The International Conference on Passive and Active Network Measurement
March 28–30, 2022

Measuring the Accessibility of Domain Name Encryption and its Impact on Internet Filtering

Nguyen Phong Hoang, Michalis Polychronakis, Phillipa Gill

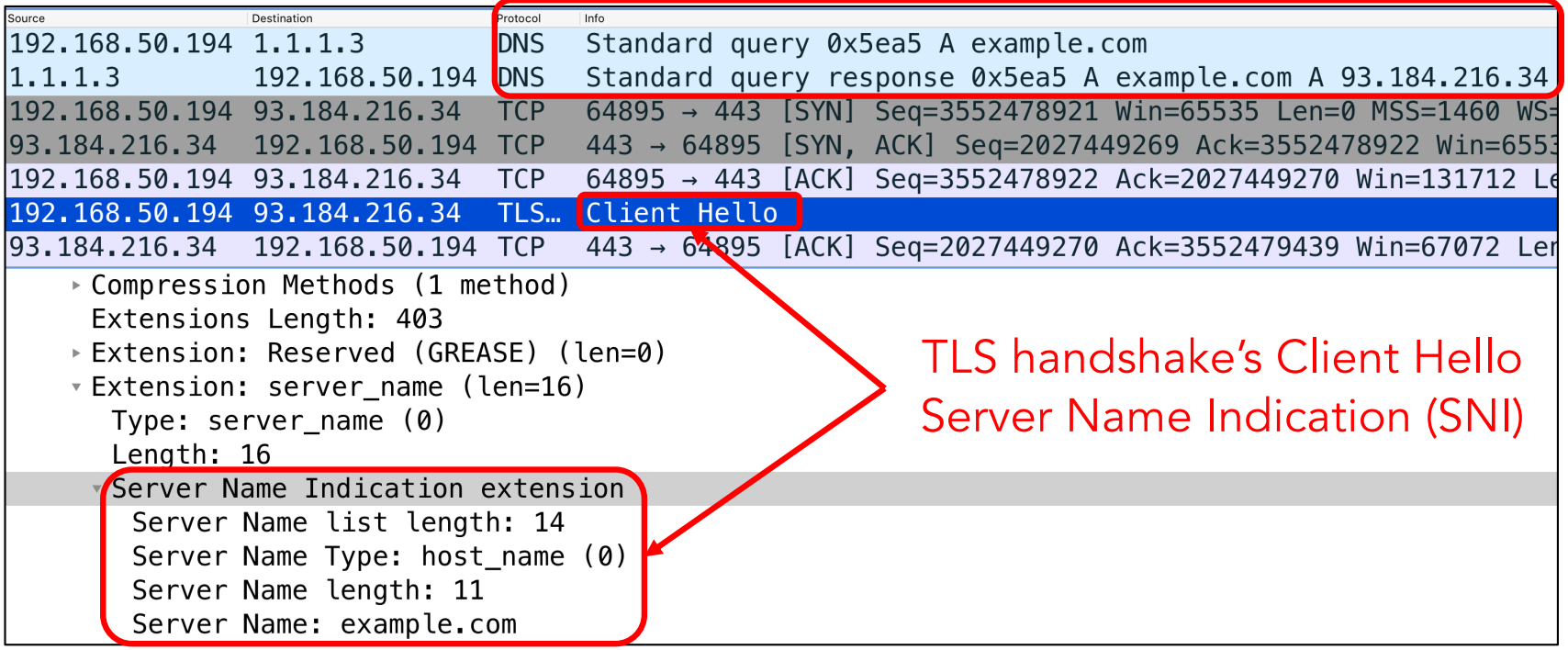
THE UNIVERSITY OF CHICAGO

Stony Brook University

Google

Plaintext domains in network traffic

DNS query/response packets



TLS handshake's Client Hello
Server Name Indication (SNI)

→ Security and privacy problems

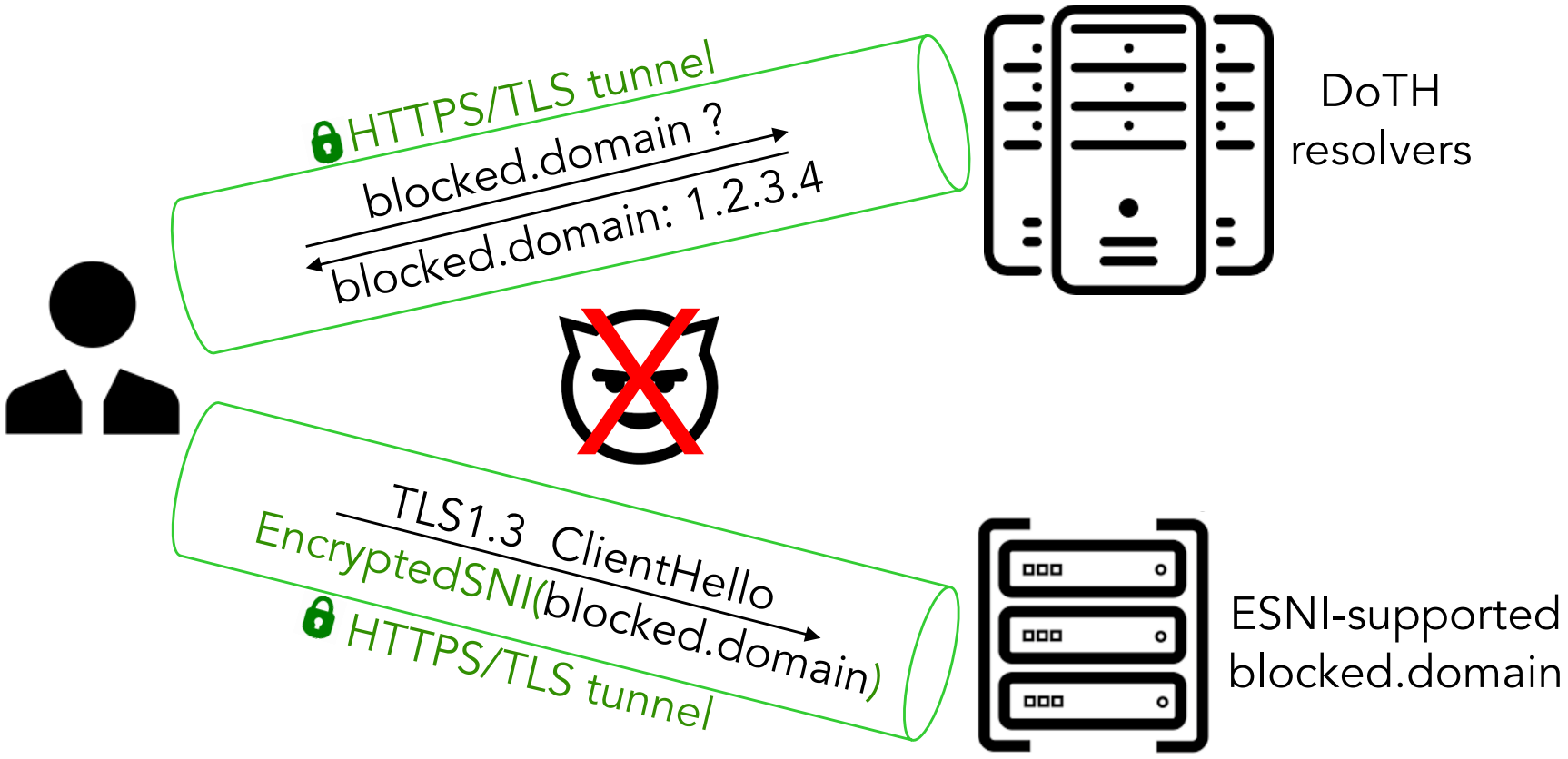
→ Susceptible to domain-based network filtering

Domain name encryption: DoT/DoH & ESNI

- **DoT:** DNS queries and responses are sent over a TLS tunnel using port 853 (RFC7858)
- **DoH:** DNS resolution is performed over HTTPS, inheriting all security benefits of the HTTPS protocol (RFC8484)
- **Encrypted SNI**: Starting from TLS1.3, the Server Name Indication extension in the Client Hello message during the TLS handshake can be ***optionally*** encrypted (RFC8744)

  → being reworked to Encrypted Client Hello (Internet draft)

Domain encryption: DoT/DoH and ESNI



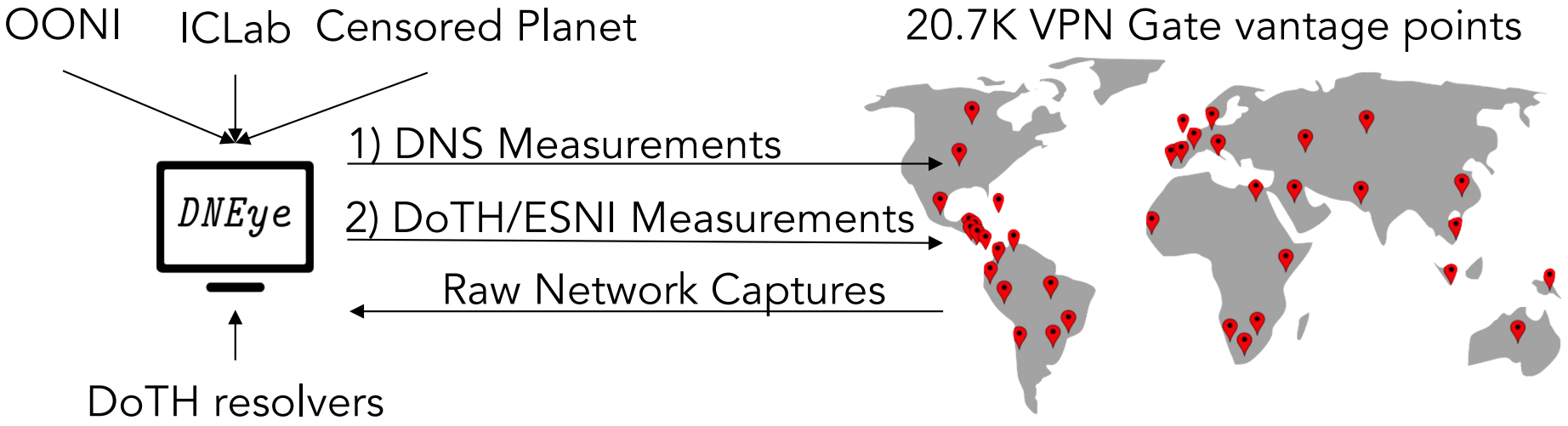
Motivation

Domain name encryption → better security and privacy

How about its impact on Internet filtering?

- Investigate whether domain name encryption technologies are being blocked by Internet filtering systems around the globe
- If not, can domain name encryption help with circumventing Internet censorship based on domain name information

DNEye



	Asia	Africa	America	Europe	Oceania
Countries	32	4	15	32	2
# of ASes	367	9	215	271	16

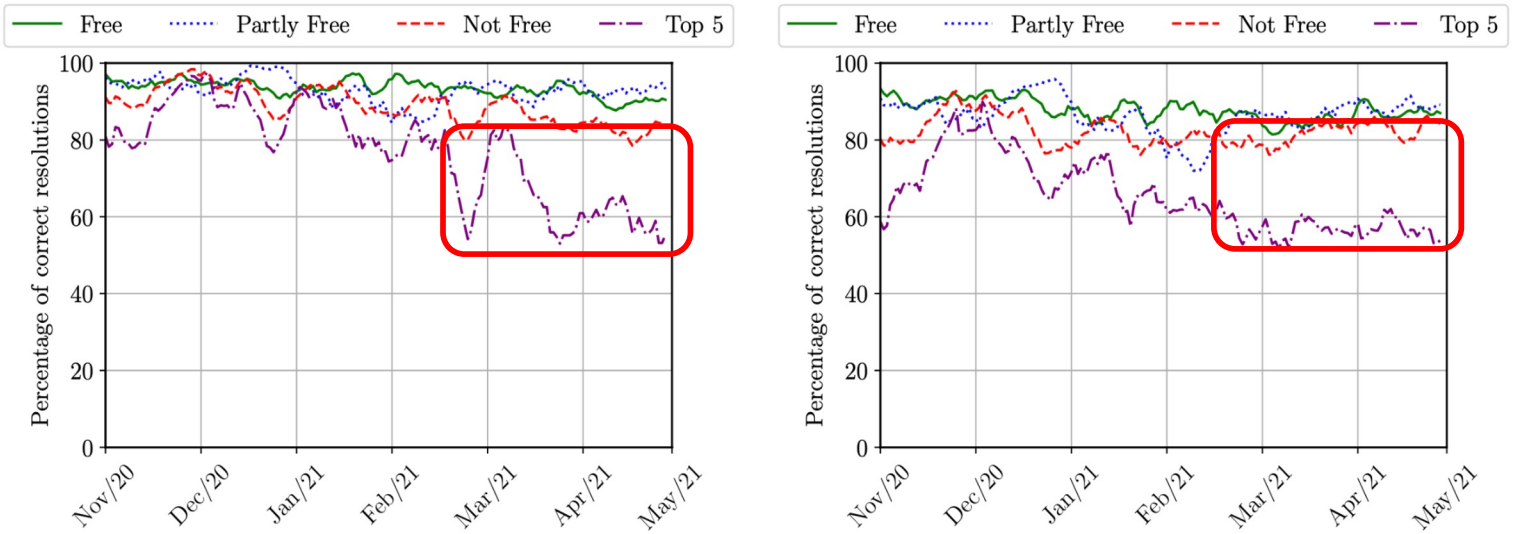
DNS-based Internet filtering is widespread

Country	Number of confirmed domains censored by DNS tampering
China	300
Russia	205
Iran	147
Indonesia	134
India	98

No major evidence of DNS-based filtering of DoTH at the AS level

- ordns.he.net blocked by China's Great Firewall via DNS poisoning
- cloudflare-dns.com and mozilla.cloudflare.com in Thailand 's AS23969

DoTH accessibility



(a) Resolutions using DoT

(b) Resolutions using DoH

Fig. 2: Percentage of correct DoTH resolutions over time.

China started blocking both DoT and DoH resolutions destined for popular DoTH resolvers from March 2021

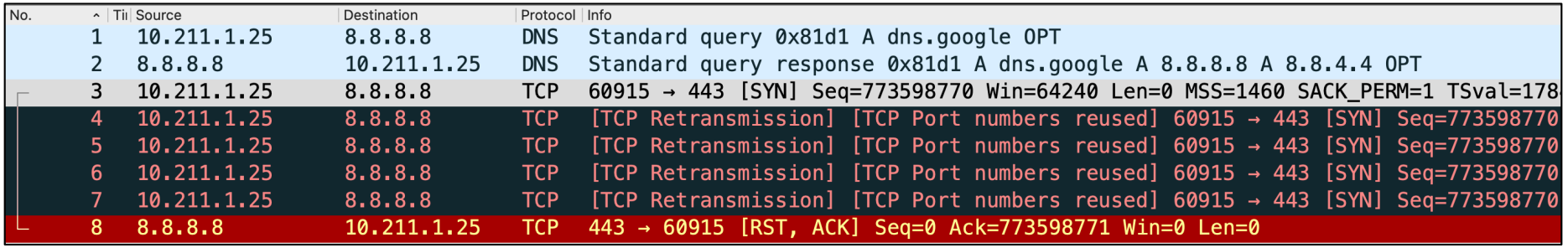
Blocking of DoT resolutions in China

Time	Source	Destination	Protocol	Info
22:22:37.…	10.211.1.25	185.228.168.9	TCP	36395 → 853 [SYN] Seq=1931890697 Win=64240 Len=0 MSS=1460
22:22:38.…	10.211.1.25	185.228.168.9	TCP	[TCP Retransmission] [TCP Port numbers reused] 36395 → 853
22:22:40.…	10.211.1.25	185.228.168.9	TCP	[TCP Retransmission] [TCP Port numbers reused] 36395 → 853
22:22:44.…	10.211.1.25	185.228.168.9	TCP	[TCP Retransmission] [TCP Port numbers reused] 36395 → 853
22:22:52.…	10.211.1.25	185.228.168.9	TCP	[TCP Retransmission] [TCP Port numbers reused] 36395 → 853
22:23:02.…	185.228.168.9	10.211.1.25	TCP	853 → 36395 [RST, ACK] Seq=0 Ack=1931890698 Win=0 Len=0

- DNS over TLS is standardized in RFC7858 with 853 being used as the default port
- Port 853 is not used by other popular applications

→ Blocking the IP:853 pair is trivial and sufficient to hinder the use of DNS over TLS

Blocking of DoH resolutions in China

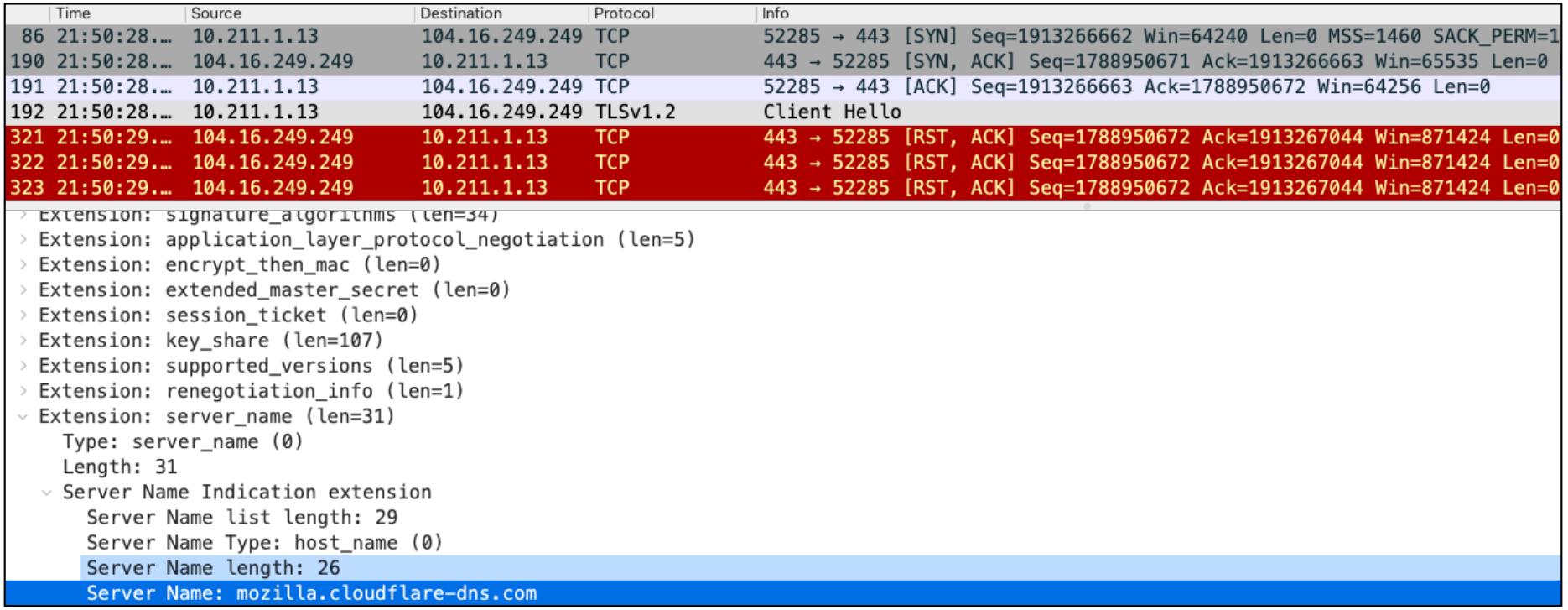


No.	Tii	Source	Destination	Protocol	Info
1		10.211.1.25	8.8.8.8	DNS	Standard query 0x81d1 A dns.google OPT
2		8.8.8.8	10.211.1.25	DNS	Standard query response 0x81d1 A dns.google A 8.8.8.8 A 8.8.4.4 OPT
3		10.211.1.25	8.8.8.8	TCP	60915 → 443 [SYN] Seq=773598770 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=178
4		10.211.1.25	8.8.8.8	TCP	[TCP Retransmission] [TCP Port numbers reused] 60915 → 443 [SYN] Seq=773598770
5		10.211.1.25	8.8.8.8	TCP	[TCP Retransmission] [TCP Port numbers reused] 60915 → 443 [SYN] Seq=773598770
6		10.211.1.25	8.8.8.8	TCP	[TCP Retransmission] [TCP Port numbers reused] 60915 → 443 [SYN] Seq=773598770
7		10.211.1.25	8.8.8.8	TCP	[TCP Retransmission] [TCP Port numbers reused] 60915 → 443 [SYN] Seq=773598770
8		8.8.8.8	10.211.1.25	TCP	443 → 60915 [RST, ACK] Seq=0 Ack=773598771 Win=0 Len=0

- DNS over HTTPS uses the popular 443 port
- IPs of popular DoH-supported DNS resolvers are widely known

→ Blocking the resolver_IP:443 pair is trivial and sufficient to hinder DNS over HTTPS services deployed by popular public resolvers

Blocking of Cloudflare DoH resolvers in Saudi Arabia

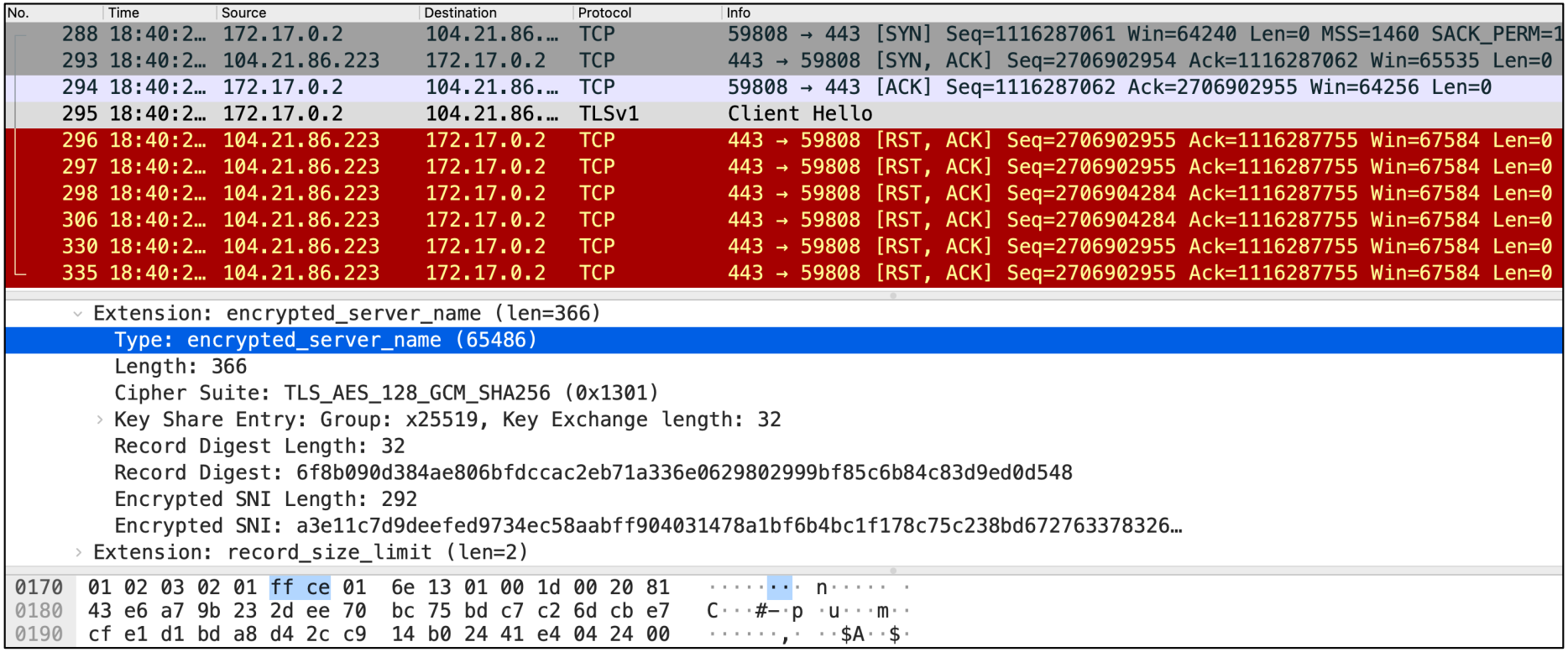


	Time	Source	Destination	Protocol	Info
86	21:50:28.…	10.211.1.13	104.16.249.249	TCP	52285 → 443 [SYN] Seq=1913266662 Win=64240 Len=0 MSS=1460 SACK_PERM=1
190	21:50:28.…	104.16.249.249	10.211.1.13	TCP	443 → 52285 [SYN, ACK] Seq=1788950671 Ack=1913266663 Win=65535 Len=0
191	21:50:28.…	10.211.1.13	104.16.249.249	TCP	52285 → 443 [ACK] Seq=1913266663 Ack=1788950672 Win=64256 Len=0
192	21:50:28.…	10.211.1.13	104.16.249.249	TLSv1.2	Client Hello
321	21:50:29.…	104.16.249.249	10.211.1.13	TCP	443 → 52285 [RST, ACK] Seq=1788950672 Ack=1913267044 Win=871424 Len=0
322	21:50:29.…	104.16.249.249	10.211.1.13	TCP	443 → 52285 [RST, ACK] Seq=1788950672 Ack=1913267044 Win=871424 Len=0
323	21:50:29.…	104.16.249.249	10.211.1.13	TCP	443 → 52285 [RST, ACK] Seq=1788950672 Ack=1913267044 Win=871424 Len=0

```
> Extension: signature_algorithms (len=34)
> Extension: application_layer_protocol_negotiation (len=5)
> Extension: encrypt_then_mac (len=0)
> Extension: extended_master_secret (len=0)
> Extension: session_ticket (len=0)
> Extension: key_share (len=107)
> Extension: supported_versions (len=5)
> Extension: renegotiation_info (len=1)
v Extension: server_name (len=31)
    Type: server_name (0)
    Length: 31
  v Server Name Indication extension
      Server Name list length: 29
      Server Name Type: host_name (0)
      Server Name length: 26
      Server Name: mozilla.cloudflare-dns.com
```

Centralized blocking of *.cloudflare-dns.com DoH resolvers in Saudi Arabia detected at different network locations

Decentralized blocking of ESNI Blocking in Russia



No.	Time	Source	Destination	Protocol	Info
288	18:40:2…	172.17.0.2	104.21.86.…	TCP	59808 → 443 [SYN] Seq=1116287061 Win=64240 Len=0 MSS=1460 SACK_PERM=1
293	18:40:2…	104.21.86.223	172.17.0.2	TCP	443 → 59808 [SYN, ACK] Seq=2706902954 Ack=1116287062 Win=65535 Len=0
294	18:40:2…	172.17.0.2	104.21.86.…	TCP	59808 → 443 [ACK] Seq=1116287062 Ack=2706902955 Win=64256 Len=0
295	18:40:2…	172.17.0.2	104.21.86.…	TLSv1	Client Hello
296	18:40:2…	104.21.86.223	172.17.0.2	TCP	443 → 59808 [RST, ACK] Seq=2706902955 Ack=1116287755 Win=67584 Len=0
297	18:40:2…	104.21.86.223	172.17.0.2	TCP	443 → 59808 [RST, ACK] Seq=2706902955 Ack=1116287755 Win=67584 Len=0
298	18:40:2…	104.21.86.223	172.17.0.2	TCP	443 → 59808 [RST, ACK] Seq=2706904284 Ack=1116287755 Win=67584 Len=0
306	18:40:2…	104.21.86.223	172.17.0.2	TCP	443 → 59808 [RST, ACK] Seq=2706904284 Ack=1116287755 Win=67584 Len=0
330	18:40:2…	104.21.86.223	172.17.0.2	TCP	443 → 59808 [RST, ACK] Seq=2706902955 Ack=1116287755 Win=67584 Len=0
335	18:40:2…	104.21.86.223	172.17.0.2	TCP	443 → 59808 [RST, ACK] Seq=2706902955 Ack=1116287755 Win=67584 Len=0

```
Extension: encrypted_server_name (len=366)
  Type: encrypted_server_name (65486)
  Length: 366
  Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
  Key Share Entry: Group: x25519, Key Exchange length: 32
  Record Digest Length: 32
  Record Digest: 6f8b090d384ae806bfdccac2eb71a336e0629802999bf85c6b84c83d9ed0d548
  Encrypted SNI Length: 292
  Encrypted SNI: a3e11c7d9deefed9734ec58aabff904031478a1bf6b4bc1f178c75c238bd672763378326…
Extension: record_size_limit (len=2)
```

```
0170  01 02 03 02 01 ff ce 01  6e 13 01 00 1d 00 20 81   ·····ÎÍ· n····· ·
0180  43 e6 a7 9b 23 2d ee 70  bc 75 bd c7 c2 6d cb e7   C···#-·p ·u···m··
0190  cf e1 d1 bd a8 d4 2c c9  14 b0 24 41 e4 04 24 00   ·····,· ··$A··$·
```

Decentralized blocking of ESNI connections in Russia based on the 2-byte signature ff ce of Encrypted SNI protocol

Filtering circumvention with domain name encryption

Country	Circumvented/ Total crawled	Other filtering techniques			
		TCP	HTTP	TLS	SS
China	130/230	11	2	84	3
Russia	53/56	1	1	1	0
Iran	0/49	1	1	47	0
Indonesia	93/98	2	2	0	1
India	20/20	0	0	0	0

- Encrypting DNS can help bypassing DNS-based censorship
- Not all domains support encrypted SNI

  → still susceptible to SNI-based blocking

Key takeaway

- Domain name encryption can help to partially circumvent Internet censorship based on DNS
- Notorious censors have already taken a step ahead to hinder the deployment of domain name encryption by
  - ✓ blocking DoTH servers
  - ✓ blocking ESNI connections

  => Domain name encryption protocols should be designed and deployed in a way such that blocking their traffic is not an option without causing large collateral damage
- SNI-based blocking is still possible as encrypted SNI has not been widely adopted

  => Encrypted Client Hello should be adopted universally