



# Melting the DNS Iceberg

Taking over your infrastructure Kaminsky style



**SEC Consult**

an atos company

 **James Kettle**  
@albinowax

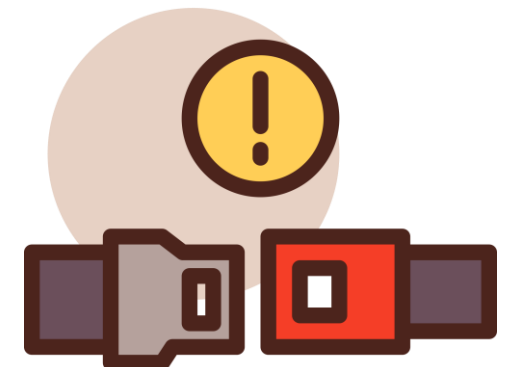
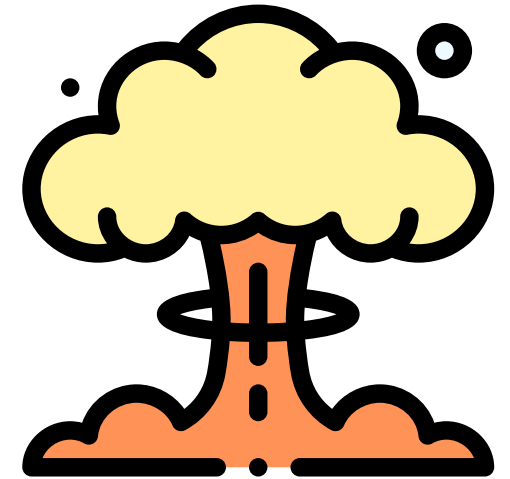
Using oldschool DNS attacks to pwn password resets. It's amazing that this still works - awesome finding by [@sec\\_consult!](#)



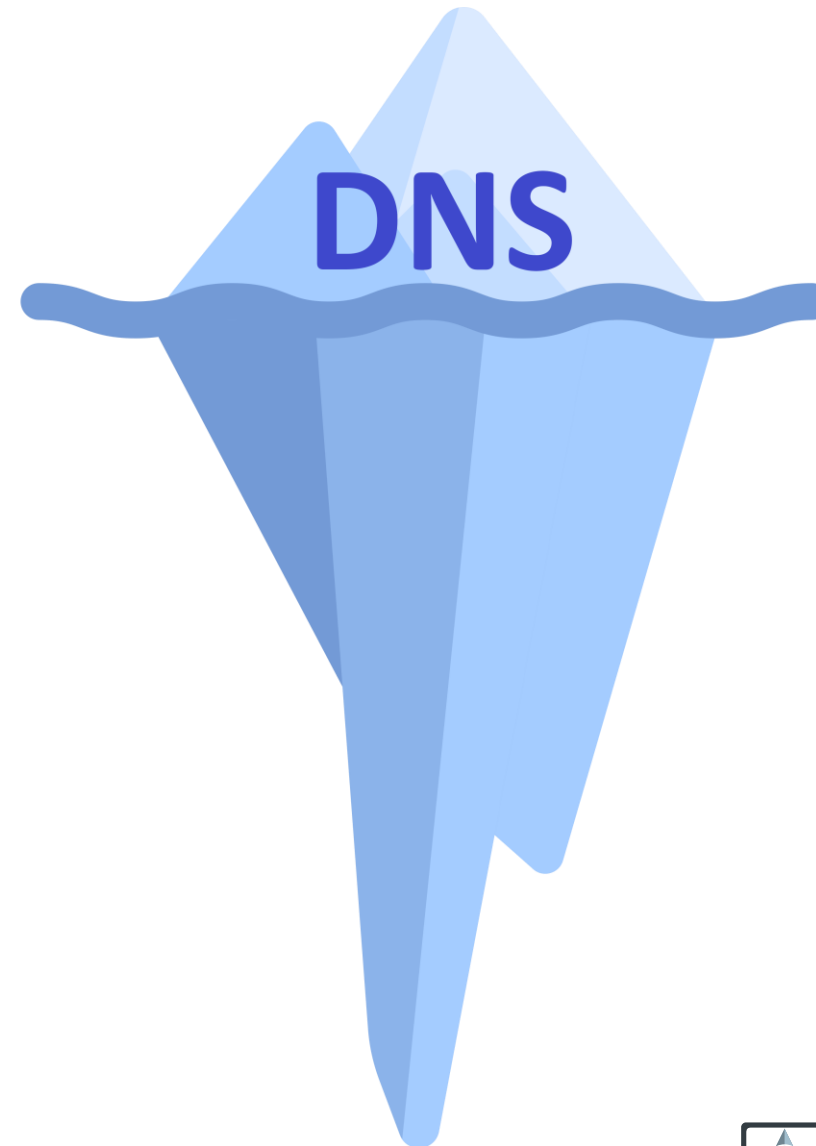
Forgot password? Taking over user accounts Kaminsky style  
The "Forgot password?" feature and how DNS vulnerabilities may allow the takeover of user accounts.  
[sec-consult.com](#)

3:27 PM · Jul 22, 2021 · Twitter Web App

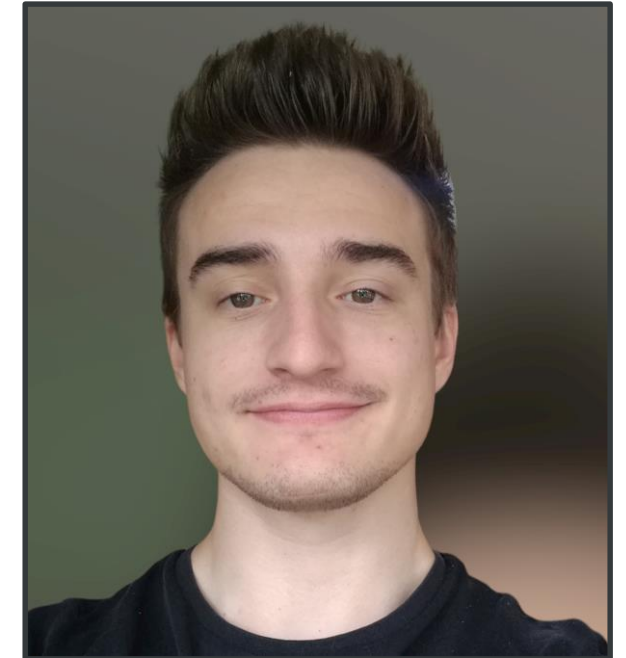
182 Retweets 8 Quote Tweets 543 Likes



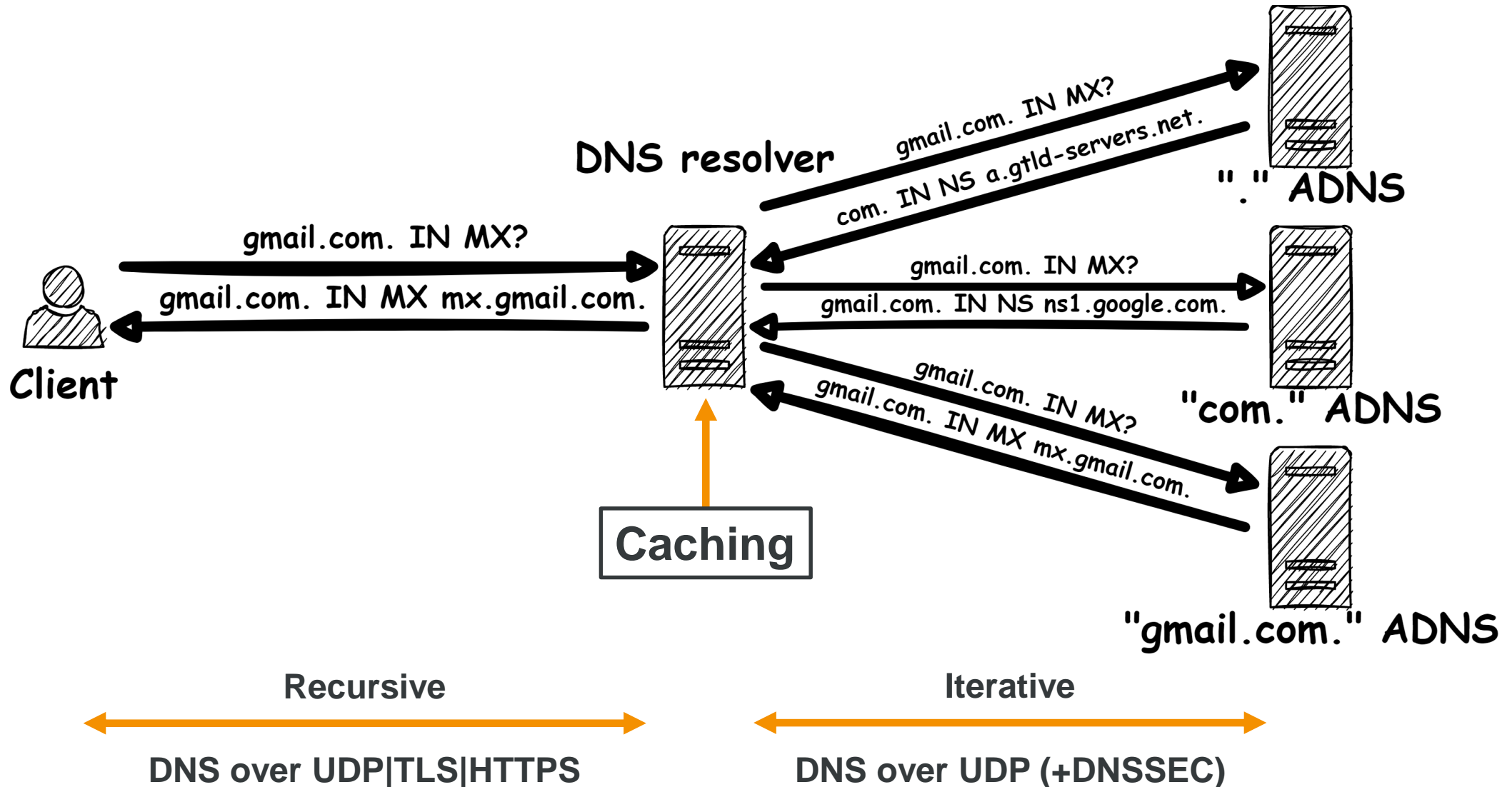
1. DNS Recap
2. The DNS Iceberg?
3. Melting the DNS Iceberg!
4. The Bottom of the Iceberg
5. Conclusion

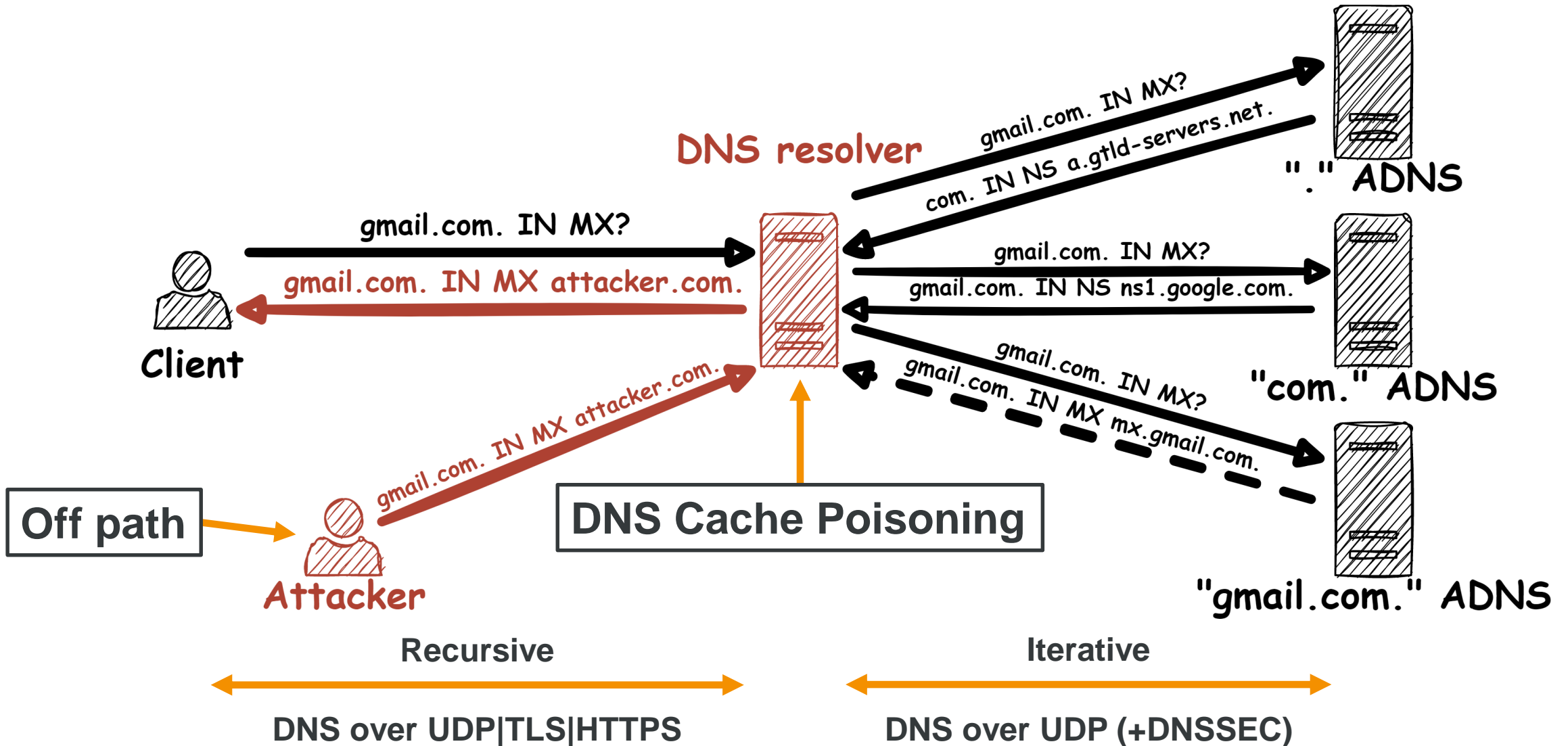


- Security Consultant @ SEC Consult since 2018
- Offensive Security Researcher, aka. broken stuff enthusiast
- **Not** a DNS (Security) Expert

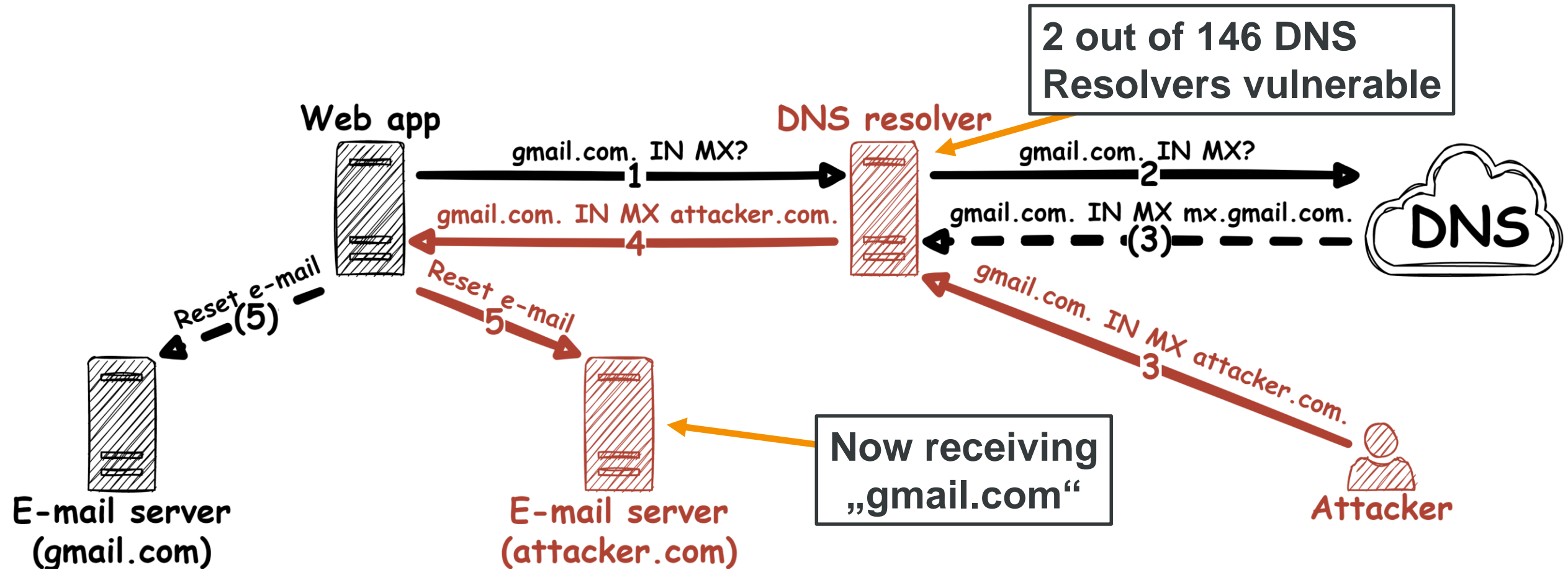


**Timo Longin**

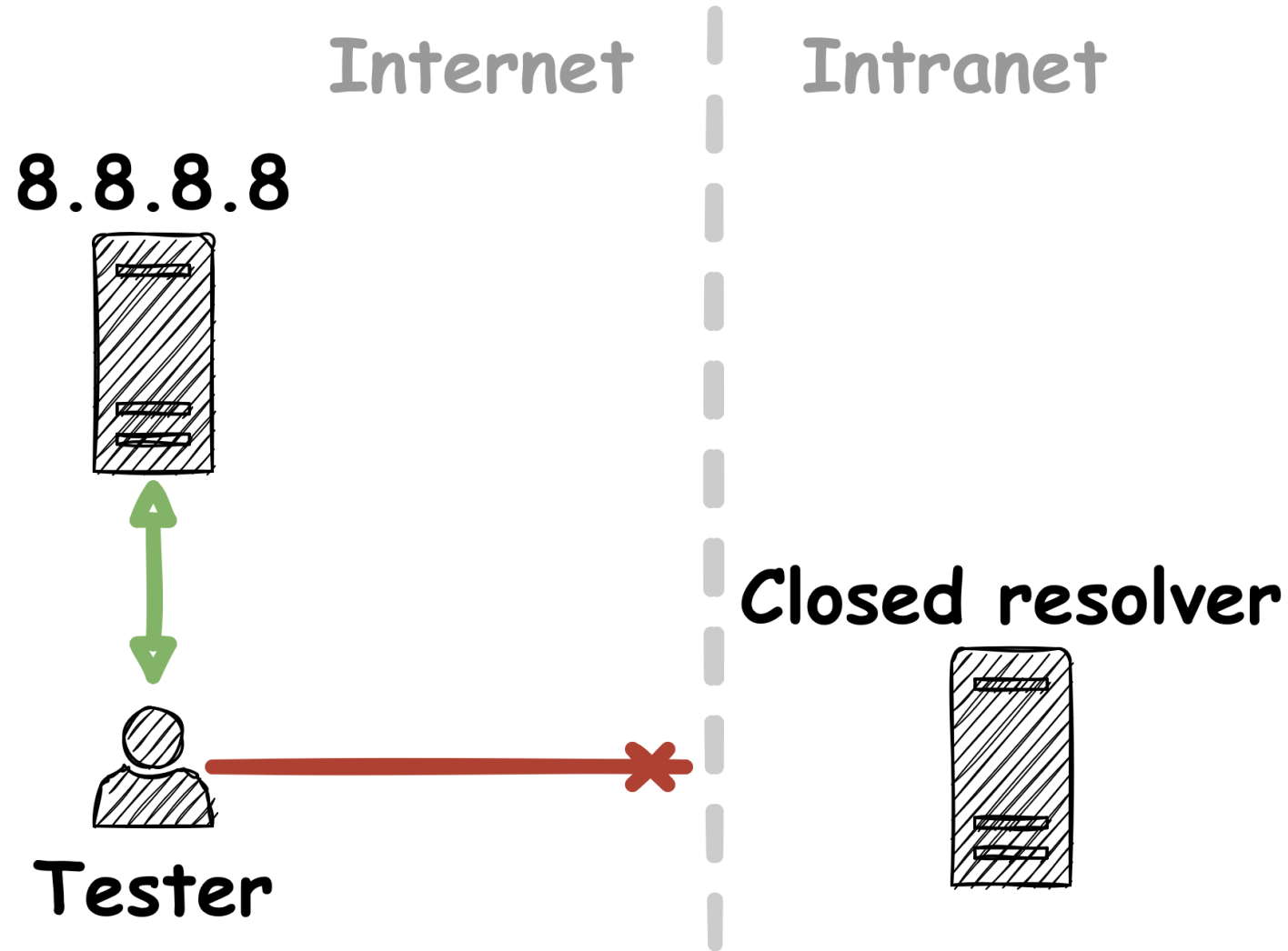


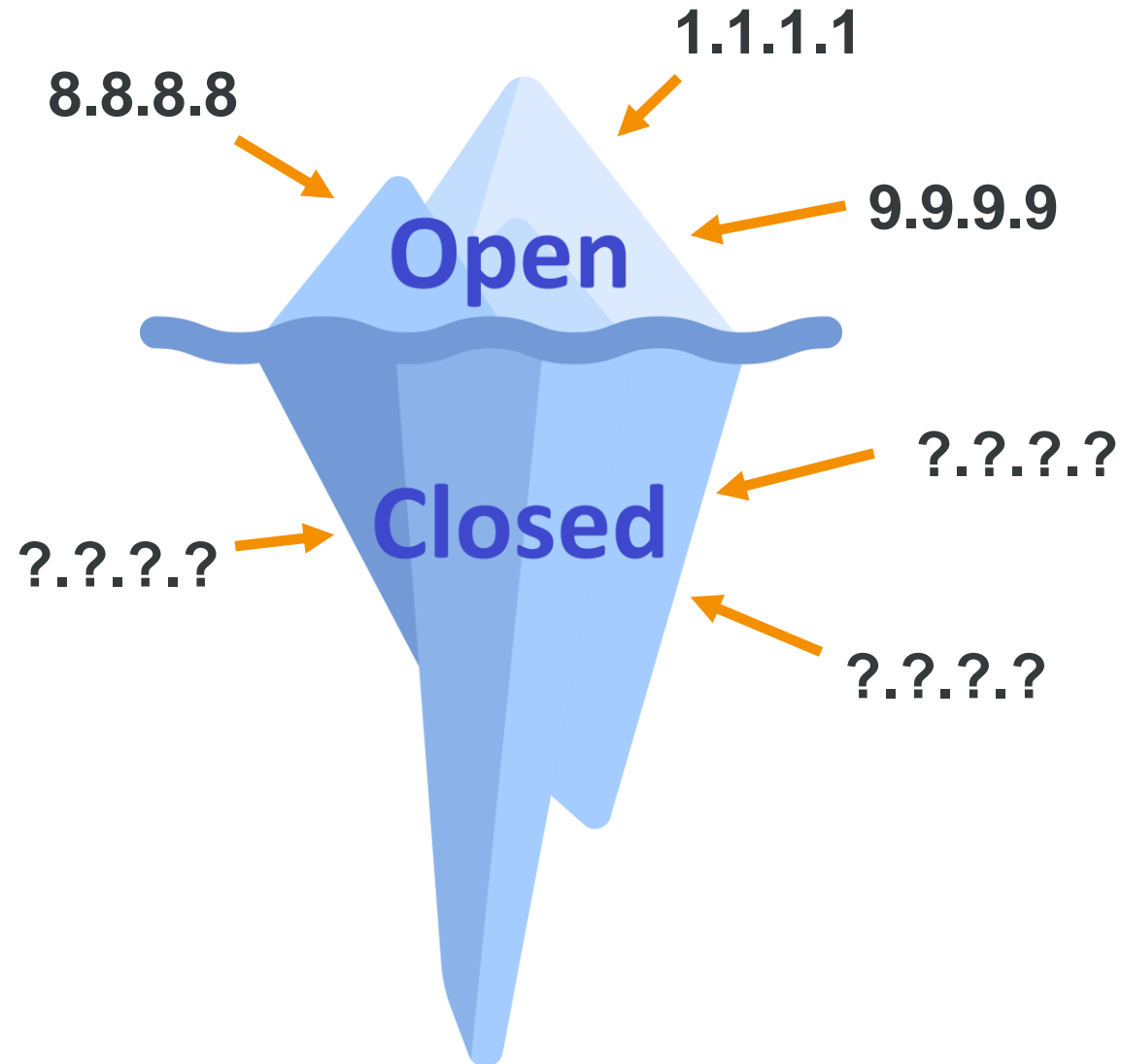


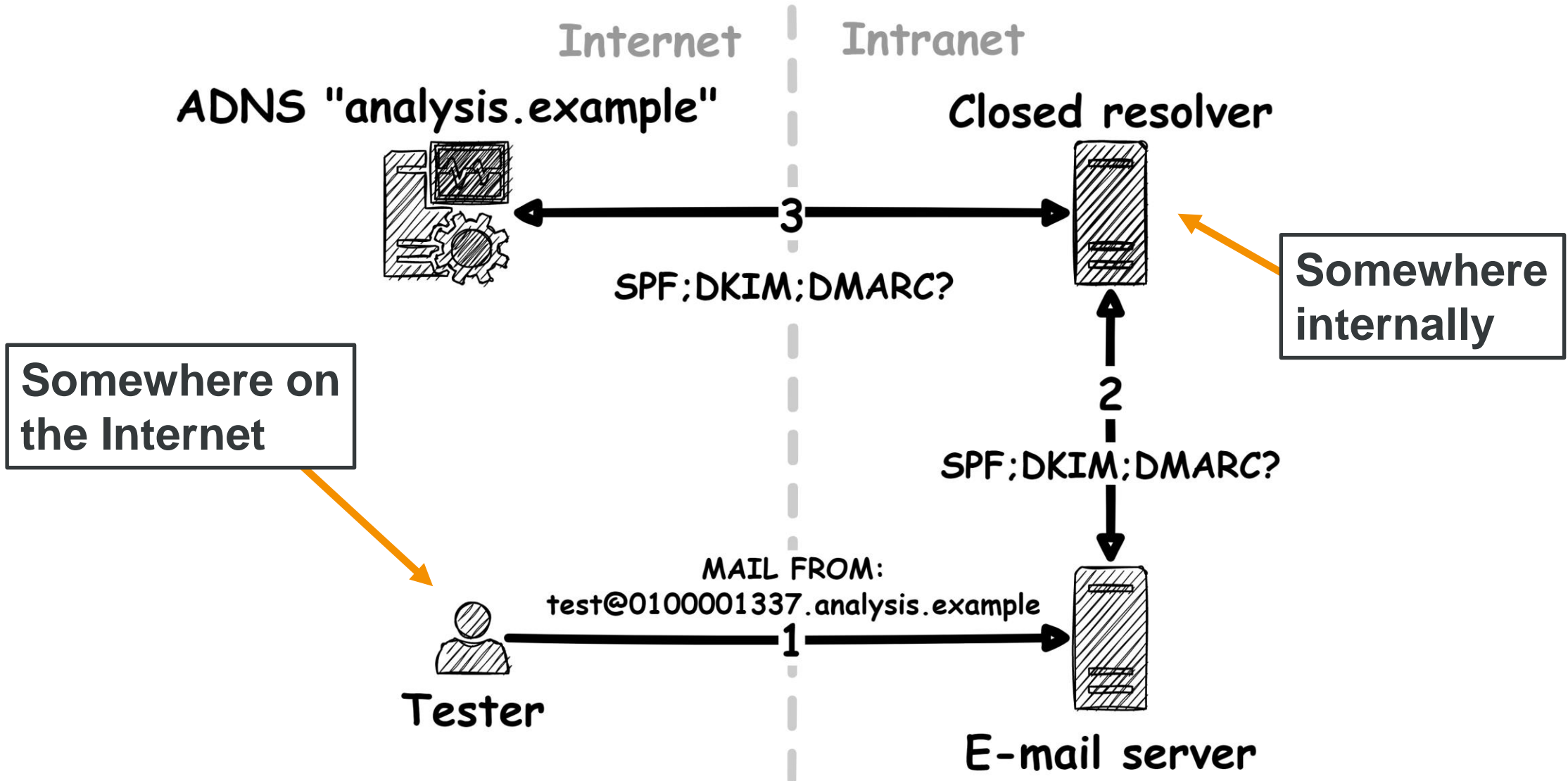












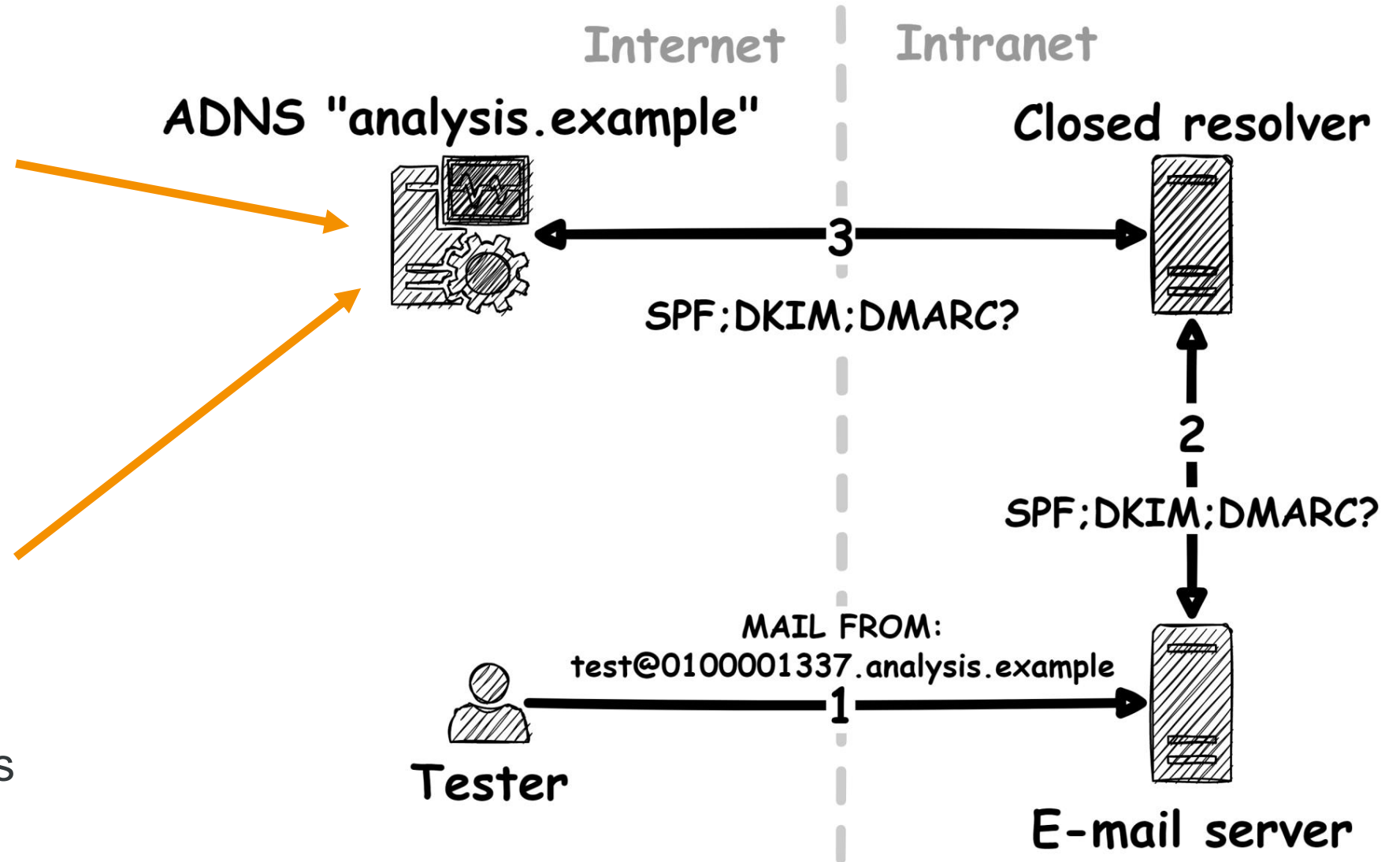
Scheffler, Sarah, et al. "The unintended consequences of email spam prevention." International Conference on Passive and Active Network Measurement. Springer, Cham, 2018.

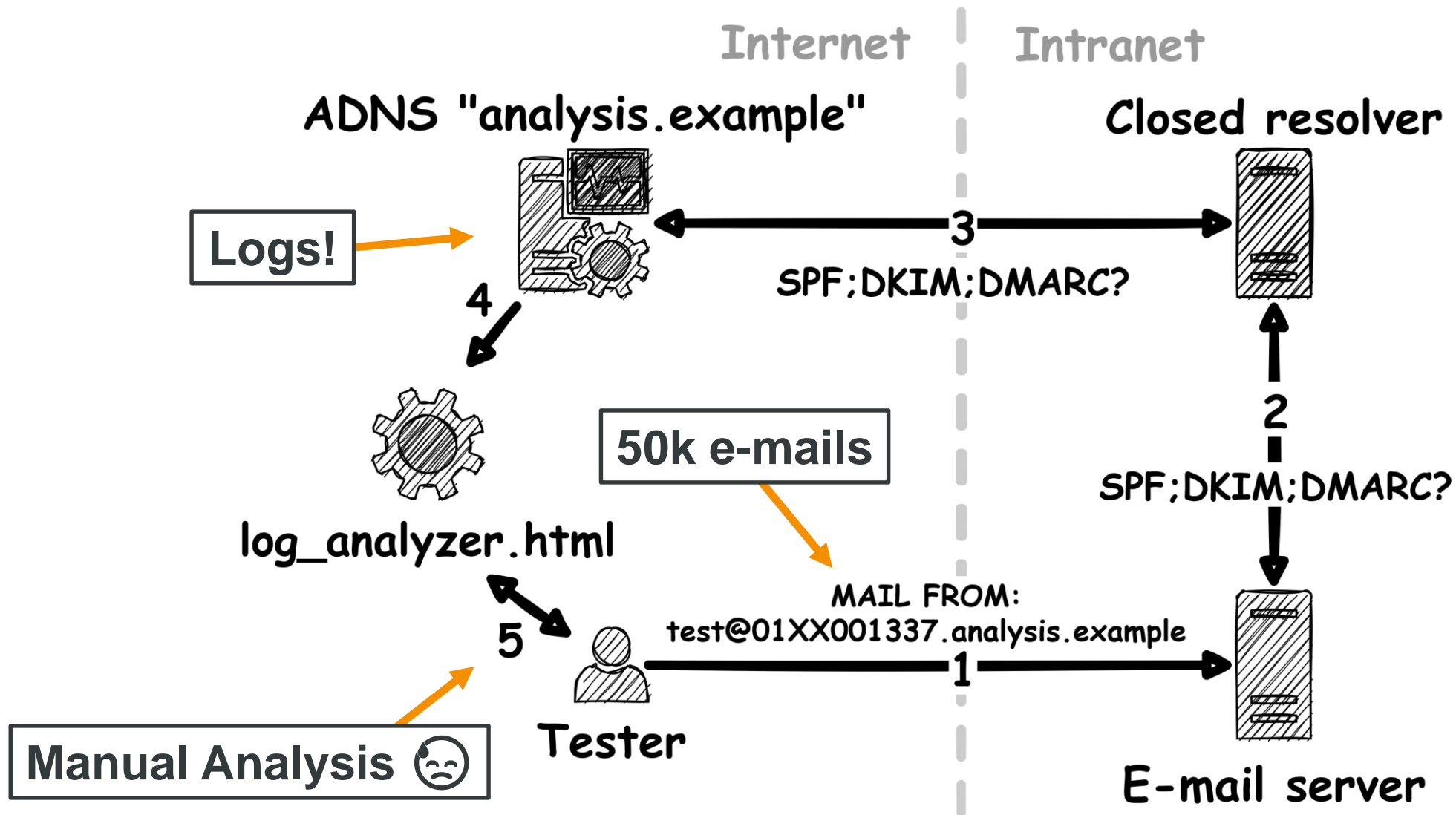
## Active Checks:

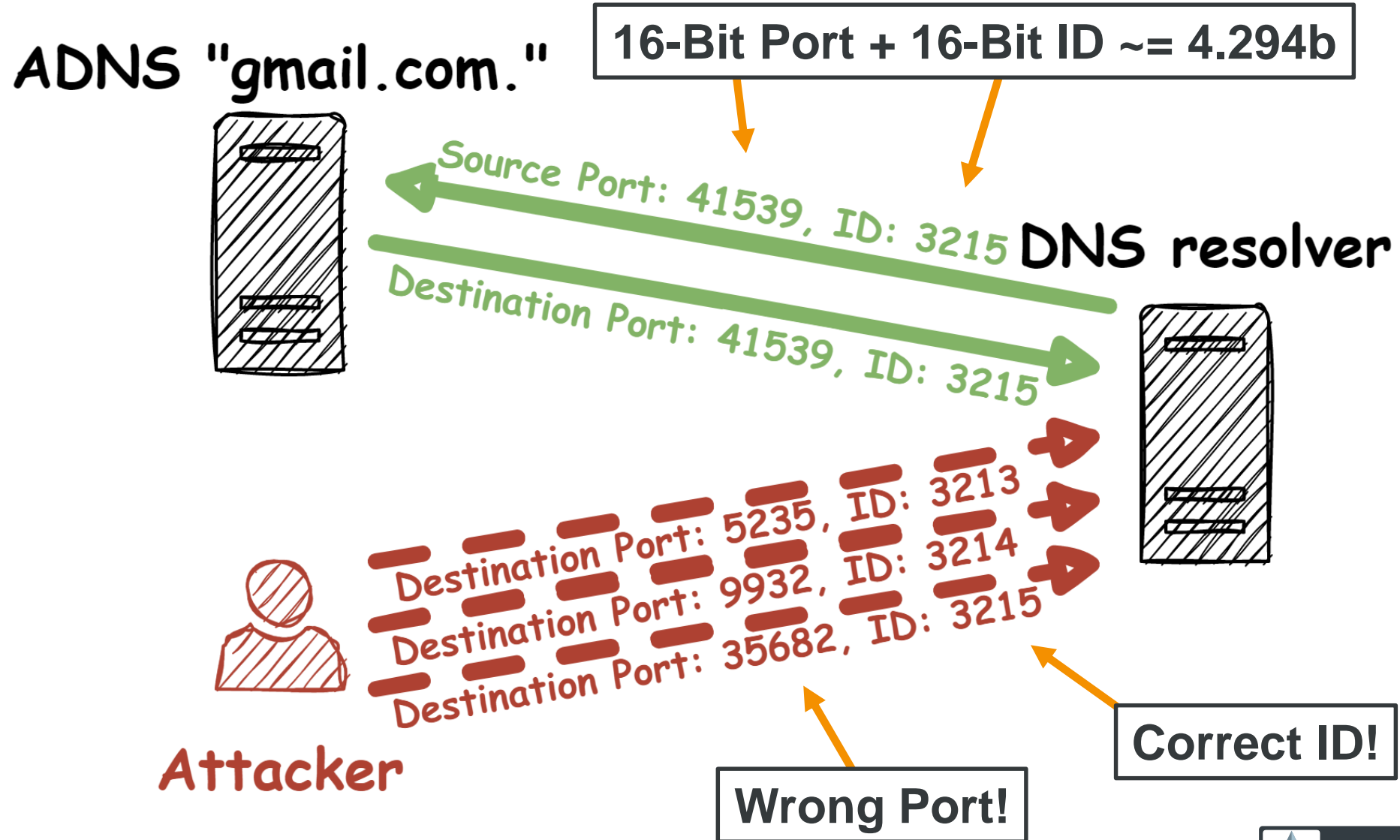
- IP Fragmentation
- Query Loops
- EDNS Usage
- ...

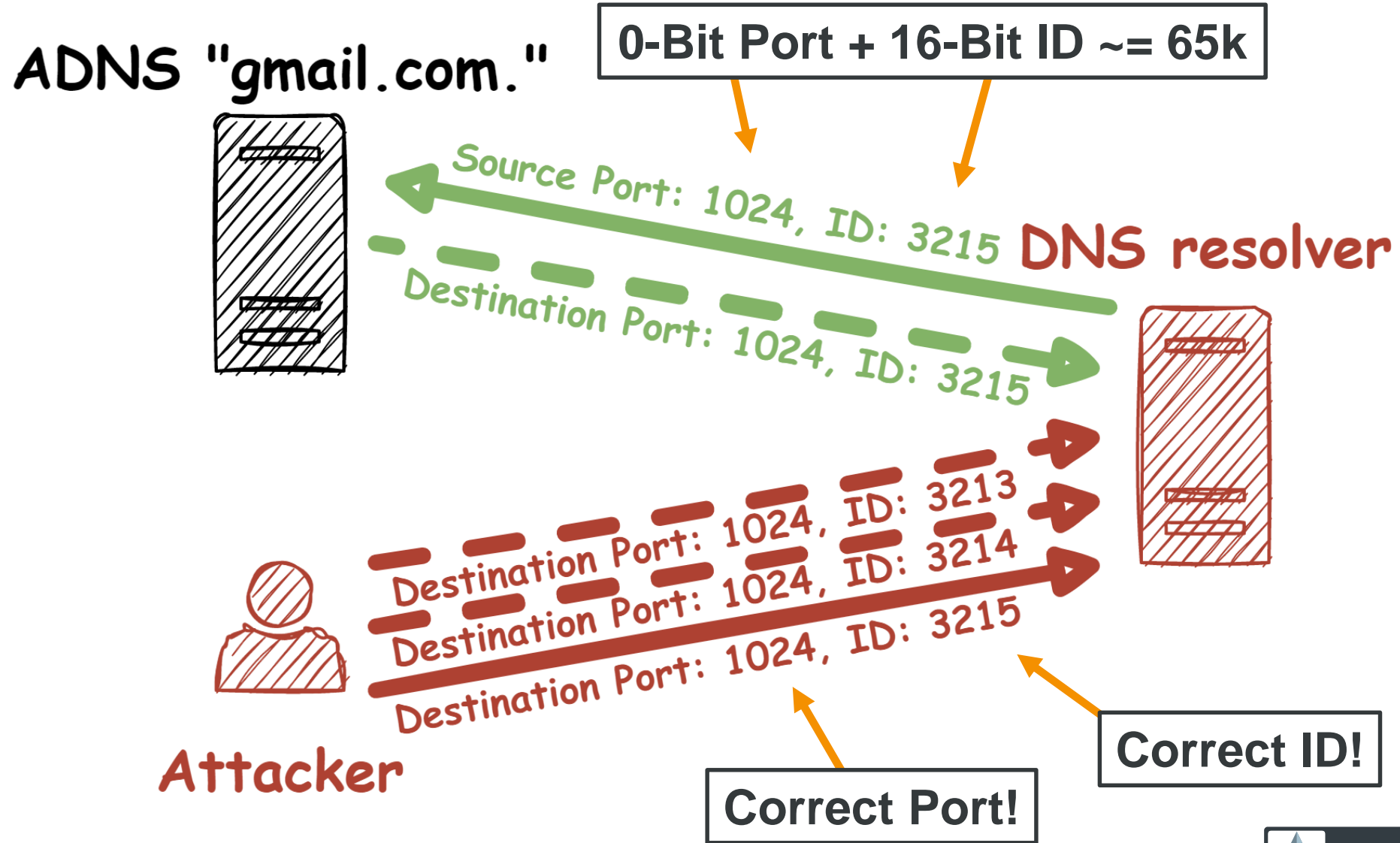
## Passive Checks:

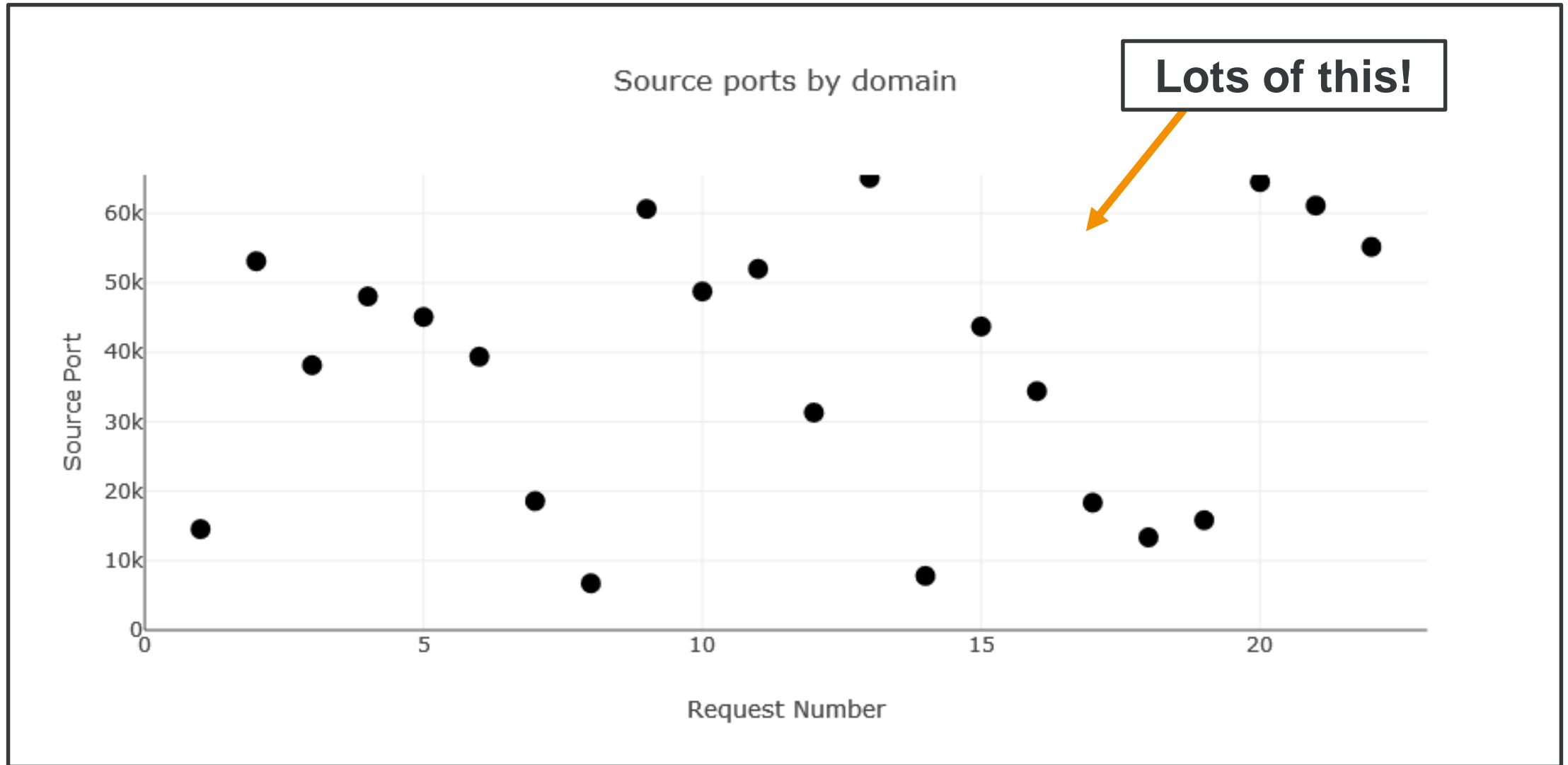
- UDP Source Ports
- DNSSEC
- DNS Cookies
- EDNS Max Size
- 0x20 Encoding
- Used IP Addresses
- ...



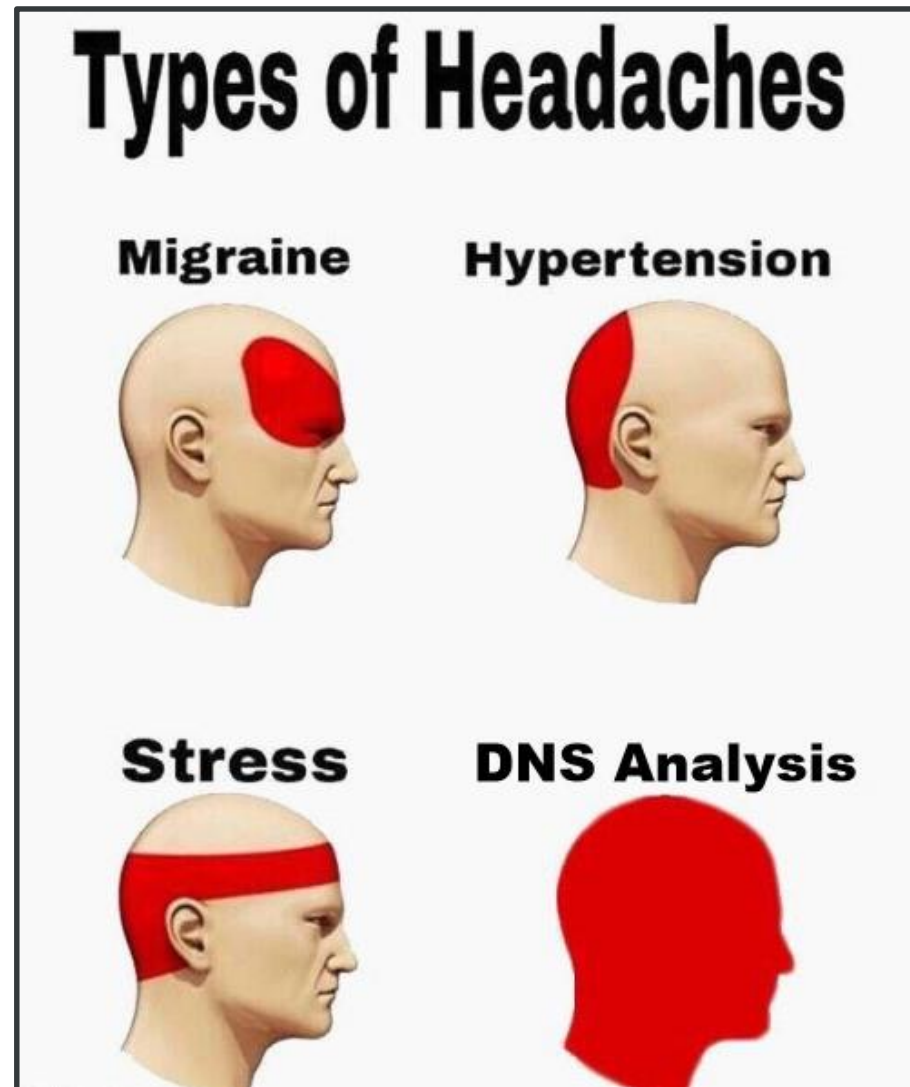


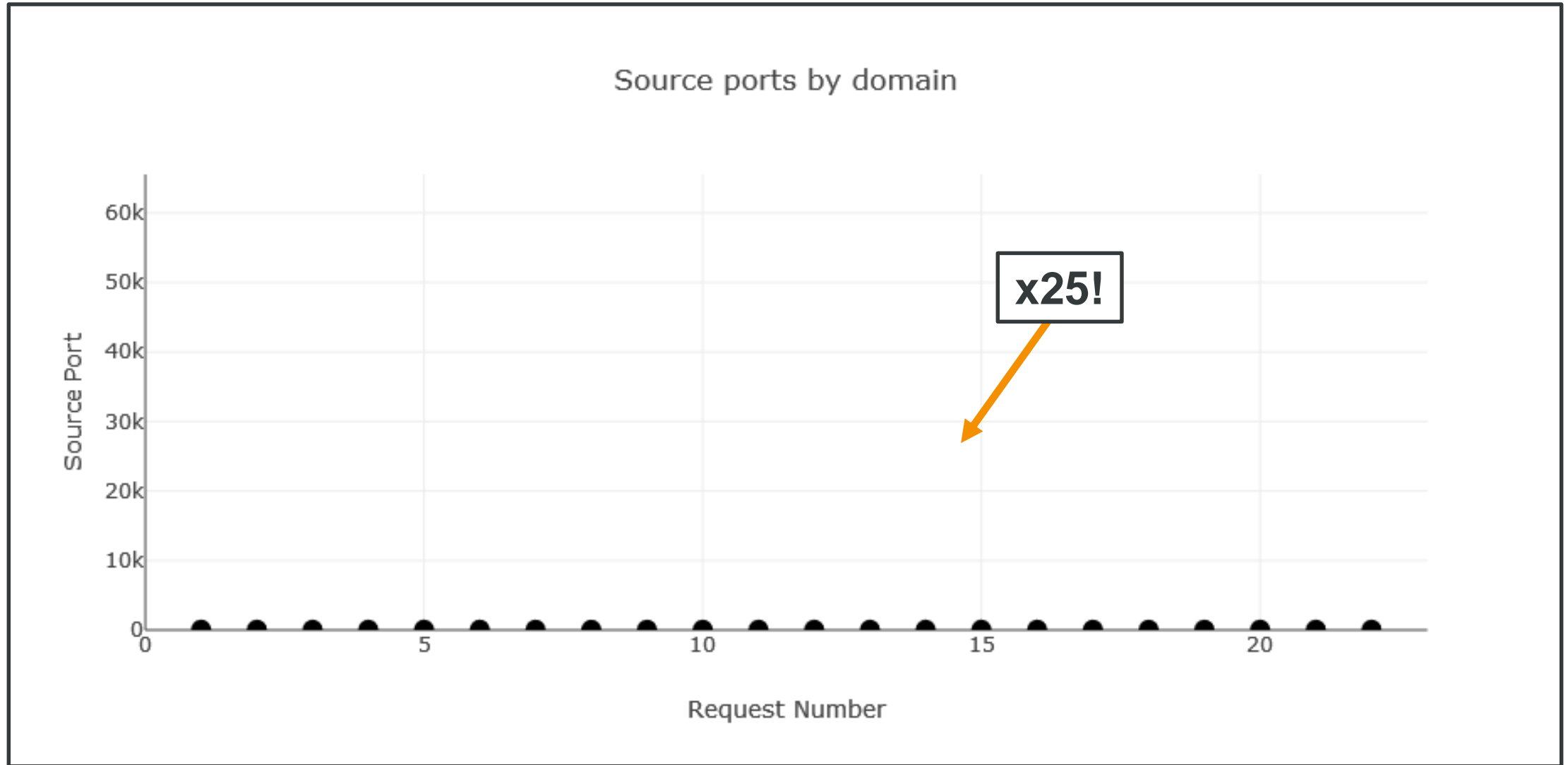












Analysis Server

Log Analyzer

<https://github.com/The-Login/DNS-Analysis-Server>

Utility Tools

DNS Triggers

# Melting the DNS Iceberg! – Burp Suite?!

Ben, Por

Hi all,

Thank you fo

The good ne

share in the

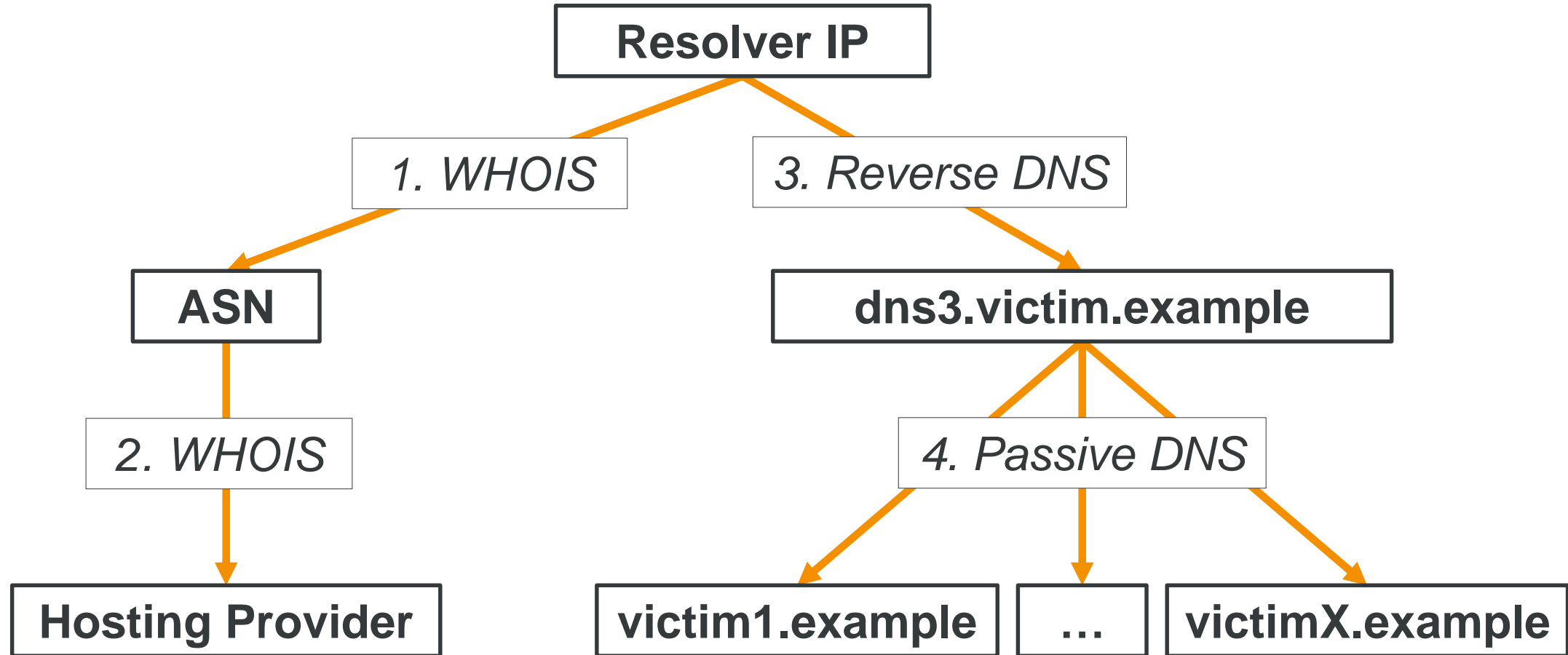
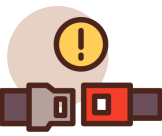
good news to

DNS Analyzer Help

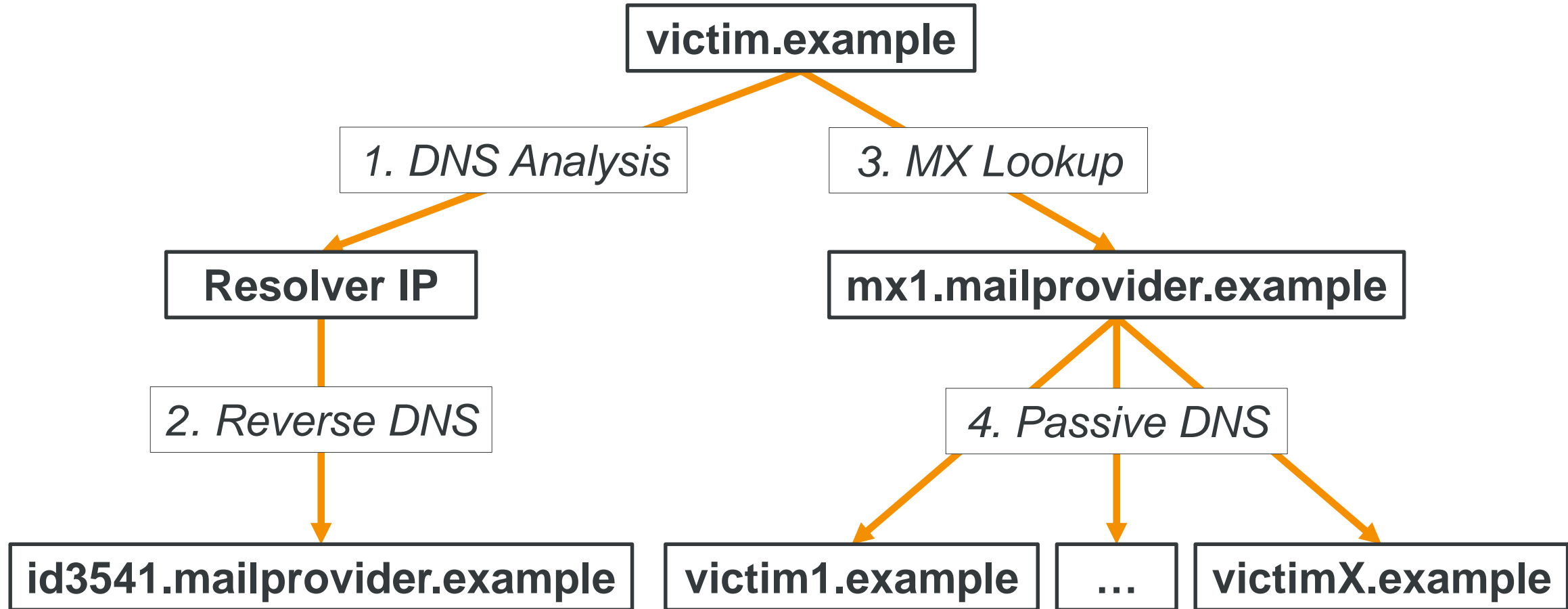
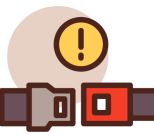
Copy to Clipboard Polling interval: 10000ms Poll now

| # | Collaborator ID  | Resolver IP    | Query Type | Timestamp                |
|---|------------------|----------------|------------|--------------------------|
| 0 | owoh9bmrfiqzh... | 172.253.206.35 | A          | 2022-11-06T09:24:20.700Z |
| 1 | owoh9bmrfiqzh... | 172.253.255.37 | A          | 2022-11-06T09:24:20.738Z |
| 2 | t4ymhguwnnqv...  | 66.185.117.244 | A          | 2022-11-06T09:25:01.855Z |
| 3 | t4ymhguwnnqv...  | 188.122.68.219 | A          | 2022-11-06T09:25:01.938Z |
| 4 | t4ymhguwnnqv...  | 188.122.68.218 | TXT        | 2022-11-06T09:25:09.594Z |
| 5 | t4ymhguwnnqv...  | 188.122.68.218 | A          | 2022-11-06T09:27:24.142Z |

# Melting the DNS Iceberg! – Going down the Rabbit Hole #1



# Melting the DNS Iceberg! – Going down the Rabbit Hole #2

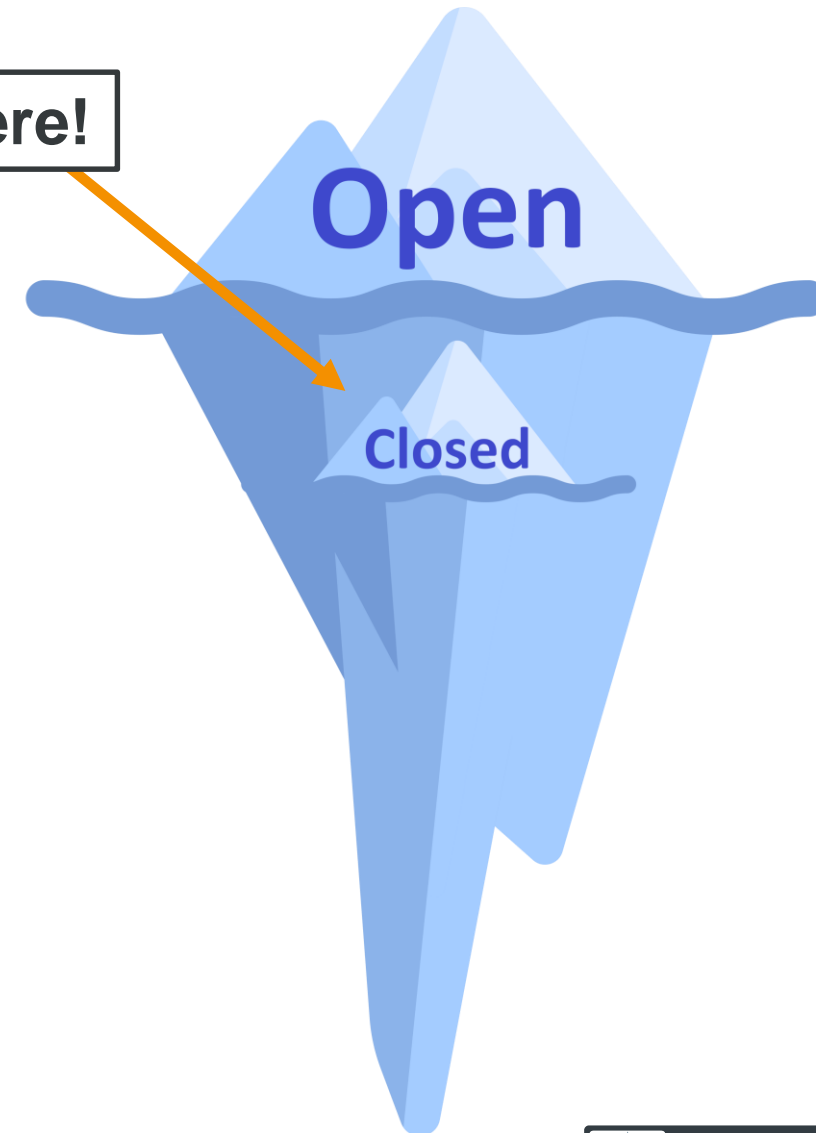


# The Bottom of the Iceberg – The (in)security of closed DNS Resolvers

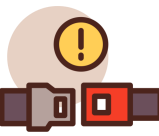


- **Initial Set:** 50k domains
- **Analyzed Set:** 7k domains
  - Open Resolvers: ~35%
  - Closed Resolvers: ~65%
- **Vulnerable Resolvers (Kaminsky):** 25
  - Open Resolvers: 2
  - Closed Resolvers: 23
- **Vulnerable Domains:** 1000+
- **Affected:** Websites and external Infrastructure
  - Corporate Infrastructure
  - Government Services
  - Political Campaigns
  - Small-Business Websites

We are here!



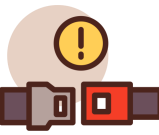
# The Bottom of the Iceberg – The (in)security of closed DNS Resolvers



**DEEPSEC**

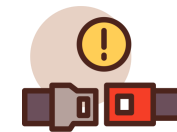


# The Bottom of the Iceberg – Now what?



**DEEP**SEC

# The Bottom of the Iceberg – Leveraging DNS



"admin"

Username or Email Address

Password

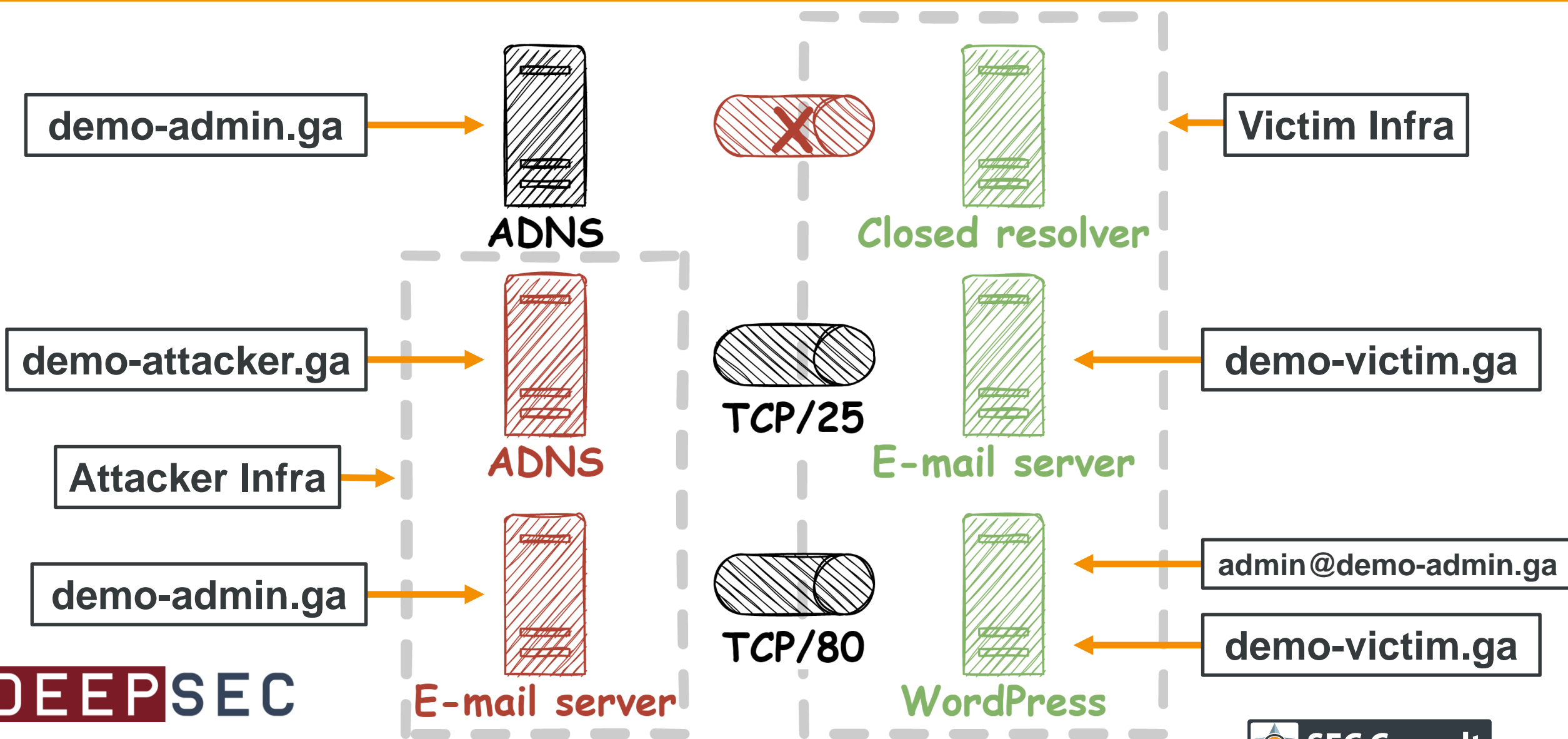
Remember Me

Lost your password?

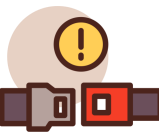
Fully patched?  
No problem!

Let's reset!

# Melting the DNS Iceberg! – Demo Infrastructure



**DEEP SEC**

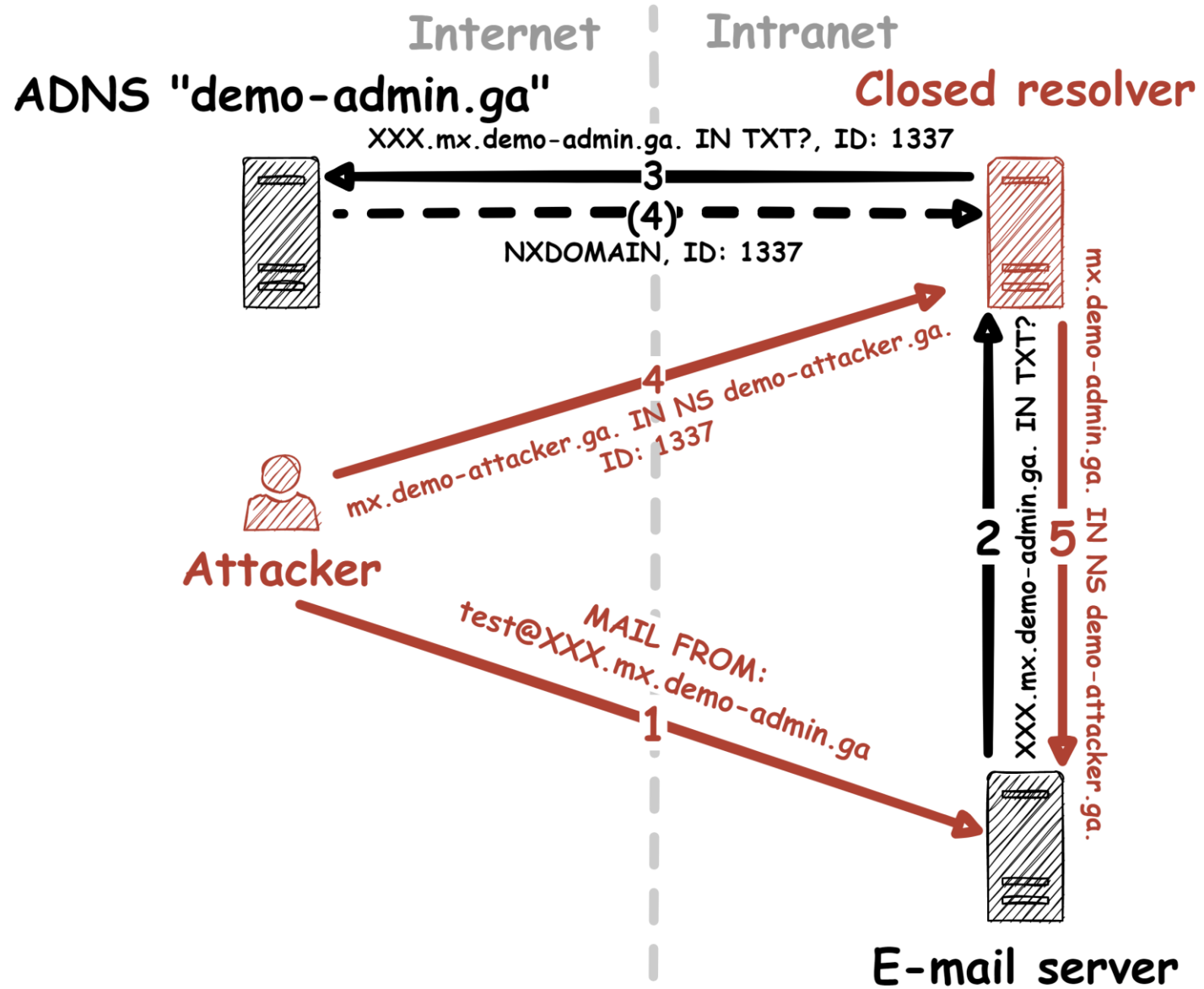
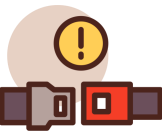


Nobody:  
Bugs right before a demo:



/build #

# Melting the DNS Iceberg! – Demo



```
root@ATTACKER:~/dns-closed-kaminsky-poc/attacker#
```

/build #






Username or Email Address

Password



Remember Me

Log In

 [Lost your password?](#)

[← Go to Demo WordPress](#)

```
root@ATTACKER:~/dns-closed-kaminsky-poc/attacker# |
```



http://demo-victim.ga/wp-login.php?action=rp&key=FigGzWIpuXhN8UcpLDw2&login=admin&wp\_lang=en\_US|

http://demo-victim.ga/wp-login.php?action=rp&key=FigGzWIpuXhN8UcpLDw2&login=admin&wp\_lang=en\_US — Visit

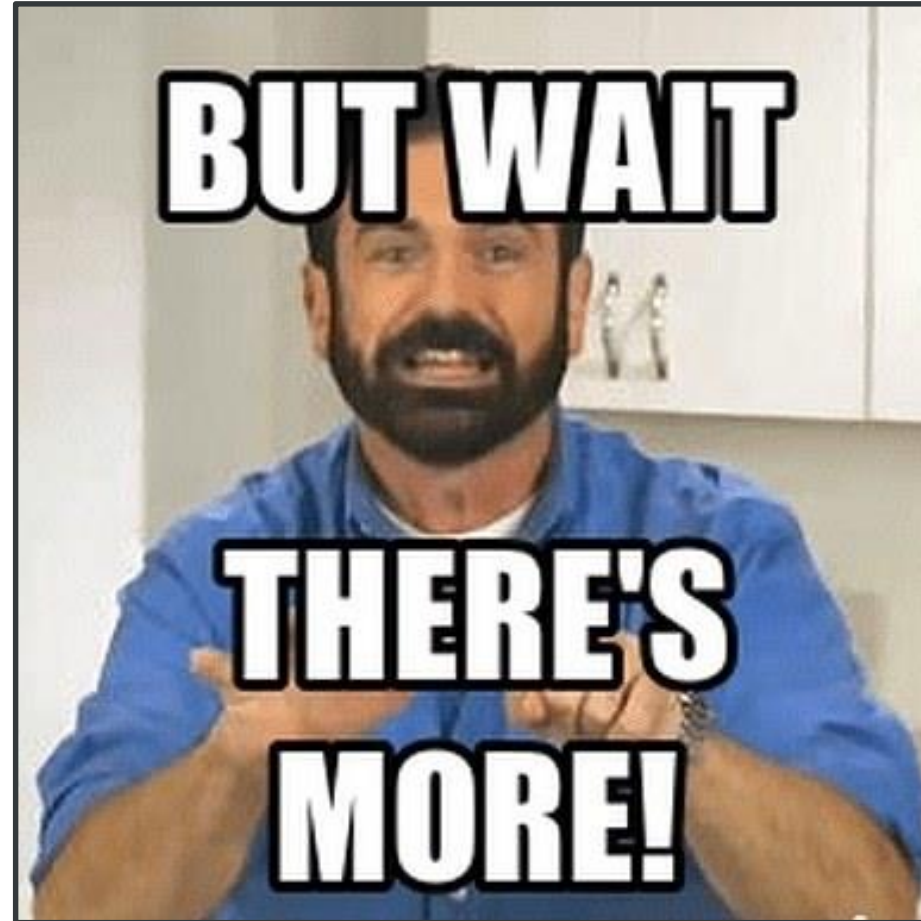
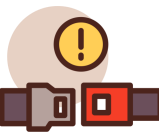
This time, search with:



Check your email for the confirmation link, then visit the [login page](#).

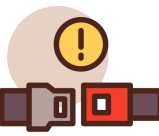
← [Go to Demo WordPress](#)

# The Bottom of the Iceberg – Leveraging DNS




**DEEP**SEC


# The Bottom of the Iceberg – Leveraging DNS



**Welcome to the  
Control Panel**

 Enter e-mail address

---

 Enter password

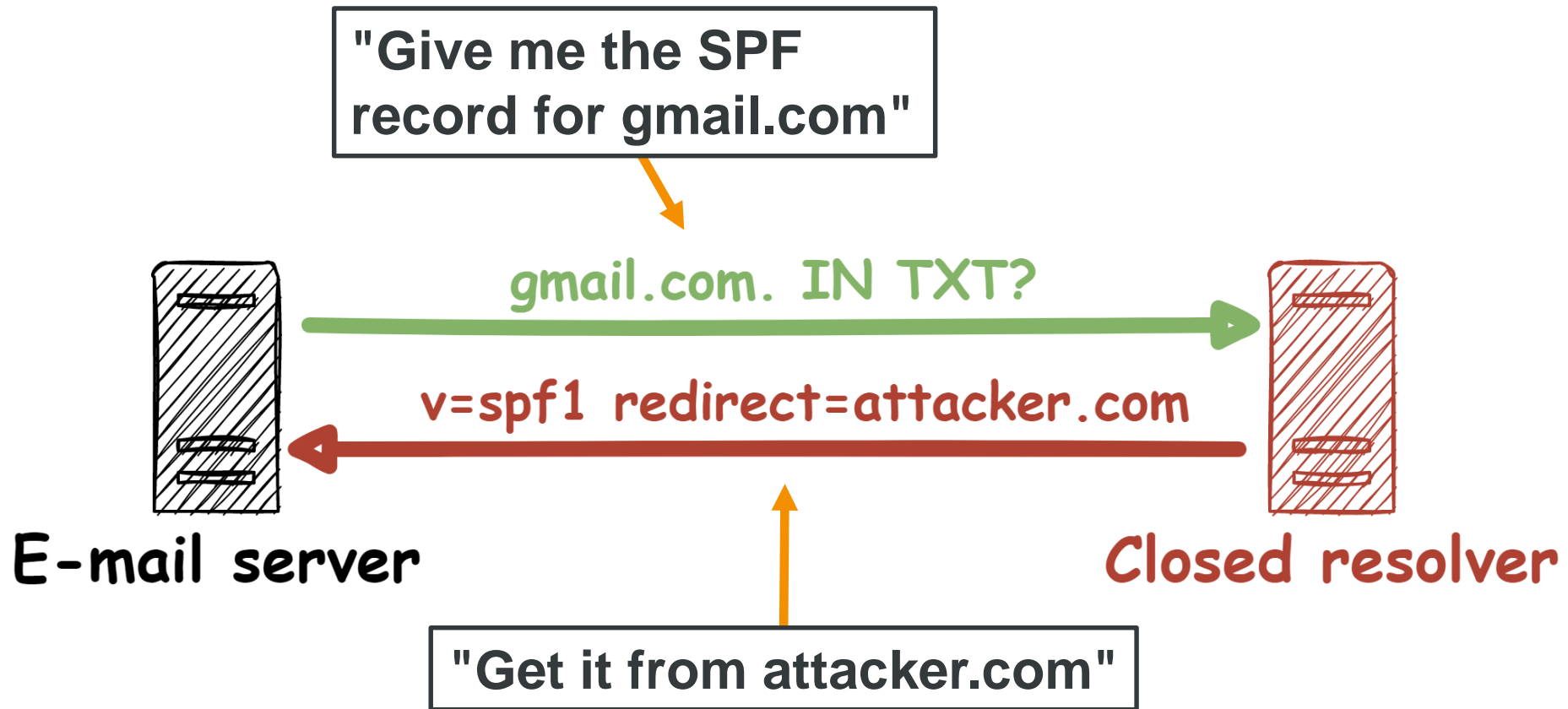
---

**LOGIN**

[Forgot your password?](#)

Let's reset them all!

# The Bottom of the Iceberg – Leveraging DNS



- **DNS vulnerabilities are still a thing**
  - Outdated/Misconfigured DNS Software
  - DNS 0-days
- **Heavily overlooked**
  - Unknown Attack Vectors
  - Unknown Impact
  - Little Coverage
- **Not the next "big thing"**



- Blue Team, Red Team, Research, ...
- Many more DNS Icebergs!
- Many more Bug Bounties!







 **PortSwigger Research**  
@PortSwiggerRes

Excellent research on password-reset hijacking via Kaminsky attacks on closed DNS resolvers, by [@sec\\_consult](#)

 [sec-consult.com](https://sec-consult.com)  
**Melting the DNS Iceberg: Taking over your infrastructure Ka...**  
Hidden DNS resolvers and how to compromise your infrastructure

2:54 PM · Oct 6, 2022 · TweetDeck

**106** Retweets   **3** Quote Tweets   **287** Likes