Post-Quantum

Cryptography Conference

How much will ML-DSA Signatures affect Web Metrics after all?

It is sometimes argued that ML-DSA signatures will increase the size of TLS handshakes by 15KB which will affect web performance significantly. As most web connections transfer much larger amounts of data, 15KB may not impact the bottom line of the most common web performance metrics. In this session, we will present a qualitative analysis of web metrics and their relation to the TLS handshake. We will demonstrate that web connections transport large amounts of web content which takes much longer than the handshake itself. We will also analyze the web page performance metrics of top websites to showcase that an additional 15KB in the handshake will have minimal impact on the user experience. The takeaway of this session will be that ML-DSA will introduce overhead, but after using simple techniques to trim the authentication data in the handshake, the practical effect on web users will not be noticeable.

Panos Kampanakis
Principal Security Engineer, Applied Scientist at Amazon Web Services (AWS)

Mila Anastasova
Applied Scientist at Amazon Web Services (AWS)

SSL.com PQ SHIELD HID KEYFACTOR ENTRUST

January 15 and 16, 2025 - Austin, TX (US) | Online

PKI Consortium

How much will ML-DSA affect Web Page Metrics?

Panos Kampanakis

Security Engineer

Amazon Web Services (AWS)

The Challenge with the cert chain

ML-DSA IN HTTP/1.1, 2, 3 CONNECTIONS

- End-entity certs include
  - 4 Signatures + 1 Public Key
- Intermediate CA certs include
  - 1 Signature + 1 Public Key
- TLS CertVerify message includes
  - 1 Signature

- Total: **15KB+ more “auth data” in the TLS handshake**

Example X.509 v3 End-entity Certificate

```
Certificate:
   Data:
       [...]
       Subject: CN=aws.amazon.com                                  1.3-2.5KB for ML-DSA
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
               Public-Key: (2048 bit)
               Modulus:
                   00:9c:bf:a3:d1:d2:e6:99:f2:43:8e:60:76:71:2a:
                   [...]
       X509v3 extensions:
              [...]
               Signed Certificate Timestamp:
                   Version   : v1 (0x0)
                   Log ID    : [...]
                  [...]                                          2.4-4.5KB for ML-DSA
                   Signature : ecdsa-with-SHA256
                               00:99:30:49:93:D0:89:DF:1B:2F:47:20:
                               [...]
               Signed Certificate Timestamp:
                   Version   : v1 (0x0)
                   Log ID    : [...]
                  [...]                                          2.4-4.5KB for ML-DSA
                   Signature : ecdsa-with-SHA256
                               D5:00:85:AF:07:E6:62:44:4D:67:F0:CA:
                               [...]
               Signed Certificate Timestamp:
                   Version   : v1 (0x0)
                   Log ID    : [...]
                  [...]                                          2.4-4.5KB for ML-DSA
                   Signature : ecdsa-with-SHA256
                               65:CA:0B:4F:21:49:19:37:2D:35:18:9D:
                               [...]
   Signature Algorithm: sha256WithRSAEncryption
   Signature Value:
       13:29:55:50:6c:87:b7:20:88:94:d9:5e:42:15:37:ec:51:ef:
       [...]                                                     2.4-4.5KB for ML-DSA
```

Points made regarding ML-DSA in WebPKI

(PARAPHRASED)

- *+15KB in the TLS handshake before we transfer **any data** seems*
  - *expensive*
  - *like a lot*

- *+15KB will slow down web user experience too much*
- *+7KB will lead to awfully high web page degradation*
- *+2KB to the TLS handshake is very painful*

WebPKI with ML-DSA @ 1Mbps, 150ms RTT

CONSERVATIVE EXAMPLE

15KB @ 1Mbps takes 120ms transfer time.

For 150ms RTT ⇆, this is 66% slowdown of th

+ DNS lookup ⇆

+ TCP handshake ⇆

+ HTTP Request-Response ⇆

lead to 19% slowdown of the TTFB.

Let's say

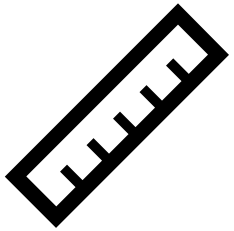
- user's eye starts noticing after the first 20KB
- the application takes 100ms to "render" that

Then the slowdown the user will experience is 120ms/892ms = 13%.

Testing Methodology

TOOLS, METRICS

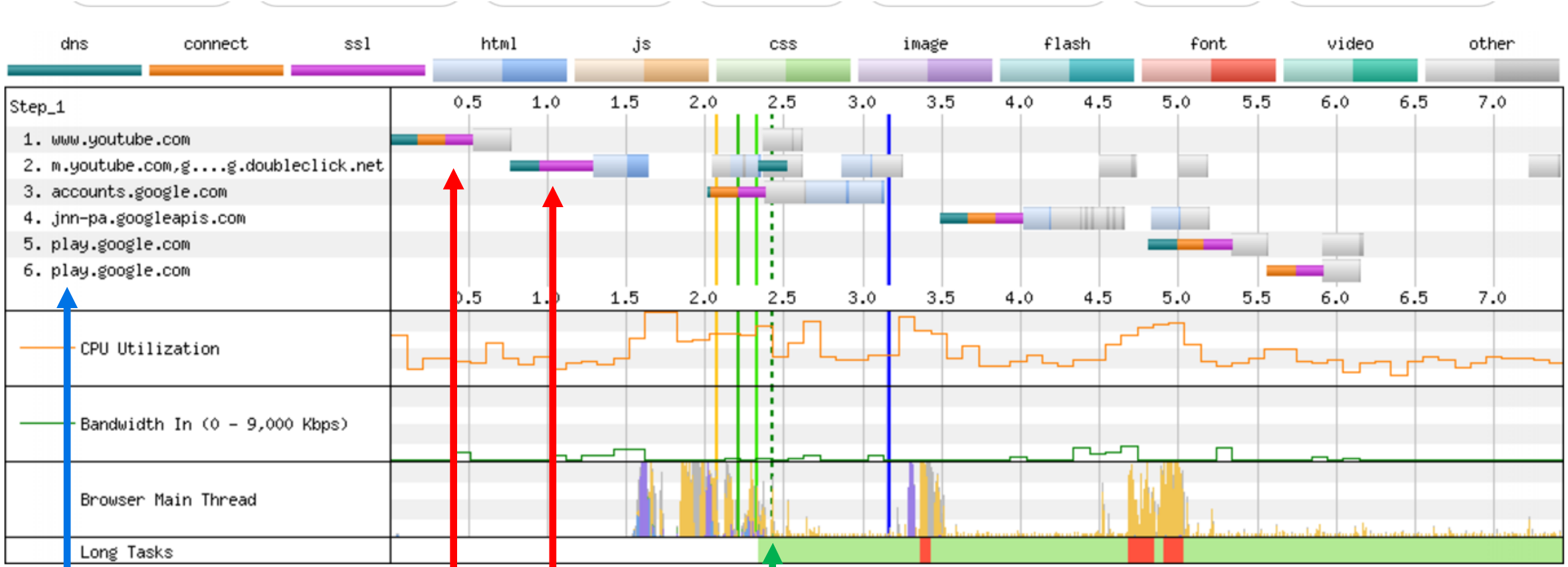
- Page Measurements webpagetest.org
  - Top 15 Web Pages (homepage)
  - Chrome Browser caching enabled
  - Scenarios (for different conns speeds and RTT)
    - 4G
    - Cable
    - 3G
- Web Metrics Investigated
  - Time-To-First-Byte (TTFB)
  - First Contentful Paint (FCP)
  - Document Complete (DC) Bytes Transferred
  - Largest Contentful Paint (LCP)
  - ~~Cumulative Layout Shift (CLS)~~
  - ~~Interaction to Next Paint (INP)~~



Core Web Vitals

Methodology: Measuring Impact on the Metric

ESTIMATING THE IMPACT OF ML-DSA ON THE WEB METRIC OF A WEB PAGE



Output from www.webpagetest.org test

Destinations serving the web content

Maximum TLS handshakes affecting the metric

Metric of interest (LCP)

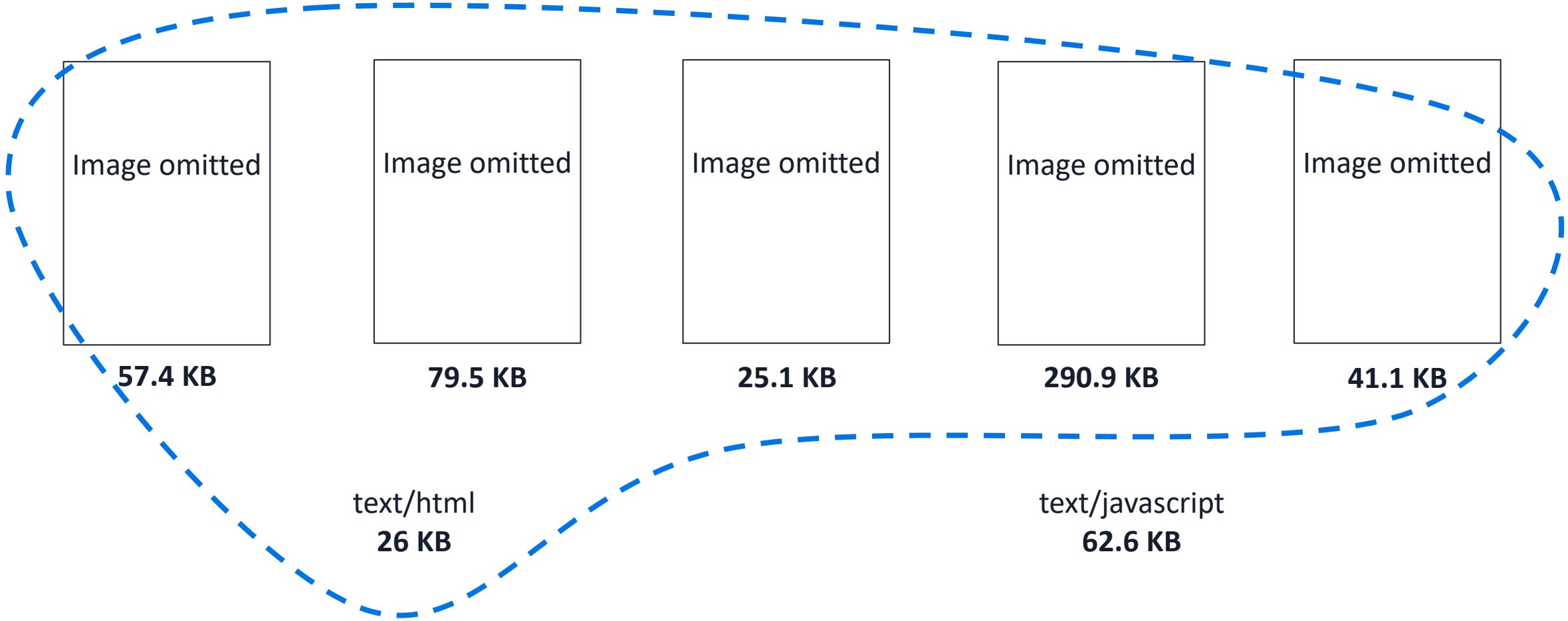
4G Slowdowns (due to ML-DSA)

9MBPS DOWN / 9MBPS UP, 170MS RTT

Website	TLS	TTFB	FCP	LCP	DC	DC KB
www.google.com	+7.8%	0.777s + 1.72%	1.199s + 1.11%	1.199s + 1.11%	2.431s + 0.55%	445
www.youtube.com	+7.8%	1.513s + 1.76%	2.315s + 1.15%	2.413s + 1.11%	3.159s + 1.27%	36
outlook.office.com	+7.8%	2.475s + 1.08%	5.214s + 1.02%	5.419s + 0.98%	3.937s + 1.02%	170
www.facebook.com	+7.8%	2.045s + 1.30%	2.348s + 1.14%	2.348s + 1.14%	3.171s + 0.84%	30
docs.google.com	+7.8%	1.488s + 0.90%	1.962s + 0.68%	1.990s + 0.67%	4.408s + 0.91%	620
www.linkedin.com	+7.8%	1.182s + 1.13%	1.437s + 0.93%	1.469s + 0.91%	1.595s + 0.84%	15
chatgpt.com	+7.8%	1.020s + 1.31%	1.752s + 0.76%	2.714s + 0.49%	1.940s + 0.69%	18
www.instagram.com	+7.8%	0.857s + 1.56%	1.725s + 0.77%	2.325s + 0.57%	1.904s + 0.70%	96
x.com	+7.8%	0.759s + 1.76%	2.321s + 1.15%	3.915s + 1.70%	4.607s + 1.74%	100
en.wikipedia.org	+7.8%	1.471s + 0.91%	2.364s + 1.13%	2.364s + 1.13%	2.453s + 1.09%	63
dadrian.io/blog/[…]	+7.8%	0.733s + 1.82%	1.777s + 1.50%	1.777s + 1.50%	1.757s + 1.52%	8
www.cnn.com	+7.8%	0.581s + 2.29%	1.538s + 0.87%	2.771s + 0.96%	14.05s + 1.04%	2,300
www.msn.com	+7.8%	0.951s + 1.40%	1.319s + 1.01%	2.319s + 1.72%	5.062s + 1.05%	590
stackoverflow.com	+7.8%	0.751s + 1.78%	1.353s + 0.99%	1.452s + 0.92%	2.001s + 1.33%	33
www.tiktok.com	+7.8%	0.874s + 1.53%	1.069s + 1.25%	6.154s + 0.43%	3.274s + 0.81%	72

Example Document Complete Transferred KB

EN.WIKIPEDIA.ORG: 583 KB



Omitted if the browser cached them recently.

4G Slowdowns (due to ML-DSA)

9MBPS DOWN / 9MBPS UP, 170MS RTT

Website	TLS	TTFB		FCP		LCP		DC		DC KB
			<2%		<1.5%		<2%		<1.5%	
www.google.com	+7.8%	0.777s	+ 1.72%	1.199s	+ 1.11%	1.199s	+ 1.11%	2.431s	+ 0.55%	445
www.youtube.com	+7.8%	1.513s	+ 1.76%	2.315s	+ 1.15%	2.413s	+ 1.11%	3.159s	+ 1.27%	36
outlook.office.com	+7.8%	2.475s	+ 1.08%	5.214s	+ 1.02%	5.419s	+ 0.98%	3.937s	+ 1.02%	170
www.facebook.com	+7.8%	2.045s	+ 1.30%	2.348s	+ 1.14%	2.348s	+ 1.14%	3.171s	+ 0.84%	30
docs.google.com	+7.8%	1.488s	+ 0.90%	1.962s	+ 0.68%	1.990s	+ 0.67%	4.408s	+ 0.91%	620
www.linkedin.com	+7.8%	1.182s	+ 1.13%	1.437s	+ 0.93%	1.469s	+ 0.91%	1.595s	+ 0.84%	15
chatgpt.com	+7.8%	1.020s	+ 1.31%	1.752s	+ 0.76%	2.714s	+ 0.49%	1.940s	+ 0.69%	18
www.instagram.com	+7.8%	0.857s	+ 1.56%	1.725s	+ 0.77%	2.325s	+ 0.57%	1.904s	+ 0.70%	96
x.com	+7.8%	0.759s	+ 1.76%	2.321s	+ 1.15%	3.915s	+ 1.70%	4.607s	+ 1.74%	100
en.wikipedia.org	+7.8%	1.471s	+ 0.91%	2.364s	+ 1.13%	2.364s	+ 1.13%	2.453s	+ 1.09%	63
dadrian.io/blog/[…]	+7.8%	0.733s	+ 1.82%	1.777s	+ 1.50%	1.777s	+ 1.50%	1.757s	+ 1.52%	8
www.cnn.com	+7.8%	0.581s	+ 2.29%	1.538s	+ 0.87%	2.771s	+ 0.96%	14.05s	+ 1.04%	2,300
www.msn.com	+7.8%	0.951s	+ 1.40%	1.319s	+ 1.01%	2.319s	+ 1.72%	5.062s	+ 1.05%	590
stackoverflow.com	+7.8%	0.751s	+ 1.78%	1.353s	+ 0.99%	1.452s	+ 0.92%	2.001s	+ 1.33%	33
www.tiktok.com	+7.8%	0.874s	+ 1.53%	1.069s	+ 1.25%	6.154s	+ 0.43%	3.274s	+ 0.81%	72

4G Slowdowns (due to ML-DSA “trimmed” (10KB))

9MBPS DOWN / 9MBPS UP, 170MS RTT

Website	TLS	TTFB <2%	FCP <1%	LCP <1.5%	DC <1%
www.google.com	+5.2%	+1.14%	+0.74%	+0.74%	+0.37%
www.youtube.com	+5.2%	+1.18%	+0.77%	+0.74%	+0.84%
outlook.office.com	+5.2%	+0.72%	+0.68%	+0.66%	+0.68%
www.facebook.com	+5.2%	+0.87%	+0.76%	+0.76%	+0.56%
docs.google.com	+5.2%	+0.60%	+0.45%	+0.45%	+0.60%
www.linkedin.com	+5.2%	+0.75%	+0.62%	+0.61%	+0.56%
chatgpt.com	+5.2%	+0.87%	+0.51%	+0.33%	+0.46%
www.instagram.com	+5.2%	+1.04%	+0.52%	+0.38%	+0.47%
x.com	+5.2%	+1.17%	+0.77%	+1.14%	+1.16%
en.wikipedia.org	+5.2%	+0.60%	+0.75%	+0.75%	+0.72%
dadrian.io/blog/[…]	+5.2%	+1.21%	+1.00%	+1.00%	+1.01%
www.cnn.com	+5.2%	+1.53%	+0.58%	+0.64%	+0.70%
www.msn.com	+5.2%	+0.93%	+0.67%	+1.15%	+0.70%
stackoverflow.com	+5.2%	+1.18%	+0.66%	+0.61%	+0.89%
www.tiktok.com	+5.2%	+1.02%	+0.83%	+0.29%	+0.54%

Cable Slowdowns (due to ML-DSA “trimmed” (10KB))

5MBPS DOWN / 1MBPS UP, 28MS RTT

Website	TLS	TTFB	FCP	LCP	DC
www.google.com	+57.1%	0.262s + 6.11%	0.548s + 2.92%	0.548s + 2.92%	1.795s + 1.78%
www.youtube.com	+57.1%	0.315s + 5.08%	0.802s + 3.99%	2.270s + 2.11%	2.277s + 2.11%
outlook.office.com	+57.1%	0.840s + 3.81%	1.801s + 3.55%	2.900s + 2.76%	1.437s + 3.34%
www.facebook.com	+57.1%	0.379s + 4.22%	0.656s + 2.44%	0.656s + 2.44%	0.759s + 2.11%
docs.google.com	+57.1%	0.489s + 3.27%	0.806s + 1.99%	0.862s + 1.86%	2.265s + 2.83%
www.linkedin.com	+57.1%	0.649s + 2.47%	0.853s + 1.88%	0.880s + 1.82%	0.953s + 1.68%
chatgpt.com	+57.1%	0.462s + 3.46%	1.094s + 1.46%	2.492s + 1.28%	1.305s + 1.23%
www.instagram.com	+57.1%	0.329s + 4.86%	0.690s + 2.32%	1.472s + 1.09%	1.394s + 1.15%
x.com	+57.1%	0.225s + 7.11%	0.877s + 3.65%	2.065s + 3.87%	1.285s + 3.74%
en.wikipedia.org	+57.1%	0.341s + 4.69%	1.002s + 3.19%	1.002s + 3.19%	1.082s + 2.96%
dadrian.io/blog/[…]	+57.1%	0.171s + 9.36%	0.552s + 5.80%	0.552s + 5.80%	0.438s + 7.31%
www.cnn.com	+57.1%	0.174s + 9.20%	0.898s + 1.78%	2.127s + 1.50%	13.97s + 1.95%
www.msn.com	+57.1%	0.225s + 7.11%	1.087s + 2.94%	2.193s + 2.18%	1.348s + 2.37%
stackoverflow.com	+57.1%	0.203s + 7.88%	0.685s + 2.34%	0.685s + 2.34%	1.079s + 2.97%
www.tiktok.com	+57.1%	0.378s + 4.23%	1.593s + 2.01%	4.530s + 1.77%	1.365s + 2.34%

1.5-6%

3G Slowdowns (due to ML-DSA “trimmed” (10KB))

1.6MBPS DOWN / 768KBPS UP, 300MS RTT

Website	TLS	TTFB	FCP	LCP	DC
www.google.com	+16.67%	1.353s + 3.70%	1.671s + 2.99%	1.760s + 2.84%	4.301s + 2.33%
www.youtube.com	+16.67%	2.676s + 3.74%	3.486s + 2.87%	3.607s + 2.77%	5.209s + 2.88%
outlook.office.com	+16.67%	2.352s + 2.13%	15.87s + 1.57%	16.25s + 1.54%	14.67s + 1.70%
www.facebook.com	+16.67%	3.335s + 3.00%	5.438s + 2.76%	5.438s + 2.76%	7.575s + 1.98%
docs.google.com	+16.67%	2.533s + 1.97%	3.497s + 1.43%	3.497s + 1.43%	5.942s + 1.68%
www.linkedin.com	+16.67%	1.827s + 2.74%	1.999s + 2.50%	2.070s + 2.42%	2.161s + 2.31%
chatgpt.com	+16.67%	1.592s + 3.14%	2.216s + 2.26%	3.052s + 1.64%	2.484s + 2.01%
www.instagram.com	+16.67%	1.469s + 3.40%	2.440s + 2.05%	2.972s + 1.68%	2.552s + 1.96%
x.com	+16.67%	1.354s + 3.69%	1.969s + 2.54%	3.569s + 1.40%	5.090s + 2.95%
en.wikipedia.org	+16.67%	2.479s + 2.02%	3.233s + 1.55%	3.233s + 1.55%	4.330s + 2.31%
dadrian.io/blog/[…]	+16.67%	1.313s + 3.81%	2.977s + 3.36%	2.977s + 3.36%	2.751s + 3.64%
www.cnn.com	+16.67%	1.139s + 4.39%	3.044s + 1.64%	4.974s + 1.01%	29.31s + 3.92%
www.msn.com	+16.67%	1.682s + 2.97%	3.620s + 1.38%	4.680s + 2.14%	3.873s + 1.29%
stackoverflow.com	+16.67%	1.356s + 3.69%	1.955s + 2.56%	2.055s + 2.43%	2.588s + 1.93%
www.tiktok.com	+16.67%	1.535s + 3.26%	1.779s + 2.81%	10.33s + 2.91%	10.67s + 2.81%

1.5-3.5%

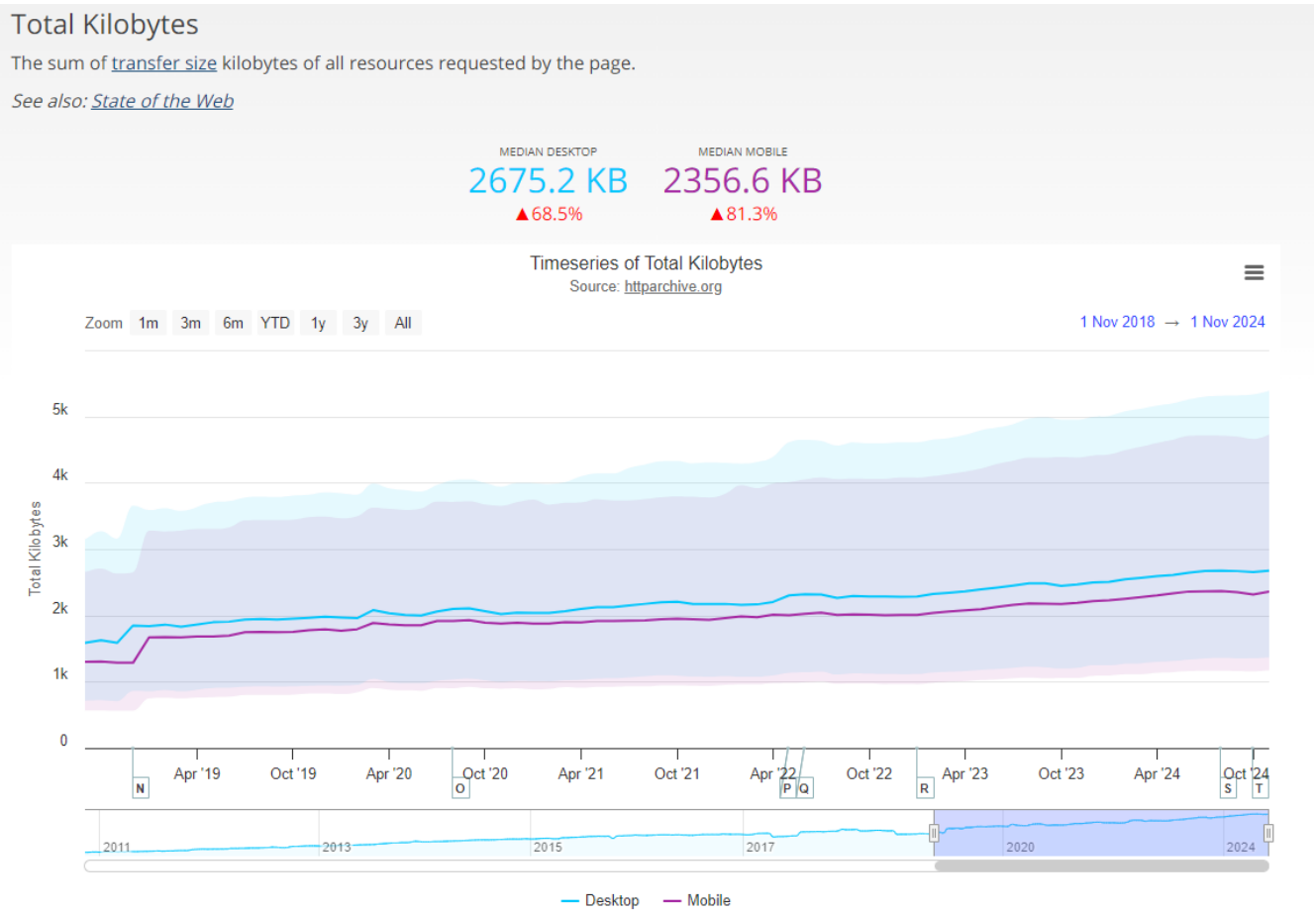
But wait, did the experiments above miss something?

> […] *For non-resumptions the median is 7.8kB and average is 551kB. This vast difference between median and average indicates that a small fraction of data-heavy connections skew the average. In fact, only 15.8% of all QUIC connections transfer more than 100kB.*
>
> […] *For the majority of QUIC connections, using ML-DSA as a drop-in replacement for classical signatures would more than double the number of transmitted bytes over the lifetime of the connection.*

Bas Westerbaan, Luke Valenta

Cloudflare Blog https://blog.cloudflare.com/another-look-at-pq-signatures

Other (contradicting) evidence



httparchive.org/reports/page-weight

Website	Xferred KB
www.google.com	445
www.youtube.com	36
outlook.office.com	170
www.facebook.com	30
docs.google.com	620
www.linkedin.com	15
chatgpt.com	18
www.instagram.com	96
x.com	100
en.wikipedia.org	63
dadrian.io/blog/[...]	8
www.cnn.com	2,300
www.msn.com	590
stackoverflow.com	33
www.tiktok.com	72

From the Cable experiments above

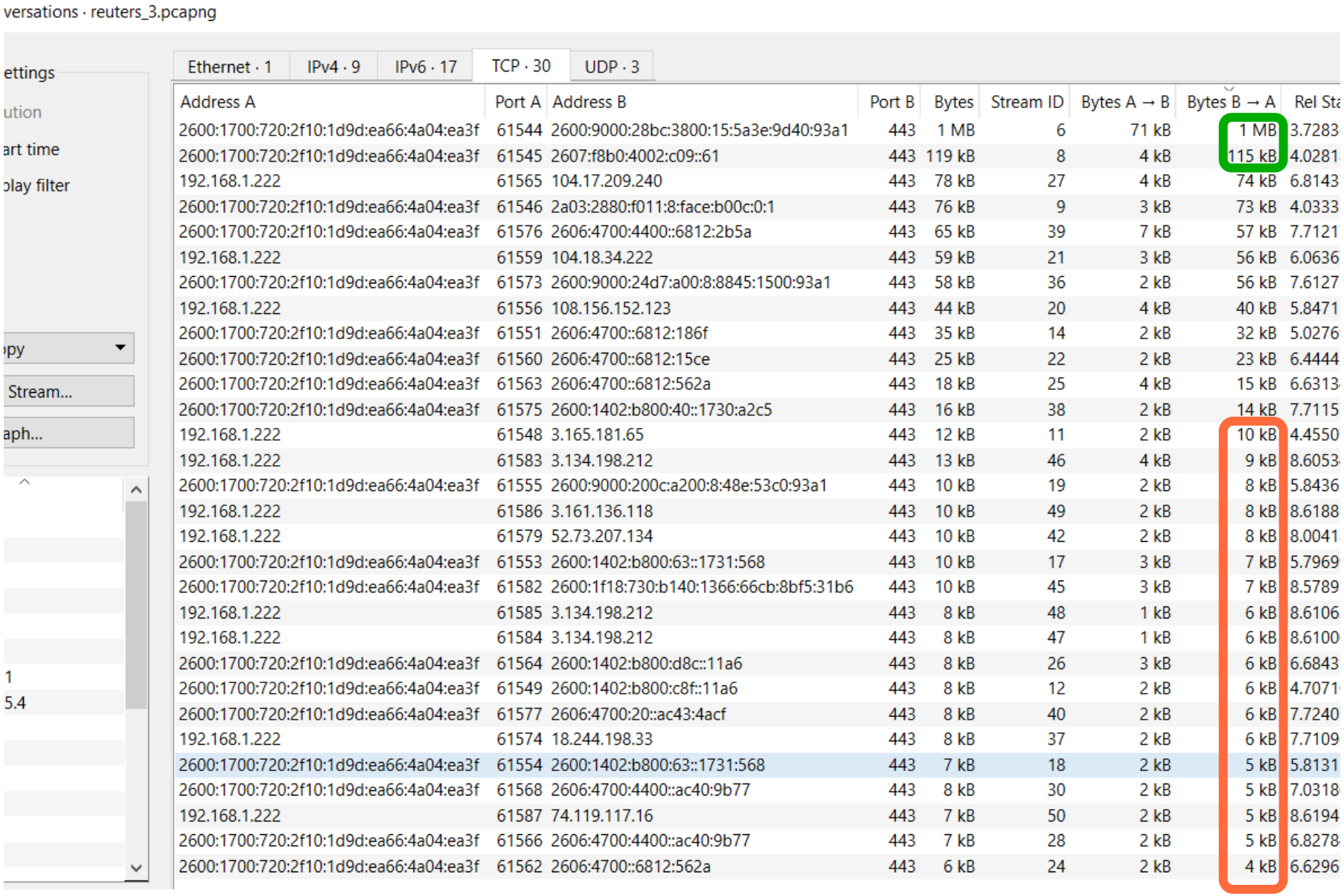
Empirical, qualitative web page investigation

(WITH ITS LIMITED EXTENT CAVEATS)

- We investigated the TLS 1.2, 1.3 and QUIC flows of **logged in** web pages
  - amazon.com
  - gmail.com
  - docs.google.com
  - youtube.com
  - instagram.com
  - facebook.com
  - x.com
  - linkedin.com
  - reddit.com
  - github.com
  - reuters.com (not logged in)
  - cnn.com (not logged in)

reuters.com (cont'd)

TCP/TLS CONNECTIONS WITH HTTP GETS



versations · reuters_3.pcapng

Ethernet · 1 | IPv4 · 9 | IPv6 · 17 | TCP · 30 | UDP · 3

Address A	Port A	Address B	Port B	Bytes	Stream ID	Bytes A → B	Bytes B → A	Rel Sta
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61544	2600:9000:28bc:3800:15:5a3e:9d40:93a1	443	1 MB	6	71 kB	1 MB	3.7283
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61545	2607:f8b0:4002:c09::61	443	119 kB	8	4 kB	115 kB	4.0281
192.168.1.222	61565	104.17.209.240	443	78 kB	27	4 kB	74 kB	6.8143
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61546	2a03:2880:f011:8:face:b00c:0:1	443	76 kB	9	3 kB	73 kB	4.0333
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61576	2606:4700:4400::6812:2b5a	443	65 kB	39	7 kB	57 kB	7.7121
192.168.1.222	61559	104.18.34.222	443	59 kB	21	3 kB	56 kB	6.0636
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61573	2600:9000:24d7:a00:8:8845:1500:93a1	443	58 kB	36	2 kB	56 kB	7.6127
192.168.1.222	61556	108.156.152.123	443	44 kB	20	4 kB	40 kB	5.8471
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61551	2606:4700::6812:186f	443	35 kB	14	2 kB	32 kB	5.0276
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61560	2606:4700::6812:15ce	443	25 kB	22	2 kB	23 kB	6.4444
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61563	2606:4700::6812:562a	443	18 kB	25	4 kB	15 kB	6.6313
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61575	2600:1402:b800:40::1730:a2c5	443	16 kB	38	2 kB	14 kB	7.7115
192.168.1.222	61548	3.165.181.65	443	12 kB	11	2 kB	10 kB	4.4550
192.168.1.222	61583	3.134.198.212	443	13 kB	46	4 kB	9 kB	8.6053
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61555	2600:9000:200c:a200:8:48e:53c0:93a1	443	10 kB	19	2 kB	8 kB	5.8436
192.168.1.222	61586	3.161.136.118	443	10 kB	49	2 kB	8 kB	8.6188
192.168.1.222	61579	52.73.207.134	443	10 kB	42	2 kB	8 kB	8.0041
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61553	2600:1402:b800:63::1731:568	443	10 kB	17	3 kB	7 kB	5.7969
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61582	2600:1f18:730:b140:1366:66cb:8bf5:31b6	443	10 kB	45	3 kB	7 kB	8.5789
192.168.1.222	61585	3.134.198.212	443	8 kB	48	1 kB	6 kB	8.6106
192.168.1.222	61584	3.134.198.212	443	8 kB	47	1 kB	6 kB	8.6100
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61564	2600:1402:b800:d8c::11a6	443	8 kB	26	3 kB	6 kB	6.6843
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61549	2600:1402:b800:c8f::11a6	443	8 kB	12	2 kB	6 kB	4.7071
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61577	2606:4700:20::ac43:4acf	443	8 kB	40	2 kB	6 kB	7.7240
192.168.1.222	61574	18.244.198.33	443	8 kB	37	2 kB	6 kB	7.7109
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61554	2600:1402:b800:63::1731:568	443	7 kB	18	2 kB	5 kB	5.8131
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61568	2606:4700:4400::ac40:9b77	443	8 kB	30	2 kB	5 kB	7.0318
192.168.1.222	61587	74.119.117.16	443	7 kB	50	2 kB	5 kB	8.6194
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61566	2606:4700:4400::ac40:9b77	443	7 kB	28	2 kB	5 kB	6.8278
2600:1700:720:2f10:1d9d:ea66:4a04:ea3f	61562	2606:4700::6812:562a	443	6 kB	24	2 kB	4 kB	6.6296

From Wireshark

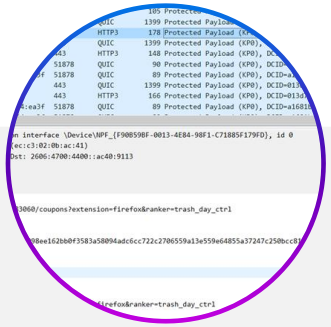
So, are web pages transferred mostly over lean connections?

BASED ON THE EMPIRICAL INVESTIGATION

- Probably not. The investigated **logged in** web pages seemed to
  - transfer large “web content” of 168KB up to 3.5MB over just a few “chubby” connections
  - which come down over HTTP/3 (QUIC) and HTTP/1.1, HTTP/2.0 (TLS 1.2, 1.3), and
  - include many, lean connections like in Cloudflare’s Blog.

- The many, lean connections seemed to serve mostly “peripheral web content”
  - Tracking, ads, identity, geolocation etc
  - HTTP 304 (for cached elements)
  - Small elements (e.g. javascript, json)
  - HTTP errors or redirects

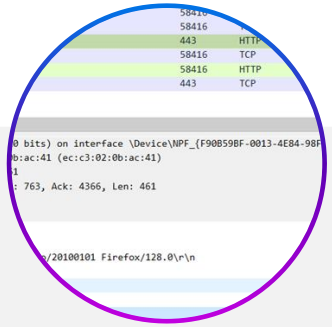
Some lean connection examples



Browser Plugin

7KB over QUIC from
capitaloneshopping.com

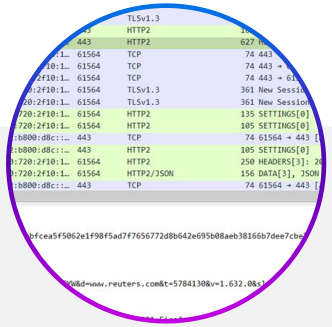
(Ads, Shopping)



linkedin.com

5KB over TCP/TLS from
li.protechts.net

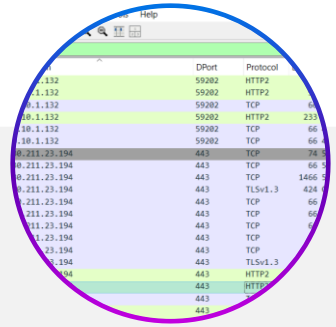
(Ads)



reuters.com

6KB over TCP/TLS from
c.go-mpulse.net

(Tracking)



msn.com

6KB over TCP/TLS from
api.btloader.com

(“Adblocking-resilient” Ads)

Takeaways

- +15KB for ML-DSA is a lot, let's trim it (e.g. draft-ietf-tls-cert-abridge, and more)

- Web pages vary a lot.
- The "chubby web content" connections will not be impacted by ML-DSA much,
- but the lean "peripheral web content" connections will.
  - Will that affect the web page's Web Metrics?
    - Probably not much, because most of this content is not "rendered".
    - But, we won't know unless we test...

- Let's start investigating Web Metrics to evaluate the impact
  - TLS handshakes and TTFB give an intuition, but not the real impact.

Thank you!

kpanos@amazon.com