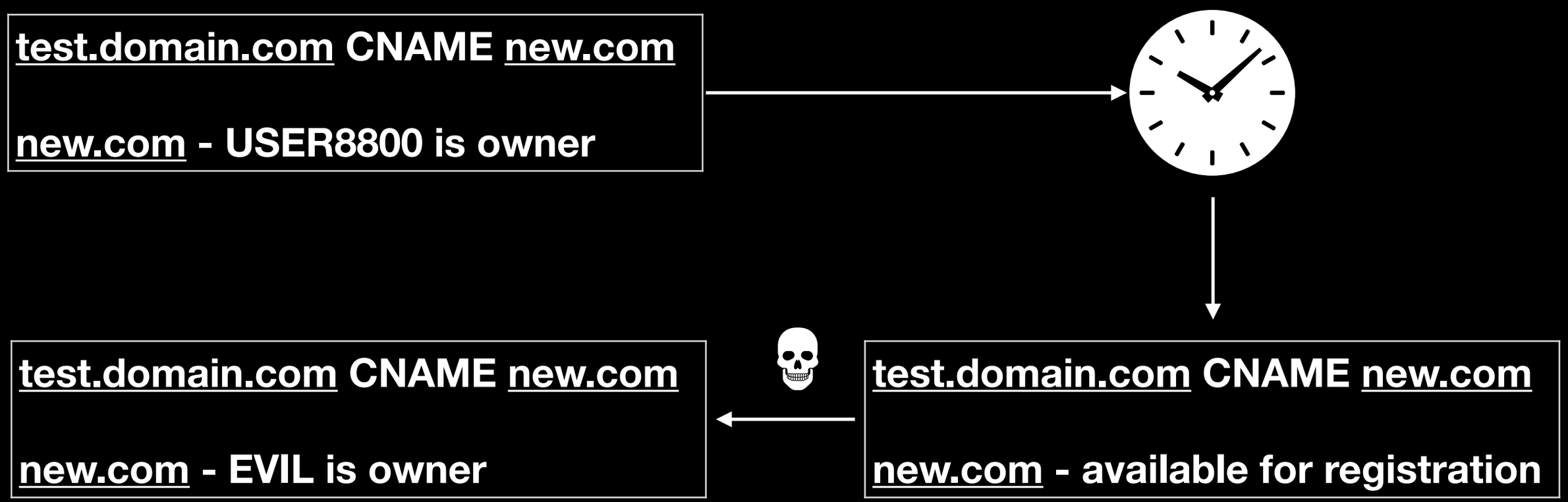
Subdomain takeover

wtf subdm. tkov.?

Subdomain takeover is a process of registering a non-existing domain name to gain control over another domain.

Main scenario:



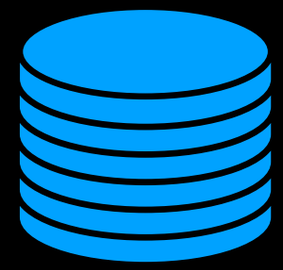
impact?

- **Fishing**
- **XSS**
- **Damage the reputation of the brand (witch associated with domain)**

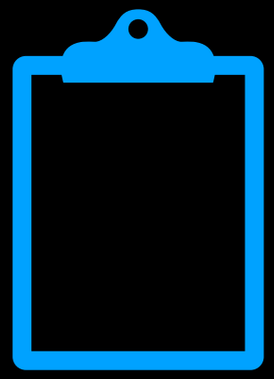
Schematics

Web browser

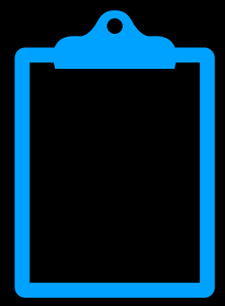
1. Give address of test.domain.com



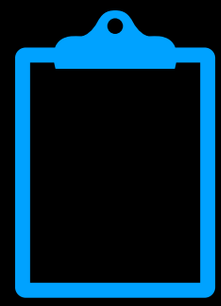
Recursive DNS resolver



Web server on new.com
IP: 1.3.3.7

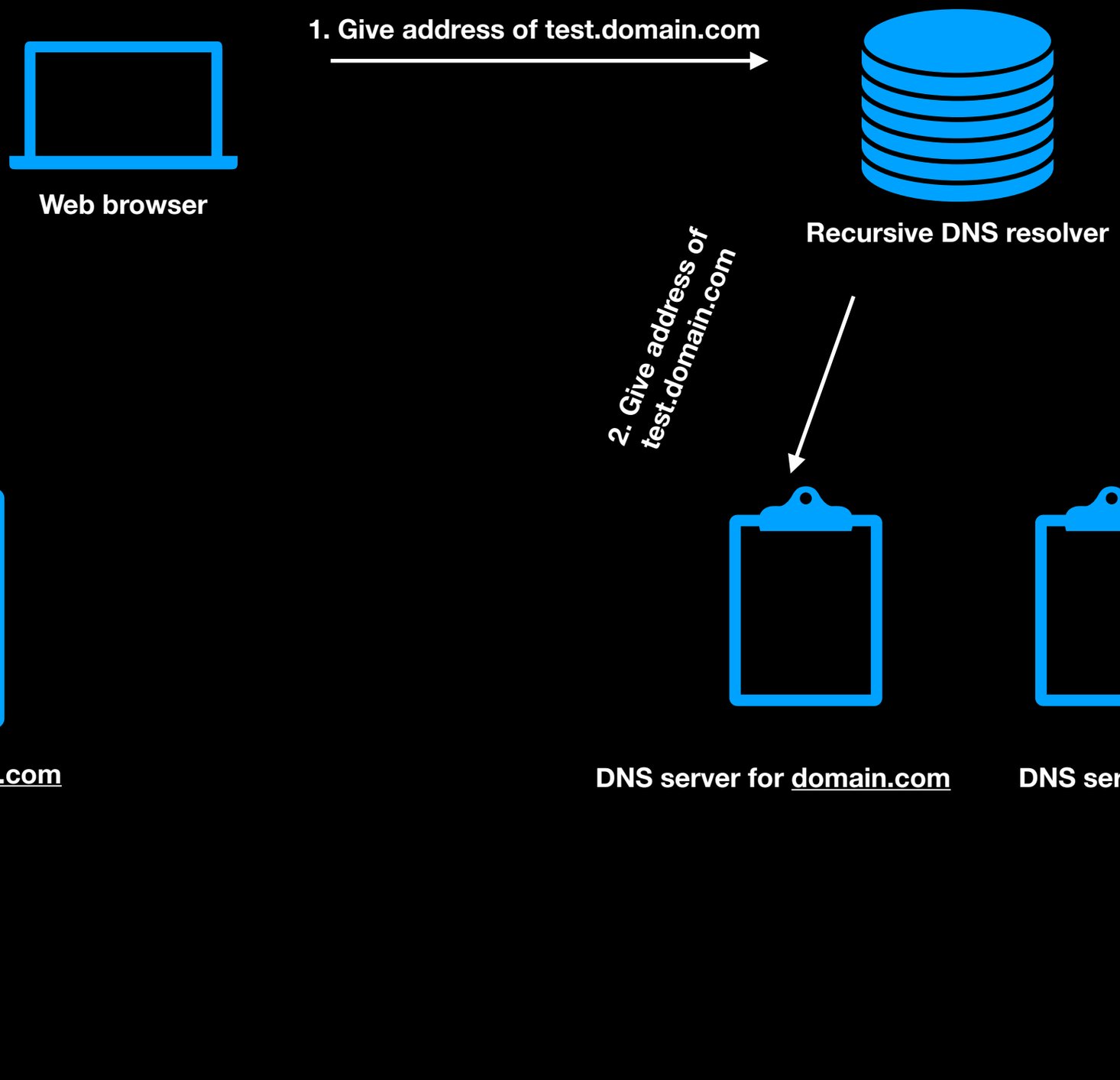


DNS server for domain.com

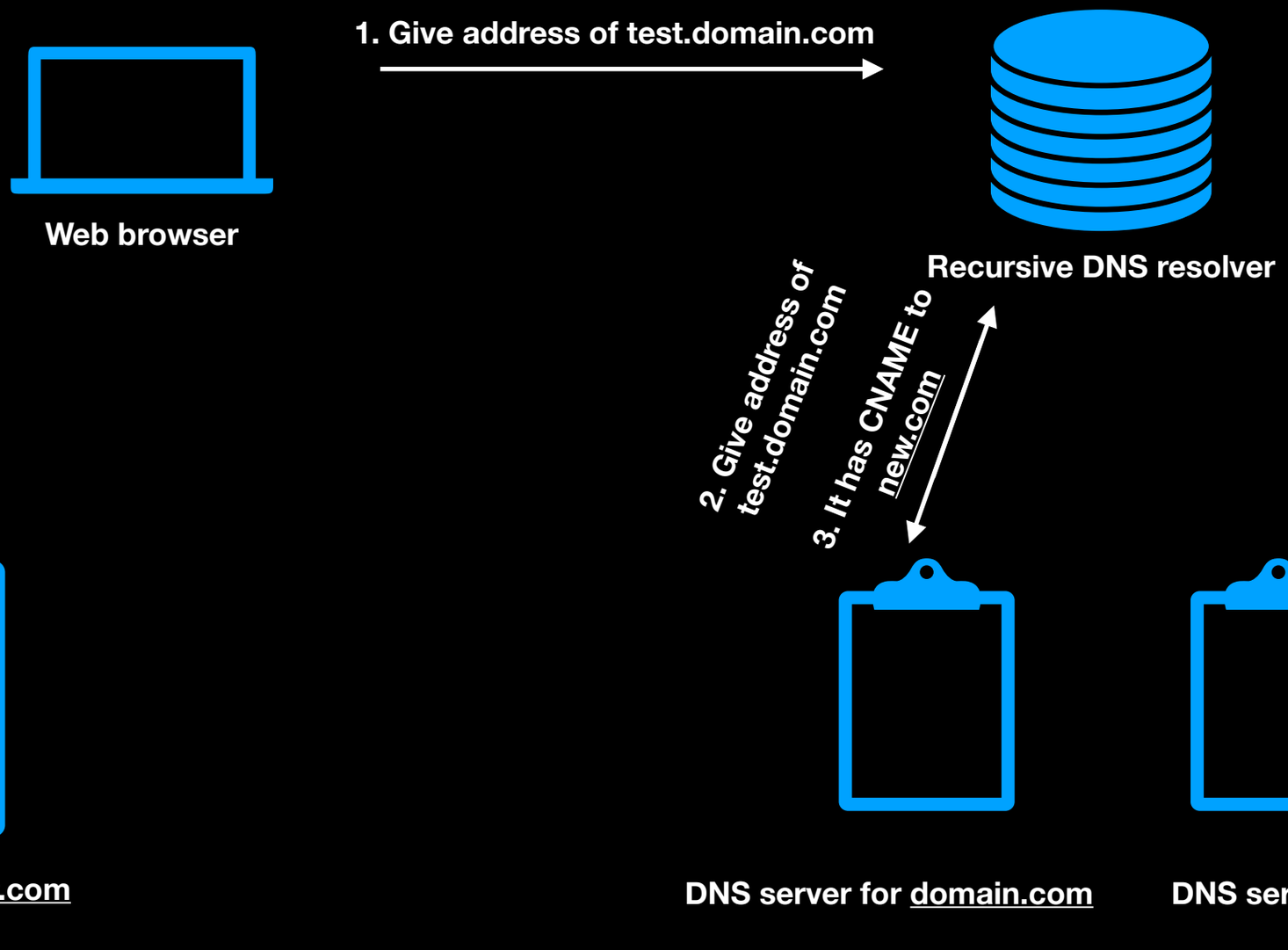


DNS server of new.com

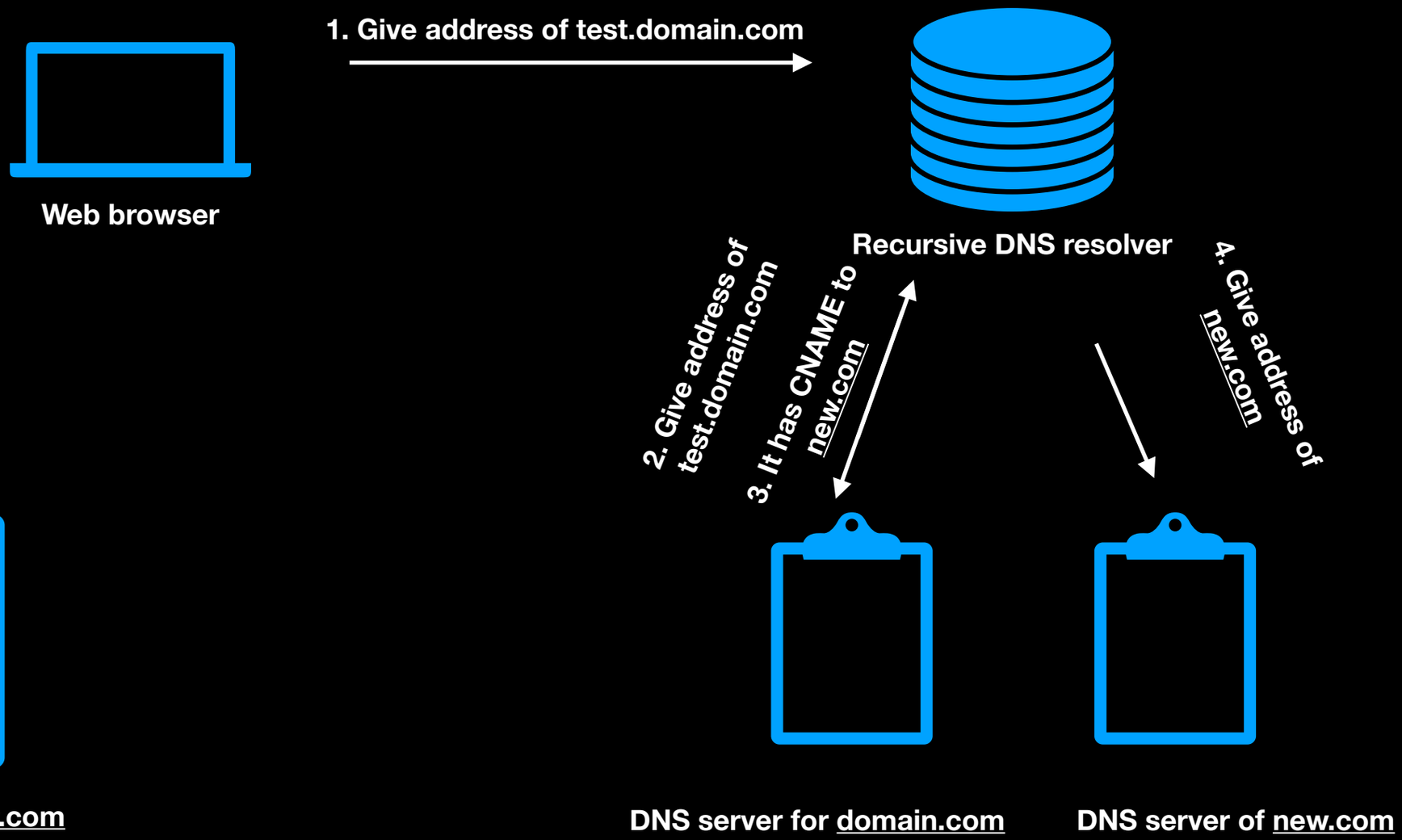
Schematics


1. Give address of test.domain.com
Web browser
Recursive DNS resolver
2. Give address of test.domain.com
Web server on new.com
IP: 1.3.3.7
DNS server for domain.com
DNS server of new.com

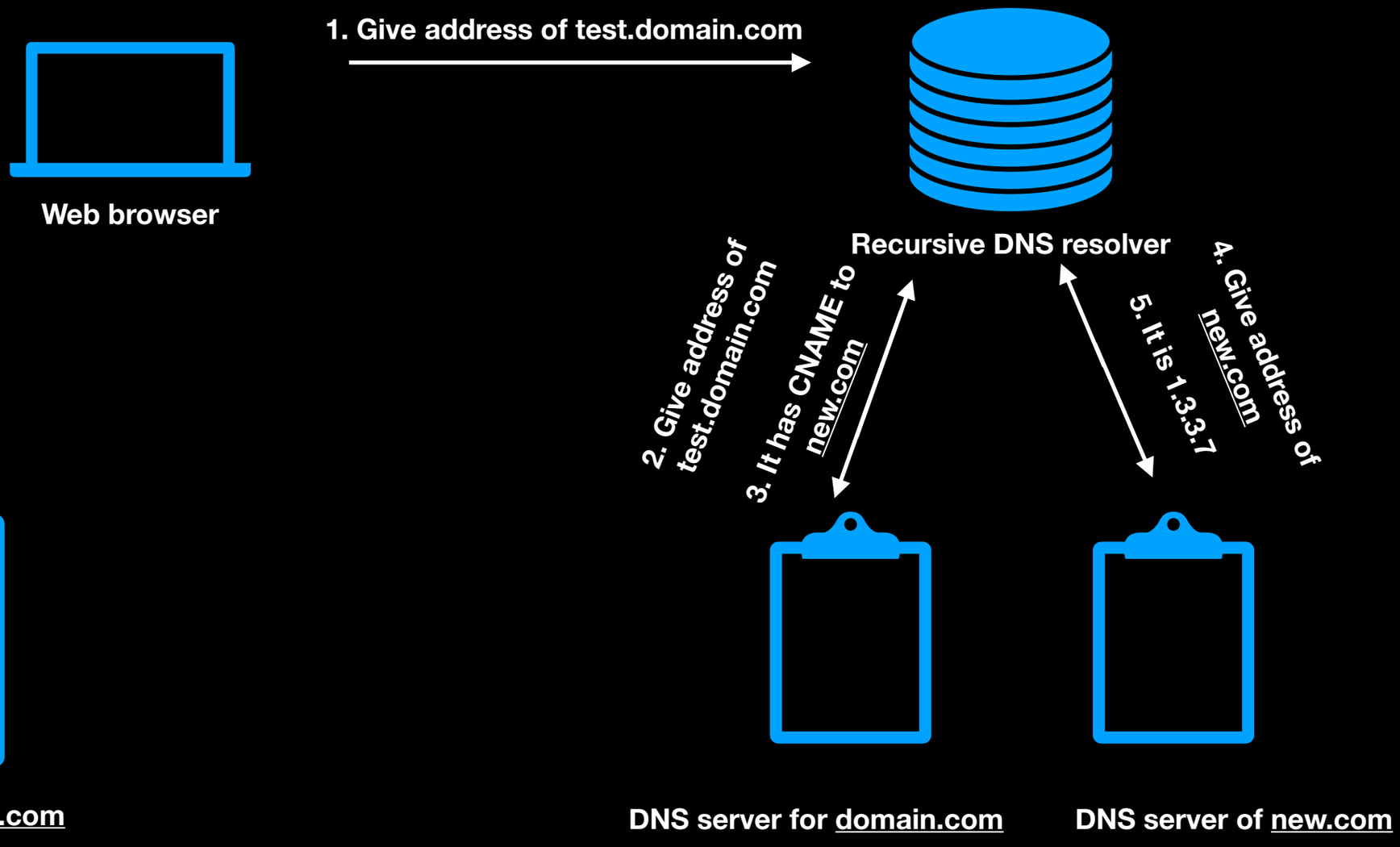
Schematics


1. Give address of test.domain.com
Web browser
Recursive DNS resolver
2. Give address of test.domain.com
3. It has CNAME to new.com
Web server on new.com
IP: 1.3.3.7
DNS server for domain.com
DNS server of new.com

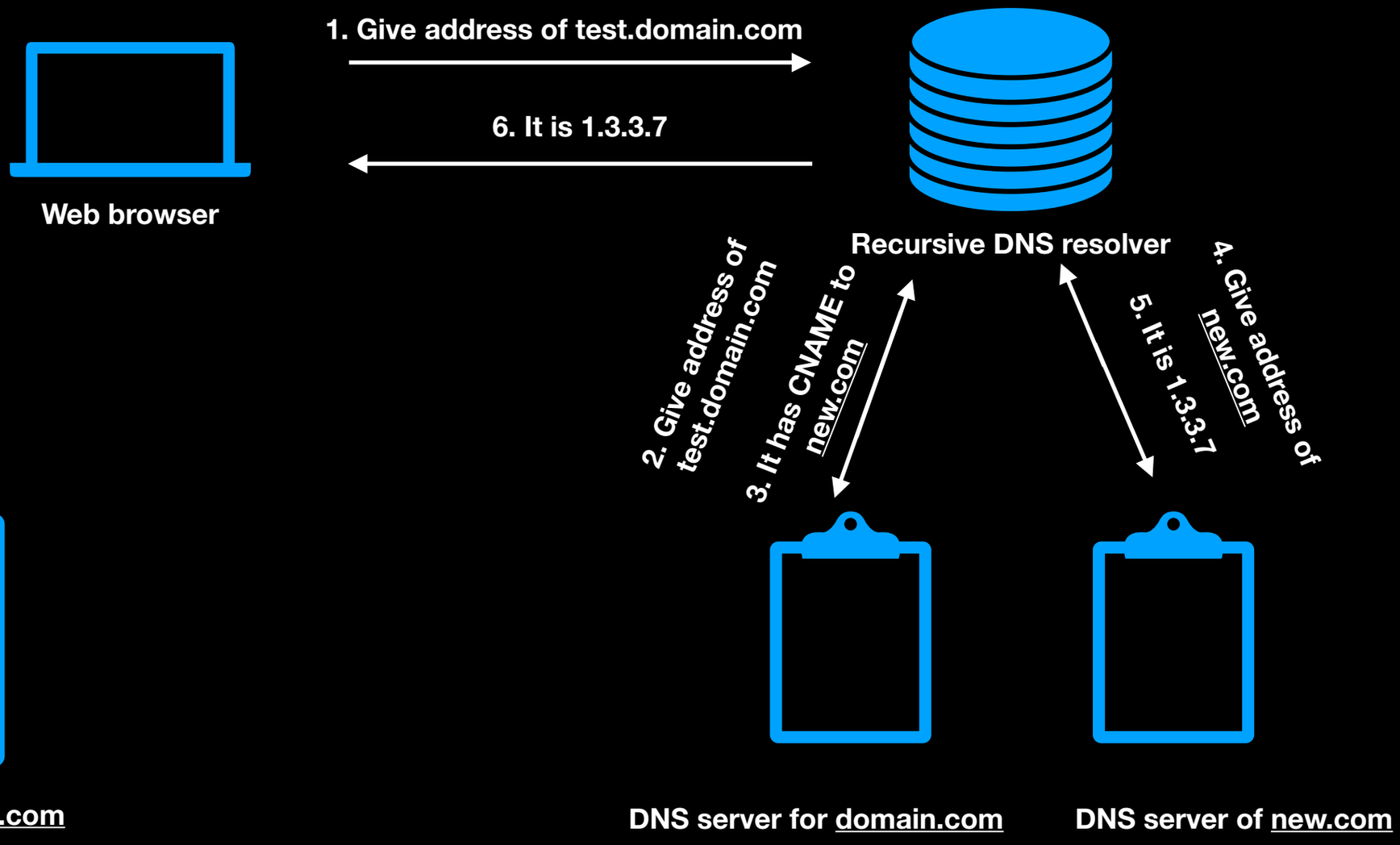
Schematics


1. Give address of test.domain.com
Web browser
Recursive DNS resolver
2. Give address of test.domain.com
3. It has CNAME to new.com
4. Give address of new.com
Web server on new.com
IP: 1.3.3.7
DNS server for domain.com
DNS server of new.com

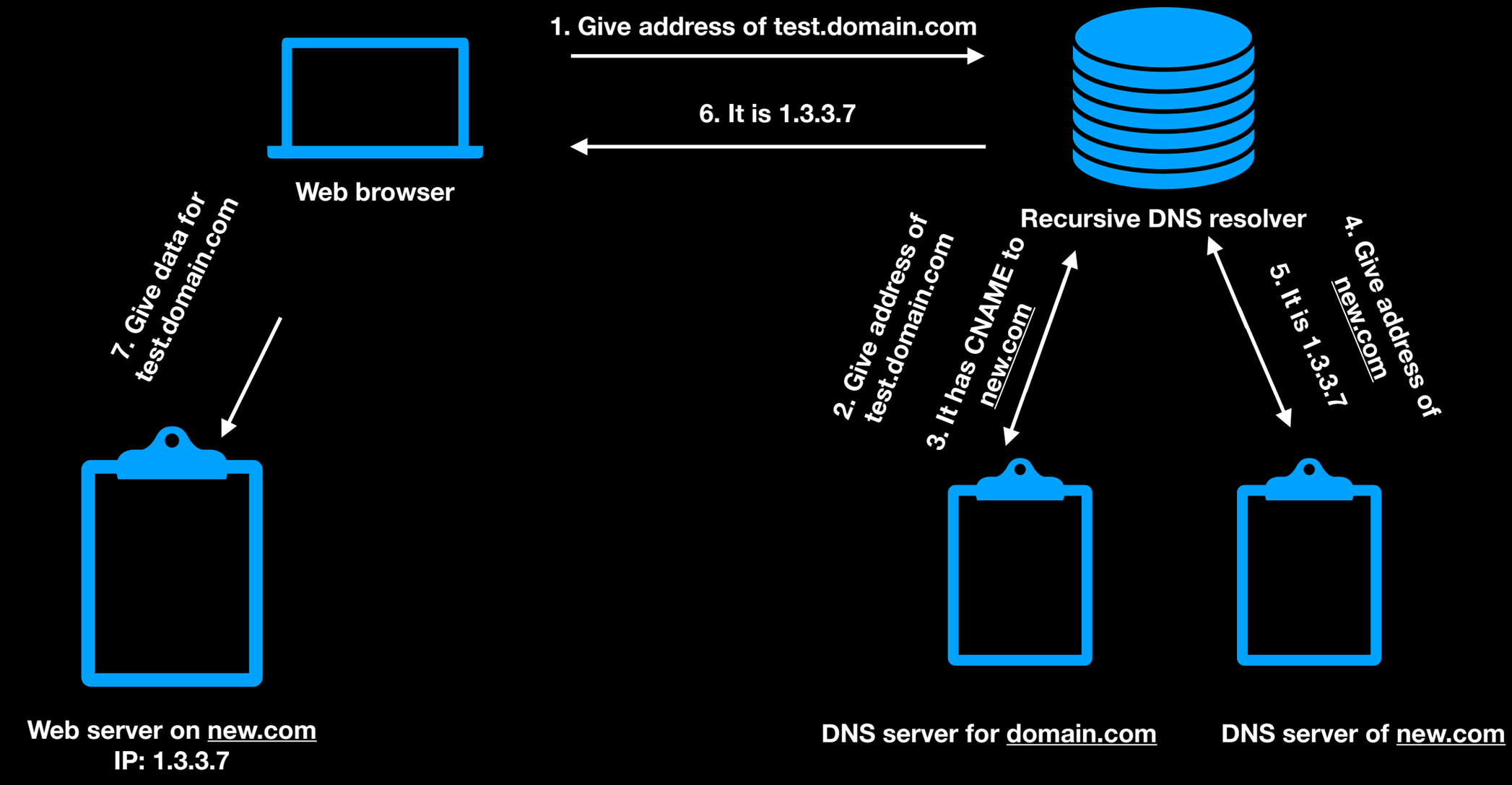
Schematics


1. Give address of test.domain.com
Web browser
Recursive DNS resolver
2. Give address of test.domain.com
3. It has CNAME to new.com
4. Give address of new.com
5. It is 1.3.3.7
Web server on new.com
IP: 1.3.3.7
DNS server for domain.com
DNS server of new.com

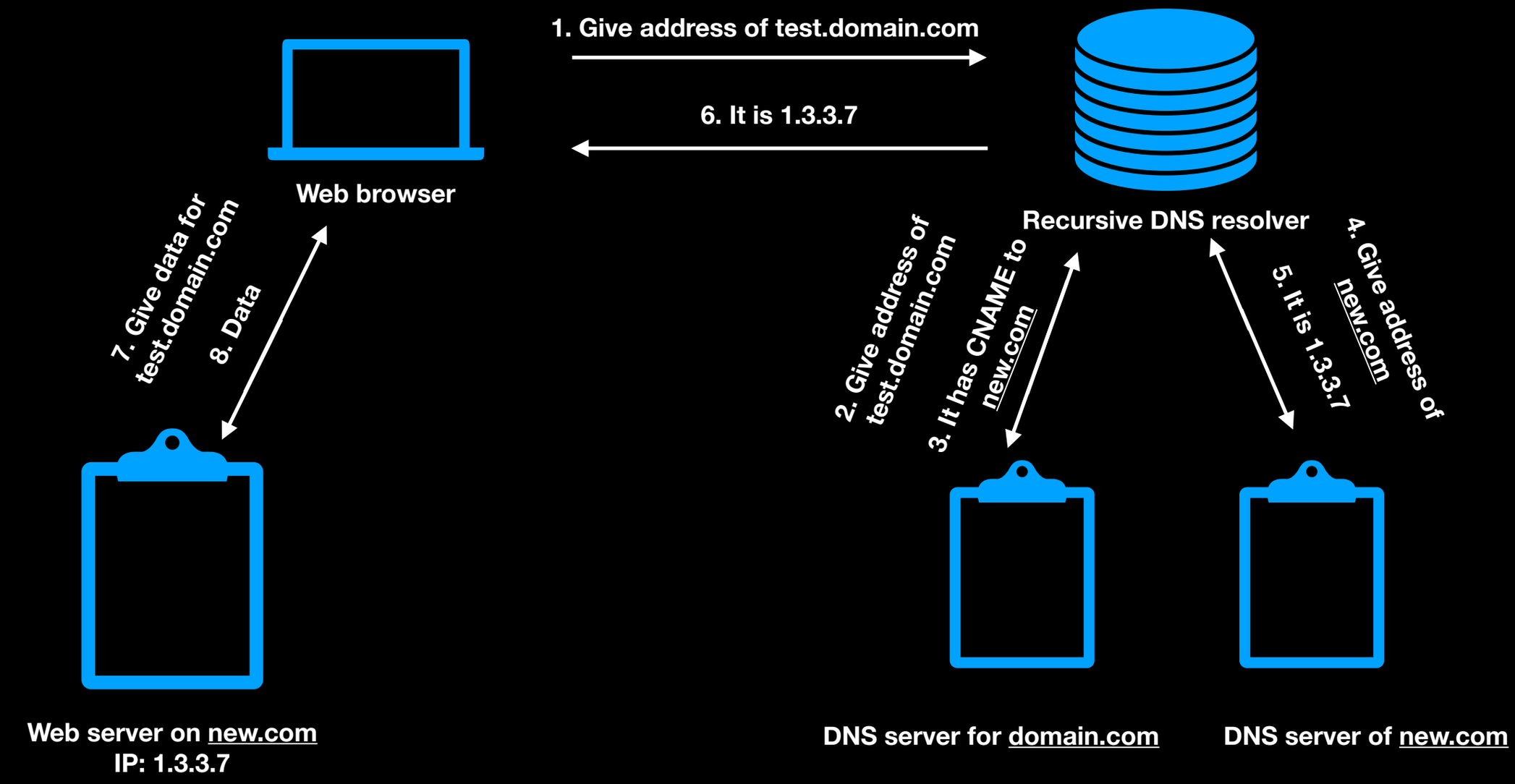
Schematics


1. Give address of test.domain.com
6. It is 1.3.3.7
Web browser
Recursive DNS resolver
2. Give address of test.domain.com
3. It has CNAME to new.com
4. Give address of new.com
5. It is 1.3.3.7
Web server on new.com
IP: 1.3.3.7
DNS server for domain.com
DNS server of new.com

Schematics


1. Give address of test.domain.com
6. It is 1.3.3.7
Web browser
Recursive DNS resolver
7. Give data for test.domain.com
2. Give address of test.domain.com
3. It has CNAME to new.com
4. Give address of new.com
5. It is 1.3.3.7
Web server on new.com
IP: 1.3.3.7
DNS server for domain.com
DNS server of new.com

Schematics


1. Give address of test.domain.com
6. It is 1.3.3.7
Web browser
Recursive DNS resolver
7. Give data for test.domain.com
8. Data
2. Give address of test.domain.com
3. It has CNAME to new.com
4. Give address of new.com
5. It is 1.3.3.7
Web server on new.com
IP: 1.3.3.7
DNS server for domain.com
DNS server of new.com

CNAME only?

No

NS and MX records are affected as well

NS subdomain takeover

Schematics are close to previous but what if

test.domain.com NS ns.new.com

test.domain.com NS ns.valid.com

$$\begin{cases} P(NS = ns\,.new\,.com) = 0.5 \\ P(NS = ns\,.valid\,.com) = 0.5 \end{cases}$$

if ns.valid.com:
cashing valid site for 6-24 hours
else:
cashing evil site with given TTL

MX subdomain takeover

Same way, but allows only to get email → **Personal data disclosure**

Real life example

Amazon CloudFront

Amazon CloudFront is a Content Delivery Network (CDN) in Amazon Web Services (AWS).

New distribution:

Generated name for distribution: SUBDOMAIN.cloudfront.net

User can set alternative name for distribution in ACF settings

Real life example

test.domain.com CNAME dc88008800.cloudfront.net

if test.domain.com is not registered in any ACF distribution as alternative name subdomain takeover is available

Important!!!
Because of ACF virtual host settings usage, right distributive defines from Host header, not DNS record

Right now this technique is not exploitable

Real life example

Subdomain takeover with Shopify, Heroku and something more ...

Valeriy Shevchenko Follow
May 16, 2018 · 5 min read

It's a typical story which happens to me time to time.

Few time on the internet and boom, i found a bunch of critical bugs.
That was not a typical bugs. And that was not a typical company. It was electric skateboard company from TOP 3 in the world. That company was not happy to disclose their official name. So let's name it—ESKATE.

I will not explain to you how to proxy you mobile phone. But i'll recommend you for doing this time to time with apps which you used for daily business. That can help you to be safer and not trust for some companies which don't care about security of their users. You can be surprised how many are there.

First thing which i found, was public tracking logs of all users which used