

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

quicreach

Reachability Dashboard Build passing Reach passing

This project has two primary purposes:

1. It provides a complete (C++) client sample application built on top of [MsQuic](#).
2. It is a tool to test the QUIC reachability of a server ([latest raw data](#)).

Extended to support QUIC RETRY.



crates.io v0.16.0 docs passing license BSD-2-Clause build passing

[quiche](#) is an implementation of the QUIC transport protocol and HTTP/3 as specified by the [IETF](#). It provides a low level API for processing QUIC packets and handling connection state. The application is responsible for providing I/O (e.g. sockets handling) as well as an event loop with support for timers.

Extended to support three TLS compression algorithms.

API'S

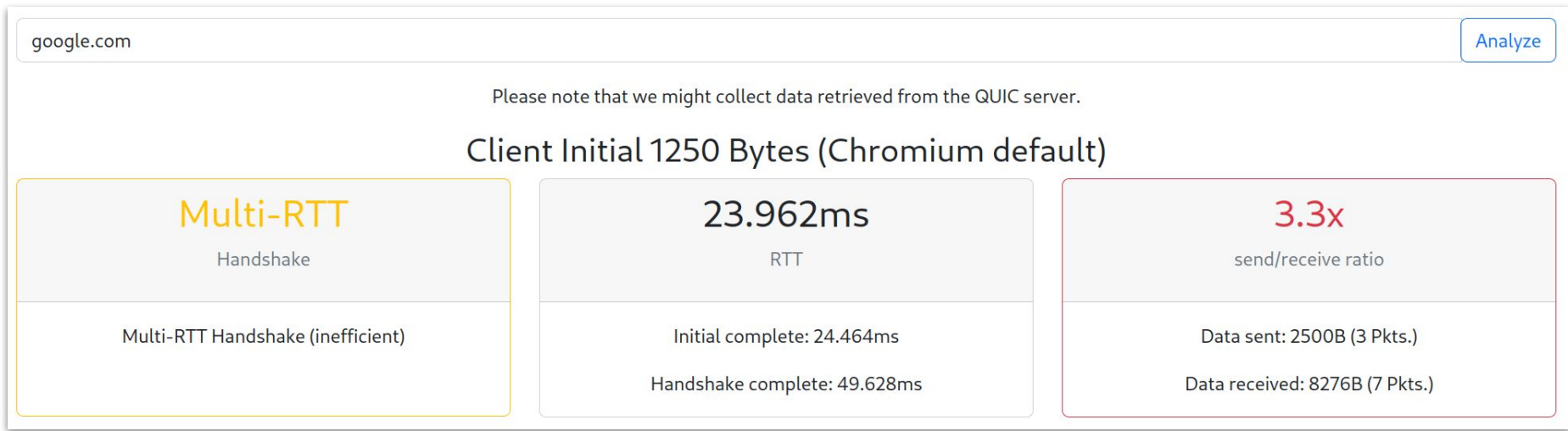
API'S EVERYWHERE!

Enter the name of the server you want to analyze.

google.com

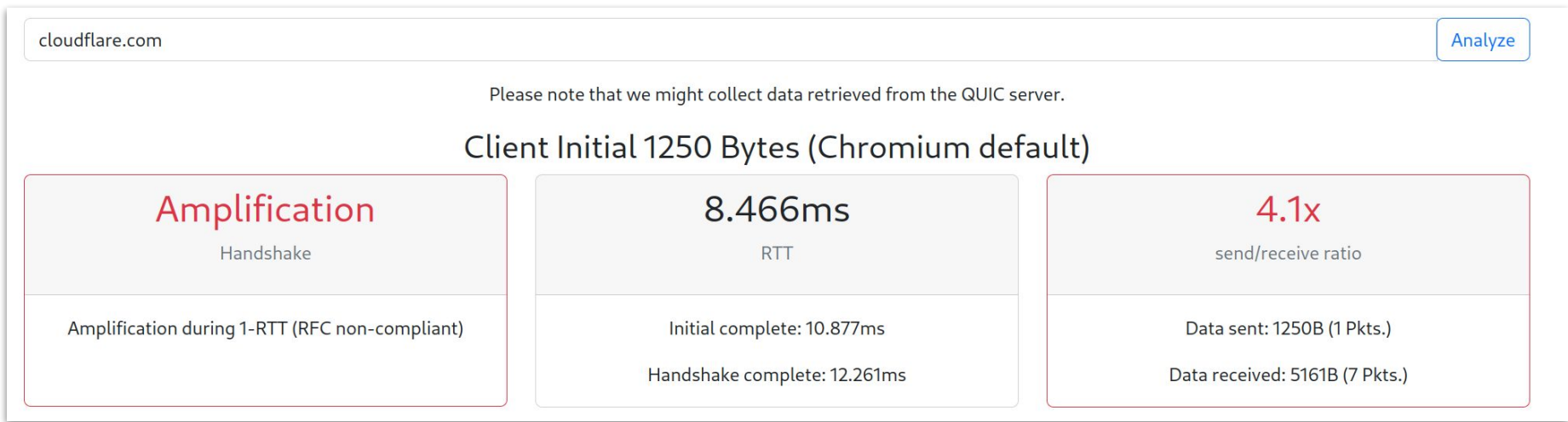
Analyze

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

facebook.com

Analyze

TLS Certificate Compression

27.5 %

reduction

zlib

Compressed: 2104B, Decompressed 2903B

28.7 %

reduction

zstd

Compressed: 2069B, Decompressed 2903B

27.8 %

reduction

brotli

Compressed: 2096B, Decompressed 2903B

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 ;).