SPEED & SECURITY

A Better User Experience with HTTP/2 & Let's Encrypt

#DPA12

HI, MY NAME IS MIKE

Executive Director of Marketing
and Creative Services

John Carroll University

@mrichwalsky

#dpa12

BABY IF YOU COULD WOULD YOU GO BACK TO THE START?

#monthebiff

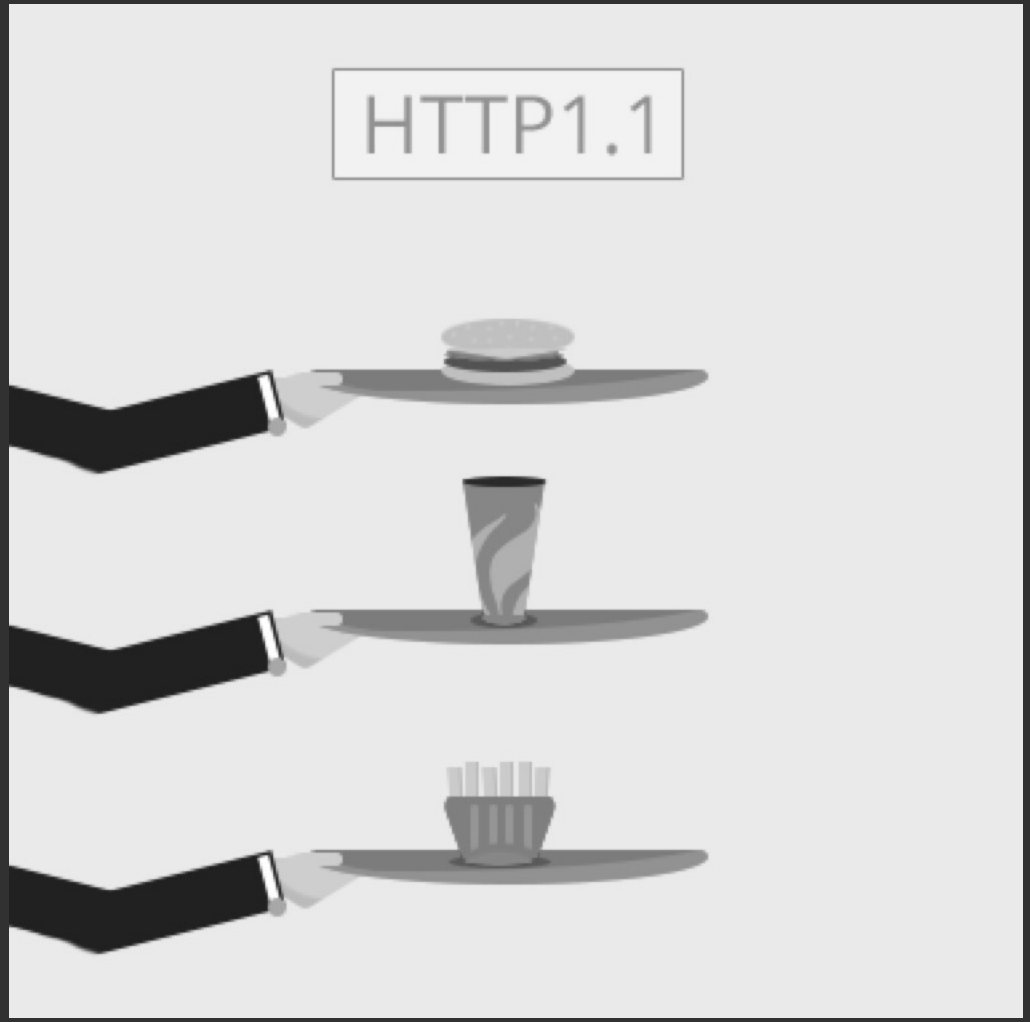
IN THE BEGINNING

- Tim Berners-Lee created HTTP
- First spec in 1991 (0.9)
- HTTP 1.1 officially released in 1997

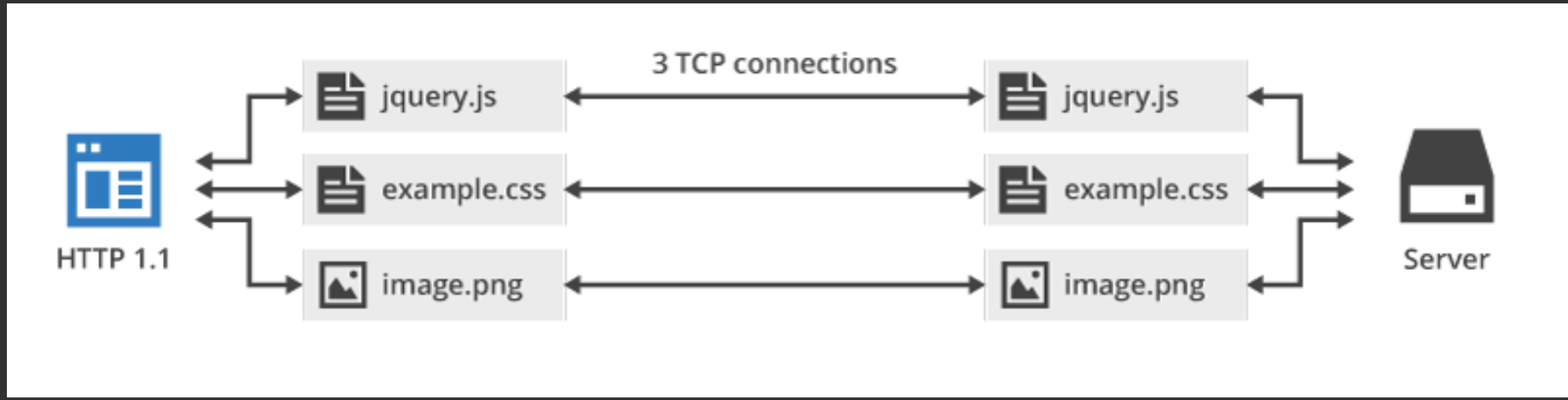
BROWSERS WHEN 1.1 WAS RELEASED

- Arena
- Netscape 2.0
- IE 2.0
- Mosiac 2.7
- Lynx 2.5


HAMBURGERS.
THE CORNERSTONE
OF ANY NUTRITIOUS
BREAKFAST.
#bigkahuna



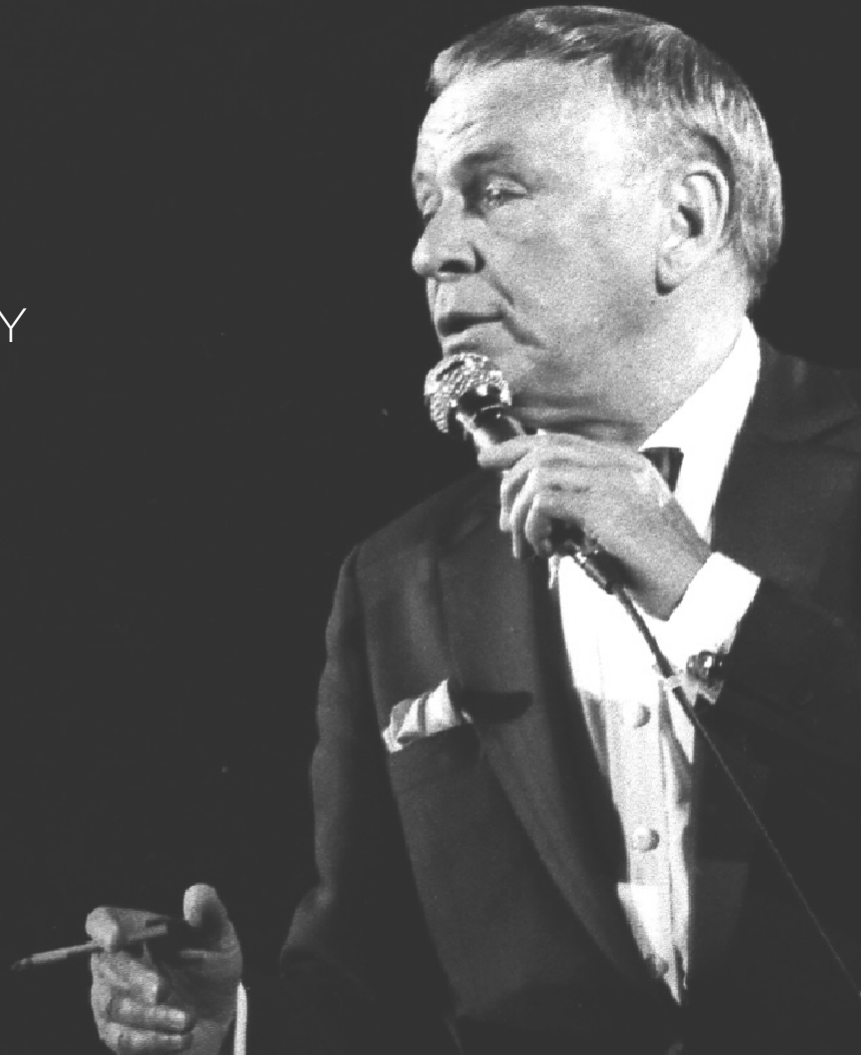
PIC BY KINSTA



PIC BY CLOUDFLARE

IT'S STILL THE SAME OLD STORY
A FIGHT FOR LOVE AND GLORY
A CASE OF DO OR DIE
THE WORLD WILL ALWAYS
WELCOME LOVERS

AS TIME GOES BY




iPhone
iPhone

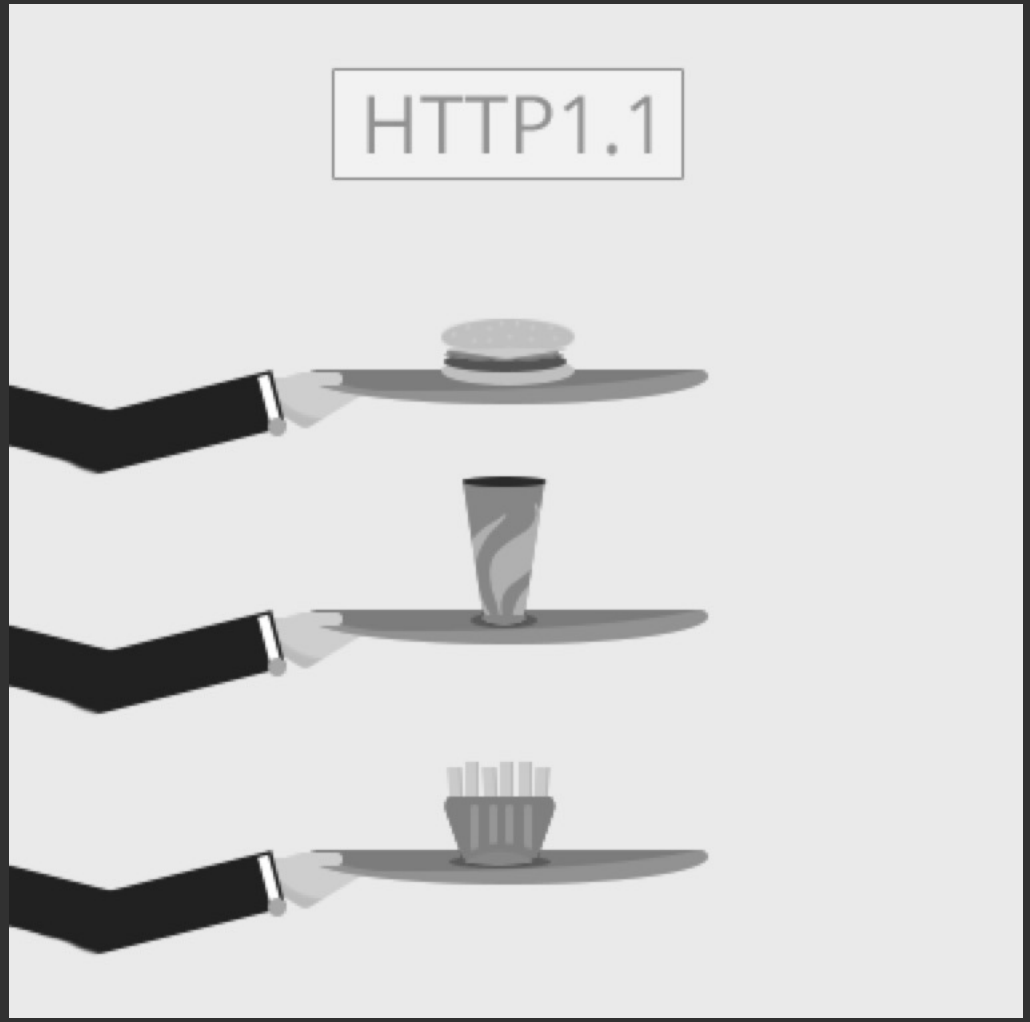
15 YEARS IS PRACTICALLY 50 LIFETIMES

- The devices and networks have gotten better
- We need better protocols, security, and scalability

NEW AND REVISED PROTOCOLS

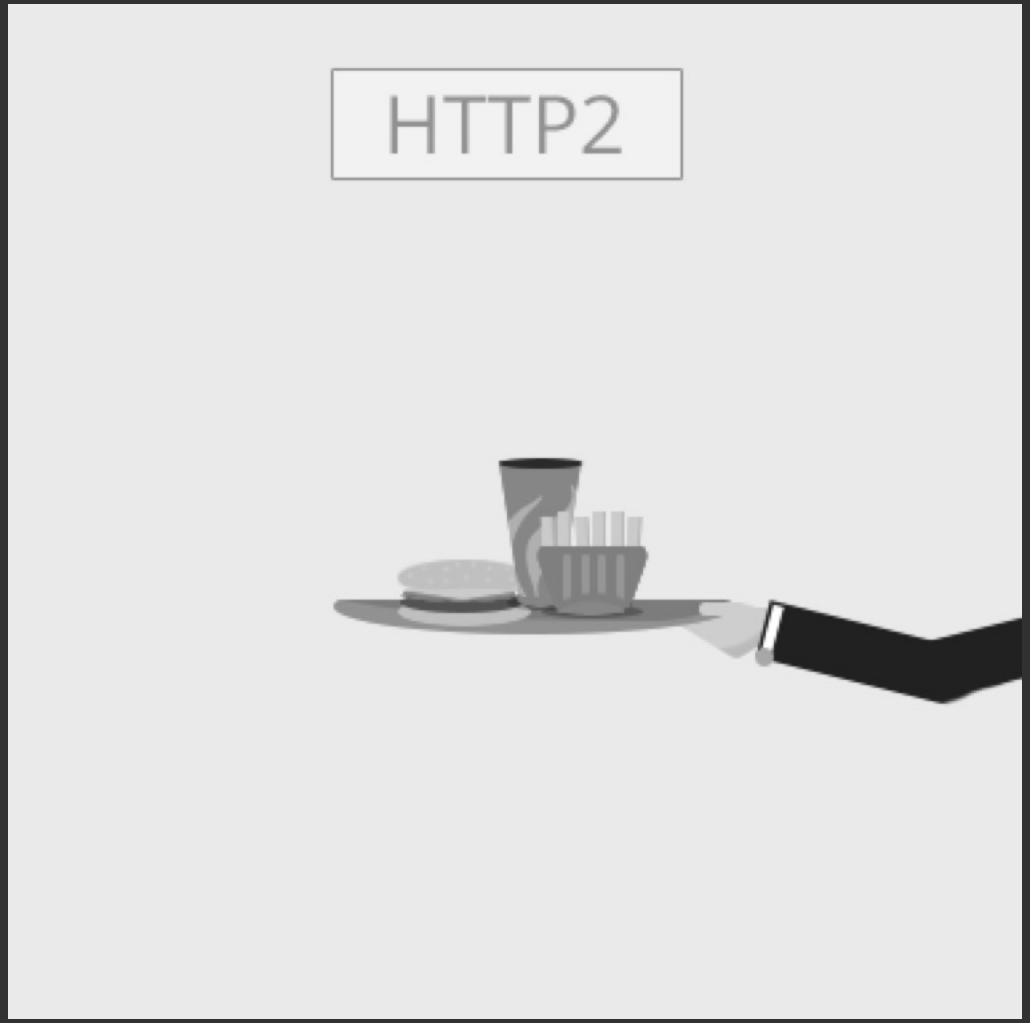
- Google created SPDY (2009)
- From that, HTTP/2
  - standardized in 2015

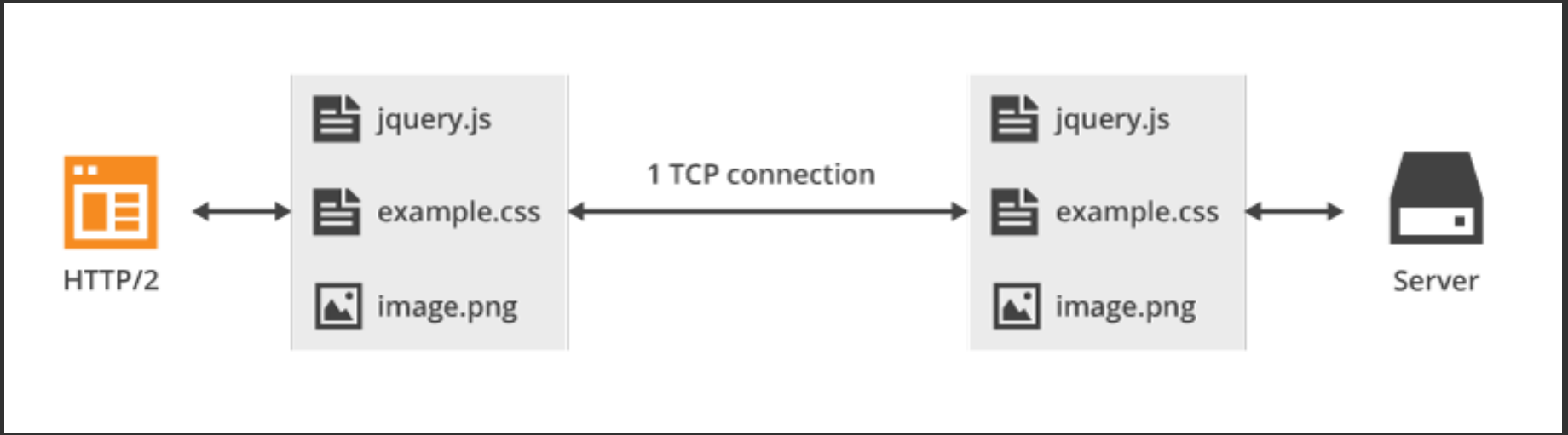
WHAT DOES HTTP/2 DO DIFFERENTLY?



PIC BY KINSTA

PIC BY KINSTA





PIC BY CLOUDFLARE

HTTP/2...

- is binary, instead of textual
- is fully multiplexed, instead of ordered and blocking
- can therefore use one connection for parallelism
- uses header compression to reduce overhead
- allows servers to “push” responses proactively into client caches

WHY IS THIS GOOD?

- Faster speeds
- Better, more efficient caching
- More efficient sending
- Already in Apache and NGINX


REAL WORLD RESULTS
TEST

WHAT'S THE CATCH?

HTTP/2 needs SSL*

* A QUICK DISCLAIMER

- Technically, the spec says you don't have to use encryption
- No browser supports HTTP/2 unencrypted.

So... moving on.

WHY HTTPS?

Implementations of HTTP/2 MUST use TLS version 1.2 [TLS12] or higher for HTTP/2 over TLS. The general TLS usage guidance in [TLSBCP] SHOULD be followed, with some additional restrictions that are specific to HTTP/2.

http://http2.github.io/http2-spec/#TLSUsage

ADDING HTTPS TO YOUR SITE IS GOOD

- Google gives bump to HTTPS sites in search results
- Peace of mind for users
- Browsers are going to start showing SSL/HTTPS more

ADDING SSL TO A SITE CAN BE A PITA

STEPS TO ACQUIRE SSL CERTS

- Purchase a certificate from a vendor
- Generate Certificate Signing Request
- Give to vendor, download package
- Install onto server
- Restart and hope it all went OK

SAY HELLO TO

LET'S ENCRYPT

LET'S ENCRYPT IS A NEW CERTIFICATE AUTHORITY.

IT'S FREE, AUTOMATED, AND OPEN.

SUPPORTING COMPANIES AND ORGS:

- Facebook
- Mozilla
- Akamai
- Cisco
- EFF
- Sucuri
- Google Chrome
- Automattic
- Shopify
- American Library Association
- OVH
- Vultr
- Many more

LET'S ENCRYPT TIMELINE

- Beta period in late 2015
- LE started offering certificates in April 2016.
- 8 million active, unexpired certs

PROS

- Free!
- Command line generation, installation, and renewal

CONS

- Basic SSL – no special EV or other levels like some places offer
- Needs to be renewed every 3 months
  - Don’t worry this can be automated

EATING THE DOGFOOD

- I use LE certs on personal and professional sites
  - https://highedwebtech.com
  - https://inside.jcu.edu

  - Go and try them out & view the SSL

LEGIT

SSL Report: highedwebtech.com (104.131.78.181)

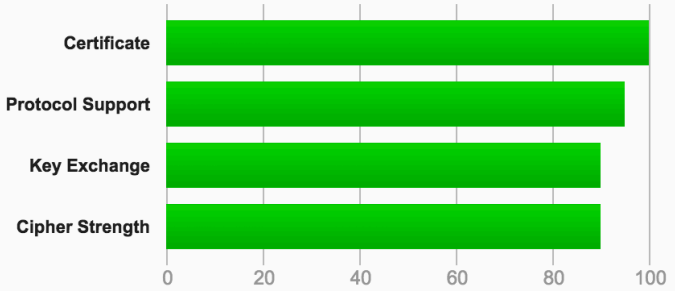
Assessed on: Tue, 18 Oct 2016 13:51:57 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

SOME SHARED HOSTS ARE STARTING TO OFFER LE CERTS

- Dreamhost
- Flywheel
- WordPress.com
- Cpanel compatibility

OK LET’S DO THIS FOR REAL

LET'S INSTALL AN SSL CERT USING LET'S ENCRYPT

HEWEB16TEST.TK

- Hey, it was free
- Hosted at DigitalOcean VPS
- Ubuntu 16.10 with Apache 2

CHECKS

- Site should serve OK
- SSL should fail
- HTTP/2 Test should fail

NOW LET'S DO HTTP/2

- DigitalOcean VPS
- Nginx
- Let's Encrypt already installed

DPA12.CF

- Nginx install
- Let’s Encrypt Installed
- HTTP/2 Test Should Fail

THE FUTURE

CHEERS!

@mrichwalsky

hewt.in/dpa12