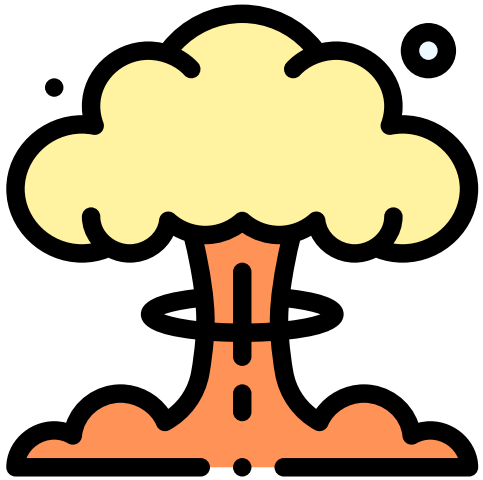
DEEPSEC

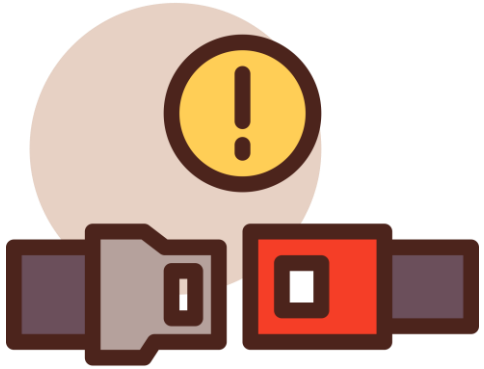
Melting the DNS Iceberg

Taking over your infrastructure Kaminsky style

SEC Consult
an atos company

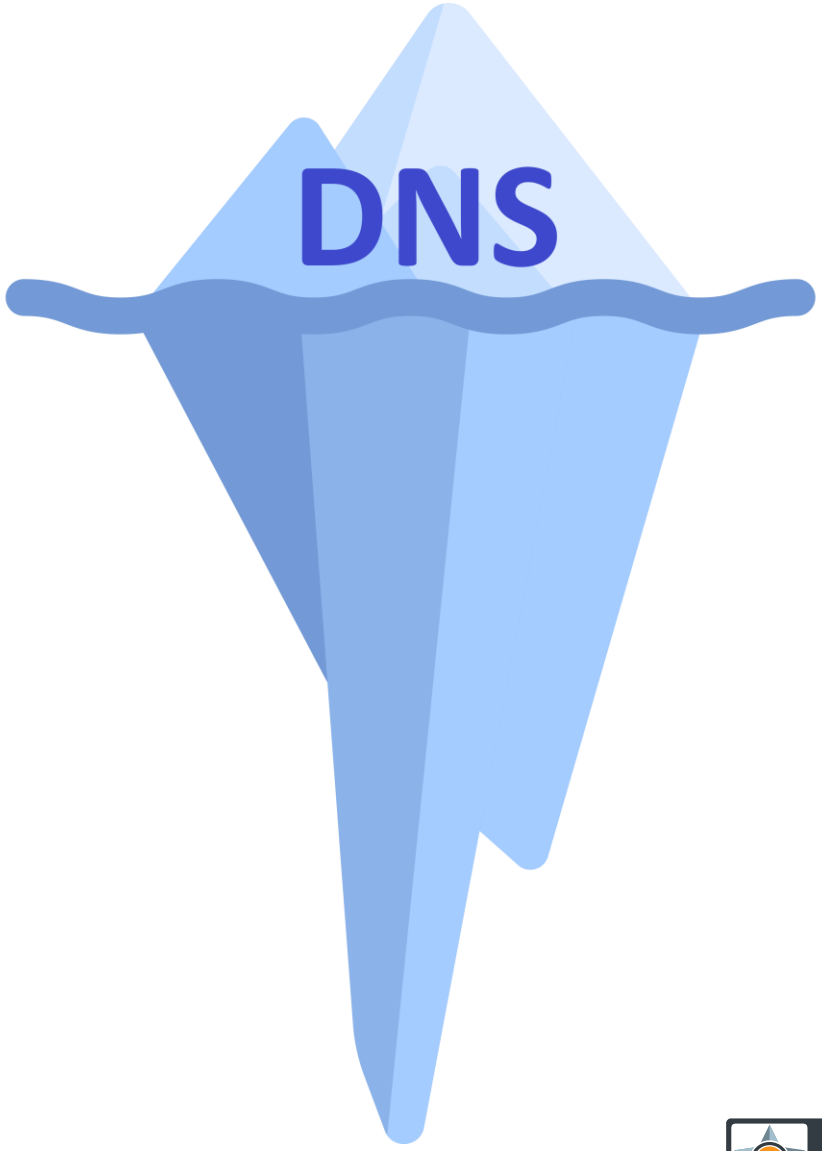
Intro





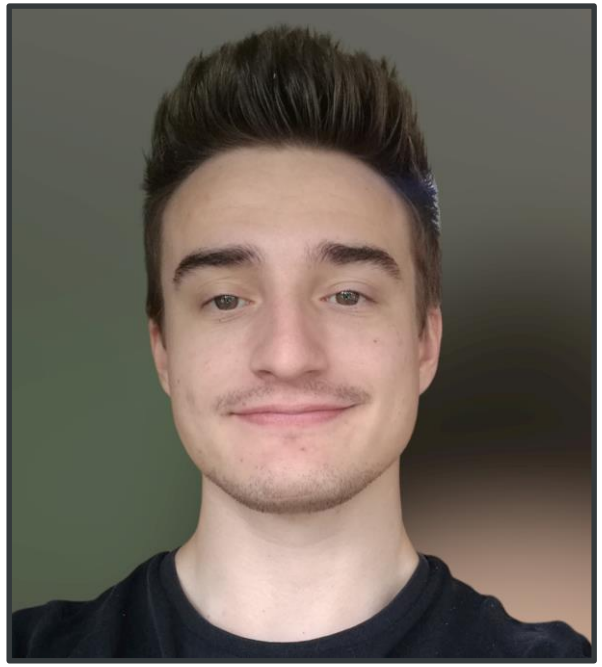
Outline

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



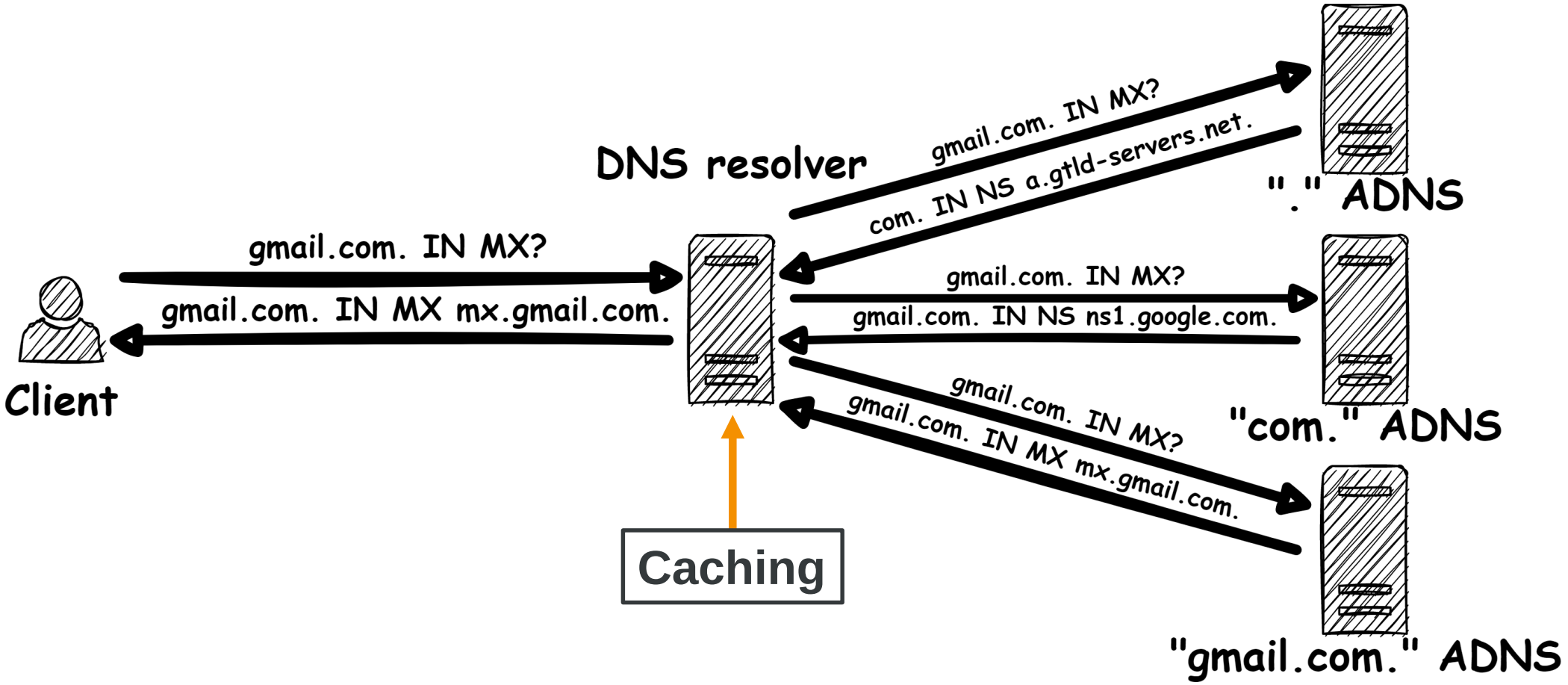
$whoami

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



Timo Longin

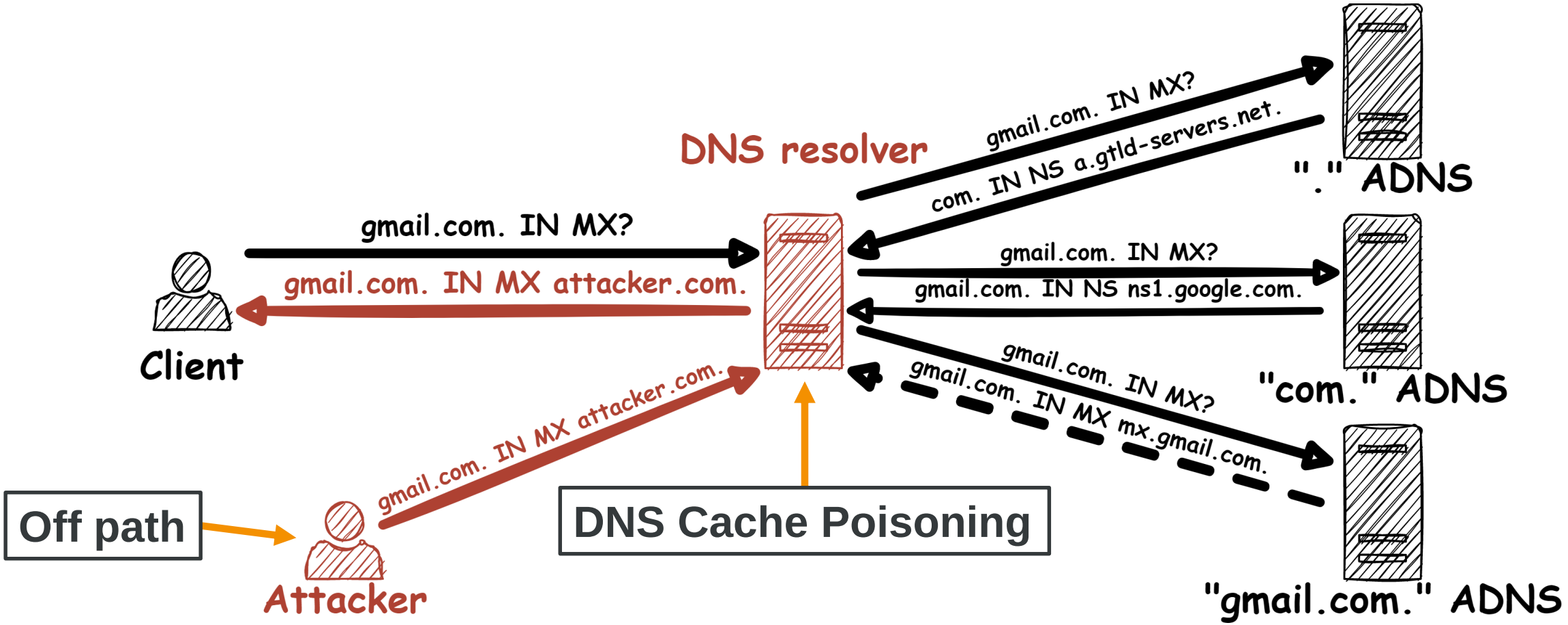
DNS (Security) Recap



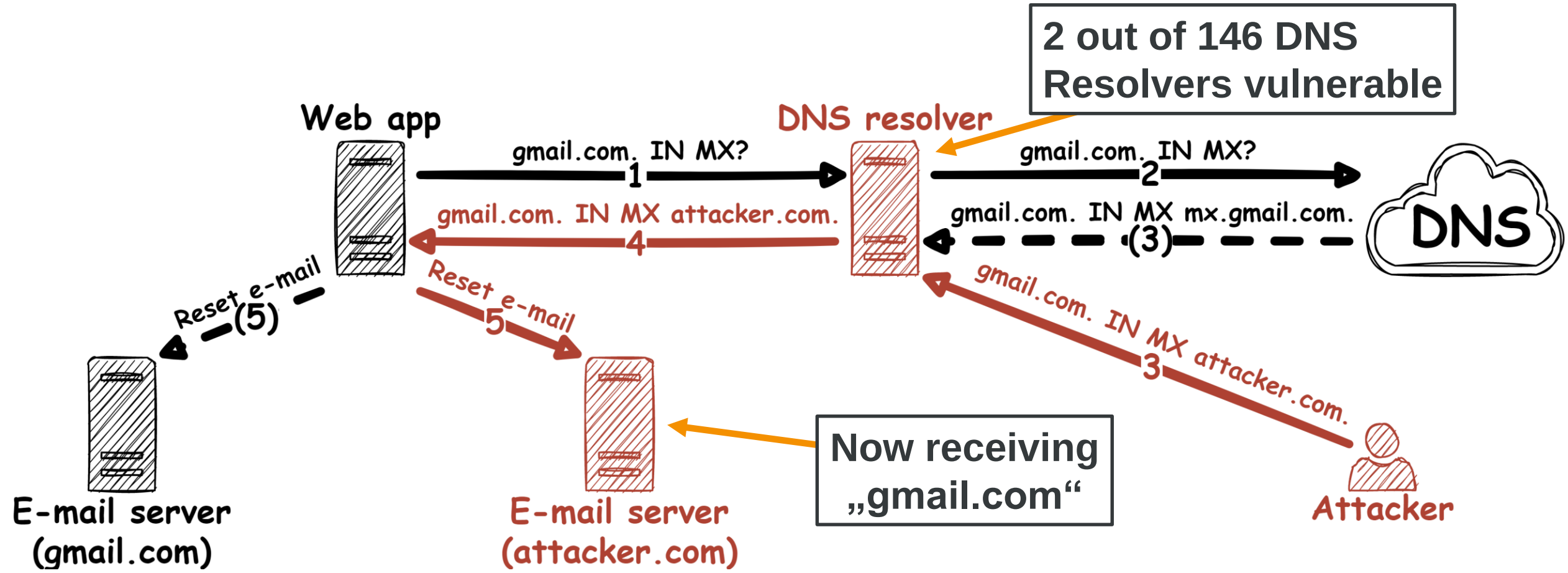
Recursive ⟷ **DNS over UDP|TLS|HTTPS**

Iterative ⟷ **DNS over UDP (+DNSSEC)**

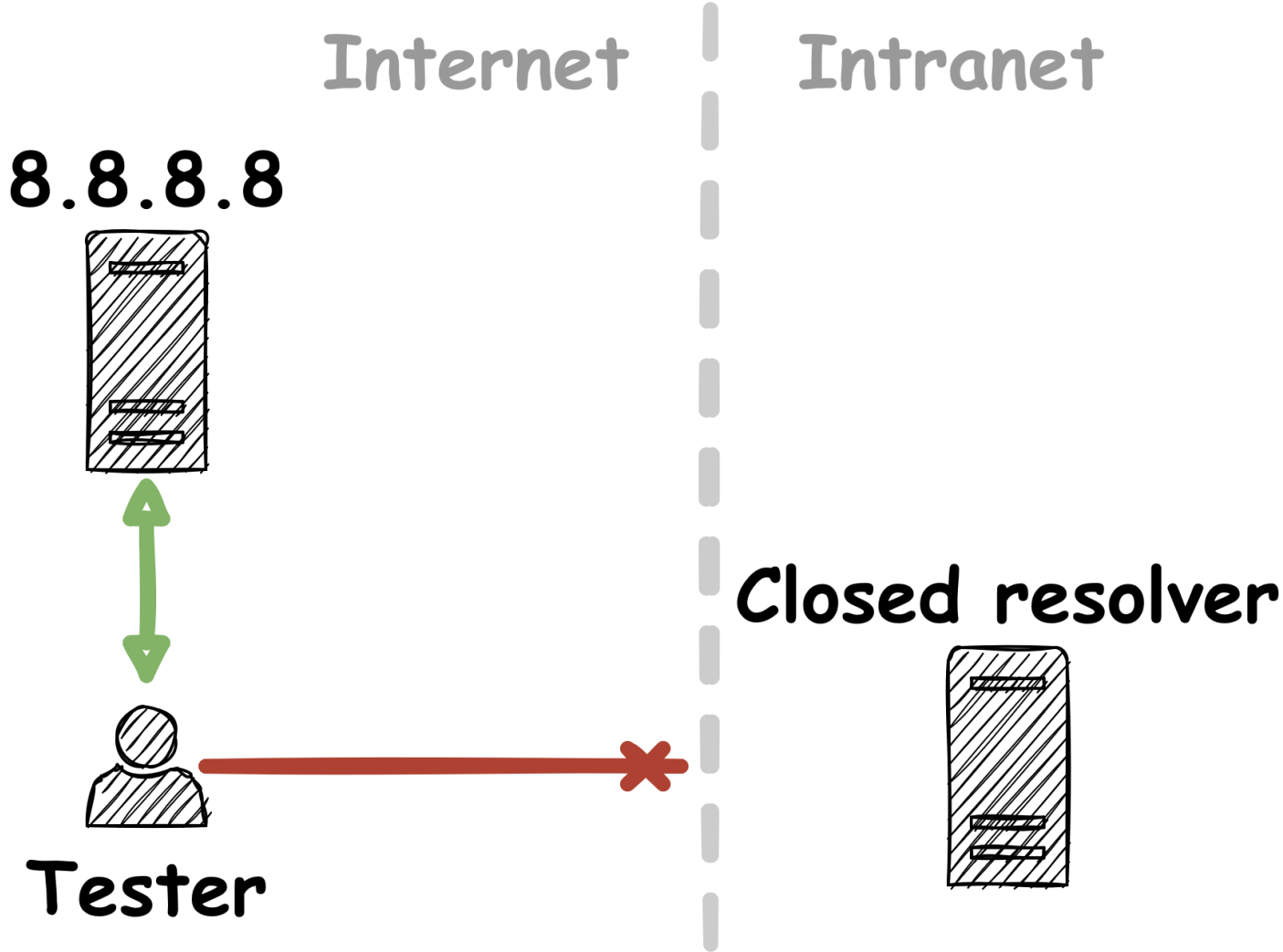
DNS (Security) Recap



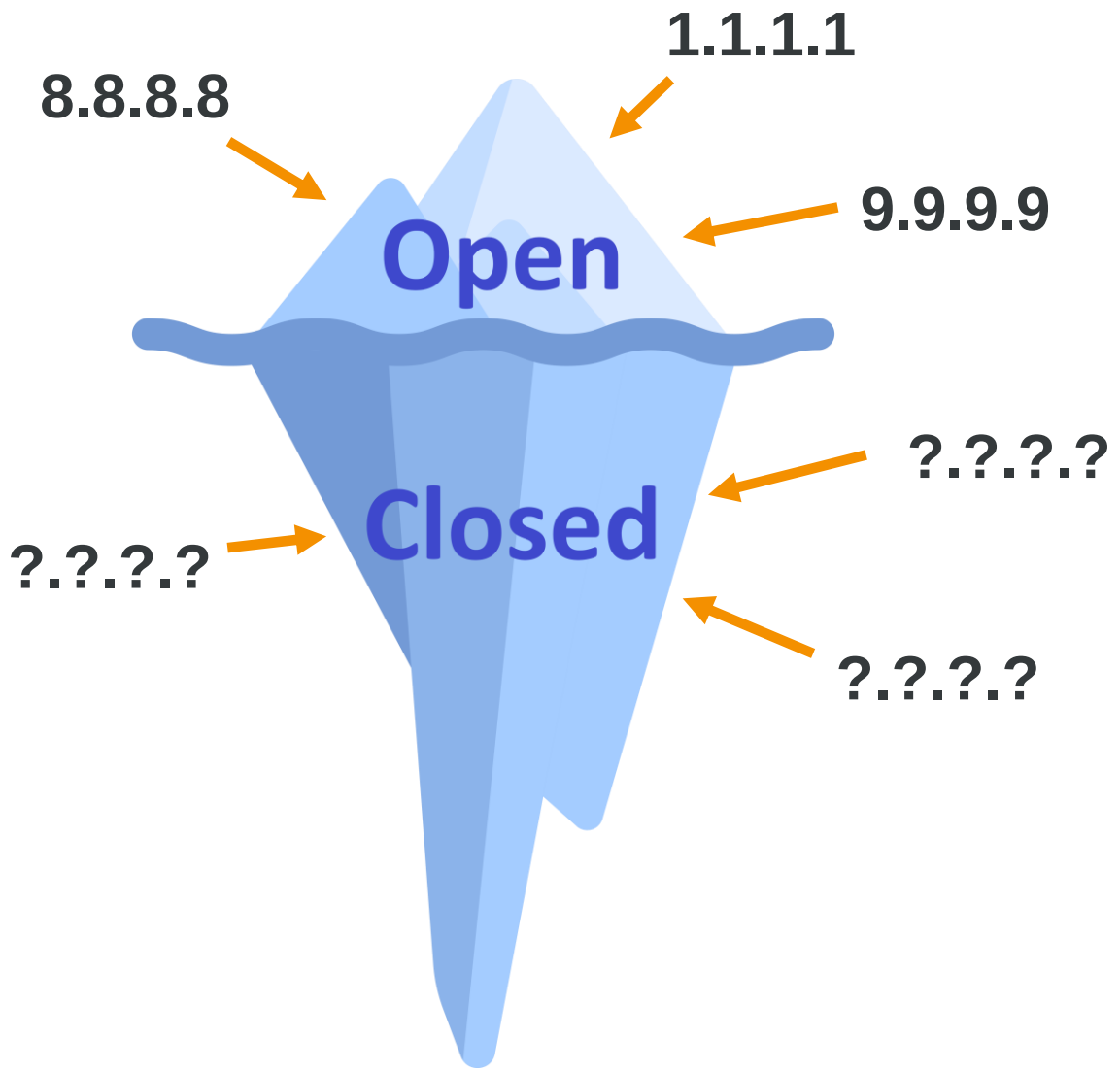
The DNS Iceberg? – Analyzing the WHAT?



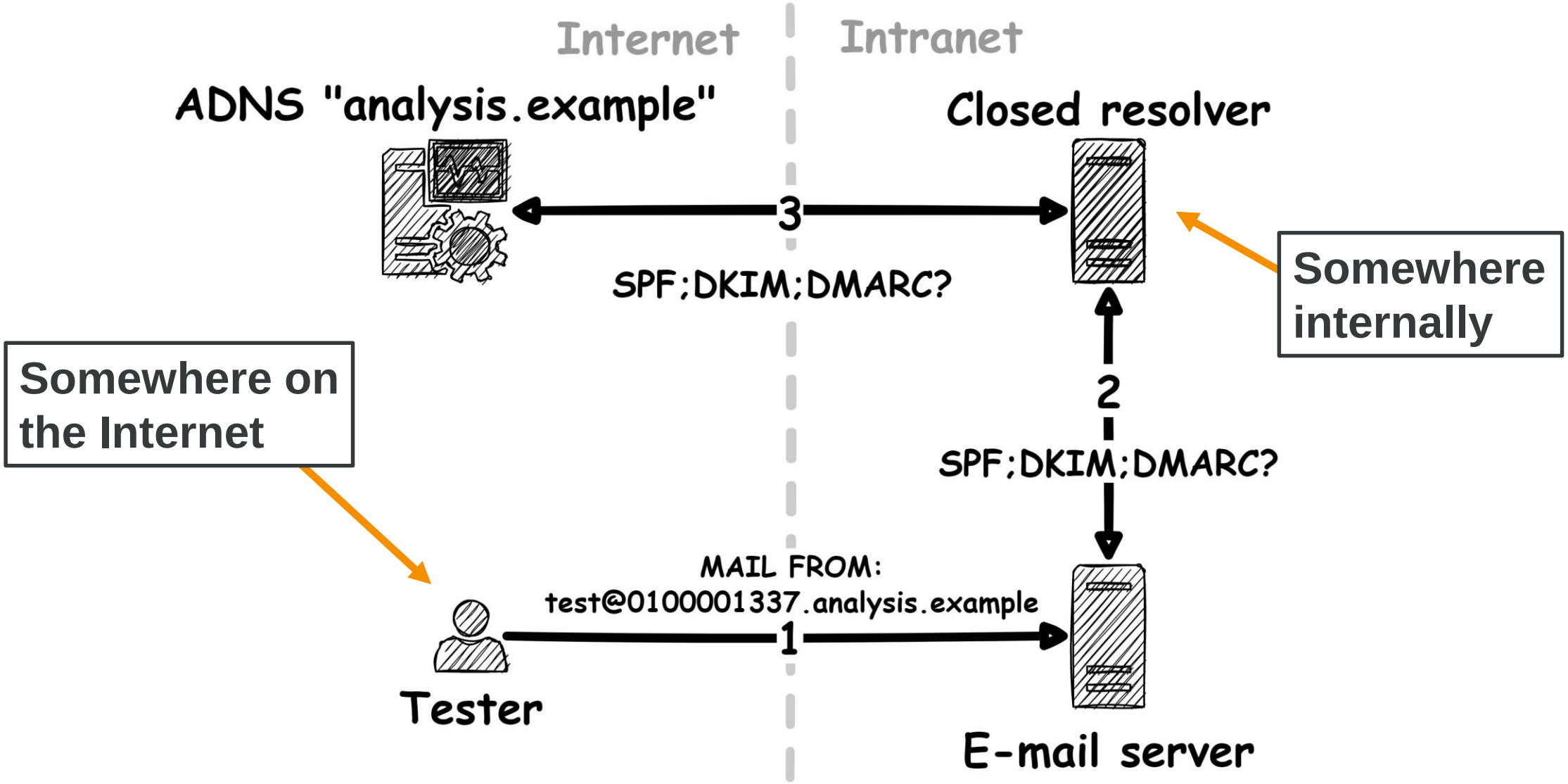
The DNS Iceberg? – Open and Closed Resolvers



The DNS Iceberg? – The DNS Iceberg



Melting the DNS Iceberg! – Reaching Closed Resolvers



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

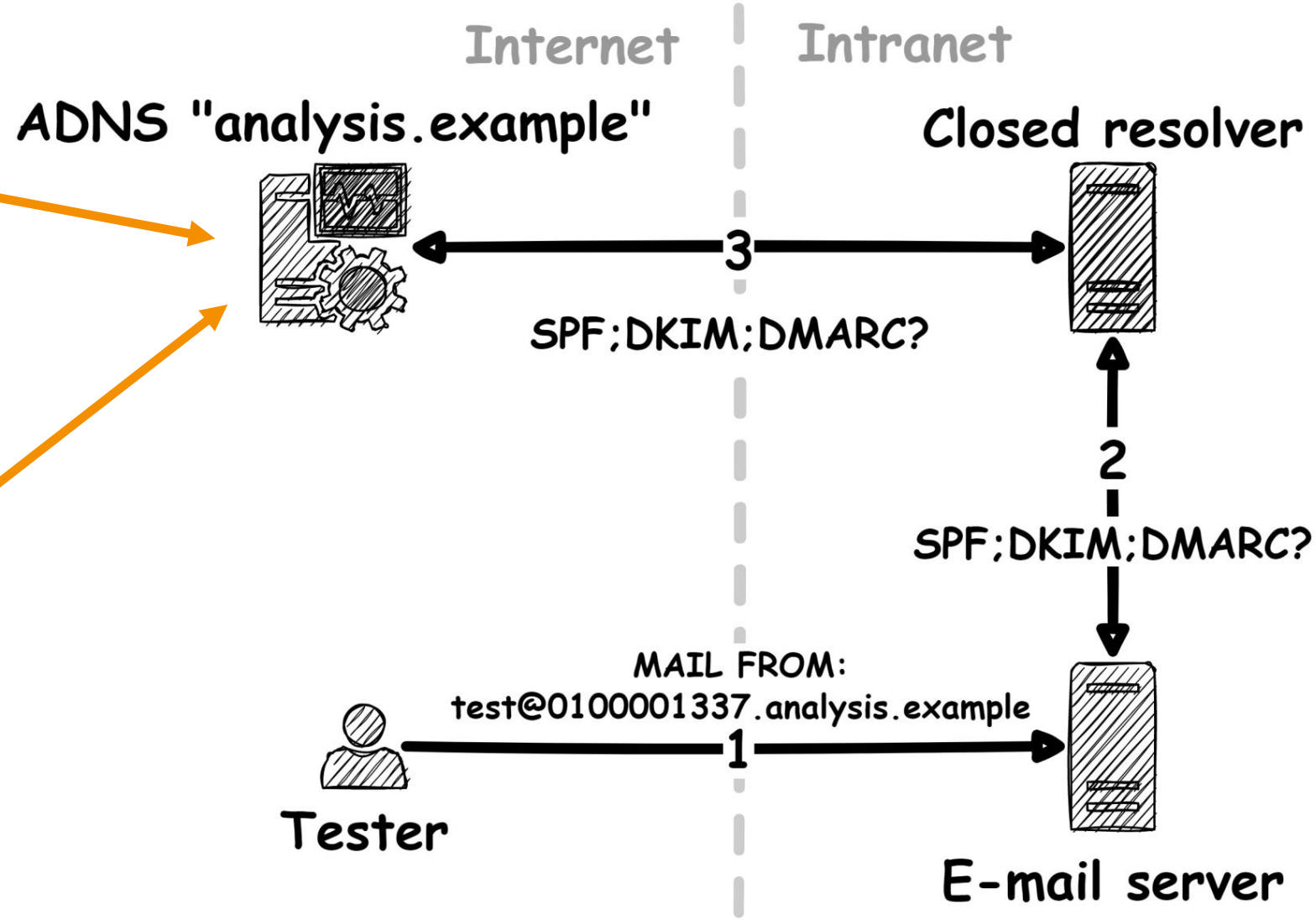
Melting the DNS Iceberg! – DNS Analysis Server

Active Checks:

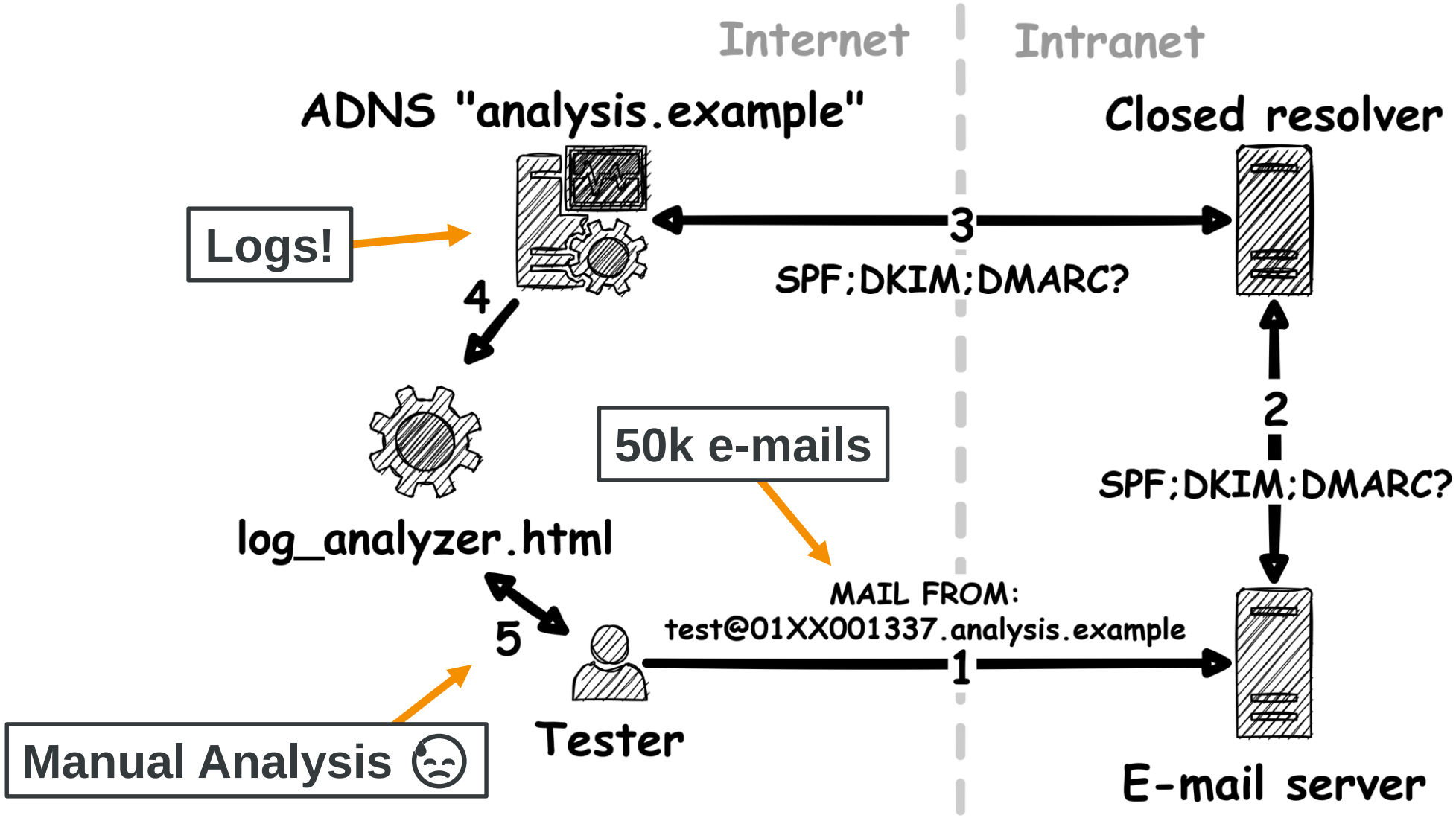
- IP Fragmentation
- Query Loops
- EDNS Usage
- …

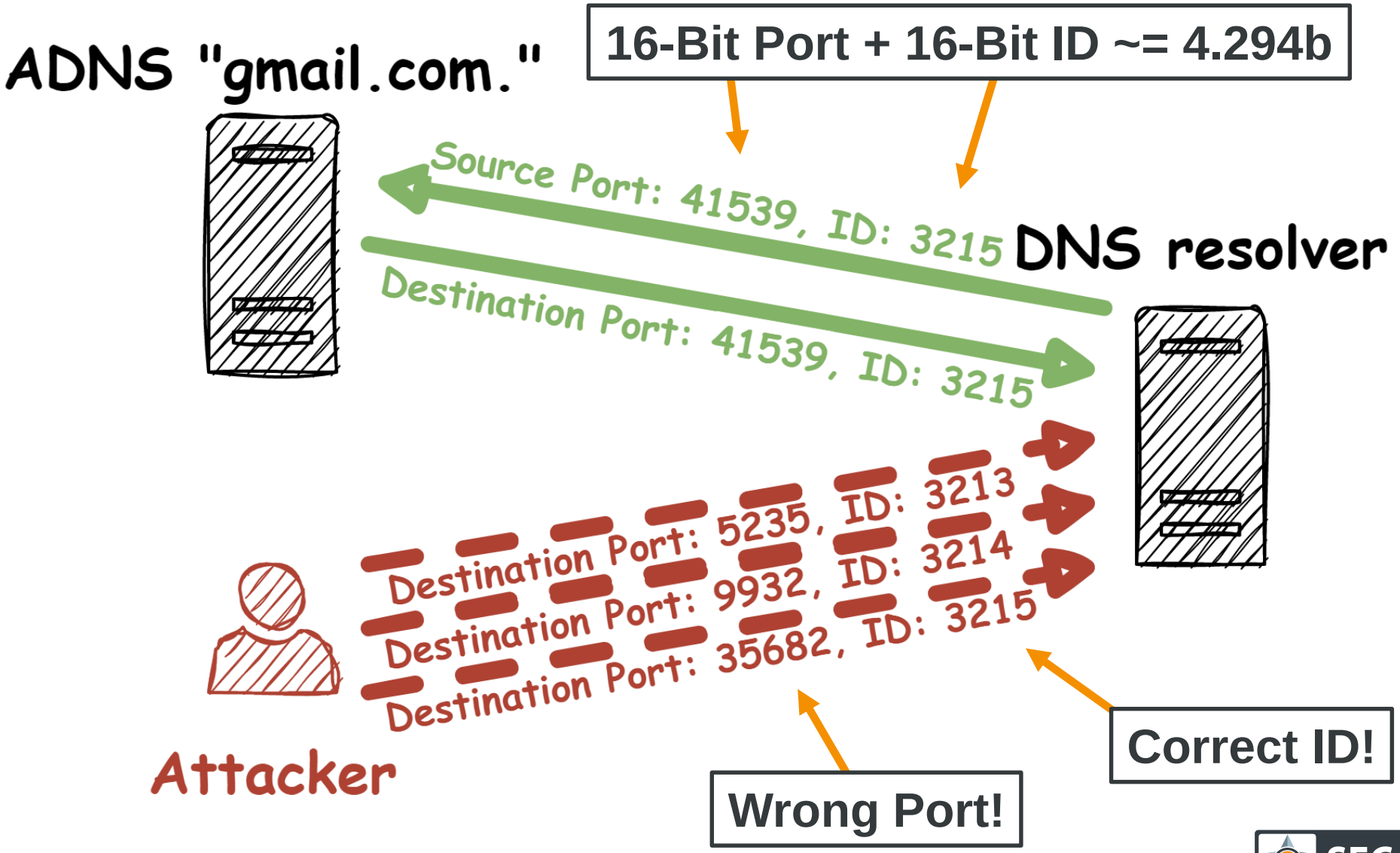
Passive Checks:

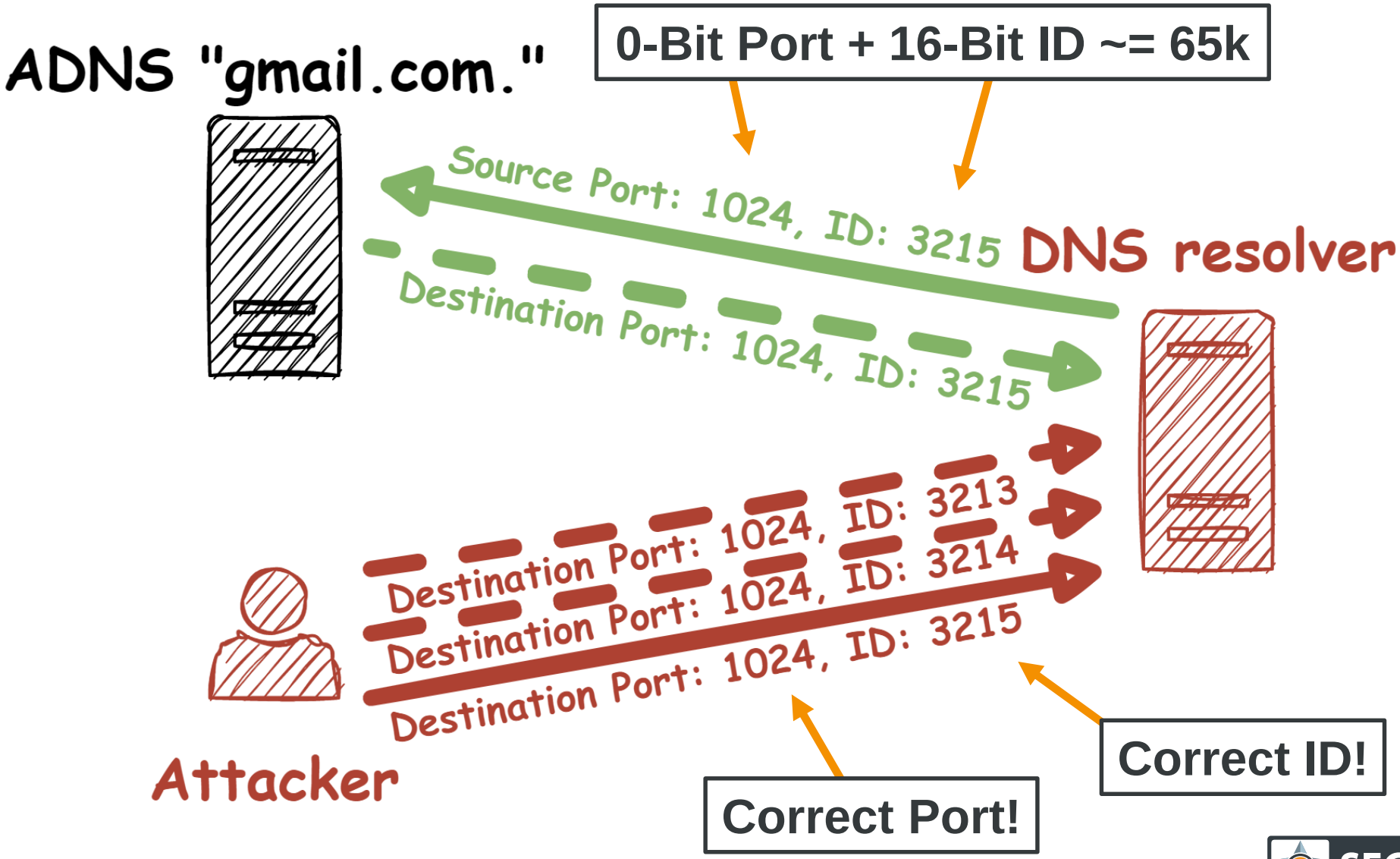
- UDP Source Ports
- DNSSEC
- DNS Cookies
- EDNS Max Size
- 0x20 Encoding
- Used IP Addresses
- …



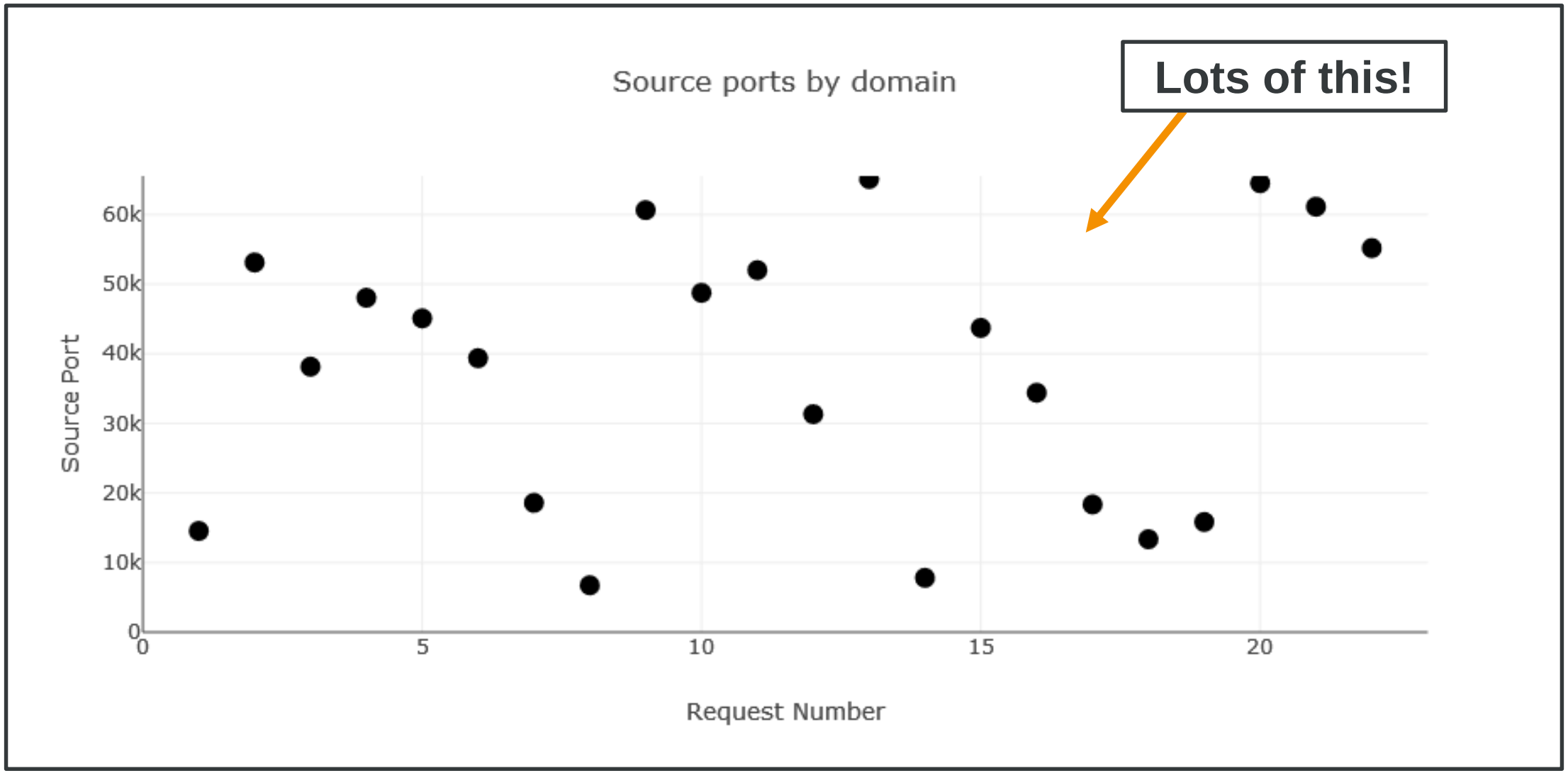
Melting the DNS Iceberg! – Testing Procedure

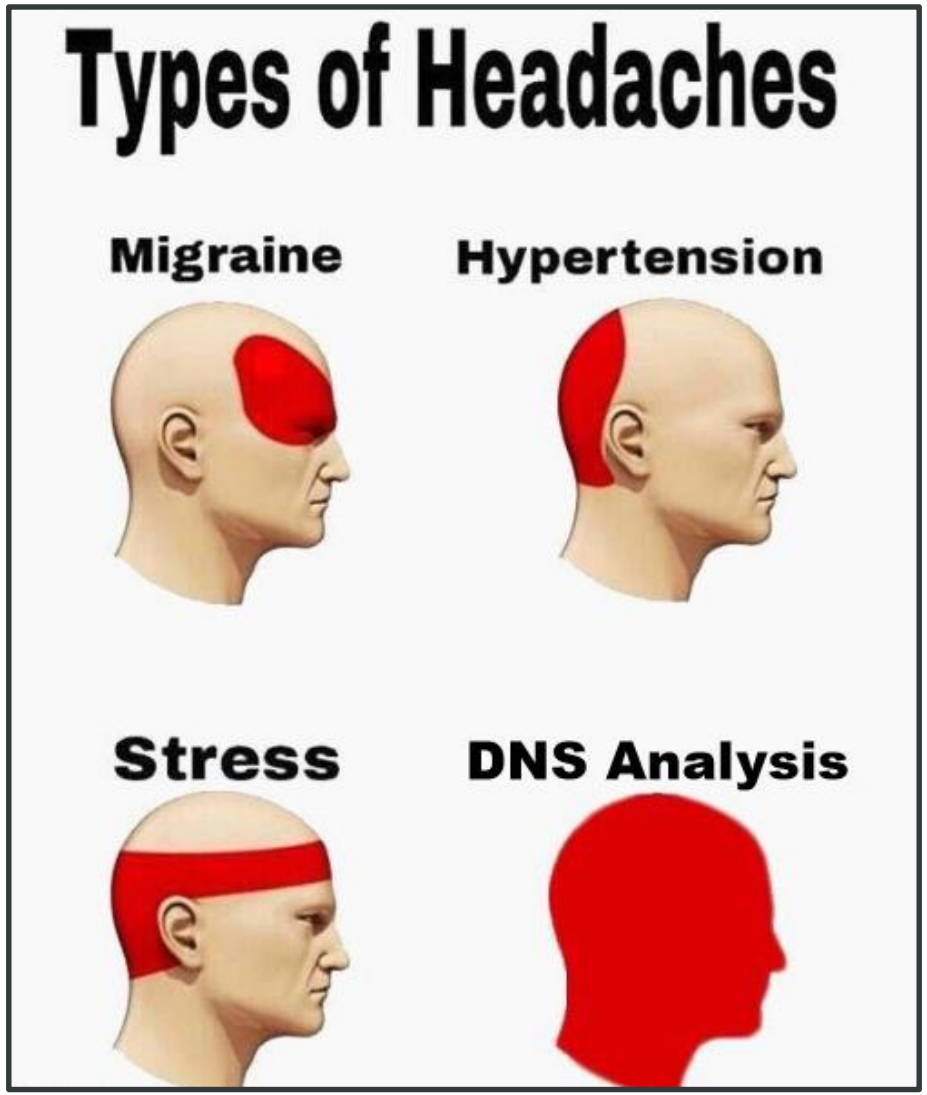




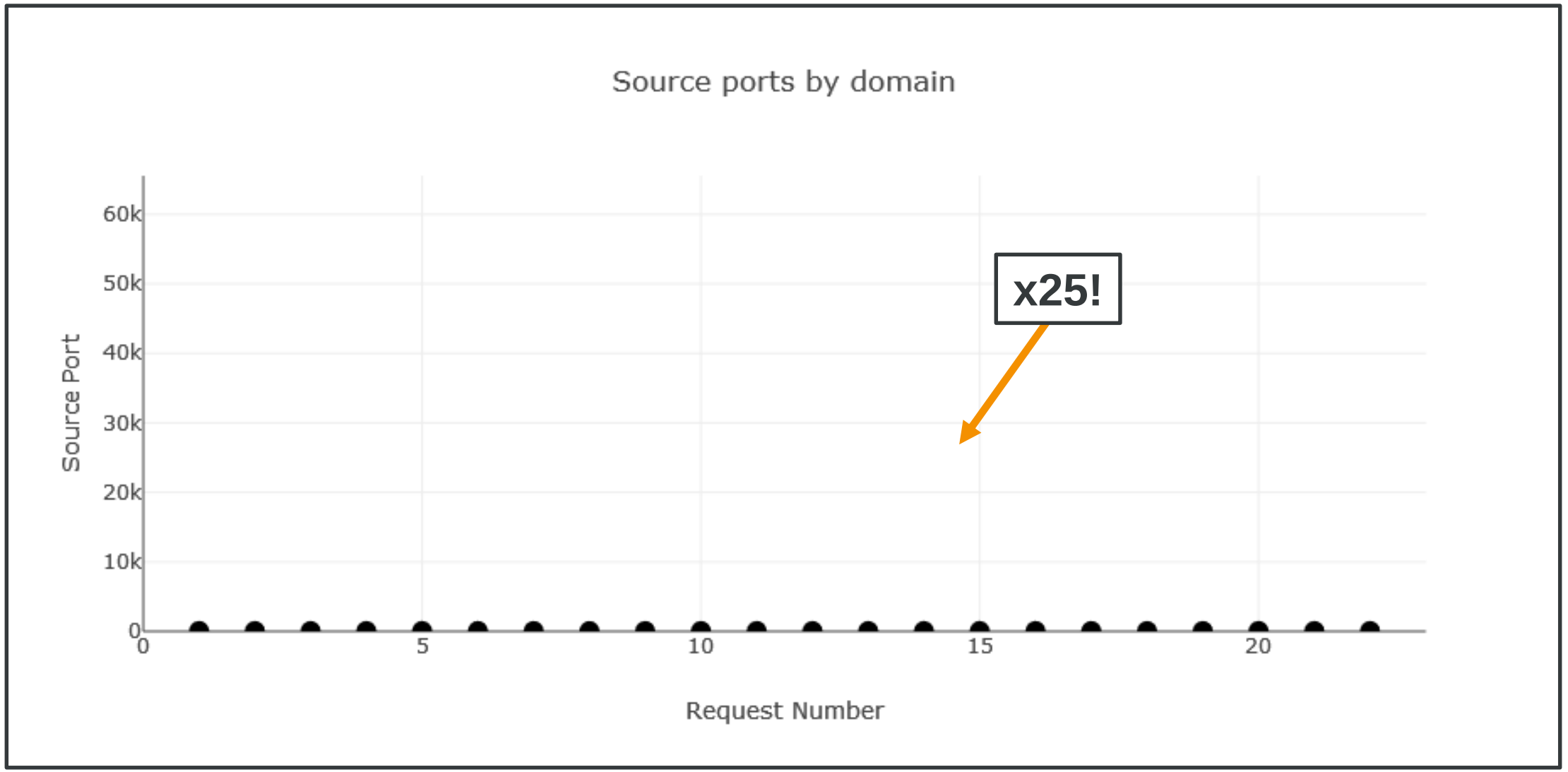


Melting the DNS Iceberg! – log_analyzer.html

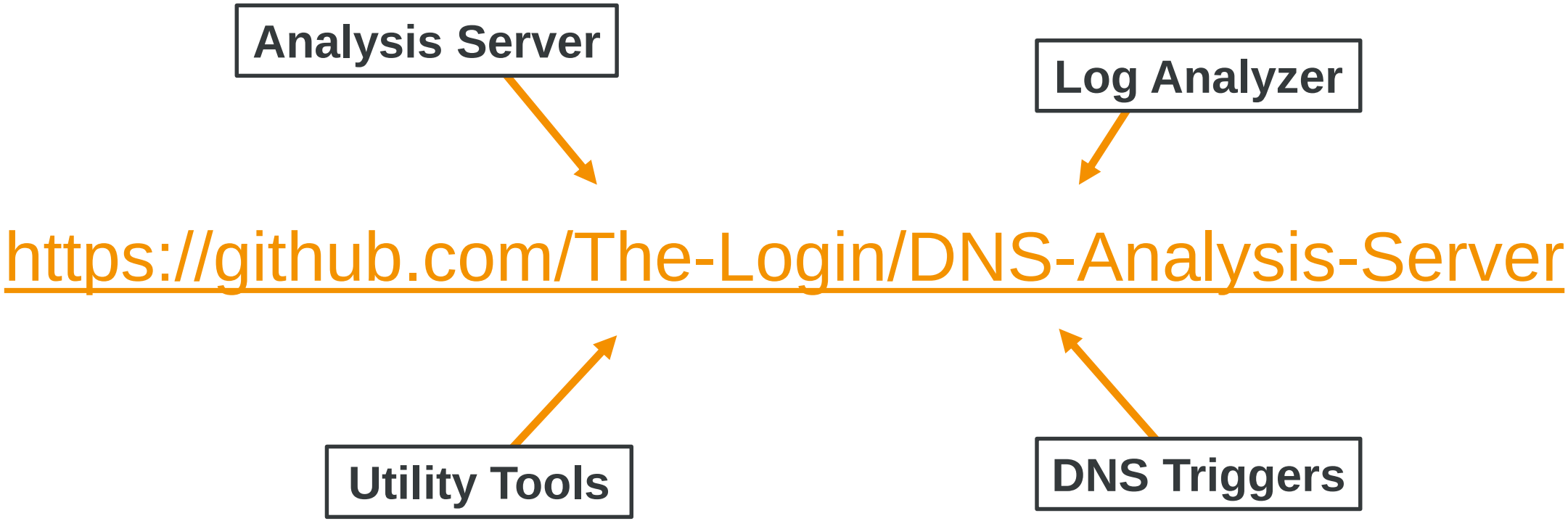




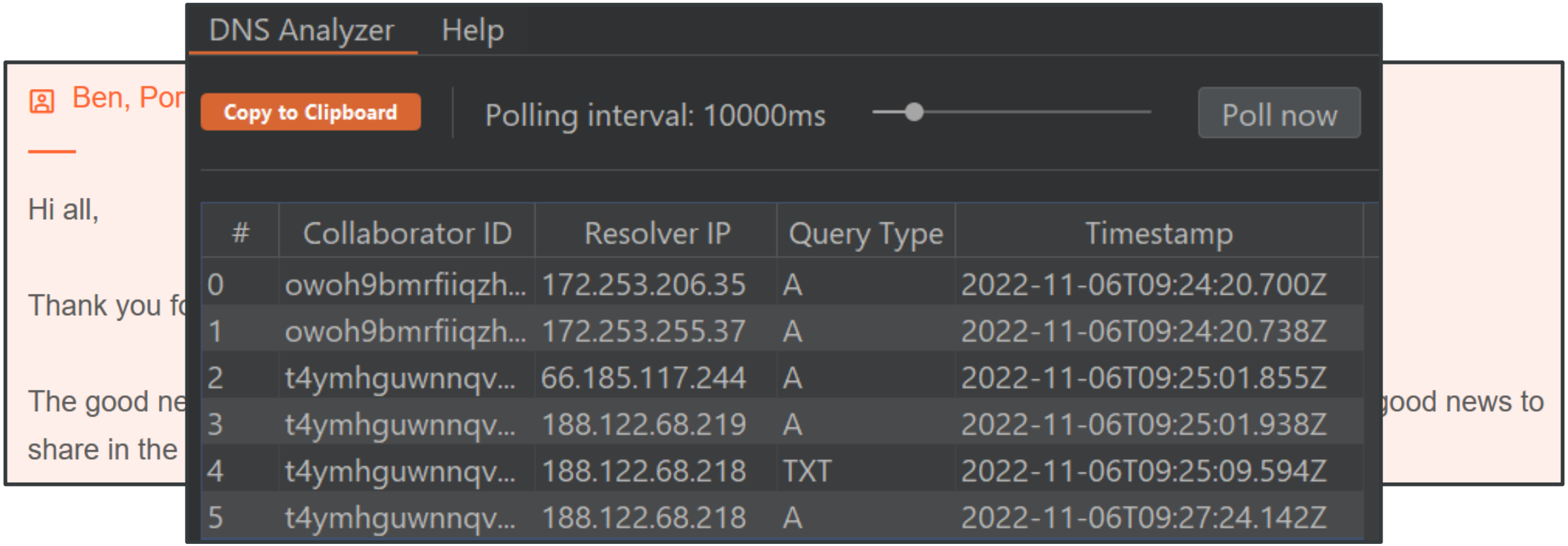
Melting the DNS Iceberg! – log_analyzer.html



Melting the DNS Iceberg! – Tooling!

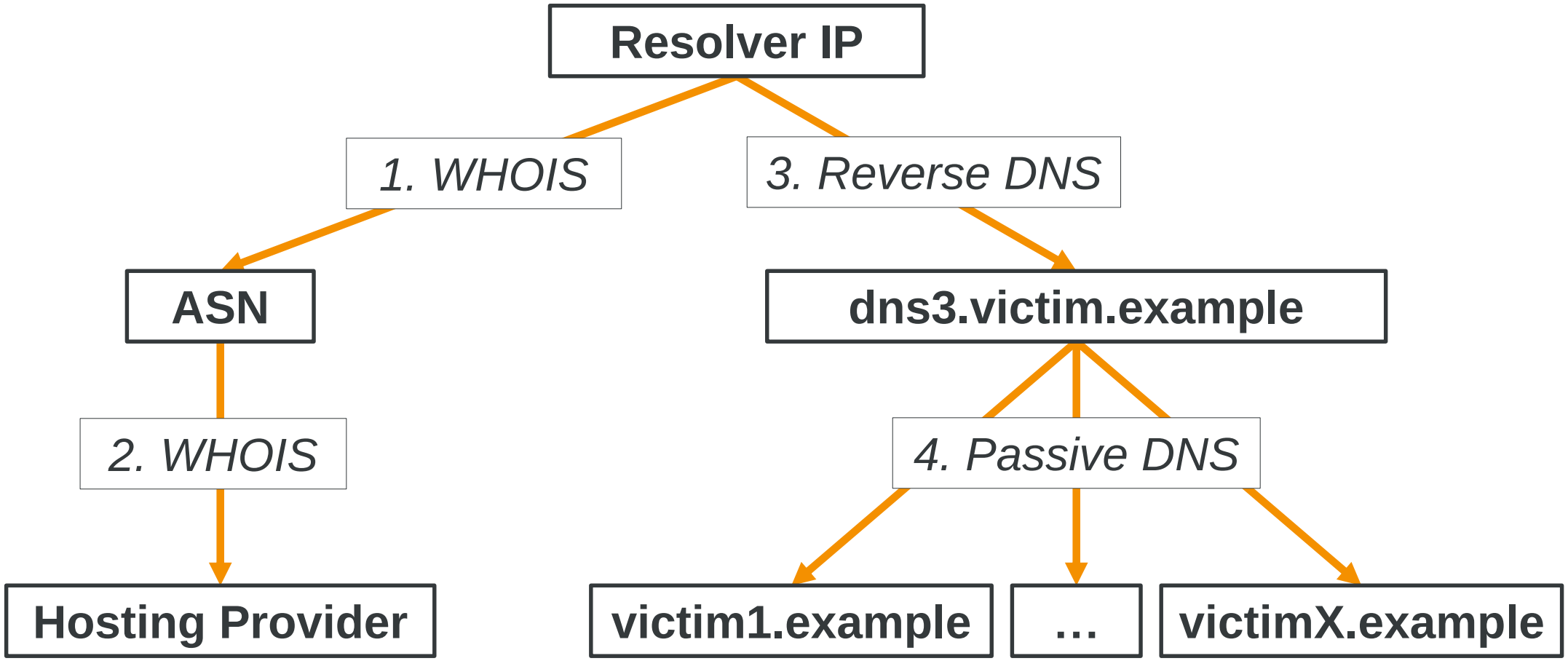


Melting the DNS Iceberg! – Burp Suite?!



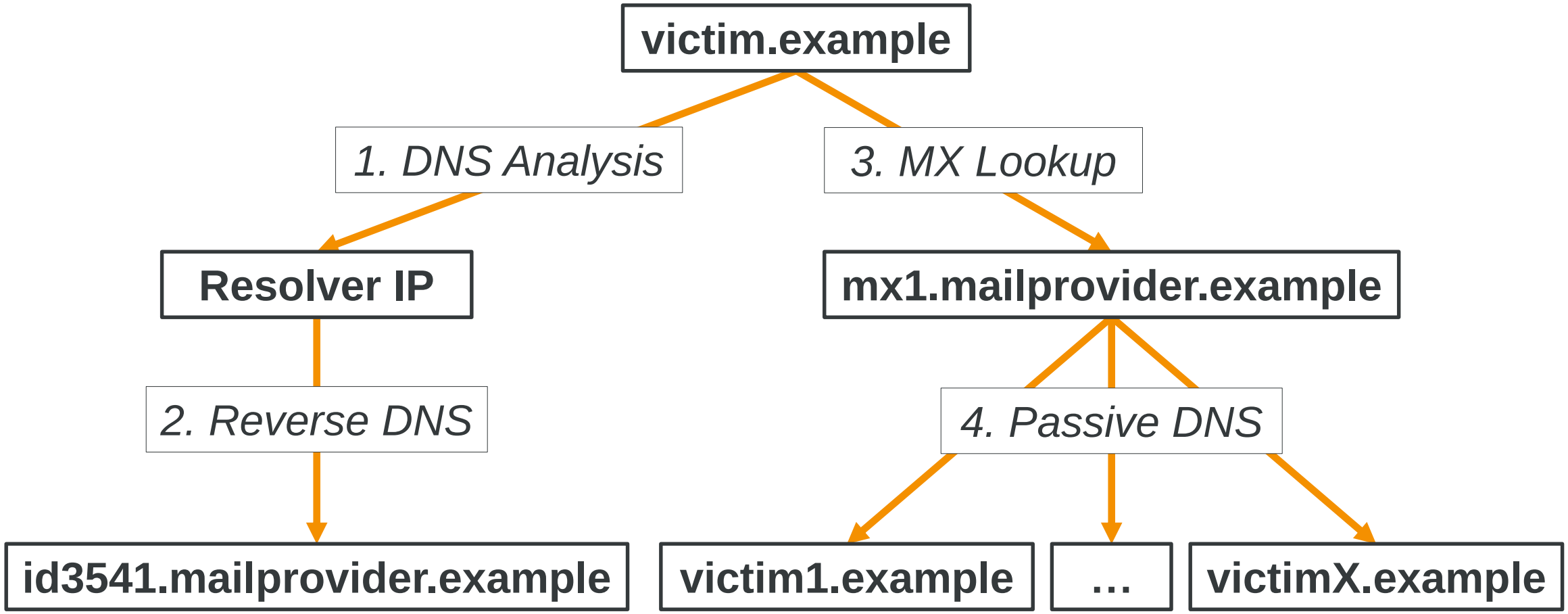
#	Collaborator ID	Resolver IP	Query Type	Timestamp
0	owoh9bmrfiiqzh...	172.253.206.35	A	2022-11-06T09:24:20.700Z
1	owoh9bmrfiiqzh...	172.253.255.37	A	2022-11-06T09:24:20.738Z
2	t4ymhguwnnqv...	66.185.117.244	A	2022-11-06T09:25:01.855Z
3	t4ymhguwnnqv...	188.122.68.219	A	2022-11-06T09:25:01.938Z
4	t4ymhguwnnqv...	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



DEEPSEC

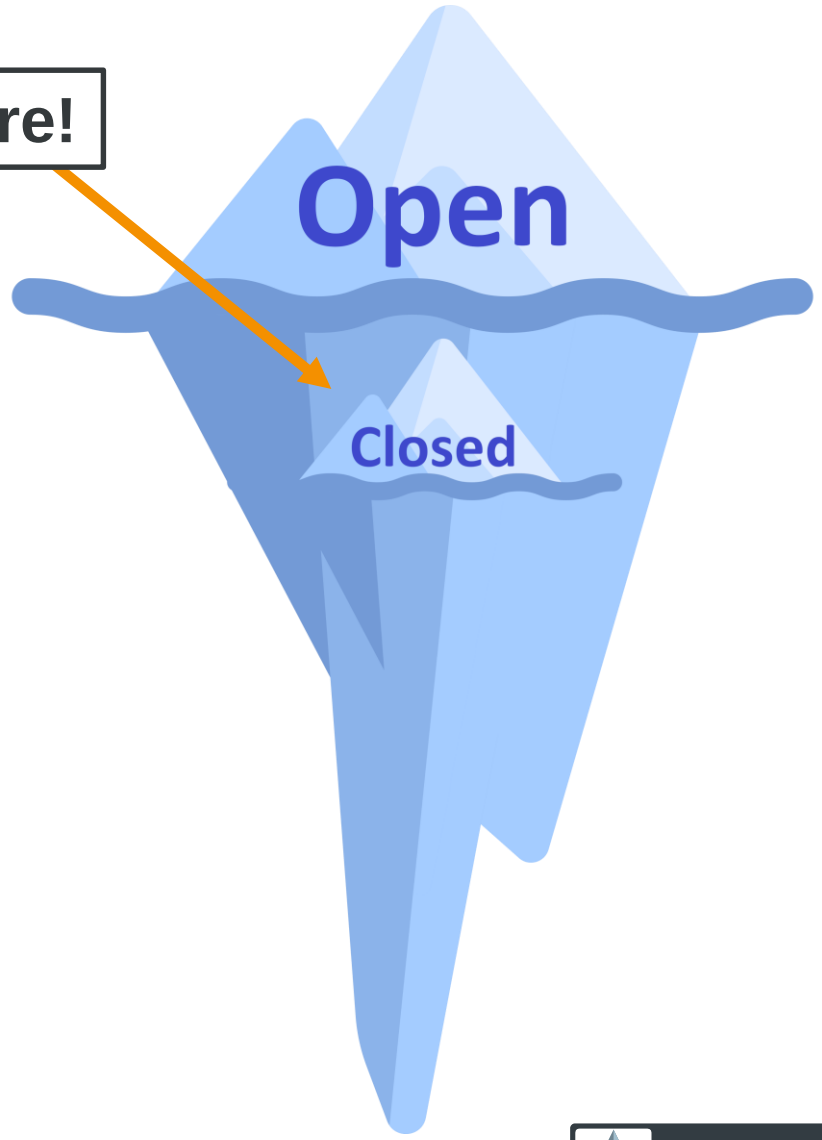
Melting the DNS Iceberg! – Going down the Rabbit Hole #2



DEEPSEC

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



DEEPSEC

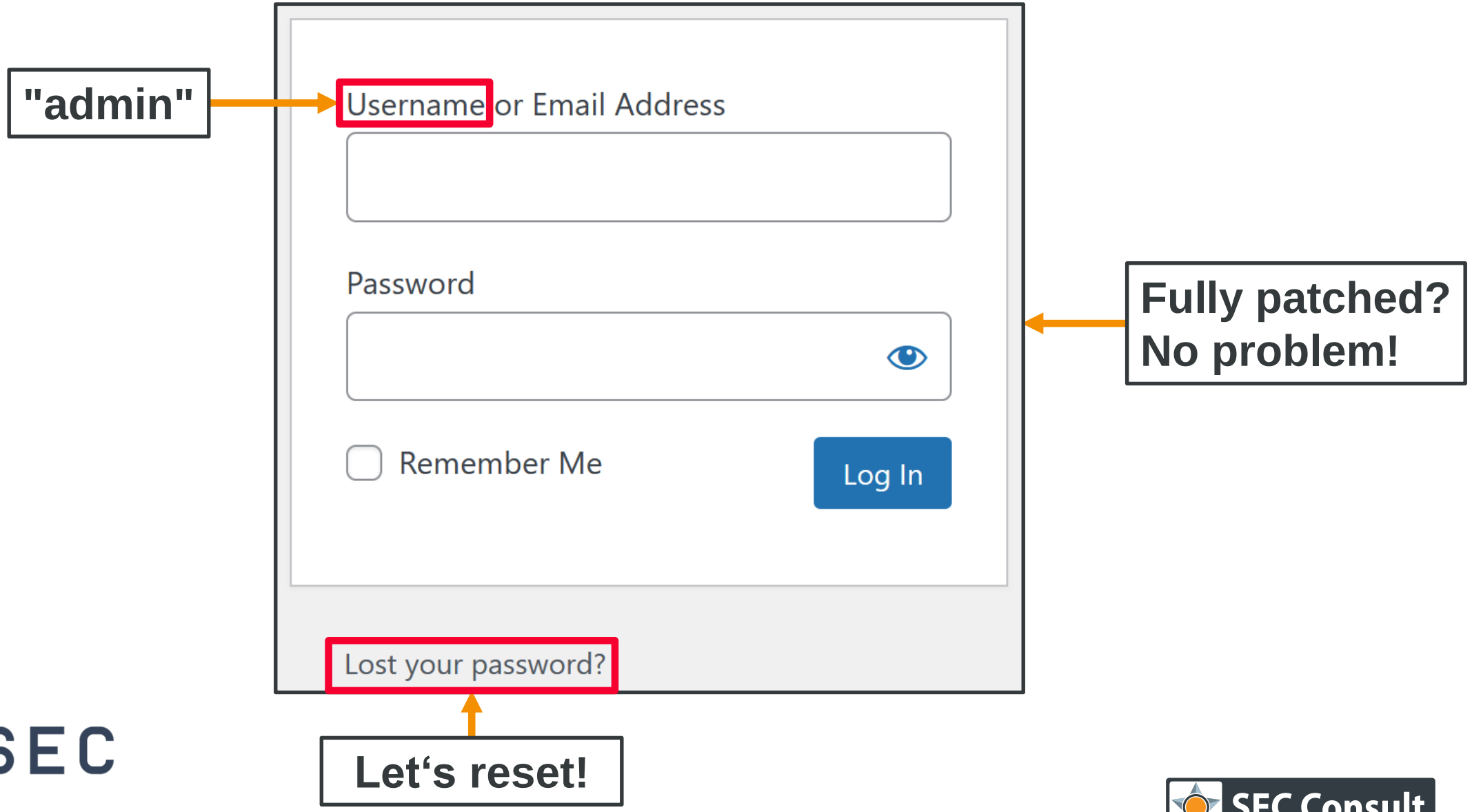
The Bottom of the Iceberg – The (in)security of closed DNS Resolvers

DEEPSEC

The Bottom of the Iceberg – Now what?

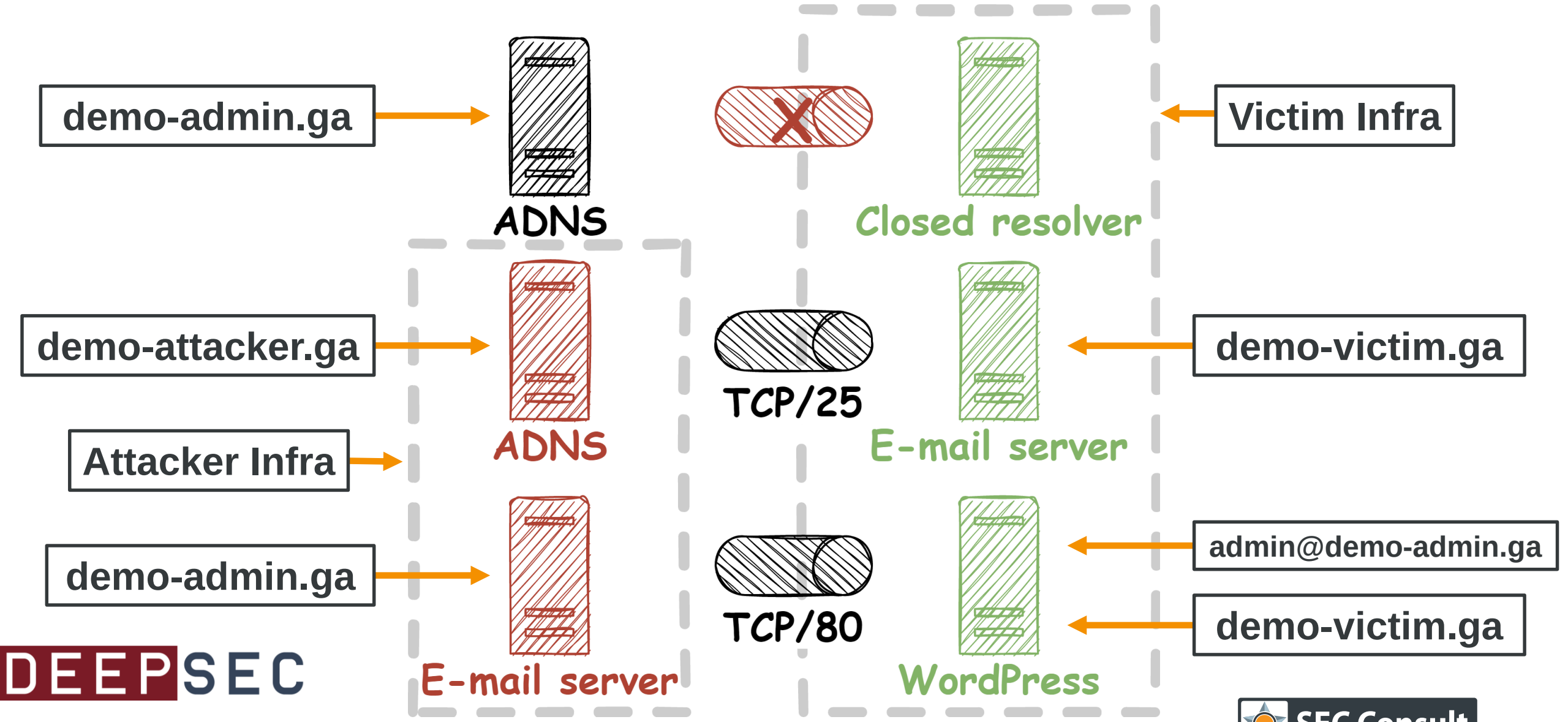
DEEPSEC

The Bottom of the Iceberg – Leveraging DNS



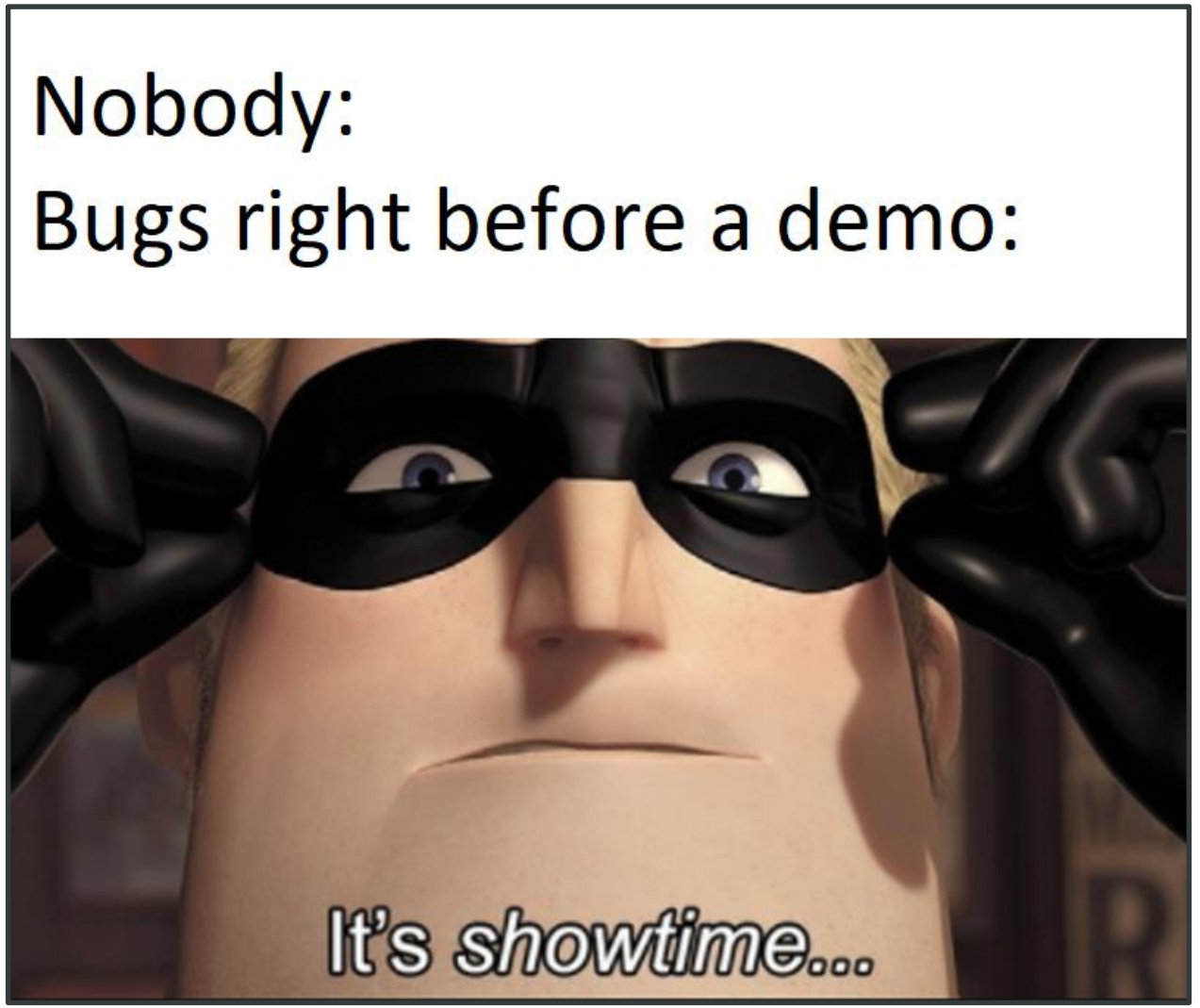
DEEPSEC

Melting the DNS Iceberg! – Demo Infrastructure



DEEPSEC

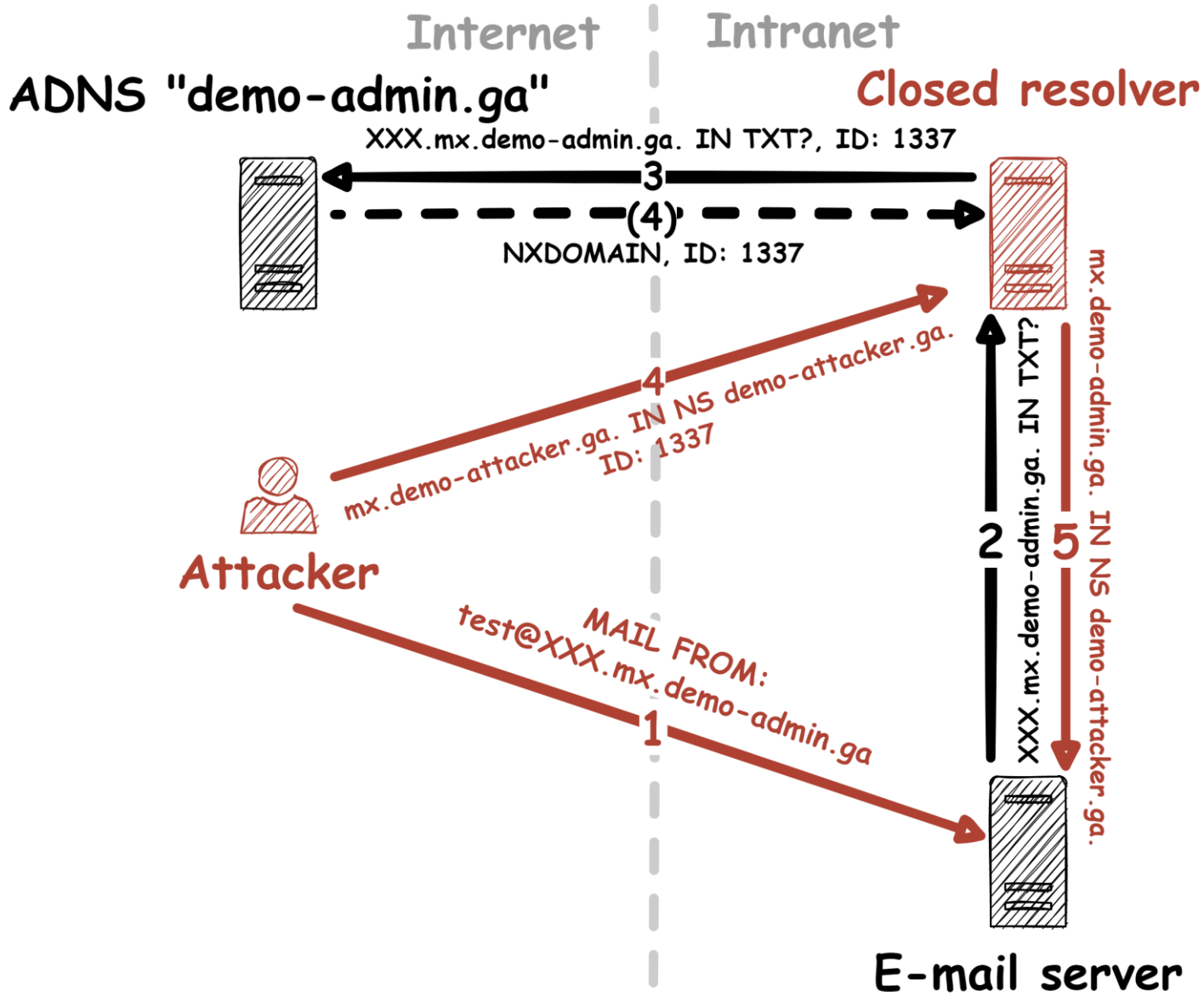
Melting the DNS Iceberg! – Demo



DEEPSEC

```
/build #
```

Melting the DNS Iceberg! – Demo



DEEPSEC

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

```
/build #
```

Username or Email Address

Password

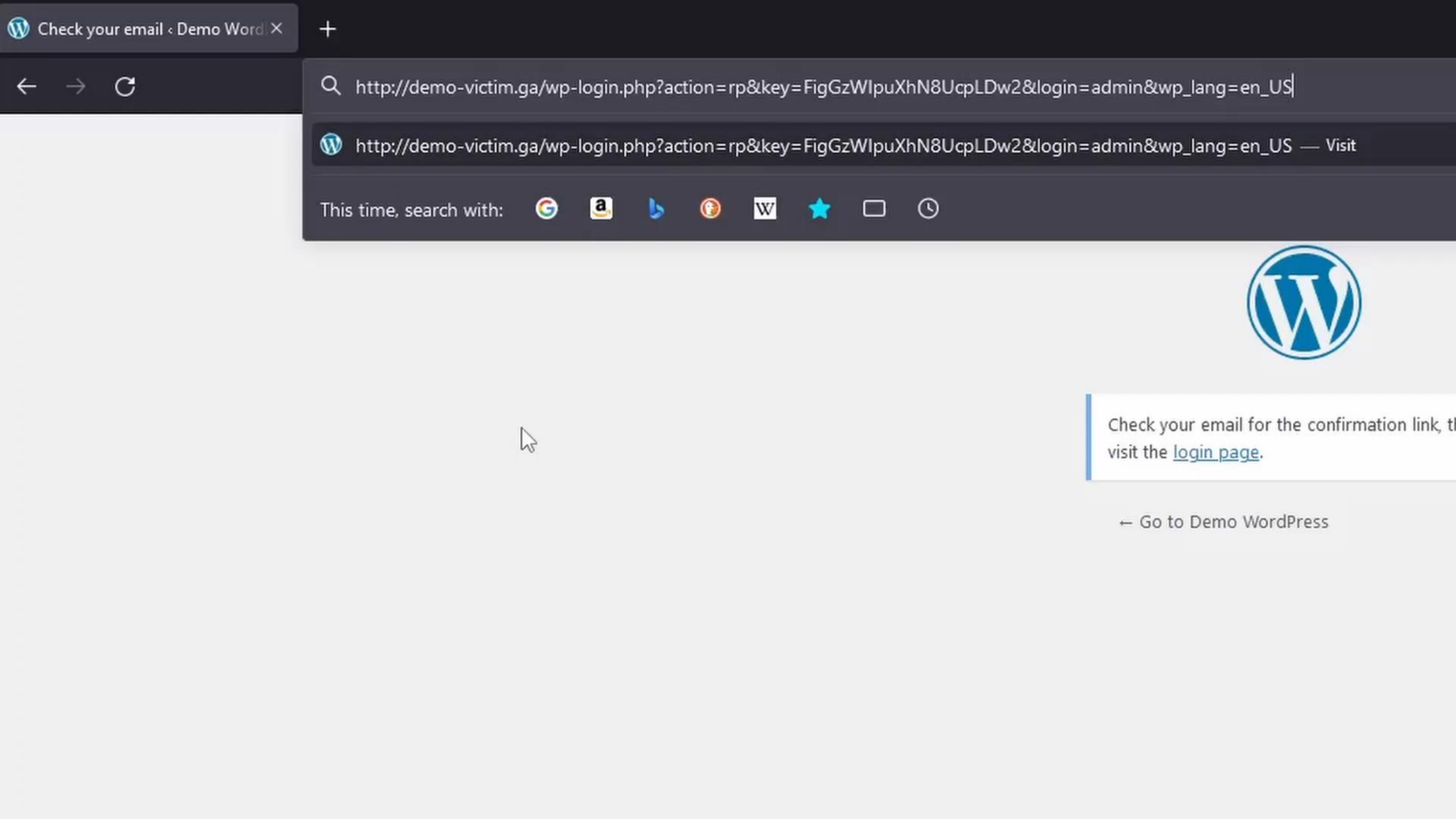
Remember Me

Log In

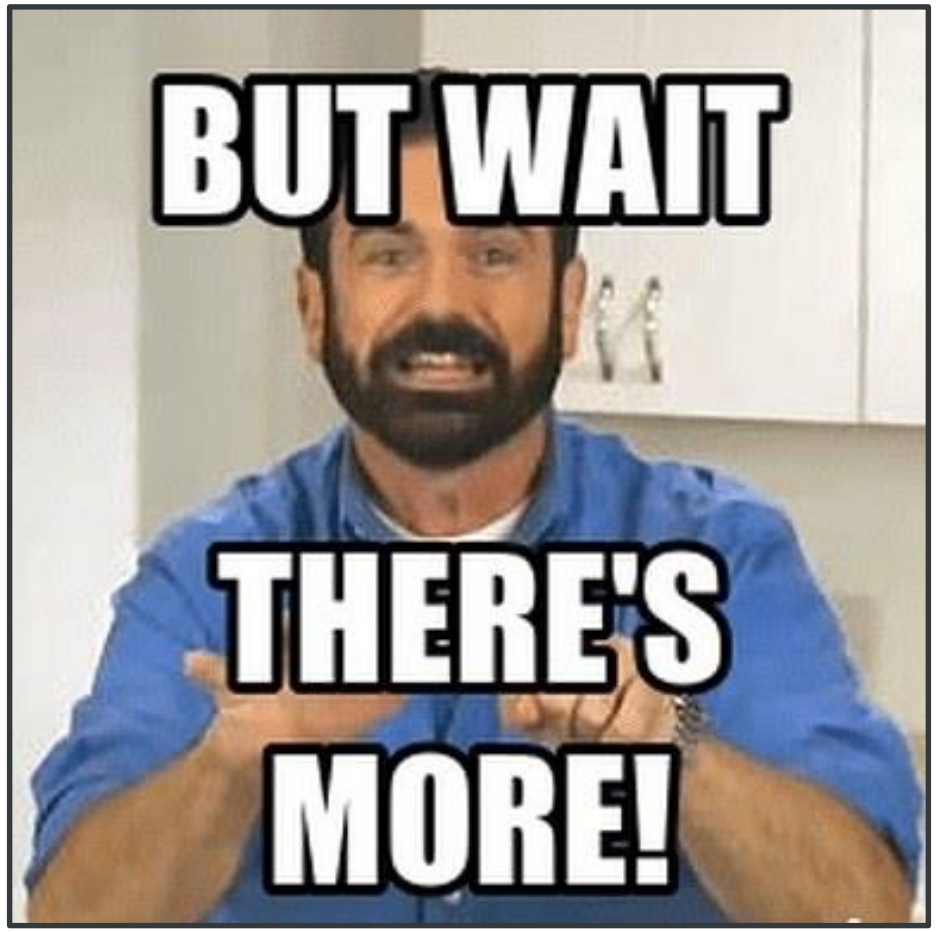
st your password?

← Go to Demo WordPress

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

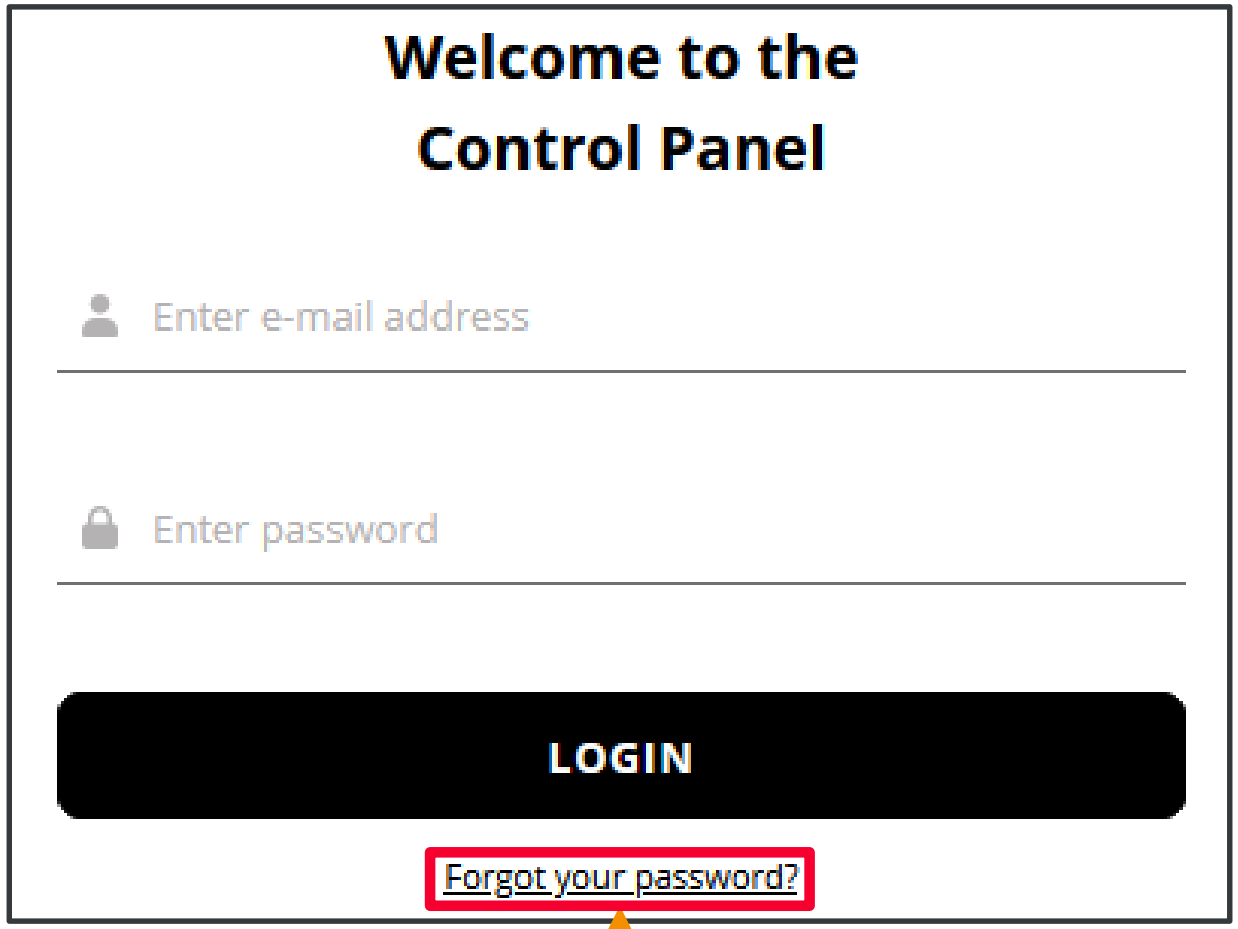

Check your email ‹ Demo Word
http://demo-victim.ga/wp-login.php?action=rp&key=FigGzWIpuXhN8UcpLDw2&login=admin&wp_lang=en_US
http://demo-victim.ga/wp-login.php?action=rp&key=FigGzWIpuXhN8UcpLDw2&login=admin&wp_lang=en_US — Visit
This time, search with:
Check your email for the confirmation link, t
visit the login page.
← Go to Demo WordPress

The Bottom of the Iceberg – Leveraging DNS



DEEPSEC

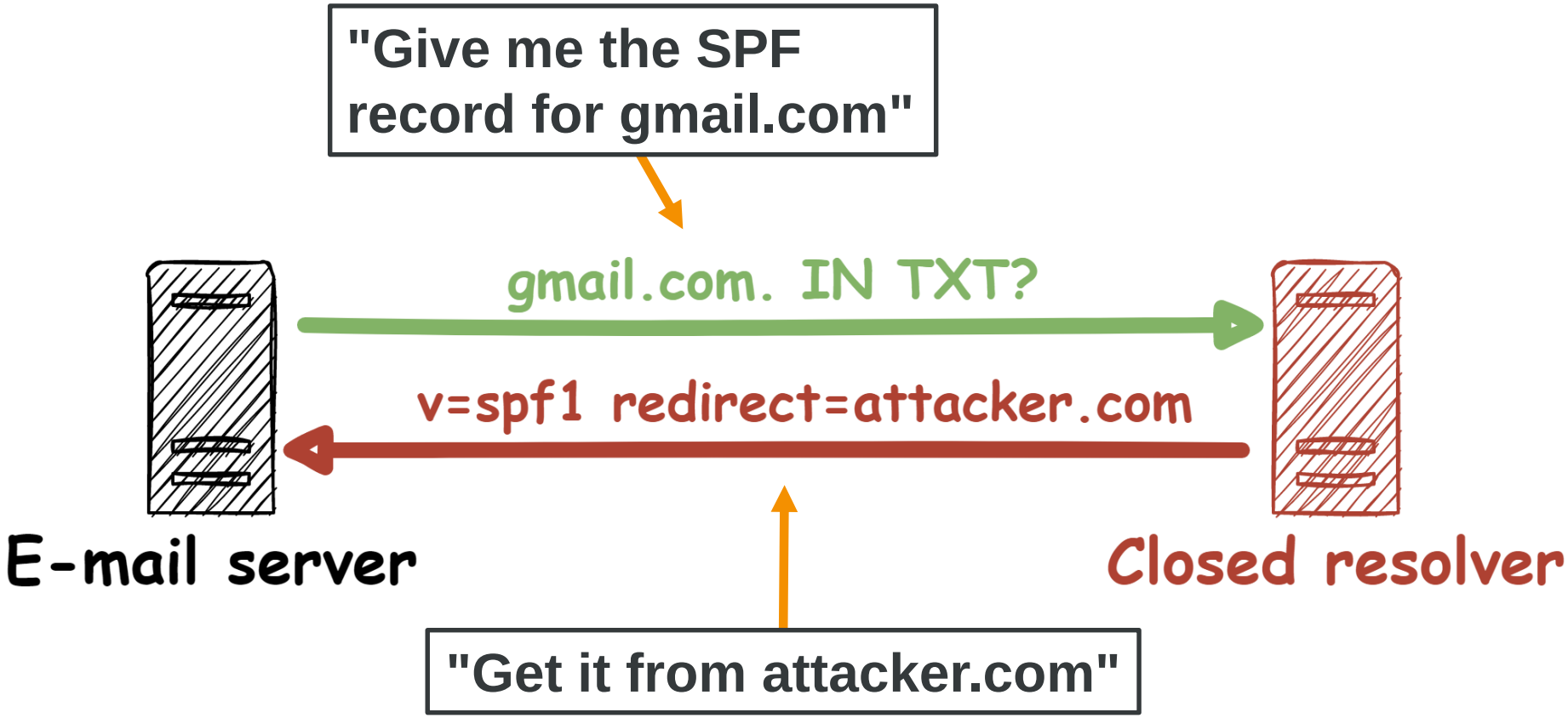
The Bottom of the Iceberg – Leveraging DNS



Let‘s reset them all!

DEEPSEC

The Bottom of the Iceberg – Leveraging DNS



DEEPSEC

Conclusion

- **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"**

Conclusion

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

Questions?