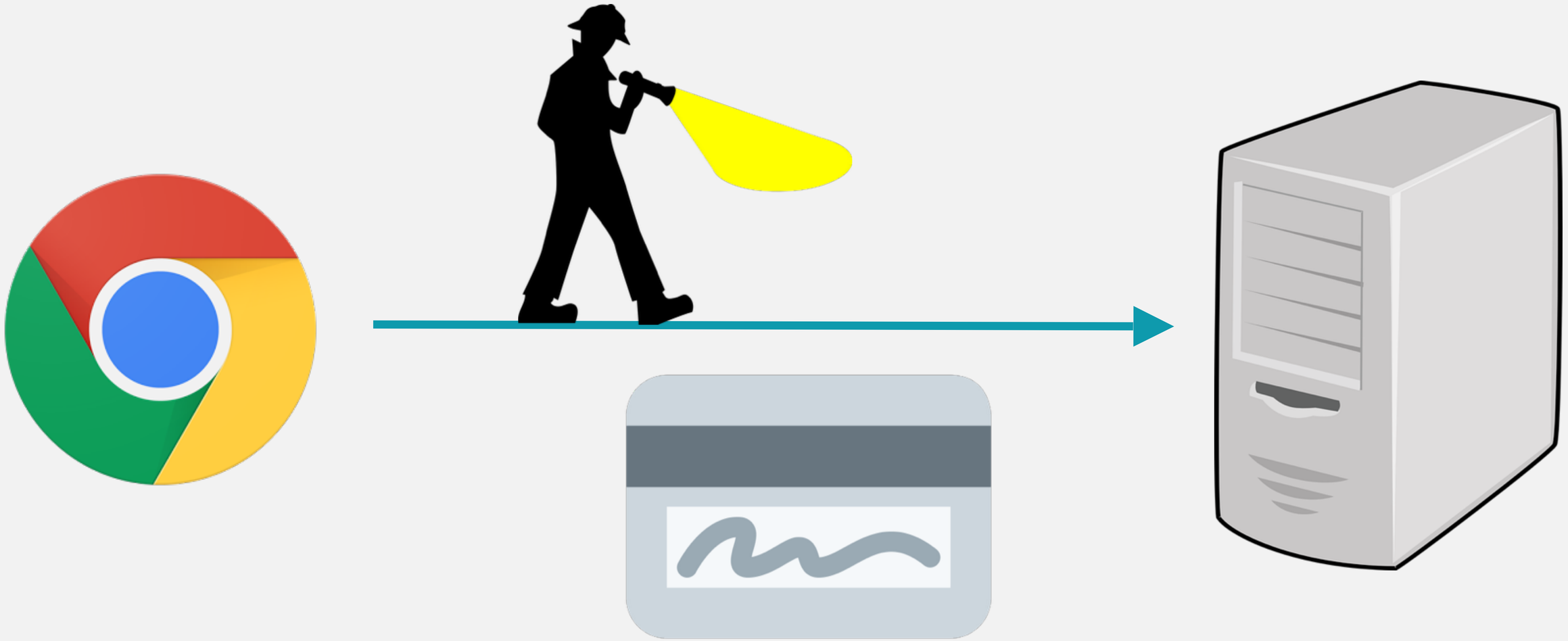
HTTPS:
Securing the Foundations

PROGRESSIVE WEB APP

ROADSHOW 2016

With great power
comes great responsibility.



Why HTTPS?

Why HTTPS?

Identity

Who are you talking to?

Why HTTPS?

Identity

Who are you talking to?

Confidentiality

Who can read your data?

Why HTTPS?

Identity

Who are you talking to?

Confidentiality

Who can read your data?

Integrity

Who can modify your data?

But what about…

Performance

Cost

Maintenance

But HTTPS is too hard…

1. My site doesn't need it!
2. It'll cause performance problems and I'll lose money
3. It costs too much to implement
4. Critical 3rd party dependancies may not support HTTPS yet

But HTTPS is too hard…

1. **My site doesn't need it!**
2. It'll cause performance problems and I'll lose money
3. It costs too much to implement
4. Critical 3rd party dependancies may not support HTTPS yet

APIs that require HTTPS

- Service Workers
- getUserMedia
- Push Notifications
- App Cache
- Encrypted Media Extensions
- Geo Location
- HTTPS/2

For more information, see:
https://www.chromium.org/Home/chromium-security/prefer-secure-origins-for-powerful-new-features

APIs that require HTTPS

- **Service Workers**
- getUserMedia
- Push Notifications
- App Cache
- Encrypted Media Extensions
- Geo Location
- HTTPS/2

For more information, see:
https://www.chromium.org/Home/chromium-security/prefer-secure-origins-for-powerful-new-features

HTTPS is a crucial part of the user experience

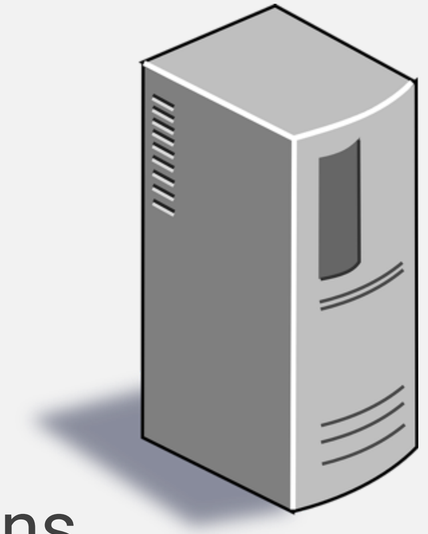
It’s no longer for especially important or security-sensitive sites only.

But HTTPS is too hard…

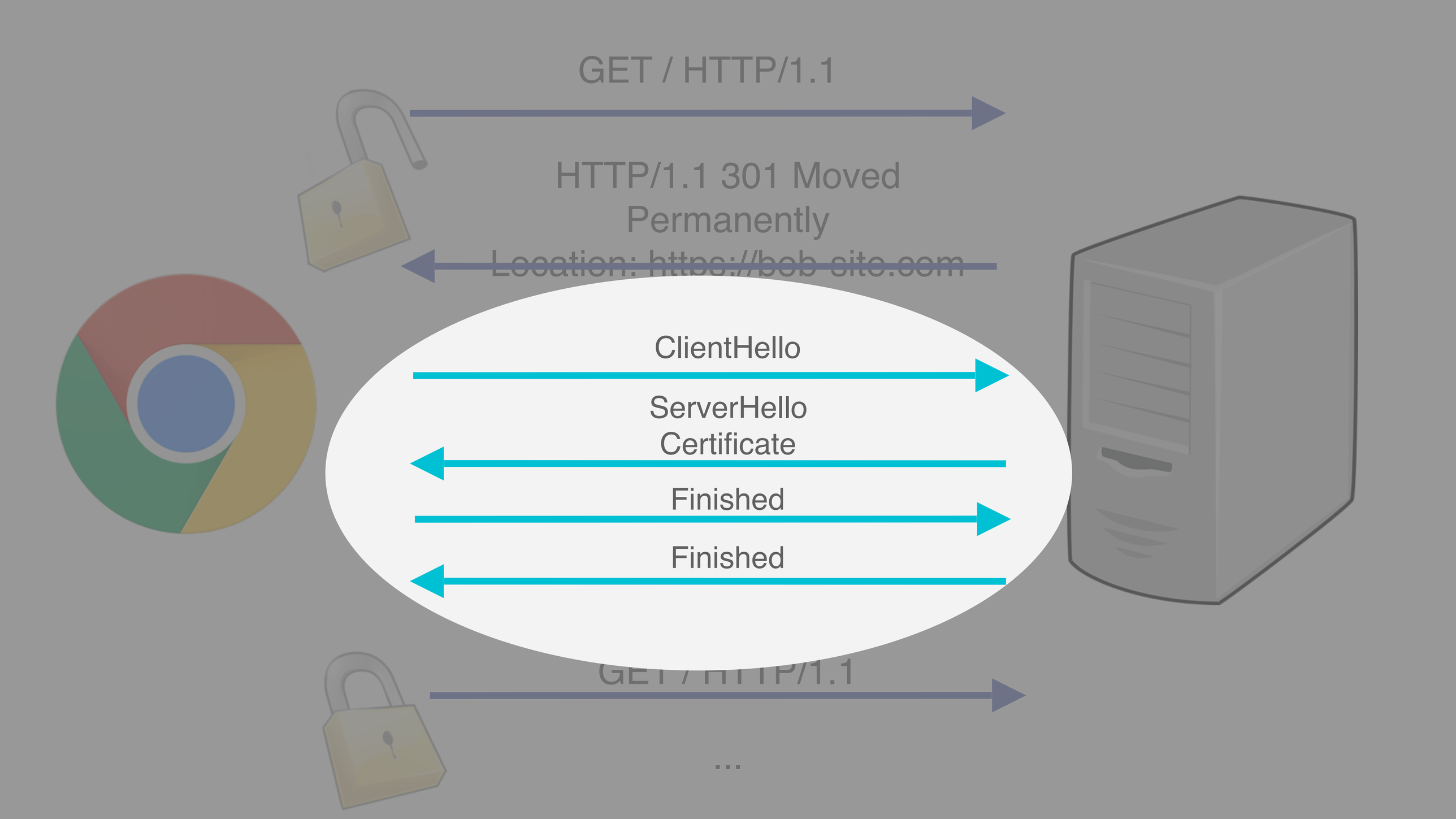
1. My site doesn't need it!
2. **It'll cause performance problems and I'll lose money**
3. It costs too much to implement
4. Critical 3rd party dependancies may not support HTTPS yet

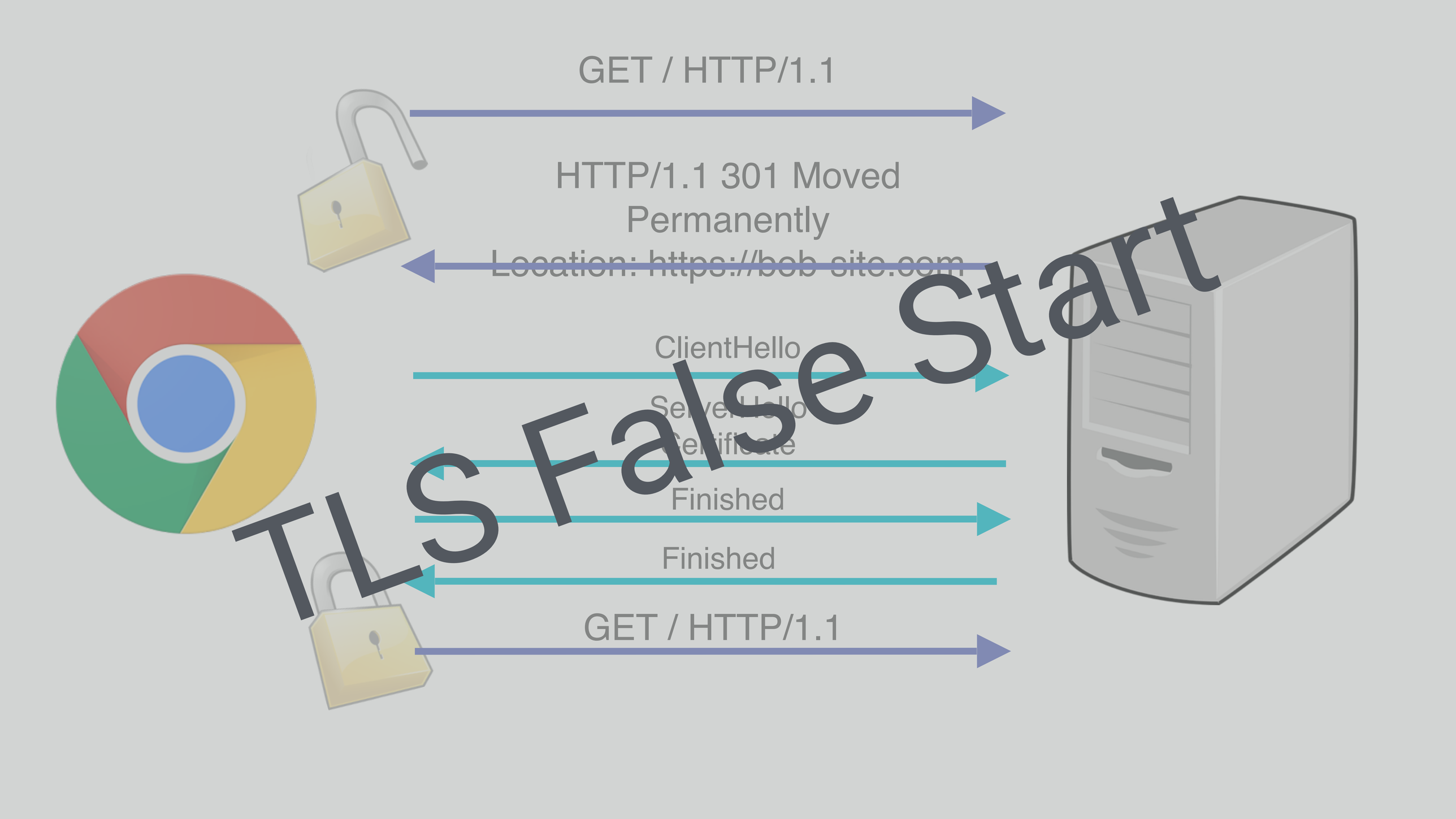
HTTP Strict Transport Security

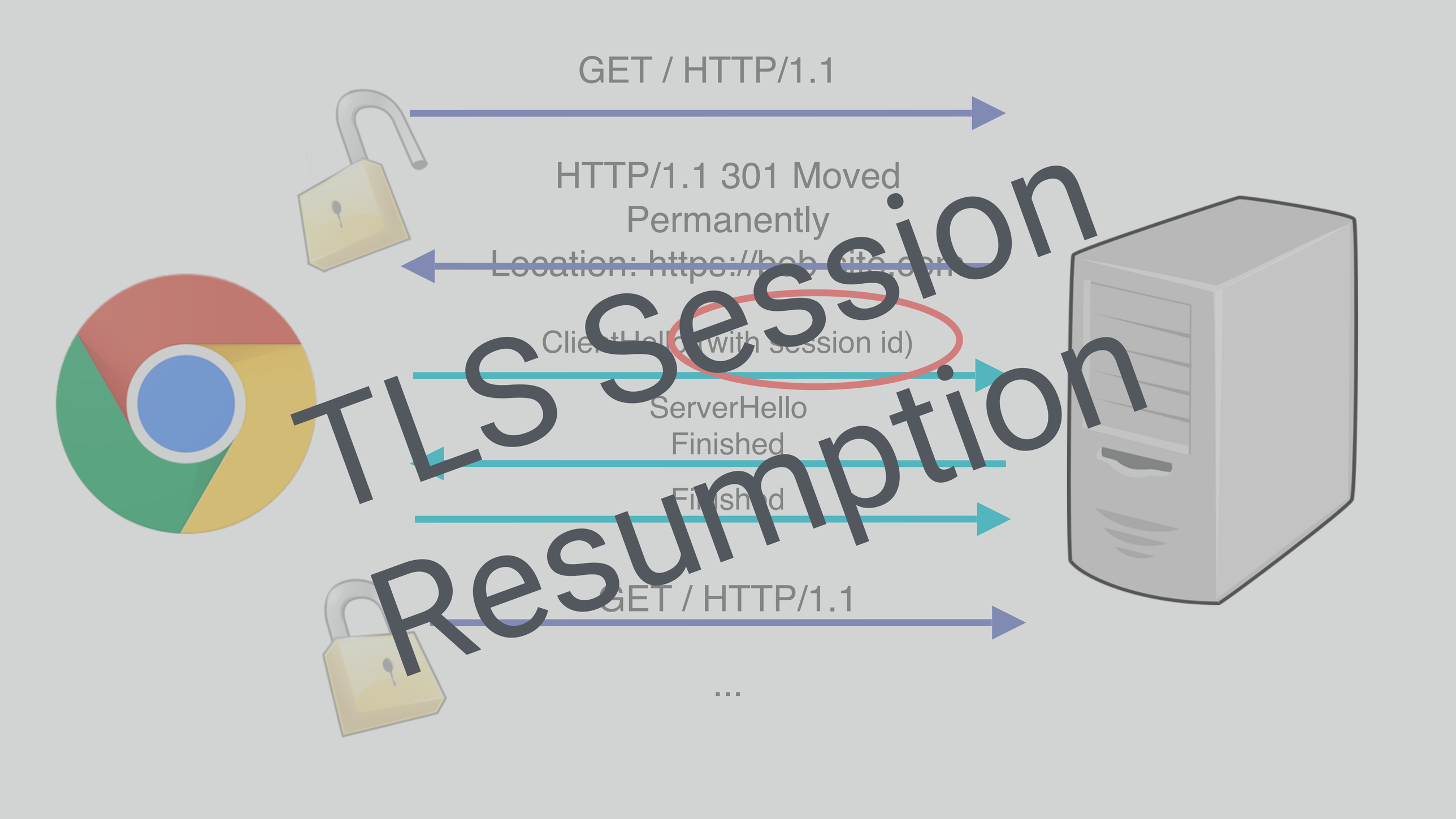
Strict-Transport-Security: max-age=2592000;
includeSubDomains



“Only access my site and all its subdomains
over HTTPS for the next month.”


GET / HTTP/1.1
HTTP/1.1 301 Moved Permanently
Location: https://bob.site.com
ClientHello
ServerHello
Certificate
Finished
Finished
GET / HTTP/1.1
...


GET / HTTP/1.1
HTTP/1.1 301 Moved Permanently
Location: https://bob-site.com
ClientHello
ServerHello
Certificate
Finished
Finished
GET / HTTP/1.1
TLS False Start


GET / HTTP/1.1
HTTP/1.1 301 Moved Permanently
Location: https://bob.site.com
ClientHello (with session id)
ServerHello
Finished
Finished
GET / HTTP/1.1
...
TLS Session Resumption

HTTPS unlocks HTTP/2

HTTP/2 unlocks massive performance wins.

When we launched [HTTPS], we saw an average of a **50ms hit for negotiation**... it was more than offset when we activated HTTP/2 a month later and saw an overall drop of ~250ms per pageview on supported devices.

- weather.com

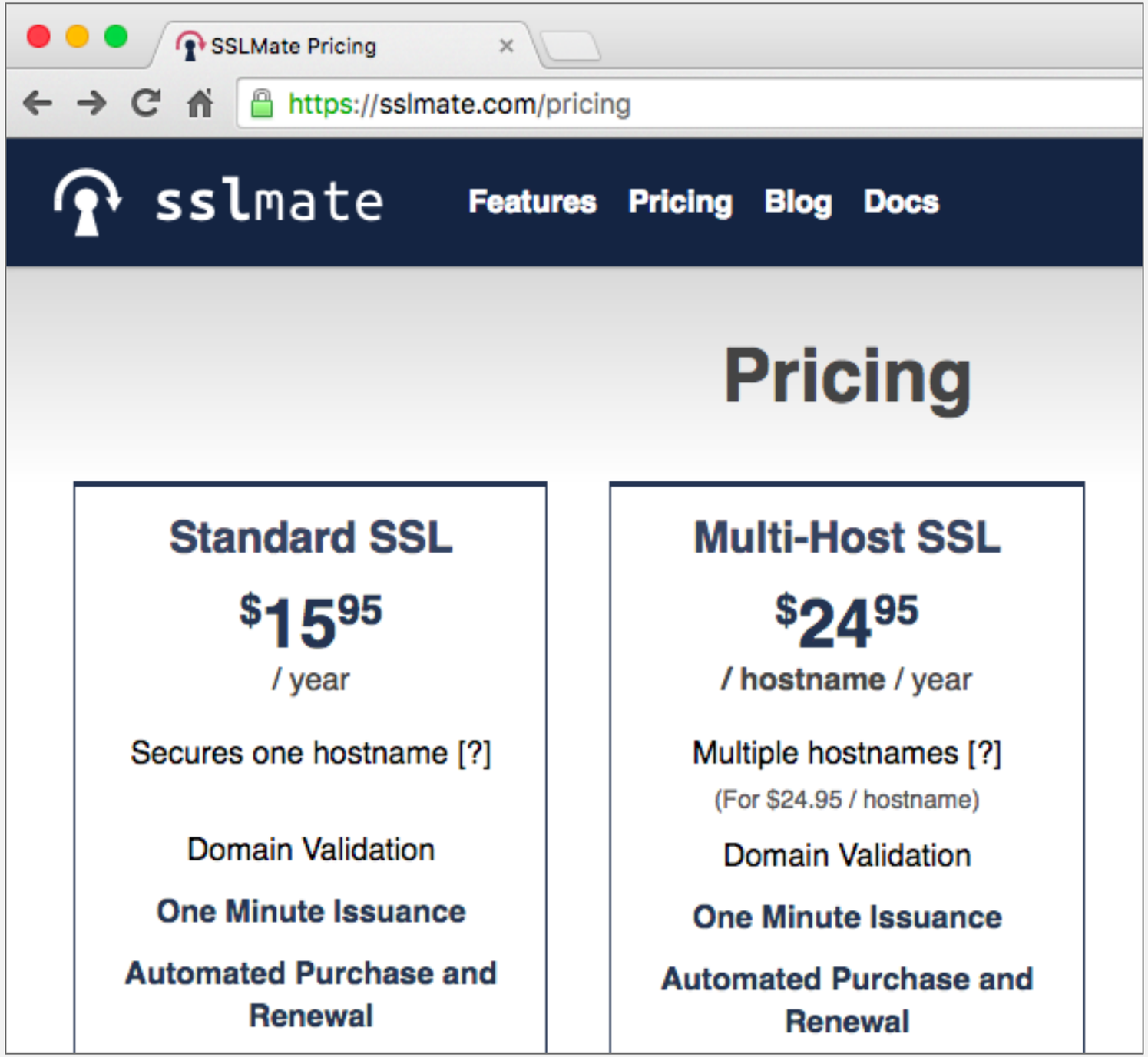
But HTTPS is too hard…

1. My site doesn't need it!
2. It'll cause performance problems and I'll lose money
3. **It costs too much to implement**
4. Critical 3rd party dependancies may not support HTTPS yet

The Cost of HTTPS

Certificate

Search Ranking

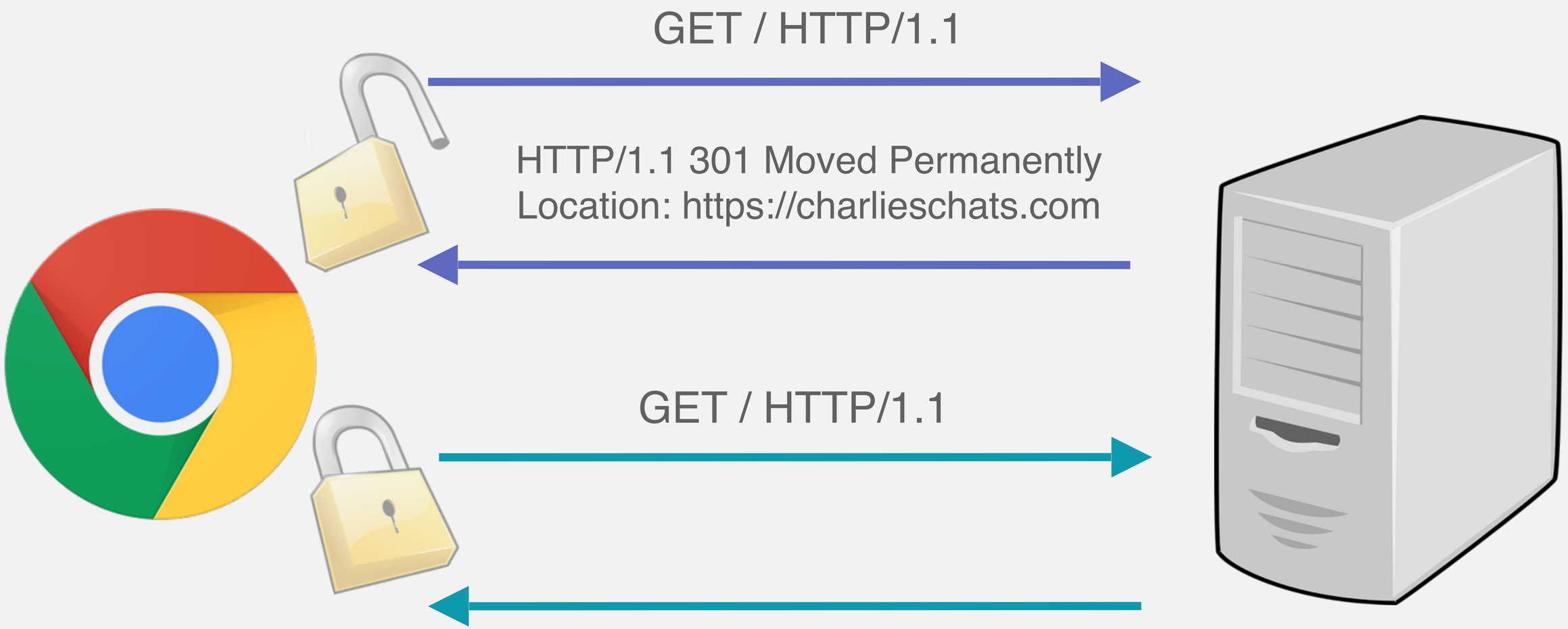

SSLMate Pricing
https://sslmate.com/pricing
sslmate
Features
Pricing
Blog
Docs
Pricing
Standard SSL
$15.95
/ year
Secures one hostname [?]
Domain Validation
One Minute Issuance
Automated Purchase and Renewal
Multi-Host SSL
$24.95
/ hostname / year
Multiple hostnames [?]
(For $24.95 / hostname)
Domain Validation
One Minute Issuance
Automated Purchase and Renewal

Let’s Encrypt

The Cost of HTTPS

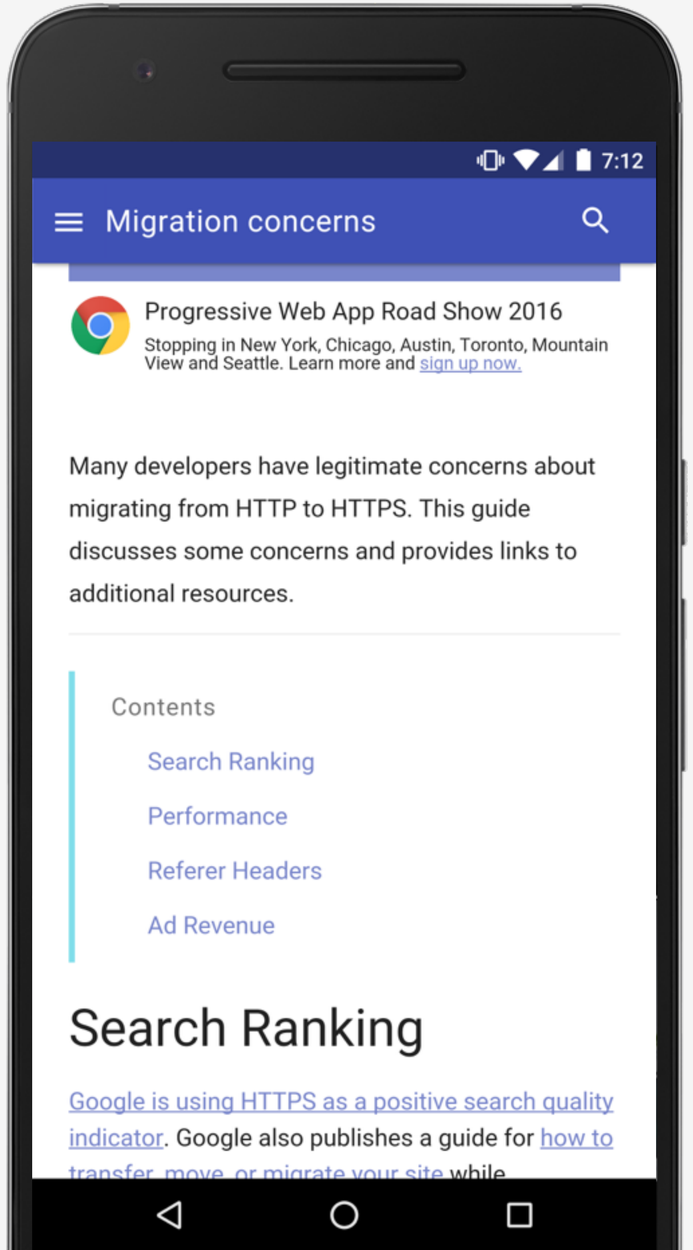
Certificate

Search Ranking


GET / HTTP/1.1
HTTP/1.1 301 Moved Permanently
Location: https://charlieschats.com
GET / HTTP/1.1
<link **rel="canonical"** href="https://charlieschats.com">

Search Ranking Guidance

developers.google.com/web/fundamentals/security/encrypt-in-transit/migration-concerns



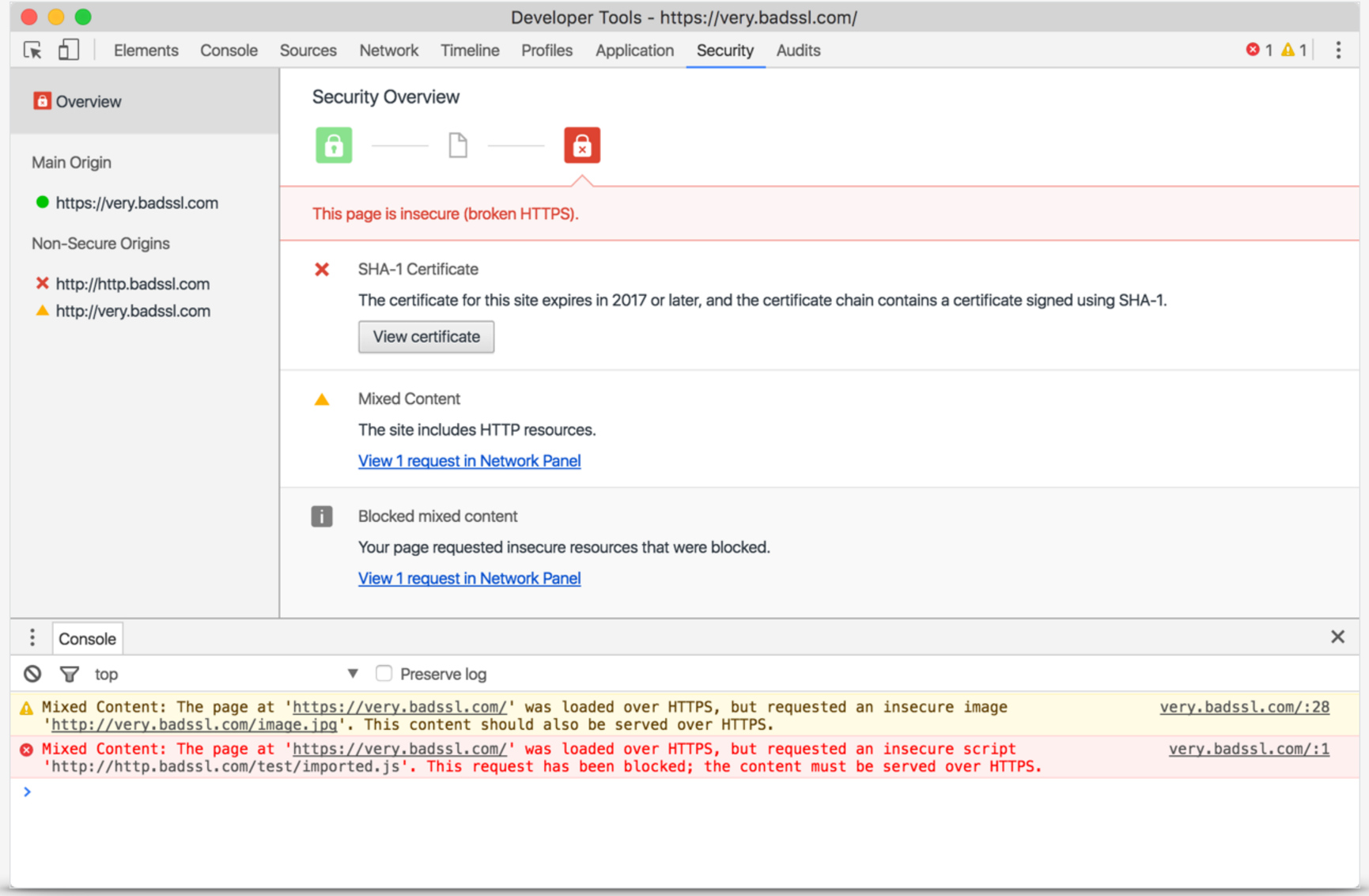
But HTTPS is too hard…

1. My site doesn't need it!
2. It'll cause performance problems and I'll lose money
3. It costs too much to implement
4. **Critical 3rd party dependancies may not support HTTPS yet**

[A] survey of our membership late last year showed **nearly 80% of member ad delivery systems supported HTTPS**.

- IAB (Interactive Advertising Bureau),
- “Adopting Encryption: The Need for HTTPS”

Chrome DevTools Security Panel



What's Next?

More resources to help

Encrypting Data in Transit

developers.google.com/web/fundamentals/security/encrypt-in-transit/

Using Content Security Policy

developers.google.com/web/fundamentals/security/csp/

Preventing Mixed Content

developers.google.com/web/fundamentals/security/prevent-mixed-content/

Thank You!