Freie Universität Berlin

QUIC Handshake Classification API @ IETF 115 Hackathon

Marcin Nawrocki, Jonas Mücke

{marcin.nawrocki, jonas.muecke}@fu-berlin.de

Design goals of QUIC handshakes.

Reduce round trip times.

TCP/TLS/HTTP handshakes coalesced into 1RTT.

Prevent UDP amplification attacks.

RFC limits response size to 3x of an (unauthenticated) request.

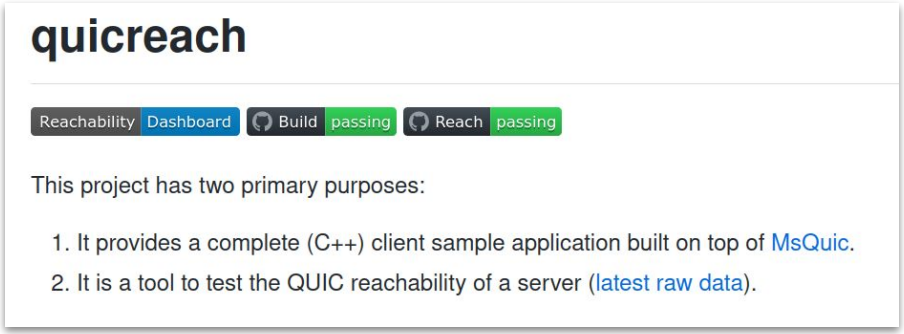
Design goals of QUIC handshakes.

Reduce round trip times

Do deployments comply with RFC 9000?

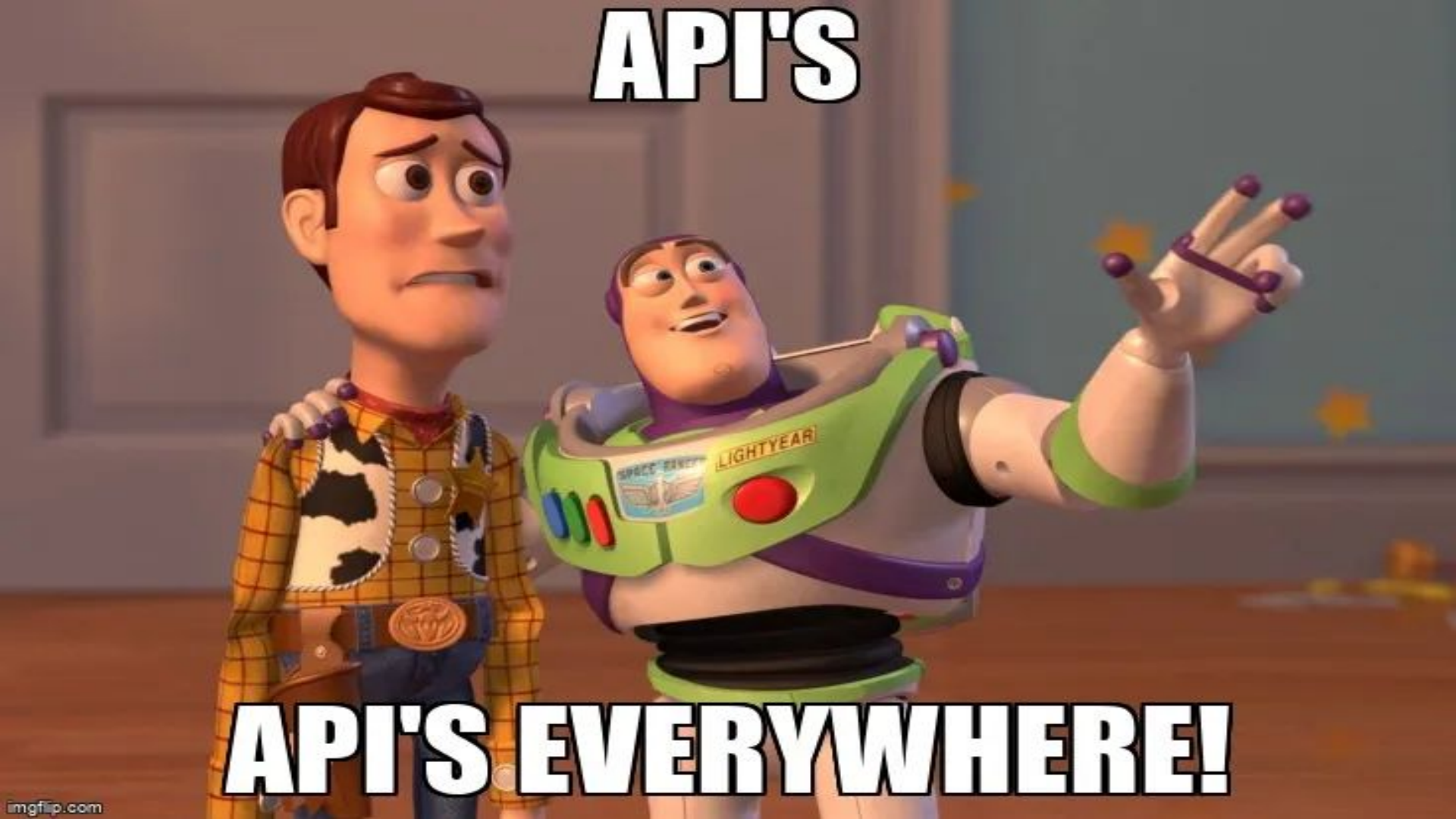
RFC limits response size to 3x of an (unauthenticated) request.

Starting point: QUIC CLI tools

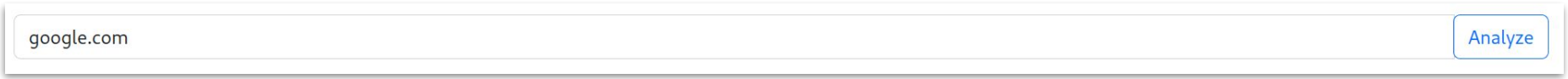


Extended to support QUIC RETRY.

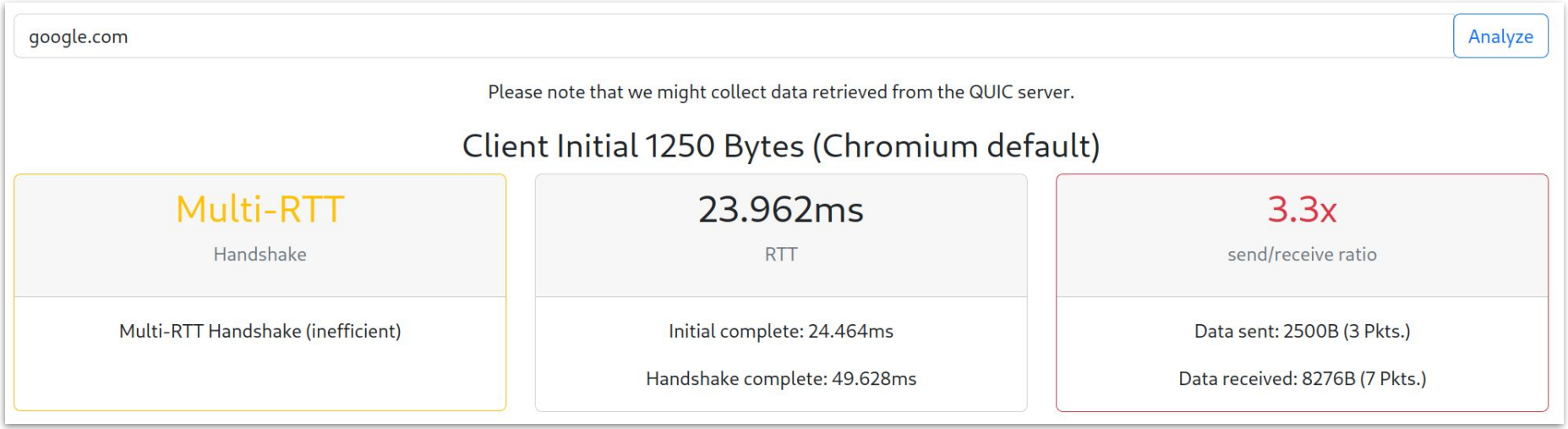
Extended to support three TLS compression algorithms.


API'S
LIGHTYEAR
API'S EVERYWHERE!
imgflip.com

Enter the name of the server you want to analyze.

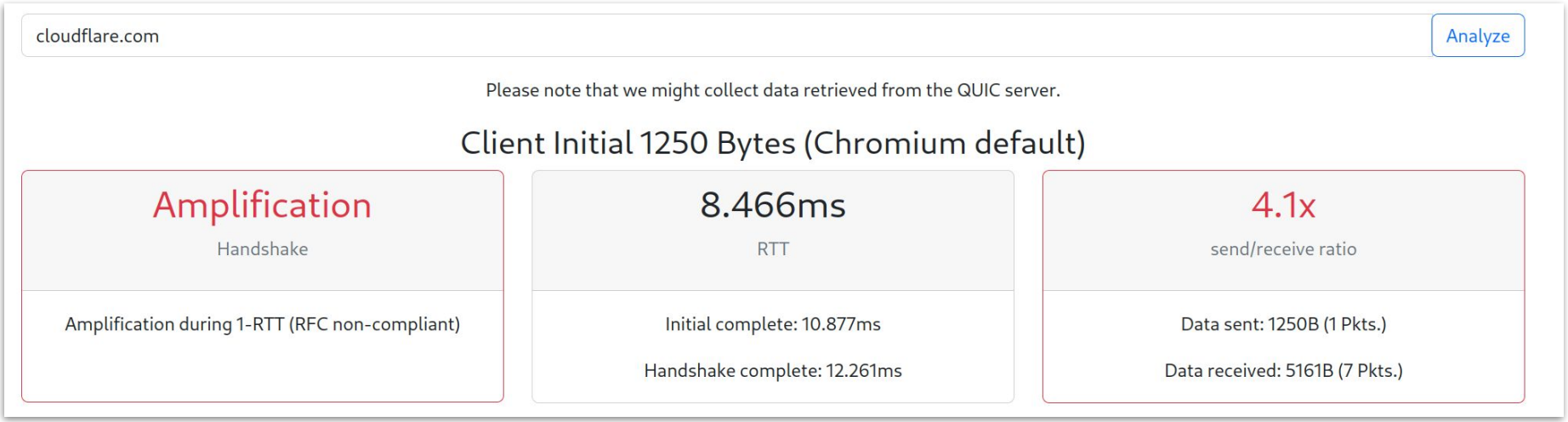


Handshake behavior: Multi-RTT



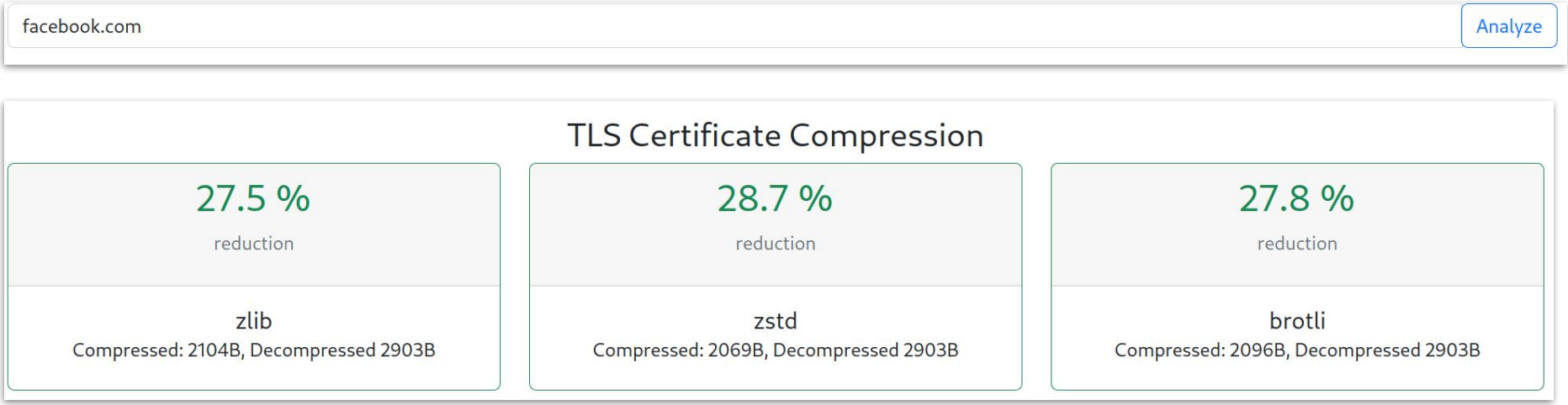
*Handshakes that do not use Retry but require multiple RTTs because of large certificates.

Handshake behavior: Amplification



*Handshakes that complete within 1-RTT but exceed the anti-amplification limit.

Save data using TLS certificate compression



Use it now! Tell us about missing handshake tests.

Currently, http://quic.nawrocki.berlin but will move to

https://understanding-quic.net

Use it now! Tell us about missing handshake tests.

Currently, http://quic.nawrocki.berlin but will move to

https://understanding-quic.net

We want to foster discussions about the good, bad, and ugly QUIC handshakes to improve deployment ;).