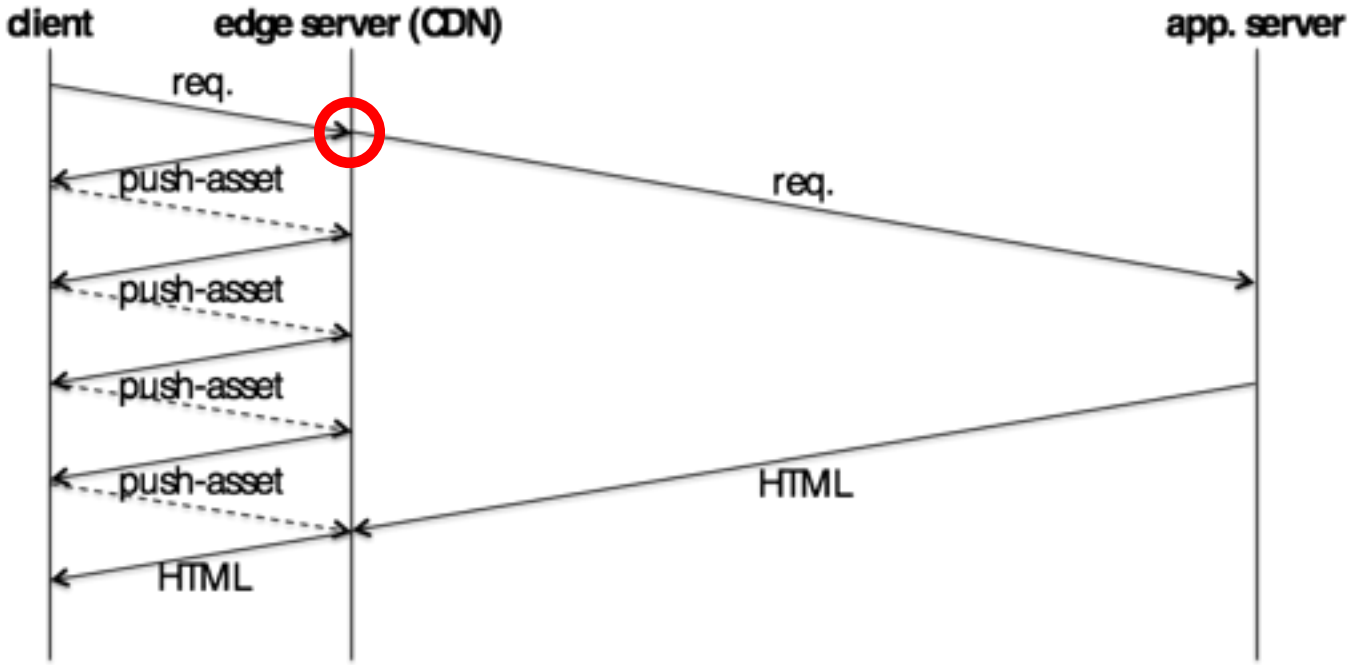
# Cache Digests for HTTP/2

DeNA Co., Ltd.

Kazuho Oku

# To push, or not to push

- a server *should not* push a resource already cached
  - reason: minimize consumed bandwidth
- but how to determine (at the point colored in red)?



# Cache Digests for HTTP/2

- client sends a *digest* of resources cached
- a digest is:
  - a Golomb-coded set containing the hashes of fresh resources being cached
  - scope is the origin
- authors: me, Mark Nottingham

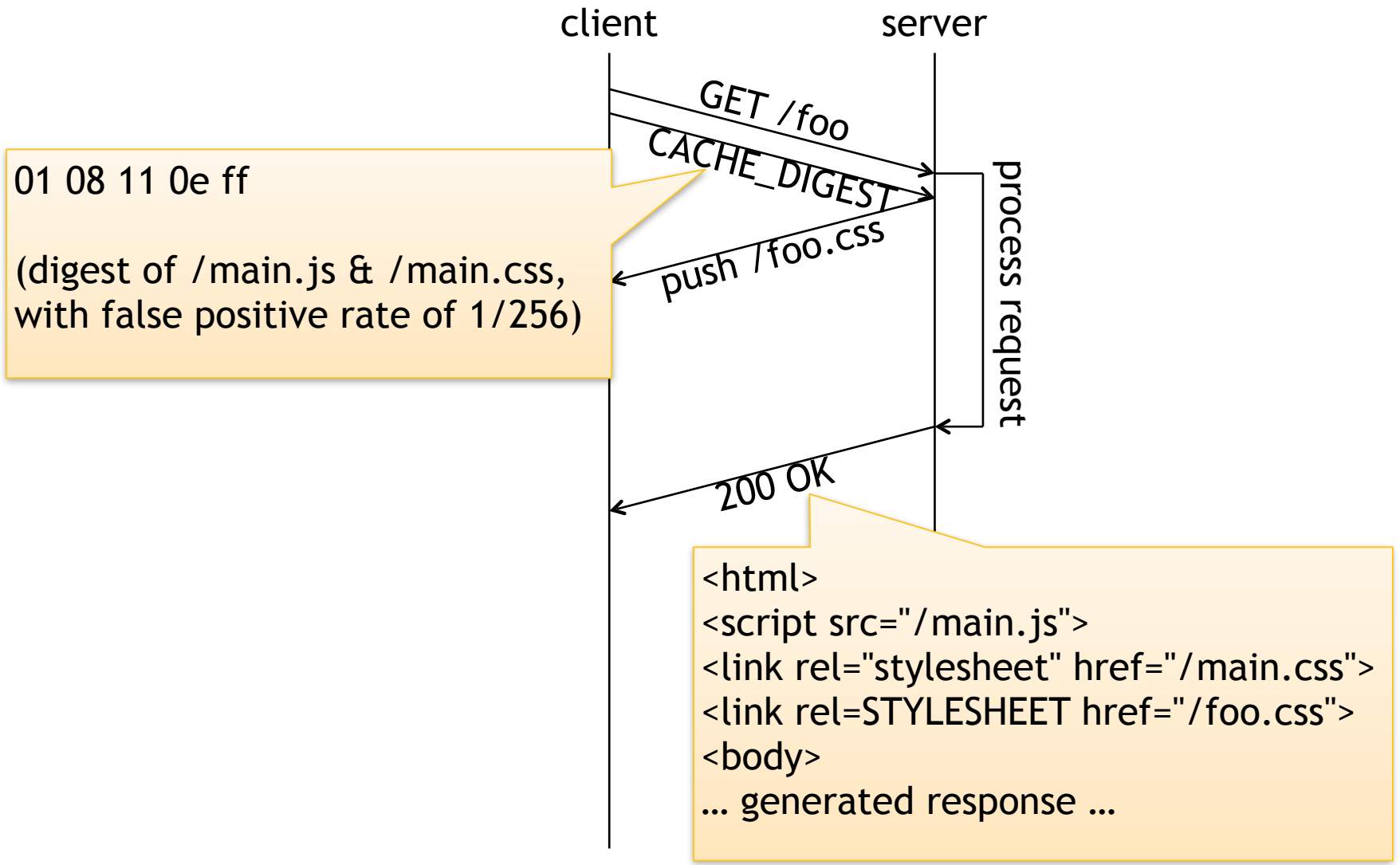
## Size of the digest

- uses Golomb-coded sets
  - compressed form of bloom filter
  - has false positives, no false negatives
    - i.e. non-cached resources marked as cached, but not the reverse
  - roughly *(1.x + log2(P)) * number_of_urls* bits
    - i.e. 1 byte-per-URL if false positive rate is set to 1/128 (P=128)
  - small P (e.g. P=2) would still be useful
    - since *some* of the resources can be detected as non-cached and be pushed

# CACHE_DIGEST frame

- CACHE_DIGEST frame
  - stream_id is fixed to 0
  - contains digest covering resources belonging to the origin of the *previous* HEADERS frame
    - reason: don't delay the arrival of the request
- client typically sends CACHE_DIGEST only once per connection, per origin
  - server can memoize what it has sent over the connection to avoid resend

# Example sequence



## Security Considerations

- cache-based fingerprinting becomes passive
  - possible mitigation: alter the cache state when other tracking identifiers (e.g. Cookie) is cleared

## Implementation Status

- server-side:
  - H2O
    - variant of the draft (uses Cookie)
  - mod_h2 (Apache)
    - variant of the draft (uses H1 header)
- client-side:
  - https://github.com/Jxck/dispenser.js (WIP)
    - ServiceWorker; modifies the cookie recognized by H2O

## Discussion after submission

- why not use HTTP header?
  - send digests using ServiceWorker
- customizable scope?
  - when connecting to a server possessing a wild-card certificate
- digest of stale resources as well?
  - need to formalize how to push validation info.
- partial vs. complete digest
  - define a flag to distinguish them, so that the server can change the push strategy

Comments?