

How does the Internet work?

And who knows what you're doing?

Tips

> no need to take photos

Tips

- > no need to take photos
- > follow along with me instead of slide deck

Tips

- > no need to take photos
- > follow along with me instead of slide deck
- > audience participation

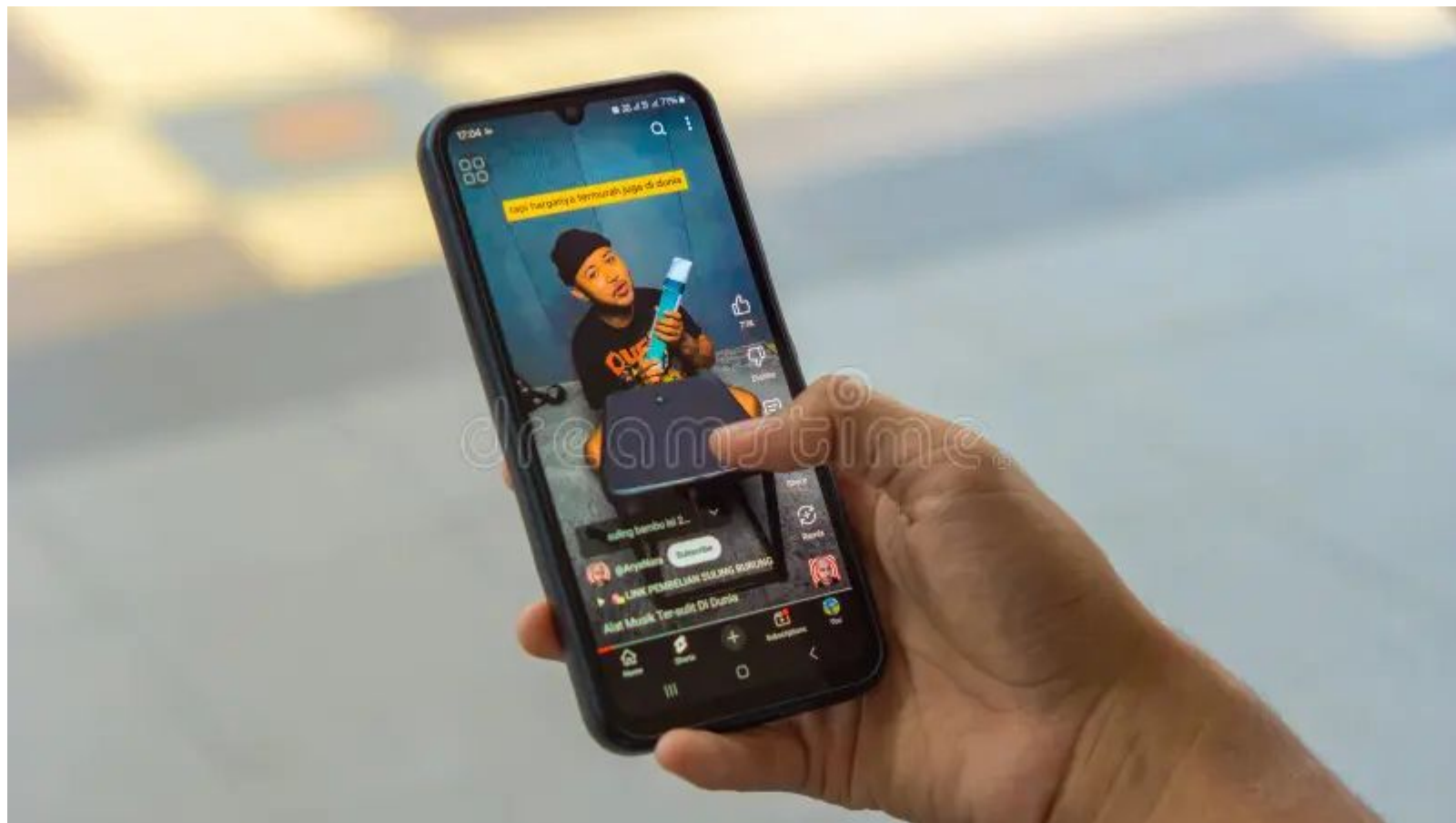
Why am I giving this talk?

Dear speaker,

We are pleased to invite you to the **COSCUP x UbuCon Asia 2026 Welcome Party**.
Your complimentary All-You-Can-Drink Ticket is available using the invite code below.



Most of us are internet users



Some of us are even programmers

```
bash
$ curl -i -X PUT httpbin.org/put -H Content-Type:application/json -d '{"hello": "world"}'
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 14 Feb 2015 17:36:55 GMT
Content-Type: application/json
Content-Length: 423
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true

{
  "args": {},
  "data": "{\"hello\": \"world\"}",
  "files": {},
  "form": {},
  "headers": {
    "Accept": "*/",
    "Content-Length": "18",
    "Content-Type": "application/json",
    "Host": "httpbin.org",
    "User-Agent": "HTTPie/1.0.0-dev"
  },
  "json": {
    "hello": "world"
  },
  "origin": "109.81.210.187",
  "url": "http://httpbin.org/put"
}
$
```

But do we understand HOW?

Why care?

> curiosity

> learn & experiment

Why care?

> curiosity

> learn & experiment

> understand WHO can see WHAT, and HOW they can BLOCK something



cat pics



Google 搜尋



cat pics



登入

AI 模式 全部 圖片 購物 書籍 影片 新聞 更多

工具



Cute



Sphynx



Cute baby



Kitten



Hairless



Cute kitten



Breed



Animal



Cute pictures



Personality



200+ Cat Pictures & Images [HD] | Downlo...
Unsplash



Cute Baby Cat Stock Photos, Images and...
Vecteezy



Cat | Breeds, Origins, History, Body Types...
Britannica



12 Curious White Cat Facts to Know Befor...
Country Living Magazine



Cats revealed in all their glory in stunning...
New Scientist



Little Cat Pictures | Download Free Image...
Unsplash



The 10 Most Popular Breeds of Cats - RAWZ
RAWZ Natural Pet Food



10 Cute Cat Pictures That Help Us Get...
Pawlicy Advisor



Cat Photos - Download Free High-Quality...
Magnific



Moment of Meow: Goofy Cats | National...
National Geographic Kids



Cute Cat Wallpaper Stock Photos, Images...
Vecteezy



Cat | Breeds, Origins, History, Body Types...
Britannica



Cat - Wikipedia
Wikipedia









Spoiler: none of them

Spoiler: none of them

(probably)



cat pics



Google 搜尋

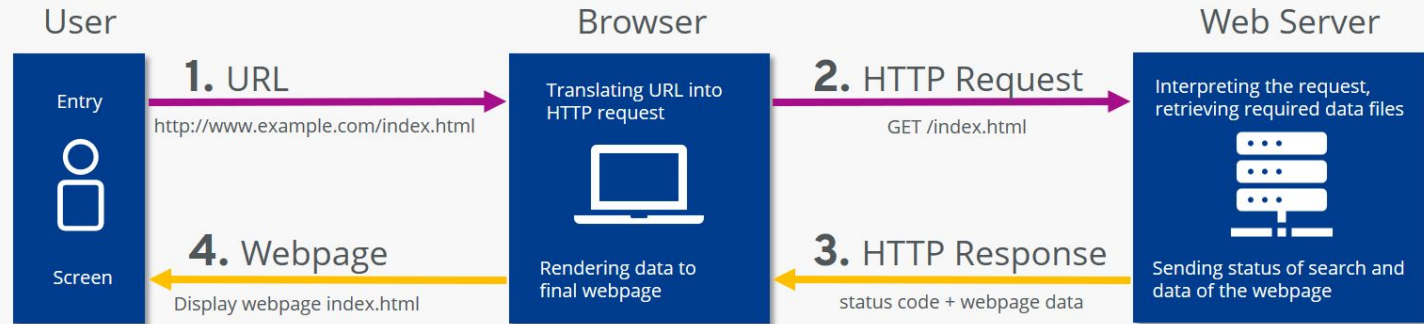


New Private Tab

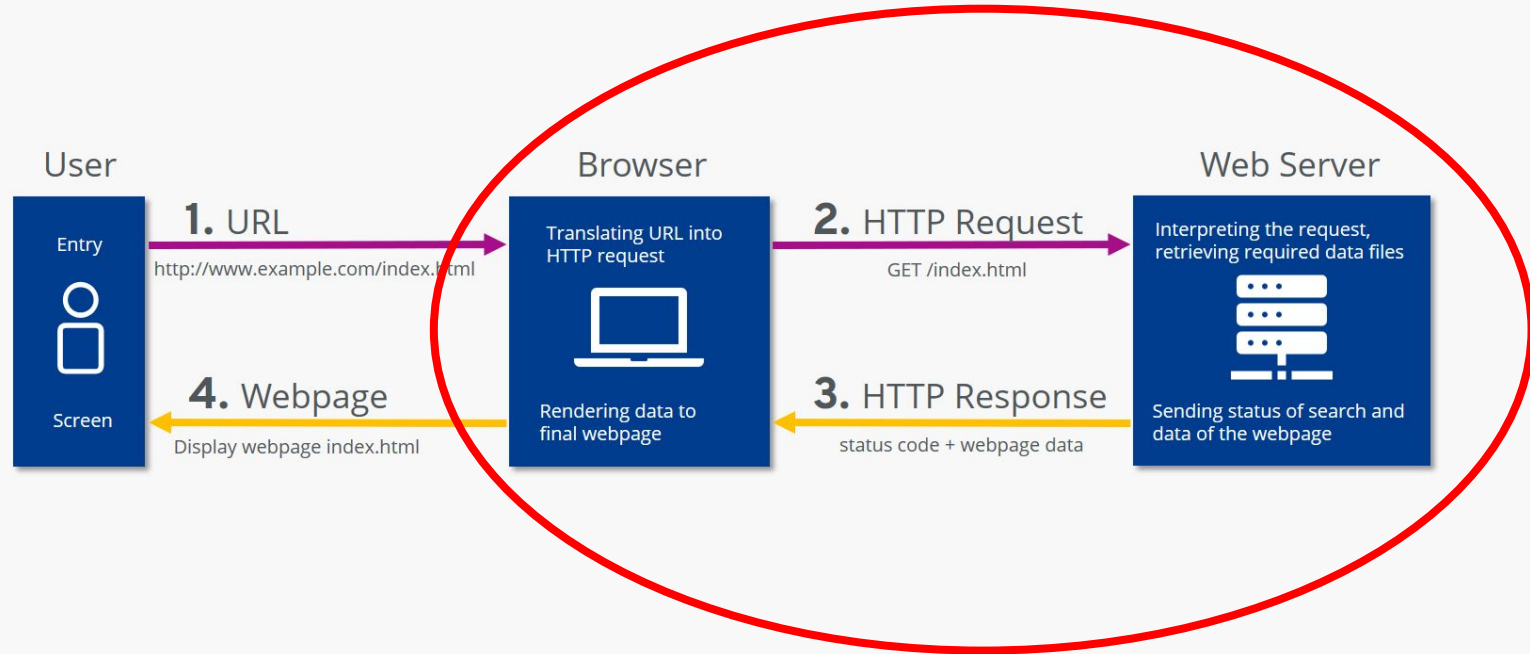


images.google.com

Communication process according to HTTP



Communication process according to HTTP



Internet architecture is complicated

> beginner, non-technical audience

Internet architecture is complicated

- > beginner, non-technical audience
- > explaining through analogies

Internet architecture is complicated

- > beginner, non-technical audience
- > explaining through analogies
- > avoid getting too technical

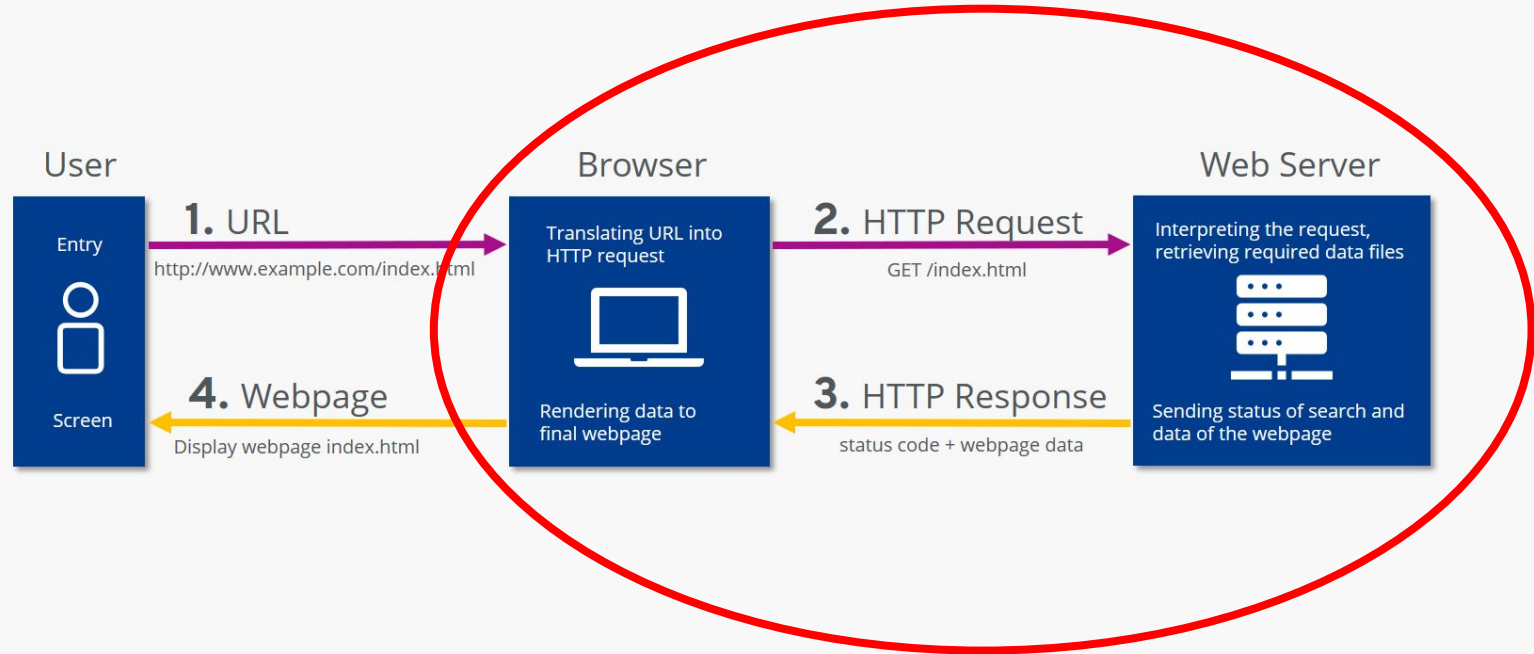
Internet architecture is complicated

- > beginner, non-technical audience
- > explaining through analogies
- > avoid getting too technical
- > generous assumptions

Assumptions

- > Only IPv4
- > Everyone has a public, routable IP
- > I will use some terms loosely (“encryption” , “key”) for simplicity

Communication process according to HTTP



YOUR
MESSAGE

Dear Mike,
Greetings from Portugal!
I'm currently sitting in a
cafe' in Lisbon, the sun is
shining and fado is playing
in the background. Have you
ever tried a Portuguese
custard tart, aka, "Pastel
de Nata"? they are just so
good! Portugal is a good
country to gain weight,
the food is delicious! ☺
cheers,
Mary

Postcard ID: PT-678910



STAMP

Mike Smith

123 Magnolia St.

Jackson, Hi 12345

U.S.A.

RECIPIENT'S
ADDRESS

POSTCARD ID



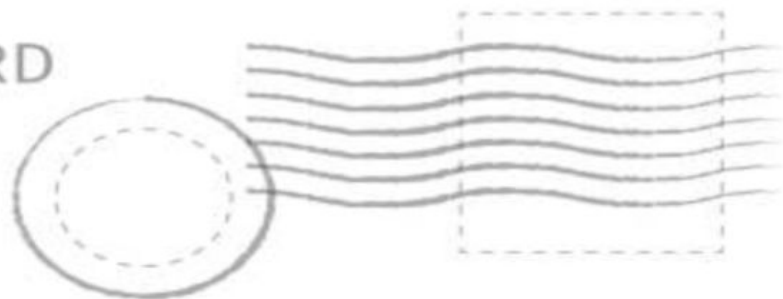




Analogy: Postcards run the internet

- > post office will handle delivery to recipient address
- > include from address to receive reply
- > Your ISP (Chunghwa, AT&T etc.) acts as the postman

POSTCARD



Give me your home page

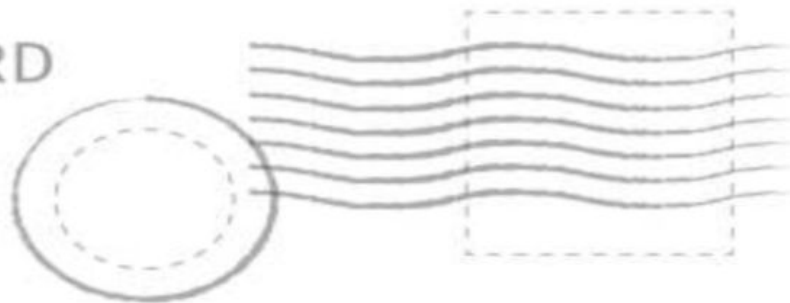
TO: images.google.com

FROM: john

Problem

- > Internet works on numeric addresses
- > “Internet Protocol” or IP Address

POSTCARD



Give me your home page

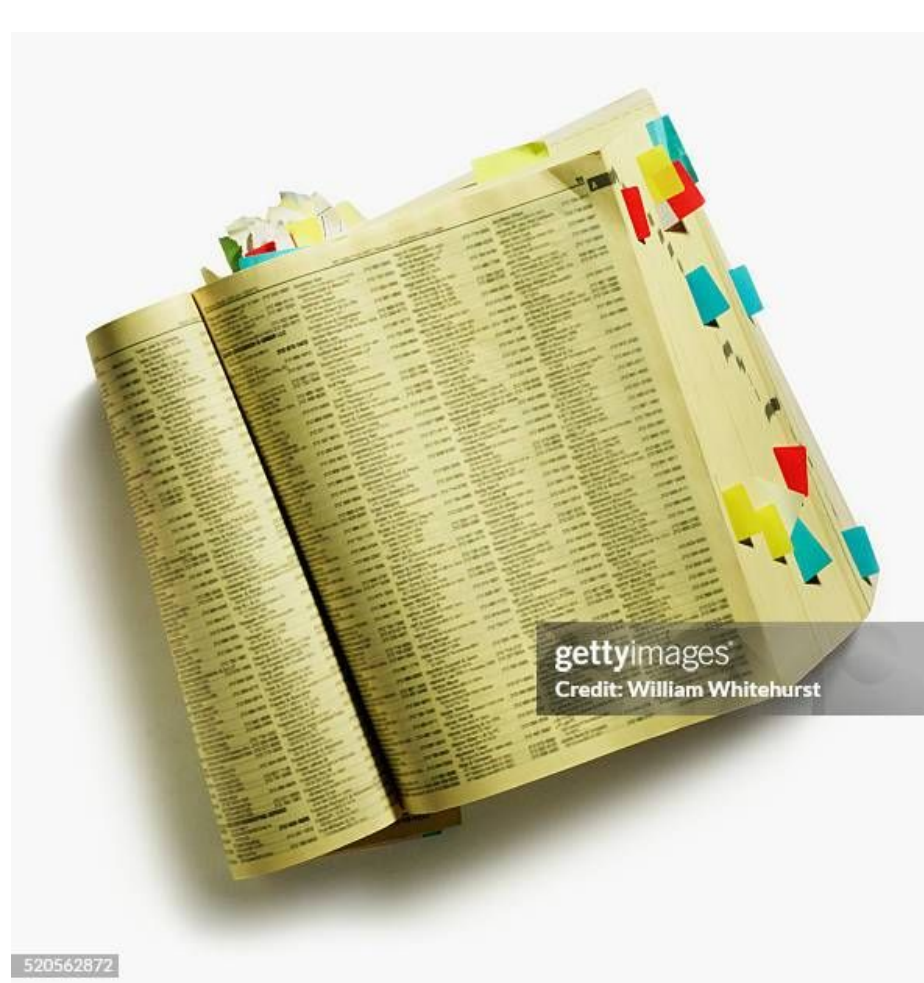
TO: 34.34.34.34

FROM: 2.2.2.2

Where did these numbers come from?

- > Your ISP gives you your IP address (e.g. 2.2.2.2)
- > How do you get googles?

1/12 Domain Rd Panmu	299 3580
Christopher G & K G	570 4569
Christopher Hay Construction	570 9475
242 Orakei Rd Remra	575 0648
Christopher J A	524 0223
2/100 Manuka Rd Glnfd	442 4032
Christopher J & P	634 0089
10 Harbour View Tce Onnga	528 6525
Christopher O F 5 Maaka Pl StJns	292 4888
Christopher O H Hunua R D 3	0-27-272 916
Christopher Pryor C Auckl	
Mobile	
Christopher R C	478 526
27 Bellbird Rse MurBy	378 074
Christopher Robin's Child Care Centre	267 120
4 Sherwood Ave GryLn	478 23
Christopher S A M	
3 Pallant St Mrewa	
Christopher S D	

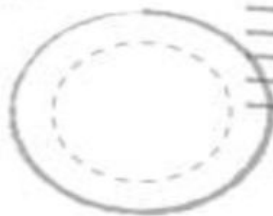


DNS (Domain Name System)

- > Special servers that give you the address for a name
- > Provided by ISP, or can use external (e.g. Google, Cloudflare)

What is google.com's
address?

POSTCARD

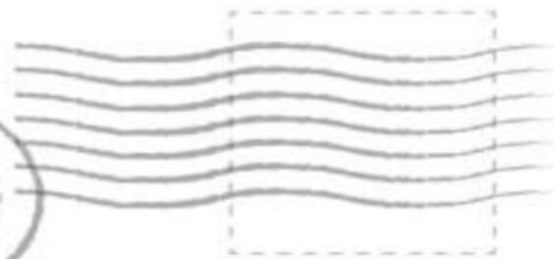
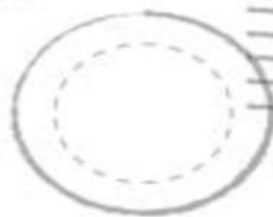


TO: 1.1.1.1

FROM: 2.2.2.2

google.com is at:
34.34.34.34

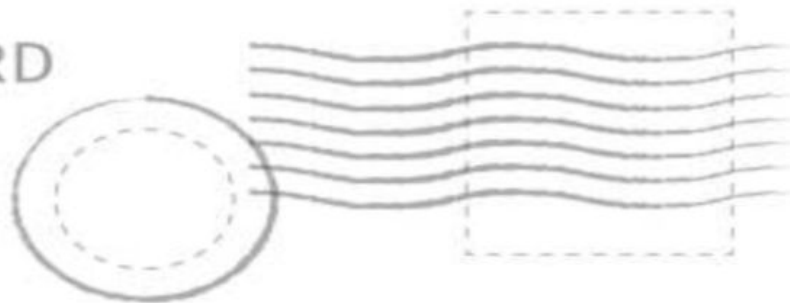
POSTCARD



TO: 2.2.2.2

FROM: 1.1.1.1

POSTCARD

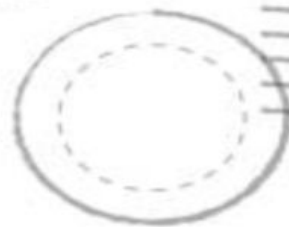


Give me your home page

TO: 34.34.34.34

FROM: 2.2.2.2

POSTCARD



```
<html>  
<title>  
.....  
</html>
```

TO: 2.2.2.2

FROM: 34.34.34.34

DNS

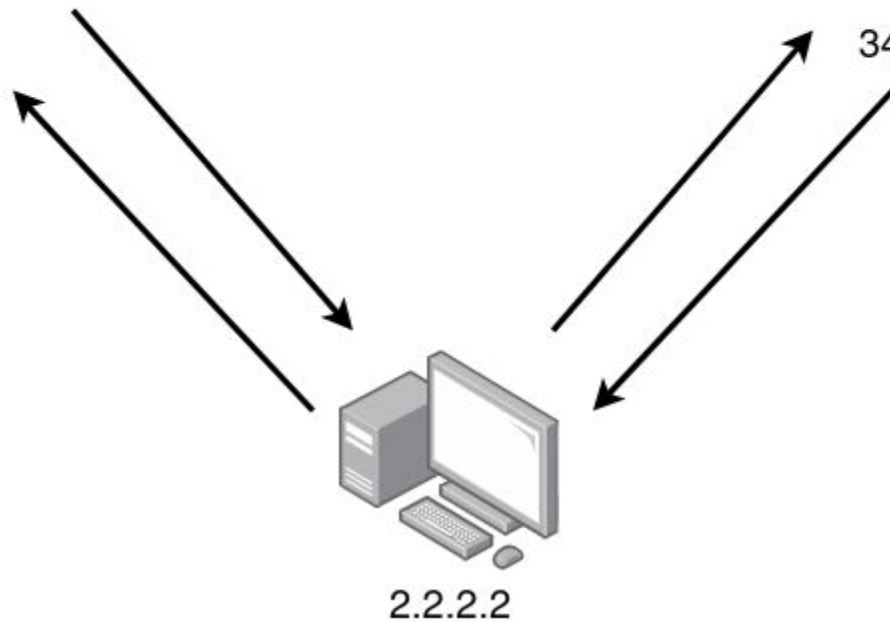


1.1.1.1

Google



34.34.34.34



2.2.2.2

DNS



1.1.1.1

Google



34.34.34.34

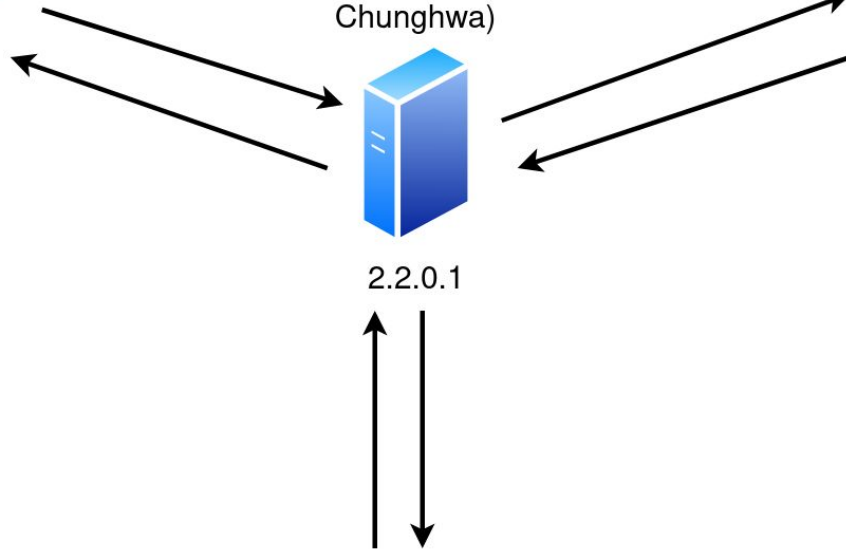
ISP (e.g.
Chunghwa)



2.2.0.1



2.2.2.2





DNS



1.1.1.1

Google



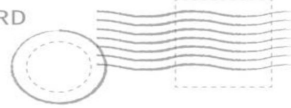
34.34.34.34

ISP (e.g.
Chunghwa)



2.2.0.1

POSTCARD

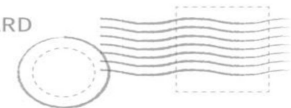


TO: 1.1.1.1

FROM: 2.2.2.2

What is google.com's
address?

POSTCARD



TO: 2.2.2.2

FROM: 34.34.34.34

<html>
<title>
.....
</html>

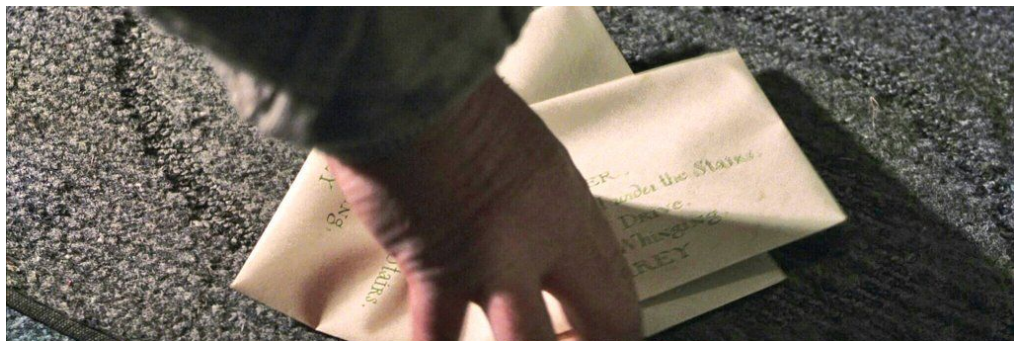


2.2.2.2

Privacy Concerns

- > ISP can see DNS requests
- > They can see which website you're accessing (just the name)
- > ISP can see HTTP requests
- > They can see WHAT you're doing on the website

Interference concerns?



DNS Request dropped

DNS



1.1.1.1

Google



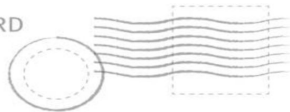
34.34.34.34

ISP (e.g.
Chunghwa)



2.2.0.1

POSTCARD



What is google.com's
address?

TO: 1.1.1.1

FROM: 2.2.2.2



2.2.2.2



HTTP response modified

DNS



1.1.1.1

ISP (e.g.
Chunghwa)



2.2.0.1

Google



POSTCARD

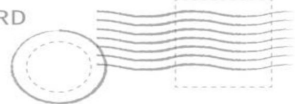


4

TO: 2.2.2.2

FROM: 34.34.34.34

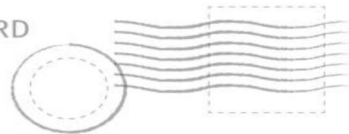
POSTCARD



TO: 1.1.1.1

FROM: 2.2.2.2

POSTCARD



TO: 2.2.2.2

FROM: 34.34.34.34

What is google.com's
address?

<html>
<title>

.....

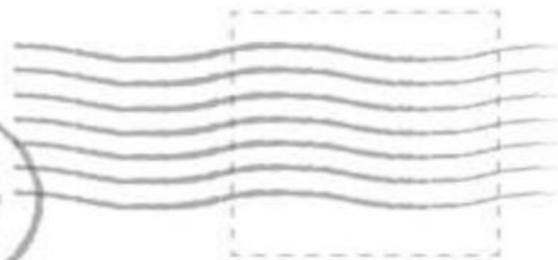
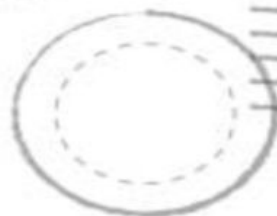
<p>
Buy Evil Corp Insurance!
</p>
</html>



2.2.2.2

Comment
"Looks Cool!"
on Dave's photo

POSTCARD



TO: 55.55.55.55

FROM: 2.2.2.2

DNS



1.1.1.1

Facebook



55.55.55.55

ISP (e.g.
Chunghwa)



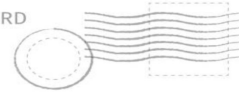
2.2.0.1



2.2.2.2

Comment
"Looks Cool!"
on Dave's photo

POSTCARD



TO: 55.55.55.55

FROM: 2.2.2.2

DNS



1.1.1.1

ISP (e.g.
Chunghwa)



2.2.0.1

Facebook



POSTCARD



TO: 55.55.55.55

FROM: 2.2.2.2

Comment
"Your stupid!"
on Dave's photo

POSTCARD



TO: 55.55.55.55

FROM: 2.2.2.2

Comment
"Looks Cool!"
on Dave's photo



2.2.2.2

DNS



1.1.1.1

Facebook



ISP (e.g.
Chunghwa)



2.2.0.1

Comment
"Your stupid!"
on Dave's photo

POSTCARD

TO: 55.55.55.55

FROM: 2.2.2.2

POSTCARD

TO: 55.55.55.55

FROM: 2.2.2.2



2.2.2.2

Comment
"Looks Cool!"
on Dave's photo



DNS



Facebook



It's spelt
"you're"

(e.g.
wa)

Comment
"Your stupid!"
on Dave's photo

POSTCARD

TO: 55.55.55.55

FROM: 2.2.2.2

POSTCARD

TO: 55.55.55.55

FROM: 2.2.2.2

Comment
"Looks Cool!"
on Dave's photo



2.2.2.2



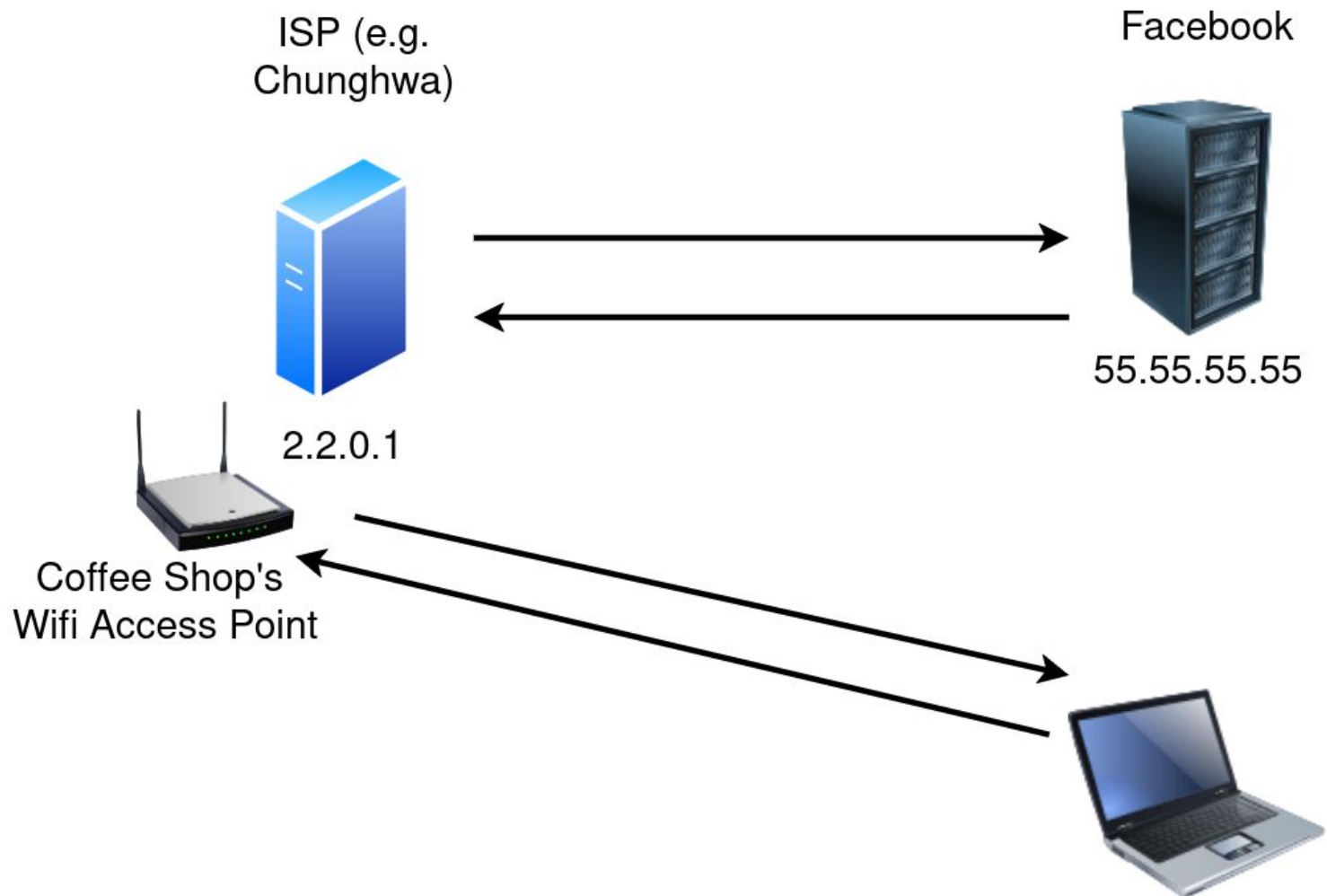
shutterstock

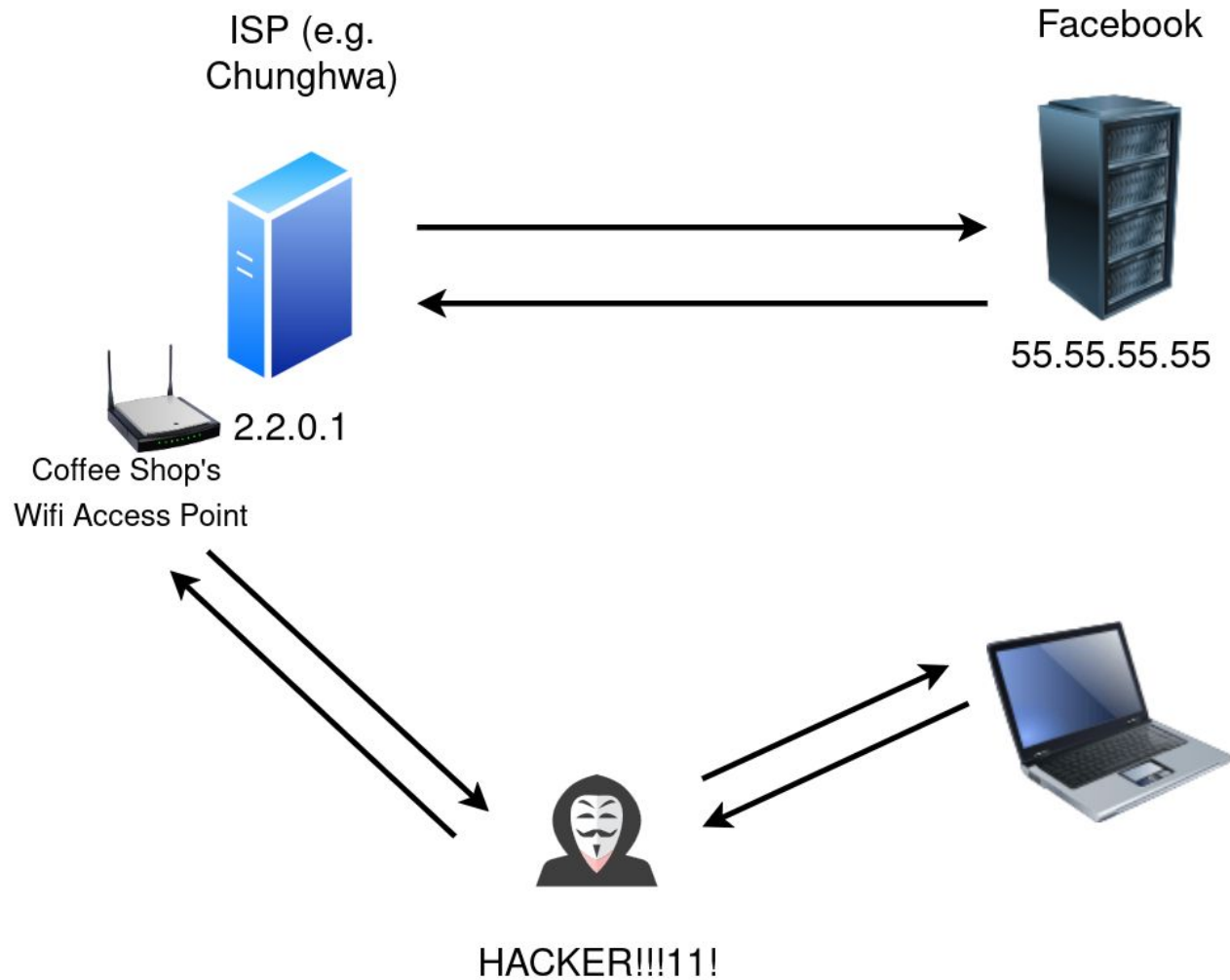
IMAGE ID: 126009806
www.shutterstock.com

However

- > It's quite unlikely an ISP would mess with requests maliciously
- > Then who can?







Man in the Middle

> Attacker inserts themselves between you and your ISP (WiFi)

Man in the Middle

- > Attacker inserts themselves between you and your ISP (WiFi)
- > Same network: ARP Poisoning (also on wired networks)

Man in the Middle

- > Attacker inserts themselves between you and your ISP (WiFi)
- > Same network: ARP Poisoning (also on wired networks)
- > Fake WiFi network, laptop auto connects (same WiFi name)

Man in the Middle

- > Attacker inserts themselves between you and your ISP (WiFi)
- > Same network: ARP Poisoning (also on wired networks)
- > Fake WiFi network, laptop auto connects (same WiFi name)
- > Is there anyone else in the middle?

DNS



1.1.1.1

Google



34.34.34.34

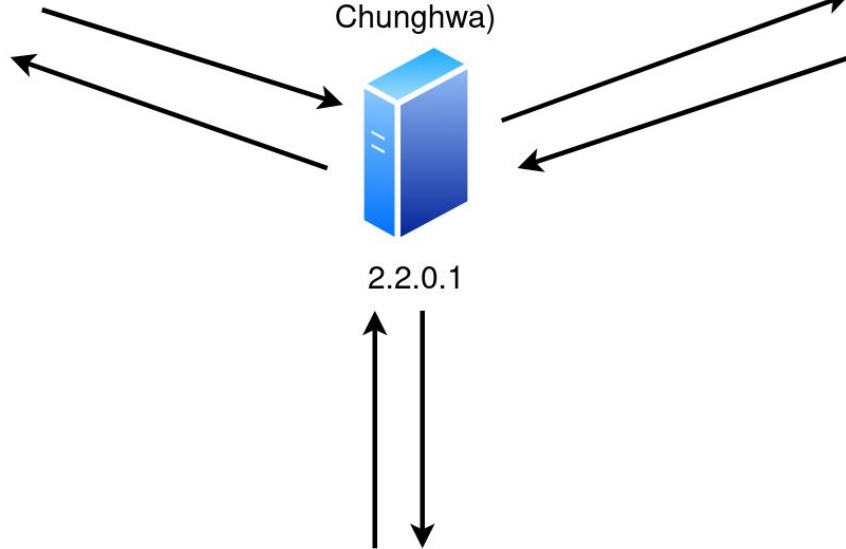
ISP (e.g.
Chunghwa)



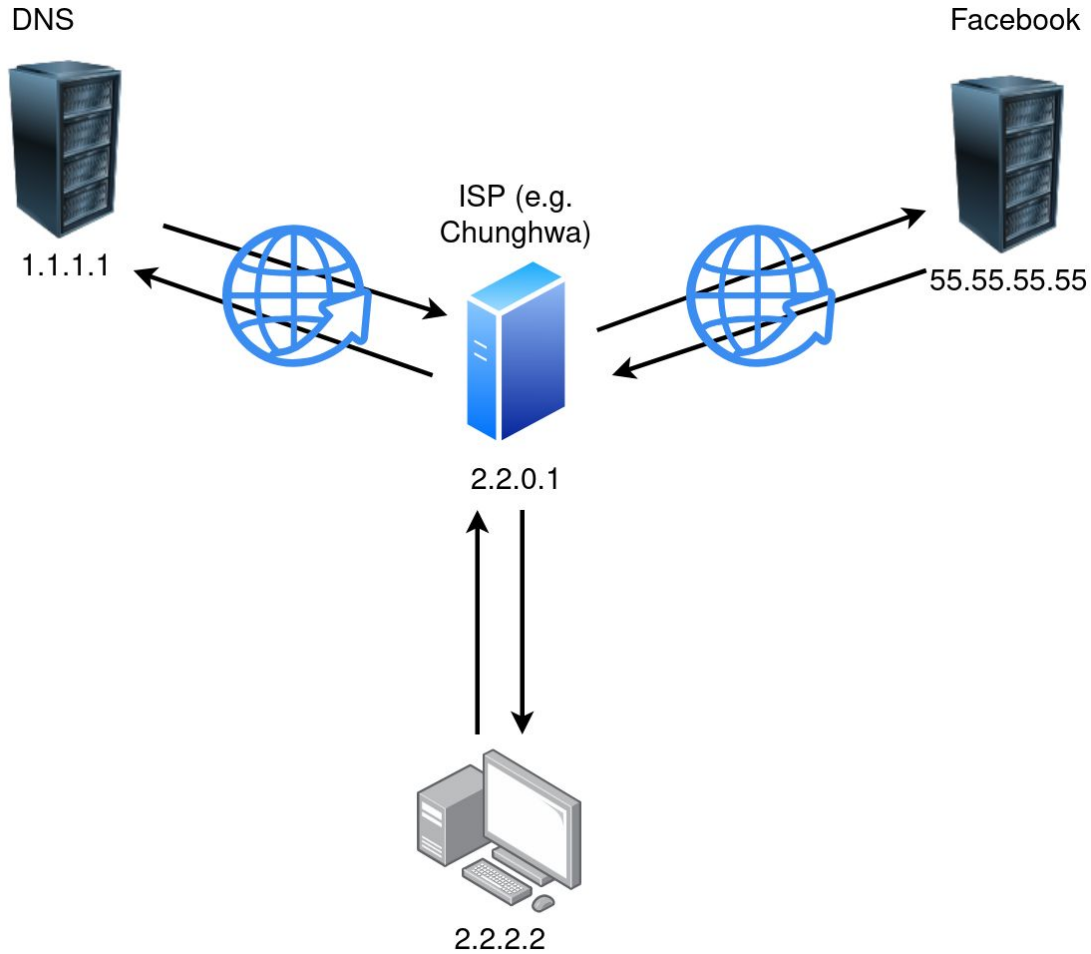
2.2.0.1



2.2.2.2



Routing over the internet

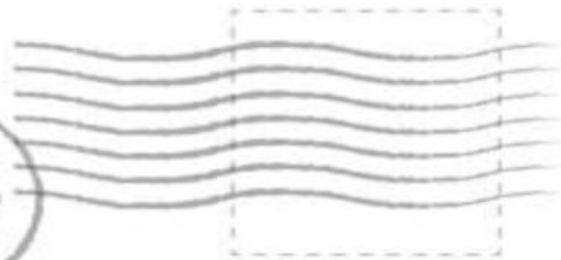
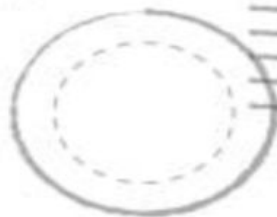






I like u

POSTCARD



TO: Macy

FROM: John

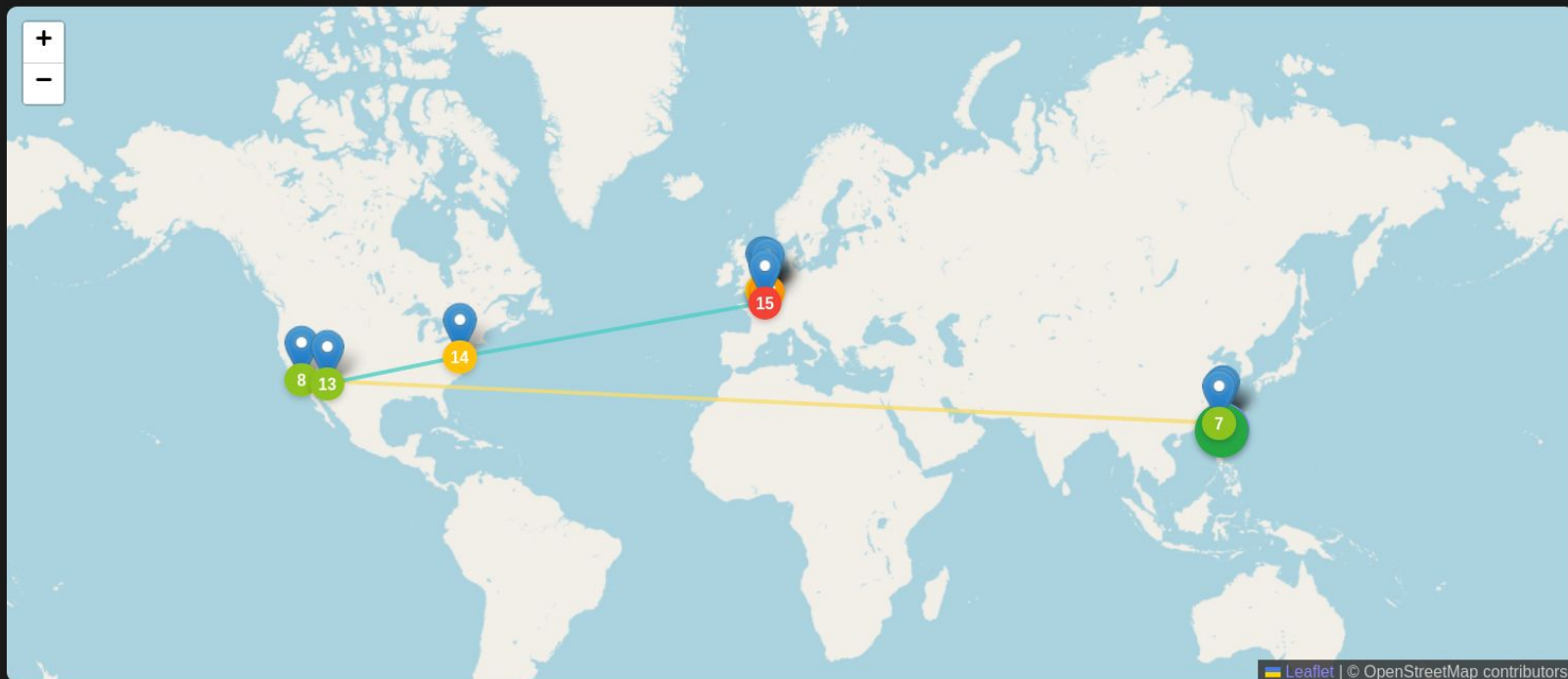


Traceroute

My traceroute [v0.96]							2026-08-08T23:35:25+0800						
arch (10.99.3.65) -> mail.saxrag.com (137.74.163.242)													
Keys: Help Display mode Restart statistics Order of fields quit													
Host							Packets		Pings				
							Loss%	Snt	Last	Avg	Best	Wrst	StDev
1.	10.99.0.1						0.5%	611	2.1	4.1	1.1	109.1	12.7
2.	59.124.108.177						1.1%	611	11.8	9.9	3.0	113.4	8.0
3.	172.28.1.1						1.3%	611	5.0	10.8	3.6	104.7	7.0
4.	168.95.82.246						3.3%	611	4.7	5.6	3.5	113.5	5.3
5.	220.128.9.242						3.9%	611	4.5	6.4	3.8	117.1	8.4
6.	220.128.7.77						0.8%	611	4.3	7.6	3.6	201.8	16.2
7.	202.39.91.105						1.0%	611	137.2	141.3	136.8	271.1	17.4
8.	202.39.84.65						3.8%	611	137.0	140.6	136.9	297.5	12.5
9.	(waiting for reply)												
10.	(waiting for reply)												
11.	(waiting for reply)												
12.	(waiting for reply)												
13.	192.99.146.128						0.7%	610	171.8	175.3	170.3	301.3	12.5
14.	192.99.146.125						2.0%	610	198.3	199.4	197.4	256.8	3.8
15.	57.128.121.12						1.3%	610	283.7	287.8	282.5	383.4	12.1
16.	54.36.50.228						67.9%	610	278.1	280.2	276.7	369.7	9.0
17.	91.121.215.178						3.1%	610	275.0	278.2	274.7	372.9	11.2
18.	37.59.16.32						5.7%	610	278.1	279.3	274.8	386.9	10.5
19.	(waiting for reply)												
20.	(waiting for reply)												
21.	(waiting for reply)												
22.	(waiting for reply)												
23.	(waiting for reply)												
24.	(waiting for reply)												
25.	137.74.163.242						96.6%	610	295.9	330.1	278.3	386.9	40.8

Route Analysis Results

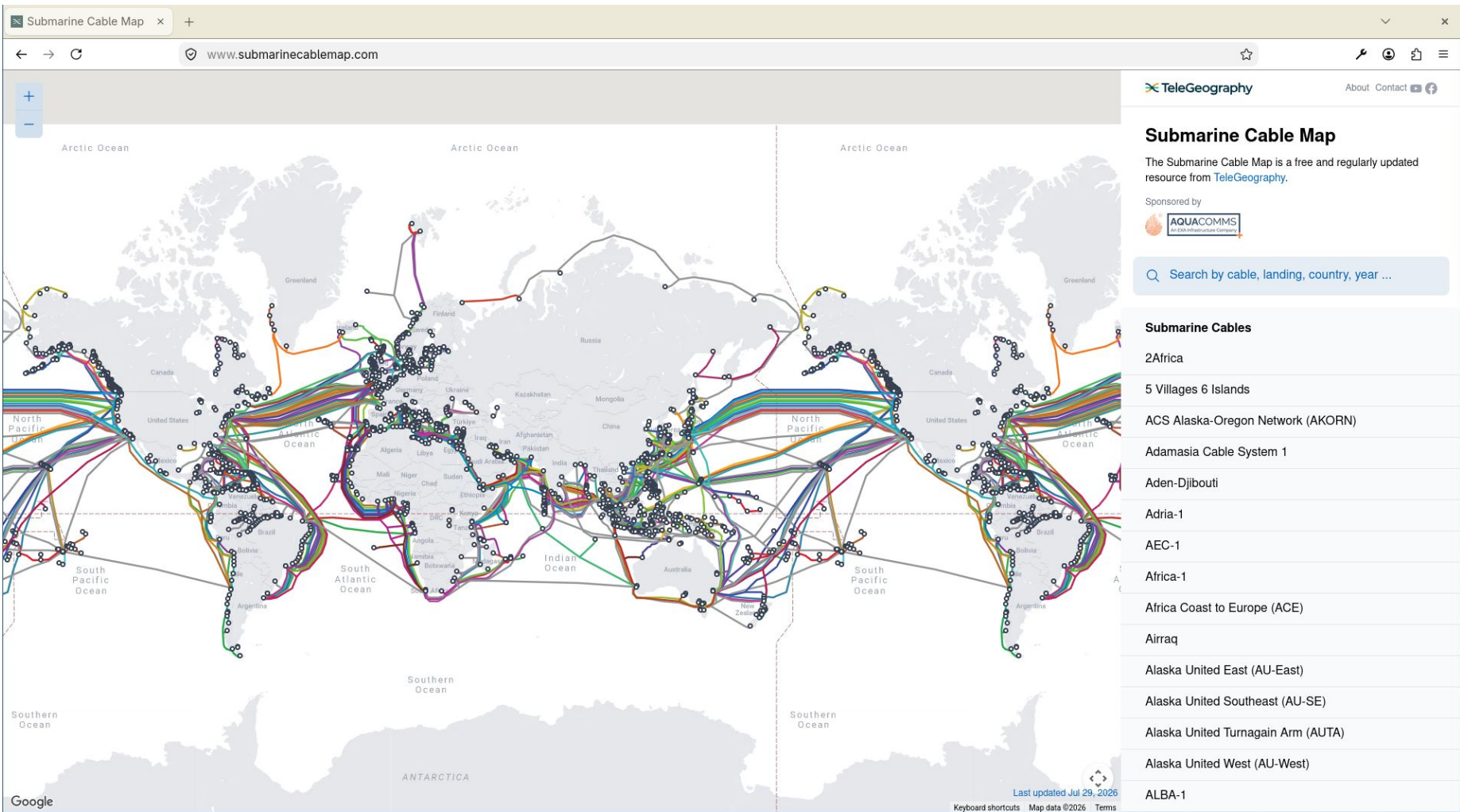
Route Map



Route Analysis Results

Route Map





Who can see what I'm doing?

> ISP (e.g. AT&T)

Who can see what I'm doing?

> ISP (e.g. AT&T)

> Coffee shop hacker

Who can see what I'm doing?

- > ISP (e.g. AT&T)
- > Coffee shop hacker
- > Data centers in 3rd countries along the route

Who can see what I'm doing?

- > ISP (e.g. AT&T)
- > Coffee shop hacker
- > Data centers in 3rd countries along the route
- > Aliens?



SPONSORED BY:



NordVPN®

SPONSORED BY:



NordVPN®

Use code
"COSCUP"
for 69%
off!

(kidding)

DNS



1.1.1.1

Google



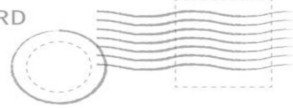
34.34.34.34

ISP (e.g.
Chunghwa)



2.2.0.1

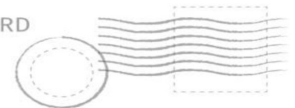
POSTCARD



TO: 1.1.1.1

FROM: 2.2.2.2

POSTCARD



TO: 2.2.2.2

FROM: 34.34.34.34

<html>
<title>
.....
</html>



2.2.2.2

What is google.com's
address?

DNS



1.1

Google



34.34.34.34

Early 1990s!

POSTCARD

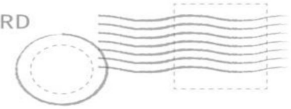


TO: 1.1

FROM:

What is google.com's
address?

POSTCARD



TO: 2.2.2.2

FROM: 34.34.34.34



2.2.2.2



Plaintext

Hello



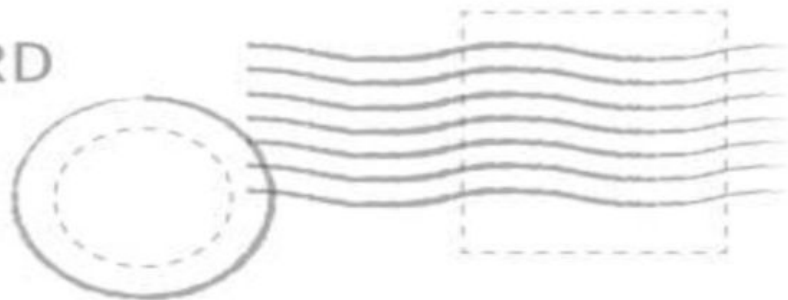
Encryption

Ciphertext

SNifgNi+uk0=

Comment
"Looks Cool!"
on Dave's photo

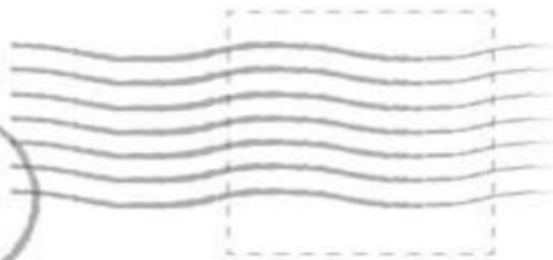
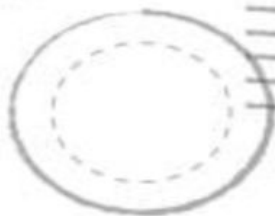
POSTCARD



TO: 55.55.55.55

FROM: 2.2.2.2

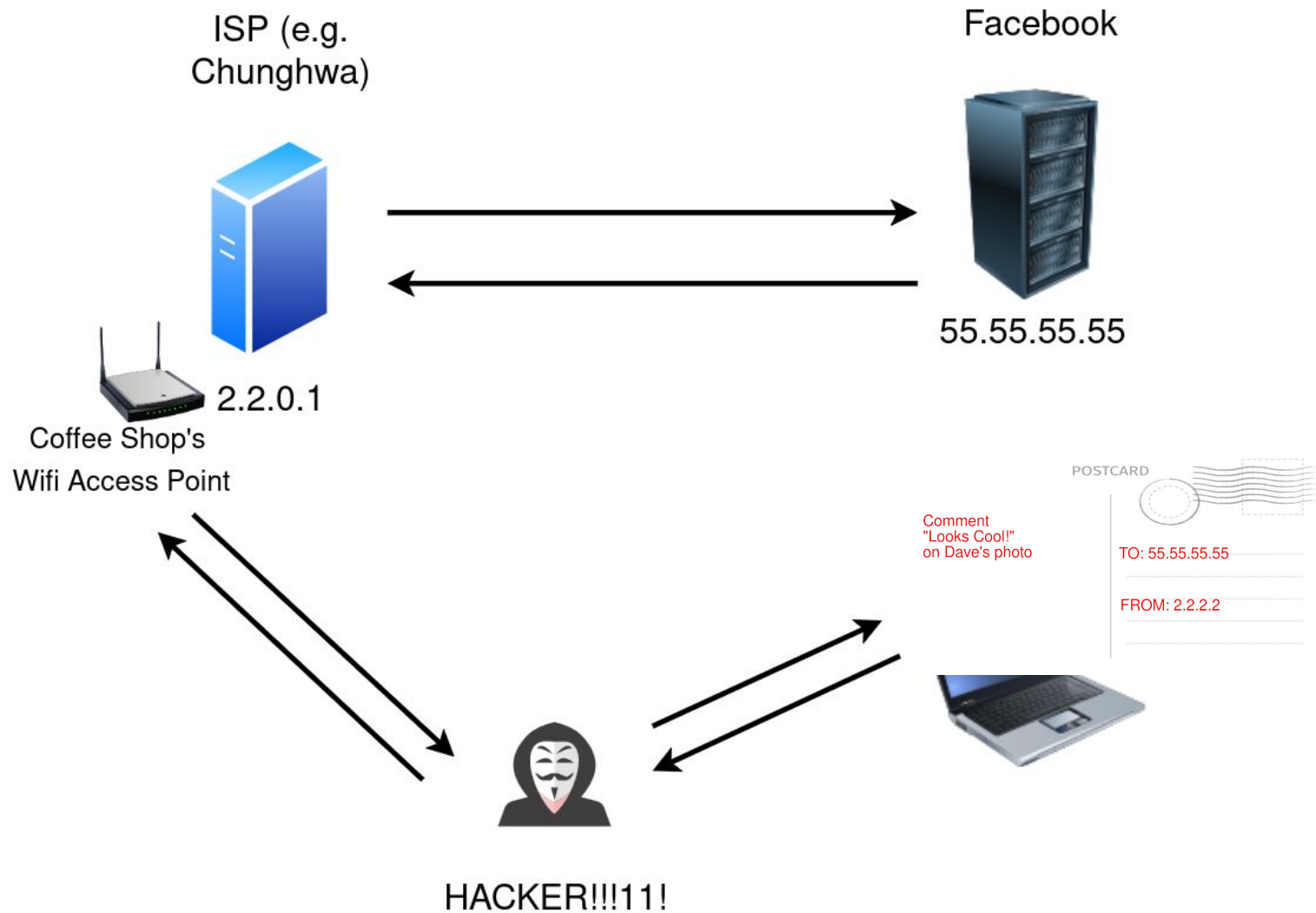
POSTCARD

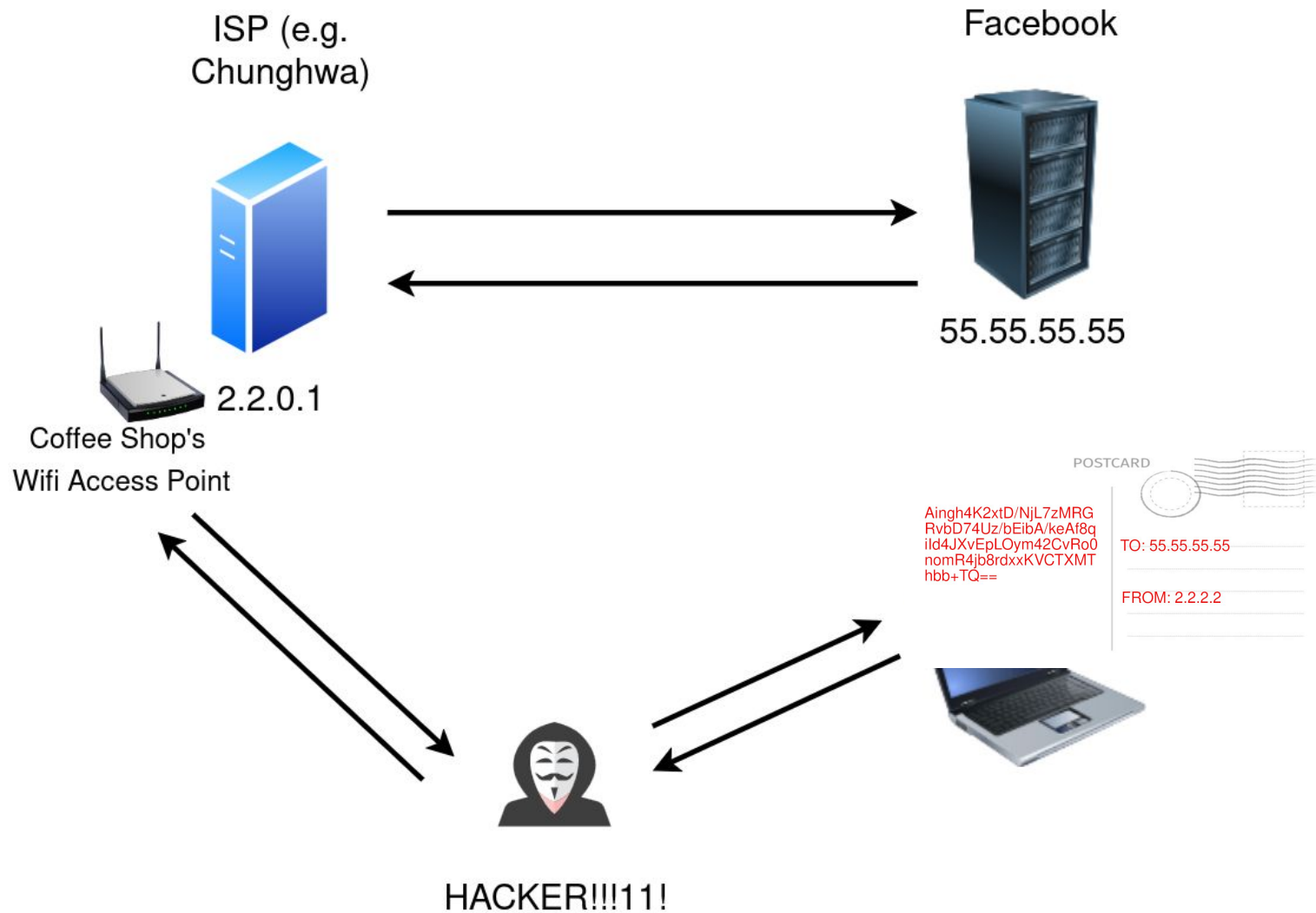


Aingh4K2xtD/NjL7zMRG
RvbD74Uz/bEibA/keAf8q
ild4JXvEpLOym42CvRo0
nomR4jb8rdxxKVCTXMT
hbb+TQ==

TO: 55.55.55.55

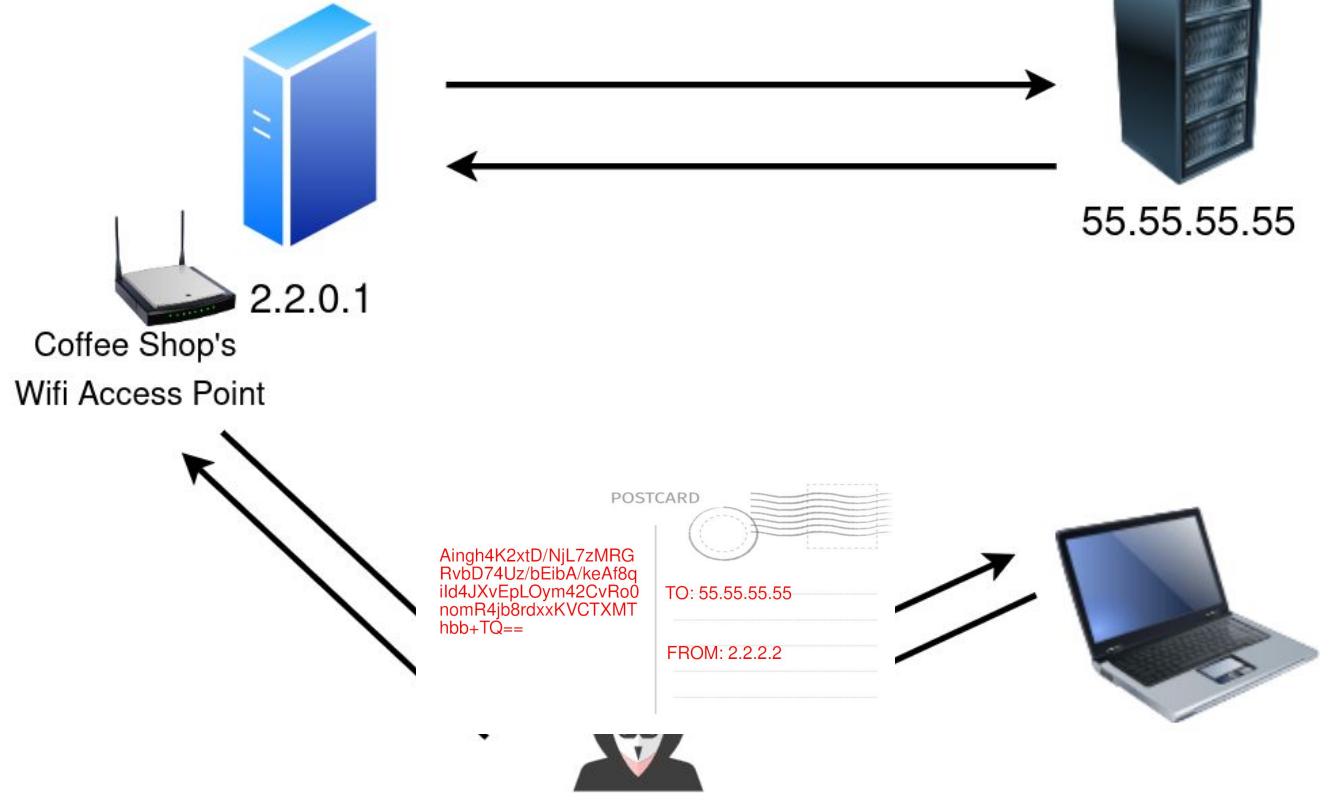
FROM: 2.2.2.2





ISP (e.g.
Chunghwa)

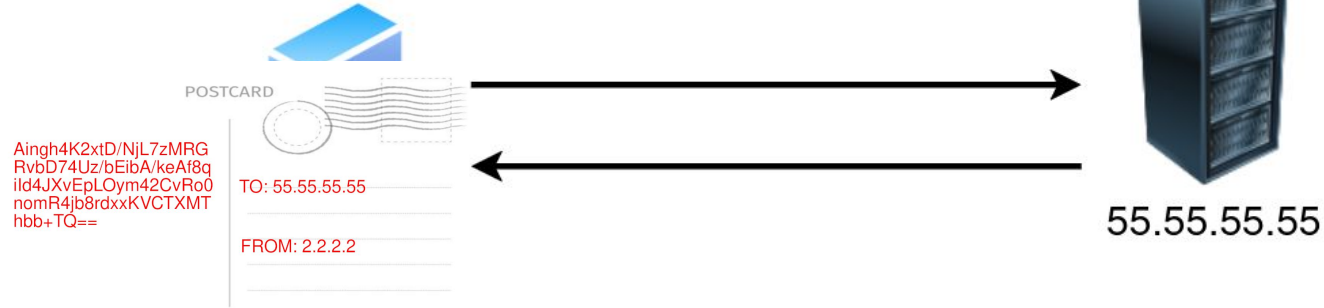
Facebook



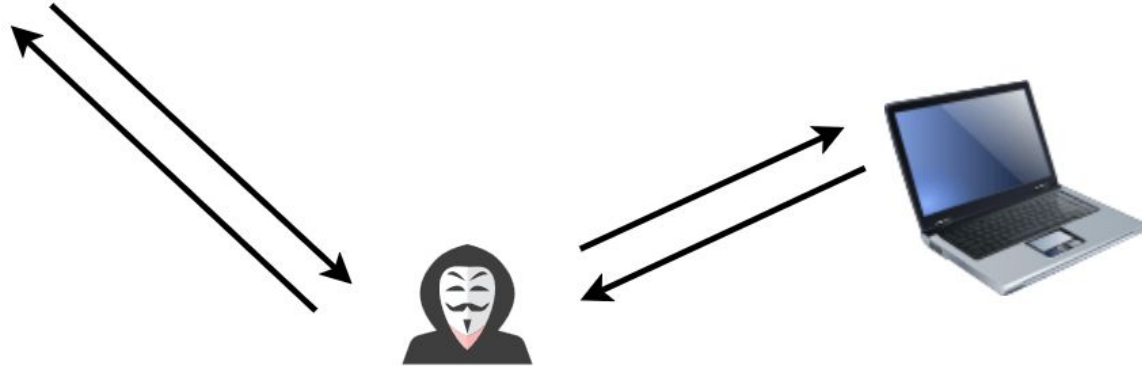
HACKER!!!11!

ISP (e.g.
Chunghwa)

Facebook



Coffee Shop's
Wifi Access Point

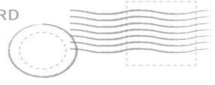


HACKER!!!11!

ISP (e.g.
Chunghwa)

Facebook

POSTCARD



Aingh4K2xD/NjL7zMRG
RvbD74Uz/bEibA/keAf8q
ild4JXvEpLOym42CvRo0
nomR4jb8rdxxKVCTXMT
hbb+TQ==

TO: 55.55.55.55

FROM: 2.2.2.2

55.55.55.55

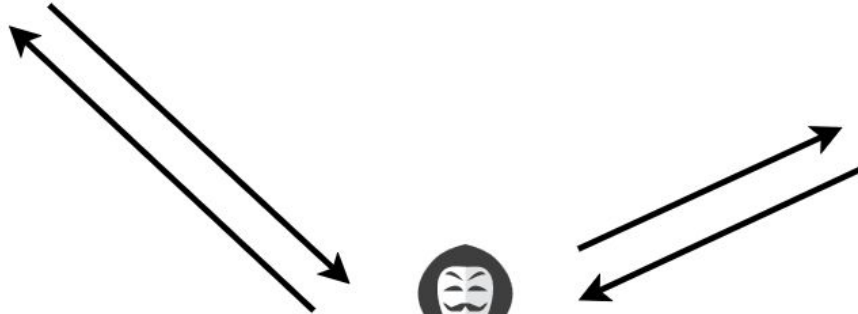
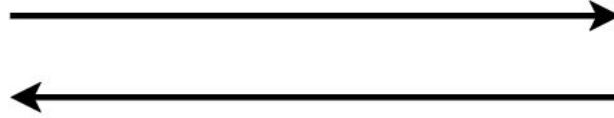


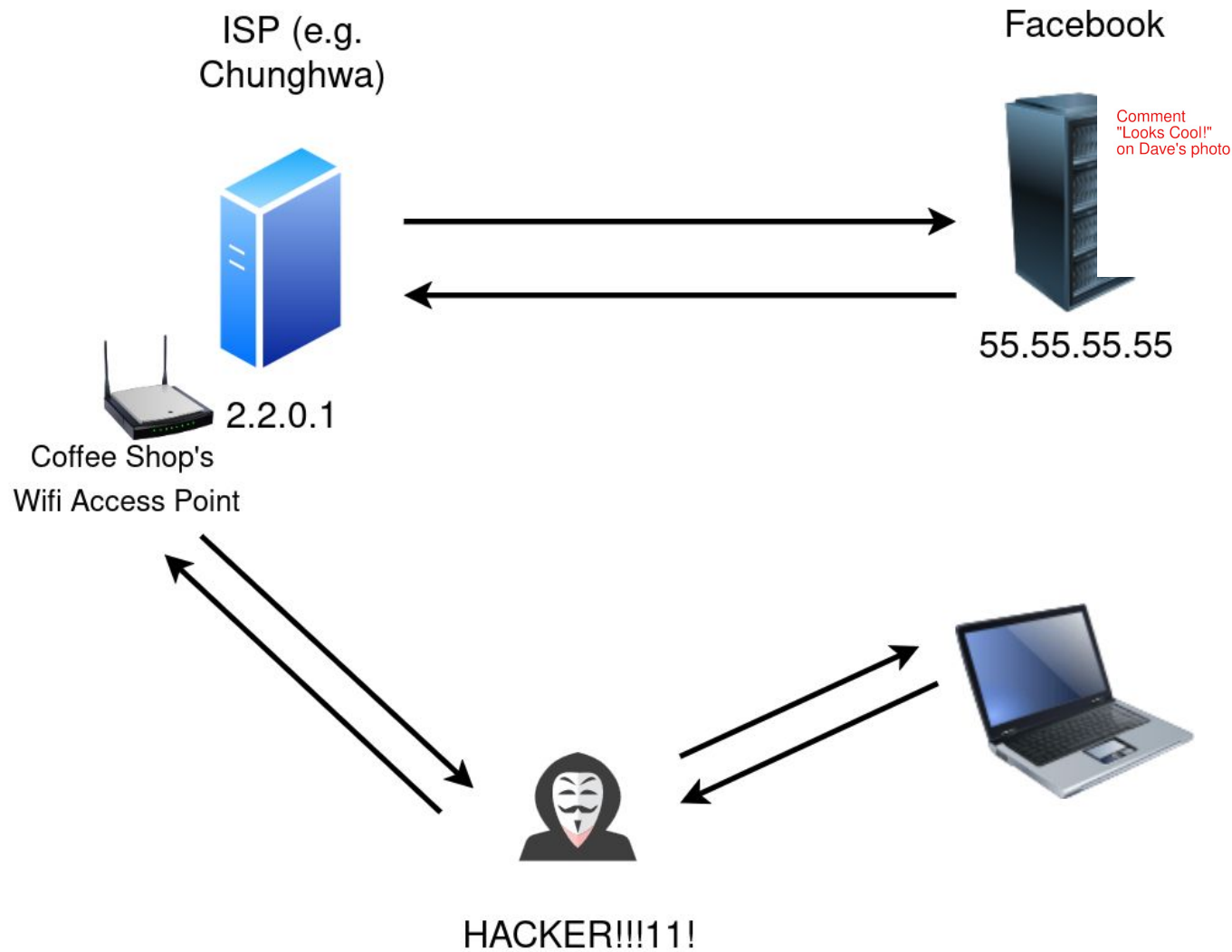
2.2.0.1

Coffee Shop's
Wifi Access Point



HACKER!!!11!





Encryption (TLS)

> No one in the middle can see the request / response

Encryption (TLS)

- > No one in the middle can see the request / response
- > Recipient can see original text by decrypting

Encryption (TLS)

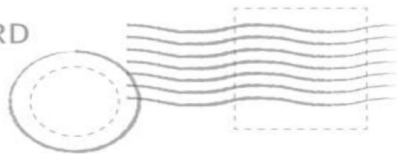
- > No one in the middle can see the request / response
- > Recipient can see original text by decrypting
- > If someone tries to modify payload, decryption fails

Encryption (TLS)

- > No one in the middle can see the request / response
- > Recipient can see original text by decrypting
- > If someone tries to modify payload, decryption fails

Aingh4K2xtD/NjL7zMRG
RvbD74Uz/bEibA/keAf8q
ild4JXvEpLOym42CvRo0
nomR4jb8rdxxKVCTXMT
hbb+TQ==

POSTCARD



TO: 55.55.55.55

FROM: 2.2.2.2

Encryption - How??

Encryption - How

> Complicated mathematics

Encryption - How

> Complicated mathematics

> Search Terms:

- AES, RSA
- Diffie-Hellman
- WebPKI

Encryption - How

> Complicated mathematics

> Search Terms:

- AES, RSA
- Diffie-Hellman
- WebPKI

> Key Exchange???

DNS

HTTPS

Facebook



1.1.1.1



ISP (e.g.
Chunghwa)



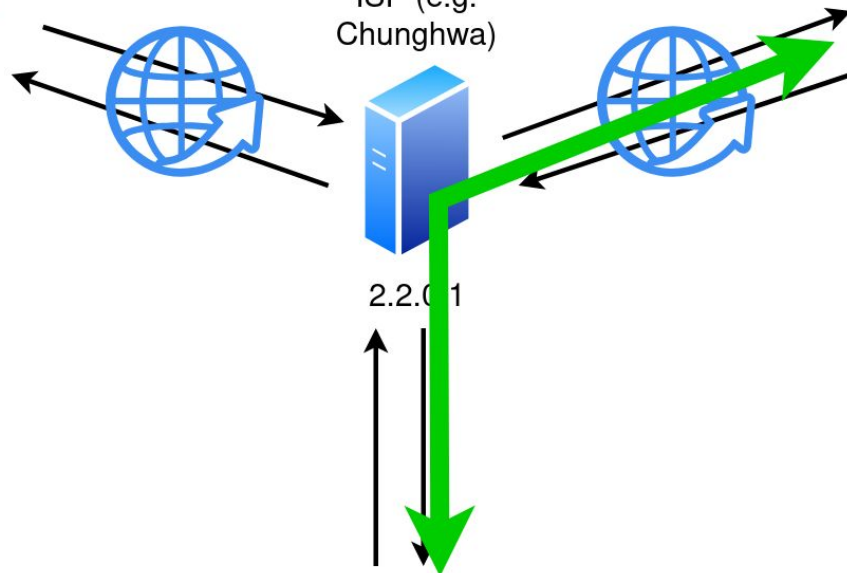
2.2.0.1



55.55.55.55



2.2.2.2



Problem?

Privacy Concerns

- > ISP can see DNS requests
- > They can see which website you're accessing (just the name)
- > ISP can see HTTP requests
- > They can see WHAT you're doing on the website

Privacy Concerns

- > ISP can see DNS requests
- > They can see which website you're accessing (just the name)
- ~~> ISP can see HTTP requests~~
- ~~> They can see WHAT you're doing on the website~~

DNS



1.1.1.1

Facebook



55.55.55.55

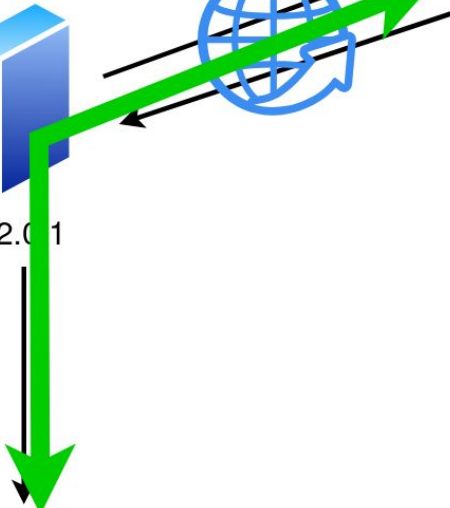
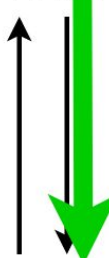
ISP (e.g.
Chunghwa)



2.2.0.1



2.2.2.2



DNS

Facebook

DNS-over-HTTPS



1.1.1.1

ISP (e.g.
Chunghwa)



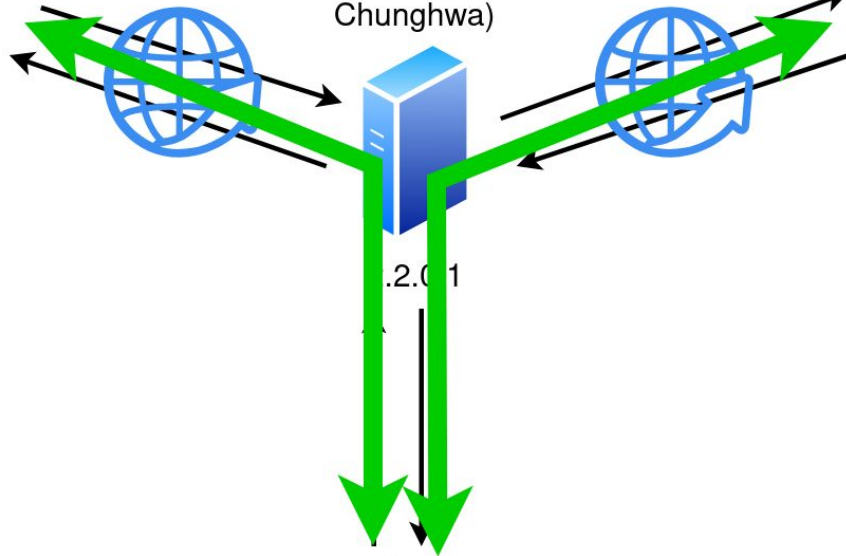
.2.0.1



55.55.55.55



2.2.2.2



Privacy Concerns

- ~~ISP can see DNS requests~~
- ~~They can see which website you're accessing (just the name)~~
- ~~ISP can see HTTP requests~~
- ~~They can see WHAT you're doing on the website~~

Problem?

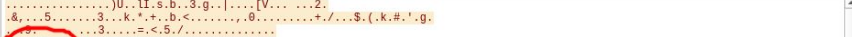
Introducing some tools

cURL - Make HTTP(S) requests on the command line

Wireshark - View the internet “postcards” of your machine

The image displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes: a packet list on the left, a packet details pane in the center, and a packet bytes pane on the right. The packet list shows a series of captured packets, with the selected packet being a TCP Reset (RST) from 192.168.1.100 to 192.168.1.101, port 80. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data of the selected packet, including the Ethernet II header, IP header, and TCP segment.

[illegible]



```
coscup.org.....
.....h2.http/1.1.....
.....+.....3.....+.....GS...q.C.).P..h.C'v'..Pg...vz.2!.NdCq.#...w3/3.1.wt.
|y..s1.Z'.....Q.6a.ADK'.....x..J.K.16.@..w.W.....]
|u.C.M|2.Y.....W...S.
|.....G.M.Z.N.
|.....S.....W.m.0.H.....q.....L.....2.....X.X.Z.....4.....>u.....!W.D.120Nn.X...O!>.....K.].....6.CP.....j
|.....r6.....U
Z'"+.A.G.....A.h...Y.-d
.....K.v.d.J.....Q..9.z..e.....Ea-7.....vak.....{.....Fh...H...0..3x.9.uQ.....
|.FF.|.E..GS.....r..l.v0 <7'..G2...5v.u.....7.8f.e.wL..G6'..A.....)*$*.....v.....z.of..3R'..qdfz.S4.=z...Q7.....I..|.
|.....B..4.S.....C..I..d..a.....T.....e.....gD..X|.E'.....l.....3..rQ.....D..f.....=.....
|3f'.....10.K/E.....2.....;G.....v.....Y.....j-p.m.....(.....
|.....F..f4.C..q.....V.....Y.....;s.....3.....0..6.p.....Wa.....12.....<.....Z.....W.....a.....v>.....?b.....c.....#!d.....PKh
|d.x.....t.....N.....@A.C&Z.07.....7.....p.....|.....1W.2
|.bl.s.....t.....=.....(%&.....)*.....G.....U.C.<.....H1.....*M.....#j.....[d15..b.....Q..n.....>.....l.....6.....2q.....s.E/.....0.....NX.1..
|.....4.....P.....T.....1K.....7.....Y.....L.WT.....h.....U|..m..Z.....R.....D.....<k.C.V.....l.....%>3x&^..i..T.B0..h'.Cg.....5.g.6.
|.....z.18.D..Bs.G.|X.....M8.....8.....hQ.....|Z.....0.....x.6|.....5M.a|.....0.....0.....z.....?2l.....u.D4.
|.....>.....S.....
|.....3.....7.....Z.....F9u.....|.....(J.X.....2V.....
|&.....5.....3.....k.....+.....b.....3.d.....L.....8.....2.....v.....g.....I.....*.....HbC.....1.....4.....f.....v.....qd.....cx.R..9.....j15.;m.DL.....\v
|q.[eS.M.FQ..E..6.....a.....a.....4...../.....H.....
|.....N.J.....J..M36.#.....1.....j.....j|L.....I..n.....<j.....A.....|.....4v>K.P..|.....%..At.8.....|.....>.....j.H.....*..R#.....5+.....47.....W.....m/.....
|.....F0.....>.....T.....1.....*.....X7.4.....[8].....76.....1.....6.....R.H.y.mw.....nM.*
|.....+.....H.....S.....R.....U.....G.....
|X...V|3.v.....'l.jnR|X.F=x.Q..7.....uX.....
|n.y.....(2...../.....%.....H^R|X.F=x.Q..7.....e24..M.KkRZ.....C.....[J;W.CX;=..m..RC.....0.....].....5.....F.....H.....[EU.....8.....f.....
|.....>.....e.....R.....|.....>.....B.E.
|T.R.6.3.1.....W.....%.....iF.....X
|.....0.....1.....AW.....
|.....0.....J.....J.....[SA]cX.....I..0.9f.....T.....0h.....Ka^..C.....p.....3.....m.....K.....R3.....Z.....Z.....C.....[.....<.....>.....m.....].....J.....
|1w.....0.....r.....D.....0.....V.....
```

```

00000000  .V.....7.....1.X.^&.2.b.....I.#.X8{.....&.....
00000001  j}.V.....3.2R1I..fH.I.gZ6..h.=.s6G0.....0.....Q..4q..}.....(.%f.....'N%k.V).....B..P.....R.....?&.s.....{.....
00000002  .%.%.....H.....s..PS.....F.....f^..%.....P..m1..l#.....N..y>7d.6.5v.....
00000003  .....2.....YL.....9Y.....%.....EK.X.V.....f.....f.....I.....I..I.q.3..?7.h.2A..
00000004  .....w.....v.....bl.....
00000005  iE6..d.h.....c.....7R.....7.....5..I.t.....^7.....Qa.....I.....w.....5.....n".
00000006  B.
00000007  T..P.....x0.....v>.gi.
00000008  +0.X.j}.^q.....q.....0.....#?.....V.....D..v..v/7.ykA.....tI...
00000009  ..3.2......01.....uZ6.....3?(.....u>.....9w.ZP?.....X.....
0000000A  O.X.b.....w.....K..a.....N.....R.....z.....u>.....P..c^
0000000B  y0Z.....X.X.UQ.....
0000000C  .....3R.....+f}.Z20.....f.....f.....bq.....0.72.2..0..$c0.....1<u.q.o.j}0.....(.....xkP.....u>.....P.....U.I.....
0000000D  .%.J.....1.I.....6fMR.....ph.....L.I..RT.....0.....0.qk.....f}.X.....}.....MO.....[e.....q.A..#?.....s3.....
0000000E  .....+Lsn.8.j}0..m.^0r.e}.Y.c7..ym.....dY.....1.a.3..28.V.\&.....H.jy..J>S3..N.....W.....&.....wX.....t.....uc[y.....
0000000F  1..0r.....j.....
00000010  .....6.....l.....B.....8.....7...../Kb.b.....DuR.....k.....L.....4(.....2.X^m.....f.....C.....k..h.I.....FZ3.ZV.I.S.u.z.Sr3.....
00000011  .....e.....f.....u.....Zr.....9.....4.....%f.L.....j.....<.....G.....G.....).....h.....^.....Adm.....}.....ZS6D.....}.....%.....T.8X.....}.....
00000012  EKW.....v.D.....
00000013  .....Q.....
00000014  .....v.....A.....^.....b=q.....r.f.4..W.s.5.....w.IRX^..B9..m.#J..j.....}.....4.....0.....P.....Z0.....Sr.....y.....}.....I'f.>}.L.....
00000015  .....7..F.51?7.A.9.0.....8l.....G.....=.....1.....8..9HY.....ow.Ir.....G.....N..h..X.....}.....1.....K.K.....L.....X.....rV.....
00000016  .....US.....7.....6.....#.....JM.P.....0.....(X.....2.....n8.....E.2.zg.j}.....f.....-79.....n.....f.....
00000017  u.....g.....g.....#.....w.....+E.....S..R.VS.W.0..E.....3.....I.....f}.a.....^.....L.....V.....u.....BQ.....}.....^.....D.....v.....v.....
00000018  .....jz.4G..l.0.k^A.....
00000019  .....?.....4.....(.....T.....E.....WS.....Q.....C.....?.....AA.....>cl.....D(S.D.....).....w.A.Q.....0..e4.S.....Q.....a.....12..2n.....=.....i.....0?.....}.....X.....0^.....U.....
0000001A  G.....Jfcw?7.y.QYw.....^.....P..Pg..B4.....?.....IA.....j}.t.....H.....h.....N.....j.....}.....0^.....F=71.rw.....ne..gC}sdc0.....{.....ml.c.....g.....r.....T.....=.....I.....
0000001B  .....Q.....Q.....L.....e.....F.....S.....X.....0.....k.....j.....0.....Hgg5.9v;m).3.....\.....
0000001C  .....1x.....1-D.....0.....J.....}.....}.....7.....h.....
0000001D  .....l>.....PD.....0.....8y.....
0000001E  .....>.....O.....C.....0.....Tw..Jp.Fy.....f.....>^.....S.....F.....UE@r.....m.....7h.....t.....r.....R.....u^A.....[.....51Vn.....$.....f.....r.....0.....
0000001F  .....B.....JxoF.....
00000020  .....m)y).G.....hN4.....A.....#.....#.....14.L1.....}.....>A.6N.....}.....SA.....R/hz6..Y.JK^.....
00000021  .....<.....C.....C.....
00000022  ...../.....j9.....7E.....c.....
00000023  .....F.....P.....Xh1A.....c.....q.....q.....Ley.....RP.P.....5Ry.....
00000024  .....BZ8.....EB[A.....^.....a.....^.....W.s.e.....<.....D.....Tr.....A.....0.....Y.....2.....K.m.j.....+.....0.....V.....6.....}.....e.....N5^.....V.....d.....7F.....qE.....jw.c.....$.

```

coscup.org.

.....h2.http/1.1...

6.4

.....+.....~.....

..)y..si.*Z.....Q.Ga.ADK"....x... \J.K..10

.u.c`M,]2.y.....W...S.

.....G.m.Z.N.

.....S. W..m.0.H.....~q.....L-...2.

..f&.....u

,...

Z.. "+..A.G.....A.h...Y.~d

ClientHello



ServerHello



ClientKeyExchange



Finished(client)



Finished(server)



Client



Server

Why include ServerName?

>

Why include ServerName?

- > Multiple websites on single IP address
- > Used by server to determine which Encryption key to use
- > RFC 3546 in 2003!

Privacy Concerns

- ~~➤ ISP can see DNS requests~~
- ~~➤ They can see which website you're accessing (just the name)~~
- ~~➤ ISP can see HTTP requests~~
- ~~➤ They can see WHAT you're doing on the website~~
- > ISP can see the TLS Handshake
- > They can see WHICH website you're accessing (just the name)

What can they do?

- > Change data?

What can they do?

➤ ~~Change data?~~

What can they do?

~~> Change data?~~

> Block websites?

ClientHello



ServerHello



ClientKeyExchange



Finished(client)



Finished(server)



Client



Server

ClientHello (SNI=facebook.com)



ServerHello



ClientKeyExchange



Finished(client)



Finished(server)



Client



Server

Solution?

>

Solution?

> Encrypt the SNI (yes really)

Solution?

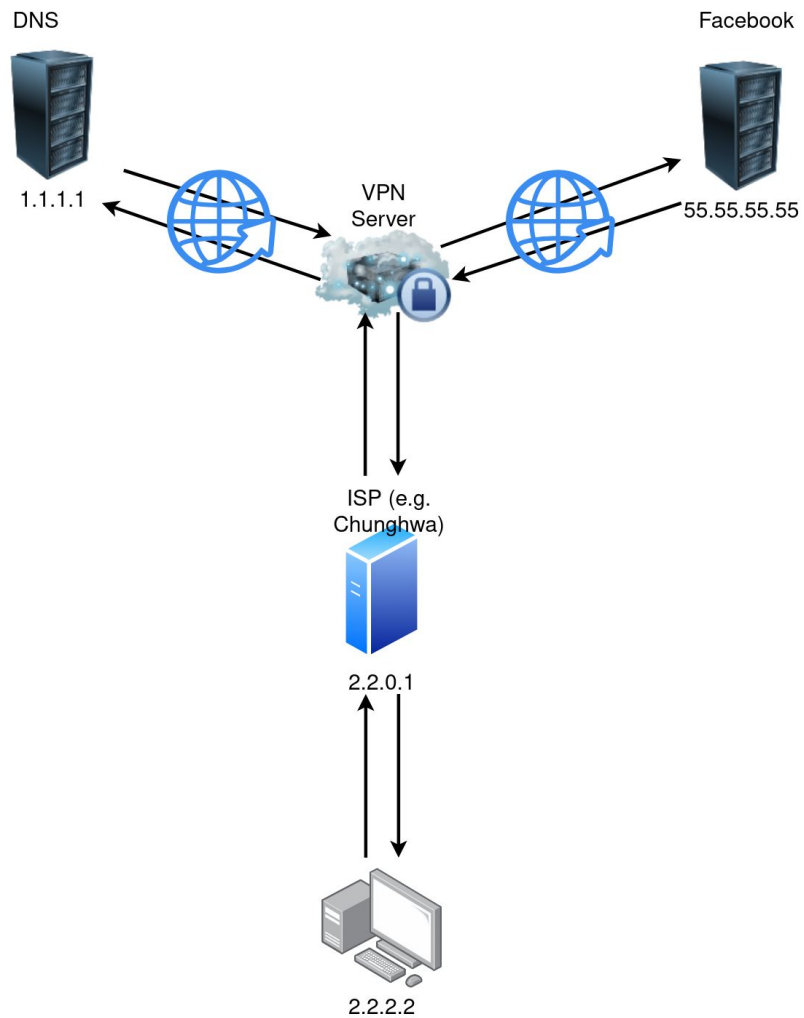
- > Encrypt the SNI (yes really)
- > Encrypted Client Hello (RFC 9849)

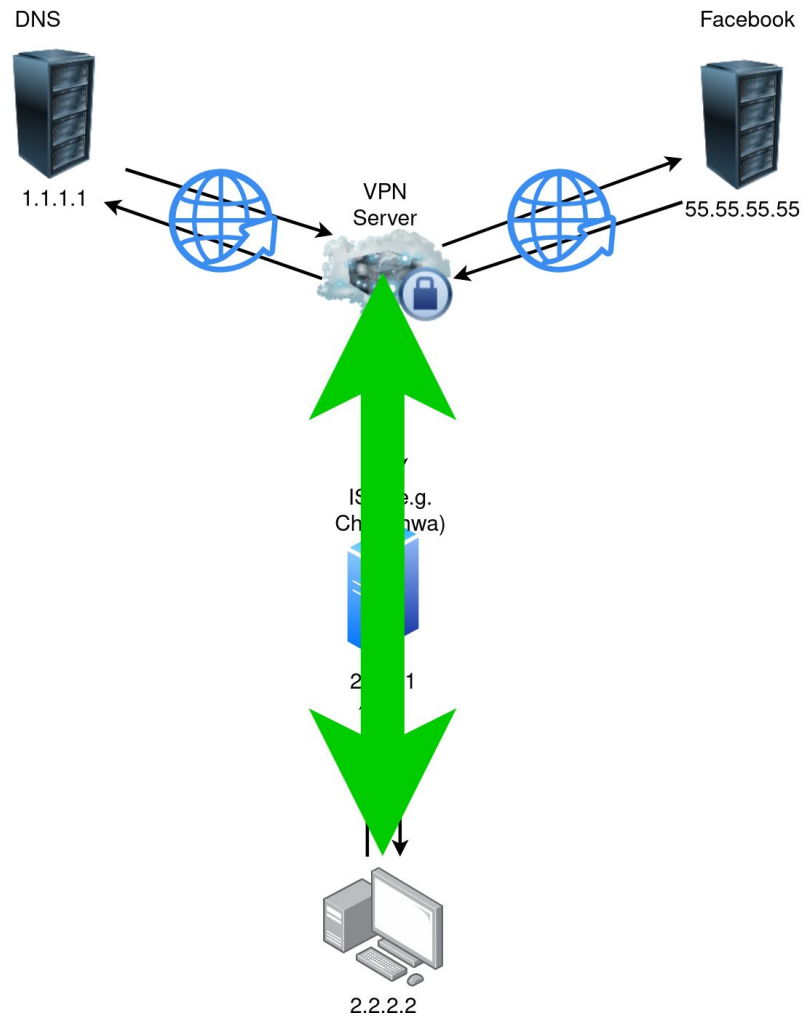
```
Frame 1393: Packet, 1956 bytes on wire (15648 bits), 1956 bytes captured (15648 bytes) on interface 0
Ethernet II, Src: Intel_3e:a5:58 (8c:c6:81:3e:a5:58), Dst: ZyxelCommuni_94:d3:d3:3d:3d:3d
Internet Protocol Version 4, Src: 10.99.3.65, Dst: 213.108.108.101
Transmission Control Protocol, Src Port: 49144, Dst Port: 443, Seq: 1, Ack: 1, Len: 1956
Transport Layer Security
  [Stream index: 6]
  TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 1885
    Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 1881
      Version: TLS 1.2 (0x0303)
      Random: df6b17eaeed10ecf1ab35d7866bd4170dafc880daa608ed701256a869cc3a72f6
      Session ID Length: 32
      Session ID: 39243b2512220effaadfb63ca77b929f4e169670161e0b7b8de38bf4c0fa
      Cipher Suites Length: 32
      Cipher Suites (16 suites)
      Compression Methods Length: 1
      Compression Methods (1 method)
      Extensions Length: 1776
      Extension: server_name (len=12) name=defo.ie
      Extension: extended_master_secret (len=0)
      Extension: renegotiation_info (len=1)
      Extension: supported_groups (len=16)
      Extension: ec_point_formats (len=2)
      Extension: session_ticket (len=0)
      Extension: application_layer_protocol_negotiation (len=14)
      Extension: status_request (len=5)
      Extension: delegated_credentials (len=10)
      Extension: signed_certificate_timestamp (len=0)
      Extension: key_share (len=1327) X25519MLKEM768, x25519, secp256r1
      Extension: supported_versions (len=5) TLS 1.3, TLS 1.2
      Extension: signature_algorithms (len=24)
      Extension: psk_key_exchange_modes (len=2)
      Extension: record_size_limit (len=2)
      Extension: compress_certificate (len=7)
      Extension: encrypted_client_hello (len=281)
        Type: Encrypted Client Hello (65033)
        Length: 281
        Client Hello Type: Outer Client Hello (0)
      Cipher Suite: HKDF-SHA256/ChaCha20Poly1305
      Config ID: 227
      Enc length: 32
      Enc: 4bed17acd379dfc77151177a7e4c1dfaadd1ffcfcdf76b832f6de4f9595c57eb7
      Payload length: 239
      Payload [...]: 865735ad48a3755eb3a6986dbae9ecc2d6170af55a94a5a0ea82d02c
      [JA4: t13d1617h2_86a278354501_3cbfd9057e0d]
      [JA4_r: t13d1617h2_002f,0035,009c,009d,1301,1302,1303,c00a,c013,c014,c02e]
      [JA3 Fullstring: 771,4865-4867-4866-49195-49199-52393-52392-49196-49200-49201-52394-52395-52396-52397-52398-52399-52400-52401-52402-52403-52404-52405-52406-52407-52408-52409-52410-52411-52412-52413-52414-52415-52416-52417-52418-52419-52420-52421-52422-52423-52424-52425-52426-52427-52428-52429-52430-52431-52432-52433-52434-52435-52436-52437-52438-52439-52440-52441-52442-52443-52444-52445-52446-52447-52448-52449-52450-52451-52452-52453-52454-52455-52456-52457-52458-52459-52460-52461-52462-52463-52464-52465-52466-52467-52468-52469-52470-52471-52472-52473-52474-52475-52476-52477-52478-52479-52480-52481-52482-52483-52484-52485-52486-52487-52488-52489-52490-52491-52492-52493-52494-52495-52496-52497-52498-52499-52500-52501-52502-52503-52504-52505-52506-52507-52508-52509-52510-52511-52512-52513-52514-52515-52516-52517-52518-52519-52520-52521-52522-52523-52524-52525-52526-52527-52528-52529-52530-52531-52532-52533-52534-52535-52536-52537-52538-52539-52540-52541-52542-52543-52544-52545-52546-52547-52548-52549-52550-52551-52552-52553-52554-52555-52556-52557-52558-52559-52560-52561-52562-52563-52564-52565-52566-52567-52568-52569-52570-52571-52572-52573-52574-52575-52576-52577-52578-52579-52580-52581-52582-52583-52584-52585-52586-52587-52588-52589-52590-52591-52592-52593-52594-52595-52596-52597-52598-52599-52600-52601-52602-52603-52604-52605-52606-52607-52608-52609-52610-52611-52612-52613-52614-52615-52616-52617-52618-52619-52620-52621-52622-52623-52624-52625-52626-52627-52628-52629-52630-52631-52632-52633-52634-52635-52636-52637-52638-52639-52640-52641-52642-52643-52644-52645-52646-52647-52648-52649-52650-52651-52652-52653-52654-52655-52656-52657-52658-52659-52660-52661-52662-52663-52664-52665-52666-52667-52668-52669-52670-52671-52672-52673-52674-52675-52676-52677-52678-52679-52680-52681-52682-52683-52684-52685-52686-52687-52688-52689-52690-52691-52692-52693-52694-52695-52696-52697-52698-52699-52700-52701-52702-52703-52704-52705-52706-52707-52708-52709-52710-52711-52712-52713-52714-52715-52716-52717-52718-52719-52720-52721-52722-52723-52724-52725-52726-52727-52728-52729-52730-52731-52732-52733-52734-52735-52736-52737-52738-52739-52740-52741-52742-52743-52744-52745-52746-52747-52748-52749-52750-52751-52752-52753-52754-52755-52756-52757-52758-52759-52760-52761-52762-52763-52764-52765-52766-52767-52768-52769-52770-52771-52772-52773-52774-52775-52776-52777-52778-52779-52780-52781-52782-52783-52784-52785-52786-52787-52788-52789-52790-52791-52792-52793-52794-52795-52796-52797-52798-52799-52800-52801-52802-52803-52804-52805-52806-52807-52808-52809-52810-52811-52812-52813-52814-52815-52816-52817-52818-52819-52820-52821-52822-52823-52824-52825-52826-52827-52828-52829-52830-52831-52832-52833-52834-52835-52836-52837-52838-52839-52840-52841-52842-52843-52844-52845-52846-52847-52848-52849-52850-52851-52852-52853-52854-52855-52856-52857-52858-52859-52860-52861-52862-52863-52864-52865-52866-52867-52868-52869-52870-52871-52872-52873-52874-52875-52876-52877-52878-52879-52880-52881-52882-52883-52884-52885-52886-52887-52888-52889-52890-52891-52892-52893-52894-52895-52896-52897-52898-52899-52900-52901-52902-52903-52904-52905-52906-52907-52908-52909-52910-52911-52912-52913-52914-52915-52916-52917-52918-52919-52920-52921-52922-52923-52924-52925-52926-52927-52928-52929-52930-52931-52932-52933-52934-52935-52936-52937-52938-52939-52940-52941-52942-52943-52944-52945-52946-52947-52948-52949-52950-52951-52952-52953-52954-52955-52956-52957-52958-52959-52960-52961-52962-52963-52964-52965-52966-52967-52968-52969-52970-52971-52972-52973-52974-52975-52976-52977-52978-52979-52980-52981-52982-52983-52984-52985-52986-52987-52988-52989-52990-52991-52992-52993-52994-52995-52996-52997-52998-52999-53000-53001-53002-53003-53004-53005-53006-53007-53008-53009-53010-53011-53012-53013-53014-53015-53016-53017-53018-53019-53020-53021-53022-53023-53024-53025-53026-53027-53028-53029-53030-53031-53032-53033-53034-53035-53036-53037-53038-53039-53040-53041-53042-53043-53044-53045-53046-53047-53048-53049-53050-53051-53052-53053-53054-53055-53056-53057-53058-53059-53060-53061-53062-53063-53064-53065-53066-53067-53068-53069-53070-53071-53072-53073-53074-53075-53076-53077-53078-53079-53080-53081-53082-53083-53084-53085-53086-53087-53088-53089-53090-53091-53092-53093-53094-53095-53096-53097-53098-53099-53100-53101-53102-53103-53104-53105-53106-53107-53108-53109-53110-53111-53112-53113-53114-53115-53116-53117-53118-53119-53120-53121-53122-53123-53124-53125-53126-53127-53128-53129-53130-53131-53132-53133-53134-53135-53136-53137-53138-53139-53140-53141-53142-53143-53144-53145-53146-53147-53148-53149-53150-53151-53152-53153-53154-53155-53156-53157-53158-53159-53160-53161-53162-53163-53164-53165-53166-53167-53168-53169-53170-53171-53172-53173-53174-53175-53176-53177-53178-53179-53180-53181-53182-53183-53184-53185-53186-53187-53188-53189-53190-53191-53192-53193-53194-53195-53196-53197-53198-53199-53200-53201-53202-53203-53204-53205-53206-53207-53208-53209-53210-53211-53212-53213-53214-53215-53216-53217-53218-53219-53220-53221-53222-53223-53224-53225-53226-53227-53228-53229-53230-53231-53232-53233-53234-53235-53236-53237-53238-53239-53240-53241-53242-53243-53244-53245-53246-53247-53248-53249-53250-53251-53252-53253-53254-53255-53256-53257-53258-53259-53260-53261-53262-53263-53264-53265-53266-53267-53268-53269-53270-53271-53272-53273-53274-53275-53276-53277-53278-53279-53280-53281-53282-53283-53284-53285-53286-53287-53288-53289-53290-53291-53292-53293-53294-53295-53296-53297-53298-53299-53300-53301-53302-53303-53304-53305-53306-53307-53308-53309-53310-53311-53312-53313-53314-53315-53316-53317-53318-53319-53320-53321-53322-53323-53324-53325-53326-53327-53328-53329-53330-53331-53332-53333-53334-53335-53336-53337-53338-53339-53340-53341-53342-53343-53344-53345-53346-53347-53348-53349-53350-53351-53352-53353-53354-53355-53356-53357-53358-53359-53360-53361-53362-53363-53364-53365-53366-53367-53368-53369-53370-53371-53372-53373-53374-53375-53376-53377-53378-53379-53380-53381-53382-53383-53384-53385-53386-53387-53388-53389-53390-53391-53392-53393-53394-53395-53396-53397-53398-53399-53400-53401-53402-53403-53404-53405-53406-53407-53408-53409-53410-53411-53412-53413-53414-53415-53416-53417-53418-53419-53420-53421-53422-53423-53424-53425-53426-53427-53428-53429-53430-53431-53432-53433-53434-53435-53436-53437-53438-53439-53440-53441-53442-53443-53444-53445-53446-53447-53448-53449-53450-53451-53452-53453-53454-53455-53456-53457-53458-53459-53460-53461-53462-53463-53464-53465-53466-53467-53468-53469-53470-53471-53472-53473-53474-53475-53476-53477-53478-53479-53480-53481-53482-53483-53484-53485-53486-53487-53488-53489-53490-53491-53492-53493-53494-53495-53496-53497-53498-53499-53500-53501-53502-53503-53504-53505-53506-53507-53508-53509-53510-53511-53512-53513-53514-53515-53516-53517-53518-53519-53520-53521-53522-53523-53524-53525-53526-53527-53528-53529-53530-53531-53532-53533-53534-53535-53536-53537-53538-53539-53540-53541-53542-53543-53544-53545-53546-53547-53548-53549-53550-53551-53552-53553-53554-53555-53556-53557-53558-53559-53560-53561-53562-53563-53564-53565-53566-53567-53568-53569-53570-53571-53572-53573-53574-53575-53576-53577-53578-53579-53580-53581-53582-53583-53584-53585-53586-53587-53588-53589-53590-53591-53592-53593-53594-53595-53596-53597-53598-53599-53600-53601-53602-53603-53604-53605-53606-53607-53608-53609-53610-53611-53612-53613-53614-53615-53616-53617-53618-53619-53620-53621-53622-53623-53624-53625-53626-53627-53628-53629-53630-53631-53632-53633-53634-53635-53636-53637-53638-53639-53640-53641-53642-53643-53644-53645-53646-53647-53648-53649-53650-53651-53652-53653-53654-53655-53656-53657-53658-53659-53660-53661-53662-53663-53664-53665-53666-53667-53668-53669-53670-53671-53672-53673-53674-53675-53676-53677-53678-53679-53680-53681-53682-53683-53684-53685-53686-53687-53688-53689-53690-53691-53692-53693-53694-53695-53696-53697-53698-53699-53700-53701-53702-53703-53704-53705-53706-53707-53708-53709-53710-53711-53712-53713-53714-53715-53716-53717-53718-53719-53720-53721-53722-53723-53724-53725-53726-53727-53728-53729-53730-53731-53732-53733-53734-53735-53736-53737-53738-53739-53740-53741-53742-53743-53744-53745-53746-53747-53748-53749-53750-53751-53752-53753-53754-53755-53756-53757-53758-53759-53760-53761-53762-53763-53764-53765-53766-53767-53768-53769-53770-53771-53772-53773-53774-53775-53776-53777-53778-53779-53780-53781-53782-53783-53784-53785-53786-53787-53788-53789-53790-53791-53792-53793-53794-53795-53796-53797-53798-53799-53800-53801-53802-53803-53804-53805-53806-53807-53808-53809-53810-53811-53812-53813-53814-53815-53816-53817-53818-53819-53820-53821-53822-53823-53824-53825-53826-53827-53828-53829-53830-53831-53832-53833-53834-53835-53836-53837-53838-53839-53840-53841-53842-53843-53844-53845-53846-53847-53848-53849-53850-53851-53852-53853-53854-53855-53856-53857-53858-53859-53860-53861-53862-53863-53864-53865-53866-53867-53868-53869-53870-53871-53872-53873-53874-53875-53876-53877-53878-53879-53880-53881-53882-53883-53884-53885-53886-53887-53888-53889-53890-53891-53892-53893-53894-53895-53896-53897-53898-53899-53900-53901-53902-53903-53904-53905-53906-53907-53908-53909-53910-53911-53912-53913-53914-53915-53916-53917-53918-53919-53920-53921-53922-53923-53924-53925-53926-53927-53928-53929-53930-53931-53932-53933-53934-53935-53936-53937-53938-53939-53940-53941-53942-53943-53944-53945-53946-53947-53948-53949-53950-53951-53952-53953-53954-53955-53956-53957-53958-53959-53960-53961-53962-53963-53964-53965-53966-53967-53968-53969-53970-53971-53972-53973-53974-53975-53976-53977-53978-53979-53980-53981-53982-53983-53984-53985-53986-53987-53988-53989-53990-53991-53992-53993-53994-53995-53996-53997-53998-53999-54000-54001-54002-54003-54004-54005-54006-54007-54008-54009-54010-54011-54012-54013-54014-54015-54016-54017-54018-54019-54020-54021-54022-54023-54024-54025-54026-54027-54028-54029-54030-54031-54032-54033-54034-54035-54036-54037-54038-54039-54040-54041-54042-54043-54044-54045-54046-54047-54048-54049-54050-54051-54052-54053-54054-54055-54056-54057-54058-54059-54060-54061-54062-54063-54064-54065-54066-54067-54068-54069-54070-54071-54072-54073-54074-54075-54076-54077-54078-54079-54080-54081-54082-54083-54084-54085-54086-54087-54088-54089-54090-54091-54092-54093-54094-54095-54096-54097-54098-54099-54100-54101-54102-54103-54104-54105-54106-54107-54108-54109-54110-54111-54112-54113-54114-54115-54116-54117-54118-54119-54120-54121-54122-54123-54124-54125-54126-54127-54128-54129-54130-54131-54132-54133-54134-54135-54136-54137-54138-54139-54140-54141-54142-54143-54144-54145-54146-54147-54148-54149-54150-54151-54152-54153-54154-54155-54156-54157-54158-54159-54160-54161-54162-54163-54164-54165-54166-54167-54168-54169-54170-54171-54172-54173-54174-54175-54176-54177-54178-54179-54180-54181-54182-54183-54184-54185-54186-54187-54188-54189-54190-54191-54192-54193-54194-54195-54196-54197-54198-54199-54200-54201-54202-54203-54204-54205-54206-54207-54208-54209-54210-54211-54212-54213-54214-54215-54216-54217-54218-54219-54220-54221-54222-54223-54224-54225-54226-54227-54228-54229-54230-54231-54232-54233-54234-54235-54236-54237-54238-54239-54240-54241-54242-54243-54244-54245-54246-54247-54248-54249-54250-54251-54252-54253-54254-54255-54256-54257-54258-54259-54260-54261-54262-54263-54264-54265-54266-54267-54268-54269-54270-54271-5427
```

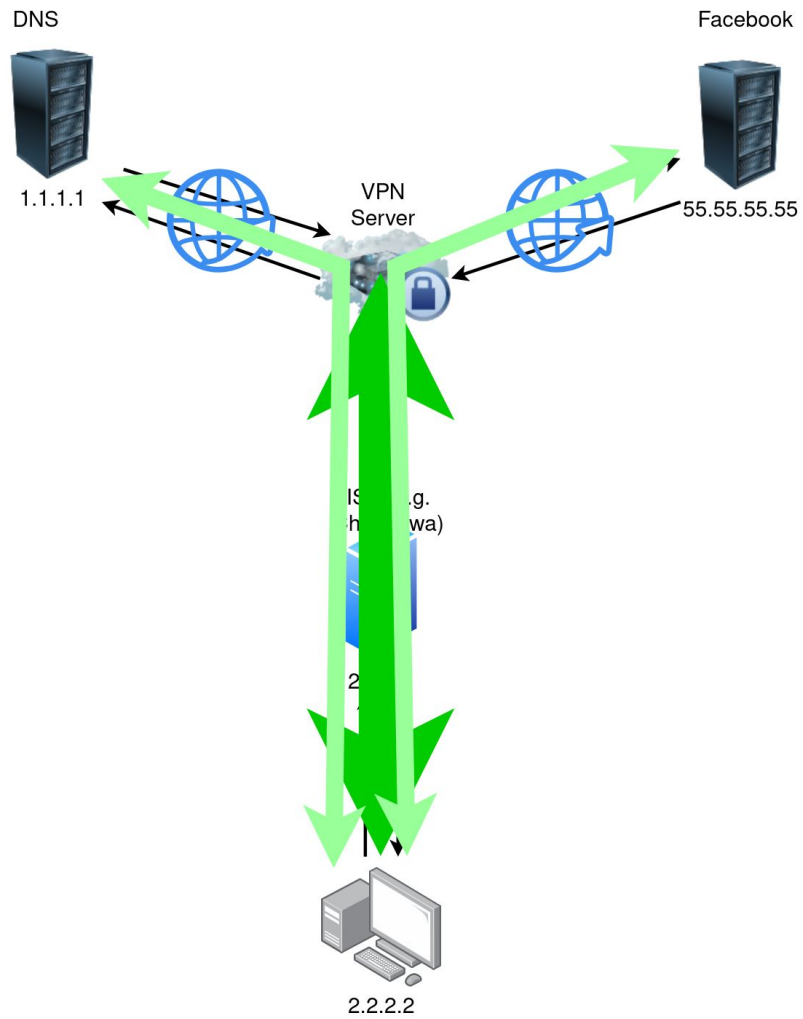
Solution?

- > Encrypt the SNI (yes really)
- > Encrypted Client Hello (RFC 9849)
- > Published 2026!

VPNS?





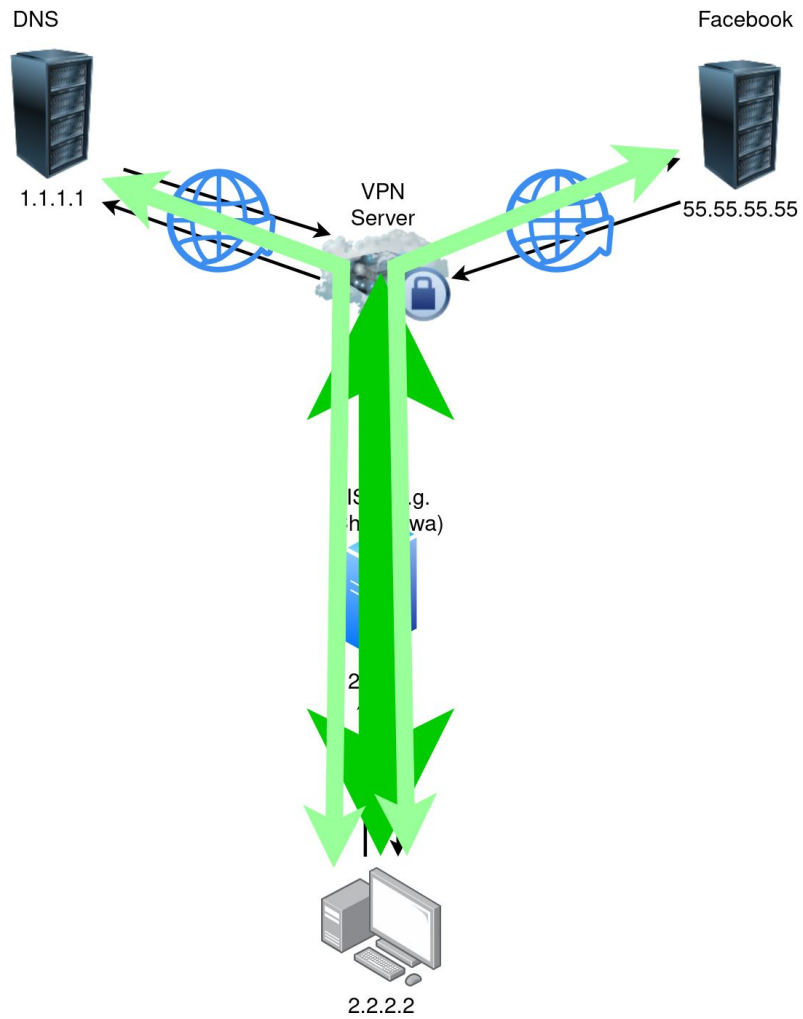


VPNS?

- > Encrypted tunnel to the VPN
- > ISP can only see random data

VPNS?

- > Encrypted tunnel to the VPN
- > ISP can only see random data
- > VPN becomes “new ISP”



VPNS?

- > Useful to circumvent Government / ISP level blocks
- > Usually in a different country

Questions?

Contact: poiasd@saxrag.com

