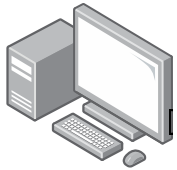
On the Importance of Encrypted-SNI (ESNI) to Censorship Circumvention

Zimo Chai, Amirhossein Ghafari, Amir Houmansadr

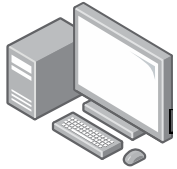
University of Massachusetts Amherst

What is SNI?

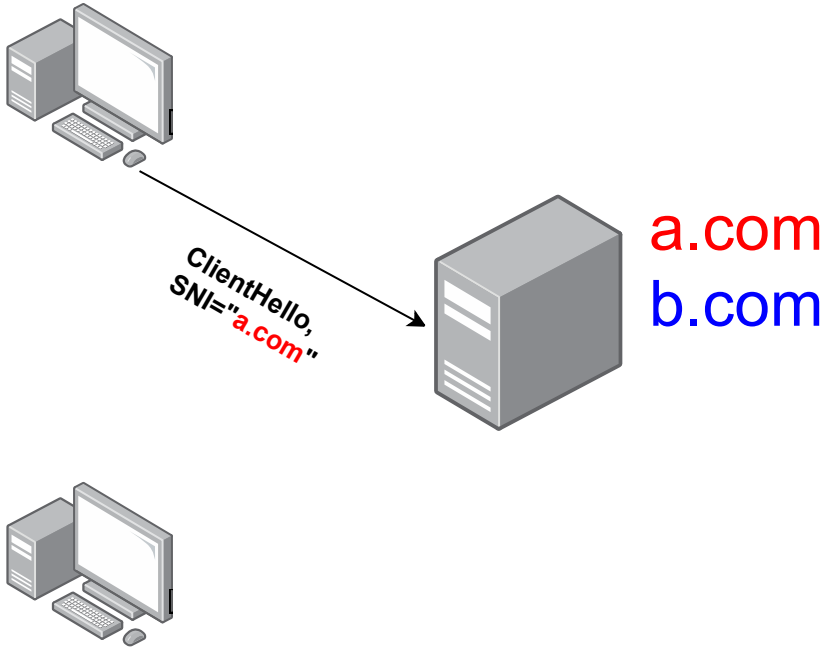
Server Name Indication (SNI) allows web-hosts to render the correct certificate



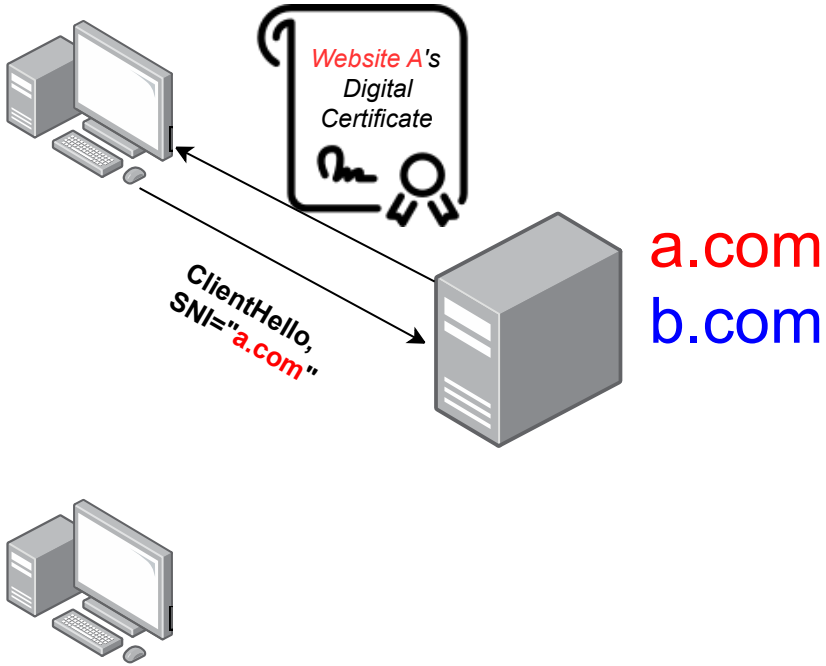
a.com
b.com



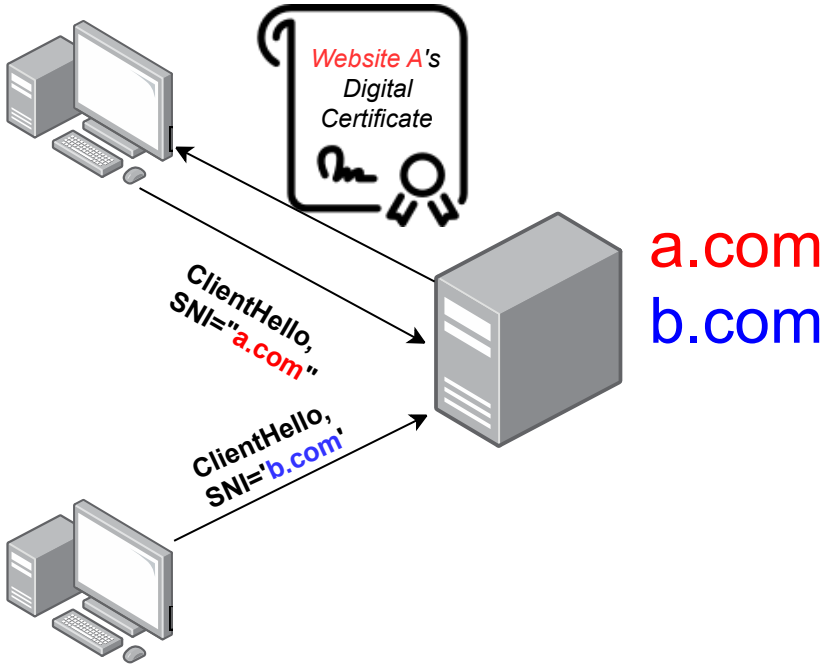
Server Name Indication (SNI) allows web-hosts to render the correct certificate



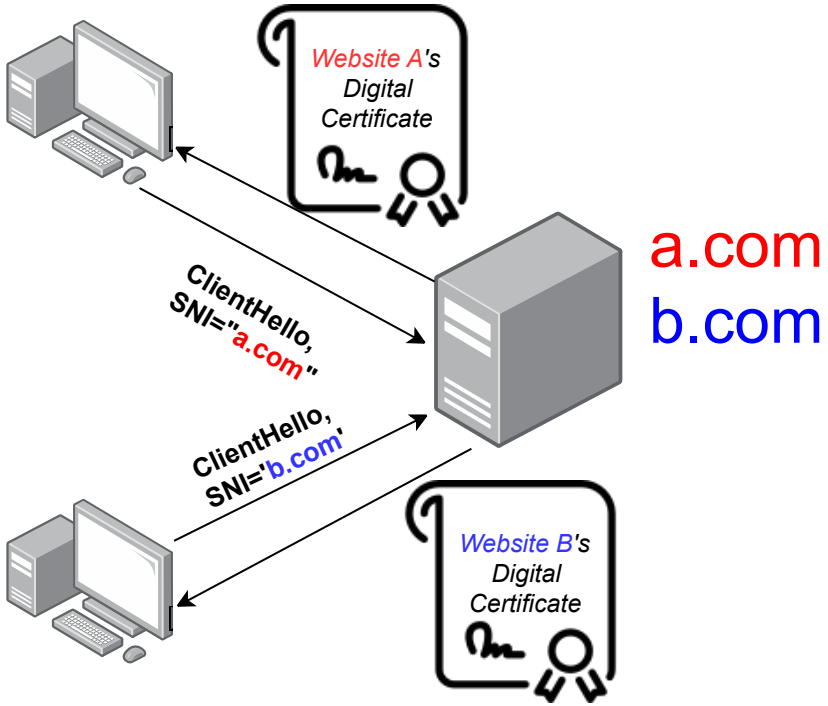
Server Name Indication (SNI) allows web-hosts to render the correct certificate



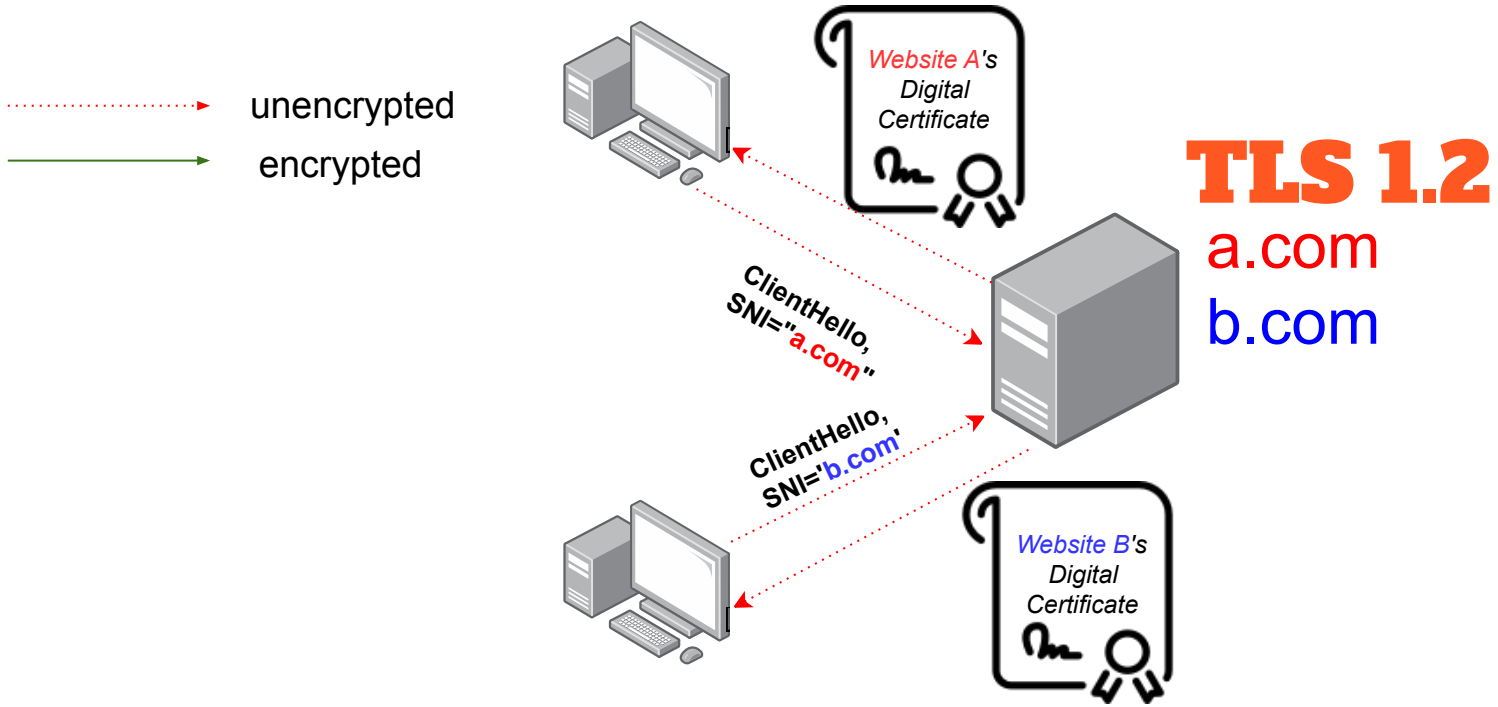
Server Name Indication (SNI) allows web-hosts to render the correct certificate



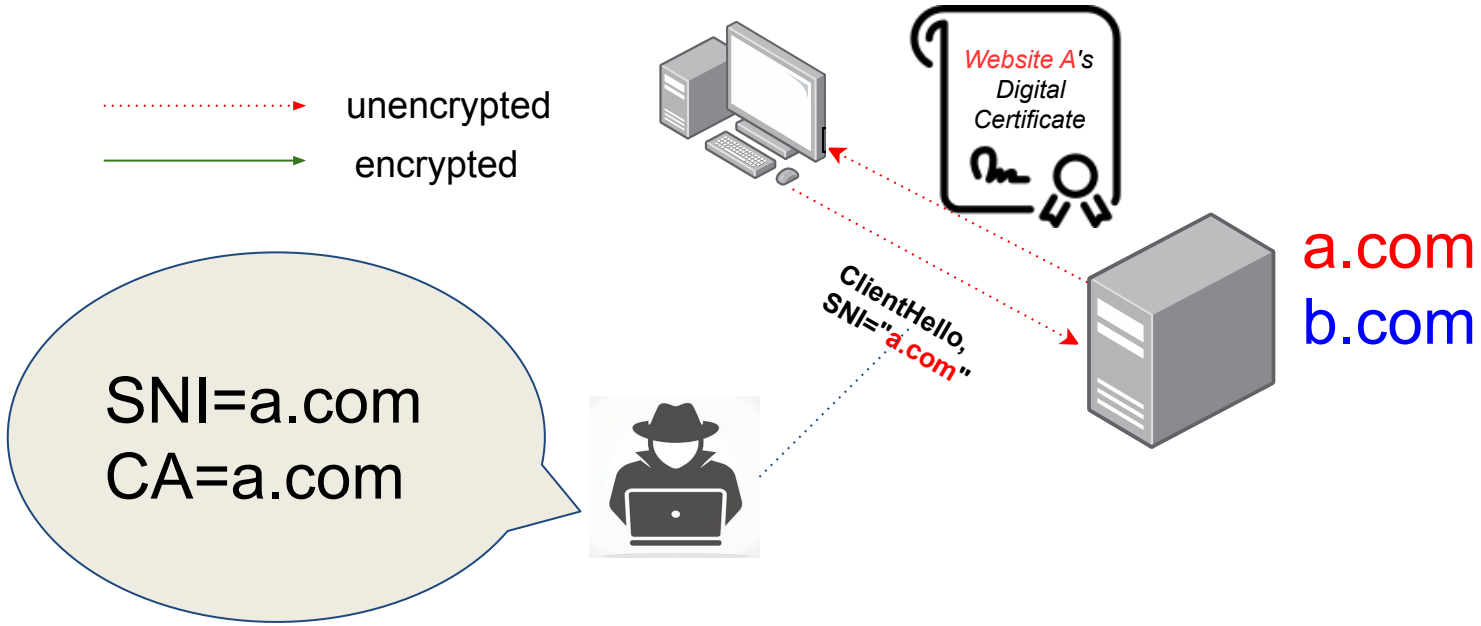
Server Name Indication (SNI) allows web-hosts to render the correct certificate



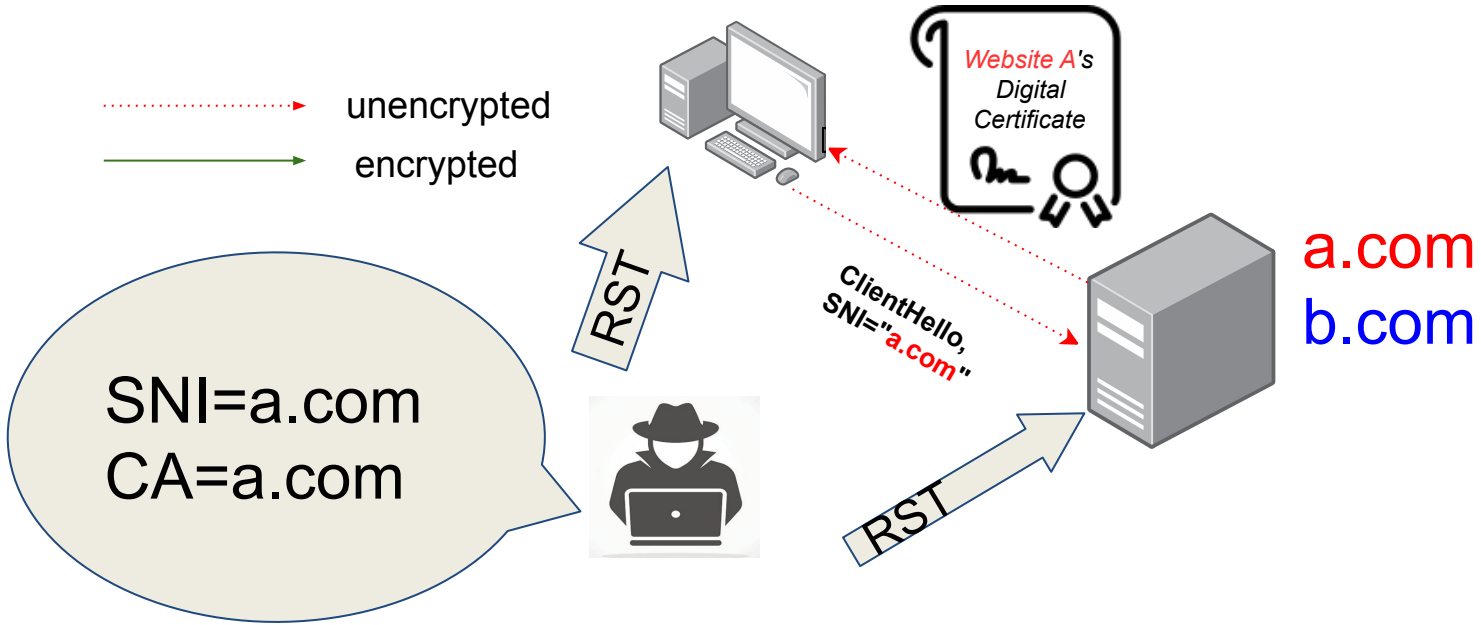
TLS 1.2: SNI and CA are NOT encrypted...



TLS 1.2: SNI and CA are NOT encrypted…



TLS 1.2: SNI and CA are NOT encrypted…



Timeline: TLS 1.3 is finalized

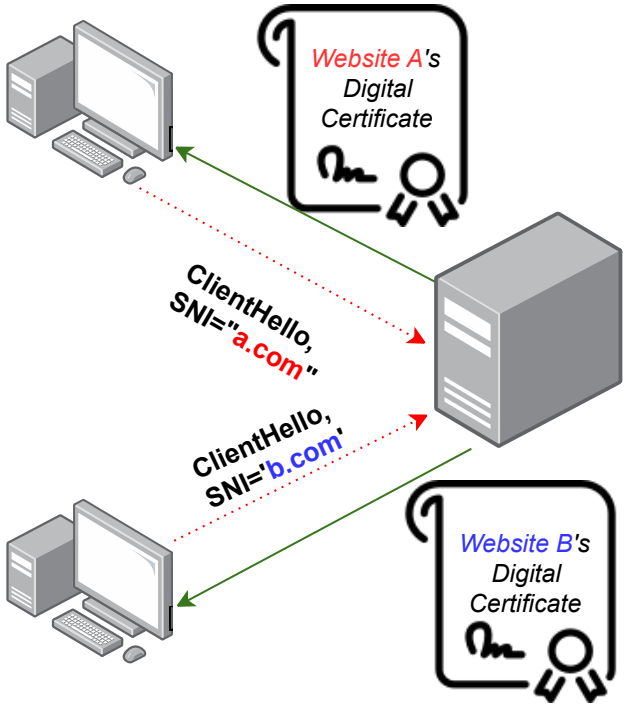
TLS 1.3 finalized

3/21/2018

TLS 1.3: SNI is still NOT encrypted...

unencrypted

encrypted



TLS 1.3

Censors exploit SNI for censorship

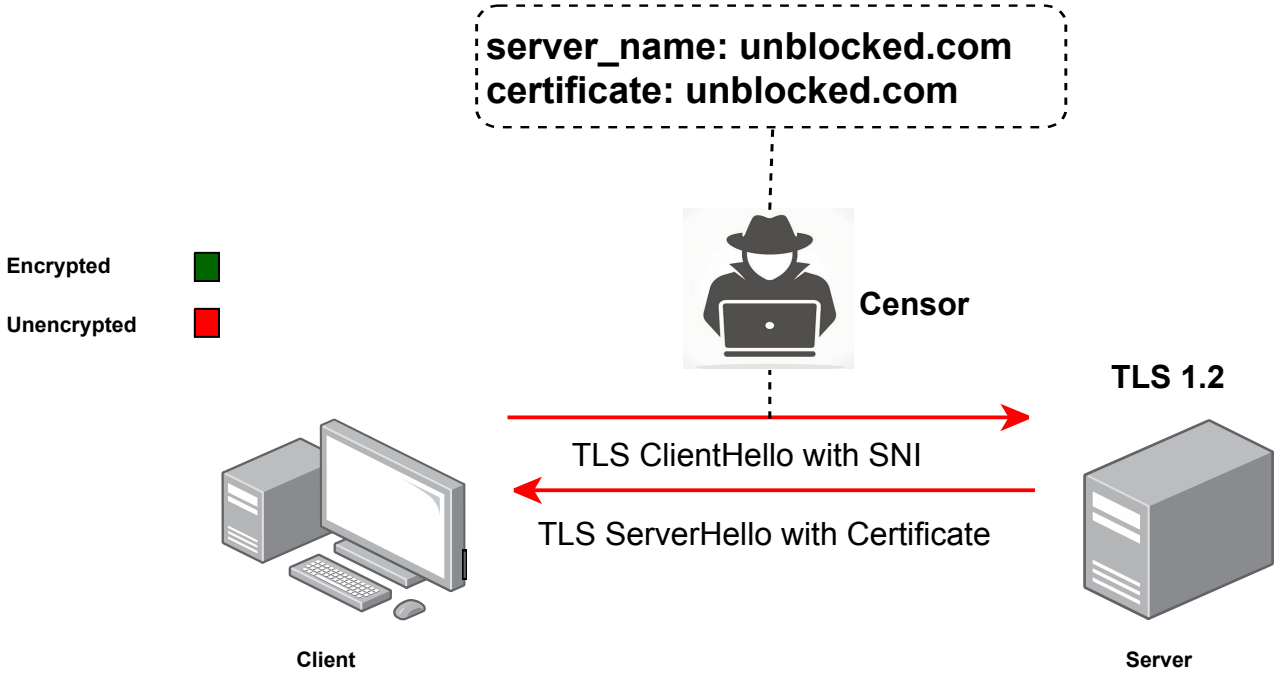
BLEEPINGCOMPUTER

South Korea is Censoring the Internet by Snooping on SNI Traffic

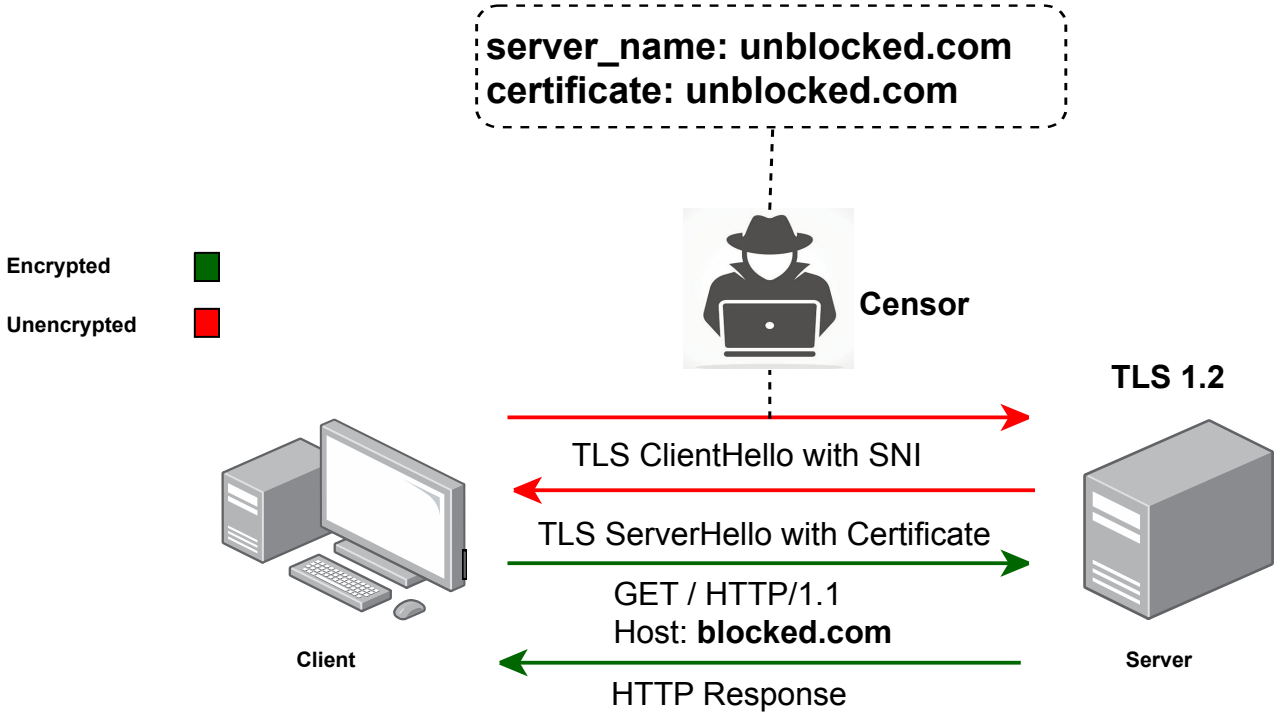
By Sergiu Gatlan

February 13, 2019 06:19 PM 1

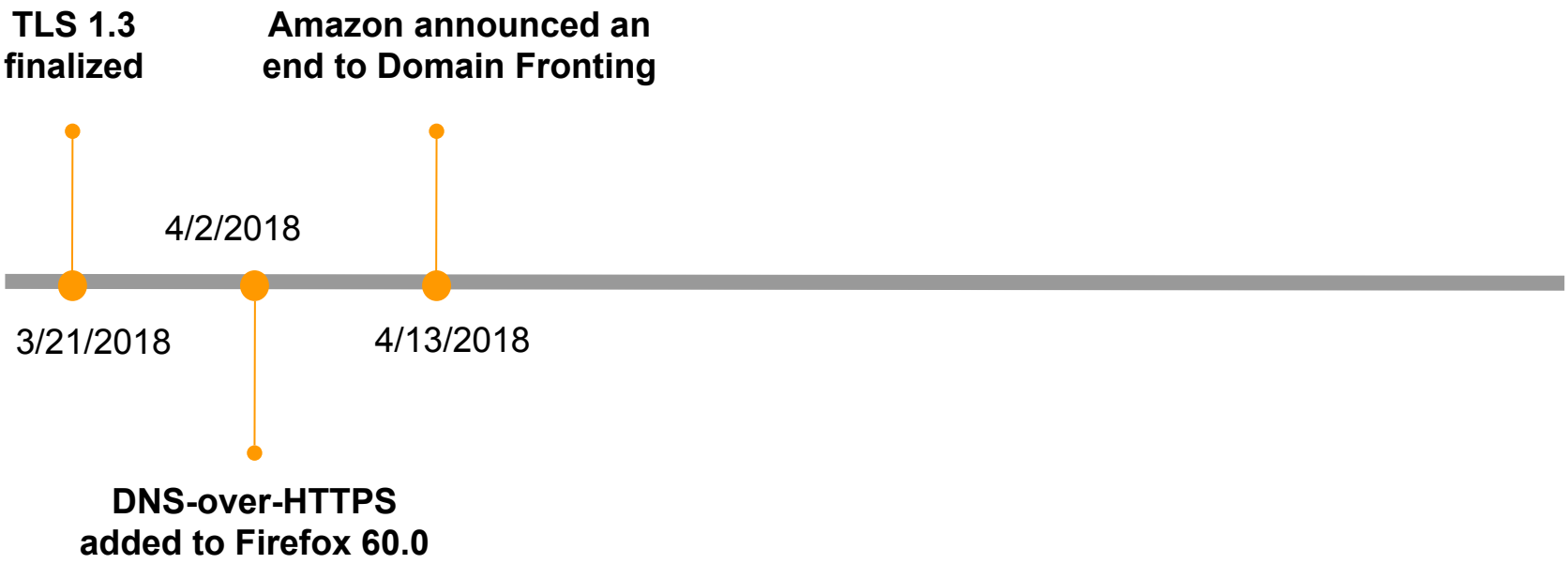
Circumvention: Domain Fronting



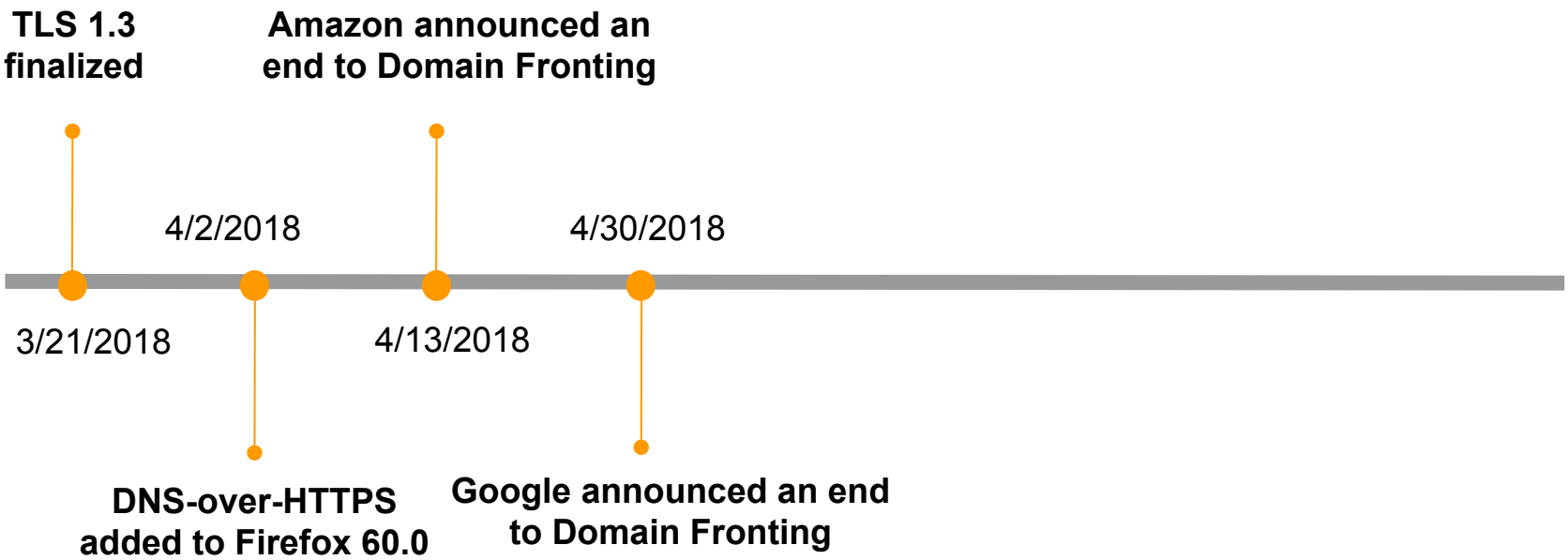
Circumvention: Domain Fronting



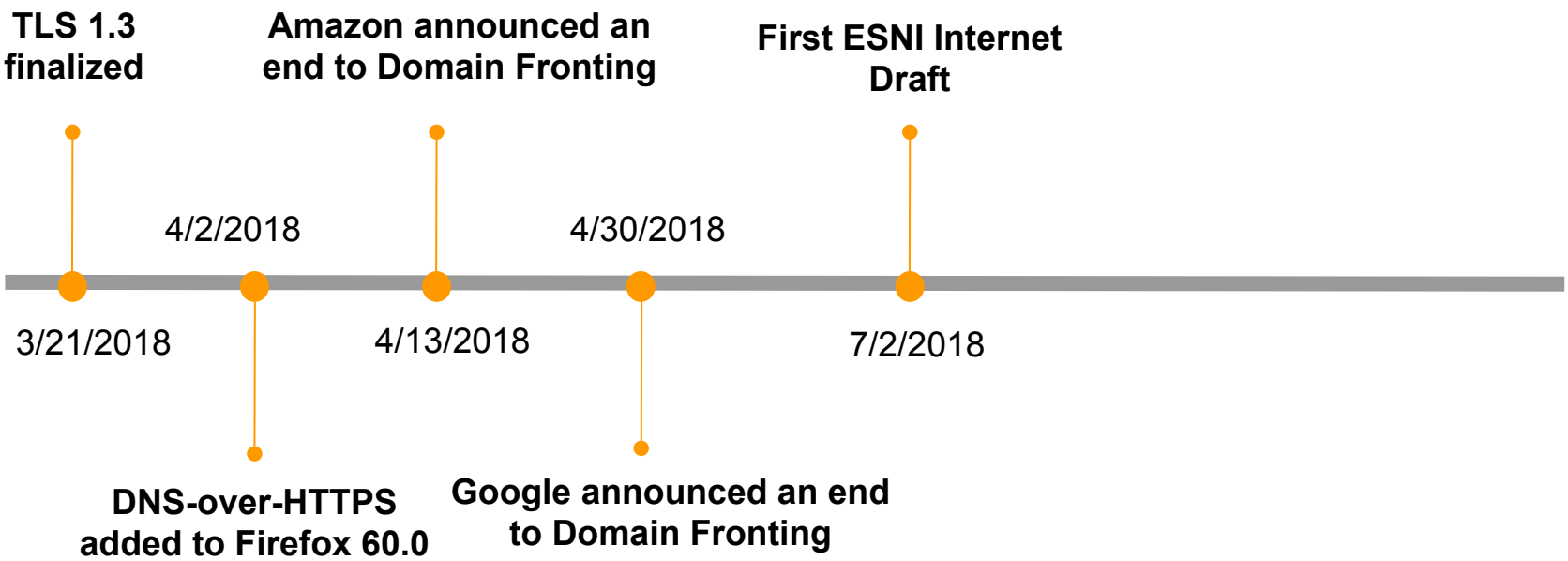
Timeline: CDNs Cease Domain Fronting



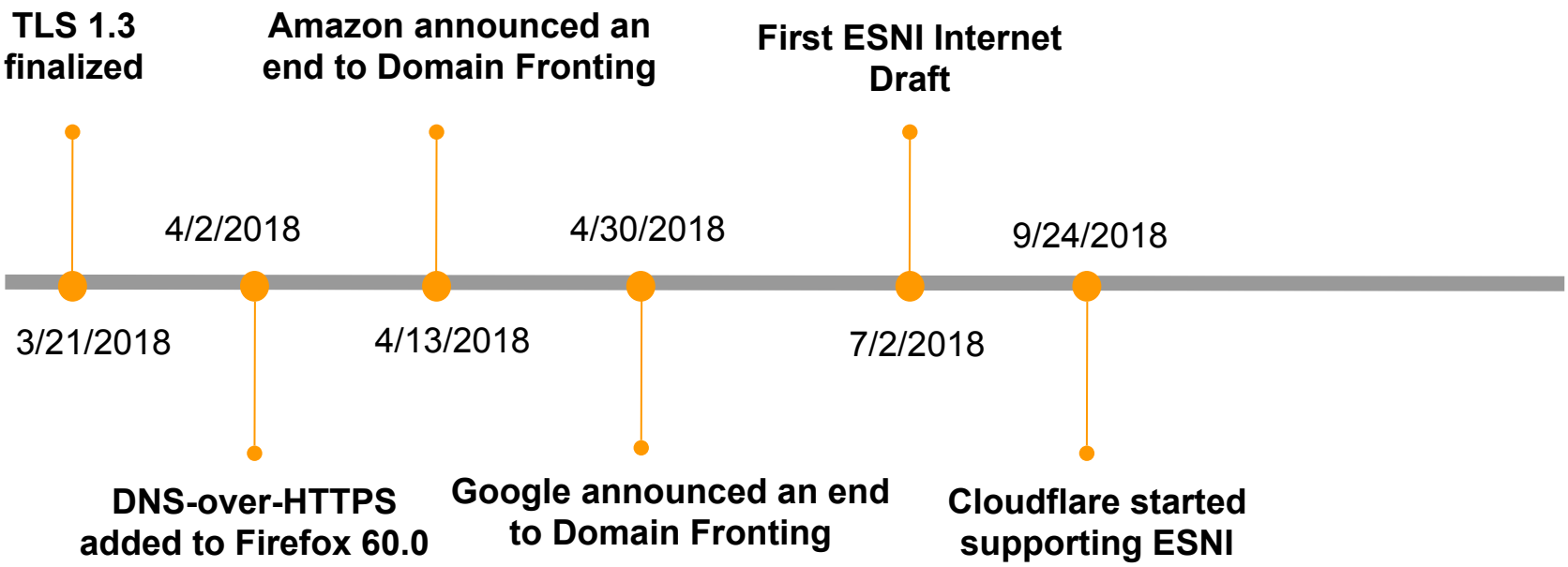
Timeline: CDNs cease domain fronting



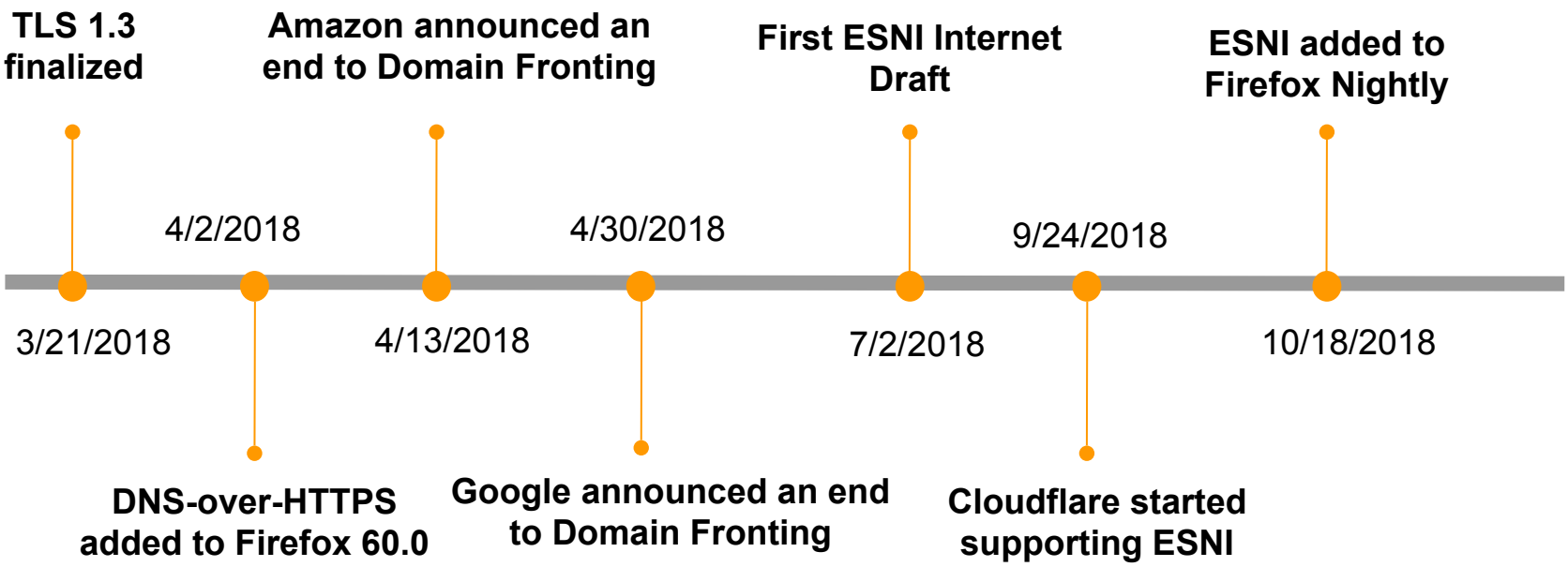
Timeline: ESNI is proposed for TLS 1.3



Timeline: Cloudflare supports ESNI

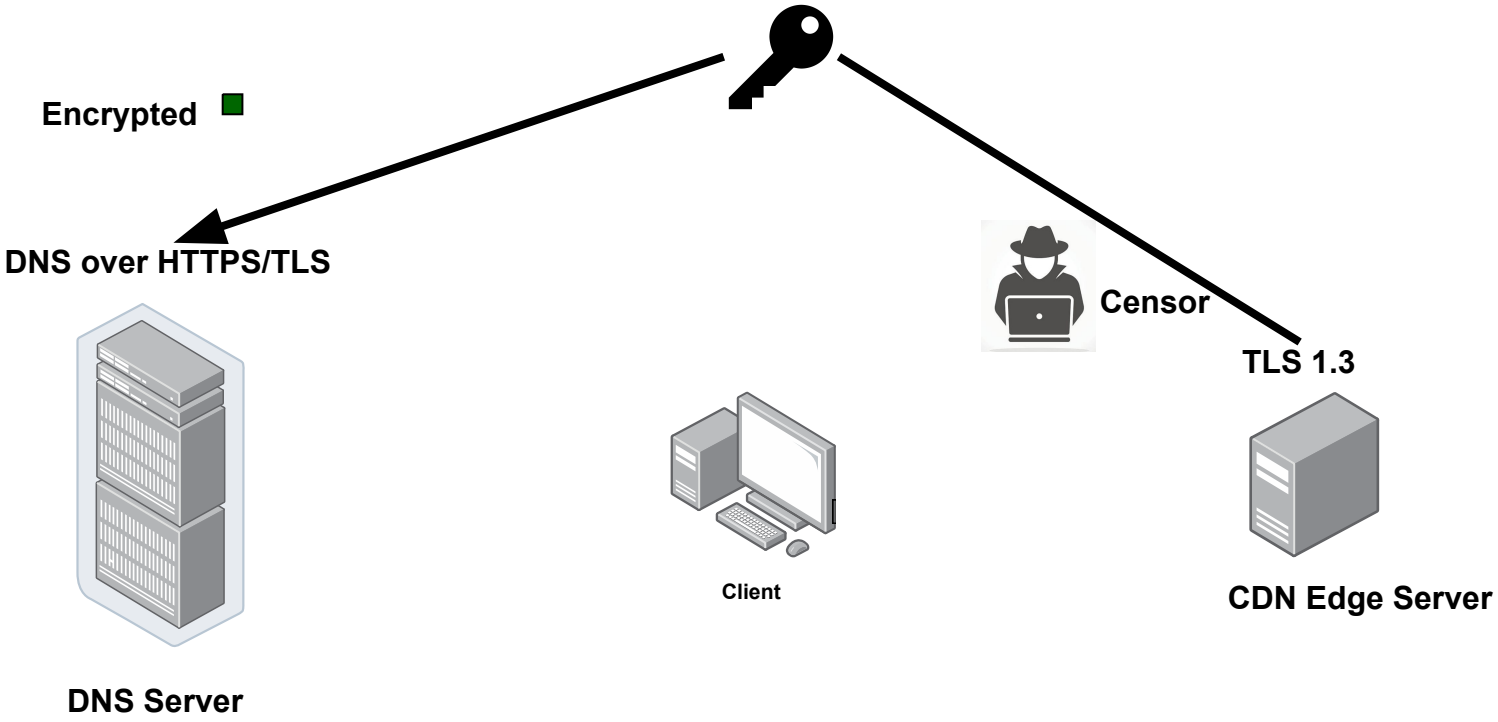


Timeline: Firefox supports ESNI

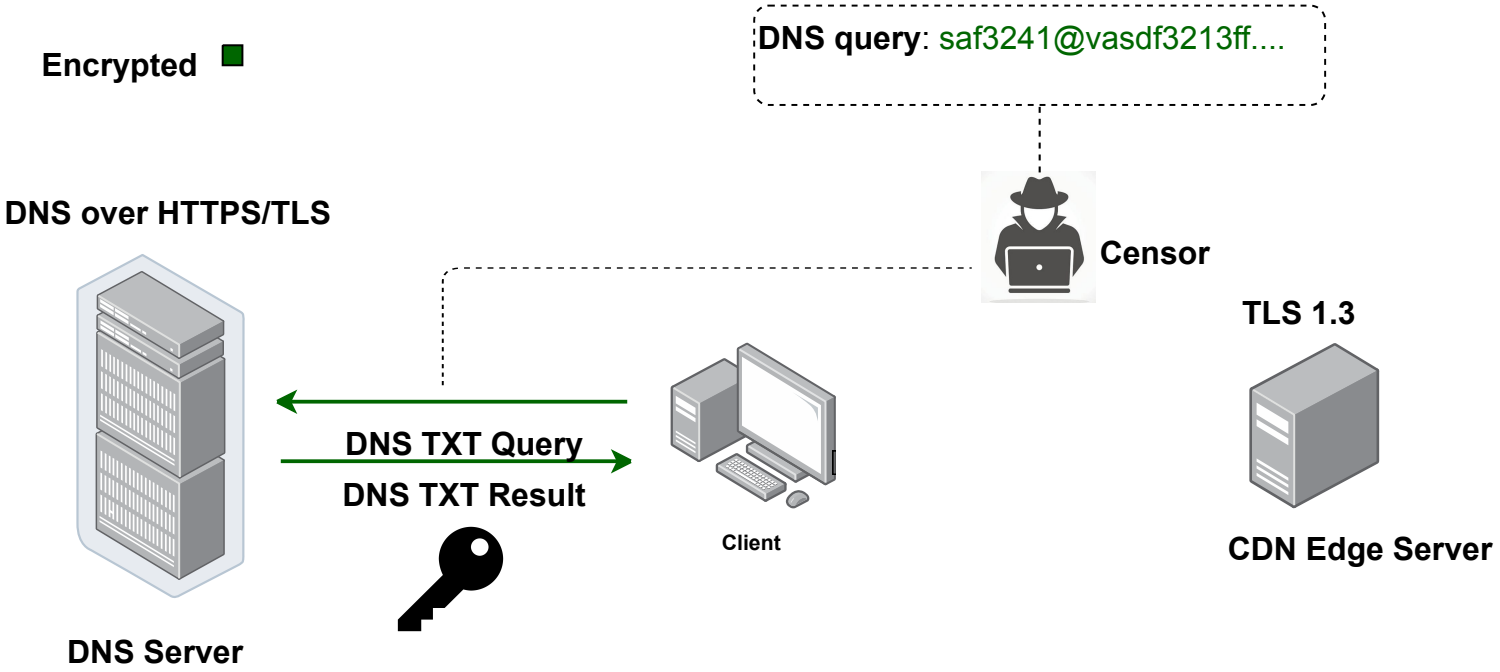


How ESNI works?

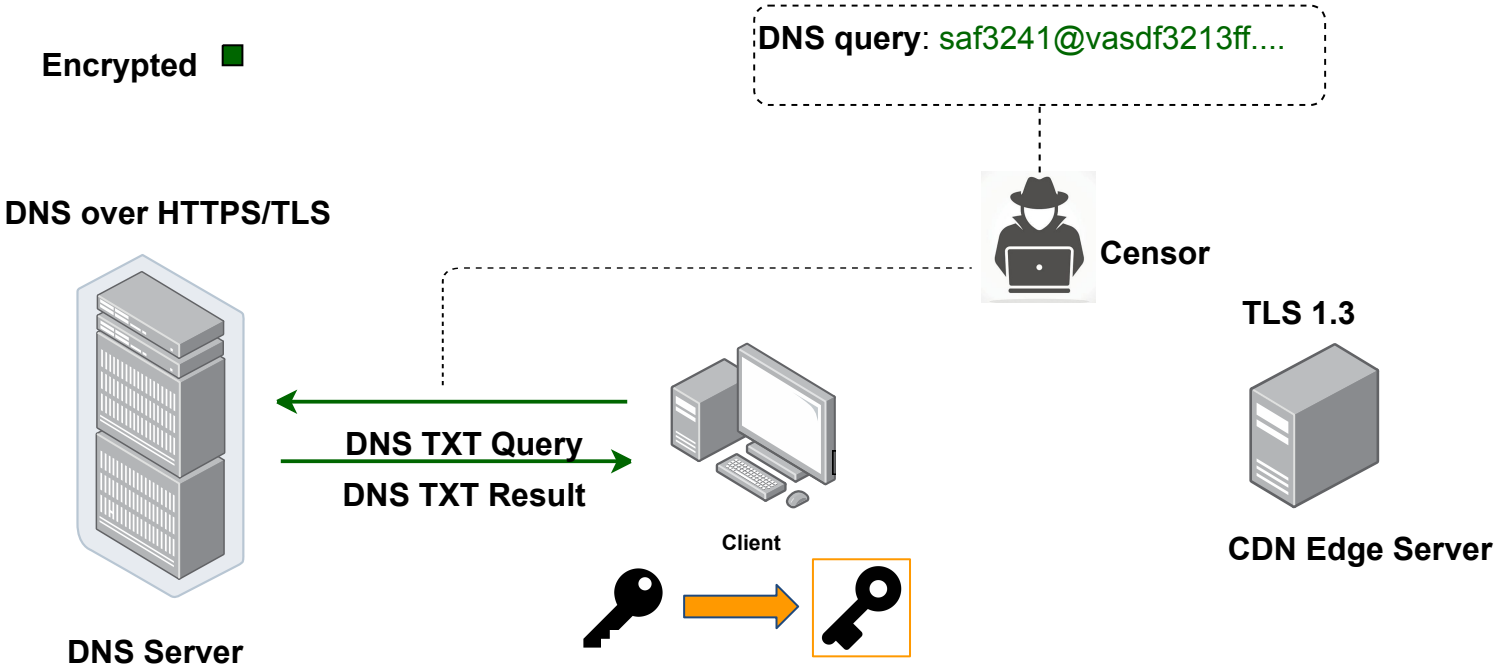
How ESNI works?



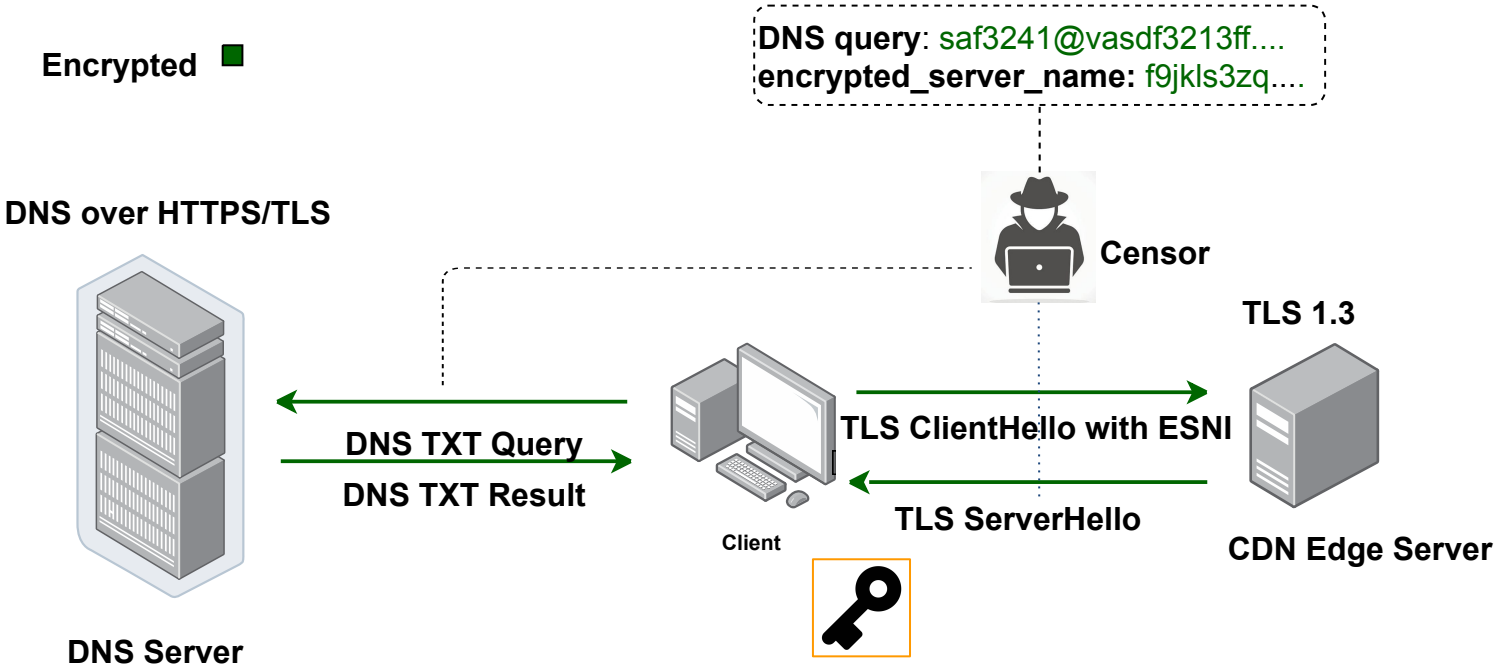
How ESNI works?



How ESNI works?



How ESNI works?



Research Questions

Research Questions

- How many websites are **supporting ESNI**?
- How many currently censored websites in China can be **unblocked** with the help of ESNI?
- Is there any censor already **censoring ESNI** traffic?

How many websites are supporting ESNI?

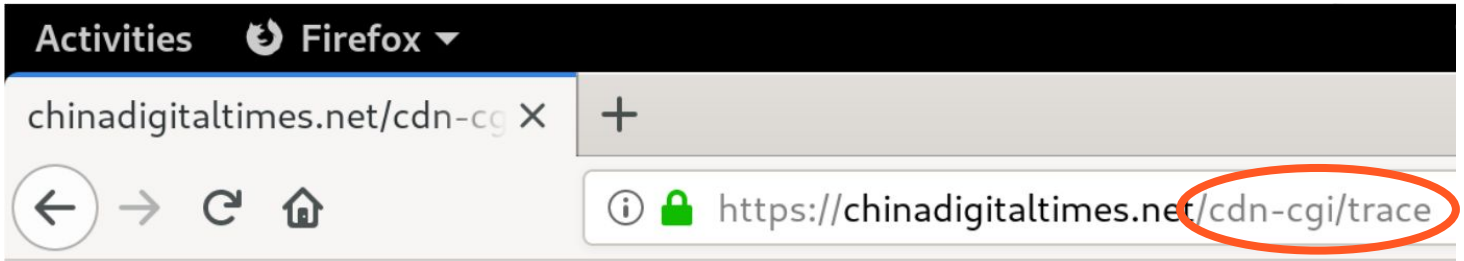
How many sites are supporting ESNI?

As of August 2019, Cloudflare is the only CDN provider supporting ESNI.

Cloudflare provides an informative debugging page for every site using its CDN service.

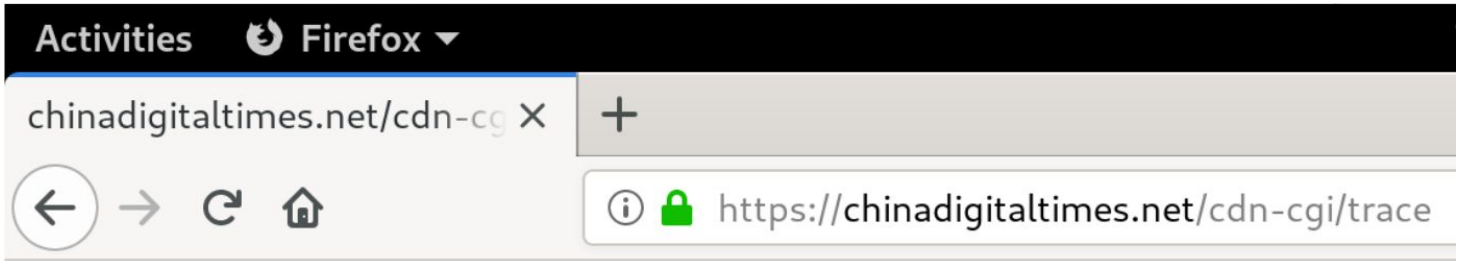
How to know if a site supports ESNI?

Cloudflare debugging page




```
fl=102f16
h=chinadigitaltimes.net
ip=
ts=1566939154.141
visit_scheme=https
uag=Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
colo=PHL
http=http/2
loc=US
tls=TLSv1.3
sni=encrypted
warp=off
```

Cloudflare debugging page




```
fl=102f16
h=chinadigitaltimes.net
ip=
ts=1566939154.141
visit_scheme=https
uag=Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
colo=PHL
http=http/2
loc=US
tls=TLSv1.3
sni=encrypted
warp=off
```

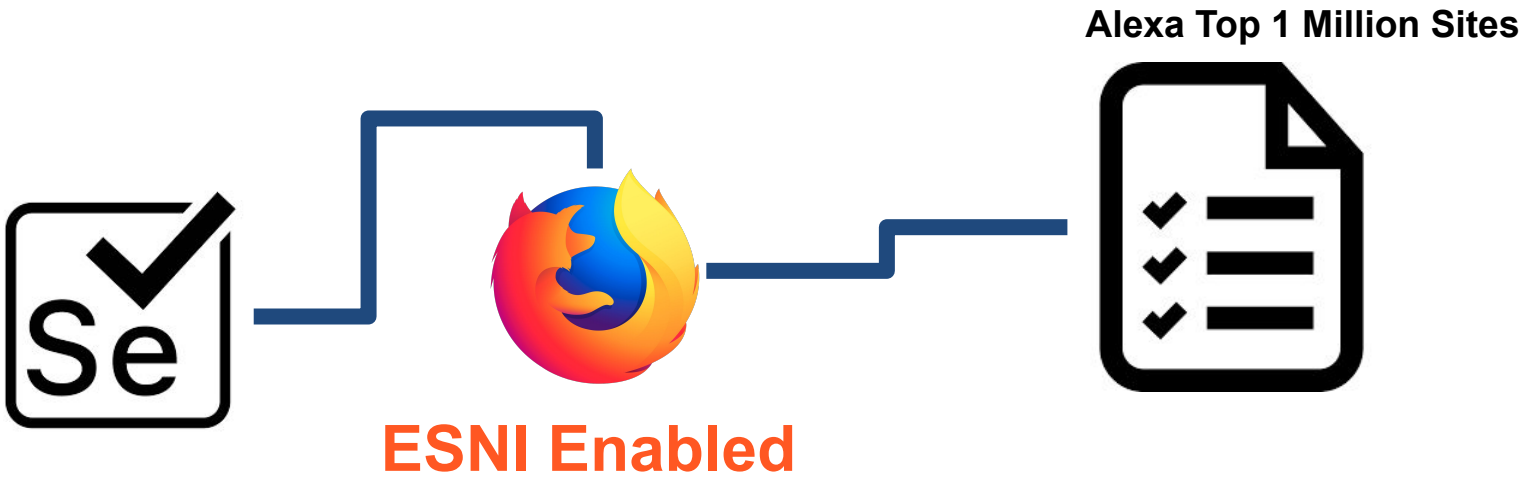
How many sites are supporting ESNI?

Location: On a VPS located in US

ESNI Enabled

How many sites are supporting ESNI?

Location: On a VPS located in US



Websites Supporting ESNI

More than

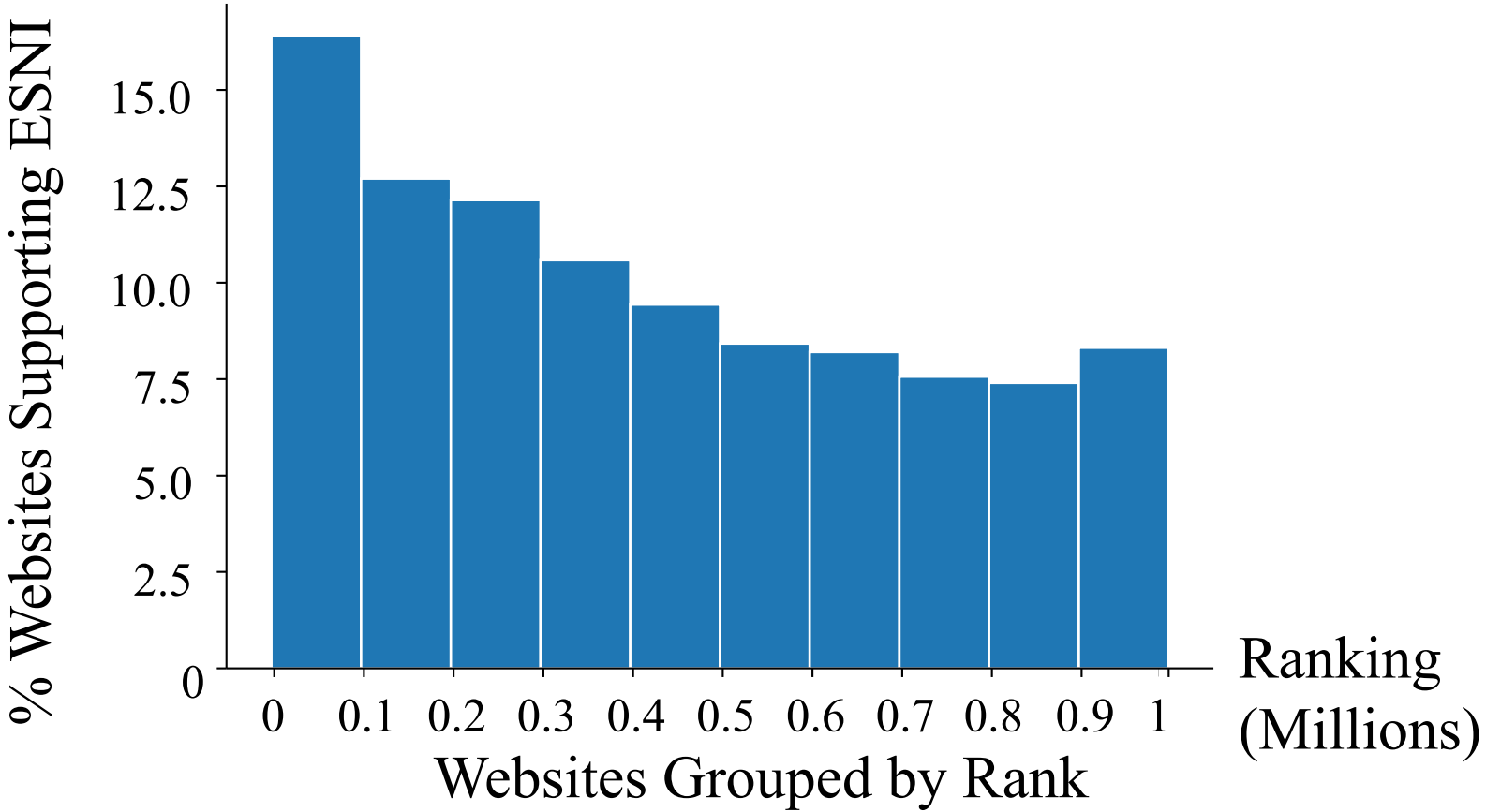
10%

of Alexa Top 1 Million sites are supporting ESNI!

Result: SNI Status and TLS Version

SNI Status	TLS Version	Number	Portion
encrypted	TLS1.3	101,190	92.56%
plaintext	TLS1.3	1,288	1.17%
	TLS1.2	6,825	6.24%
off	TLS1.2	5	0.005%
	-	14	0.012 %
Total		109,322	100%

ESNI adoption with Sites Popularity



Research Questions

- How many websites are **supporting ESNI**?

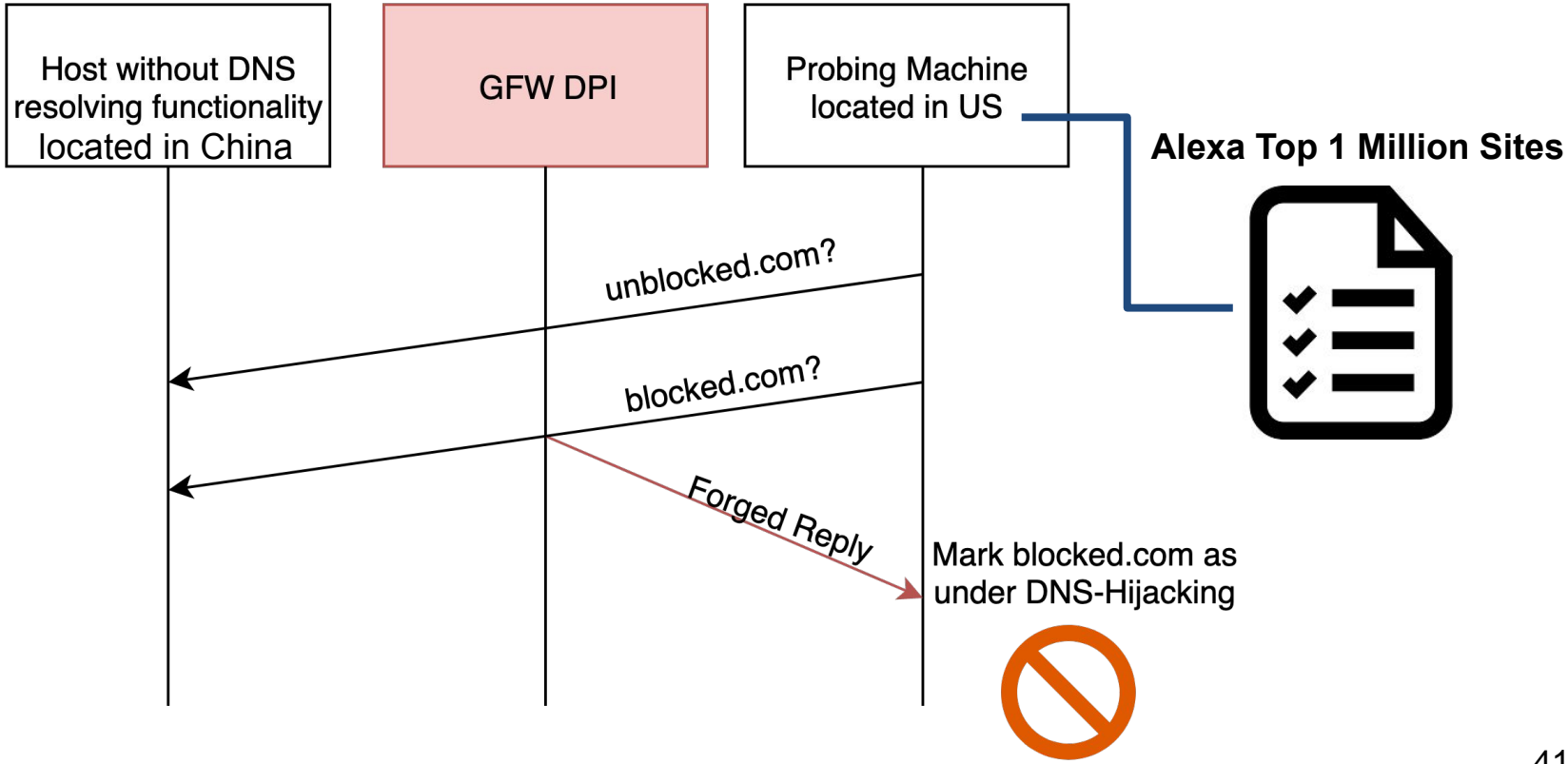
- How many currently censored websites in China can be **unblocked** with the help of ESNI?

How websites are censored in China?

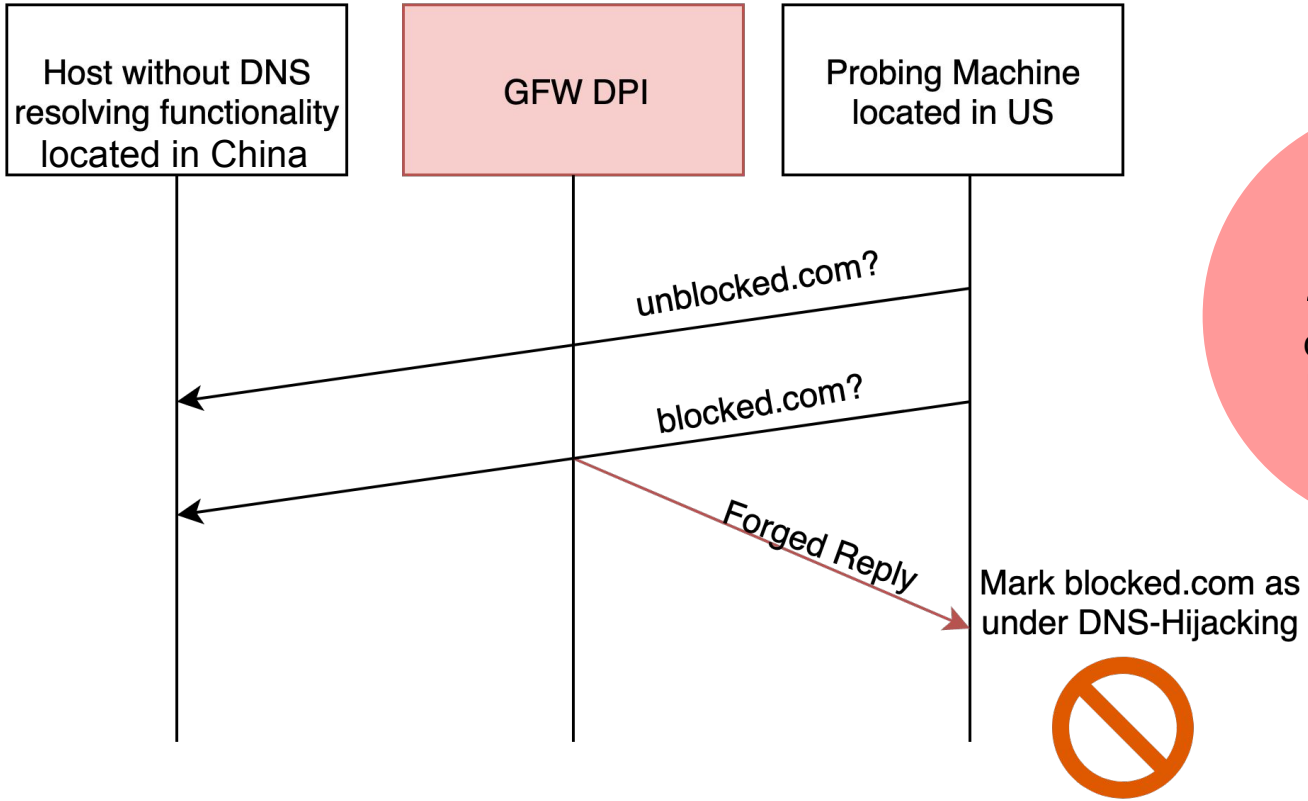
Major Censorship techniques in China

- DNS Hijacking
- IP Blocking
- SNI Filtering

Detect DNS Hijacking - Result

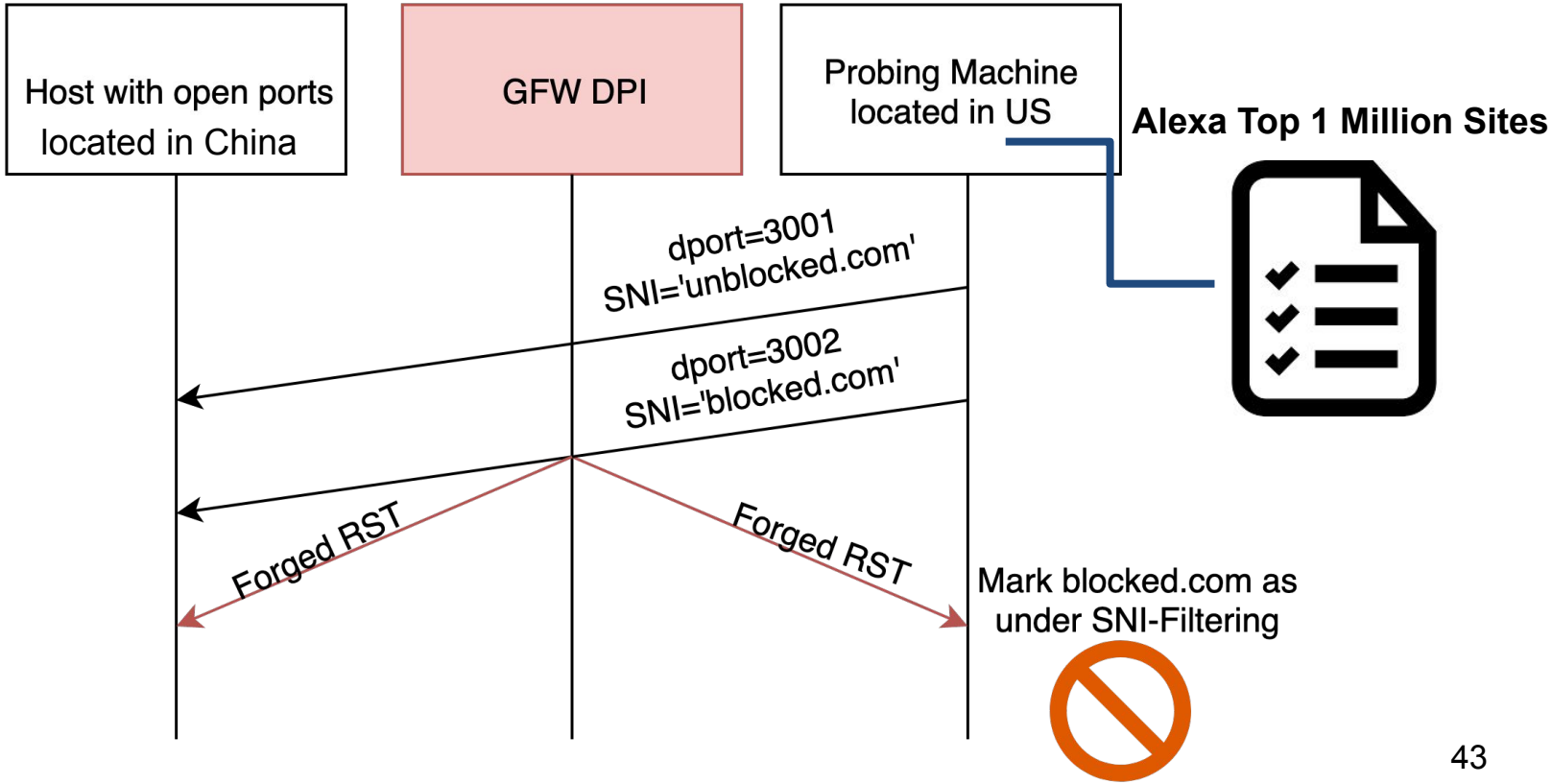


Detect DNS Hijacking - Result

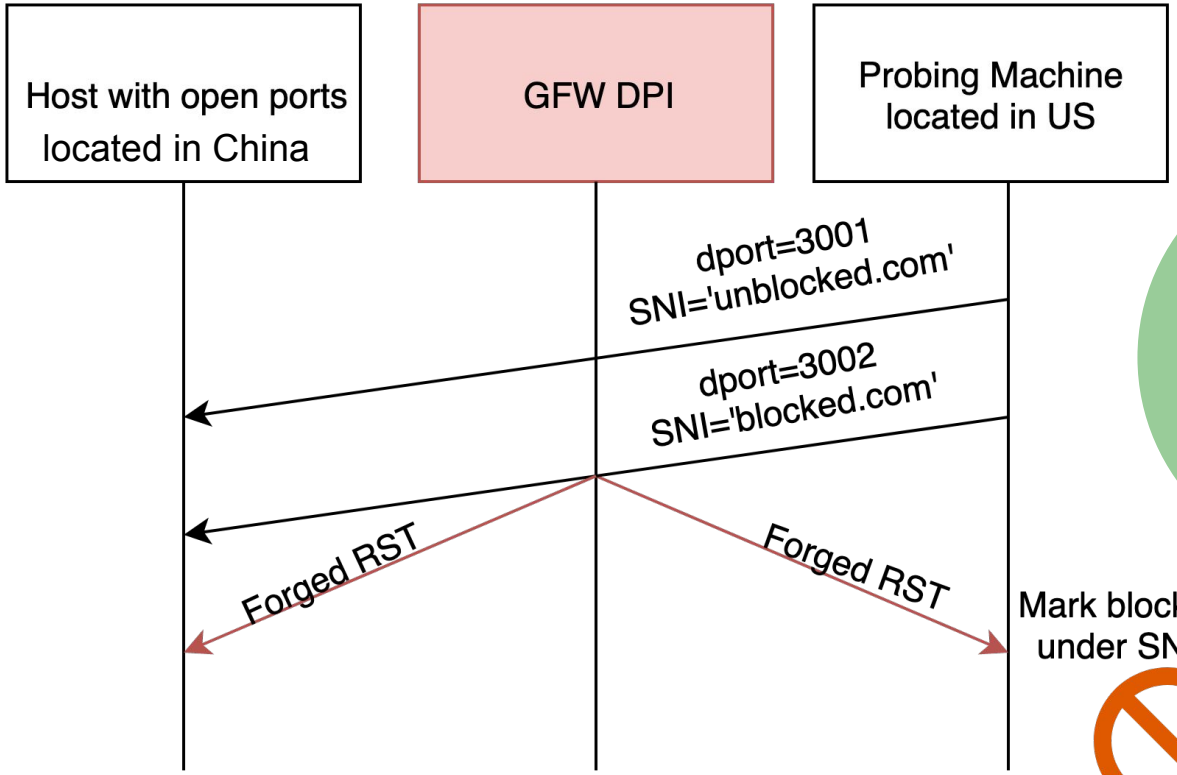


24,128
domains under DNS-Hijacking

Detect SNI Filtering - Setup



Detect SNI Filtering - Result



21,446
domains under
SNI-Filtering

Detect IP Blocking - IP List

Alexa Top 1 Million Sites

Resolve from
Hong Kong

DNS

Select the **first IP** in an answer

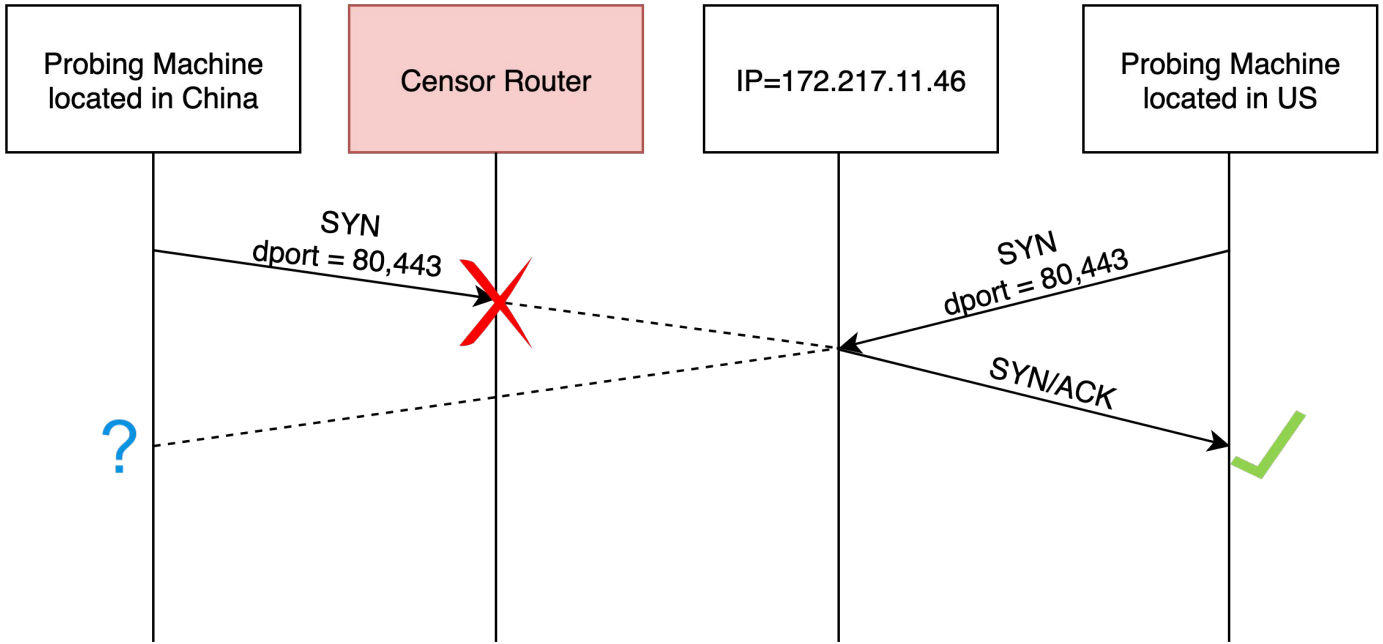
Detect IP Blocking - IP List

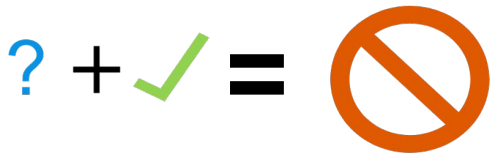
Alexa Top 1 Million Sites

Resolve from
Hong Kong
DNS
Select the **first IP** in an answer

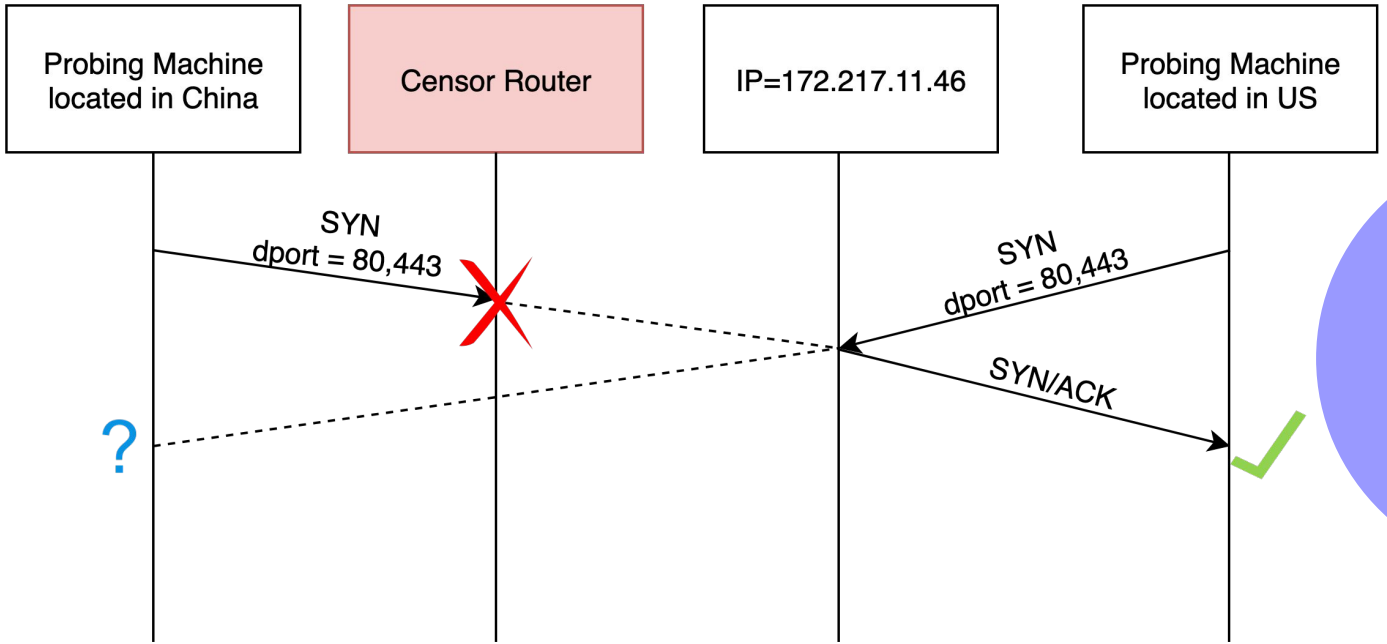
539,456 unique IPs

Detect IP Blocking - Setup

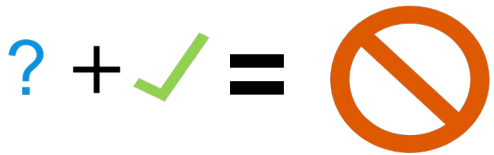




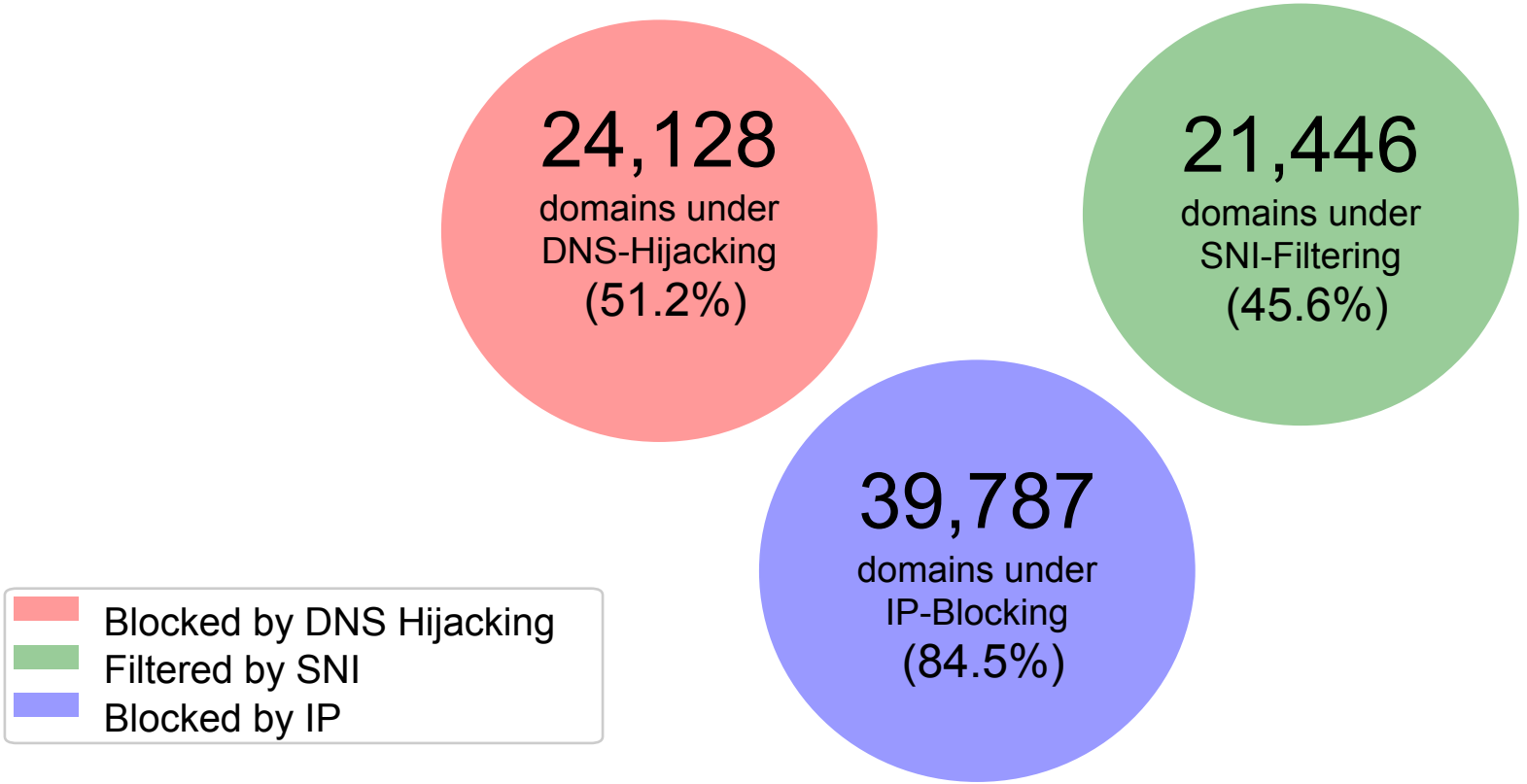
Detect IP Blocking - Result



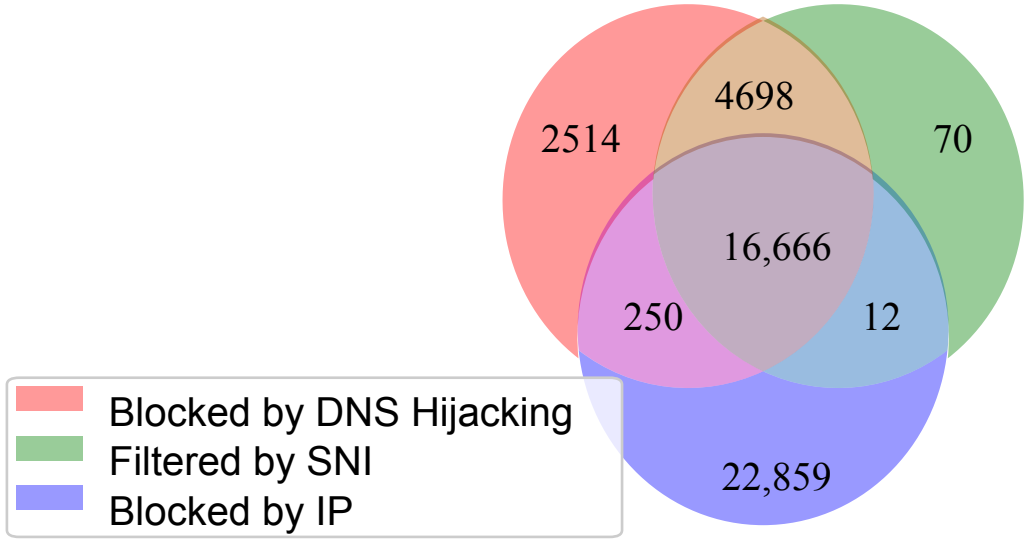
39,787
domains under
IP-Blocking



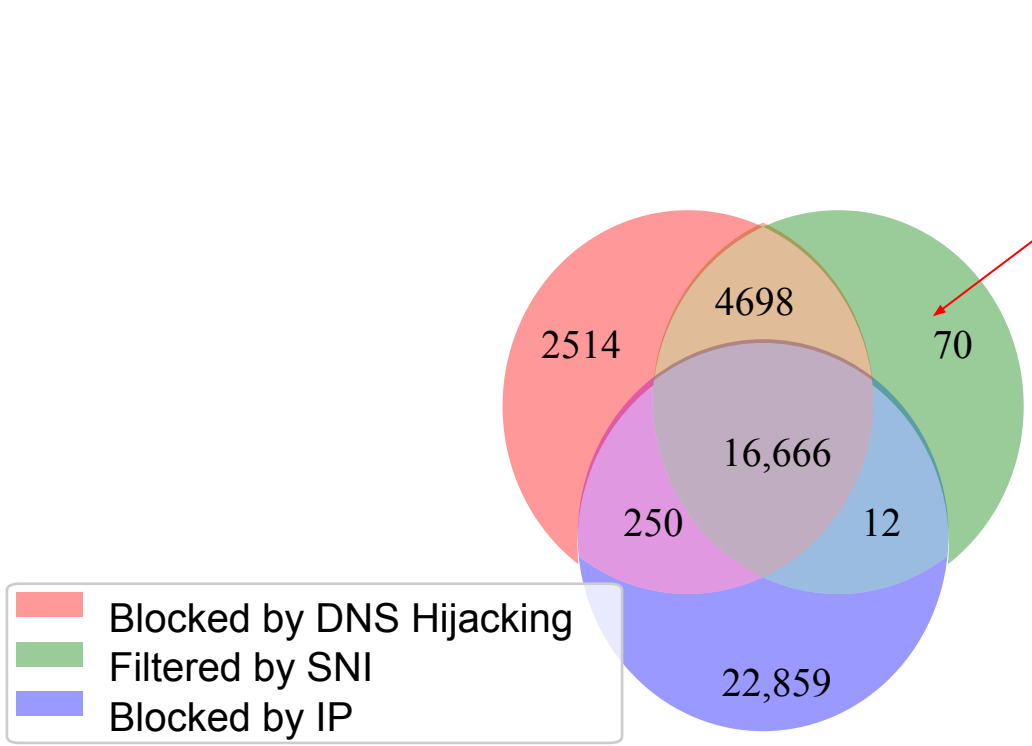
47,069 sites censored among Alexa Top 1M



Domains under different censorship

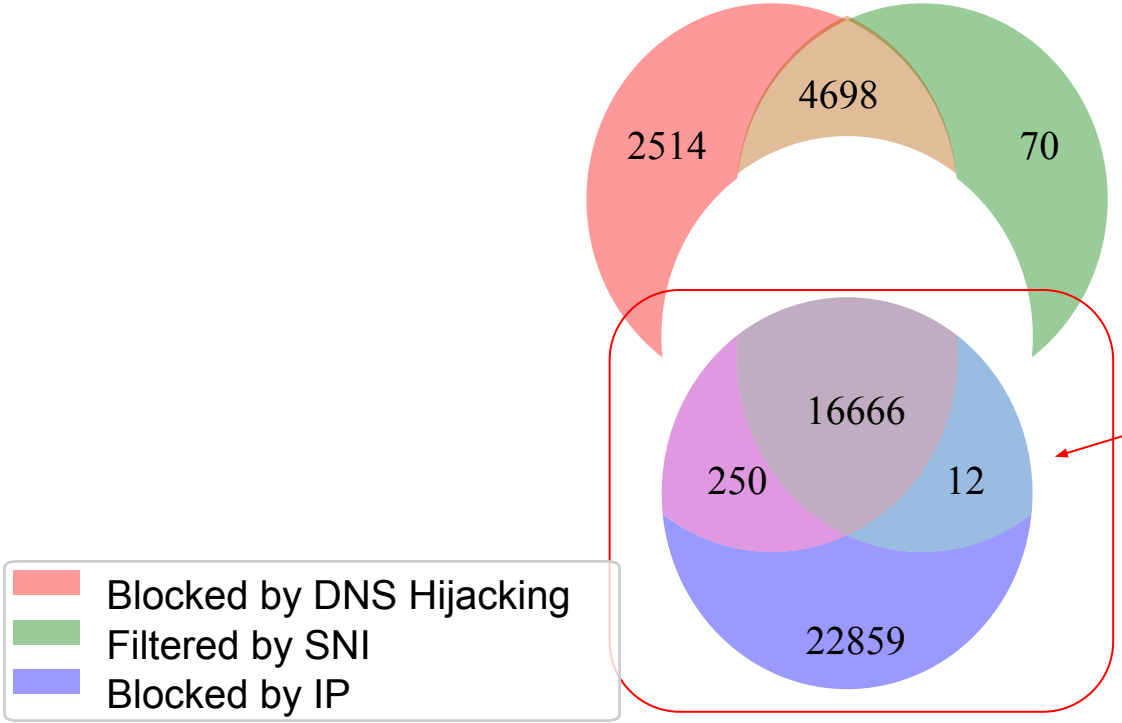


Domains under different censorship



70 sites are exclusively under SNI - Filtering

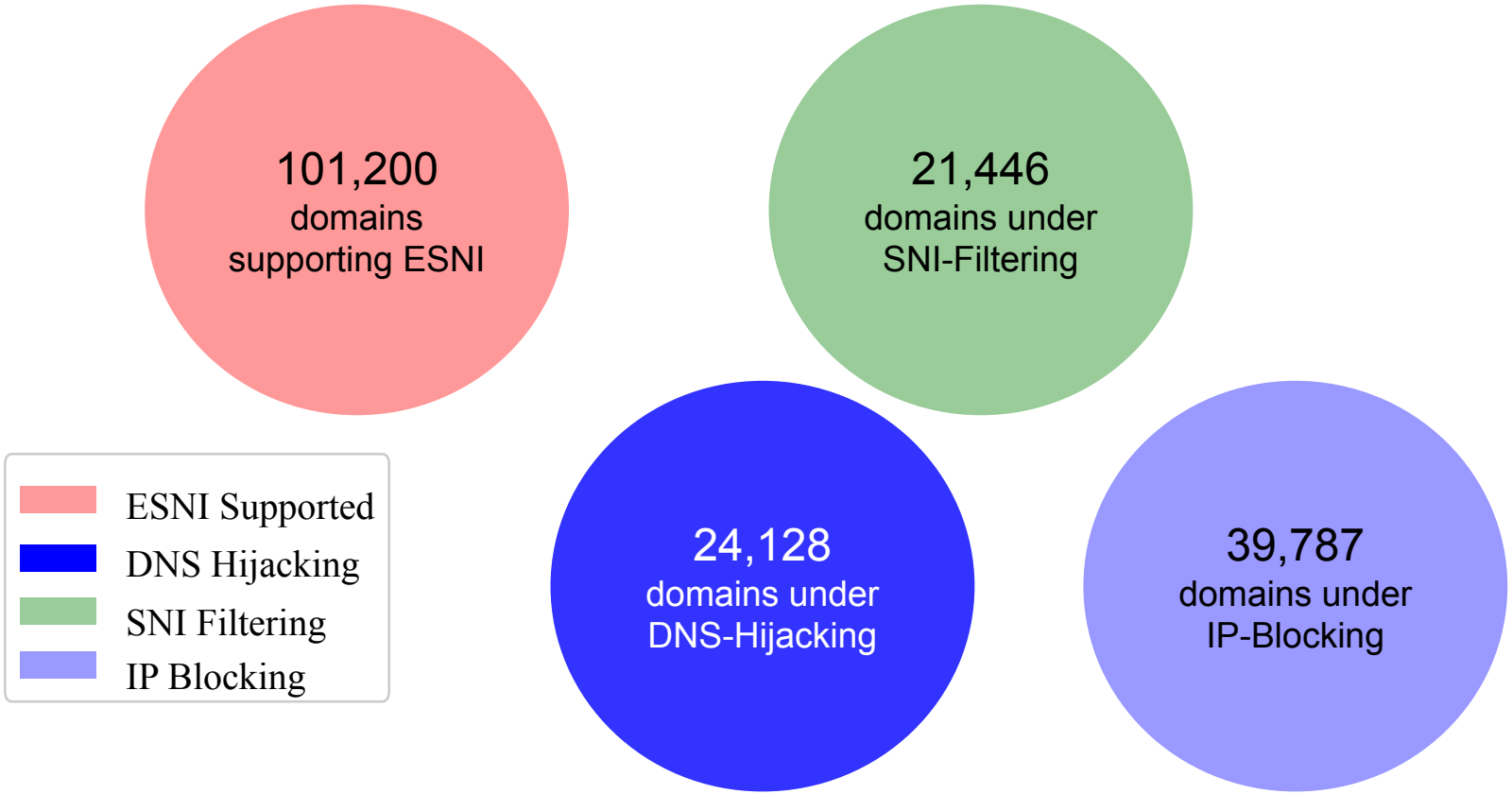
Domains under different censorship



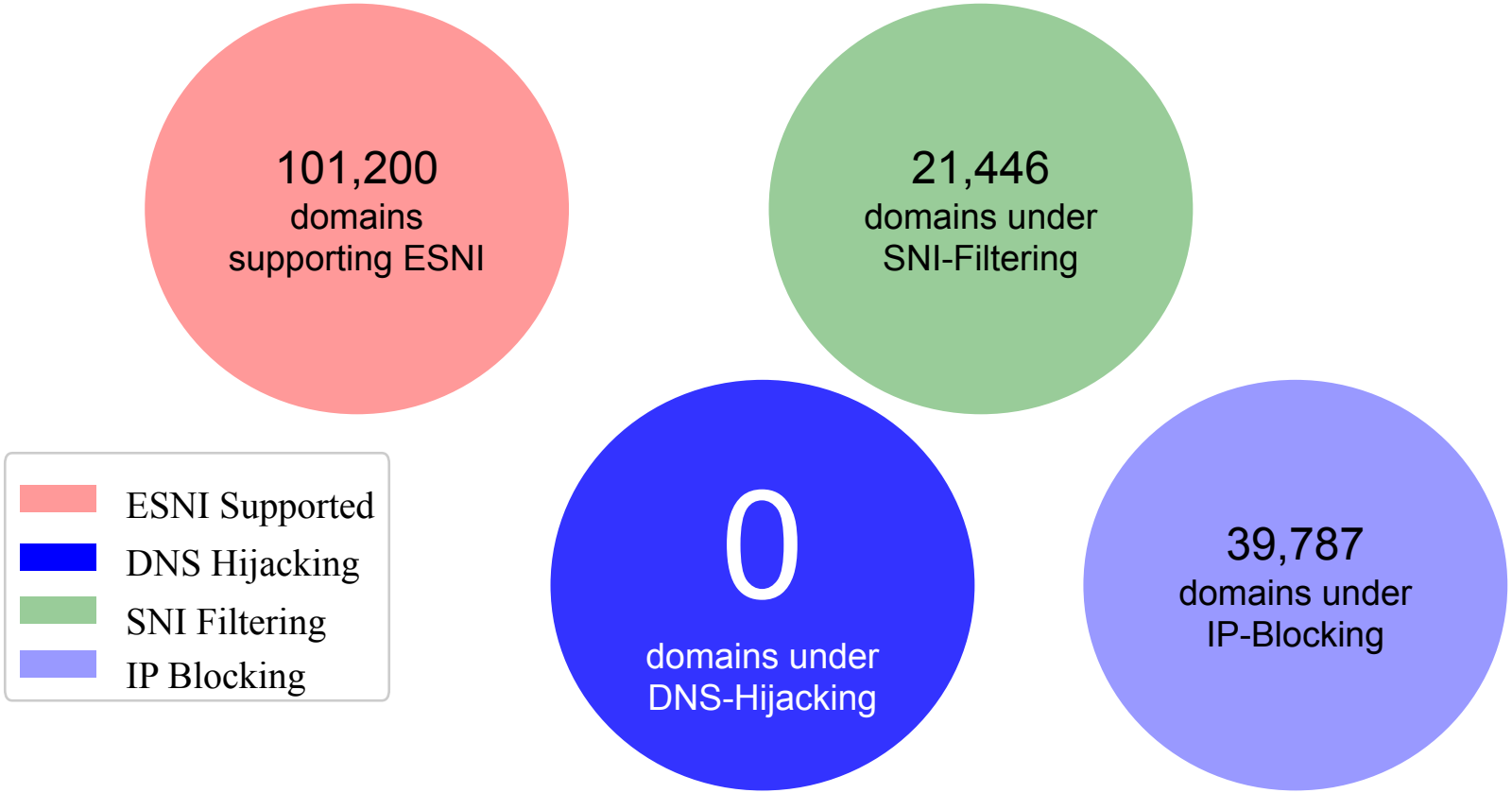
84.5% censored websites remain blocked in China

Effectiveness of ESNI

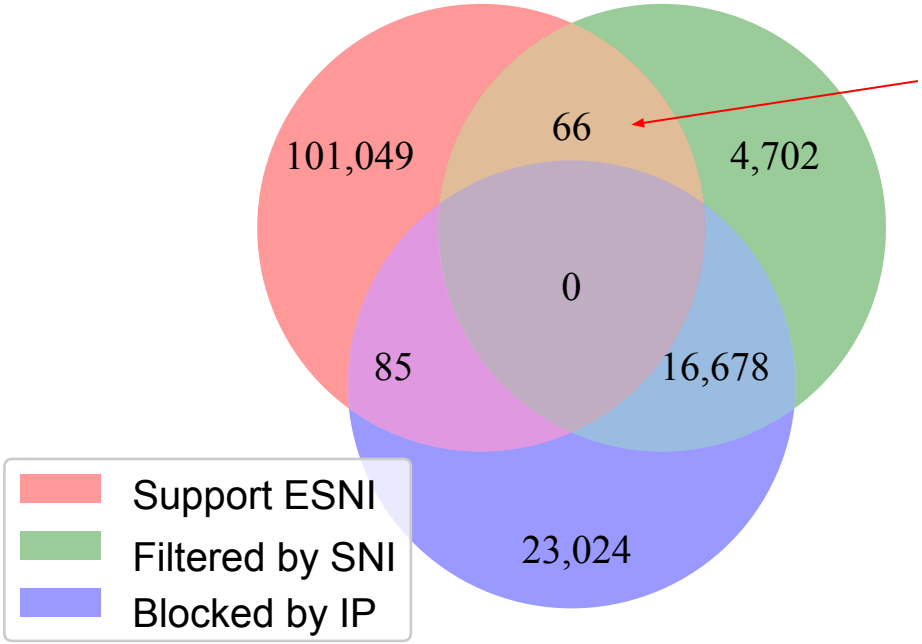
Effectiveness of ESNI



Assume DNS-based censorship evaded



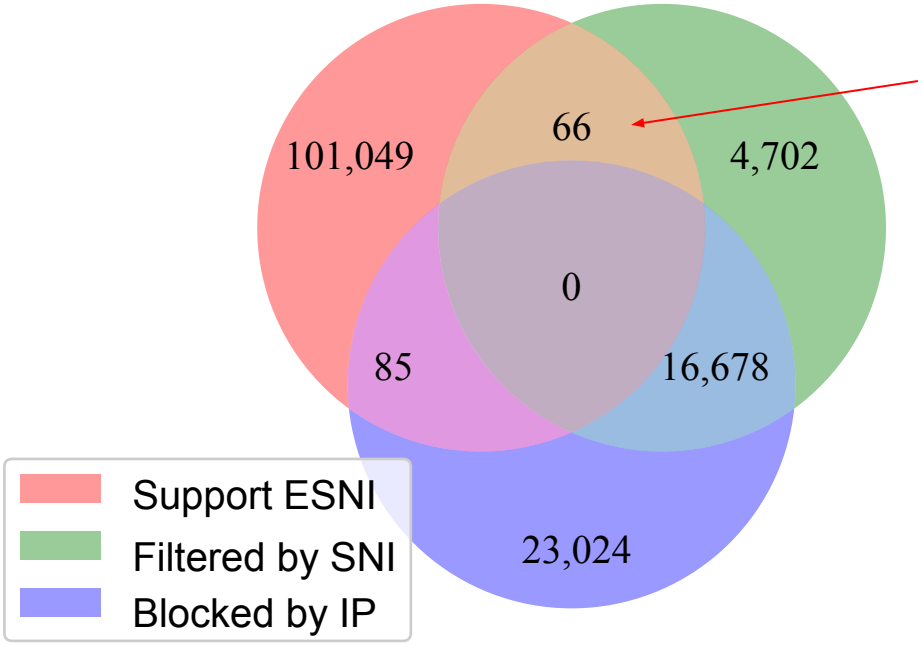
Current Effectiveness of ESNI



66 sites can be unblocked by ESNI

Censored websites VS. ESNI supporting websites

Current Effectiveness of ESNI

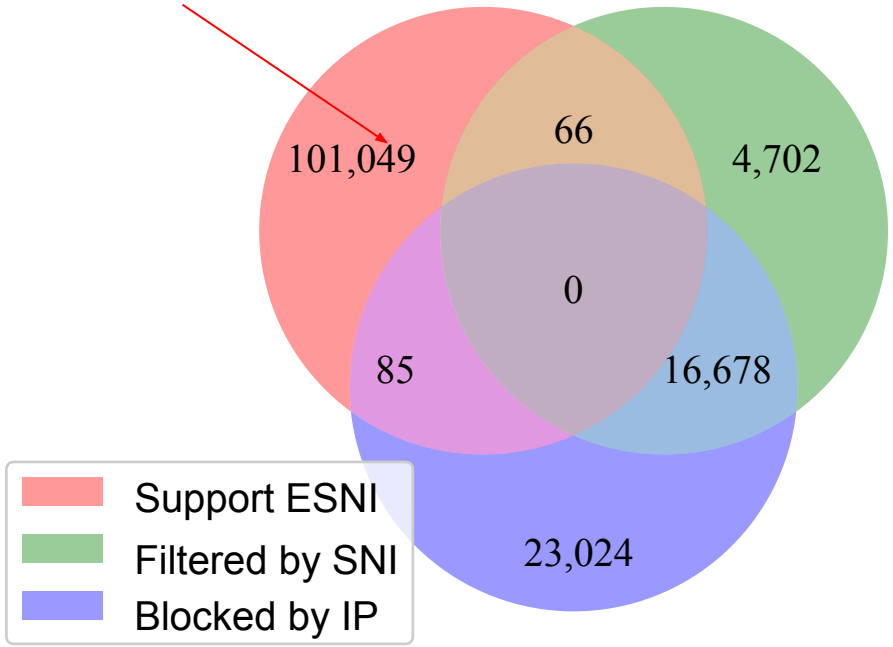


66 sites can be unblocked by ESNI

medium.com
boxun.com
chinadigitaltimes.net
bannedbook.org
rsf.org
amnesty.org.au
….

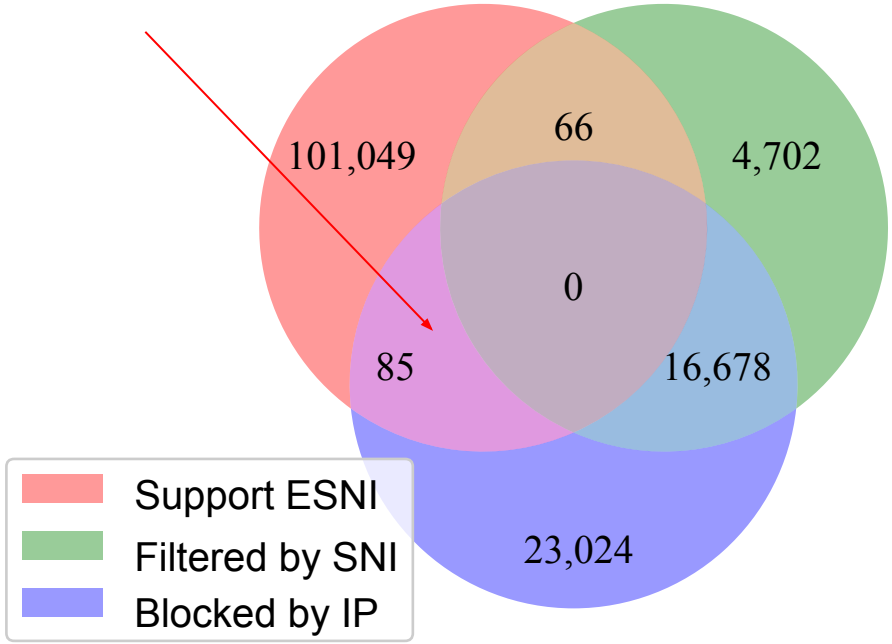
Censored websites VS. ESNI supporting websites

ESNI increases the cost of blocking 101k sites



Censored websites VS. ESNI supporting websites

IPs belong to CDN edge server are blocked



Censored websites VS. ESNI supporting websites

Monitoring **E**SNI-based Censorship

Any area already censoring ESNI traffic?

Nick Sullivan ✓
@grittygrease

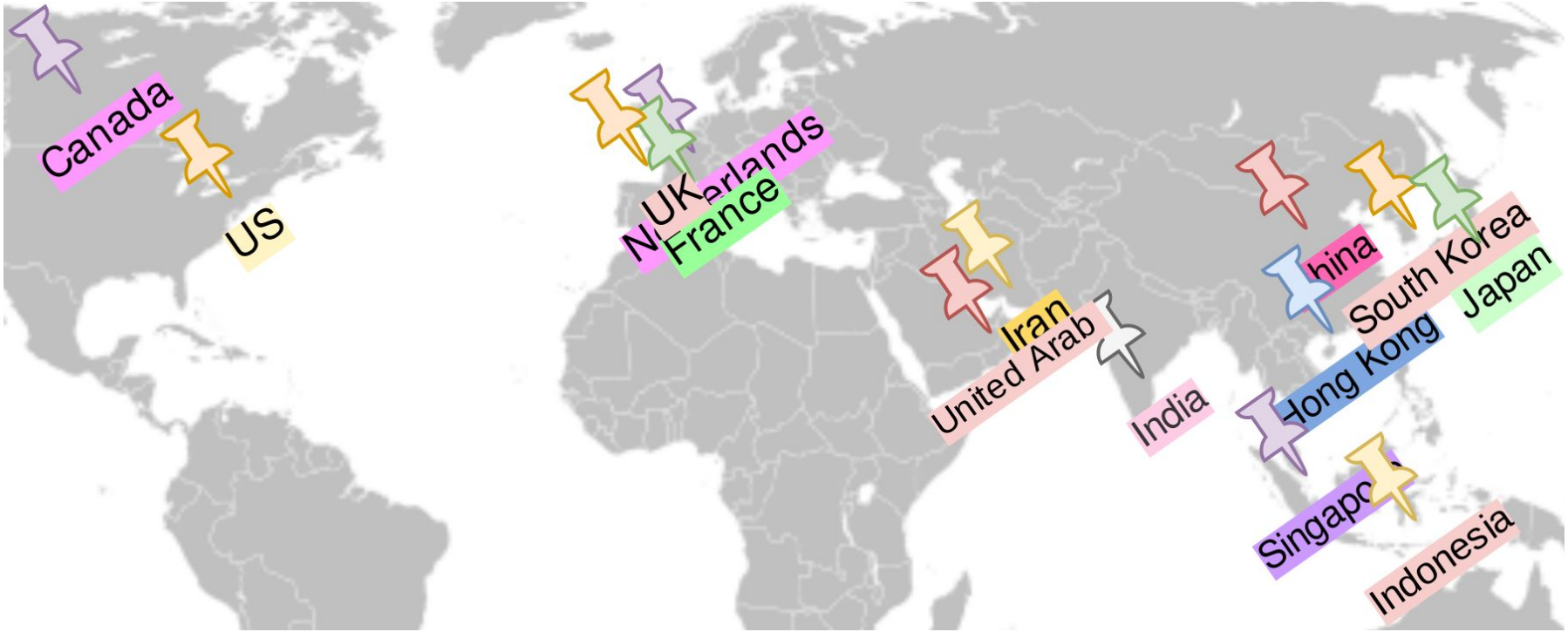
Follow

And it looks like they're blocking encrypted SNI outright (according to accounts on the ground). In some ways, this is our fault for not agreeing on a final spec and pushing it out to more clients faster. The politics around network privacy engineering are tricky. Cliffs abound.

> **Joseph Lorenzo Hall, PhD** @JoeBeOne
> Looks like South Korea has started filtering the internet across all ISPs using SNI (one thing we can't yet encrypt under TLS 1.3). Fuuuuuuck bugzil.la/1494901#c3 #censorship

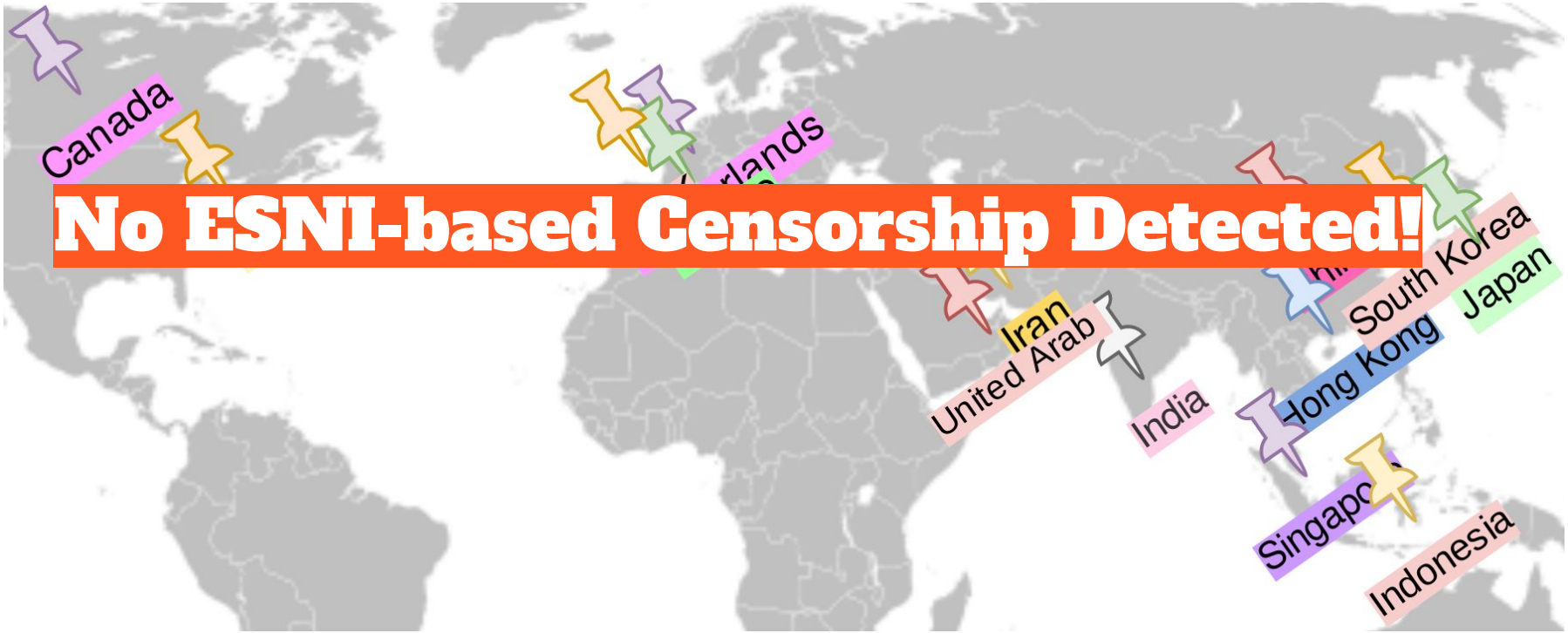
7:48 PM - 12 Feb 2019

Monitoring ESNI-based Censorship from 14 Different Areas



Monitoring ESNI-based Censorship - Setup

Monitoring from 14 Different Areas



Conclusions

Conclusions

- **10%** websites among Alexa Top 1M are **supporting ESNI**.

Conclusions

- **10%** websites among Alexa Top 1M are **supporting ESNI**.
- **84.5%** currently censored websites will **remain blocked** in China even if DNS- and SNI-based censorship are evaded.

Conclusions

- **10%** websites among Alexa Top 1M are **supporting ESNI**.
- **84.5%** currently censored websites will **remain blocked** in China even if DNS- and SNI-based censorship are evaded.
- Only **66** websites currently censored in China can be **unblocked by ESNI**.

Conclusions

- **10%** websites among Alexa Top 1M are **supporting ESNI**.
- **84.5%** currently censored websites will **remain blocked** in China even if DNS- and SNI-based censorship are evaded.
- Only **66** websites currently censored in China can be **unblocked by ESNI**.
- **No** **ESNI-based censorship** is detected in our experiment across **14** different areas.

Contacts

Zimo Chai - CS MS/PhD Student
zchai@cs.umass.edu

SPIN Lab, with Amir Houmansadr
https://people.cs.umass.edu/~amir/Research.html

We have released all our probing tools and datasets at http://traces.cs.umass.edu/index.php/Network, to maintain reproducibility and to benefit future research works.

Let's Enable ESNI Now!

1. Open **about:config** in Firefox
2. Set **network.security.esni.enabled** to **true**
3. Set **network.trr.mode** to **3**
4. Set **network.trr.uri** to https://1.1.1.1/dns-query
5. Check if it works: https://www.cloudflare.com/ssl/encrypted-sni