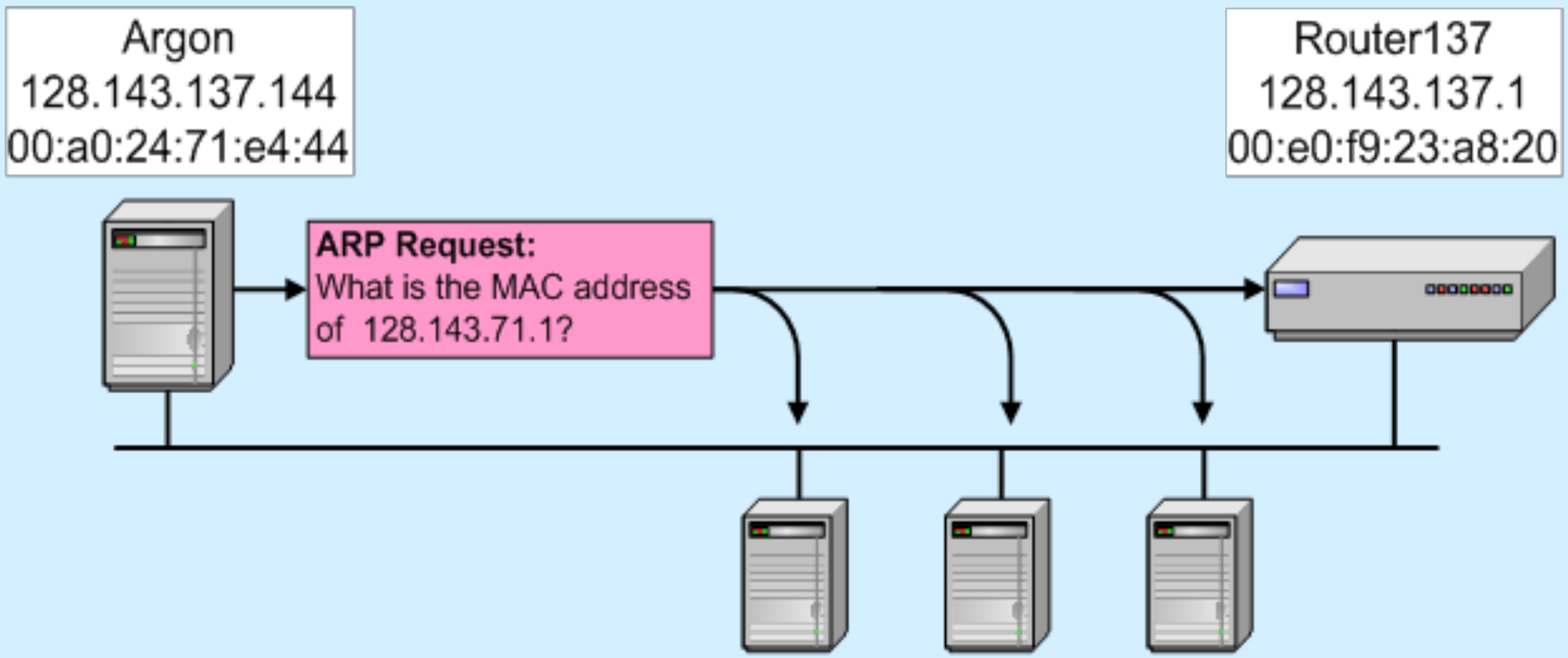
# DNS Hijacking



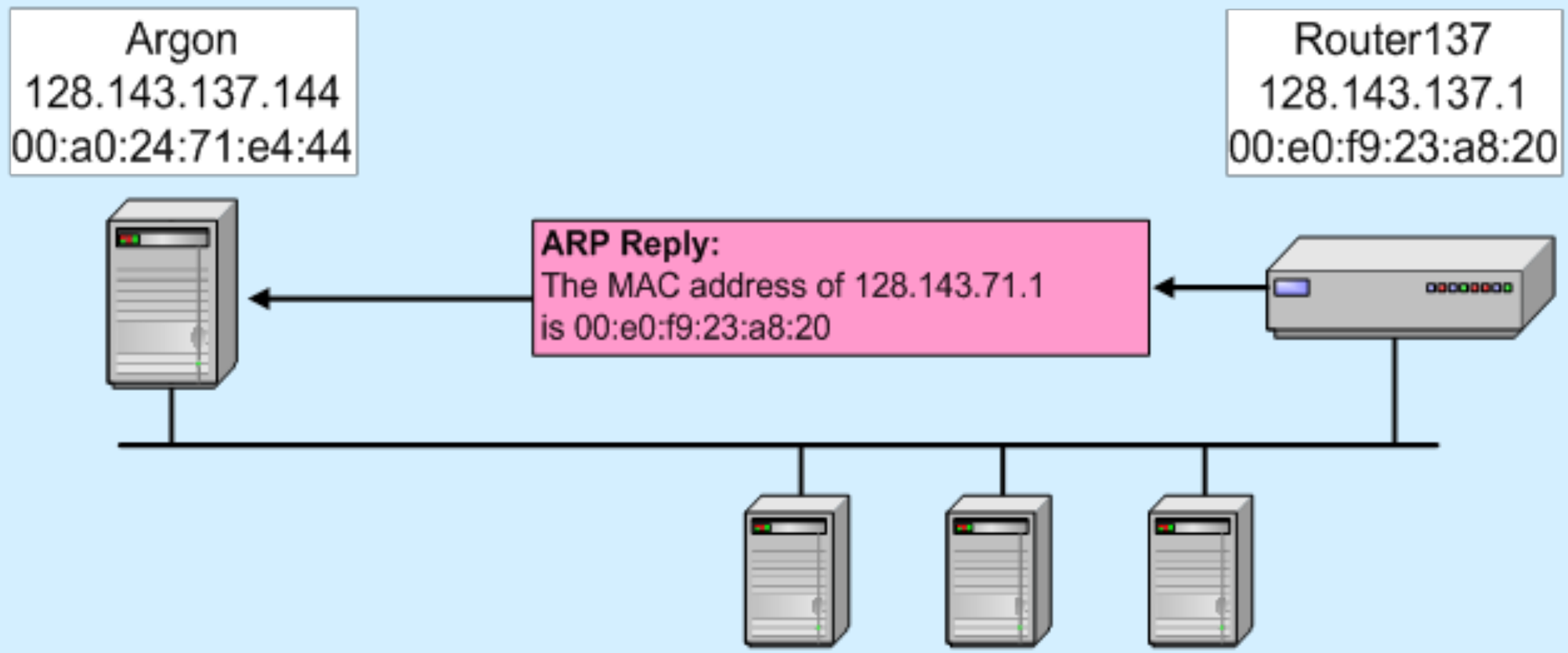
# ARP Spoofing



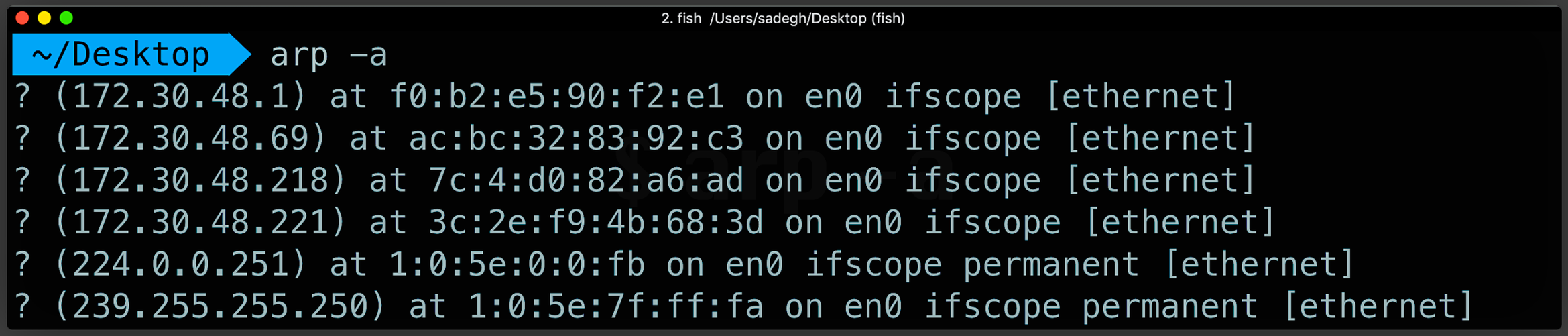
# How ARP Works?



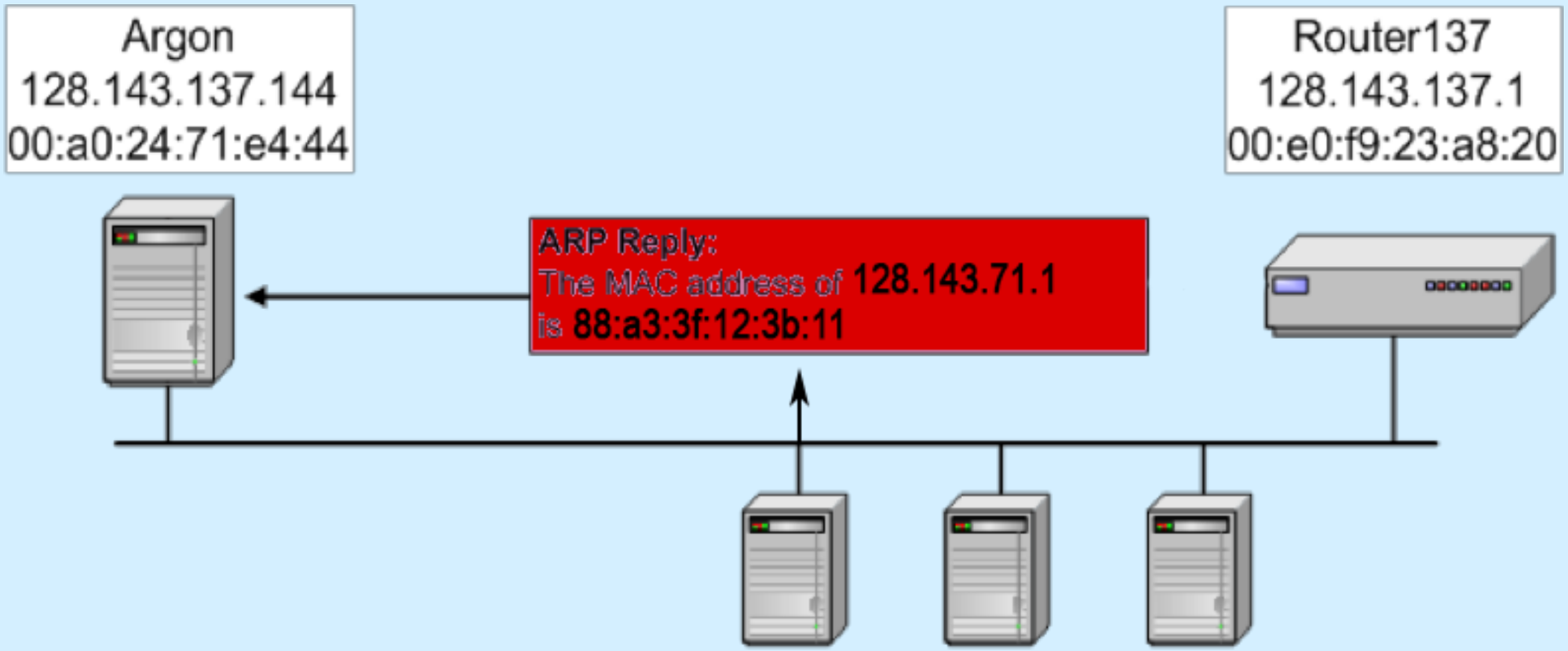
# How ARP Works?



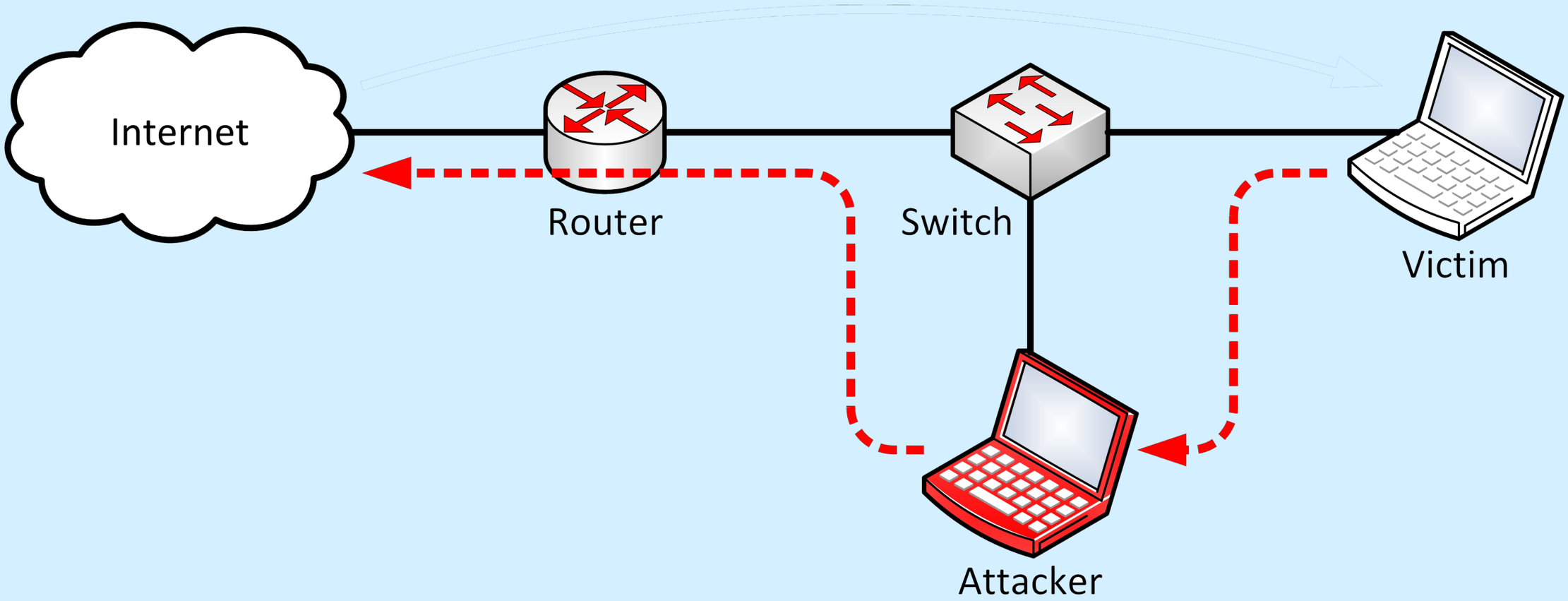
# ARP Cache


2. fish /Users/sadegh/Desktop (fish)
~/Desktop arp -a
? (172.30.48.1) at f0:b2:e5:90:f2:e1 on en0 ifscope [ethernet]
? (172.30.48.69) at ac:bc:32:83:92:c3 on en0 ifscope [ethernet]
? (172.30.48.218) at 7c:4:d0:82:a6:ad on en0 ifscope [ethernet]
? (172.30.48.221) at 3c:2e:f9:4b:68:3d on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]

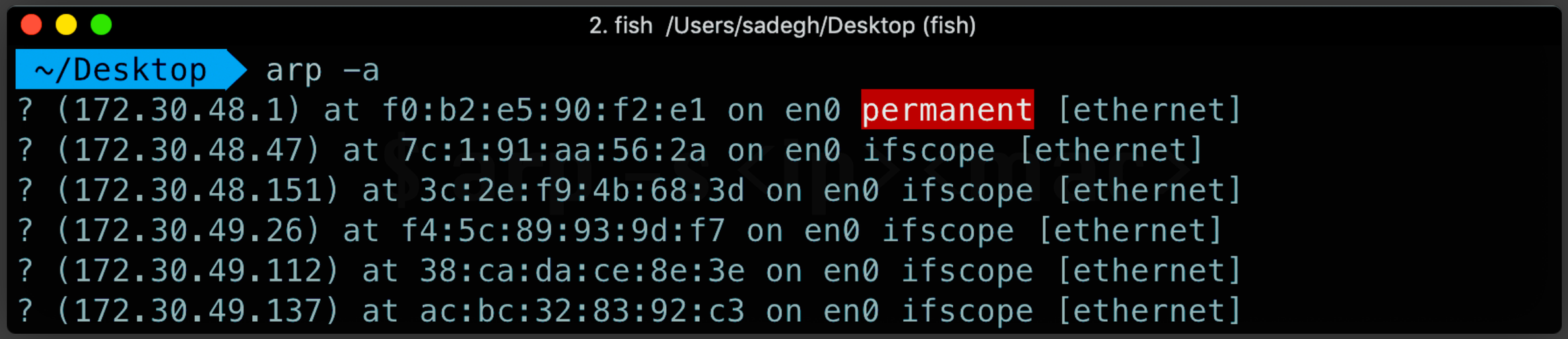
# ARP Spoofing



# ARP Spoofing

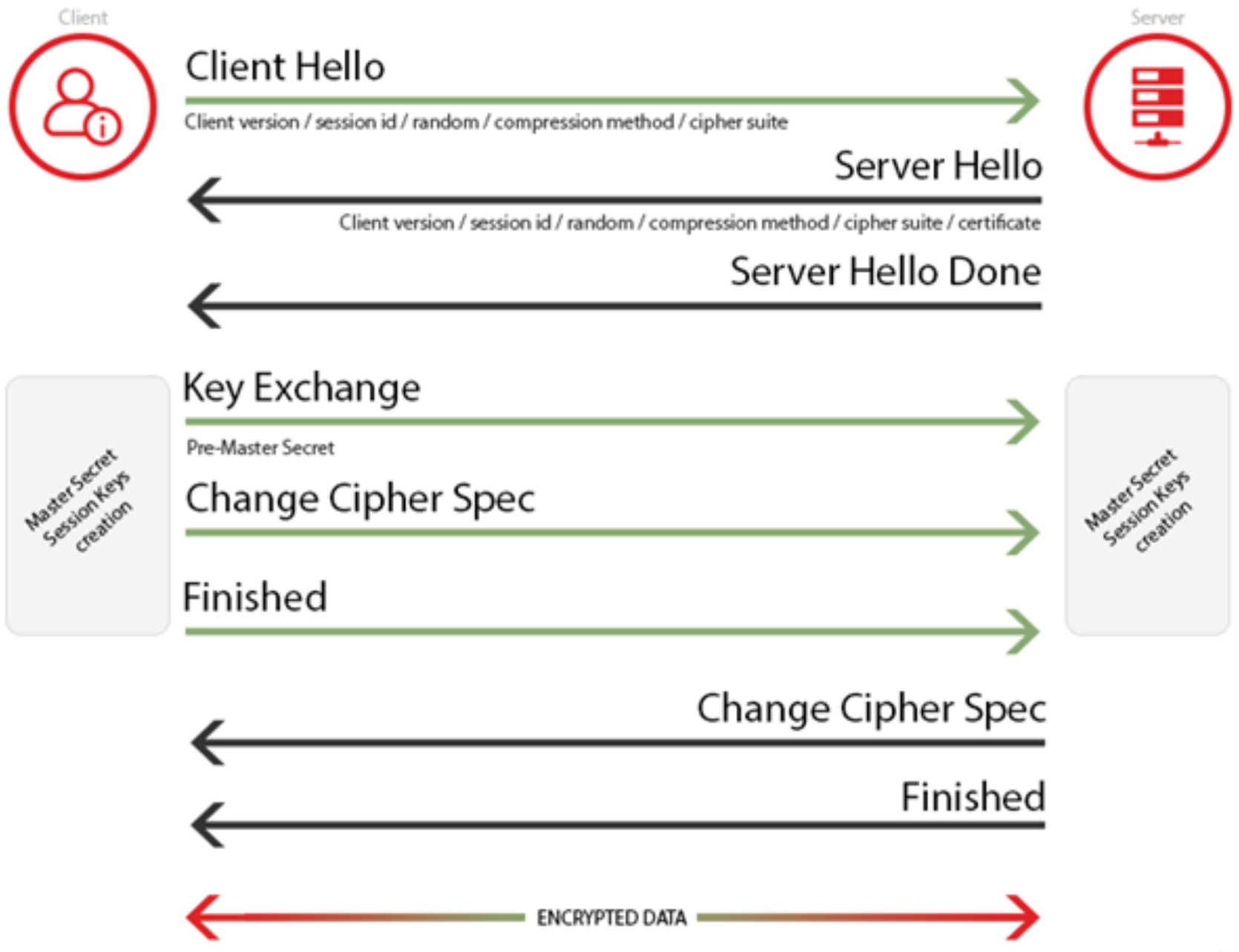


# ARP Spoof Defenses

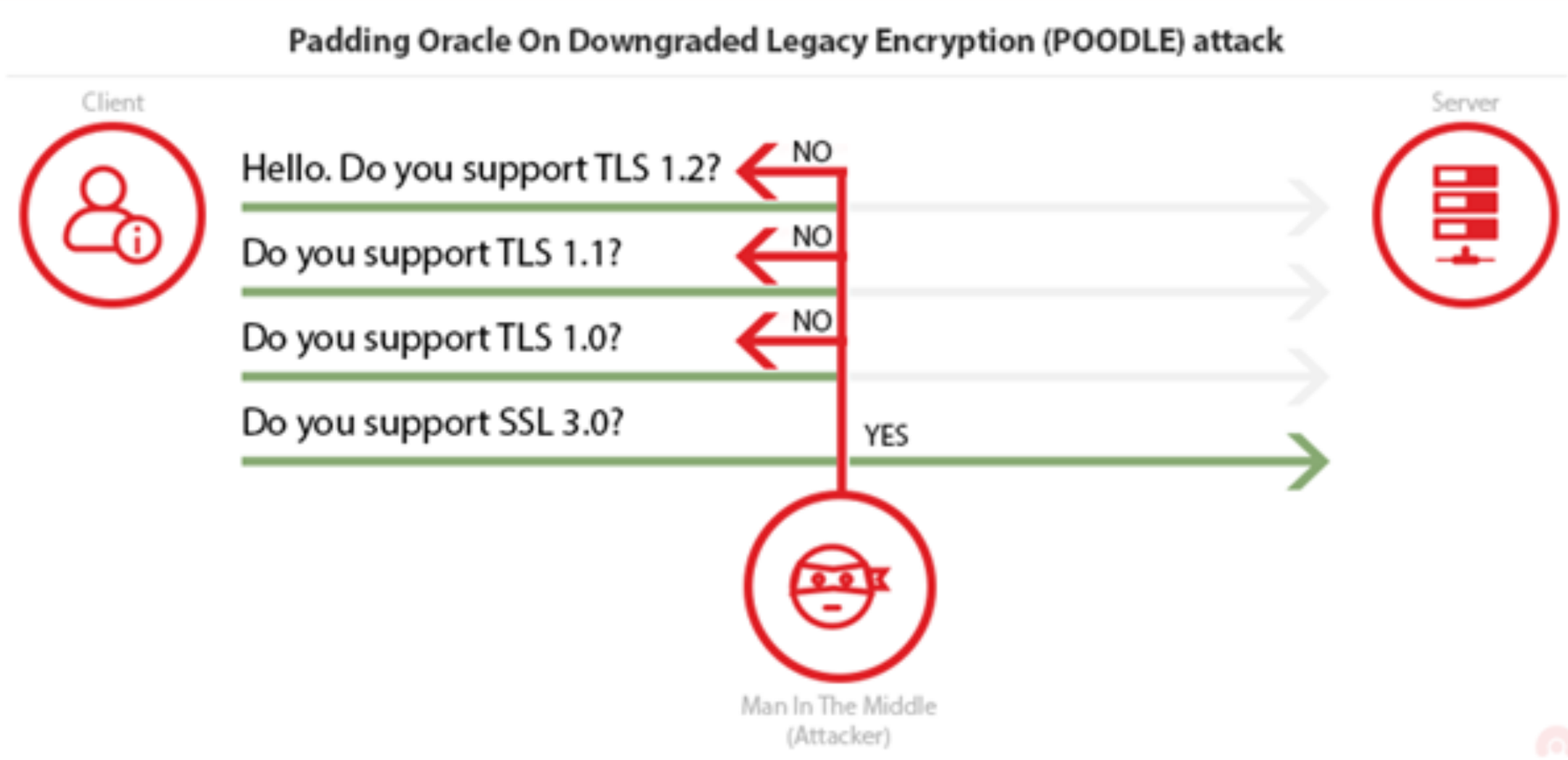



CLONE
</>

# SSL

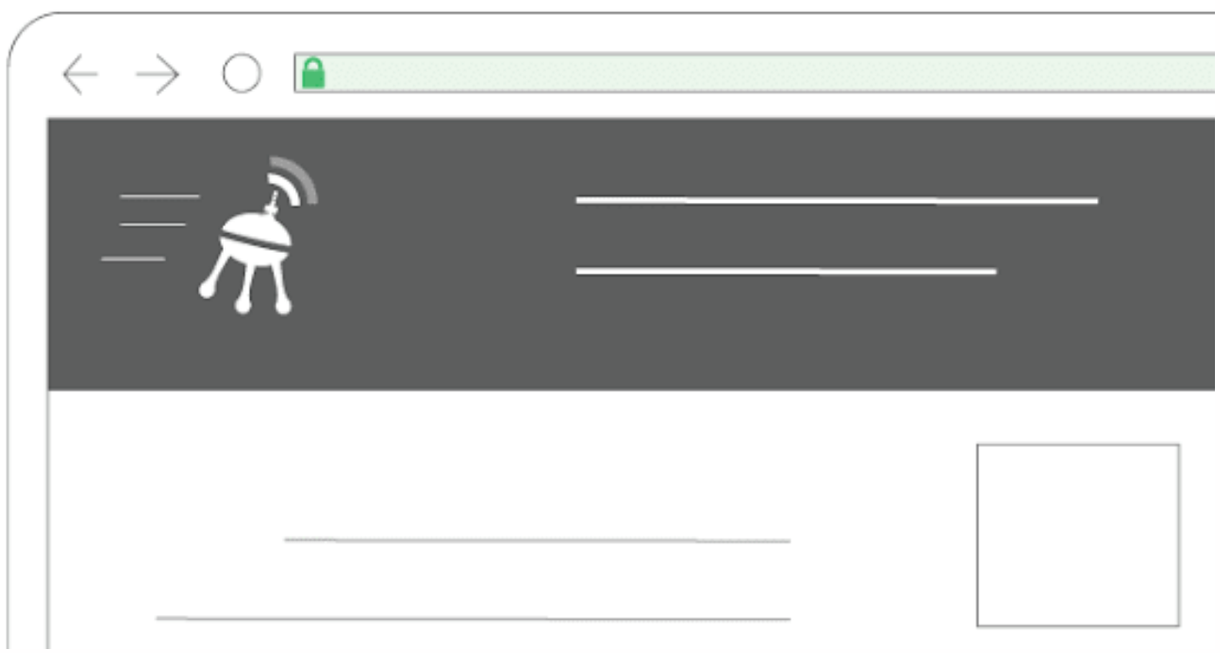

Client
Server
Client Hello
Client version / session id / random / compression method / cipher suite
Server Hello
Client version / session id / random / compression method / cipher suite / certificate
Server Hello Done
Key Exchange
Pre-Master Secret
Master Secret
Session Keys
creation
Change Cipher Spec
Finished
Master Secret
Session Keys
creation
Change Cipher Spec
Finished
ENCRYPTED DATA

# SSL STRIP


Padding Oracle On Downgraded Legacy Encryption (POODLE) attack
Client
Server
Hello. Do you support TLS 1.2?
NO
Do you support TLS 1.1?
NO
Do you support TLS 1.0?
NO
Do you support SSL 3.0?
YES
Man In The Middle
(Attacker)

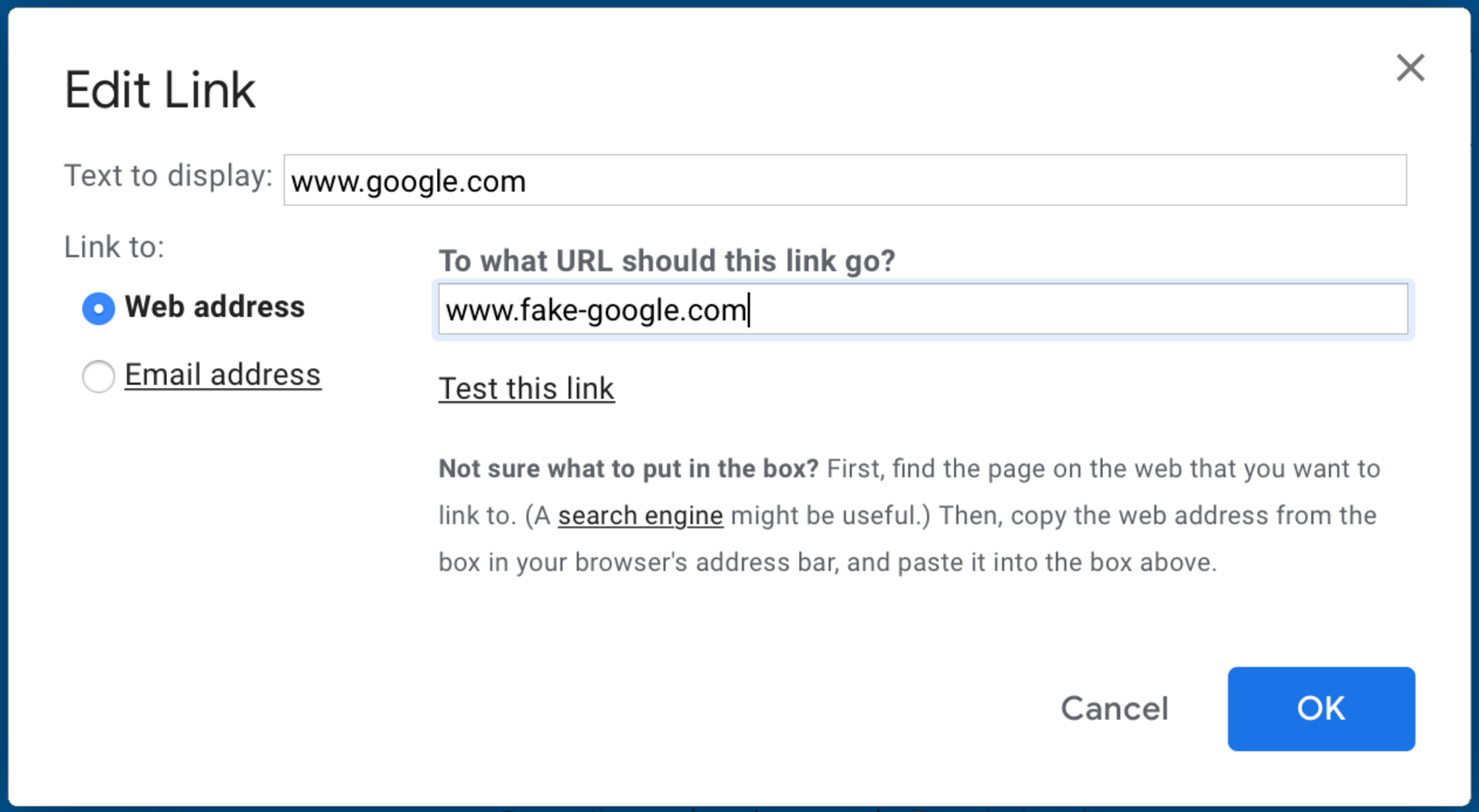
# HTTP Strict Transport Security (HSTS)

HSTS does not allow an unsecure version of a page to be shown by the browser



# Link Manipulation

# Hiding the URL



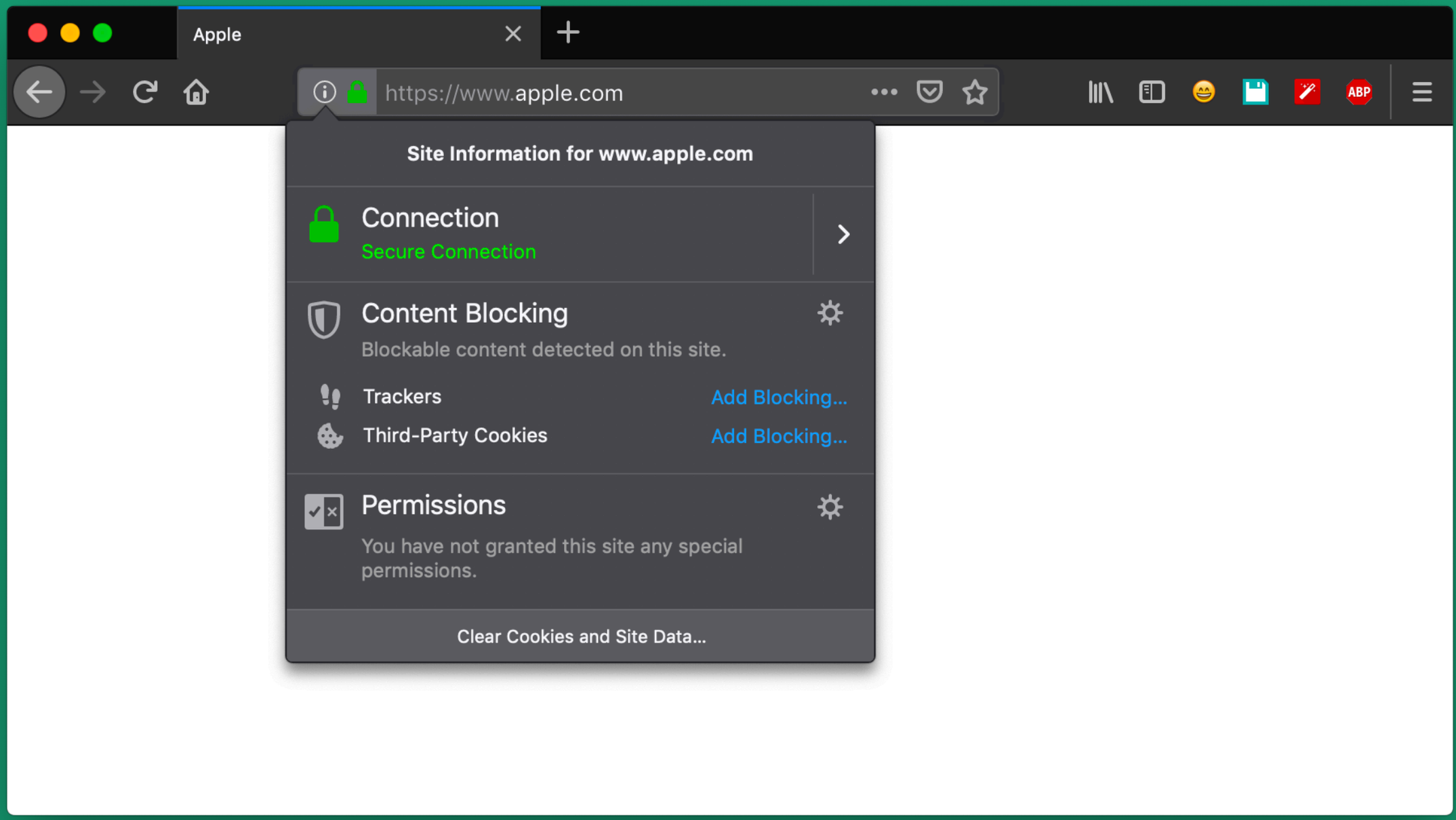
# Typosquatting

- A common misspelling: **exemple.com**
- A misspelling based on typos: **examlpe.com**
- A differently phrased domain name: **examples.com**
- A different top-level domain: **example.org**
- An abuse of the Top-Level Domain: **example.om**
- Missing dot typos: **wwwexample.com**

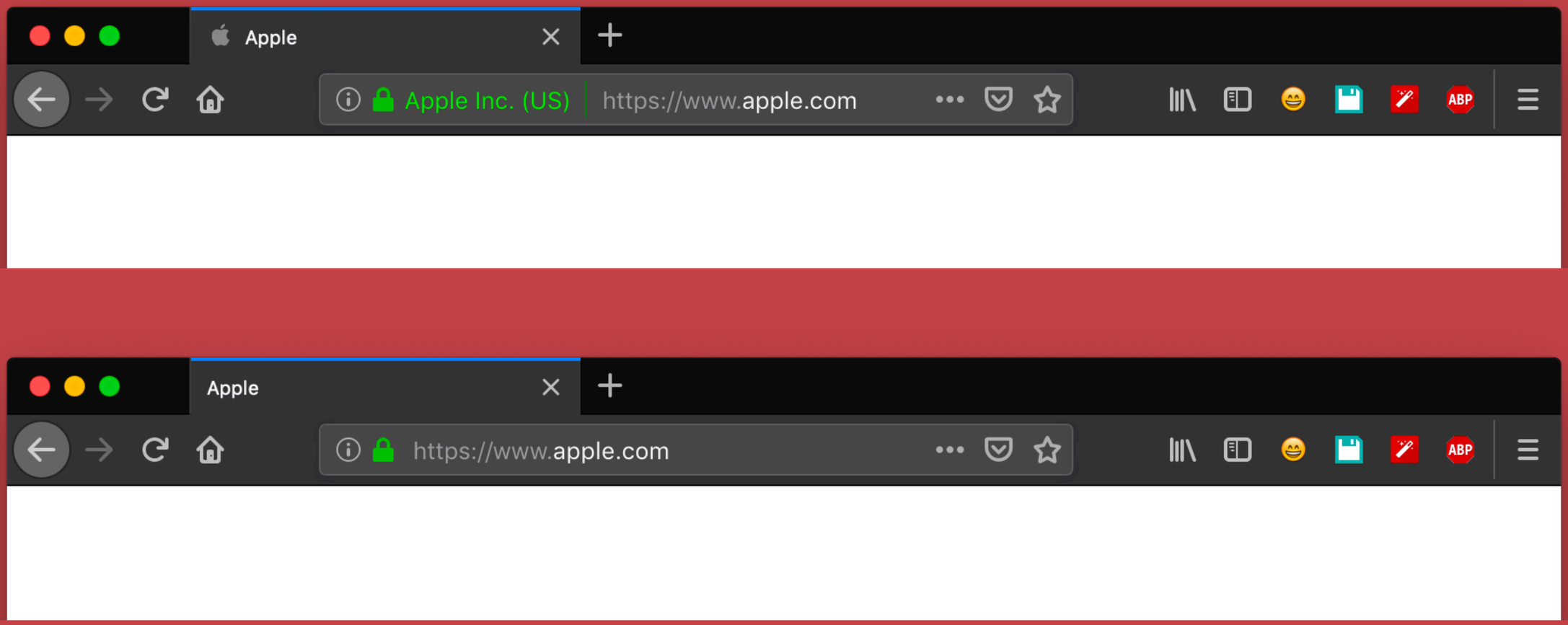
# DNSTWIST

```
dnstwist 1.02b by <marcin@ulikowski.pl>

usage: ./dnstwist.py [OPTION]... DOMAIN

Find similar-looking domain names that adversaries can use to attack you. Can
detect typosquatters, phishing attacks, fraud and corporate espionage. Useful
as an additional source of targeted threat intelligence.

positional arguments:
  domain                domain name or URL to check

optional arguments:
  -h, --help            show this help message and exit
  -c, --csv             print output in CSV format
  -j, --json            print output in JSON format
  -r, --registered      show only registered domain names
  -w, --whois           perform lookup for WHOIS creation/update time (slow)
  -g, --geoip           perform lookup for GeoIP location
  -b, --banners         determine HTTP and SMTP service banners
  -s, --ssdeep          fetch web pages and compare their fuzzy hashes to
                        evaluate similarity
  -m, --mxcheck         check if MX host can be used to intercept e-mails
  -d FILE, --dictionary FILE
                        generate additional domains using dictionary FILE
  -t NUMBER, --threads NUMBER
                        start specified NUMBER of threads (default: 10)
elceef@osiris:~/dnstwist$
```

# Is it safe?

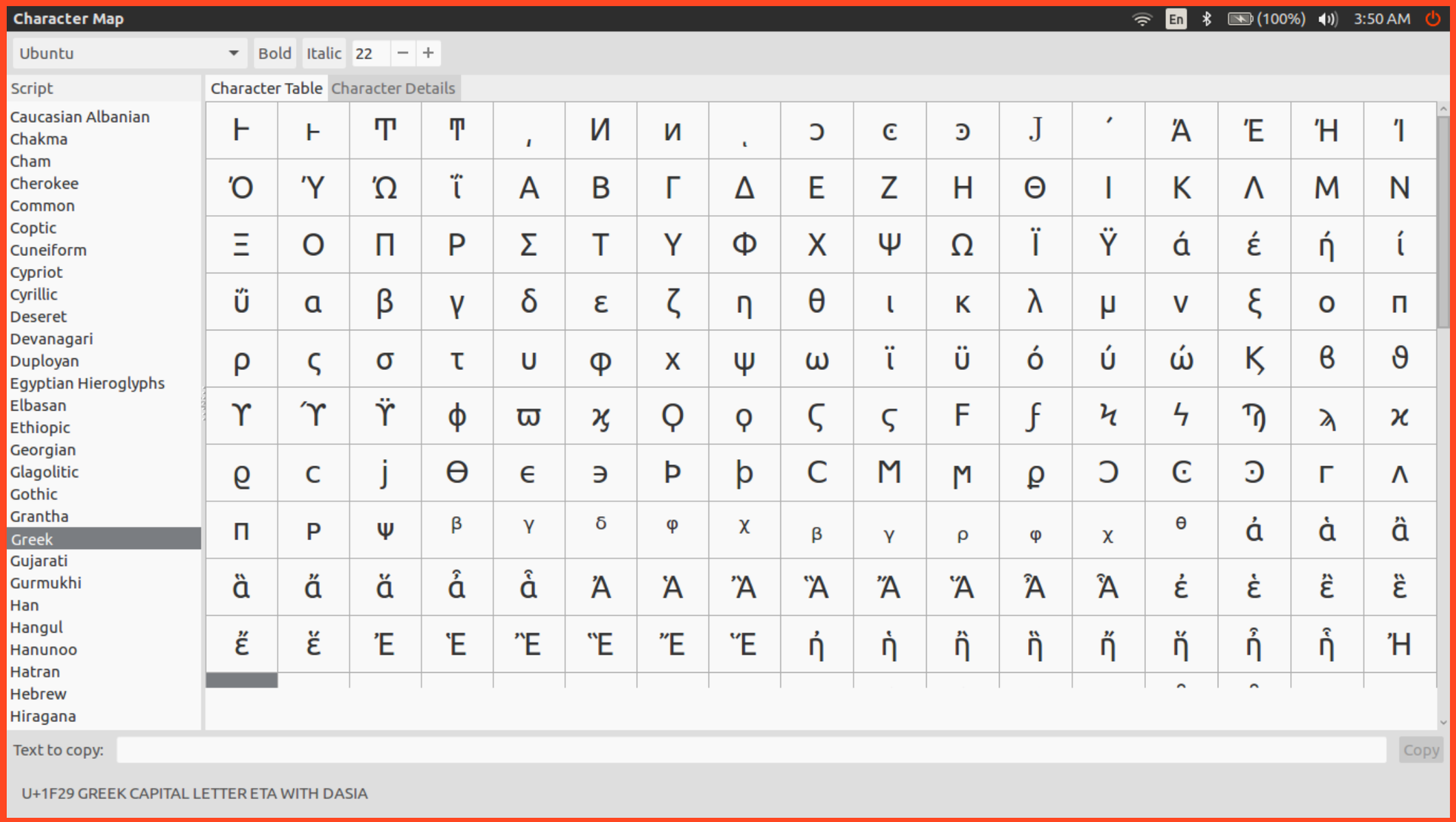

Apple
https://www.apple.com
Site Information for www.apple.com
Connection
Secure Connection
Content Blocking
Blockable content detected on this site.
Trackers
Add Blocking...
Third-Party Cookies
Add Blocking...
Permissions
You have not granted this site any special permissions.
Clear Cookies and Site Data...

# No!


Apple
Apple Inc. (US)
https://www.apple.com
ABP

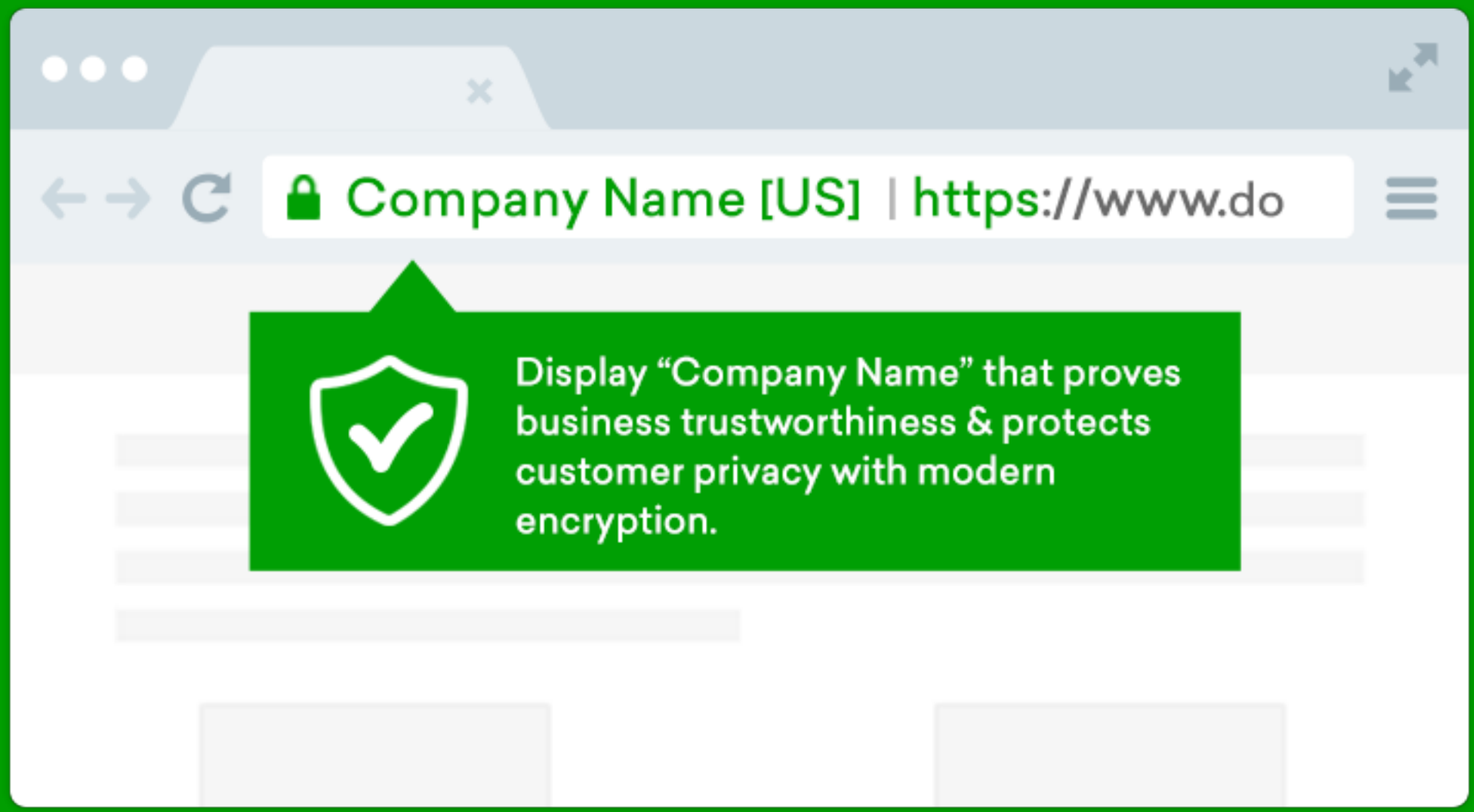

Apple
https://www.apple.com
ABP

# Homograph attacks



# Homograph attacks

# Extended Validation SSL Certificate



# Email Phishing

# Email Spoofing

```
Feedback-ID: 27-RECOVERY-anexp#givab-fa--mdv2-fa:account-notifier
X-Notifications: 7034de9cf9000000
Message-ID: <si4avgGDzO9aarxMBhzO3g.0@notifications.google.com>
Subject: Critical security alert for your linked Google Account
From: Google <no-reply@accounts.google.com>
To: hayerisadegh@gmail.com
Content-Type: multipart/alternative; boundary="000000000000505bce057e035f2b"

--000000000000505bce057e035f2b
Content-Type: text/plain; charset="UTF-8"; format=flowed; delsp=yes
Content-Transfer-Encoding: base64

WW91ciBhY2NvdW50IGhheWVyaXNhZGVnaEBnbWFpbC5jb20gaXMgbGlzdGVkIGFzIHRoZSByZWNv
dmVyeSBlbWFpbCBmb3INCmFqb29yc2VydmVyQGdtYWlsLmNvbS4gRG9uJ3QgcmVjb2duaXplIHRo
aXMgYWNjb3VudD8gQ2xpY2sgaGVyZQ0KPGh0dHBzOi8vYWNjb3VudHMuZ29vZ2xlLmNvbS9BY2Nv
dW50RGlzYXZvdz9hZHQ9QU9YOGtpckwySTMyUGw2bWs3eUptdlNDZ05BN3JwRzJOQjZRZjZnMTl5
d1Jjd09mclAyYWEtSUI3b21RUS1ERl9uVVMmcmZuPTI3JmFuZXhwPWdpdmFiLWZhLS1tZHYyLWZh
Pg0KU2lnbi1pbiBhdHRlbXB0IHdhcyBibG9ja2VkIGZvciB5b3VyIGxpbmtlZCBHb29nbGUgQWNj
b3VudA0KDQoNCmFqb29yc2VydmVyQGdtYWlsLmNvbQ0KU29tZW9uZSBqdXN0IHVzZWQgeW91ciBw
YXNzd29yZCB0byB0cnkgdG8gc2lnbiBpbiB0byB5b3VyIGFjY291bnQgZnJvbSBhDQpub24tR29v
Z2xlIGFwcC4gR29vZ2xlIGJsb2NrZWQgdGhlbSwgYnV0IHlvdSBzaG91bGQgY2hlY2sgd2hhdCBo
YXBwZW5lZC4NClJldmlld2lldyB5b3VyIGFjY291bnQgYWN0aXZpdHkgdG8gbWFrZSBzdXJlIG5v
ZSBlbHNlIGhhcyBhY2Nlc3MuDQpDaGVjayBhY3Rpdml0eQ0KPGh0dHBzOi8vYWNjb3VudHMuZ29v
Z2xlLmNvbS9BY2NvdW50Q2hvb3Nlcj9FbWFpbD1ham9vcnNlcnZlckBnbWFpbC5jb20mY29udGlu
dWU9aHR0cHM6Ly9teWFjY291bnQuZ29vZ2xlLmNvbS9hbGVydC9udC8xNTQ1OTI3ODMxMDAwP3Jm
```

nail

Search mail

# Spoofed Email

Inbox ×

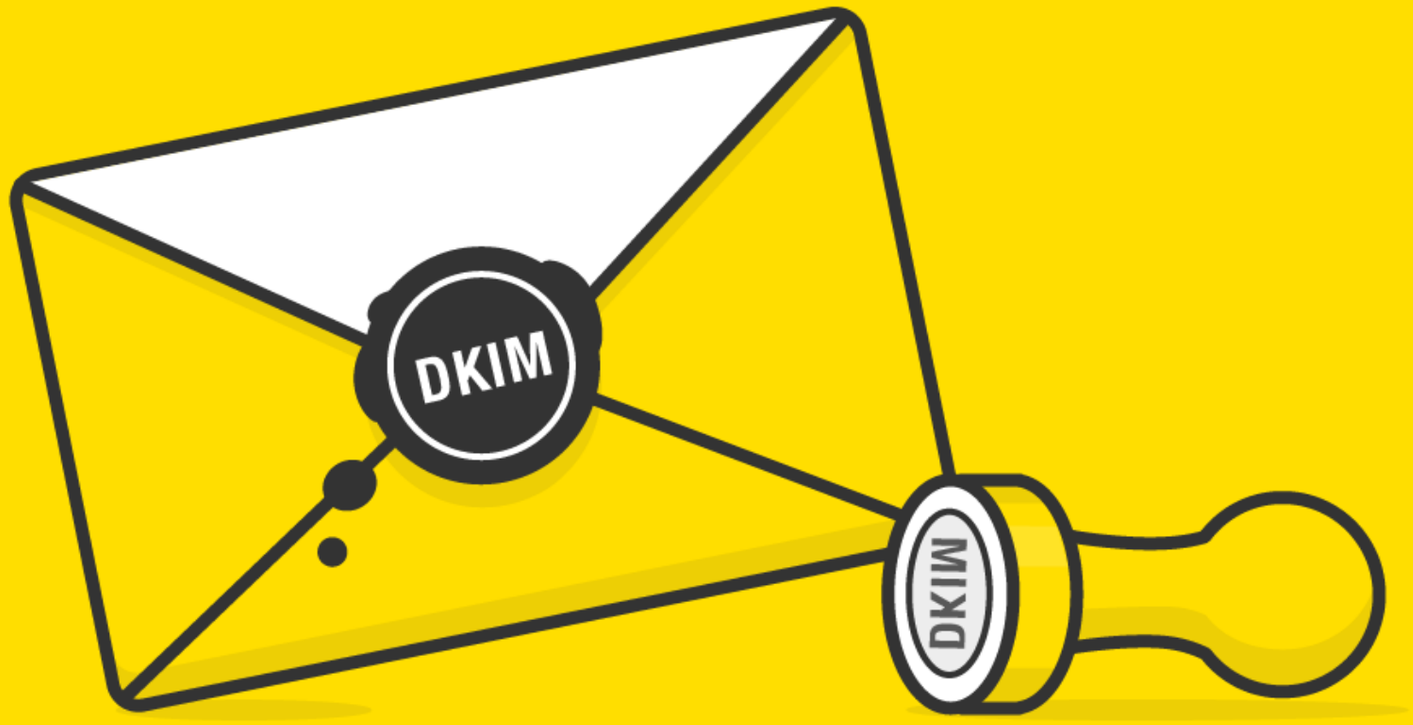
**spoofed@ut.ac.ir** <spoofed@ut.ac.ir>

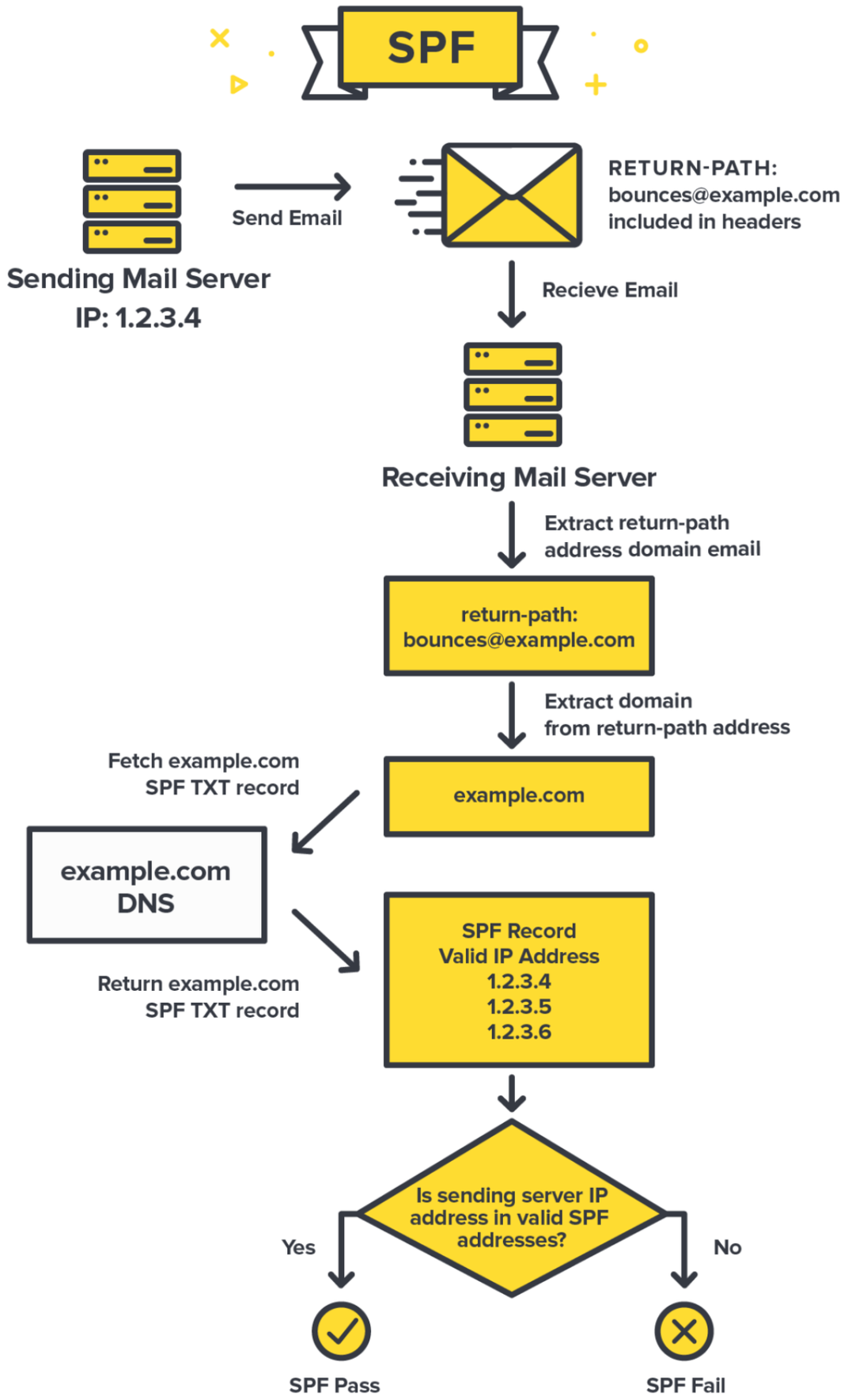
to me

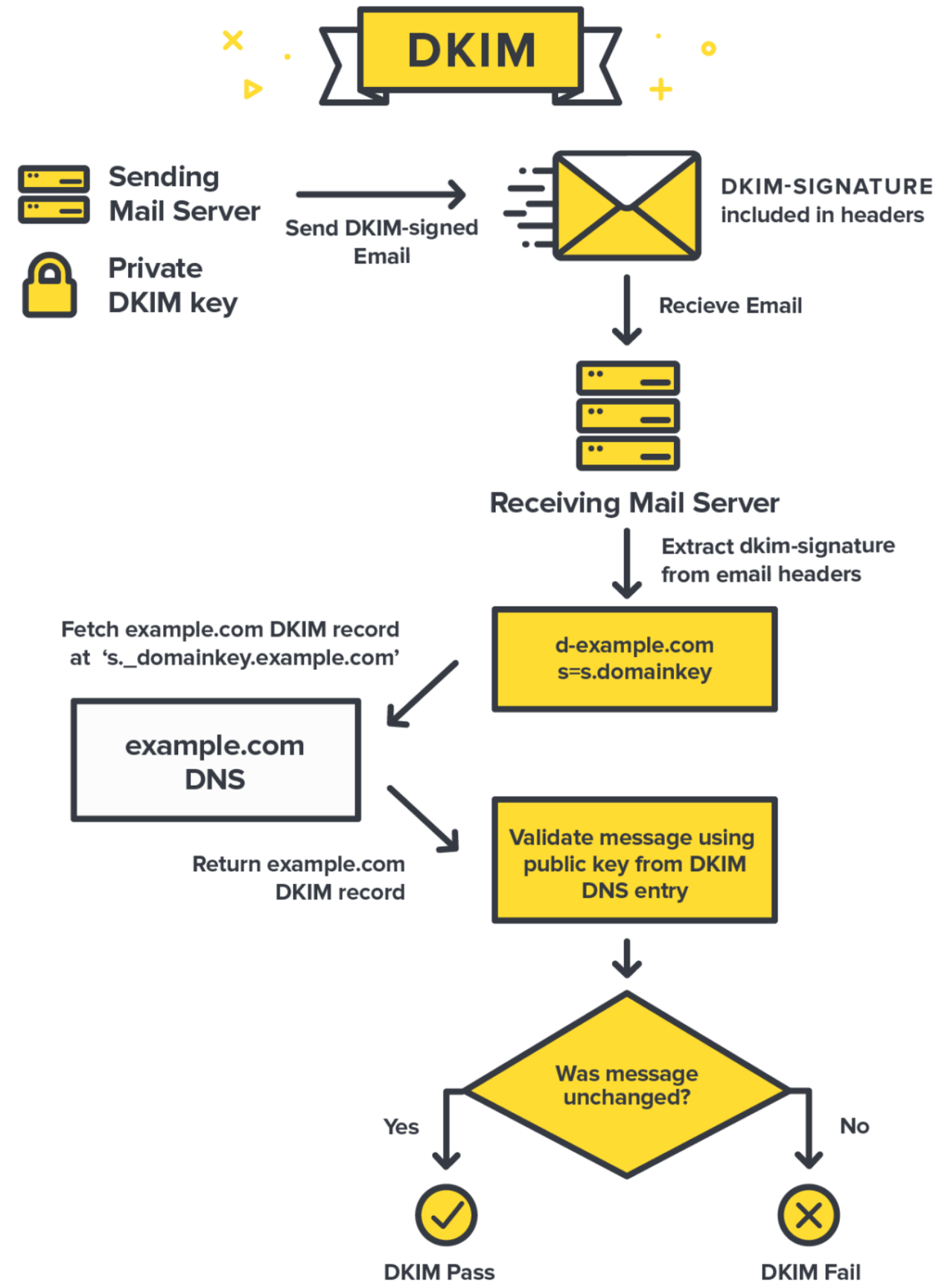
Reply

Forward

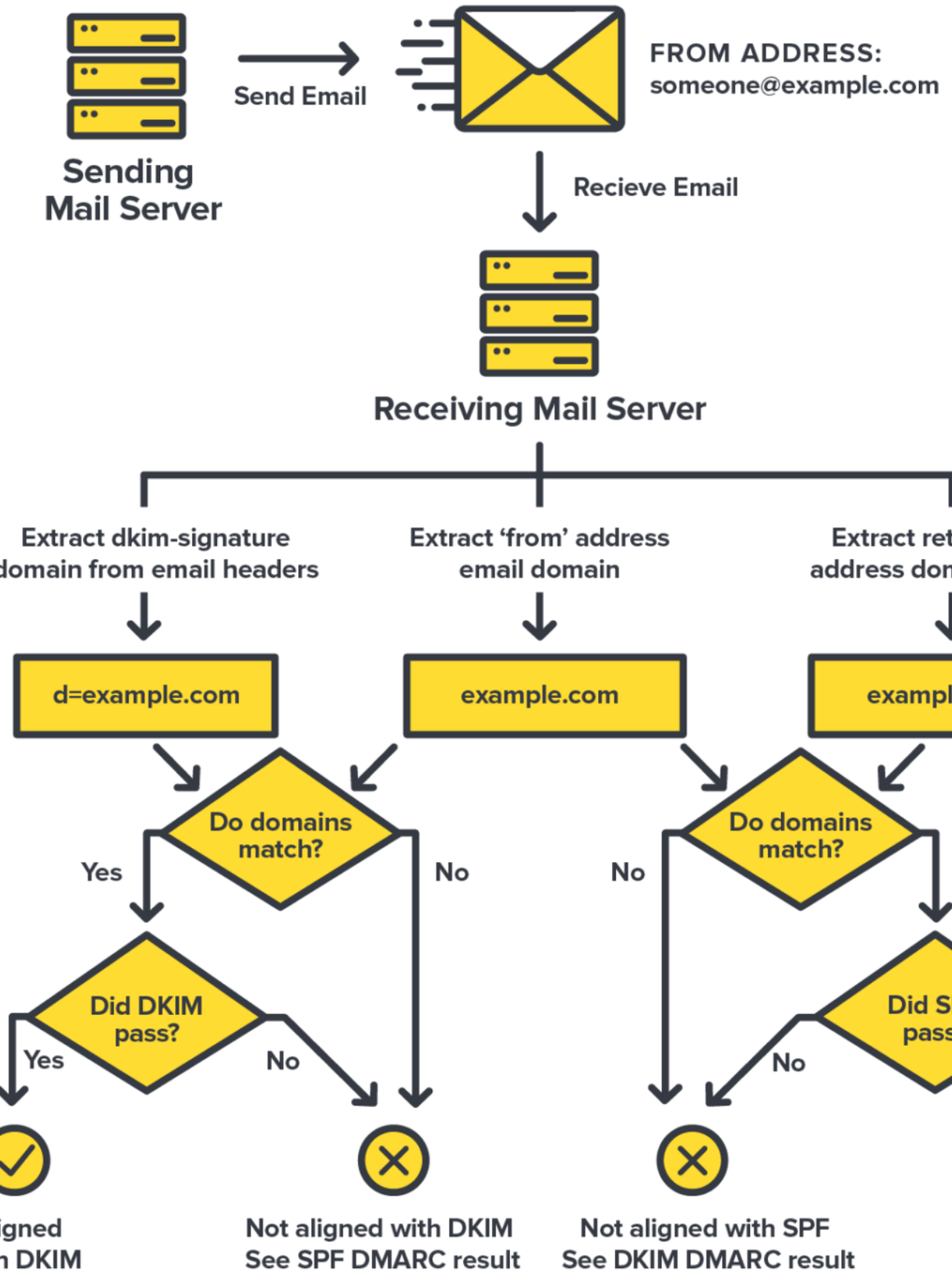
# Defense Email Spoofing




SPF
Send Email
Sending Mail Server
IP: 1.2.3.4
RETURN-PATH:
bounces@example.com
included in headers
Recieve Email
Receiving Mail Server
Extract return-path
address domain email
return-path:
bounces@example.com
Extract domain
from return-path address
Fetch example.com
SPF TXT record
example.com
example.com
DNS
SPF Record
Valid IP Address
1.2.3.4
1.2.3.5
1.2.3.6
Return example.com
SPF TXT record
Is sending server IP
address in valid SPF
addresses?
Yes
No
SPF Pass
SPF Fail


DKIM
Sending Mail Server
Private DKIM key
Send DKIM-signed Email
DKIM-SIGNATURE included in headers
Recieve Email
Receiving Mail Server
Extract dkim-signature from email headers
d-example.com s=s.domainkey
Fetch example.com DKIM record at 's._domainkey.example.com'
example.com DNS
Return example.com DKIM record
Validate message using public key from DKIM DNS entry
Was message unchanged?
Yes
No
DKIM Pass
DKIM Fail

# DMARC


Sending Mail Server
Send Email
FROM ADDRESS:
someone@example.com
Recieve Email
Receiving Mail Server
Extract dkim-signature domain from email headers
Extract 'from' address email domain
Extract return-path address domain email
d=example.com
example.com
example.com
Do domains match?
Yes
No
Did DKIM pass?
Yes
No
Do domains match?
No
Yes
Did SPF pass?
No
Yes
Aligned with DKIM
Not aligned with DKIM See SPF DMARC result
Not aligned with SPF See DKIM DMARC result
Aligned wth SPF

# Site Key

Bank of America Sign In

Secure Area | En Español

## Enter your Passcode

If your SiteKey is correct, enter your Passcode to sign in. If this isn't your SiteKey, do not enter your Passcode.

SiteKey lets you know you're at a Bank of America site and not a fraudulent one.

### Your SiteKey

site key name

Passcode

Sign in

Quick help

- Don't recognize your SiteKey?
- Are Passcodes case-sensitive?
- Forgot or need help with my Passcode

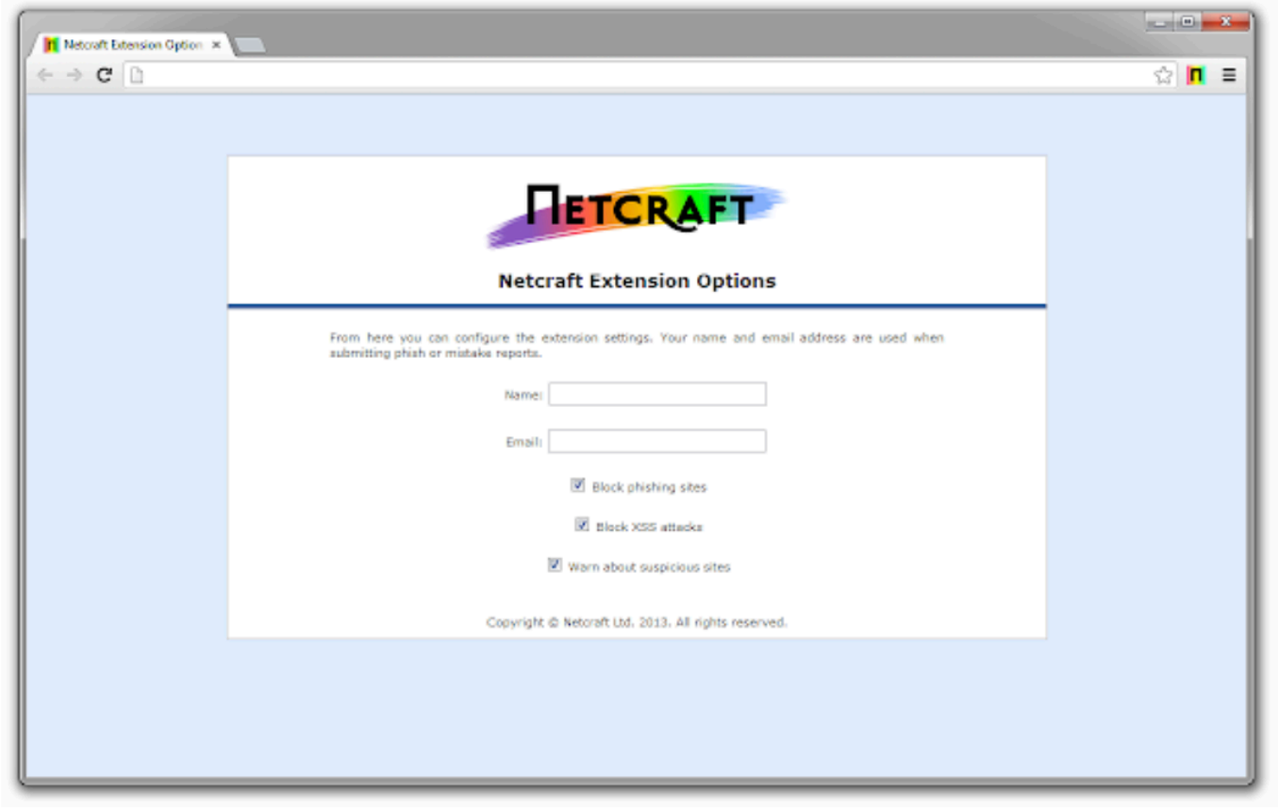
# Netcraft Extension

Offered by: www.netcraft.com

4.5 stars | 123 | Productivity | 40,726 users

Add to Chrome

Overview | Reviews | Support | Related



# DEMO