

model=MacBookPro11,1" "osxvers=17" (309)
10:11:55.160097 IP 31.133.136.177.5353 > 224.0.0.251.5353: 0 [1a] PTR (QM)? _smb._tcp.local. (72)
10:11:55.160515 IP 31.133.138.157.5353 > 224.0.0.251.5353: 0*- [0q] 3/0/6 (Cache flush) TXT "rpHN=1a6925a7eb85" "rpFl=0x2000" "rpVr=180.4" "rpHA=d2a7130d66f9" "rpAD=0b317fdb0588" "rpHI=48ec799123d3" "rpBA=93:47:98:8F:41:F0", PTR macbot._companion-link._tcp.local., TXT "model=MacBook10,1" "osxvers=19" "ecolor=157,157,160" (410)
10:11:55.161043 IP 31.133.129.229.137 > 31.133.143.255.137: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
10:11:55.172797 IP 192.17.23.217.43 > 31.133.138.171.59303: Flags [P.], seq 79560:80580, ack 67861, win 5963, length 1020
10:11:55.172890 IP 31.133.138.171.59303 > 192.17.23.217.443: Flags [.], ack 80580, win 4080, length 0
10:11:55.178540 IP 31.133.138.171.50190 > 52.96.51.104.443: Flags [S], seq 3078952158, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 1076035316 ecr 0,sackOK,eol], length 0
10:11:55.193603 IP 52.96.51.104.443 > 31.133.138.171.50190: Flags [R.], seq 0, ack 3078952159, win 8212, length 0
10:11:55.194481 IP 31.133.138.171.50191 > 40.100.162.24.443: Flags [S], seq 1099117591, win 65535, options [mss 1460,no p,wscale 6,nop,nop,TS val 1076035331 ecr 0,sackOK,eol], length 0
10:11:55.194913 IP 31.133.138.171.50193 > 40.100.162.24.443: Flags [F.], seq 4244328818, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 1076035332 ecr 0,sackOK,eol], length 0
10:11:55.201504 IP 31.133.138.171.5224.0.0.251 > 31.133.138.171.50192: Flags [v2, report], seq 721.0.0.251, length 0
10:11:55.209721 IP 40.100.162.8.443 > 31.133.138.171.50192: Flags [R.], seq 0, ack 2768536748, win 8212, length 0
10:11:55.209724 IP 40.100.162.24.443 > 31.133.138.171.50191: Flags [R.], seq 0, ack 1099117592, win 8212, length 0
10:11:55.213671 IP 31.133.138.171.50193 > 52.96.51.104.443: Flags [S], seq 2768536747, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 1076035349 ecr 0,sackOK,eol], length 0
10:11:55.229502 IP 52.96.51.104.443 > 31.133.138.171.50193: Flags [R.], seq 0, ack 2768536748, win 8212, length 0
10:11:55.230620 IP 31.133.138.171.50194 > 40.100.162.24.443: Flags [S], seq 730766292, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 1076035366 ecr 0,sackOK,eol], length 0
10:11:55.231308 IP 31.133.138.171.50195 > 40.100.162.8.443: Flags [S], seq 4080278356, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 1076035366 ecr 0,sackOK,eol], length 0

What Can You Learn from an IP?

Simran Patil and Nikita Borisov

University of Illinois at Urbana-Champaign



@SimranPatil25 @nikitab

In the beginning...



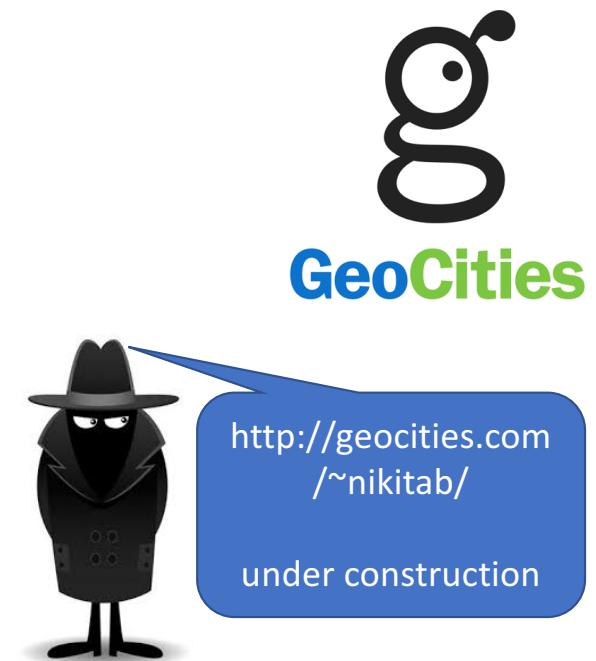
```
GET /~nikitab/ HTTP/1.1  
Host: geocities.com
```

...

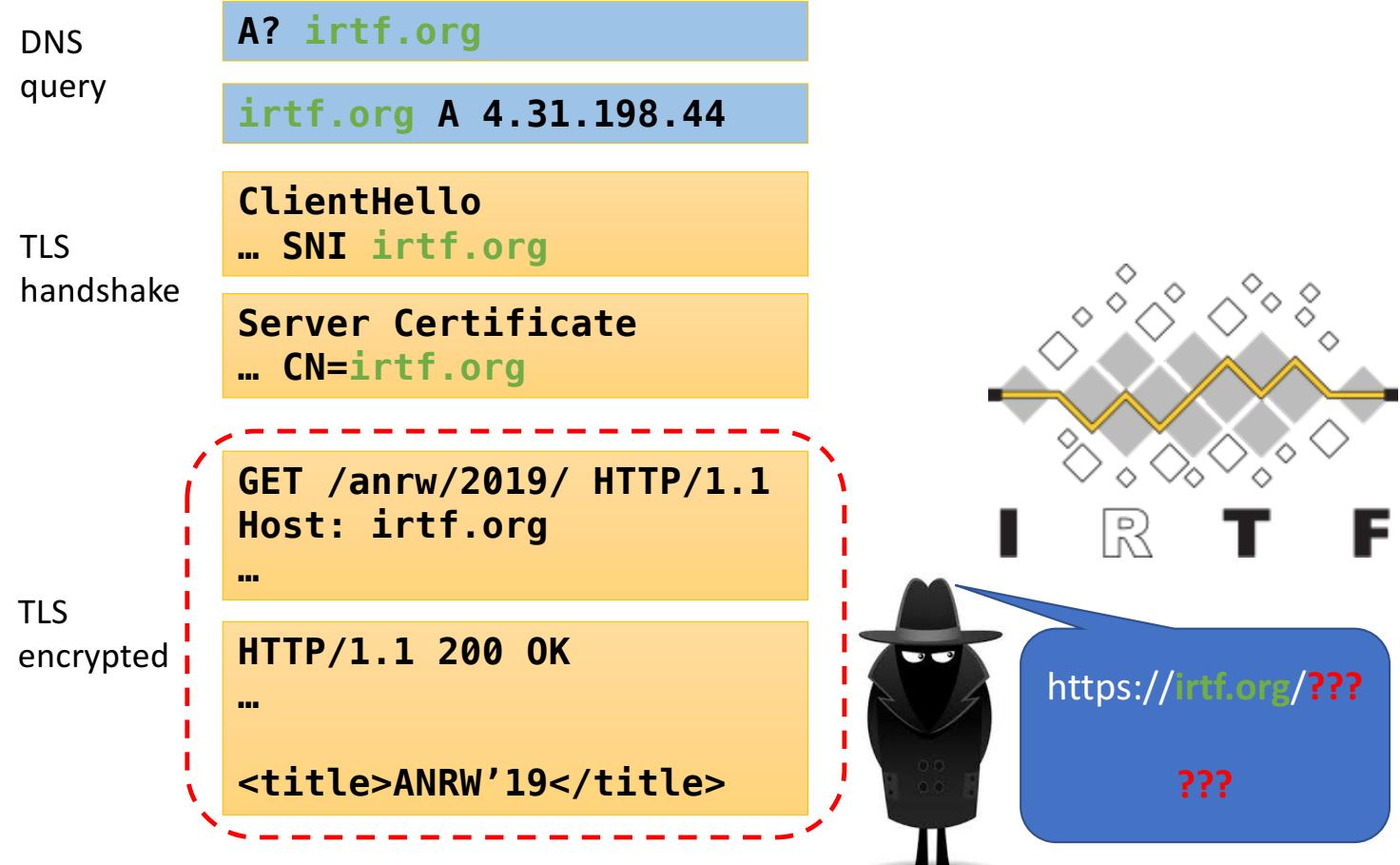
```
HTTP/1.1 200 OK
```

...

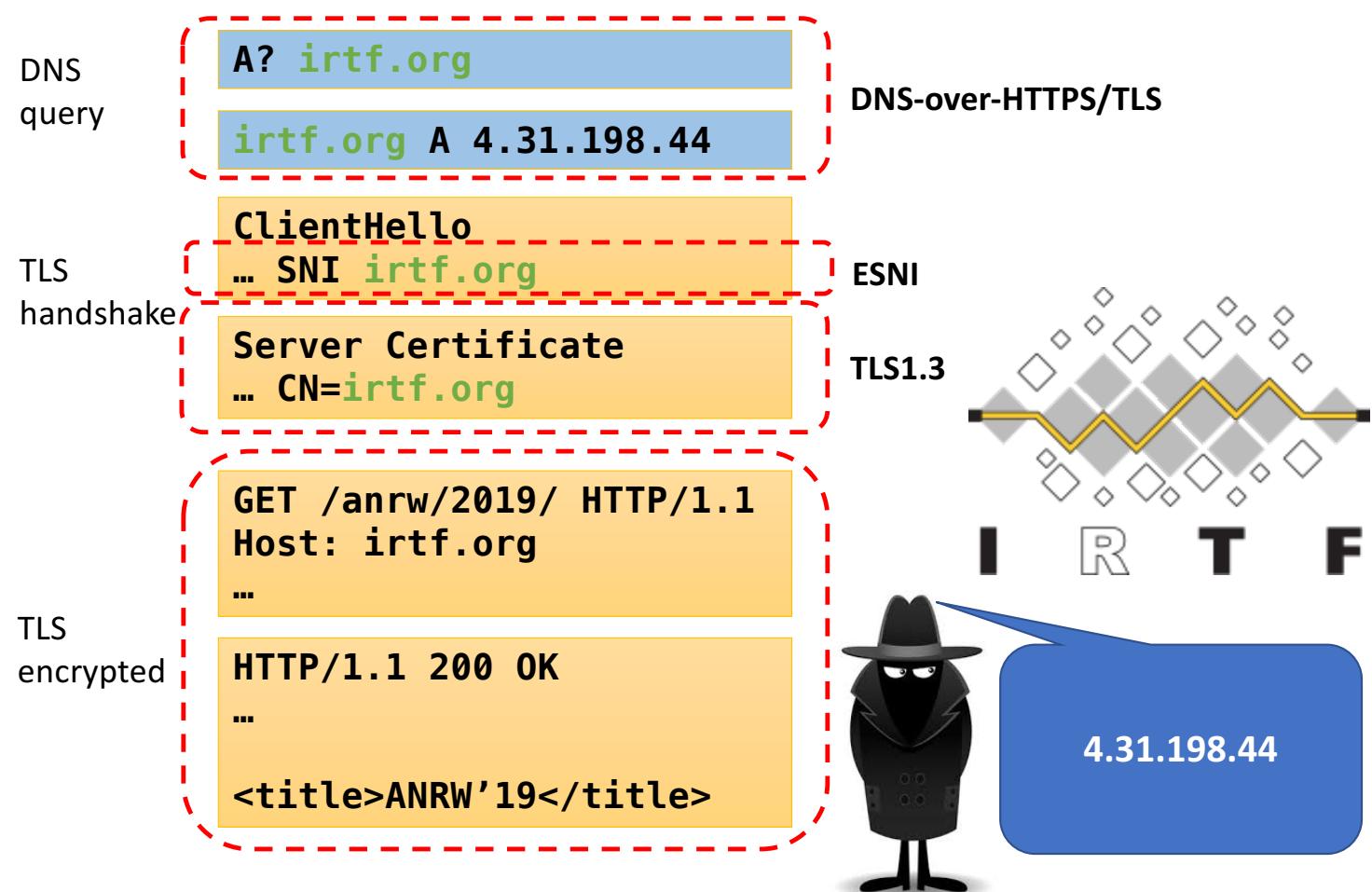
```
<blink>this page is  
under  
construction</blink>
```



Today



Soon?



What can you learn from a domain name?

drugrehab.ca

vim.org

whatisabrony.com

dailystormer.name

www.lgbtcenters.org

foxnews.com

lymphoma.ca

nickleback.com

anime-expo.org

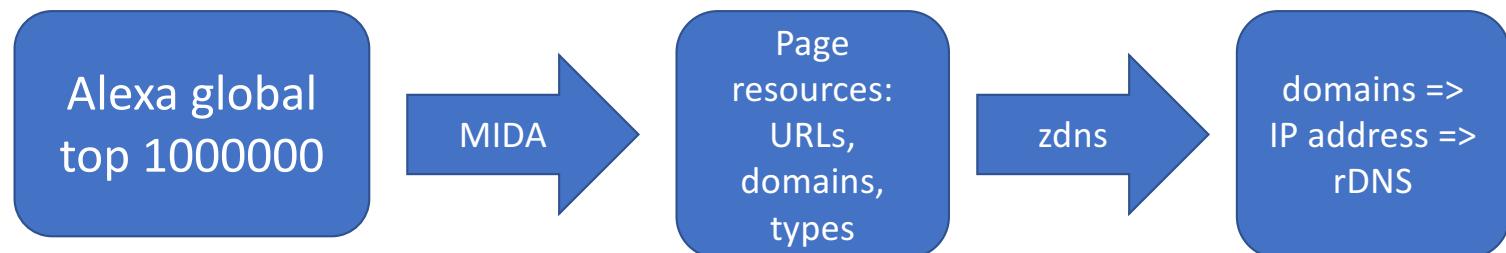
aljazeera.com

www.oshawamosque.com

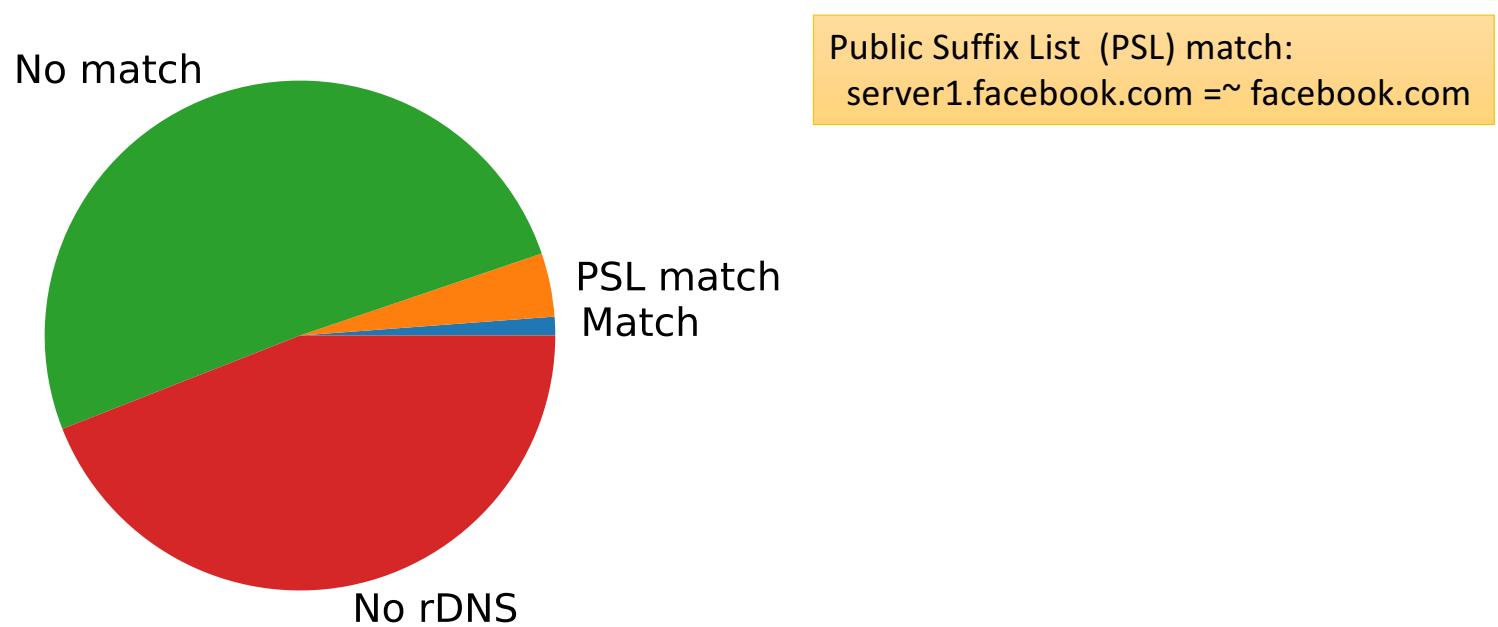
furrycons.com

montrealcathedral.ca

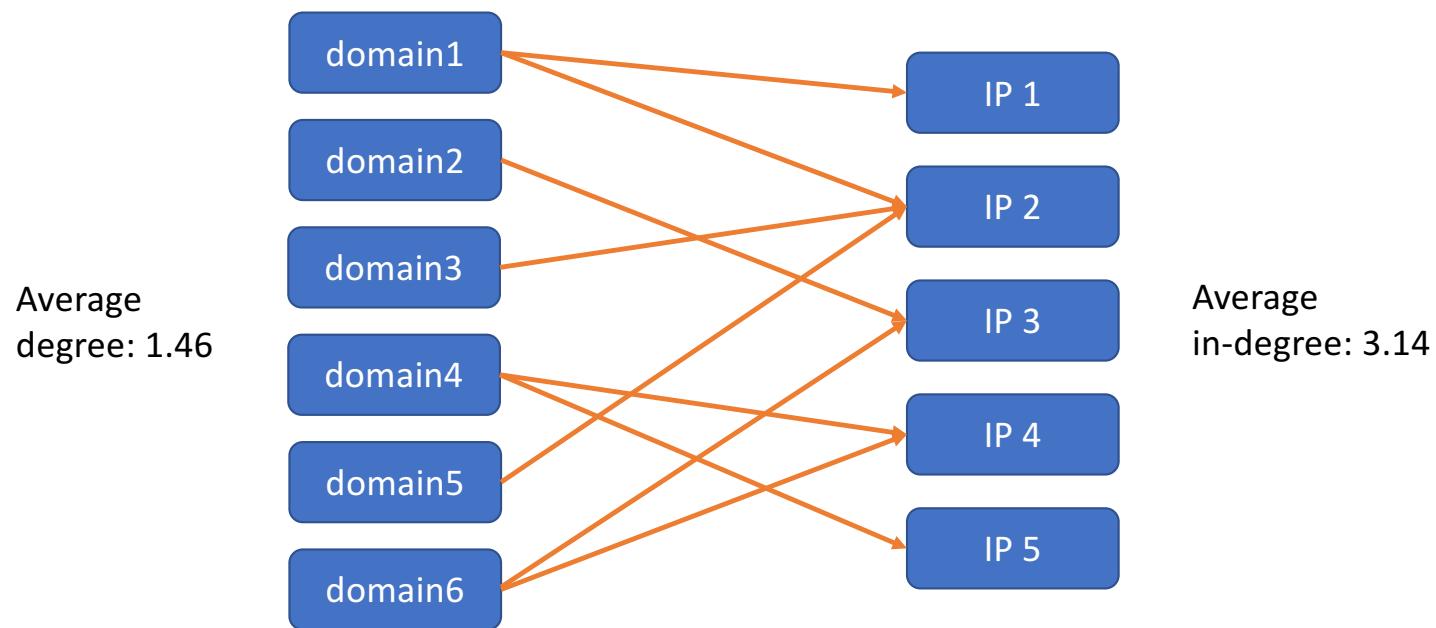
Methodology



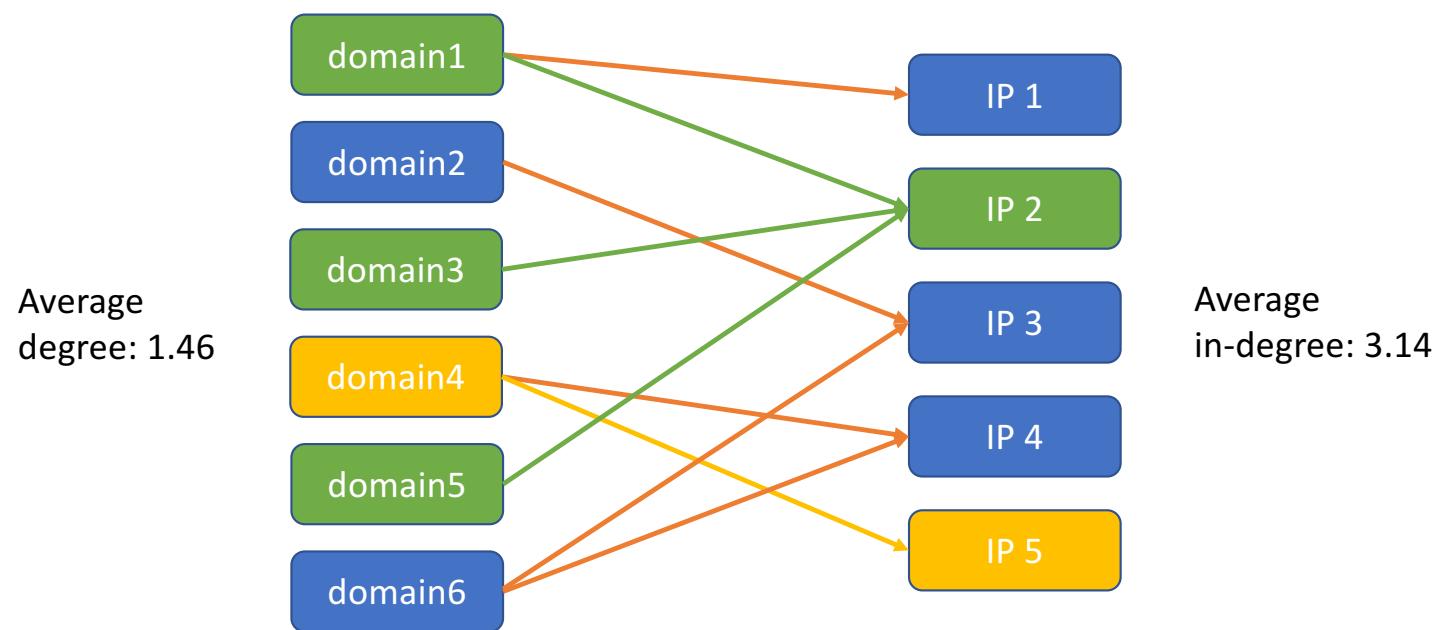
rDNS



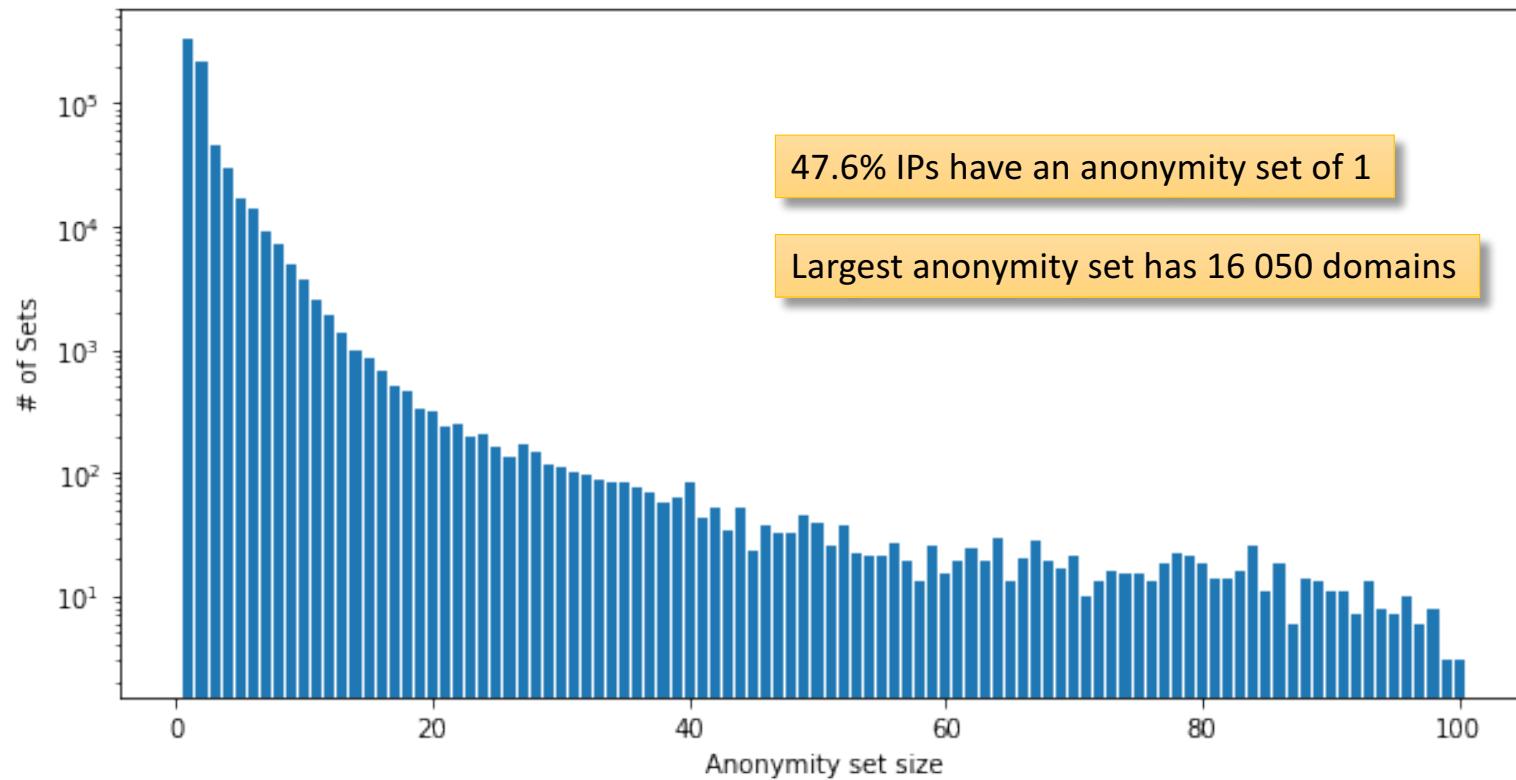
Domains and IPs



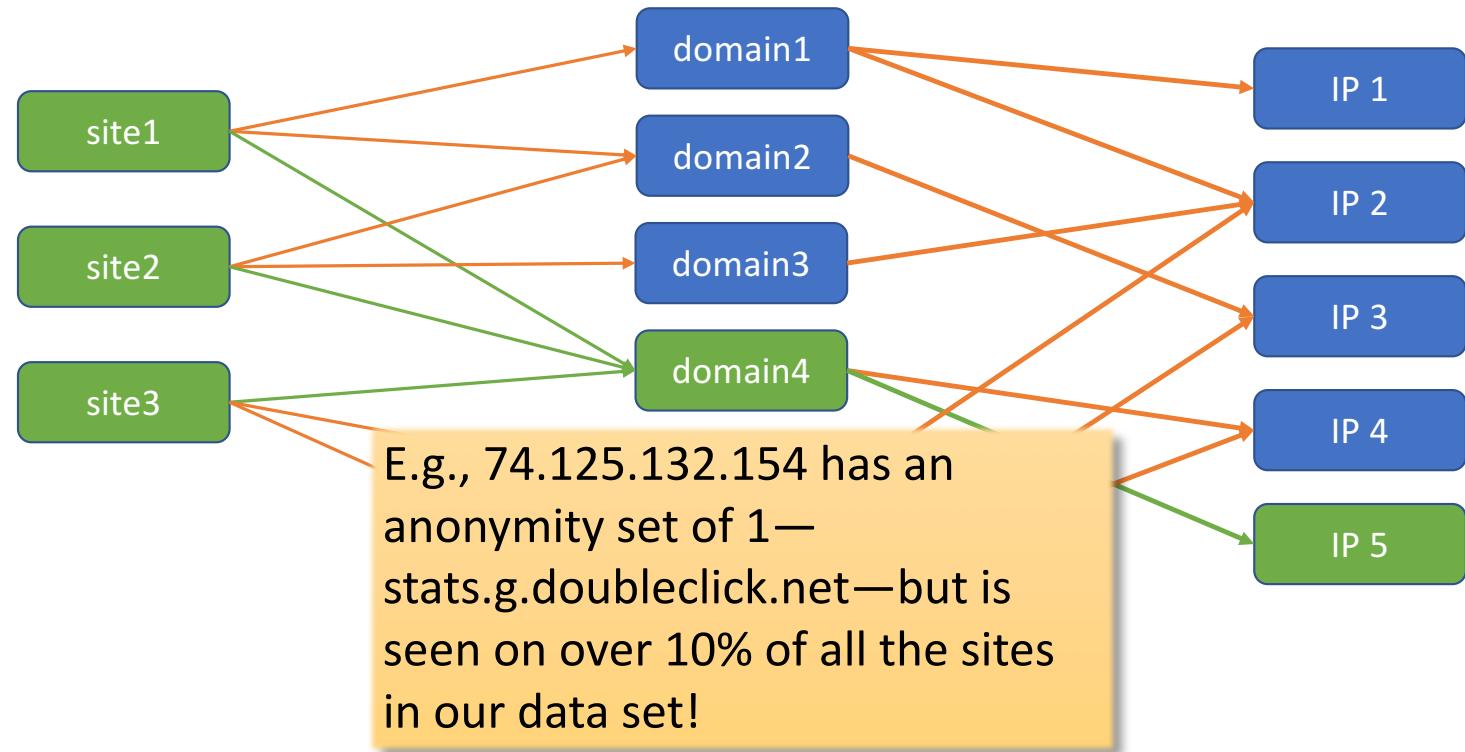
IP Anonymity Set



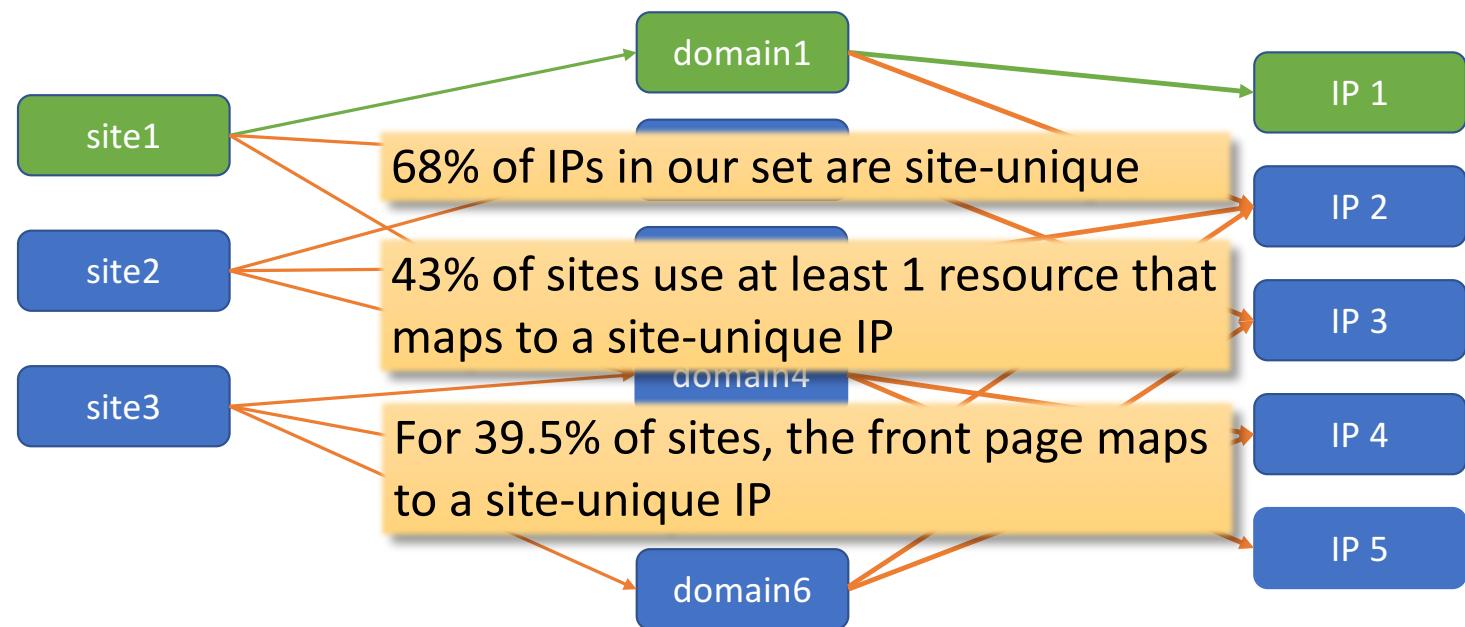
IP Anonymity Sets



Site-unique IPs



Site-unique IPs



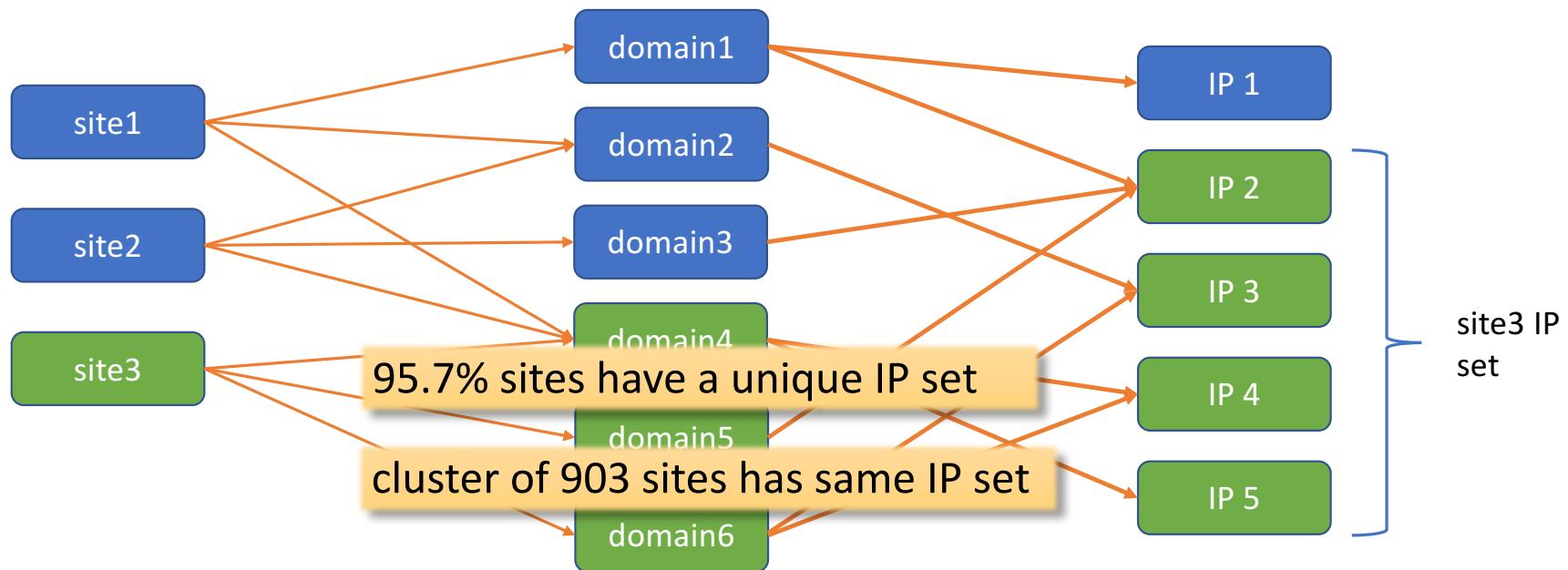
Page Load Fingerprints

	queen-elizabeth-montreal		www.fairmont.com	document	23.64.109.196:443
	fairmont-prod.js		cloud.moovweb.net	js	192.33.31.70:443
	font.css		www.fairmont.com	css	23.64.109.196:443
	fairmont.min.css		d1r80pgesju2u.cloud...	css	99.84.112.4:443
	tripadvisor.min.css		d1r80pgesju2u.cloud...	css	99.84.112.4:443
	3colbigbanner.min.css		www.fairmont.com	css	23.64.109.196:443
	s_code.js		d1r80pgesju2u.cloud...	js	99.84.112.4:443
	accorhotelsconnect.js		secure.accorhotels.ws	js	193.200.231.133:443
	WebResource.axd		www.fairmont.com	js	23.64.109.196:443
	593e534a-7cf8-4956-b5a9-4c8da07c...		www.fairmont.com	jpg	23.64.109.196:443



**23.64.109.196
192.33.31.70
98.84.112.4
193.200.231.133**

Site IP sets



What about CDNs?

- Many CDNs **could** use same IP address for all sites but **don't**
 - Ported IP space
 - Connections w/o SNI
- In our data set 200K domains are hosted by CloudFlare, using 91K IPs
 - Including 3% of the sites with a site-unique front page IP
- Randomizing or normalizing IP addresses could help

Conclusions

- DNS privacy offers limited protection
 - For web browsing
 - Against an adversary with a good prior list of sites
- In our Alexa 1M crawl dataset
 - 48% of all IPs map to a single domain
 - 68% of all IPs map to a single site
 - 43% of all sites contain a site-unique IP
 - 95% of sites have a unique IP set
- Changes to web hosting infrastructure could help
 - Normalize or randomize CDN IP addresses