@thisNatasha

Solving HTTP Problems With Code and Protocols

Natasha Rooney

WEB

HTTP

TLS

TCP

IP

7. **Application** Data	HTTP / IMAP
6. Data **Presentation**, Encryption	SSL / TLS
5. **Session** and connection management	-
4. **Transport** of packets and streams	TCP / UDP
3. Routing and delivery of datagrams on the **Network**	IP / IPSec
2. Local **Data** Connection	Ethernet
1. **Physical** data connection (cables)	CAT5

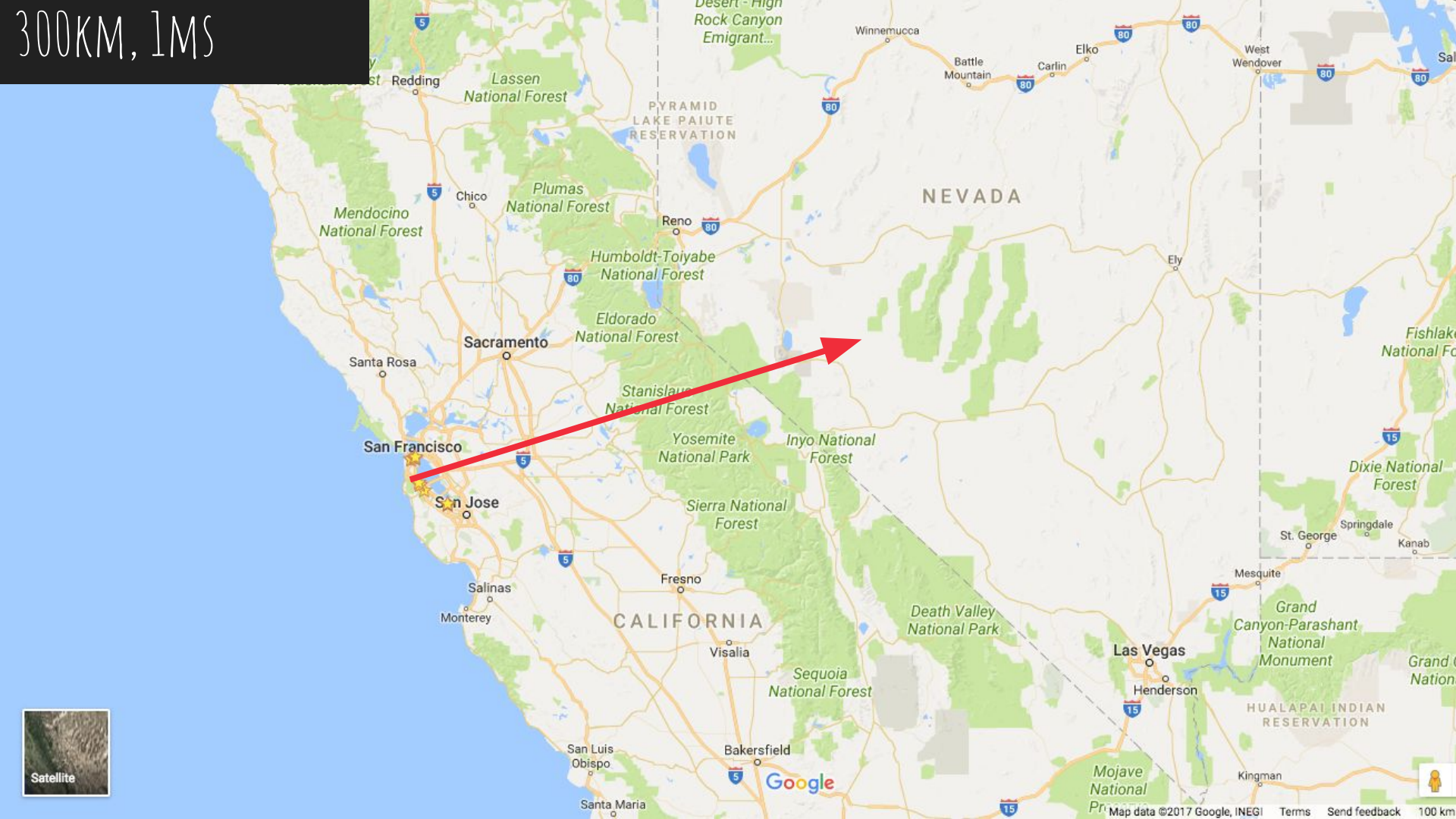
Some fundamental limitations

300,000,000 m/s

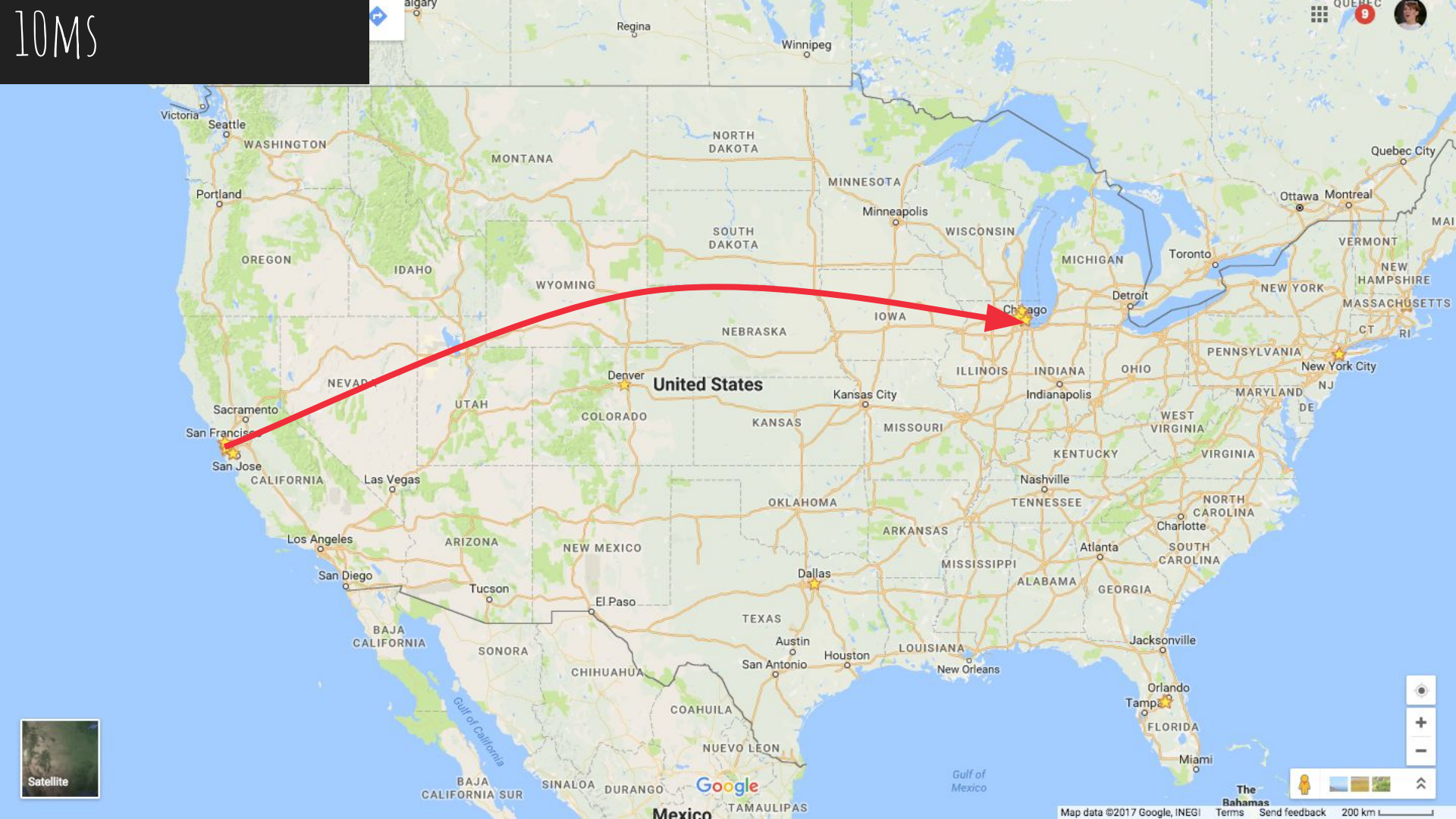
300,000,000 m/s

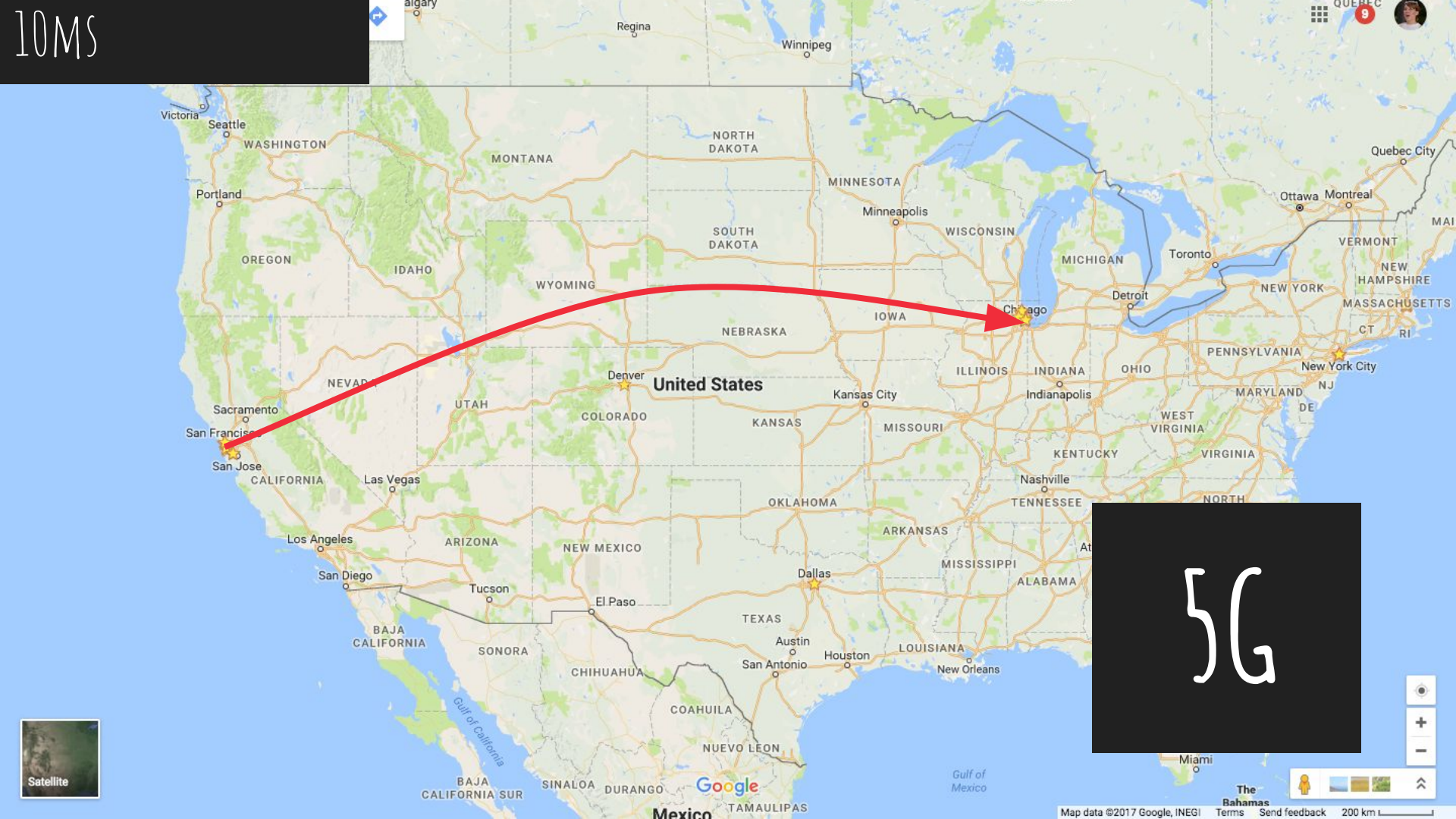
Speed of Light

300KM, 1MS


Redding
Lassen National Forest
Chico
Plumas National Forest
Mendocino National Forest
Reno
Humboldt-Toiyabe National Forest
Eldorado National Forest
Sacramento
Santa Rosa
San Francisco
San Jose
Stanislaus National Forest
Yosemite National Park
Inyo National Forest
Sierra National Forest
Fresno
Salinas
Monterey
CALIFORNIA
Visalia
Sequoia National Forest
Bakersfield
San Luis Obispo
Santa Maria
Death Valley National Park
Las Vegas
Henderson
Mesquite
St. George
Springdale
Kanab
Dixie National Forest
Grand Canyon-Parashant National Monument
HUALAPAI INDIAN RESERVATION
Kingman
Mojave National
NEVADA
Ely
Elko
Carlin
Battle Mountain
Winnemucca
West Wendover
PYRAMID LAKE PAIUTE RESERVATION
Desert - High Rock Canyon Emigrant...
Satellite
Google
Map data ©2017 Google, INEGI
Terms
Send feedback
100 km

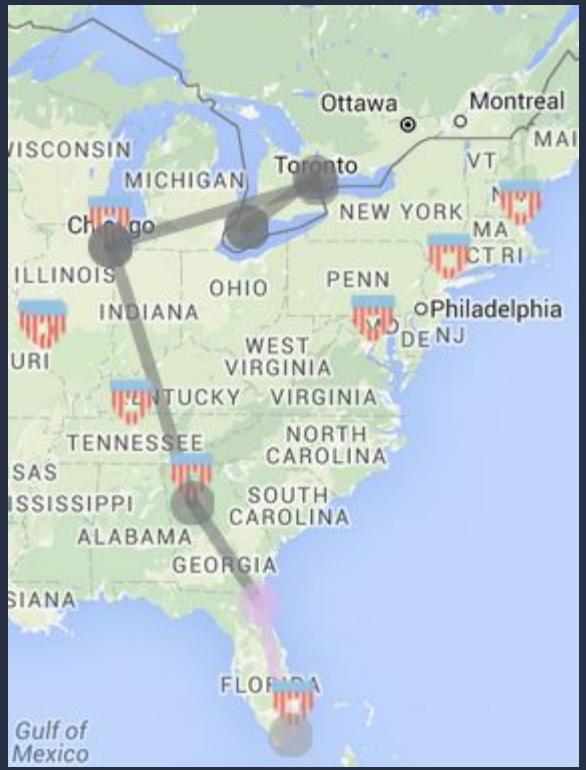
10MS


Regina
Winnipeg
Victoria
Seattle
WASHINGTON
MONTANA
NORTH DAKOTA
MINNESOTA
Minneapolis
Portland
OREGON
IDAHO
SOUTH DAKOTA
WISCONSIN
WYOMING
MICHIGAN
Toronto
Ottawa
Montreal
Quebec City
IOWA
Detroit
NEBRASKA
Denver
United States
Kansas City
ILLINOIS
INDIANA
OHIO
Indianapolis
PENNSYLVANIA
New York City
Sacramento
San Francisco
San Jose
CALIFORNIA
UTAH
COLORADO
KANSAS
MISSOURI
Las Vegas
OKLAHOMA
Nashville
TENNESSEE
KENTUCKY
WEST VIRGINIA
VIRGINIA
Los Angeles
ARIZONA
NEW MEXICO
ARKANSAS
Charlotte
NORTH CAROLINA
Atlanta
SOUTH CAROLINA
MISSISSIPPI
ALABAMA
GEORGIA
San Diego
Tucson
El Paso
Dallas
TEXAS
BAJA CALIFORNIA
SONORA
CHIHUAHUA
Austin
San Antonio
Houston
LOUISIANA
New Orleans
Jacksonville
Orlando
Tampa
FLORIDA
Miami
COAHUILA
NUEVO LEON
Gulf of California
Gulf of Mexico
BAJA CALIFORNIA SUR
SINALOA
DURANGO
TAMAULIPAS
Mexico
The Bahamas
Satellite
Google
Map data ©2017 Google, INEGI
Terms
Send feedback
200 km

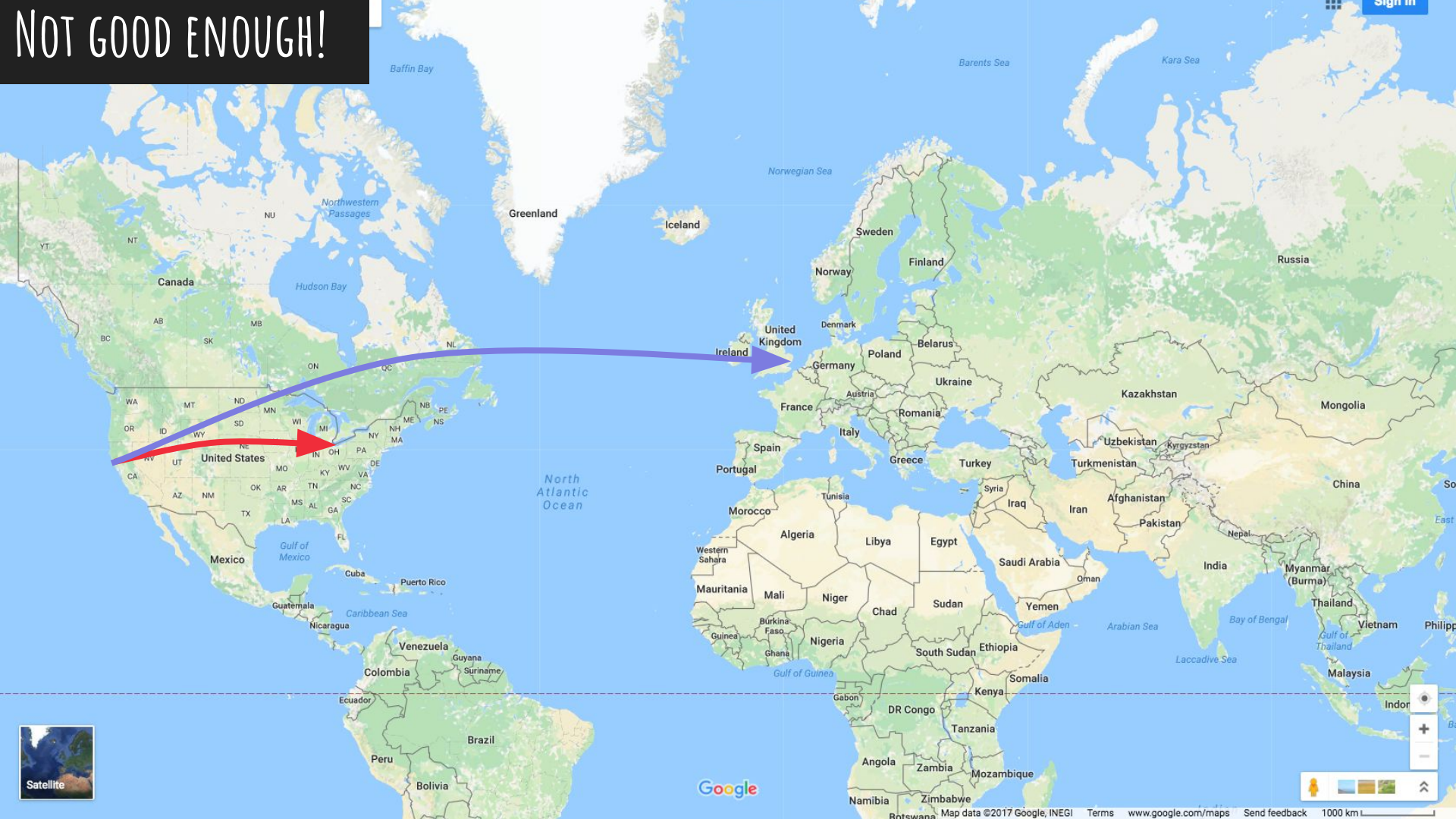

10MS
5G
United States
Mexico
Satellite
Google
Map data ©2017 Google, INEGI
Terms
Send feedback
200 km

And as the crow flies...

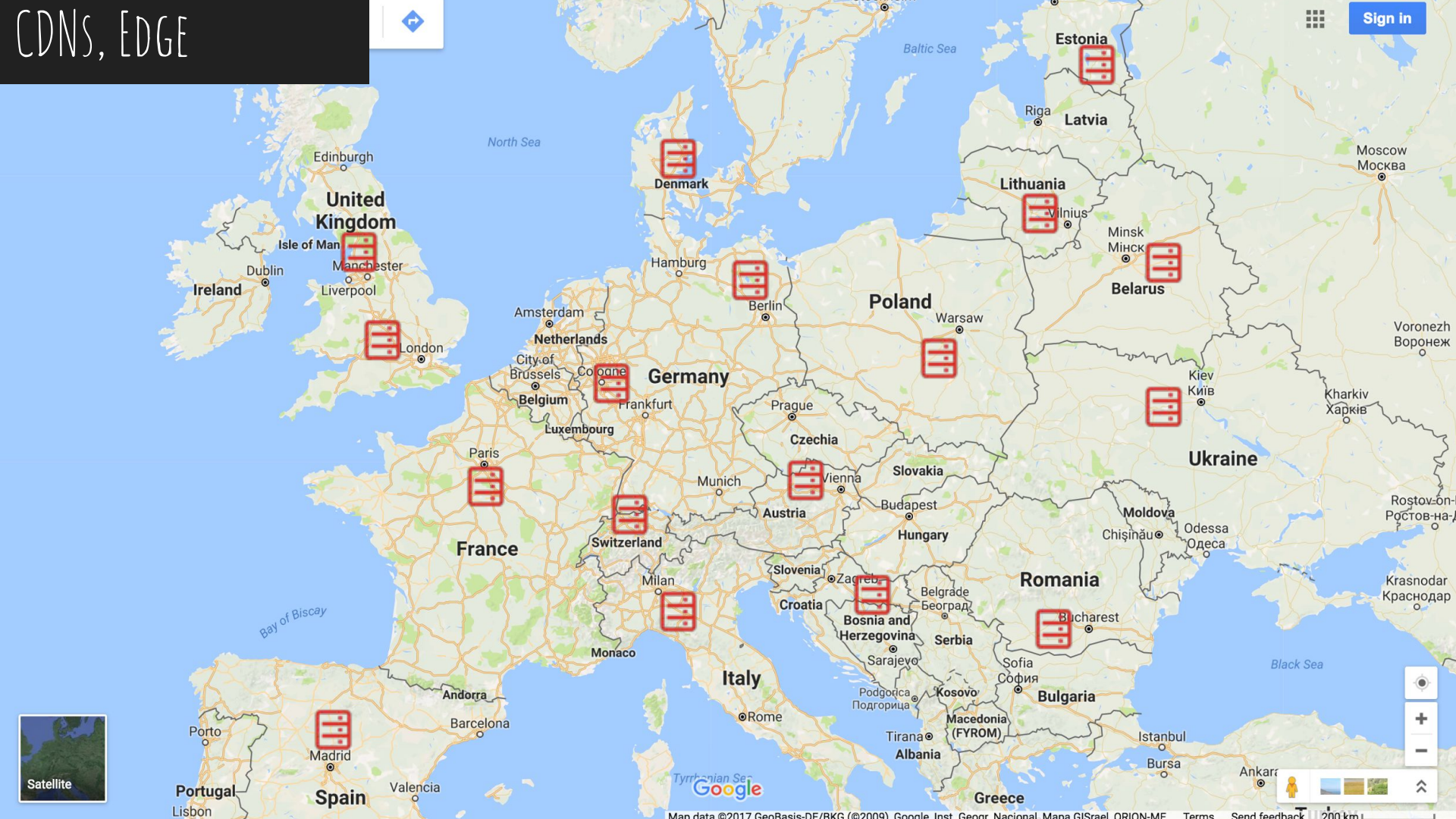
Hops

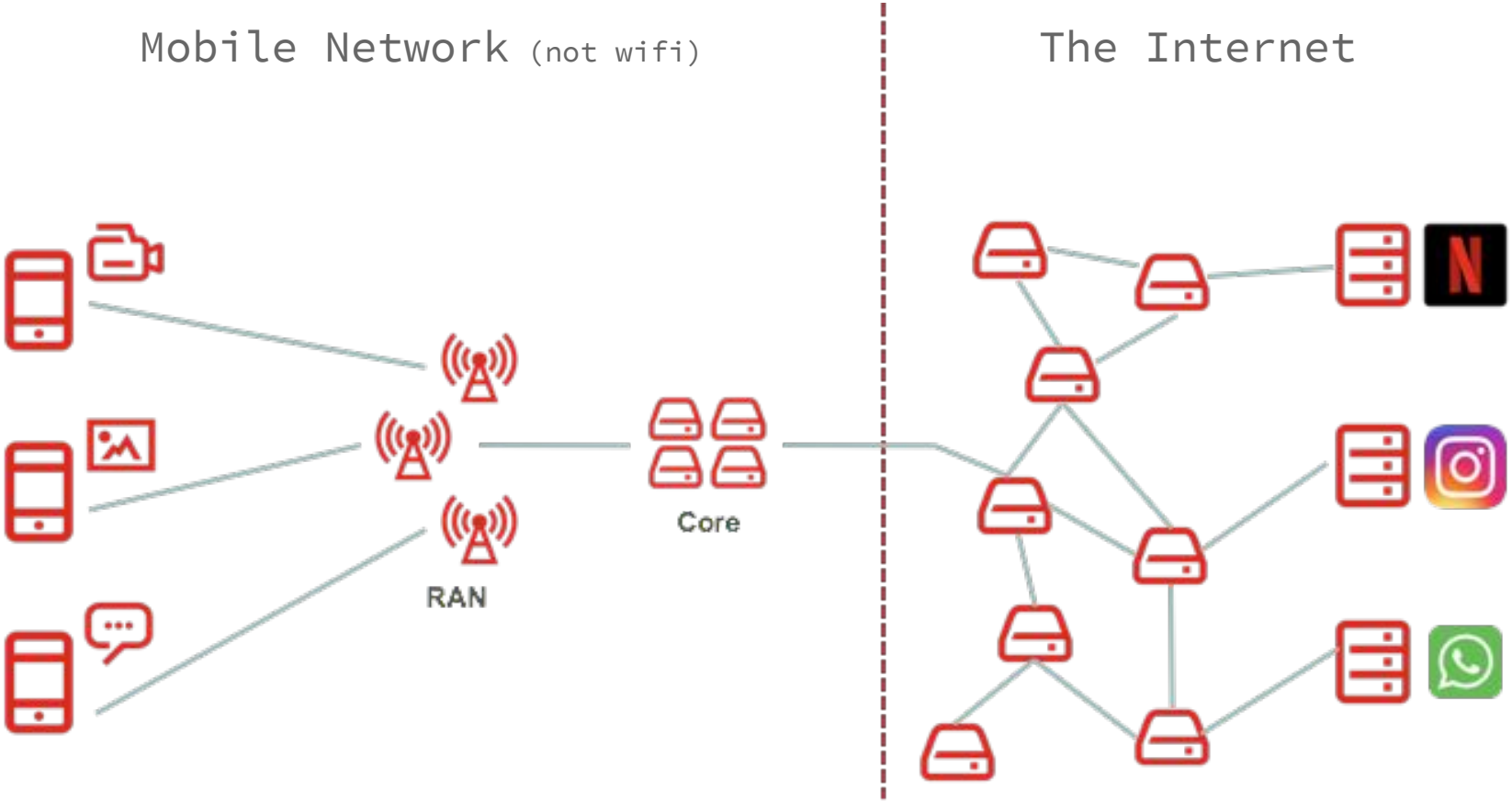

Ottawa
Montreal
VISCONSIN
MICHIGAN
Toronto
VT
NEW YORK
MA
CT RI
ILLINOIS
OHIO
PENN
INDIANA
Philadelphia
DE NJ
WEST
VIRGINIA
VIRGINIA
TENNESSEE
NORTH
CAROLINA
SOUTH
CAROLINA
ALABAMA
GEORGIA
Gulf of
Mexico

Not good enough!



CDNs, Edge


Sign in
Estonia
Baltic Sea
Riga
Latvia
North Sea
Edinburgh
Denmark
Lithuania
Moscow
Москва
United Kingdom
Isle of Man
Vilnius
Minsk
Минск
Hamburg
Dublin
Manchester
Ireland
Liverpool
Berlin
Belarus
Poland
Amsterdam
Warsaw
Netherlands
Voronezh
Воронеж
City of Brussels
Cologne
Germany
London
Kiev
Київ
Belgium
Frankfurt
Kharkiv
Харків
Prague
Luxembourg
Czechia
Paris
Ukraine
Munich
Vienna
Slovakia
Austria
Budapest
Moldova
Rostov-on-
Ростов-на-
Switzerland
Hungary
Chișinău
Odesa
Одеса
France
Slovenia
Zagreb
Milan
Romania
Krasnodar
Краснодар
Croatia
Belgrade
Београд
Bay of Biscay
Bucharest
Bosnia and Herzegovina
Serbia
Monaco
Sarajevo
Sofia
София
Black Sea
Italy
Andorra
Podgorica
Подгорица
Kosovo
Bulgaria
Barcelona
Rome
Macedonia (FYROM)
Porto
Tirana
Istanbul
Madrid
Albania
Bursa
Satellite
Portugal
Spain
Valencia
Tyrrhenian Sea
Ankara
Lisbon
Google
Greece
Map data ©2017 GeoBasis-DE/BKG (©2009), Google, Inst. Geogr. Nacional, Mapa GISrael, ORION-ME
Terms
Send feedback
200 km


Mobile Network (not wifi)
The Internet
RAN
Core

Amount of data

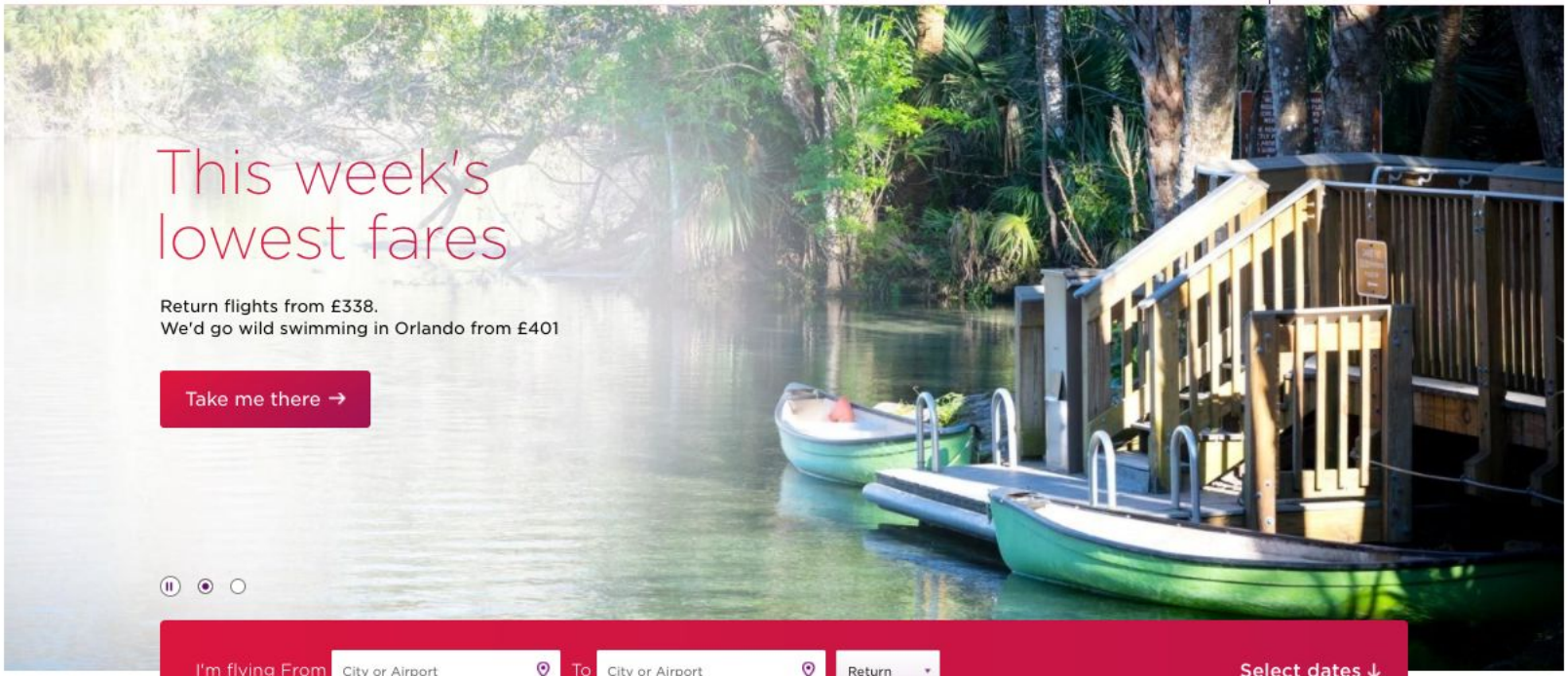
Book flights with Virgin Atlantic

www.virginatlantic.com

virgin atlantic

Book | My booking | Check in | Where we fly | Travel info | Experience

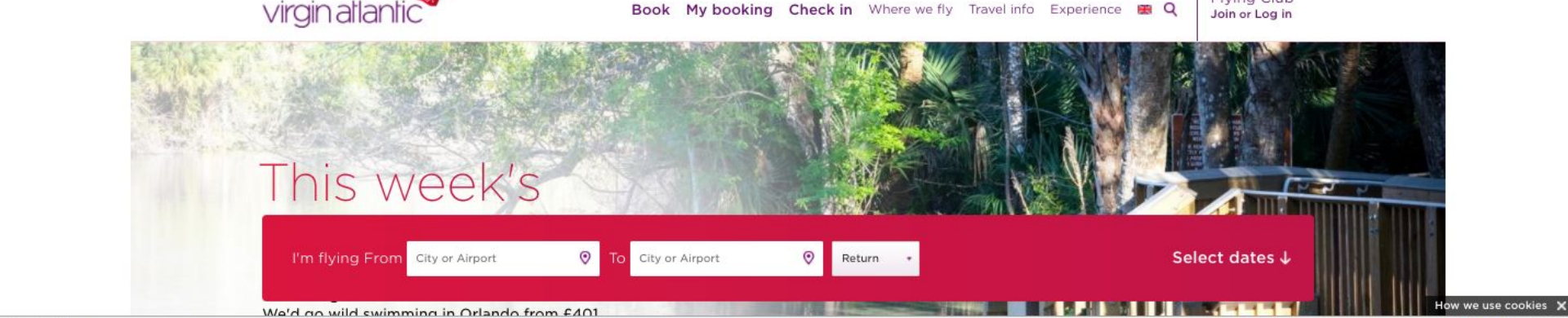
Flying Club
Join or Log in



I'm flying From City or Airport To City or Airport Return Select dates ↓

DESTINATIONS →

Get inspired



Elements | Console | Sources | Network | Performance | Memory | Application | Security | Audits

2 3

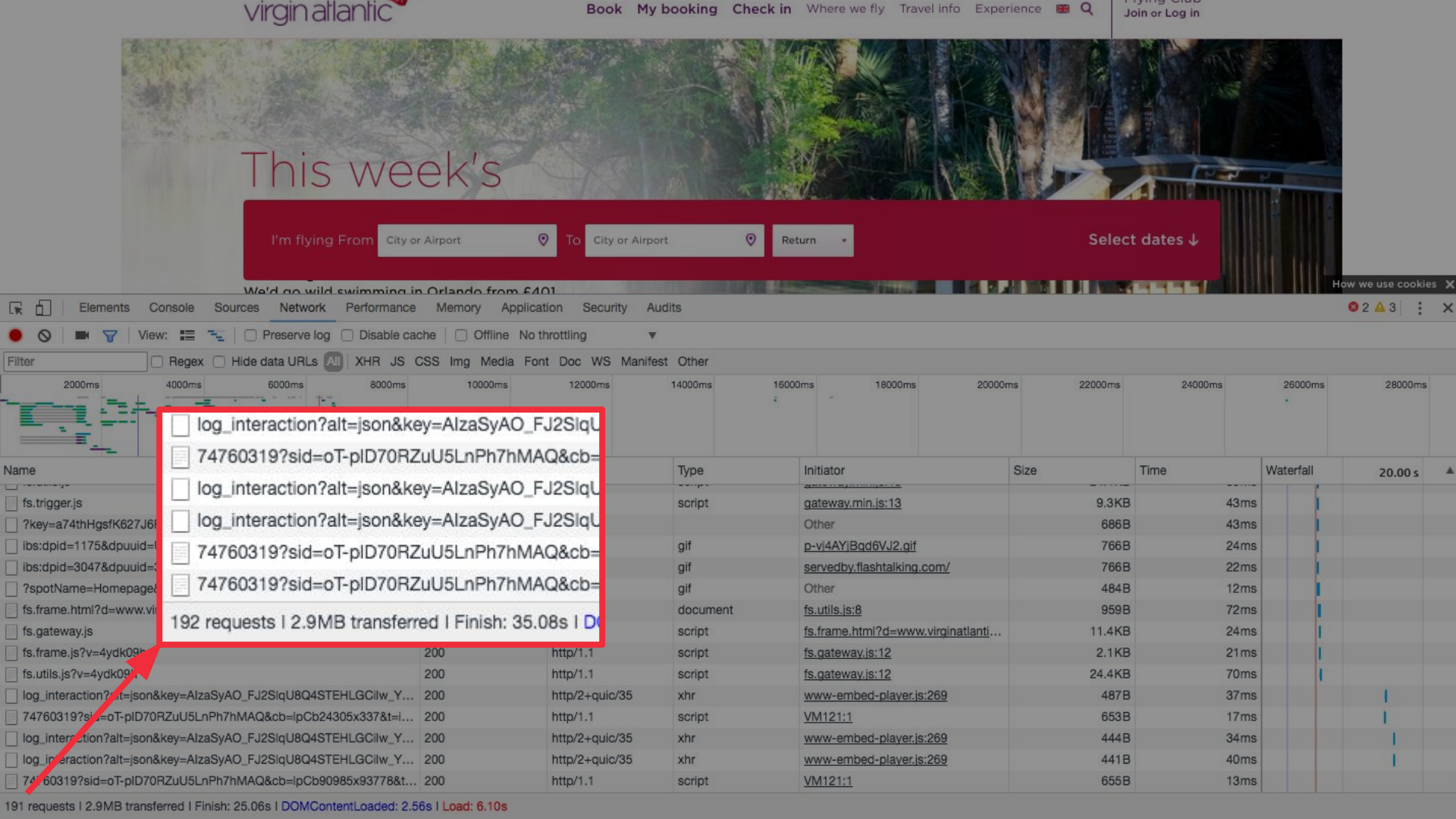
View: | Preserve log | Disable cache | Offline | No throttling

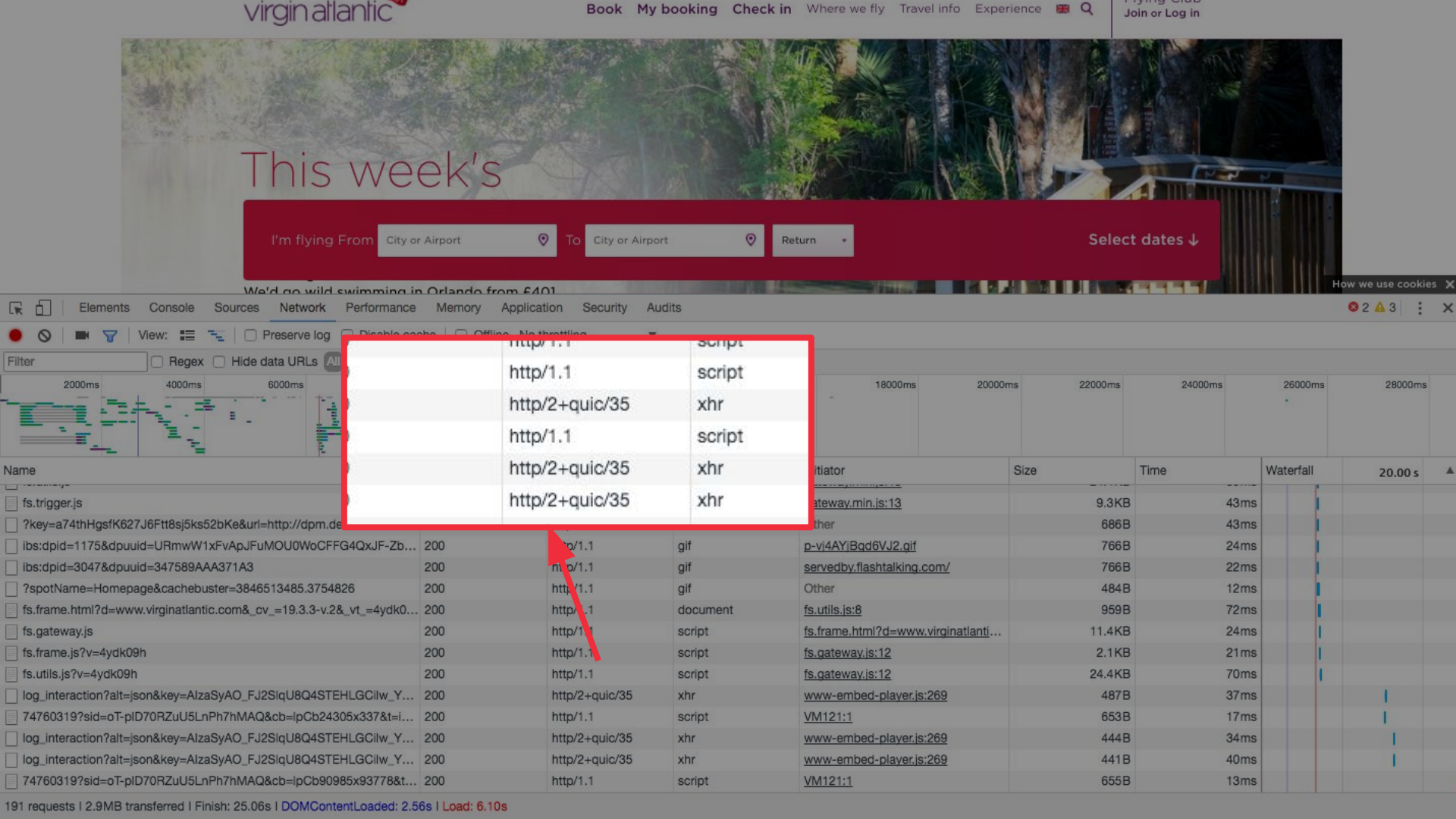
Filter | Regex | Hide data URLs | All | XHR | JS | CSS | Img | Media | Font | Doc | WS | Manifest | Other

2000ms 4000ms 6000ms 8000ms 10000ms 12000ms 14000ms 16000ms 18000ms 20000ms 22000ms 24000ms 26000ms 28000ms

Name	Status	Protocol	Type	Initiator	Size	Time	Waterfall 20.00 s
fs.trigger.js	200	http/1.1	script	gateway.min.js:13	9.3KB	43ms	
?key=a74thHgsfK627J6Ftt8sj5ks52bKe&url=http://dpm.demdex.net/i…	302	http/1.1		Other	686B	43ms	
ibs:dpid=1175&dpuuid=URmwW1xFvApJFuMOU0WoCFFG4QxJF-Zb…	200	http/1.1	gif	p-vj4AYjBqd6VJ2.gif	766B	24ms	
ibs:dpid=3047&dpuuid=347589AAA371A3	200	http/1.1	gif	servedby.flashtalking.com/	766B	22ms	
?spotName=Homepage&cachebuster=3846513485.3754826	200	http/1.1	gif	Other	484B	12ms	
fs.frame.html?d=www.virginatlantic.com&_cv_=19.3.3-v.2&_vt_=4ydk0…	200	http/1.1	document	fs.utils.js:8	959B	72ms	
fs.gateway.js	200	http/1.1	script	fs.frame.html?d=www.virginatlanti…	11.4KB	24ms	
fs.frame.js?v=4ydk09h	200	http/1.1	script	fs.gateway.js:12	2.1KB	21ms	
fs.utils.js?v=4ydk09h	200	http/1.1	script	fs.gateway.js:12	24.4KB	70ms	
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y…	200	http/2+quic/35	xhr	www-embed-player.js:269	487B	37ms	
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=lpCb24305x337&t=i…	200	http/1.1	script	VM121:1	653B	17ms	
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y…	200	http/2+quic/35	xhr	www-embed-player.js:269	444B	34ms	
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y…	200	http/2+quic/35	xhr	www-embed-player.js:269	441B	40ms	
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=lpCb90985x93778&t…	200	http/1.1	script	VM121:1	655B	13ms	

191 requests | 2.9MB transferred | Finish: 25.06s | DOMContentLoaded: 2.56s | Load: 6.10s


virgin atlantic
Book
My booking
Check in
Where we fly
Travel info
Experience
Join or Log in
This week's
I'm flying From
City or Airport
To
City or Airport
Return
Select dates
How we use cookies
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
Preserve log
Disable cache
Offline
No throttling
Filter
Regex
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
2000ms
4000ms
6000ms
8000ms
10000ms
12000ms
14000ms
16000ms
18000ms
20000ms
22000ms
24000ms
26000ms
28000ms
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=
192 requests | 2.9MB transferred | Finish: 35.08s | D
Name
Type
Initiator
Size
Time
Waterfall
20.00 s
fs.trigger.js
script
gateway.min.js:13
9.3KB
43ms
?key=a74thHgsfK627J6
Other
686B
43ms
ibs:dpid=1175&dpuuid=
gif
p-vj4AYjBqd6VJ2.gif
766B
24ms
ibs:dpid=3047&dpuuid=
gif
servedby.flashtalking.com/
766B
22ms
?spotName=Homepage
gif
Other
484B
12ms
fs.frame.html?d=www.vi
document
fs.utils.js:8
959B
72ms
fs.gateway.js
script
fs.frame.html?d=www.virginatlanti...
11.4KB
24ms
fs.frame.js?v=4ydk09
200
http/1.1
script
fs.gateway.js:12
2.1KB
21ms
fs.utils.js?v=4ydk09
200
http/1.1
script
fs.gateway.js:12
24.4KB
70ms
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y...
200
http/2+quic/35
xhr
www-embed-player.js:269
487B
37ms
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=lpCb24305x337&t=i...
200
http/1.1
script
VM121:1
653B
17ms
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y...
200
http/2+quic/35
xhr
www-embed-player.js:269
444B
34ms
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y...
200
http/2+quic/35
xhr
www-embed-player.js:269
441B
40ms
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=lpCb90985x93778&t...
200
http/1.1
script
VM121:1
655B
13ms
191 requests | 2.9MB transferred | Finish: 25.06s | DOMContentLoaded: 2.56s | Load: 6.10s


virgin atlantic
Book
My booking
Check in
Where we fly
Travel info
Experience
Join or Log in
This week's
I'm flying From
City or Airport
To
City or Airport
Return
Select dates
How we use cookies
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
Preserve log
Filter
Regex
Hide data URLs
2000ms
4000ms
6000ms
18000ms
20000ms
22000ms
24000ms
26000ms
28000ms
http/1.1 script
http/2+quic/35 xhr
http/1.1 script
http/2+quic/35 xhr
http/2+quic/35 xhr
Name
Initiator
Size
Time
Waterfall
20.00 s
fs.trigger.js
9.3KB
43ms
686B
43ms
ibs:dpid=1175&dpuuid=URmwW1xFvApJFuMOU0WoCFFG4QxJF-Zb... 200 gif p-vj4AYjBqd6VJ2.gif 766B 24ms
ibs:dpid=3047&dpuuid=347589AAA371A3 200 gif servedby.flashtalking.com/ 766B 22ms
?spotName=Homepage&cachebuster=3846513485.3754826 200 gif Other 484B 12ms
fs.frame.html?d=www.virginatlantic.com&_cv_=19.3.3-v.2&_vt_=4ydk0... 200 document fs.utils.js:8 959B 72ms
fs.gateway.js 200 script fs.frame.html?d=www.virginatlanti... 11.4KB 24ms
fs.frame.js?v=4ydk09h 200 script fs.gateway.js:12 2.1KB 21ms
fs.utils.js?v=4ydk09h 200 http/1.1 script fs.gateway.js:12 24.4KB 70ms
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y... 200 http/2+quic/35 xhr www-embed-player.js:269 487B 37ms
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=lpCb24305x337&t=i... 200 http/1.1 script VM121:1 653B 17ms
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y... 200 http/2+quic/35 xhr www-embed-player.js:269 444B 34ms
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y... 200 http/2+quic/35 xhr www-embed-player.js:269 441B 40ms
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=lpCb90985x93778&t... 200 http/1.1 script VM121:1 655B 13ms
191 requests | 2.9MB transferred | Finish: 25.06s | DOMContentLoaded: 2.56s | Load: 6.10s

Speed & Distance

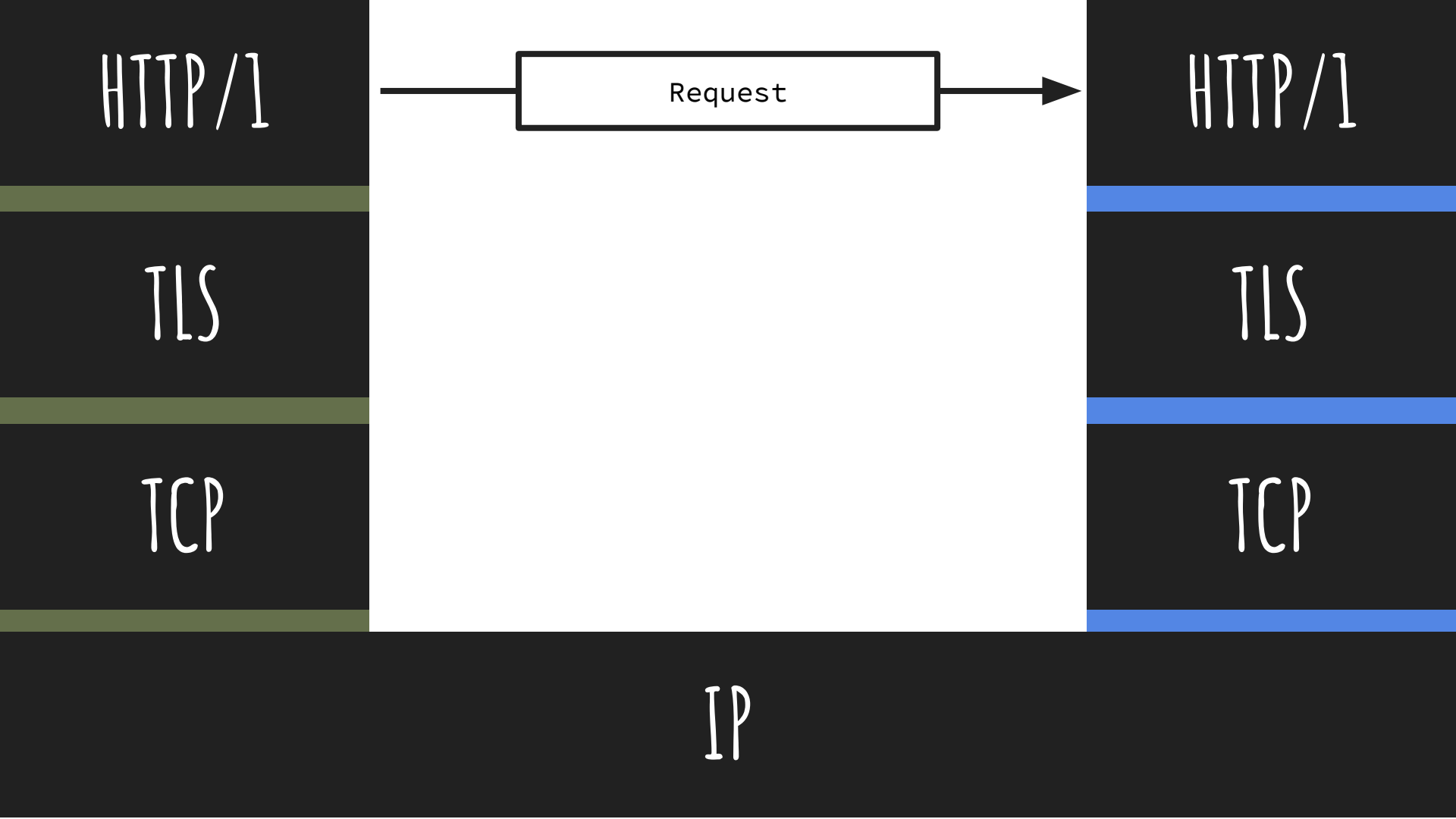
Capped by Speed of Light

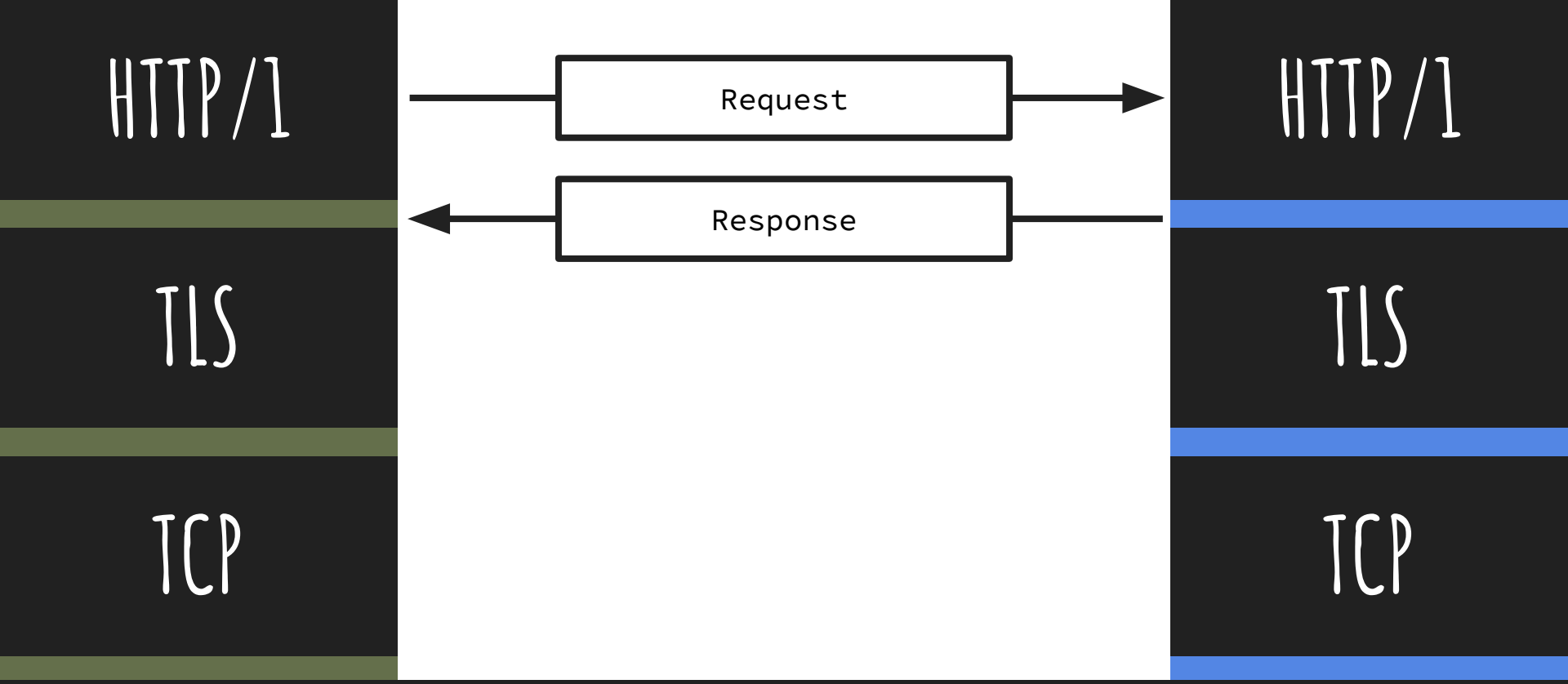
Amount of Data

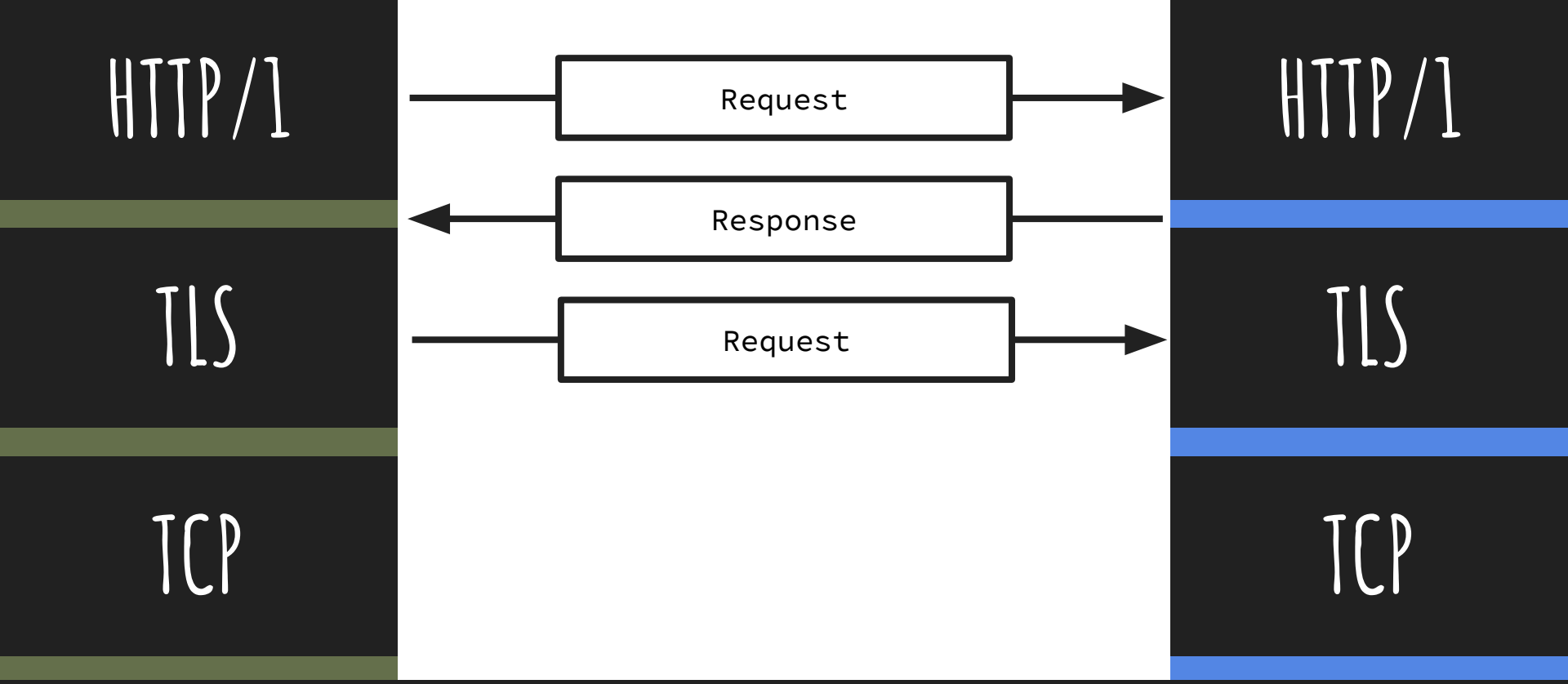
>100 objects per site
800k to 2.5mb data
>50 resources on same domain

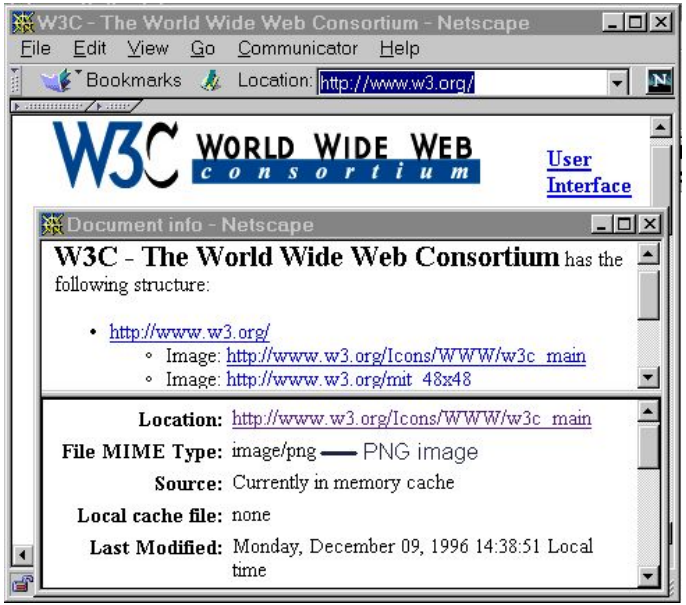
Mostly because of physics. Not much you can do about that.

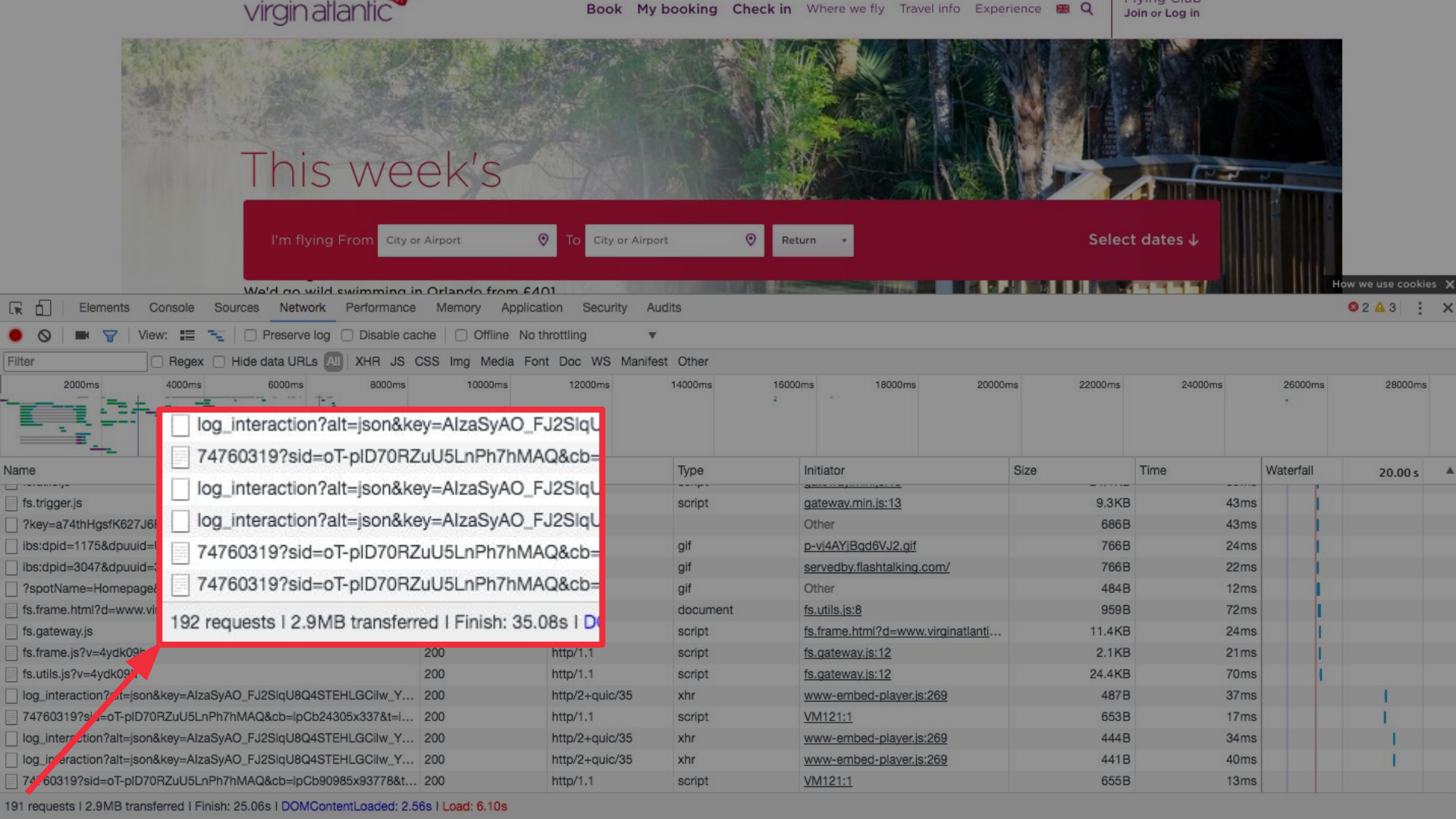
HTTP/1


HTTP/1
Request
HTTP/1
TLS
TLS
TCP
TCP
IP

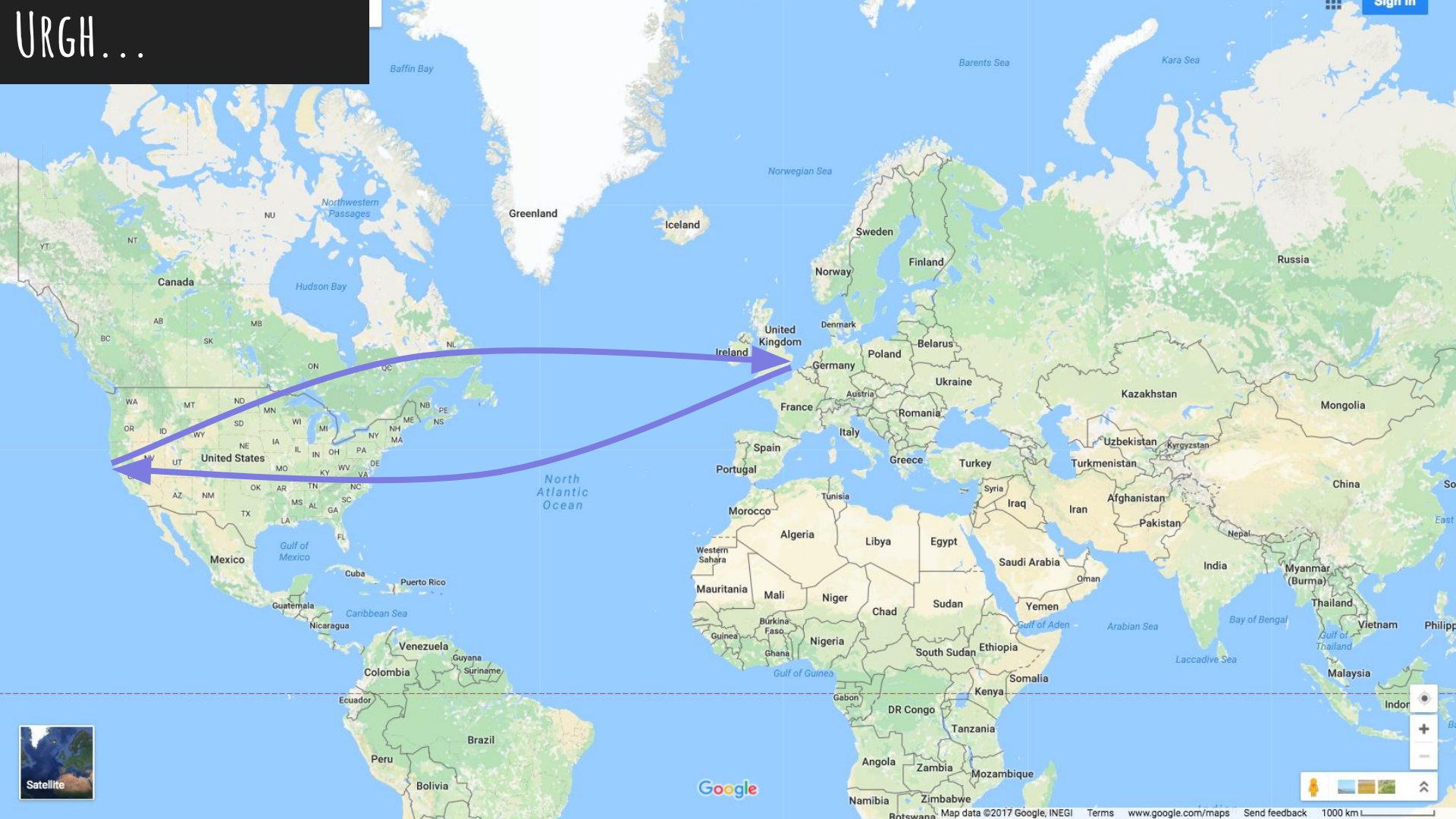

HTTP/1
Request
HTTP/1
Response
TLS
TLS
TCP
TCP
IP


HTTP/1
TLS
TCP
Request
Response
Request
HTTP/1
TLS
TCP
IP


W3C - The World Wide Web Consortium - Netscape
File Edit View Go Communicator Help
Bookmarks Location: http://www.w3.org/
WORLD WIDE WEB
consortium
User Interface
Document info - Netscape
W3C - The World Wide Web Consortium has the following structure:
http://www.w3.org/
Image: http://www.w3.org/Icons/WWW/w3c_main
Image: http://www.w3.org/mit_48x48
Location: http://www.w3.org/Icons/WWW/w3c_main
File MIME Type: image/png — PNG image
Source: Currently in memory cache
Local cache file: none
Last Modified: Monday, December 09, 1996 14:38:51 Local time


virgin atlantic
Book
My booking
Check in
Where we fly
Travel info
Experience
Join or Log in
This week's
I'm flying From
City or Airport
To
City or Airport
Return
Select dates
How we use cookies
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
Preserve log
Disable cache
Offline
No throttling
Filter
Regex
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
2000ms
4000ms
6000ms
8000ms
10000ms
12000ms
14000ms
16000ms
18000ms
20000ms
22000ms
24000ms
26000ms
28000ms
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=
192 requests | 2.9MB transferred | Finish: 35.08s | D
Name
Type
Initiator
Size
Time
Waterfall
20.00 s
fs.trigger.js
script
gateway.min.js:13
9.3KB
43ms
?key=a74thHgsfK627J6
Other
686B
43ms
ibs:dpid=1175&dpuuid=
gif
p-vj4AYjBqd6VJ2.gif
766B
24ms
ibs:dpid=3047&dpuuid=
gif
servedby.flashtalking.com/
766B
22ms
?spotName=Homepage
gif
Other
484B
12ms
fs.frame.html?d=www.vi
document
fs.utils.js:8
959B
72ms
fs.gateway.js
script
fs.frame.html?d=www.virginatlanti...
11.4KB
24ms
fs.frame.js?v=4ydk09
200
http/1.1
script
fs.gateway.js:12
2.1KB
21ms
fs.utils.js?v=4ydk09
200
http/1.1
script
fs.gateway.js:12
24.4KB
70ms
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y...
200
http/2+quic/35
xhr
www-embed-player.js:269
487B
37ms
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=lpCb24305x337&t=i...
200
http/1.1
script
VM121:1
653B
17ms
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y...
200
http/2+quic/35
xhr
www-embed-player.js:269
444B
34ms
log_interaction?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y...
200
http/2+quic/35
xhr
www-embed-player.js:269
441B
40ms
74760319?sid=oT-pID70RZuU5LnPh7hMAQ&cb=lpCb90985x93778&t...
200
http/1.1
script
VM121:1
655B
13ms
191 requests | 2.9MB transferred | Finish: 25.06s | DOMContentLoaded: 2.56s | Load: 6.10s

URGH...


Baffin Bay
Barents Sea
Kara Sea
Norwegian Sea
Greenland
Iceland
Northwestern Passages
Hudson Bay
Canada
Sweden
Finland
Norway
Russia
United Kingdom
Ireland
Denmark
Germany
Poland
Belarus
Ukraine
France
Austria
Romania
Kazakhstan
Mongolia
Italy
Spain
Portugal
Greece
Turkey
Uzbekistan
Kyrgyzstan
Turkmenistan
China
Syria
Iraq
Iran
Afghanistan
Pakistan
Nepal
India
Myanmar (Burma)
Thailand
Vietnam
Philipp
Tunisia
Morocco
Algeria
Libya
Egypt
Western Sahara
Saudi Arabia
Oman
Yemen
Mauritania
Mali
Niger
Chad
Sudan
Burkina Faso
Guinea
Nigeria
Ghana
South Sudan
Ethiopia
Somalia
Kenya
Gabon
DR Congo
Tanzania
Angola
Zambia
Mozambique
Namibia
Zimbabwe
Botswana
United States
Mexico
Gulf of Mexico
Cuba
Puerto Rico
Guatemala
Nicaragua
Caribbean Sea
Venezuela
Guyana
Suriname
Colombia
Ecuador
Brazil
Peru
Bolivia
North Atlantic Ocean
Gulf of Aden
Arabian Sea
Bay of Bengal
Laccadive Sea
Gulf of Guinea
Gulf of Thailand
Malaysia
Satellite
Google
Map data ©2017 Google, INEGI
Terms
www.google.com/maps
Send feedback
1000 km

Spriting


Chip's Challenge Tiles
ripped by Lotos.
Different palettes (found in help)

Inlining


```
<!DOCTYPE html>
<html lang="en">
    <head>
        <title>threejs webgl - inline tone mapping</title>
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width, user-scalable=no, minimum-scale=1.0,
        <style>
            body {
                color: #fff;
                font-family:Monospace;
                font-size:13px;
                text-align:center;

                background-color: #000;

                margin: 0px;
                overflow: hidden;
            }

            a { color: #ff2 }

            #info {
                position: absolute;
                top: 0px; width: 100%;
                padding: 5px;
            }
        </style>
    </head>
    <body>

        <div id="container"></div>
        <div id="info"><a href="http://threejs.org" target="_blank" rel="noopener">threejs</a>
processing step or float/half buffers by <a href="http://clara.io/" target="_blank" rel="nooper

        <script src="../build/three.js"></script>
        <script src="js/controls/OrbitControls.js"></script>

        <script src="js/Detector.js"></script>
        <script src="js/libs/stats.min.js"></script>

        <script src="js/libs/dat.gui.min.js"></script>
        <script src="js/loaders/RGBELoader.js"></script>
        <script src="js/loaders/HDRCubeTextureLoader.js"></script>
        <script src="js/pmrem/PMREMGenerator.js"></script>
        <script src="js/pmrem/PMREMCubeUVPacker.js"></script>

        <script src="js/postprocessing/EffectComposer.js"></script>
        <script src="js/postprocessing/RenderPass.js"></script>
        <script src="js/postprocessing/MaskPass.js"></script>
        <script src="js/postprocessing/ShaderPass.js"></script>
        <script src="js/shaders/CopyShader.js"></script>

        <script>

            if ( ! Detector.webgl ) Detector.addGetWebGLMessage();
```


ember install ember-service-worker
TRIFORK
IBM
betfair

W3C Working Draft

TABLE OF CONTENTS

Service Workers 1

W3C Working Draft, 2 November 2017

This version:
https://www.w3.org/TR/2017/WD-service-workers-1-20171102/

Latest published version:
https://www.w3.org/TR/service-workers-1/

Editor's Draft:
https://w3c.github.io/ServiceWorker/v1/

Previous Versions:
https://www.w3.org/TR/2016/WD-service-workers-1-20161011/

Issue Tracking:
GitHub
Inline In Spec

Editors:
Alex Russell (Google)
Jungkee Song (Samsung Electronics)
Jake Archibald (Google)
Marijn Kruisselbrink (Google)

Tests:
web-platform-tests service-workers/ (ongoing work)

▶ V1 Branch

Have a Service Worker?

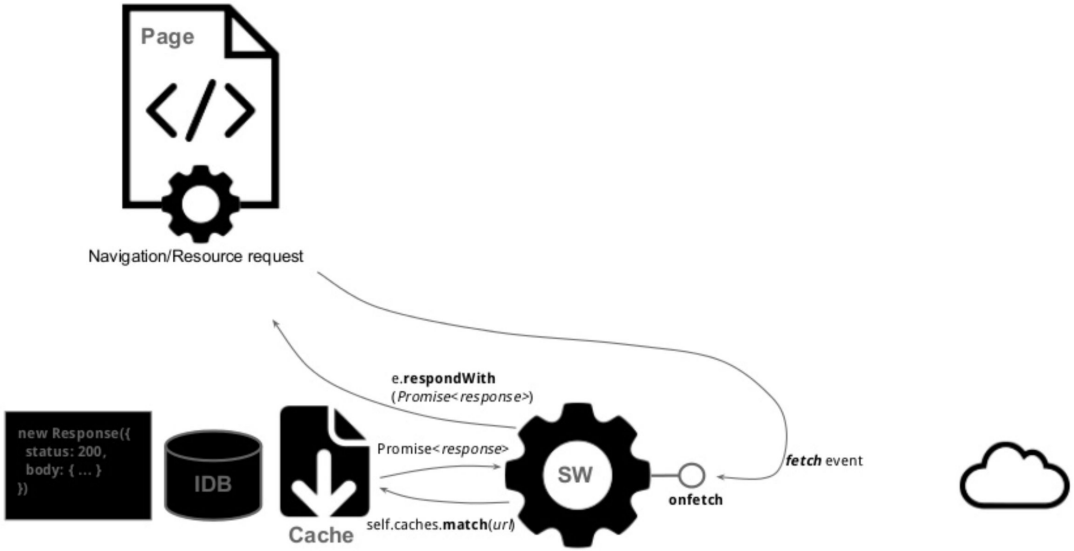


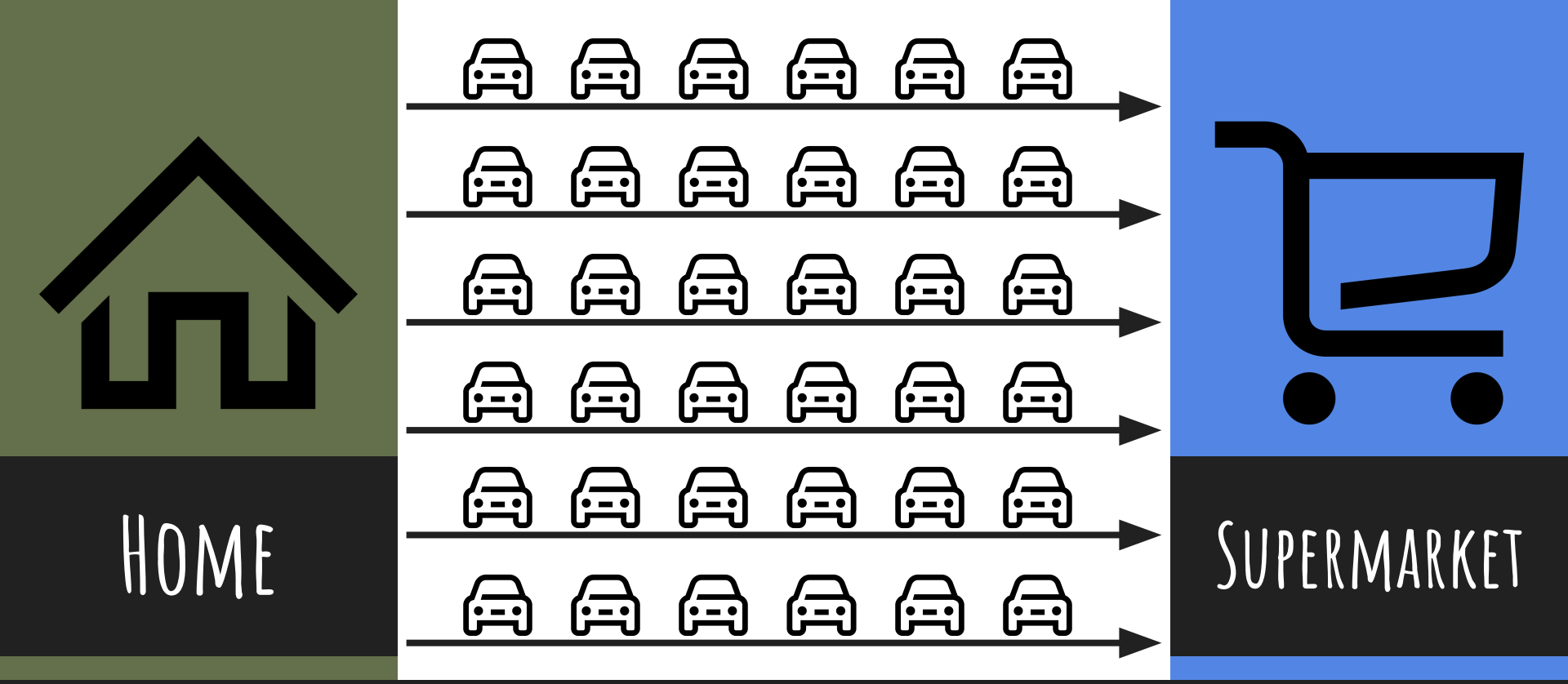
Image source: @jungkees

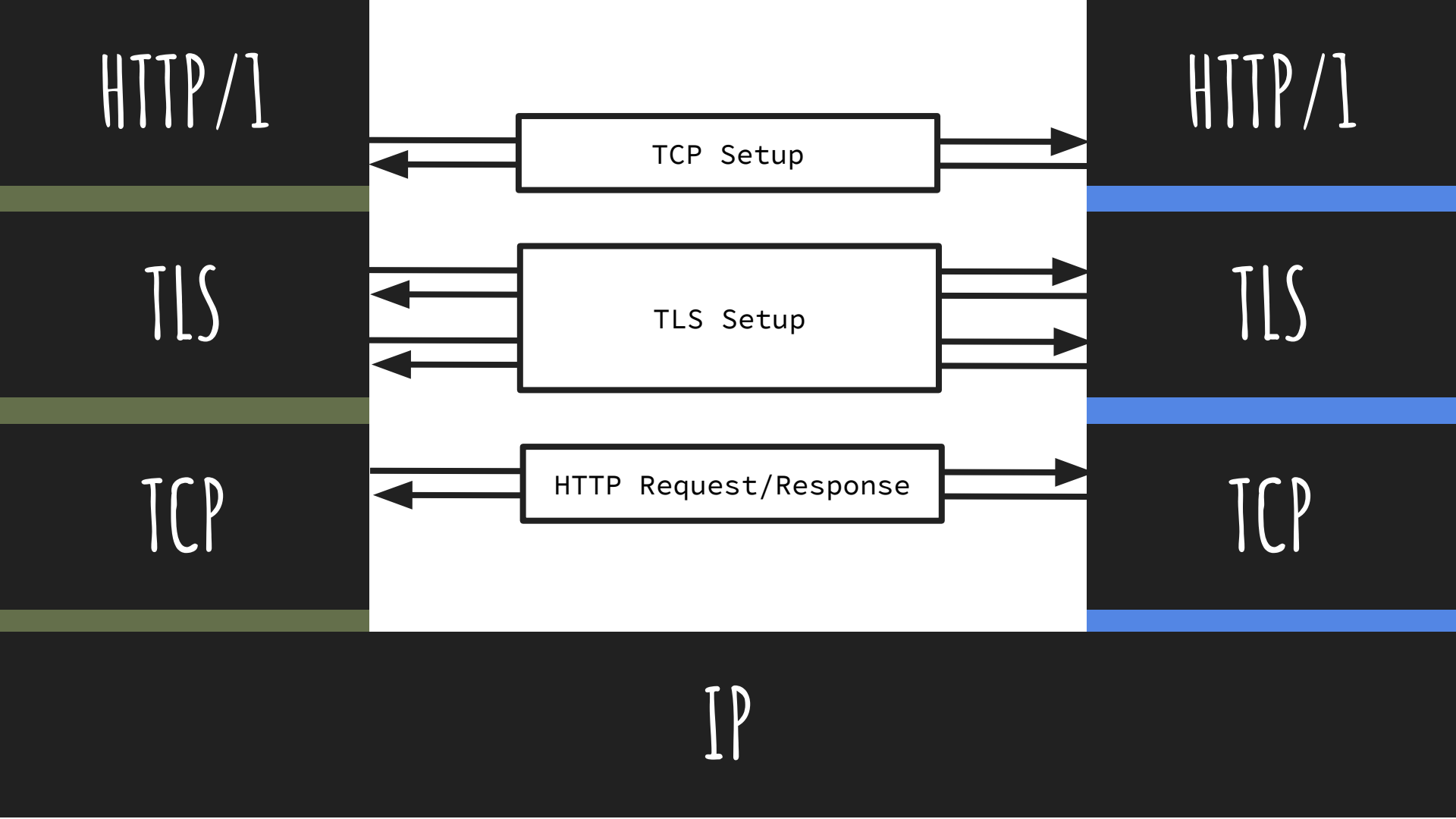
Pipelining

Home

Supermarket

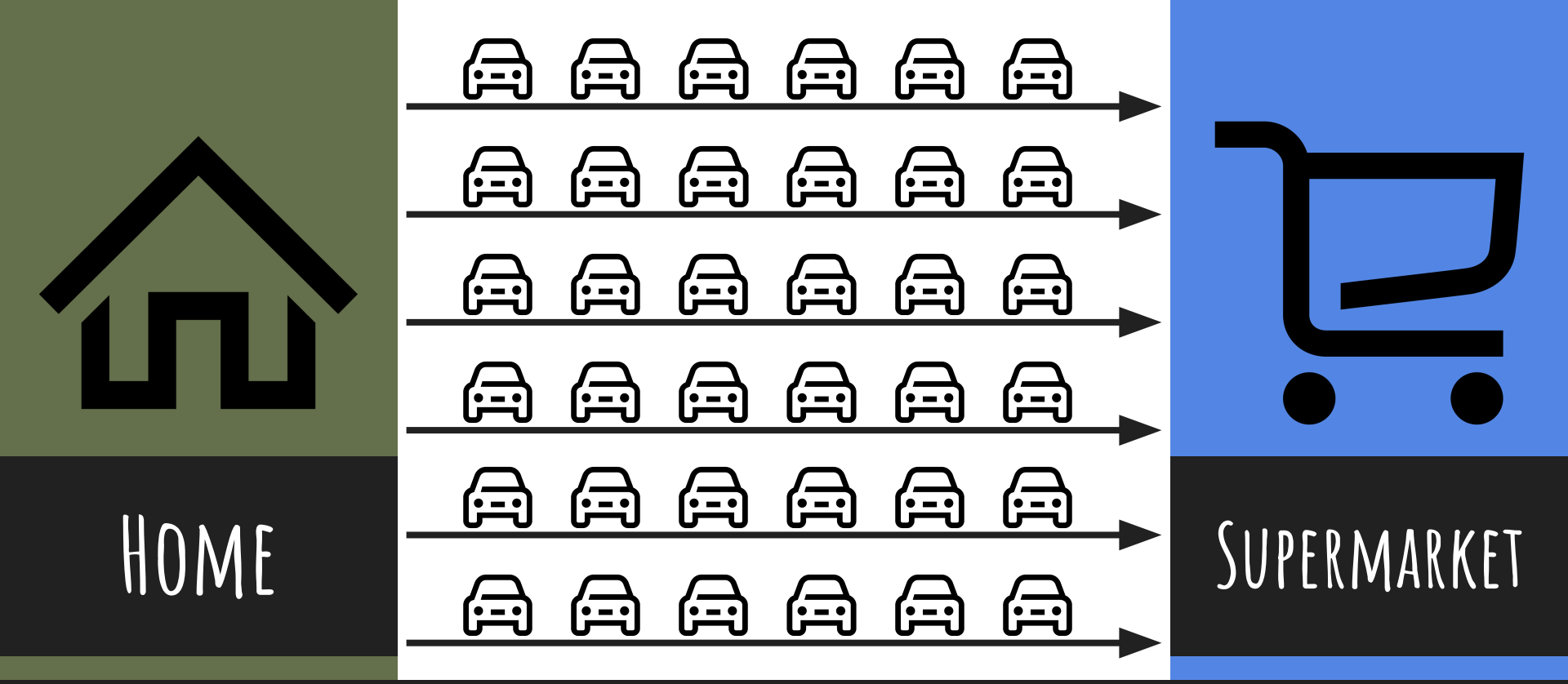
Roads


Home
Supermarket
Roads


HTTP/1
TLS
TCP
TCP Setup
TLS Setup
HTTP Request/Response
HTTP/1
TLS
TCP
IP

HTTP/2

SPDY


Home
Supermarket
Roads

Home

Supermarket

Roads

SPDY

A Protocol by Google

2009

Header Compression

Parallel Connections

Multiplexing

Priority Marking

Server Push

TLS (to work)

SPDY

A Protocol by Google

The Internet Engineering Task Force (IETF®)

The goal of the IETF is to make the Internet work better.

The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. Newcomers to the IETF should start here.

News

- IETF 104 in Prague!
- IETF Blog
- IETF Daily Dose

Next Meeting: IETF 99 Prague, Czech Republic

IETF 99, Prague, Czech Republic (UTC +2)
July 16-21, 2017

- Register
- Important Dates
- Wiki
- Agenda
- Meeting Materials
- Remote Participation
- Hackathon (open to public)

Email Archives

A new mail archive tool realizing the requirements developed in RFC 6778 is now in use:

- Search all IETF email archives

If you choose to log in, use your datatracker credentials.

(Read full announcement in the archives here.)

Recent Meeting: IETF 98 - Chicago, IL

- IETF 98 Information
- IETF 98 Proceedings

Internet-Drafts and RFCs Quick Search

Search

TECHNICAL REPORTS

By date

By group

WEB AND INDUSTRY

Automotive

Publishing

Entertainment (TV and Broadcasting)

Web and Telecommunications

Web of Data

Web of Things

Web Payments

Web Security

WEB FOR ALL

Accessibility

Internationalization

W3C A to Z

W3C Announces its First Publishing Summit and New Publishing Standards Work

19 June 2017 | Archive

PUBLISHING@W3C

W3C opened today registration for its first ever W3C Publishing Summit to be held 9-10 November 2017 in San Francisco, California, co-located with the W3C's Technical Plenary and Advisory Committee meetings (TPAC 2017), and calls for speakers by 15 July 2017. The inaugural W3C Publishing Summit will show how publishers are using today's Web technologies to make publications more effective and workflows more efficient.

W3C launched last week its new Publishing Working Group, just a few months following the combination of IDPF and W3C, with a mission to provide the necessary technologies on the Open Web Platform to make the combination of traditional publishing and the Web complete in terms of accessibility, usability, portability, distribution, archiving, offline access, and reliable cross referencing.

Read the Media Advisory and Blog post to learn about the event and major milestones for Publishing at W3C.

W3C Invites Implementations of HTML 5.1 2nd Edition

20 June 2017 | Archive

First Public Working Draft: CSS Overflow Module Level 4

13 June 2017 | Archive

XSL Transformations (XSLT) Version 3.0 is now a W3C Recommendation

8 June 2017 | Archive

Skip

The World Wide Web Consortium (W3C) is an international community that develops open standards to ensure the long-term growth of the Web.
W3C operates under our Code of Ethics and Professional Conduct.
Become a Friend of W3C to support the W3C mission and free developer tools.

W3C BLOG

Bringing Publications to the Web: First Steps
29 June 2017 by Tzviya Siegman

Possible future directions for data on the Web
27 June 2017 by Phil Archer

Tim Berners-Lee awarded 2016 ACM A.M. Turing Prize
22 June 2017 by Coralie Mercier

JOBS

Open position for a Web Accessibility Engineer (China)

VALIDATORS, MORE SOFTWARE

The Internet Engineering Task Force (IETF®)

The goal of the IETF is to make the Internet work better.

The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. Newcomers to the IETF should start here.

News

- IETF 104 in Prague!
- IETF Blog
- IETF Daily Dose

Next Meeting: IETF 99 Prague, Czech Republic

IETF 99, Prague, Czech Republic (UTC +2)
July 16-21, 2017

- Register
- Important Dates
- Wiki
- Agenda
- Meeting Materials
- Remote Participation
- Hackathon (open to public)

Email Archives

A new mail archive tool realizing the requirements developed in RFC 6778 is now in use:

- Search all IETF email archives

If you choose to log in, use your datatracker credentials.

(Read full announcement in the archives here.)

Recent Meeting: IETF 98 - Chicago, IL

- IETF 98 Information
- IETF 98 Proceedings

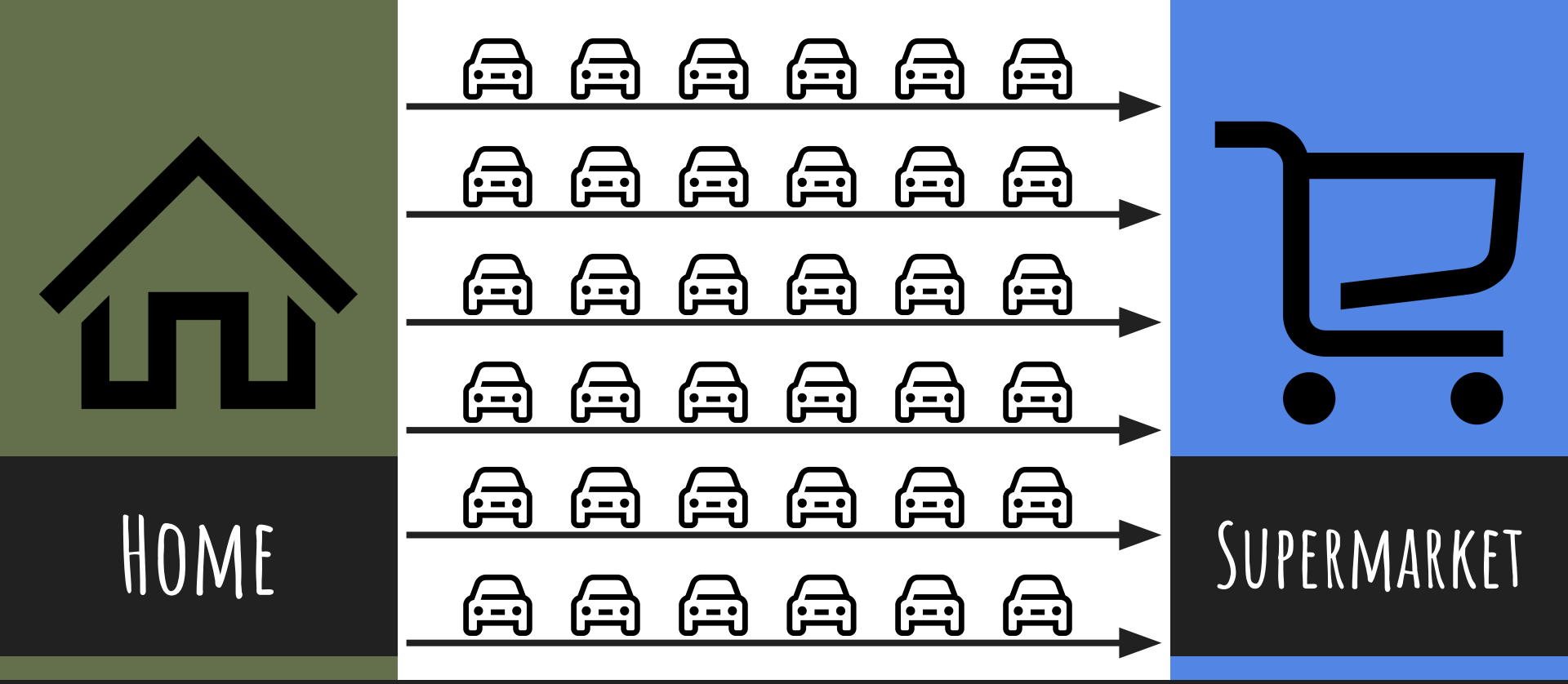
Internet-Drafts and RFCs Quick Search

Search

HTTP/2

“Idea was to maintain HTTP semantics but change how it is transported.”

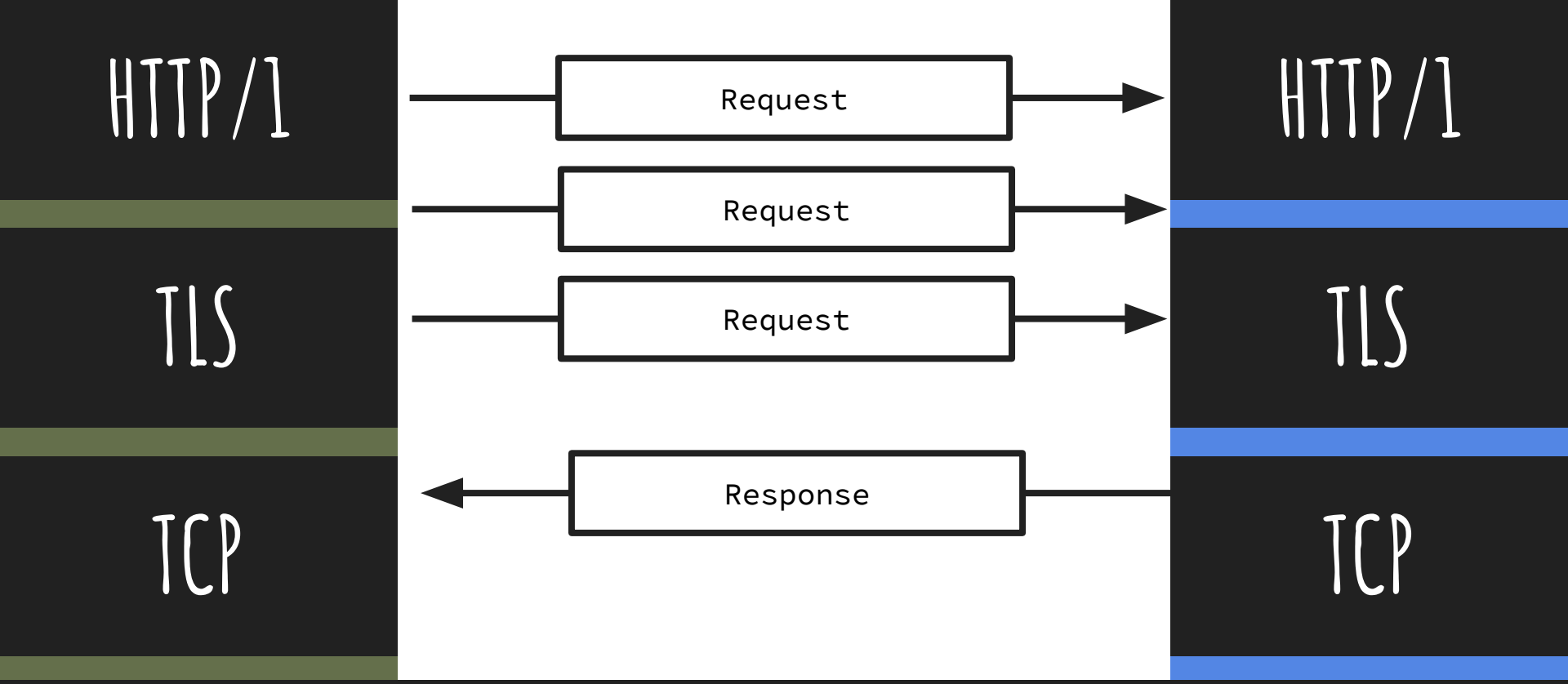
Daniel Stenberg
https://daniel.haxx.se/blog/


Home
Supermarket
Roads

Home

Supermarket

Roads


HTTP/1
TLS
TCP
Request
Request
Request
Response
HTTP/1
TLS
TCP
IP

HTTP2

A Protocol by IETF
(SDPY base)

Binary

Header Compression

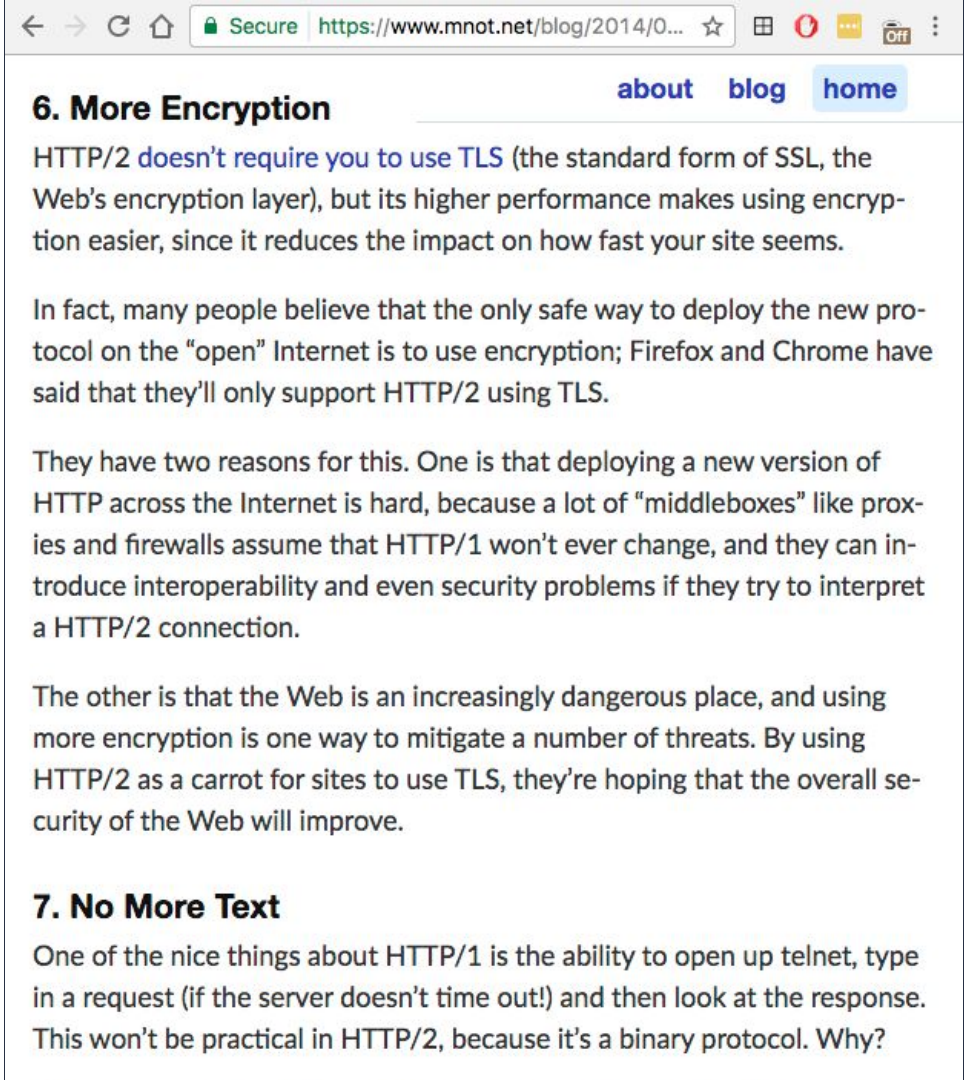
Multiplexing

Server Push

TLS...

HTTP2

A Protocol by IETF
(SDPY base)



@thisNatasha

Stats

Gimme gimme

35% Requests

70% HTTPS Connections

13% Top 1,000,000 Sites

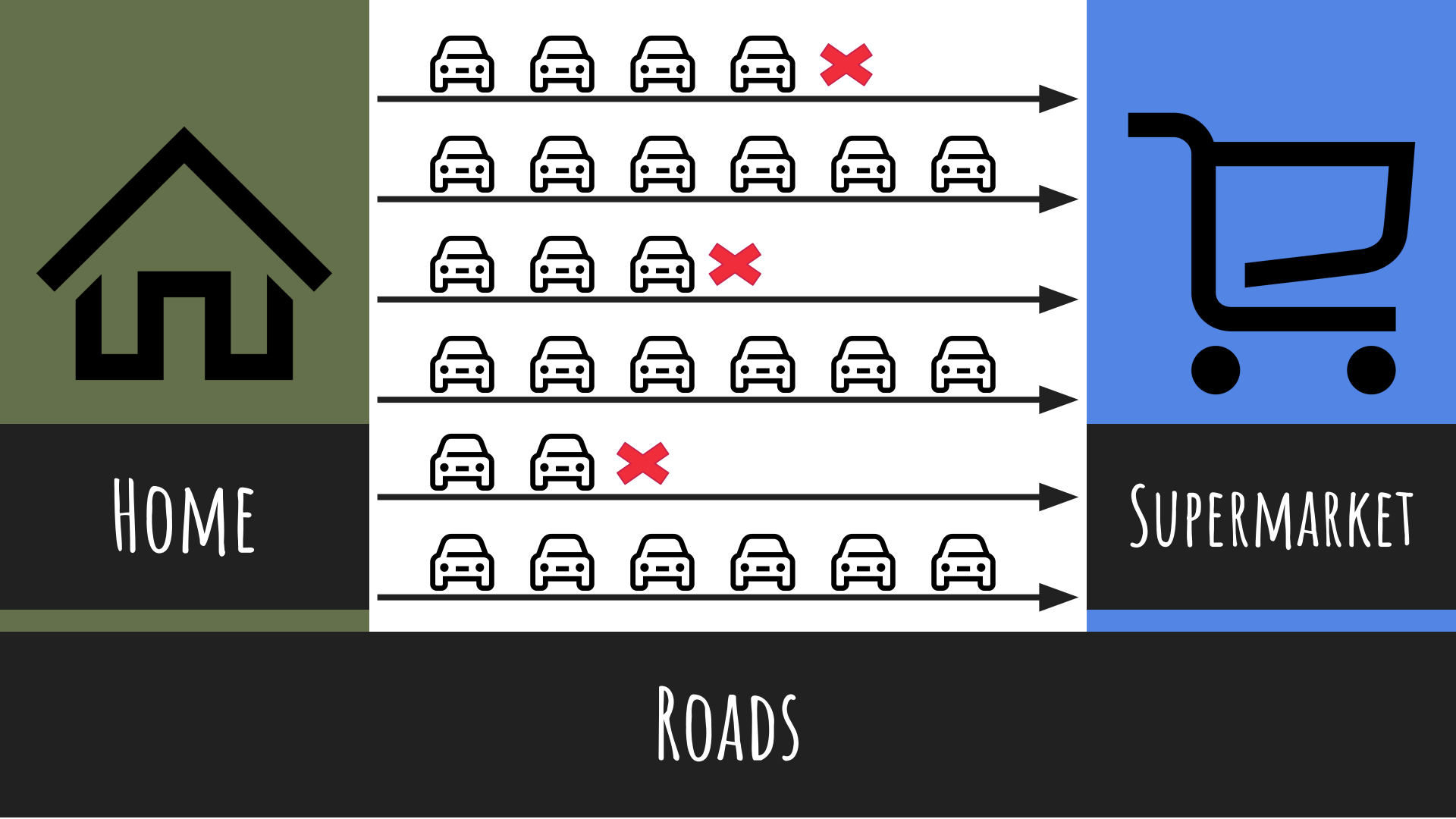
29% Top 1000 Sites

“90% your site”

2% PACKET LOSS

HTTP1 is better.

Head of line blocking


Home
Supermarket
Roads

Home

Supermarket

Roads

Not good enough!

Home

Supermarket

Roads

Not good enough!

Home

Supermarket

Roads

(Can happen on any protocol with in-order delivery)

QUIC

“Idea was to maintain HTTP semantics but change how it is transported.”

Daniel Stenberg
https://daniel.haxx.se/blog/

TCP

HOME

SUPERMARKET

ROADS

Transport Layer

TCP

Suffers from
Head of Line Blocking

UDP

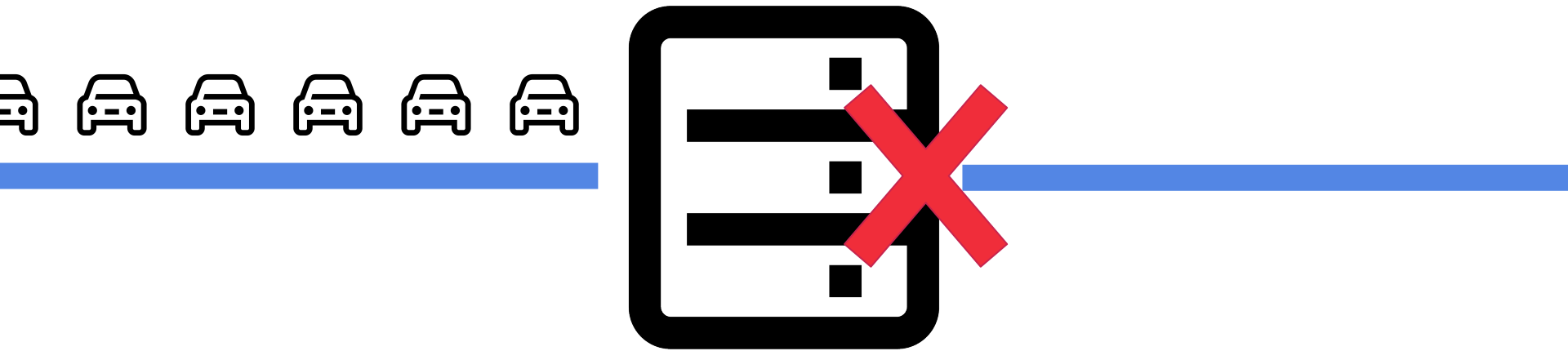
Can work...with help.

“We want QUIC to work on today’s internet”

Jana Iyengar
QUIC Editor, Google

Ossification

Why TCP or UDP only?



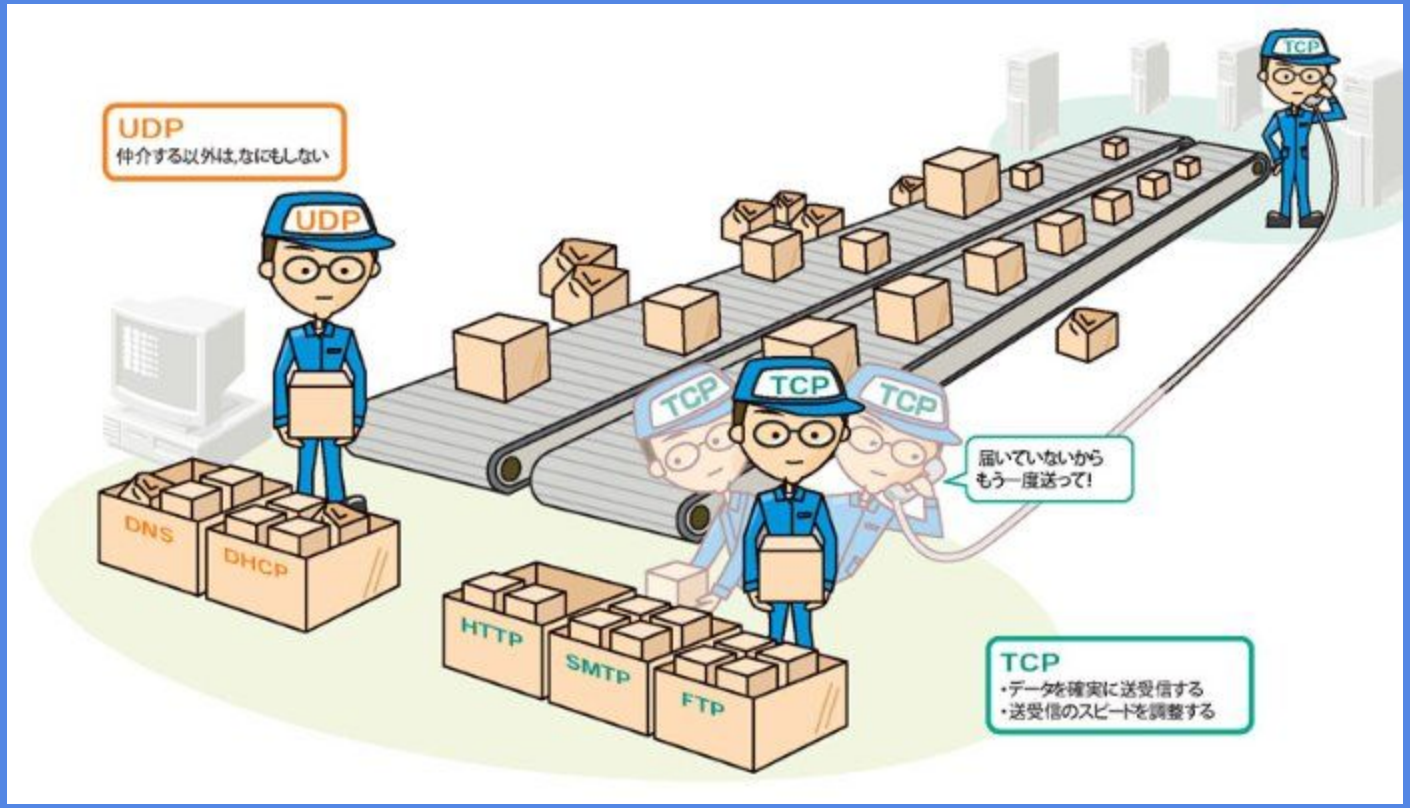


Image source: http://itpro.nikkeibp.co.jp/


HTTP/2
TLS 1.2+
TCP
Congestion Control
Application
QUIC
Google Crypto
UDP
IP

HTTP/2

TLS 1.2+

TCP

Congestion Control

Application

QUIC

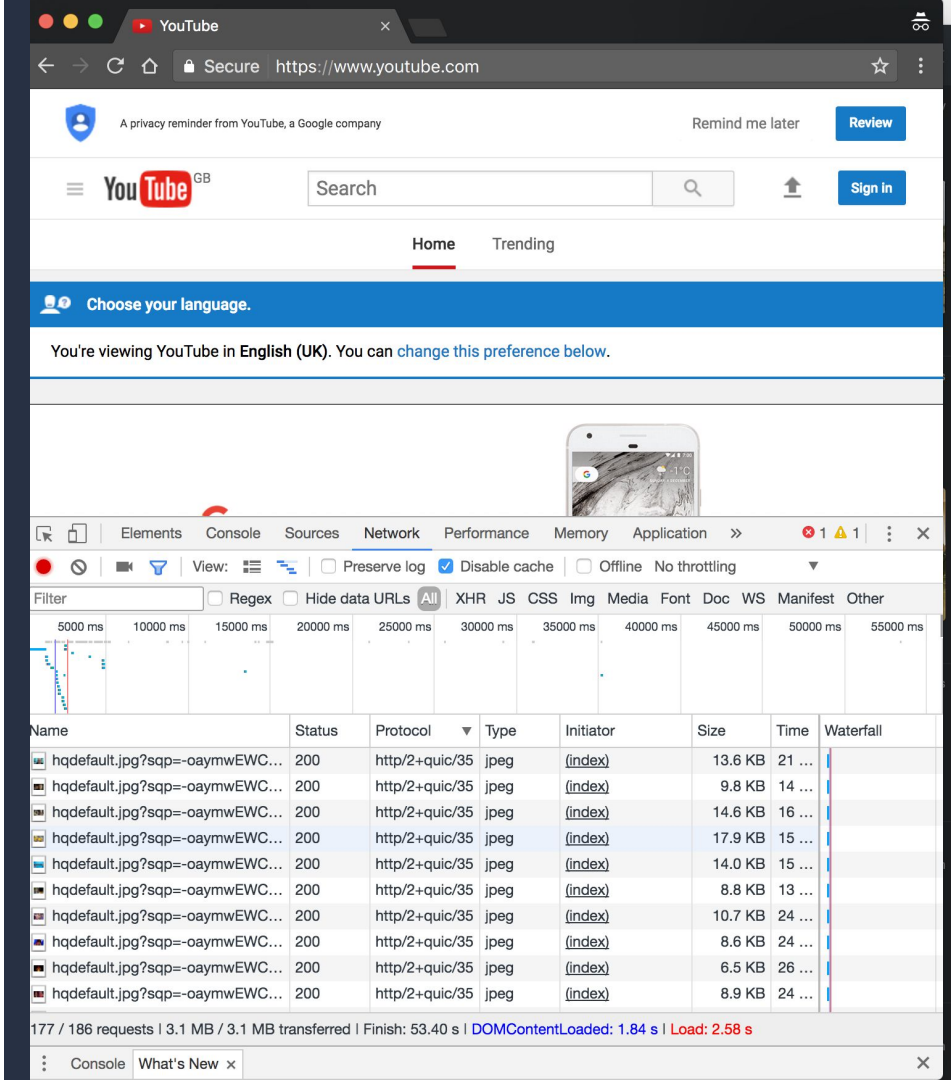
Google Crypto

UDP

IP

QUIC

A Protocol by Google



HTTP/2

TLS 1.2+

TCP

HTTP OVER QUIC

QUIC

TLS 1.3

UDP

IP

“A "stream" is an independent, bidirectional sequence of frames exchanged between the client and server within an HTTP/2 connection…

A single HTTP/2 connection can contain multiple concurrently open streams…”

Hypertext Transfer Protocol Version 2 (HTTP/2), RFC7540

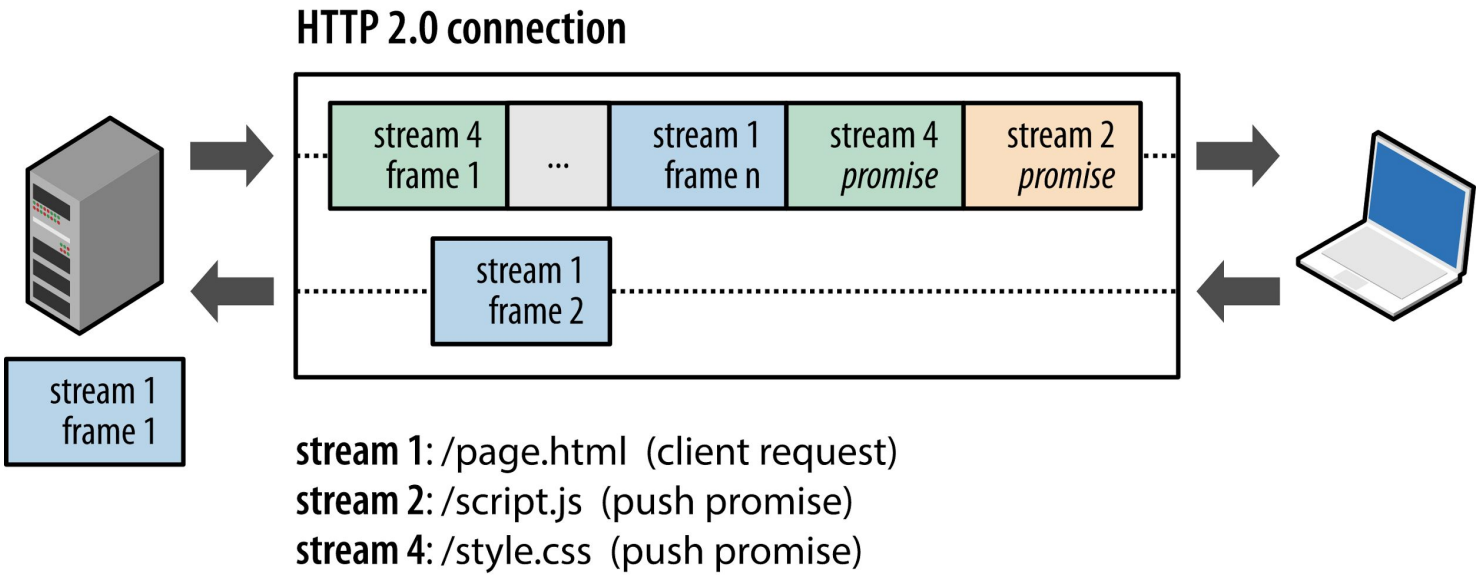
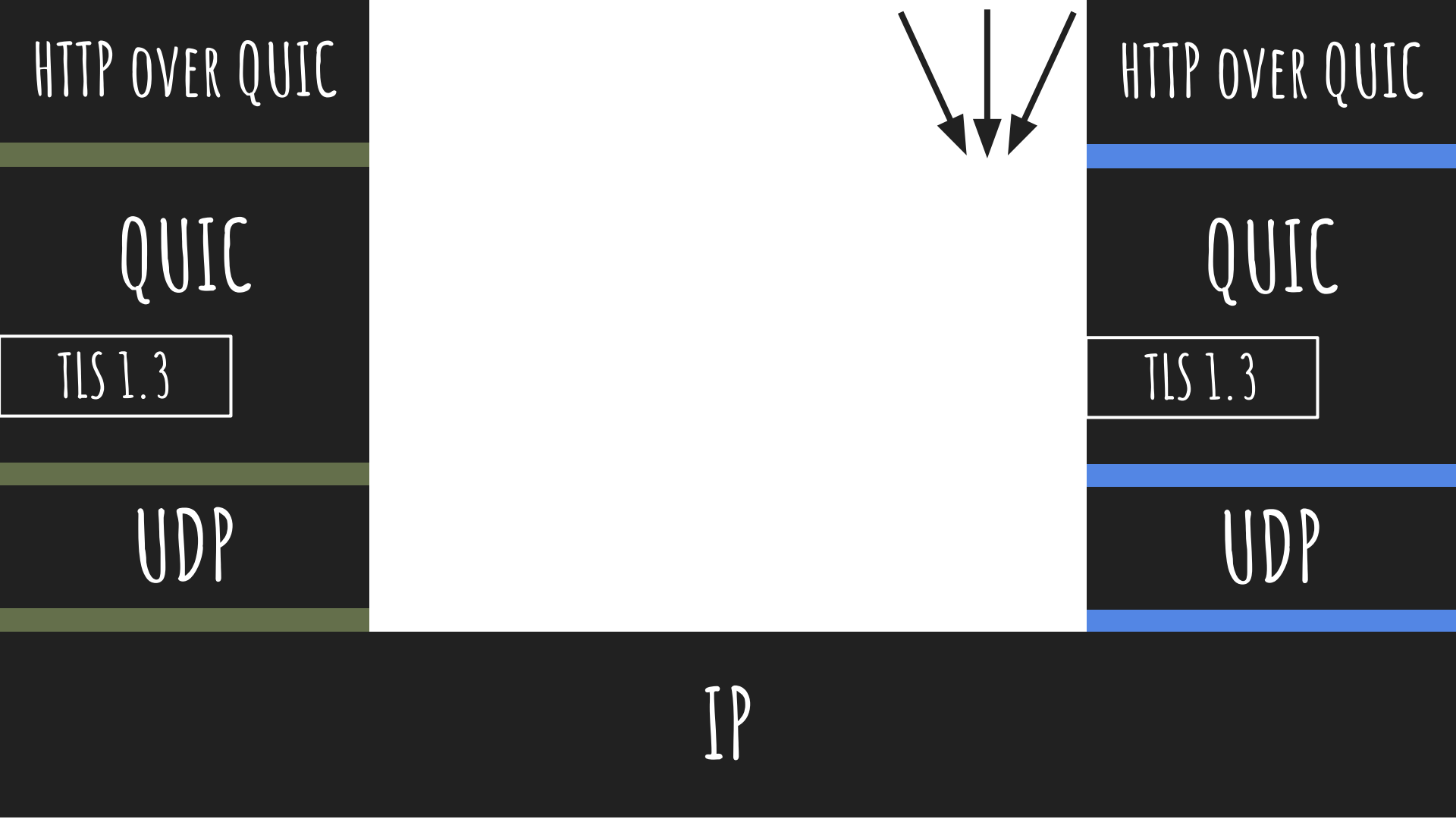
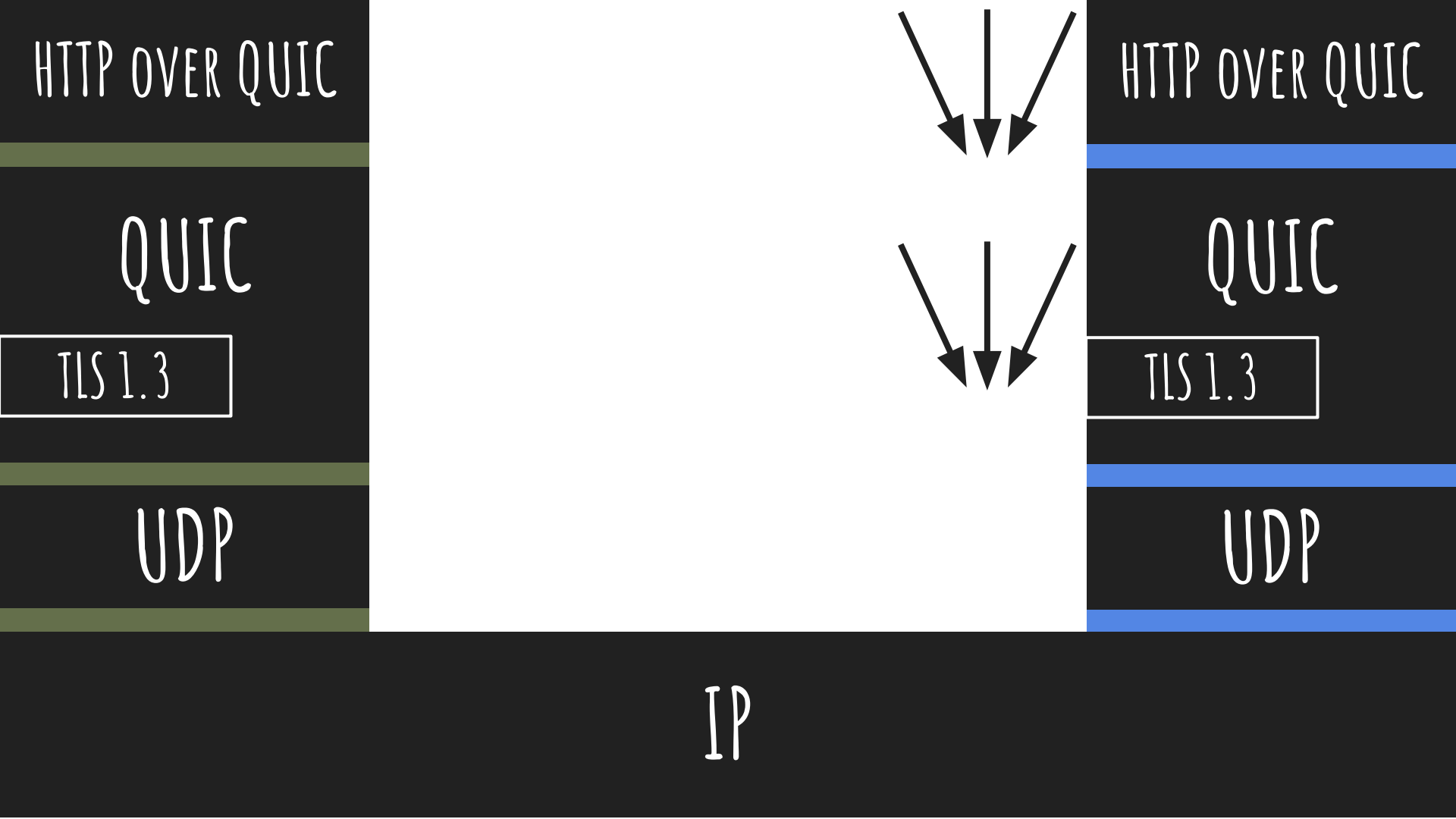
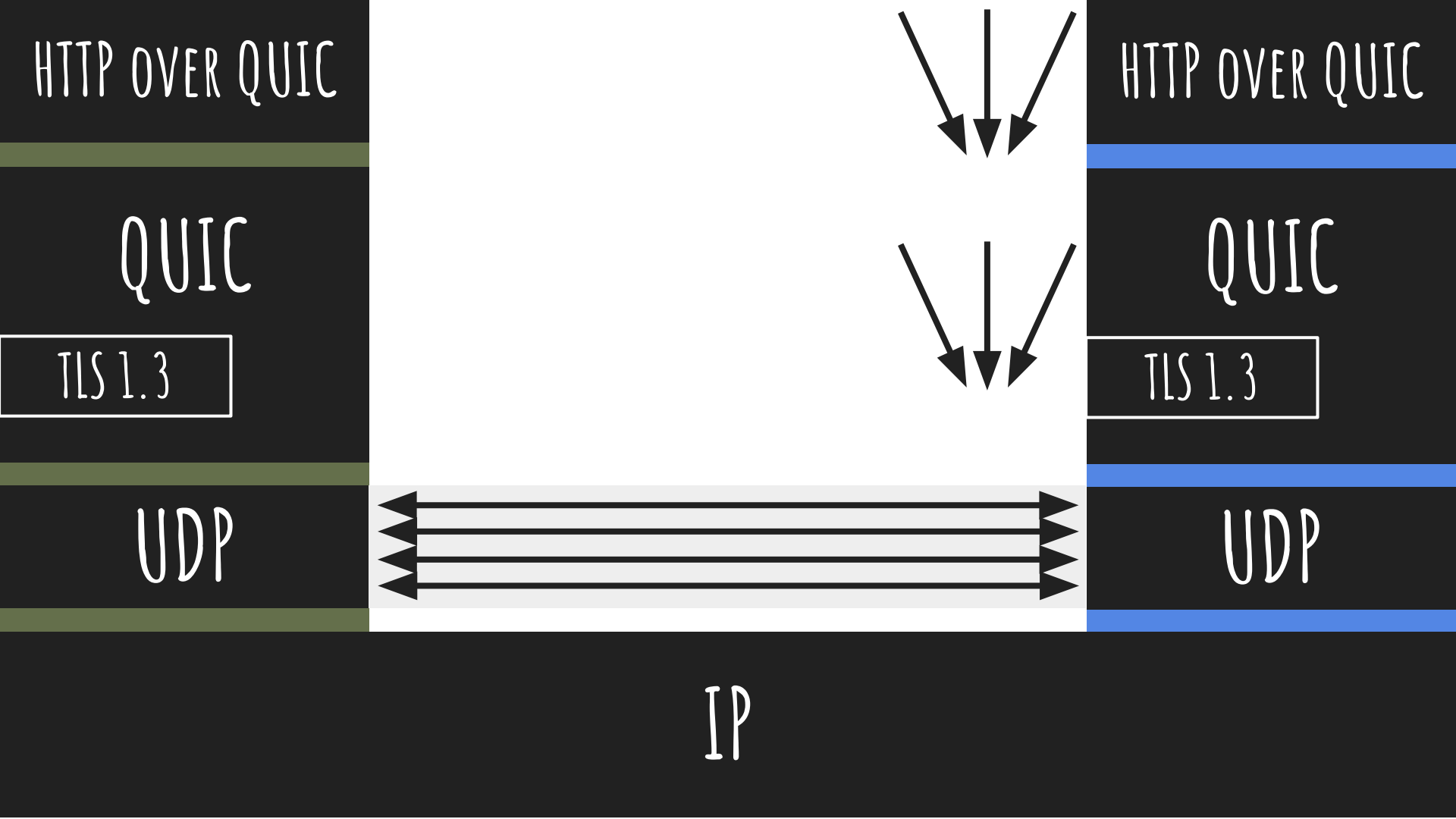
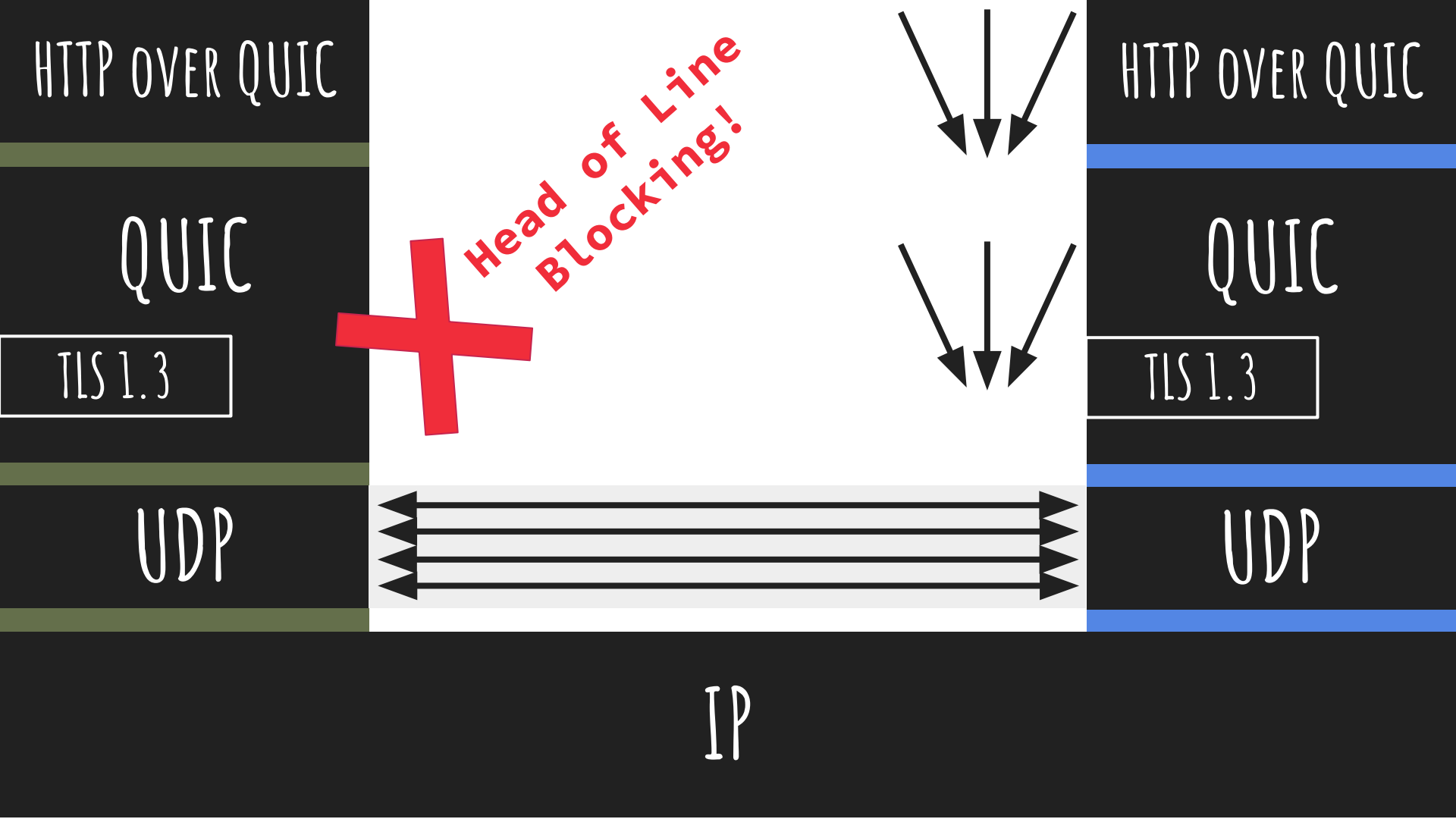


Image source: High Performance Browser Networking https://hpbn.co/http2/

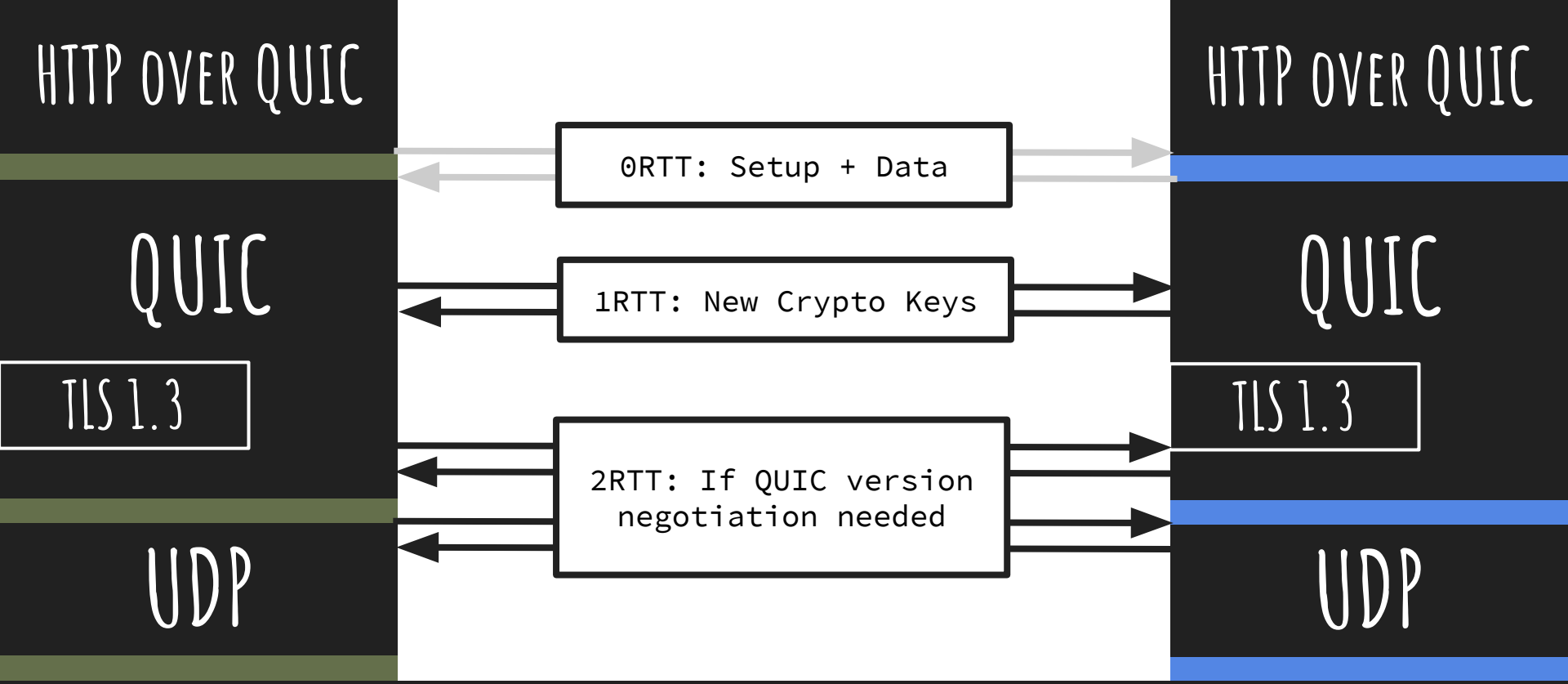

HTTP OVER QUIC
QUIC
TLS 1.3
UDP
HTTP OVER QUIC
QUIC
TLS 1.3
UDP
IP


HTTP over QUIC
QUIC
TLS 1.3
UDP
HTTP over QUIC
QUIC
TLS 1.3
UDP
IP

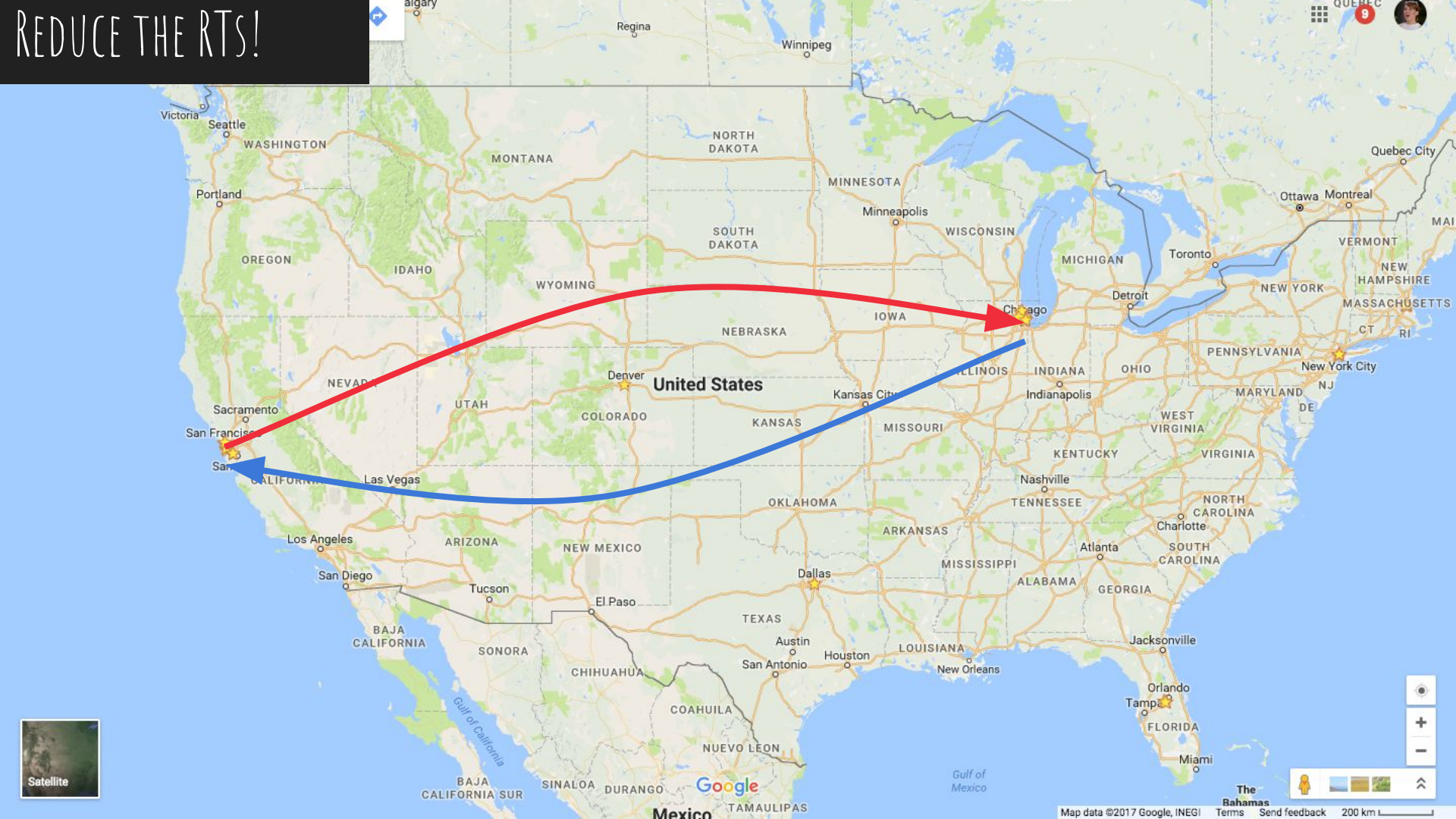

HTTP over QUIC
QUIC
TLS 1.3
UDP
HTTP over QUIC
QUIC
TLS 1.3
UDP
IP


HTTP over QUIC
QUIC
TLS 1.3
UDP
Head of Line Blocking!
HTTP over QUIC
QUIC
TLS 1.3
UDP
IP

Mostly because of physics. Not much you can do about that.


HTTP over QUIC
QUIC
TLS 1.3
UDP
0RTT: Setup + Data
1RTT: New Crypto Keys
2RTT: If QUIC version negotiation needed
HTTP over QUIC
QUIC
TLS 1.3
UDP
IP

Reduce the RTs!



capturing events (77240)

Capture
Export
Import
Proxy
Events
Timeline
DNS
Sockets
Alt-Svc
HTTP/2
QUIC
SDCH
Cache
Modules
HSTS
Bandwidth
Prerender

- QUIC Enabled: true
- Origins To Force QUIC On:
- Connection options:
- Load Server Info Timeout Multiplier: 0.25
- Enable Connection Racing: false
- Disable Disk Cache: false
- Prefer AES: false
- Maximum Number Of Lossy Connections: undefined
- Packet Loss Threshold: undefined
- Delay TCP Race: true
- Store Server Configs In Properties File: null
- Idle Connection Timeout In Seconds: 30
- Disable PreConnect If 0RTT: false
- Disable QUIC On Timeout With Open Streams: false
- Race Cert Verification: false

QUIC sessions

View live QUIC sessions

Host	Version	Peer address	Connection UID	Active stream count	Active streams	Total stream count	Packets Sent	Packets Lost	Packets Received	Connected
0.docs.google.com:443	QUIC_VERSION_35	108.177.119.189:443	4320267434055741040	3	967, 969, 971	484	2286	0	3116	true
apis.google.com:443 clients5.google.com:443 notifications.google.com:443 ogs.google.com:443 play.google.com:443	QUIC_VERSION_35	172.217.19.206:443	7163347322057347084	0	None	5	61	0	104	true
clients4.google.com:443 play.google.com:443	QUIC_VERSION_35	172.217.19.206:443	4955303205670954227	0	None	3	17	0	13	true
csi.gstatic.com:443	QUIC_VERSION_35	216.58.212.227:443	2195032741195196864	0	None	154	415	0	415	true
encrypted-tbn0.gstatic.com:443	QUIC_VERSION_35	172.217.19.206:443	11763837326739299402	0	None	40	164	0	249	true
fonts.gstatic.com:443 ssl.gstatic.com:443 www.gstatic.com:443	QUIC_VERSION_35	172.217.19.195:443	3632702018728176705	0	None	5	34	0	57	true
i.ytimg.com:443	QUIC_VERSION_35	172.217.19.206:443	5413815142526720918	0	None	1	37	0	70	true
r1---sn-aiglndk.googlevideo.com:443	QUIC_VERSION_35	209.85.230.102:443	9346861099862968819	0	None	14	1108	0	2211	true
r6---sn-5hnedn7z.googlevideo.com:443	QUIC_VERSION_35	74.125.100.188:443	11821379144642082471	0	None	1	464	0	930	true
s.youtube.com:443 www.youtube.com:443	QUIC_VERSION_35	172.217.19.206:443	5087965363789303966	0	None	41	448	0	800	true
www.google.co.uk:443	QUIC_VERSION_35	172.217.19.195:443	16461072303236918760	0	None	50	339	0	561	true
www.google.com:443	QUIC_VERSION_35	172.217.19.196:443	6765651486238199233	0	None	2	8	0	8	true
www.googleadservices.com:443	QUIC_VERSION_35	172.217.17.34:443	3955002652180487648	0	None	2	7	0	5	true

7% Internet Traffic

35% Google Egress Traffic

How does this affect me?

ABSTRACTION

Is a computer scientist’s friend / fiend


LAYER VIOLATION
IT'S A CRIME.

WEB

HTTP

TLS

TCP

IP

7. **Application** Data	HTTP / IMAP
6. Data **Presentation**, Encryption	SSL / TLS
5. **Session** and connection management	-
4. **Transport** of packets and streams	TCP / UDP
3. Routing and delivery of datagrams on the **Network**	IP / IPSec
2. Local **Data** Connection	Ethernet
1. **Physical** data connection (cables)	CAT5

Some things

If you have to do something...

@thisNatasha

Manage your resources logically

Detect on upgrade header and adapt

Measure

Remember Physics!

Recap

We made it!

RTTs, Physics, Data

SPDY, HTTP2, QUIC

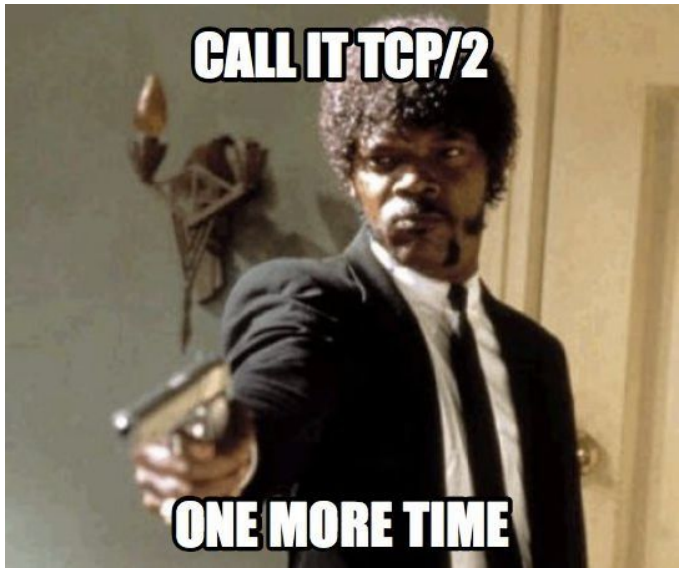
Header compression

Multiplexing & Streams

Head of Line Blocking

Make protocols for today's internet


http3


CALL IT TCP/2
ONE MORE TIME


QUIC

IETF QUIC WG

IETF QUIC Working Group

https://datatracker.ietf.org/wg/quic/charter/ quic@ietf.org

Repositories 4 People 5

Pinned repositories

base-drafts
Internet-Drafts that make up the base QUIC specification
Makefile ★ 146 33

ops-drafts
Applicability and Manageability Statements
Makefile ★ 1 6

wg-materials
Agenda, Minutes, Presentations
Python ★ 34 16

Search repositories... Type: All Language: All

base-drafts

Internet-Drafts that make up the base QUIC specification

tls http protocol standards transport ietf quic

Makefile ★ 146 33 Updated 10 hours ago

wg-materials

Agenda, Minutes, Presentations

Top languages

Makefile Python HTML

Most used topics

ietf quic standards

People 5 >

@thisNatasha

Thank-you

People: Martin Thomson, Mark Nottingham, Jana Iyengar, Mike Bishop, Eric Rescola, Ian Swett

@thisNatasha

@thisNatasha

@thisNatasha

OSI Model

@thisNatasha

7. **Application** Data	HTTP / IMAP
6. Data **Presentation**, Encryption	SSL / TLS
5. **Session** and connection management	-
4. **Transport** of packets and streams	TCP / UDP
3. Routing and delivery of datagrams on the **Network**	IP / IPSec
2. Local **Data** Connection	Ethernet
1. **Physical** data connection (cables)	CAT5

TLS / Handshake Cheat Sheet

Handshake Flow

Client Hello	Client sends TLS Version, **Ciphersuites**, Compression methods
Server Hello, Certificate	- Server selects cipher & compression method - Server send certificate - Client **authenticates**
Key Exchange	Pre-master secret exchanged between client & server, client validates certificate
Master Secret	Client & Server can compute Master Secret.
MAC	Server verifies MAC, returns to client to verify also.
Finished	Handshake complete.

Ciphers, Standards and Terms

Key Exchange Method: creates the pre master secret. Premaster secret is combined with PRF to create master secret	RSA, DHE_RSA, ECDHE_RSA, ECDHE_ECDSA
Authentication Method: Uses public key crypto and certificates public key together. Once certificate is validated the client can used public key.	RSA or ECDSA Certs: X.509, ASN.1 DER encoding.

Master Secret	Integrity Validation	Encryption
Pre-master secret: combines params to help client and server create master secret.	**PRF**: Pseudorandom Function. Takes a secret, a seed, and a unique label. TLS1.2 suites use PRF based on HMAC and SHA256	3DES, AES, ARIA, CAMELLIA, RC4, and SEED [1] Steam: adds MAC [2] Block: adds IV and padding after encryption [3] Encryption (AEAD): encryption and integrity validation, using nonce, no padding, no IV.
Master Secret: both server and client create this from pre-master secret to symmetrically encrypt	**MAC:** used for integrity validation in handshake and record.	

Authentication — Algorithm — Strength — Mode

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Key Exchange — Cipher — MAC or PRF

TLS Handshake

Cli-ant

[1] Client Hello

Server Hello [2]
Certificate [3]
Server Key Exchange [4]
Server Hello Done [5]

[6] Client Key Exchange
[7] (Change Cipher Spec)
[8] Finished

(Change Cipher Spec) [9]
Finished [10]

Ser-ver

TCP and TLS with Session Tickets

TCP Fast Open Handshake

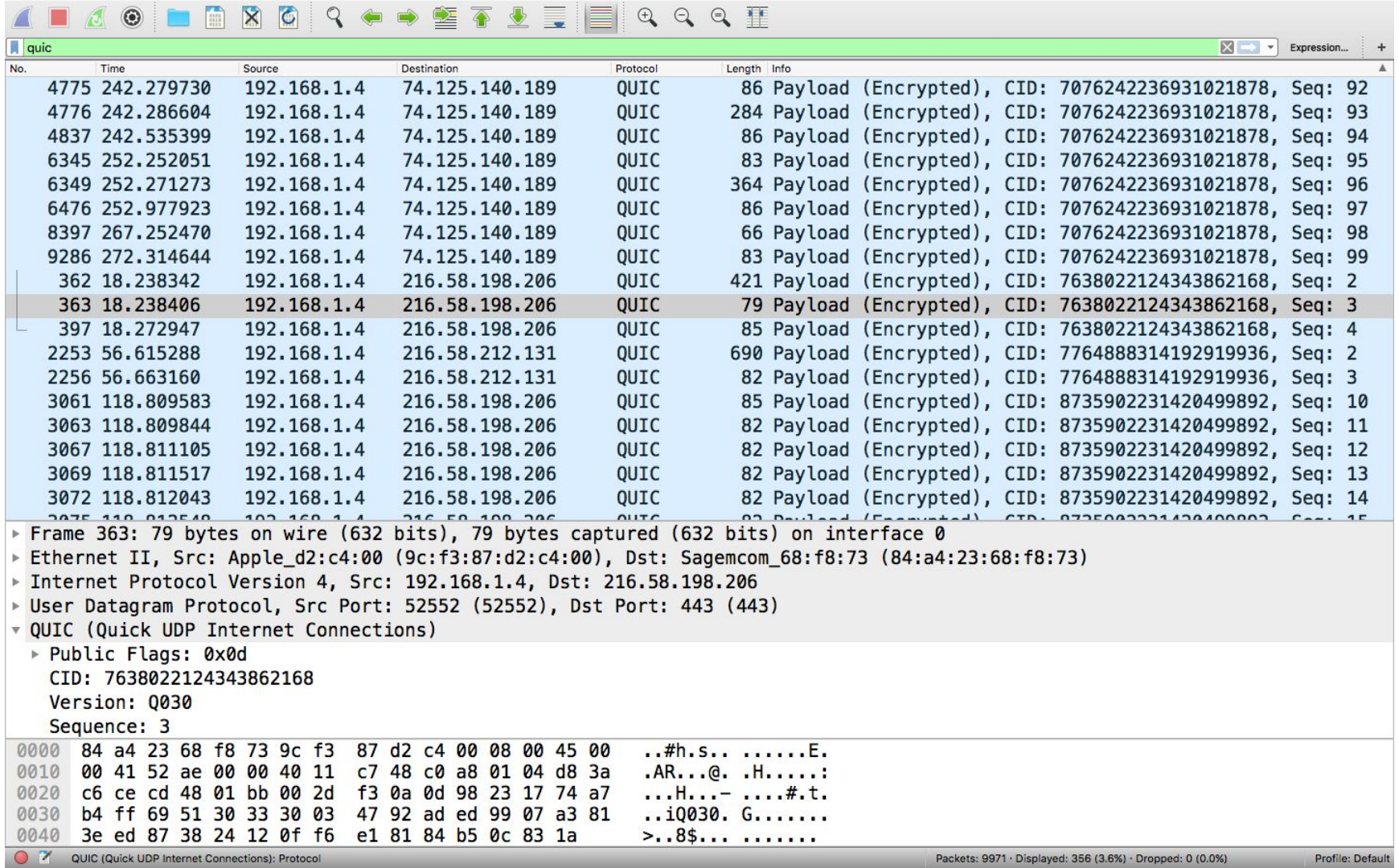
[1] Client Hello

Server Hello [2]
(Change Cipher Spec) [3]
Finished [4]

[5] (Change Cipher Spec)
[6] Finished

Cli-ant

Ser-ver


quic
Expression...
No. Time Source Destination Protocol Length Info
4775 242.279730 192.168.1.4 74.125.140.189 QUIC 86 Payload (Encrypted), CID: 7076242236931021878, Seq: 92
4776 242.286604 192.168.1.4 74.125.140.189 QUIC 284 Payload (Encrypted), CID: 7076242236931021878, Seq: 93
4837 242.535399 192.168.1.4 74.125.140.189 QUIC 86 Payload (Encrypted), CID: 7076242236931021878, Seq: 94
6345 252.252051 192.168.1.4 74.125.140.189 QUIC 83 Payload (Encrypted), CID: 7076242236931021878, Seq: 95
6349 252.271273 192.168.1.4 74.125.140.189 QUIC 364 Payload (Encrypted), CID: 7076242236931021878, Seq: 96
6476 252.977923 192.168.1.4 74.125.140.189 QUIC 86 Payload (Encrypted), CID: 7076242236931021878, Seq: 97
8397 267.252470 192.168.1.4 74.125.140.189 QUIC 66 Payload (Encrypted), CID: 7076242236931021878, Seq: 98
9286 272.314644 192.168.1.4 74.125.140.189 QUIC 83 Payload (Encrypted), CID: 7076242236931021878, Seq: 99
362 18.238342 192.168.1.4 216.58.198.206 QUIC 421 Payload (Encrypted), CID: 7638022124343862168, Seq: 2
363 18.238406 192.168.1.4 216.58.198.206 QUIC 79 Payload (Encrypted), CID: 7638022124343862168, Seq: 3
397 18.272947 192.168.1.4 216.58.198.206 QUIC 85 Payload (Encrypted), CID: 7638022124343862168, Seq: 4
2253 56.615288 192.168.1.4 216.58.212.131 QUIC 690 Payload (Encrypted), CID: 7764888314192919936, Seq: 2
2256 56.663160 192.168.1.4 216.58.212.131 QUIC 82 Payload (Encrypted), CID: 7764888314192919936, Seq: 3
3061 118.809583 192.168.1.4 216.58.198.206 QUIC 85 Payload (Encrypted), CID: 8735902231420499892, Seq: 10
3063 118.809844 192.168.1.4 216.58.198.206 QUIC 82 Payload (Encrypted), CID: 8735902231420499892, Seq: 11
3067 118.811105 192.168.1.4 216.58.198.206 QUIC 82 Payload (Encrypted), CID: 8735902231420499892, Seq: 12
3069 118.811517 192.168.1.4 216.58.198.206 QUIC 82 Payload (Encrypted), CID: 8735902231420499892, Seq: 13
3072 118.812043 192.168.1.4 216.58.198.206 QUIC 82 Payload (Encrypted), CID: 8735902231420499892, Seq: 14
Frame 363: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Ethernet II, Src: Apple_d2:c4:00 (9c:f3:87:d2:c4:00), Dst: Sagemcom_68:f8:73 (84:a4:23:68:f8:73)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 216.58.198.206
User Datagram Protocol, Src Port: 52552 (52552), Dst Port: 443 (443)
QUIC (Quick UDP Internet Connections)
Public Flags: 0x0d
CID: 7638022124343862168
Version: Q030
Sequence: 3
0000 84 a4 23 68 f8 73 9c f3 87 d2 c4 00 08 00 45 00 ..#h.s.. ......E.
0010 00 41 52 ae 00 00 40 11 c7 48 c0 a8 01 04 d8 3a .AR...@. .H.....:
0020 c6 ce cd 48 01 bb 00 2d f3 0a 0d 98 23 17 74 a7 ...H...- ....#.t.
0030 b4 ff 69 51 30 33 30 03 47 92 ad ed 99 07 a3 81 ..iQ030. G.......
0040 3e ed 87 38 24 12 0f f6 e1 81 84 b5 0c 83 1a >..8$... ....
QUIC (Quick UDP Internet Connections): Protocol
Packets: 9971 · Displayed: 356 (3.6%) · Dropped: 0 (0.0%)
Profile: Default

Transport Overhead

Table 9.1. Transport overhead for each of the widely available ciphers

Cipher	TLS Record	IV/Nonce	Padding (average/worst)	HMAC/Tag	Total (average)
AES-128-CBC-SHA	5	16	8 / 16	20	49
AES-128-CBC-SHA256	5	16	8 / 16	32	61
AES-128-GCM-SHA256	5	8	-	16	29
AES-256-CBC-SHA	5	16	8 / 16	20	49

Min