A quick update on IETF Documents

Special-Use Names Problem Statement

draft-ietf-dnsop-sutld-ps

Extended DNS Errors

draft-wkumari-dnsop-extended-error

DNS Errors are not expressive

- So errors are overloaded, and applications have to "guess" which is right
- This causes both debugging difficulty **and** security issues
- REFUSED is used for ACLs and Lame Delegations
  - Hard to know which.
- SERVFAIL is used for, well, many things, including DNSSEC failures
  - ... and this causes security issues

Mommy said "No!", I'll ask Daddy instead.

- 12.6% of people perform DNSSEC validation
- 4.3% of people fall back to non-validating resolvers
- So, 34% of DNSSEC users are not actually getting DNSSEC protection.

Extended Errors

- Annotate DNS Errors with additional information
  - ...and a hint about what to do
    - e.g: a stub probably shouldn't ask the next, non-validating recursive
- Planning on defining a number of errors, getting DNSOP to define more
  - ... and an extensible registry to permit, er, extension.

TTL Stretching / Serve Stale

draft-wkumari-dnsop-ttl-stretching,
draft-tale-dnsop-serve-stale

Remember the Dyn attacks?

- Fun, weren't they?
- Paypal, Netflix, Github, Twitter, Spotify, Amazon, PagerDuty, Fastly, Cloudflare, many others
- Attacker capabilities keep going up
- Not really Dyn's "fault" - users want short TTLs, means authoritative servers need to be always reachable
- Users unwilling to pay sufficient to keep ahead

Proposal

If the recursive server cannot reach the authoritative server, simply extend the TTL

Stale bread is better than no bread at all.

Open Questions

1. Is this actually true?
2. For how long can we do this?
3. Aggressive retry?

All that Matters

DNS RR for TLS SNI

draft-schwartz-dns-sni

All Bad

Purpose

- HTTPS / TLS encrypts the conversation
- and DPRIVE will (soon) protect the DNS lookup
- but the TLS SNI still leaks the site name
- revealing where you are going
- Like www.bieberfever.com or more seriously www.hrc.org

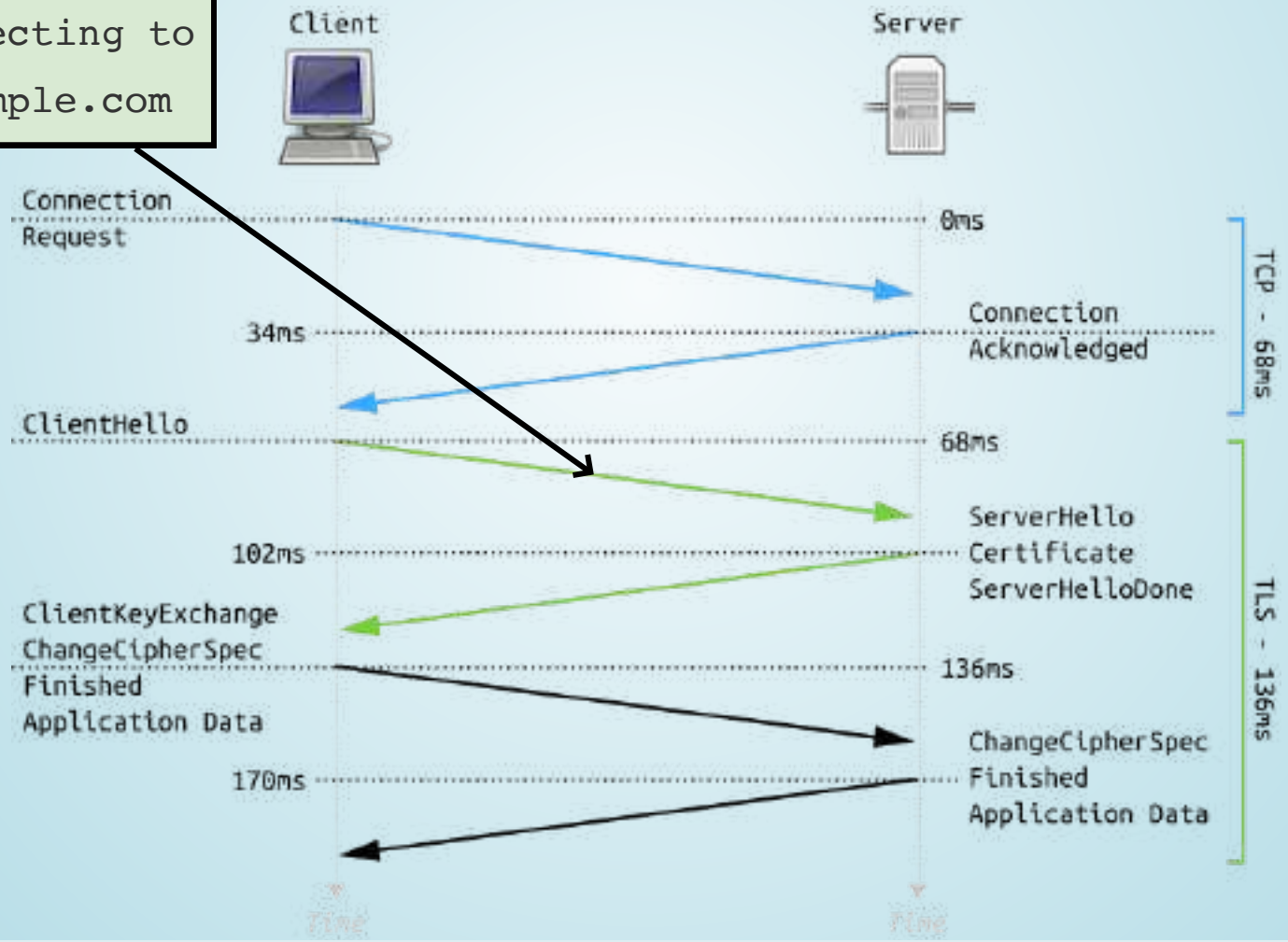
Metadata is important!

"We kill people based on metadata."

-- Former NSA director Michael Hayden

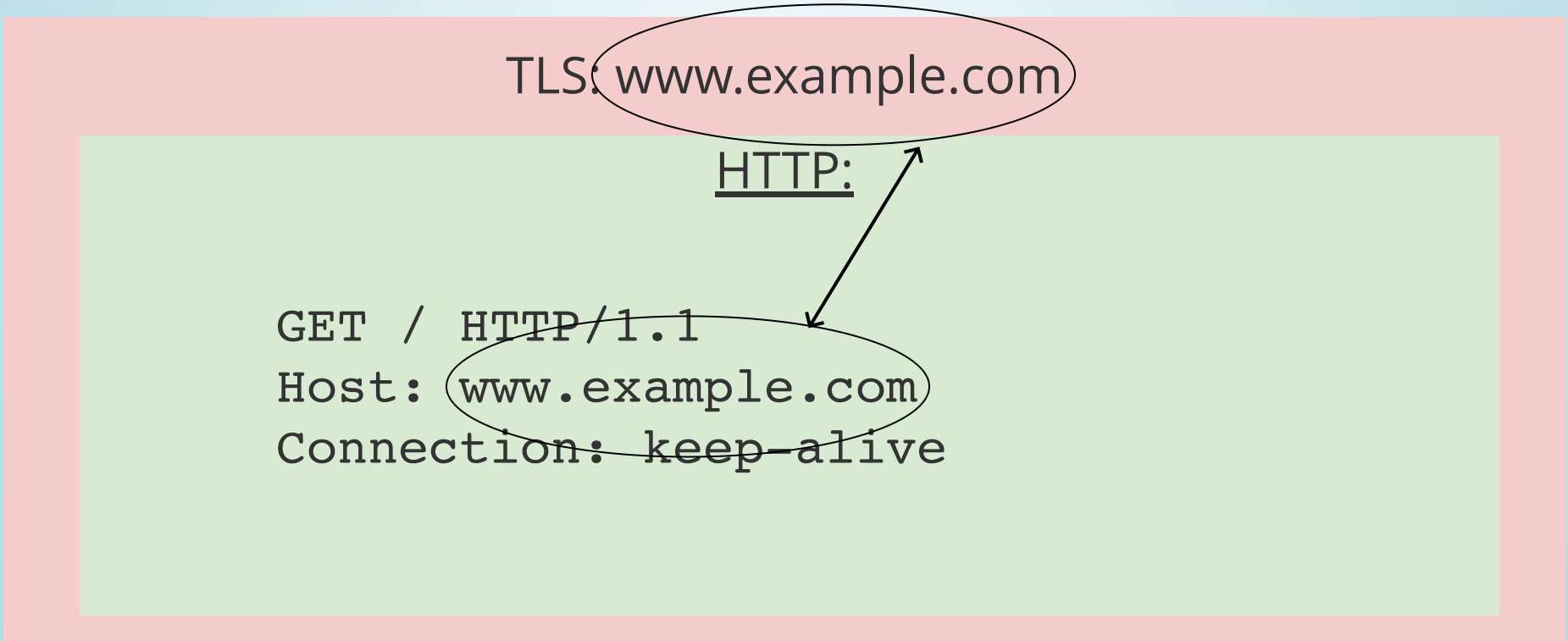
Trust
TLS SNI

I'm connecting to www.example.com



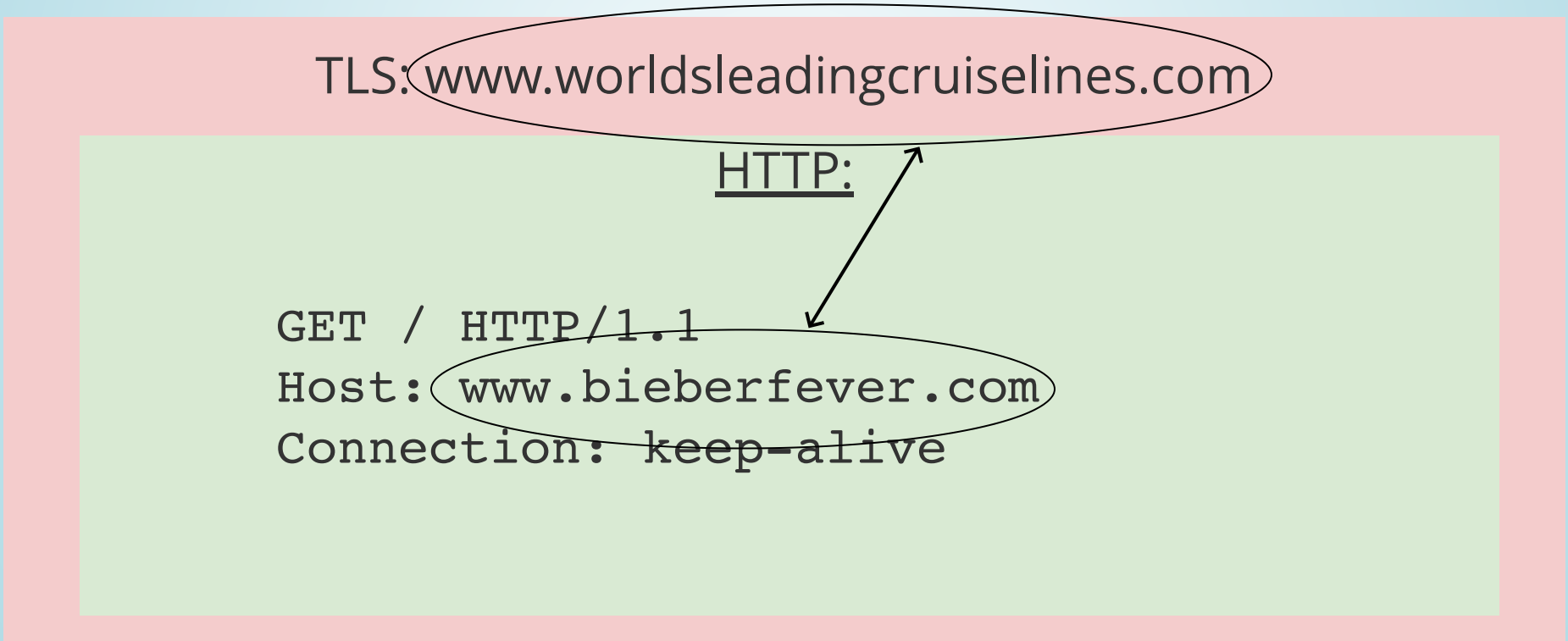
Overboard

TLS SNI



Change Me

Domain Fronting

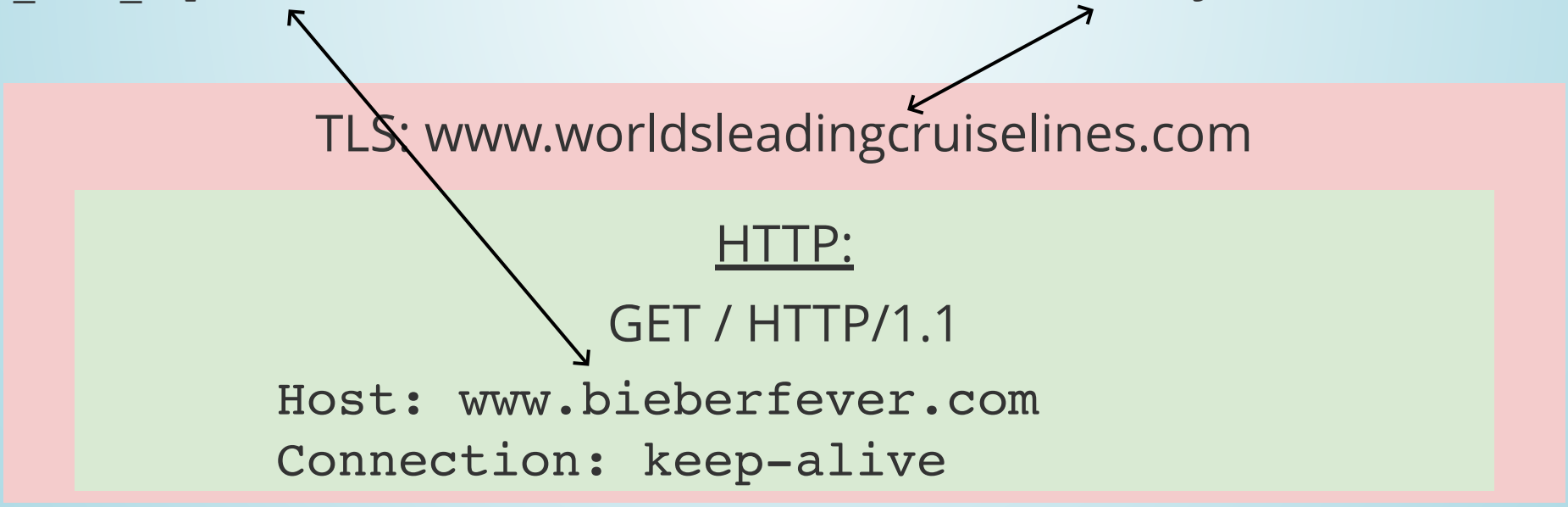


Nothing like us

The proposal

- Publish which "outer" hostname to use for a given "inner" hostname

```
_443._tcp.www.bieberfever.com.  IN SNI www.worldsleadingcruiselines.com
```



Believe

Questions?
(pray)