Needing the DoH

The ongoing encryption and centralization of DNS

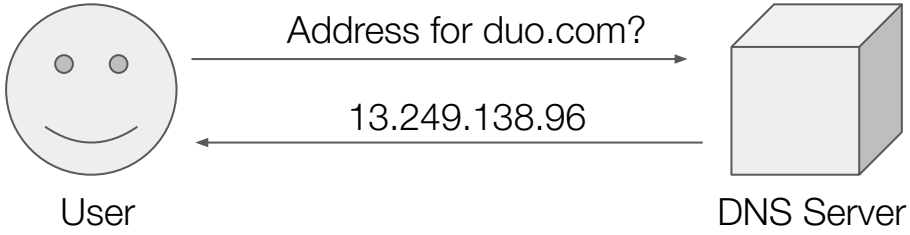
Eldridge Alexander
Duo Security
@magiceldridge

DUO LABS

DNS

The Path to Encryption

Paul Mockapetris and Jon Postel created DNS in 1983.



DUO LABS

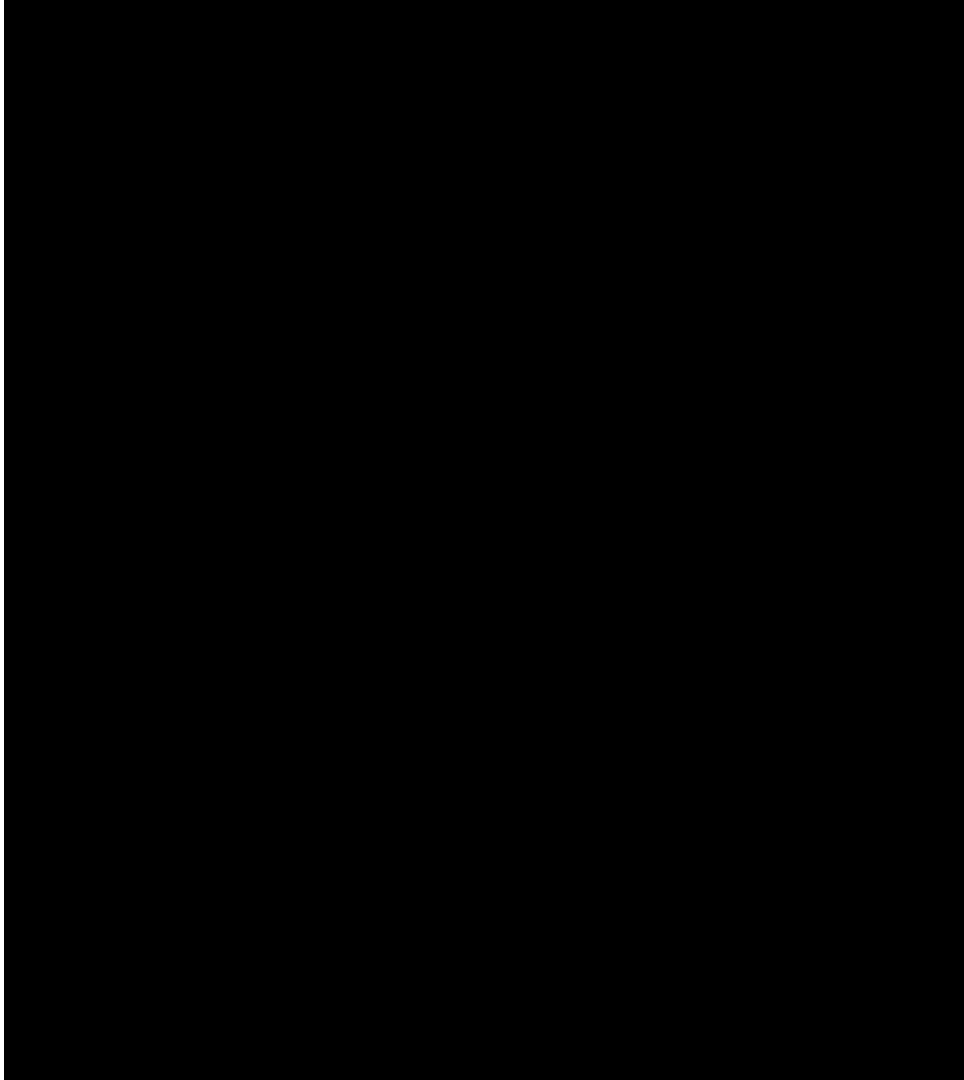
Why was it unencrypted?

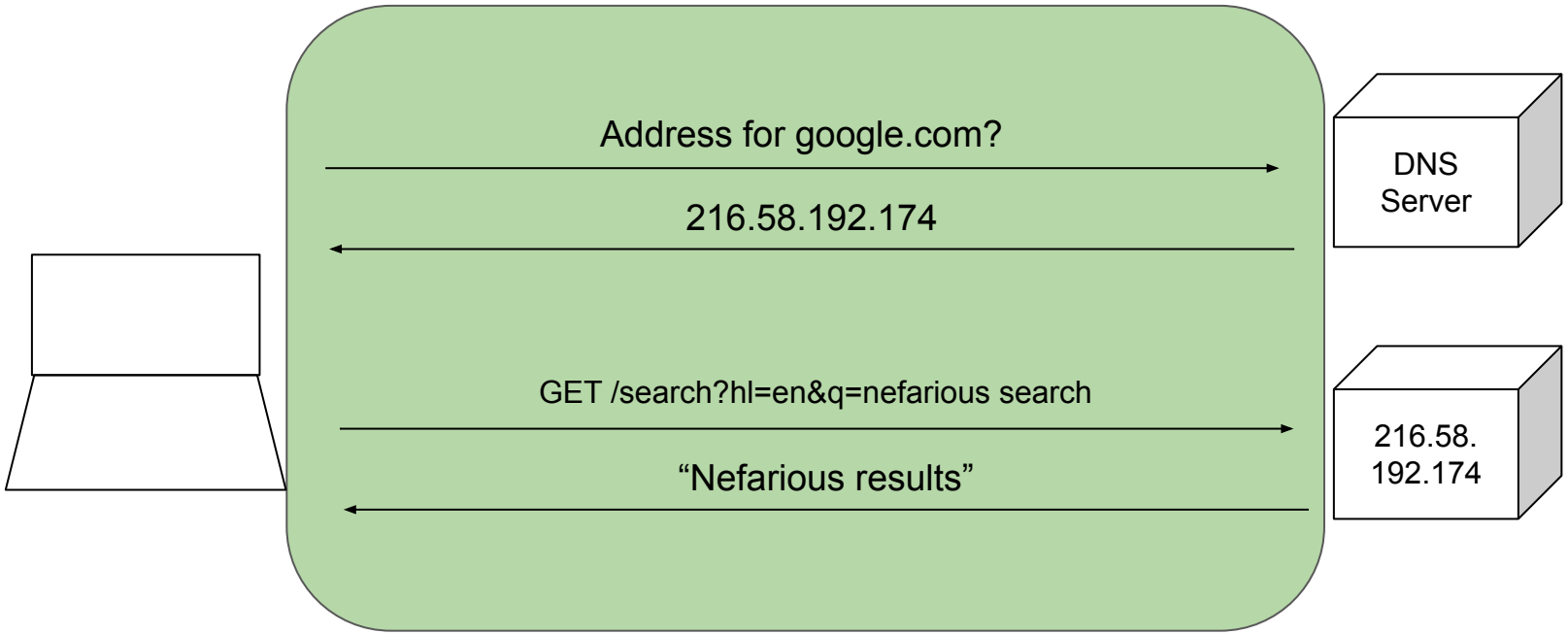
“The fact that the DNS doesn’t have much security was pretty much intentional at the start, because the problem was to get people to accept the whole idea of a distributed system, which at the time was quite controversial. People would say, “If I can’t access the network, I can’t get work done.”

- Paul Mockapetris

DUO LABS

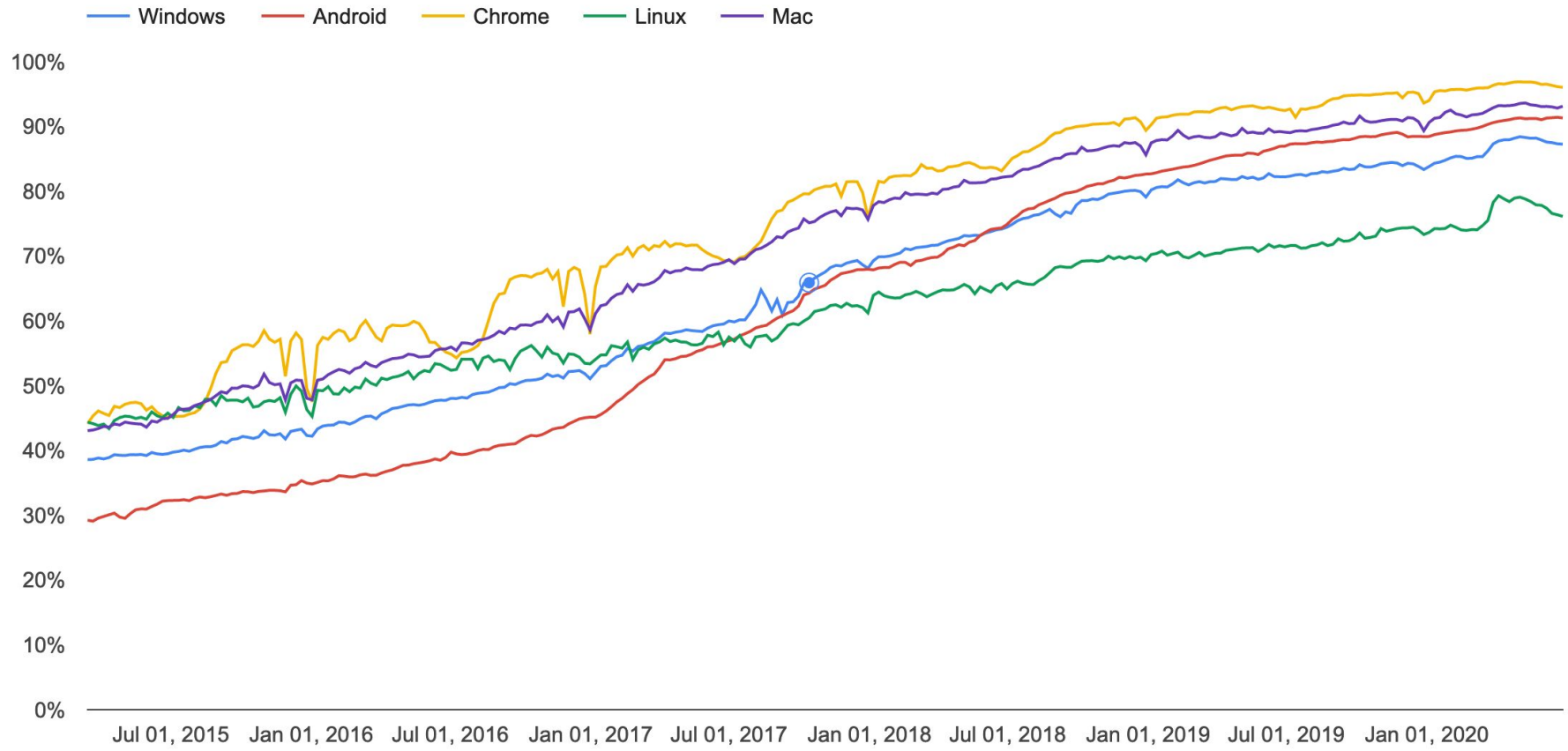
Why is this relevant now?



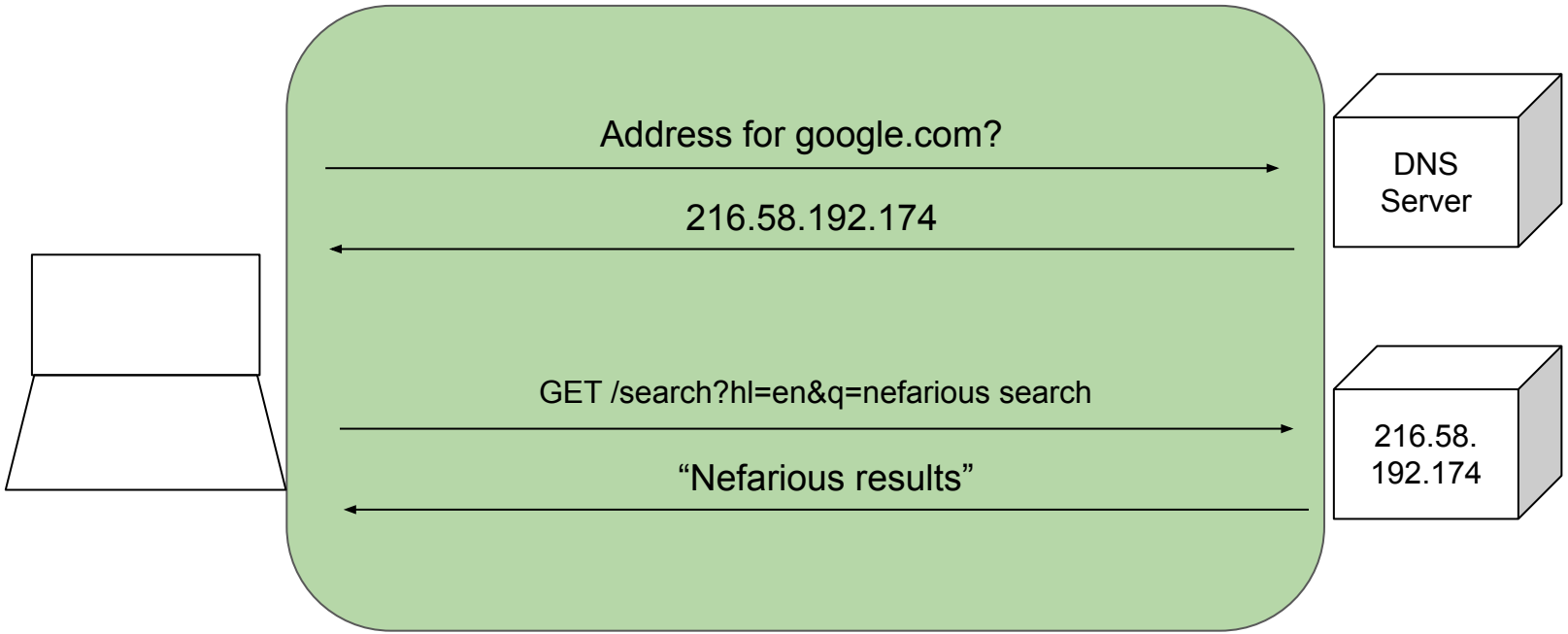

Address for google.com?
216.58.192.174
DNS Server
GET /search?hl=en&q=nefarious search
“Nefarious results”
216.58.
192.174

DUO LABS

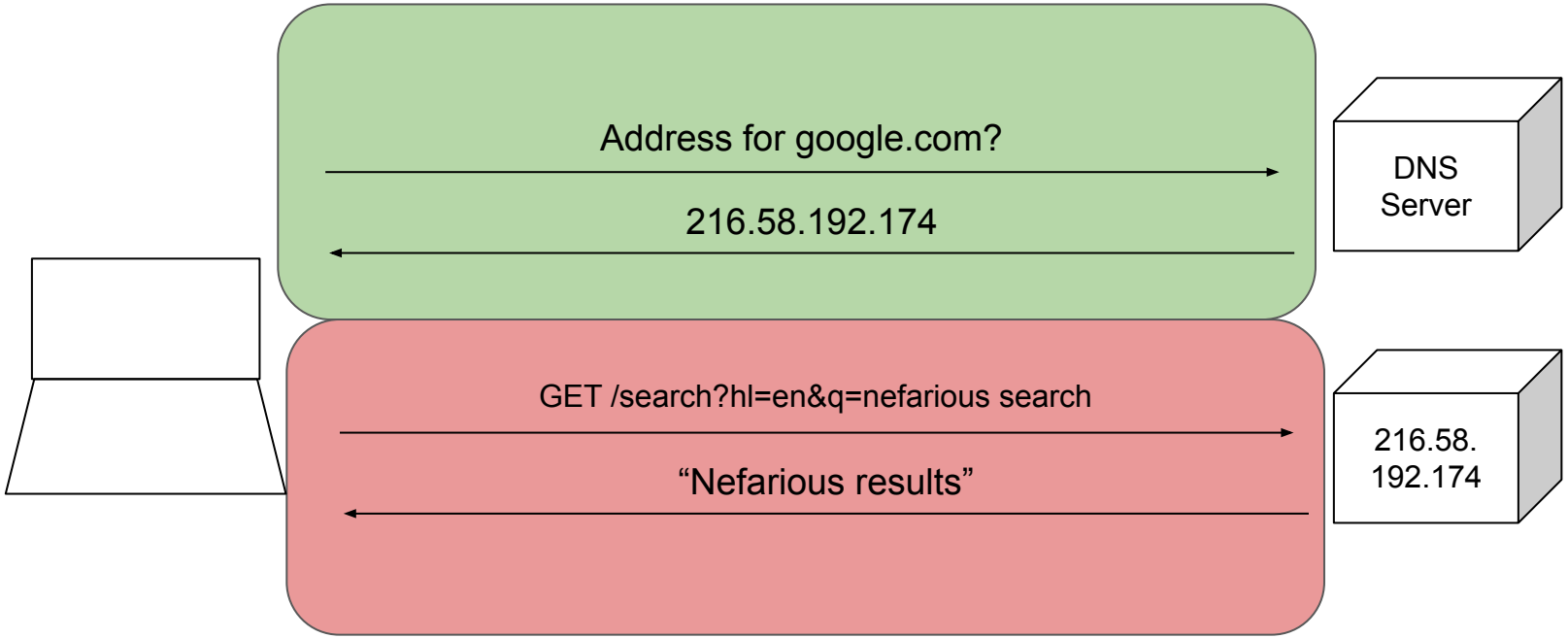
Percentage of pages loaded over HTTPS in Chrome by platform



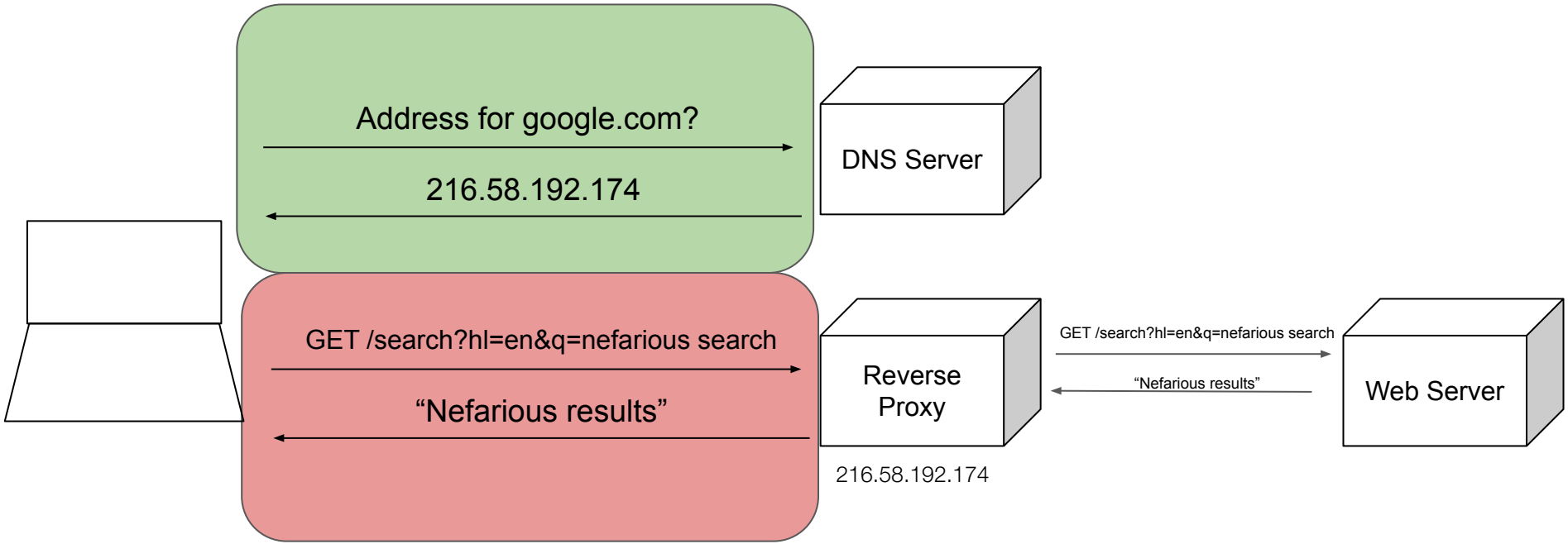
Source: https://transparencyreport.google.com/https


Address for google.com?
216.58.192.174
DNS Server
GET /search?hl=en&q=nefarious search
“Nefarious results”
216.58.
192.174

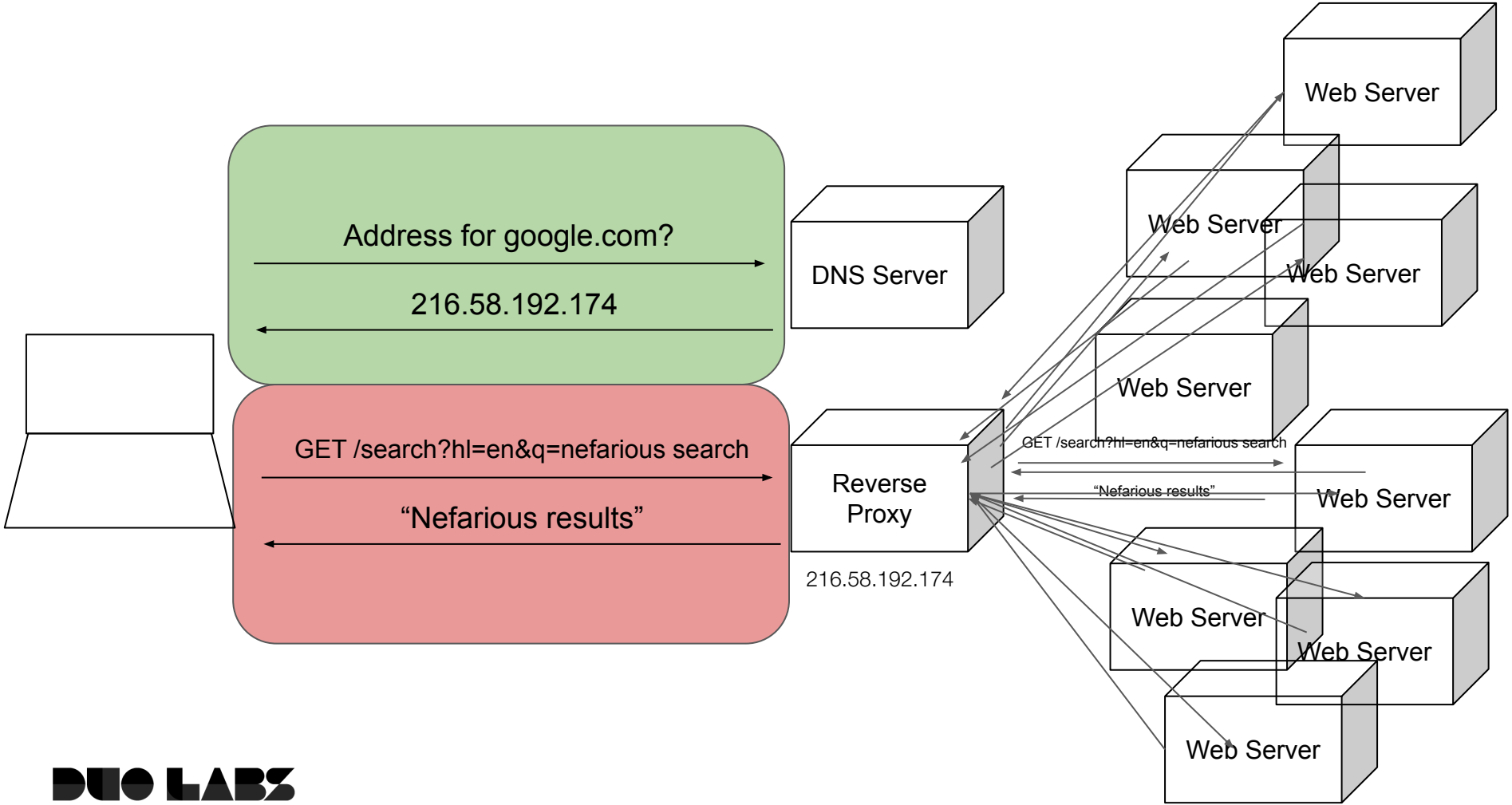
DUO LABS


Address for google.com?
216.58.192.174
DNS Server
GET /search?hl=en&q=nefarious search
“Nefarious results”
216.58.
192.174

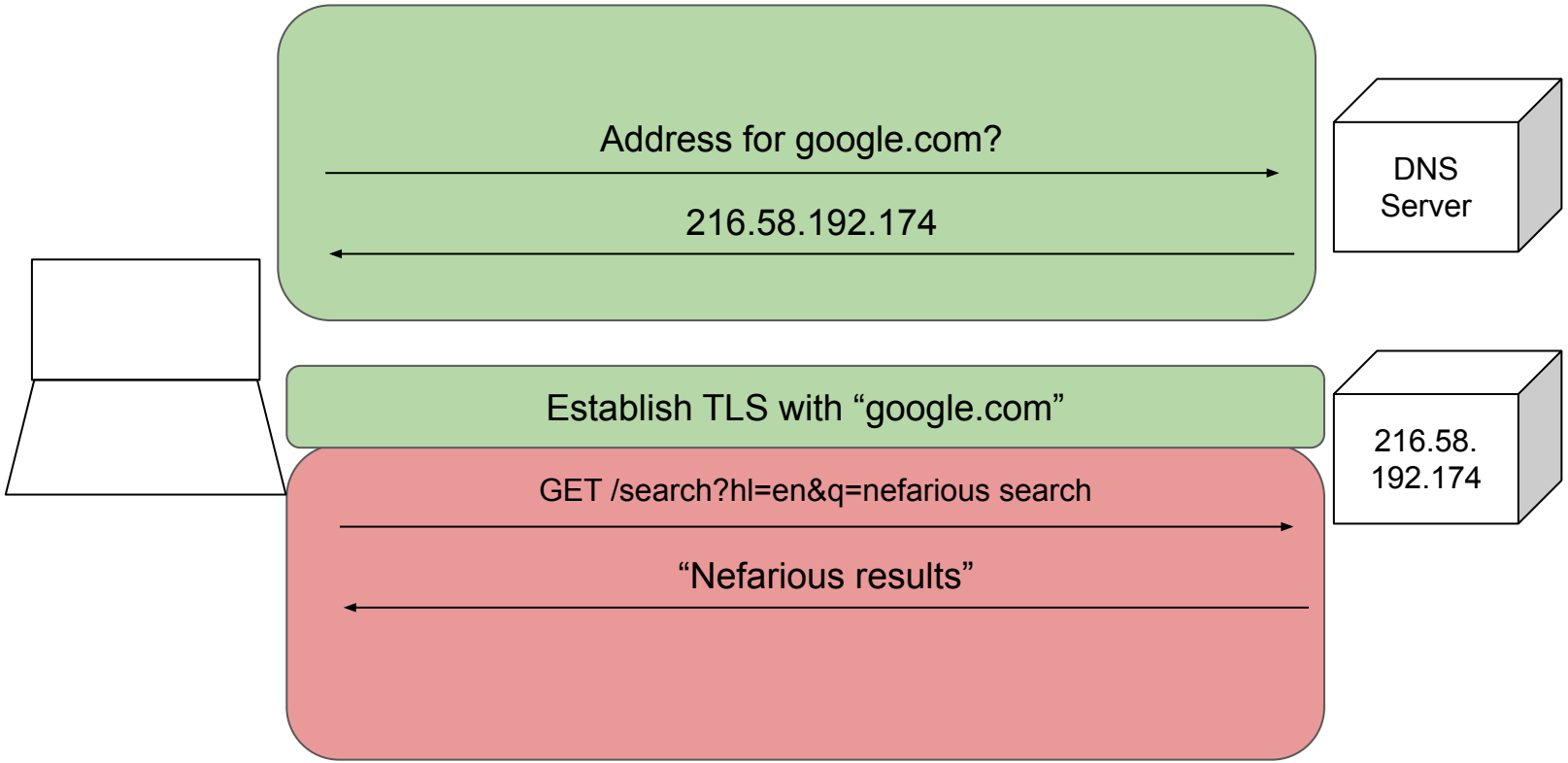
DUO LABS


Address for google.com?
216.58.192.174
DNS Server
GET /search?hl=en&q=nefarious search
“Nefarious results”
Reverse Proxy
216.58.192.174
GET /search?hl=en&q=nefarious search
“Nefarious results”
Web Server

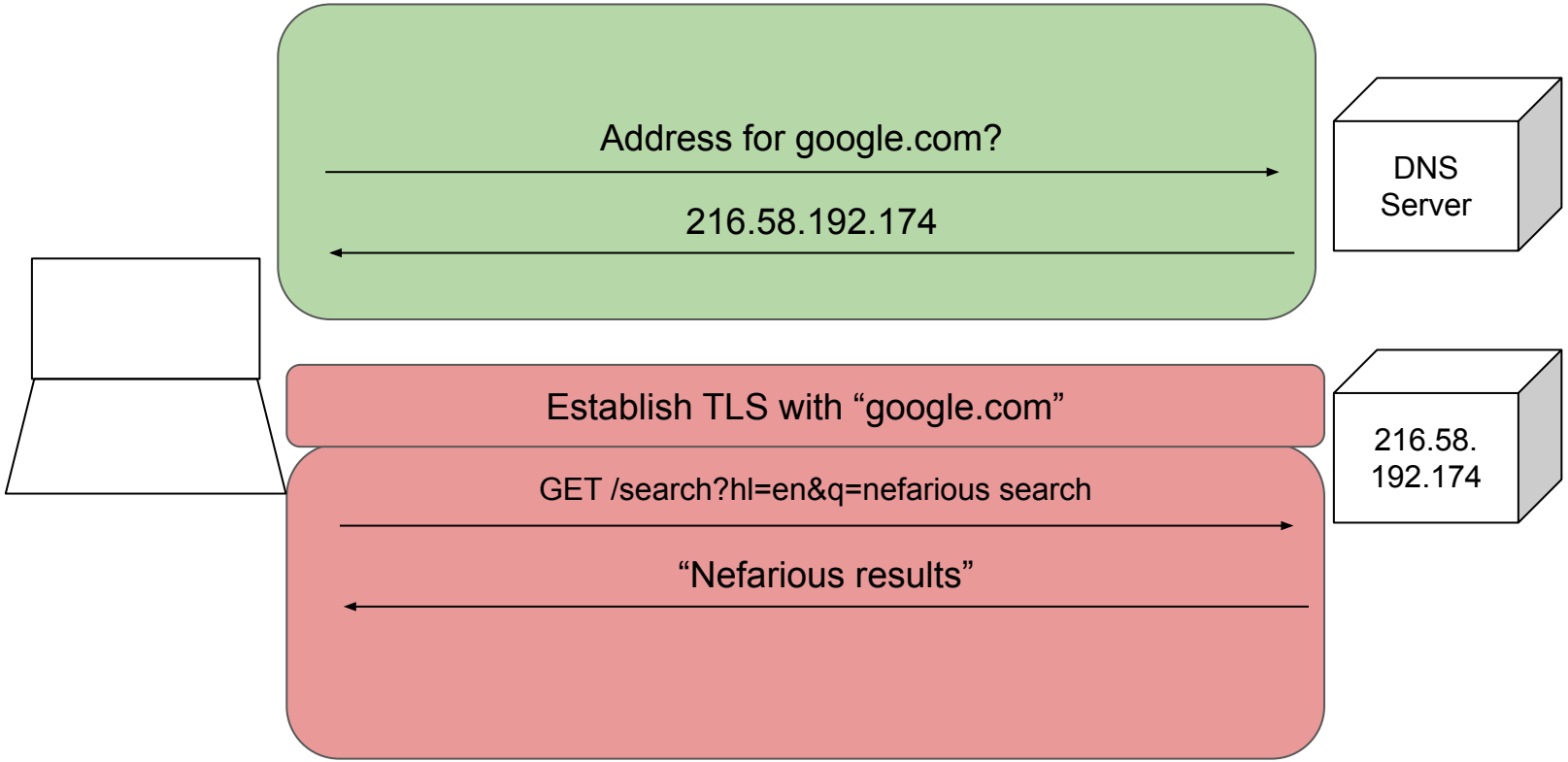
DUO LABS


Address for google.com?
216.58.192.174
DNS Server
GET /search?hl=en&q=nefarious search
“Nefarious results”
Reverse Proxy
216.58.192.174
Web Server
Web Server
Web Server
Web Server
GET /search?hl=en&q=nefarious search
“Nefarious results”
Web Server
Web Server
Web Server
Web Server

DUO LABS


Address for google.com?
216.58.192.174
DNS Server
Establish TLS with “google.com”
GET /search?hl=en&q=nefarious search
“Nefarious results”
216.58.
192.174

DUO LABS


Address for google.com?
216.58.192.174
DNS Server
Establish TLS with “google.com”
GET /search?hl=en&q=nefarious search
“Nefarious results”
216.58.
192.174

DUO LABS

Middleware through the years

- DNS query
- Destination IP Address
- HTTP connection
- SNI in the HTTP TLS handshake

DUO LABS

Middleware through the years

- DNS query
- ~~Destination IP Address~~
- ~~HTTP connection~~
- ~~SNI in the HTTP TLS handshake~~

DUO LABS

Why is this relevant now?

It’s basically the only thing left

DUO LABS

Middleware

Middleware

Benign

Visibility

Malware blocking

Data loss prevention

Malicious

Non-stakeholder data aggregation

Response alteration

Reconnaissance

New Standards

- DNS over TLS (DoT)
- DNS over HTTPS (DoH)
- DNScrypt

DUO LABS

New Concerns

Encrypted DNS Concerns

Centralization

Centralization of DNS into a handful of service providers

Reduced visibility

Reduced visibility for benign network operators

DNS in Layer 7

A relatively unprecedented move of DNS into the Application Layer

DUO LABS

Centralization

- Prevents data aggregation/manipulation by service providers
- Lack of broad support means DoT/DoH users are centralizing data

DUO LABS

Reduced visibility

- Enterprise Monitoring
- DNS Redirection
- DNS as a Control Plane

DUO LABS

Moving to the Application Layer

- Slow inroads at system level caused some applications to include it
- For consumers, major privacy win
- Security loss for network operators

DUO LABS

Next Steps?

More OS Support

More provider support

VIMES

Demo

1.1.1.1 — the Internet's Fastest

https://1.1.1.1/help

1.1.1.1

Connection Information

Please include this URL when you create a post in the community forum.

```
https://1.1.1.1
/help#eyJpcONmIjoiWWVzIiwiaXNEb3QiOiJZZXMiLCJpcORvaCI6Ik5vIiwicmVzb2x2ZXJJc
COxLjEuMS4xIjoiWWVzIiwicmVzb2x2ZXJJcCOxLjAuMC4xIjoiWWVzIiwicmVzb2x2ZXJJcCOy
NjA2OjQ3MDA6NDcwMDo6MTExMSI6IlllcyIsInJlc29sdmVySXAtMjYwNjo0NzAwOjQ3MDA6OjE
wMDEiOiJZZXMiLCJkYXRhY2VudGVyTG9jYXRpb24iOiJEVFciLCJpc1dhcnAiOiJObyIsImlzcE
5hbWUiOiJDbG91ZGZsYXJlIiwiaXNwOYNuTjoiMTM2MzUifQ==
```

Click to copy

Debug Information

Connected to 1.1.1.1	Yes
Using DNS over HTTPS (DoH)	No
Using DNS over TLS (DoT)	Yes
Using DNS over WARP	No
AS Name	Cloudflare
AS Number	13335
Cloudflare Data Center	DTW

Connectivity to Resolver IP Addresses

4:40 PM

Updates

Supporting Platforms Then

- Android 9+

DUO LABS

Supporting Platforms Now

- Android 9+
- Windows 10
- macOS
- iOS
- Firefox
- Chrome

DUO LABS

Also

- Curl
- Comcast DNS
- Cox DNS
- Hurricane Electric
- Cisco Umbrella
- CoreDNS
- Quad9

DUO LABS

Conclusions

Conclusions

- DoT/DoH removed and added some concerns
- New concerns are less entirely new, and more a move of where functionality is performed
- Benefits can be realized without sacrificing control as long as legacy approaches are modified

DUO LABS

Needing the DoH

The ongoing encryption and centralization of DNS

Eldridge Alexander
Duo Security
@magiceldridge

DUO LABS