POPAI: (DNS) POisoning Prevention System

Past & Future

Yehuda Afek, Harel Berger, Anat Bremler Barr

OARC-46 Edinburgh May 16 2026

Motivation - DNS Cache Poisoning is still kicking…

DNS CVEs

CVE-2023-30464
CVE-2023-28457
CVE-2021-43105
CVE-2021-3448
CVE-2020-25684
CVE-2017-12132
CVE-2008-3217
CVE-2008-1447
CVE-2008-1454
CVE-2008-1146
CVE-2007-2926
CVE-2002-2211
CVE-2002-2212
CVE-2002-2213

DNS cache poisoning bugs hits Symantec shops

Spyware served up by fiendish, widespread attack

John Leyden

Tue 8 Mar 2005 16:33 UTC

Analyst Comment

DNS-based attacks back from the cold

The financial sector has emerged as a prime target, bearing the brunt of the impact of DNS attacks.

GlobalData. | GlobalData Thematic Intelligence November 6, 2023

2023

[TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets

SP-2024 Xiang Li; Wei Xu; Baojun Liu; Mingming Zhang; Zhou Li; Jia Zhang]

N - DNS Cache Poisoning is still kicking…

DNS Cache Poisoning Remains Pervasive — and Highly Dangerous

CVE-2008-1447
CVE-2008-1454
CVE-2008-1146
CVE-2007-2926
CVE-2002-2211
CVE-2002-2212
CVE-2002-2213

…oning bugs hits Symantec

cola

The financial sector has emerged … the impact of DNS attacks.

GlobalData. | GlobalData Thematic Intelligence | November 6, 2023

2023

[TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets

SP-2024 Xiang Li; Wei Xu; Baojun Liu; Mingming Zhang; Zhou Li; Jia Zhang]

PoPAI

POisoning **P**revention by **A**uthentication & **I**ntegrity

- IPS/FW module
- Fast & Efficient
- Detection & Mitigation
- of ***all*** Statistical DNS Poisoning attacks
- Past & Future
- zero FN and negligible FP

PoPAI

all Statistical DNS Poisoning attacks

1st statistical

1. Standard Statistical attacks

2nd Fragment

2. Fragmentation attacks

3rd Out-of-Bailiwick

3. Out-of-Bailiwick attacks

PoPAI

__all__ Statistical DNS Poisoning attacks

1st statistical

1. Standard Statistical attacks

2nd Fragment

2. Fragmentation attacks

3rd Out-of-Bailiwick

3. Out-of-Bailiwick attacks

We do not detect or mitigate Session hijacking attacks:

1. MITM poisoning attacks
2. BGP hijacking attacks

Past

Detection Module vs. Attacks

Paper	Type		#Pkts	POPS
Schuba et al. [12] 1993	-		1	-
V. Sacramento [41] 2002	S	✓	2^{16}	Rℓ1
Klein, Amit [42] 2007	S	✓	>100	Rℓ1
Kaminsky, Dan [13] 2008	S	✓	$200 \cdot q$	Rℓ1
Herzberg et al. [18] 2012	S	✓	2^{16}	Rℓ1
Herzberg et al. [18] 2012	S_{Frag}	✓	2^{16}	Rℓ2
Herzberg et al. [43] 2013	B_{Frag}	✓	1	Rℓ2
Herzberg et al. [44] 2013	S_{Frag}	✓	$\sim 2^{11}$	Rℓ2
Herzberg et al. [45] 2013	S, S_{Frag}	✓	2^{16}	Rℓ1
Zheng et al. [46] 2020	B_{Frag}	✓	1	Rℓ2
Man et al. [47] 2020	S	✓	2^{16}	Rℓ1
Dai et al. [48] 2021	S_{Frag}	✓	64	Rℓ1
Klein et al. [49] 2021	S	✓	2^{16}	Rℓ1
Jeitner et al. [50] 2022	S	✓	2^{16}	Rℓ1
Jeitner et al. [50] 2022	S	✓	2^{16}	Rℓ1
Li et al. [17] 2023	S_{OoB}	✓	2^{16}	Rℓ3
Heftring et al. [51] 2023	S_{Frag}	✓	2^{16}	Rℓ2
Li et al. [22] 2024	S	✓	2^{16}	Rℓ1

Past

Mitigated CVEs

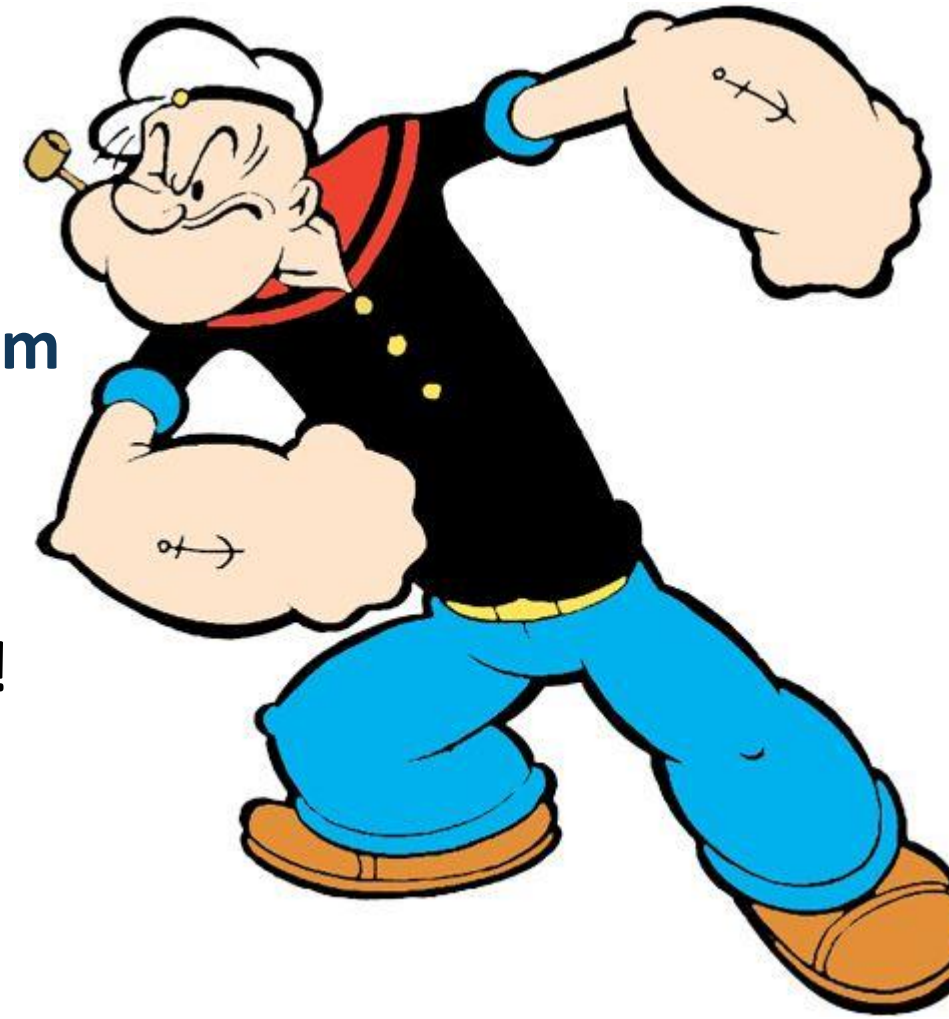
CVE	Type	Vendor	POPS
2023-30464 [88]	S	CoreDNS	Rℓ1
2023-28457 [89]	S	Microsoft DNS, Technitium	Rℓ1
2021-43105 [90]	B_{OOB}	Technitium	Rℓ3
2021-3448 [91]	S	dnsmasq	Rℓ1
2020-25684 [92, 93]	S	dnsmasq,Cisco, OpenWRT	Rℓ1
2017-12132 [94]	S_{Frag}	-	Rℓ2
2008-3217 [95]	S	PowerDNS	Rℓ1
2008-1447 [96]	S	BIND, Microsoft DNS	Rℓ1
2008-1454 [97]	B_{OOB}	Microsoft DNS	Rℓ3
2008-1146 [98]	S	OpenBSD's BIND	Rℓ1
2007-2926 [99]	S	ISC BIND	Rℓ1
2002-2211 [100]	S	BIND	Rℓ1
2002-2212 [101]	S	Fujitsu UXP/V	Rℓ1
2002-2213 [102]	S	Infoblox DNS	Rℓ1

PoPAI

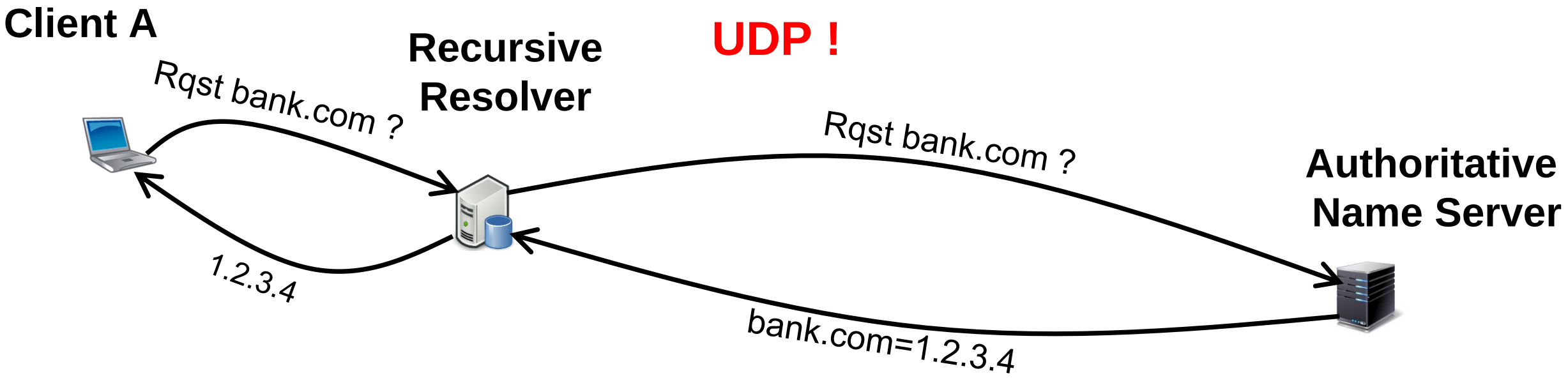
Past & Future

- **Mythos-ready for the DNS Vulnerability Storm**

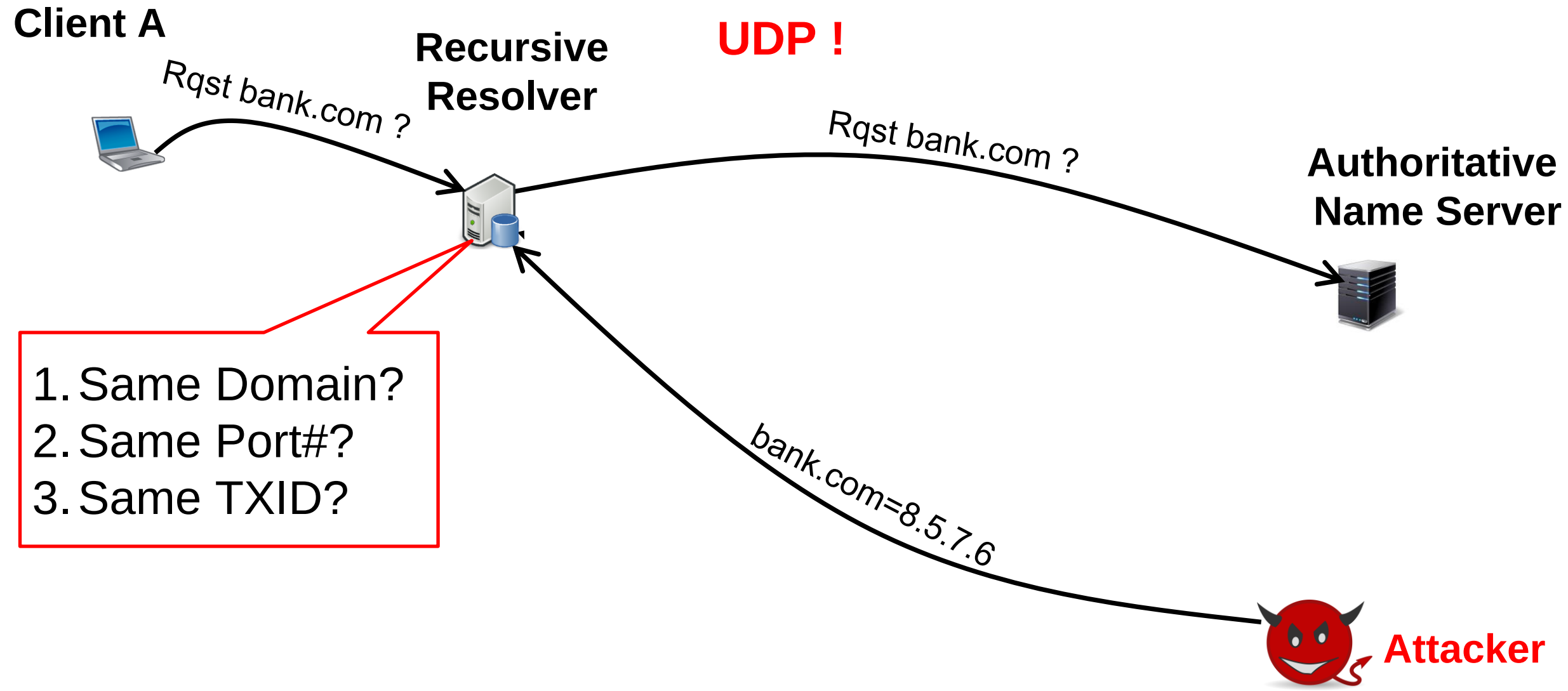
- disclosure ←→ exploitation time is shrinking!



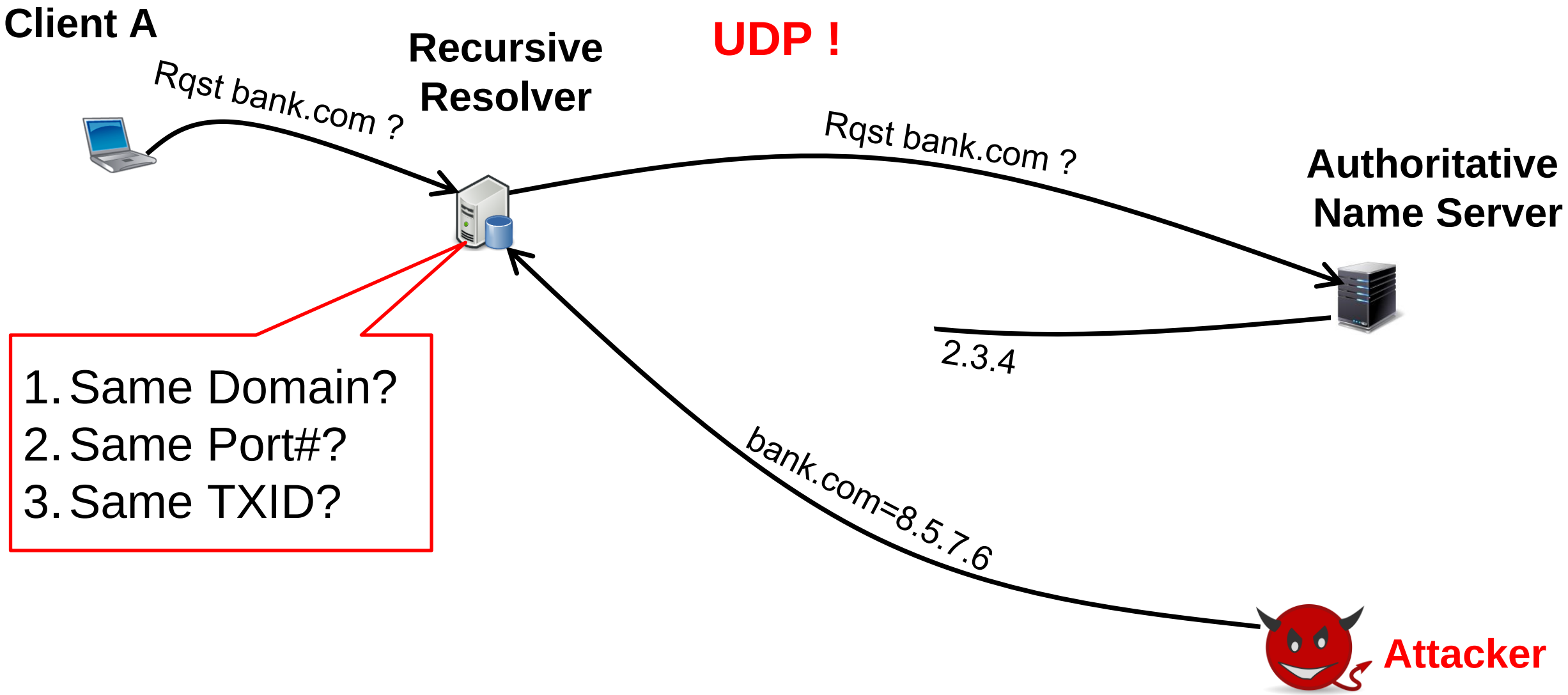
High level DNS request



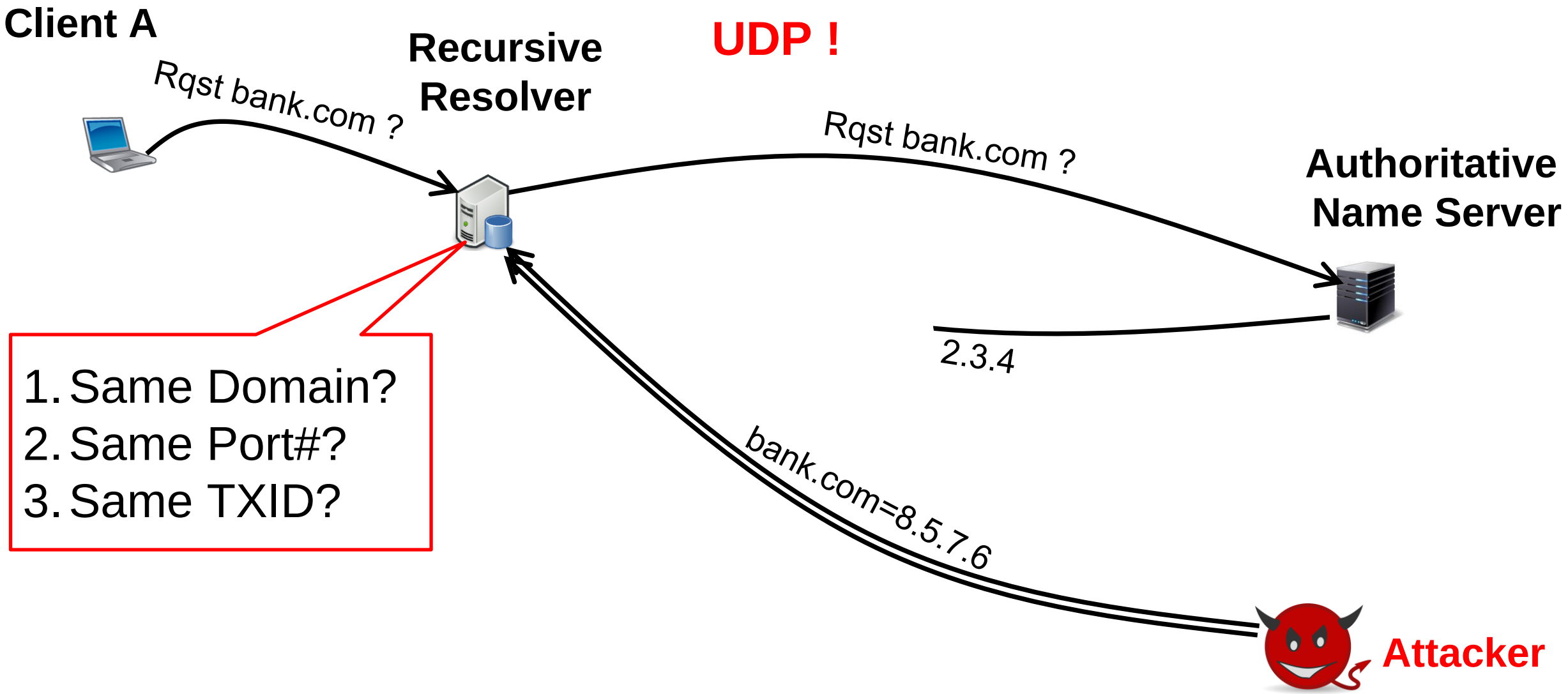
1st statistical Poisoning Attack



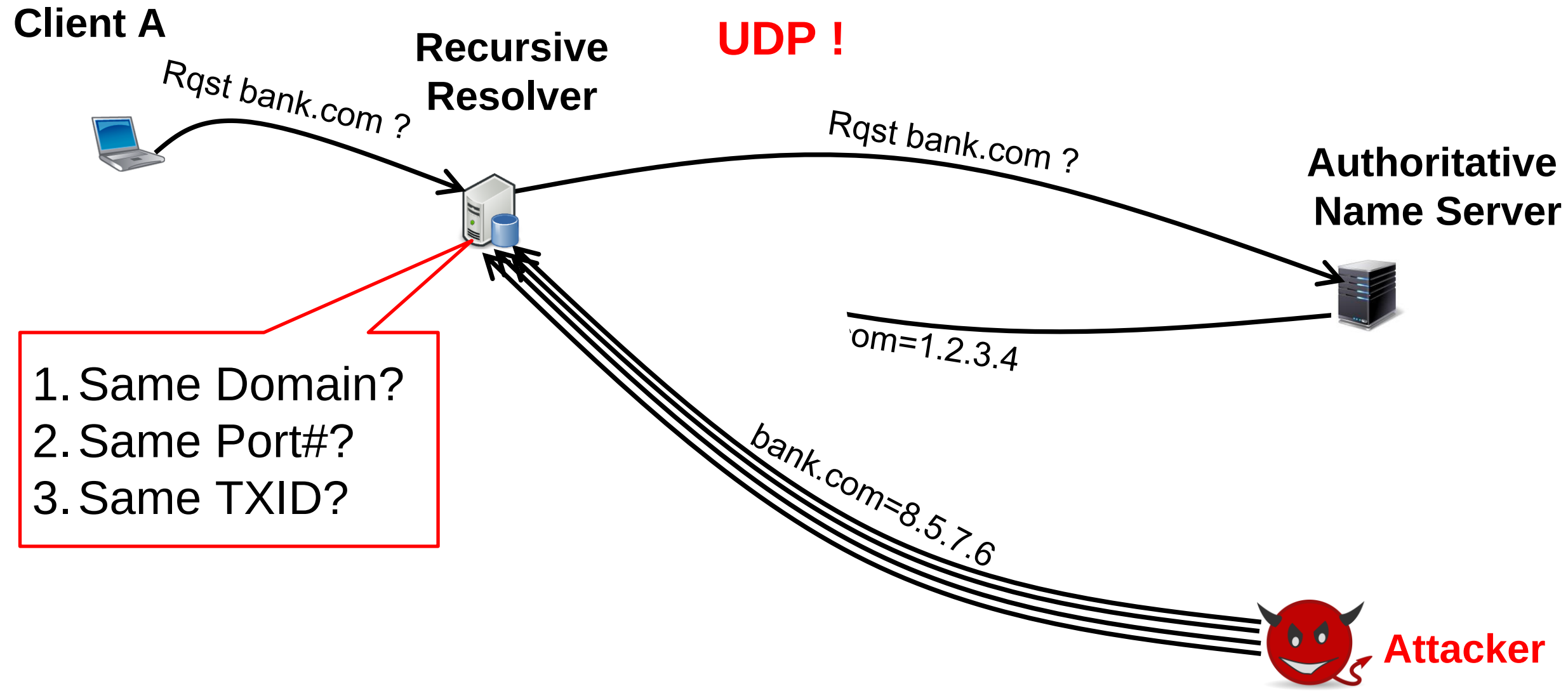
1st statistical Poisoning Attack



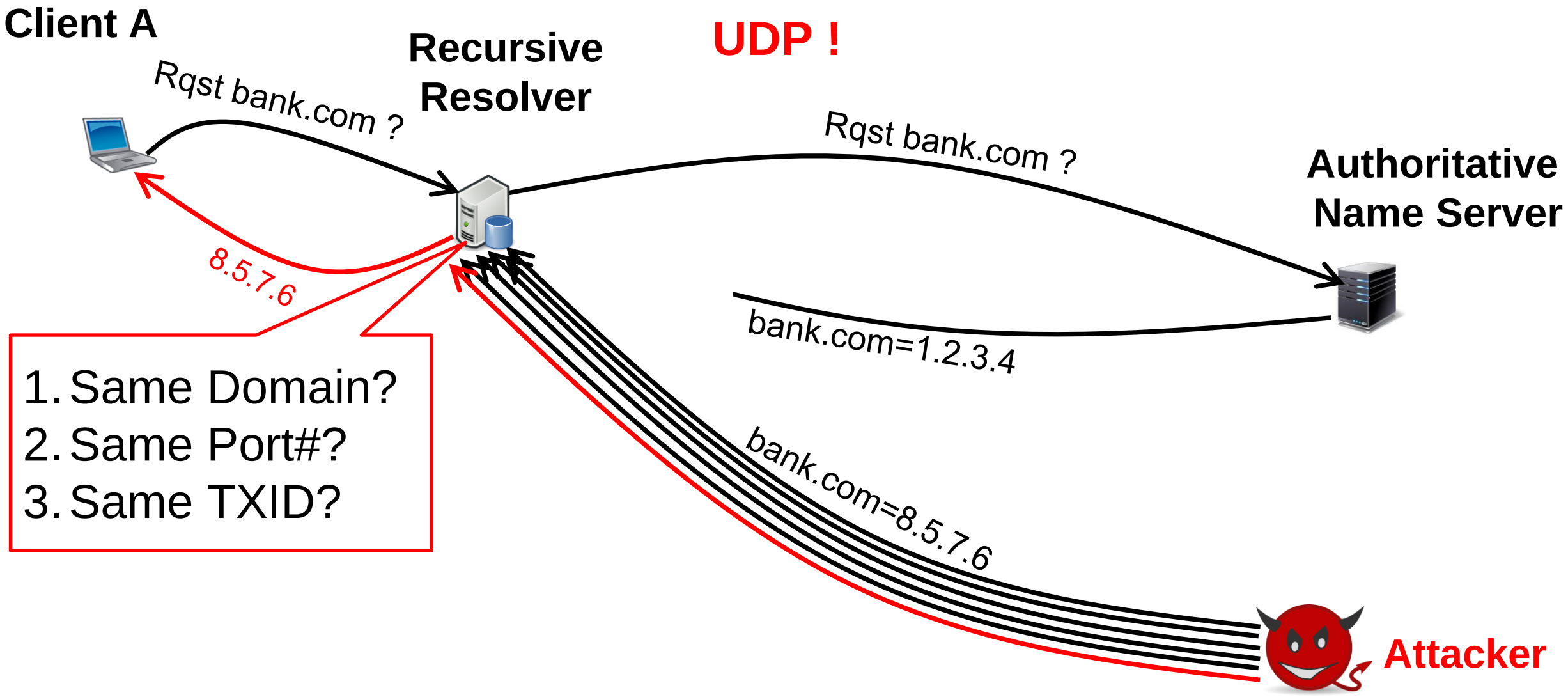
1st statistical Poisoning Attack



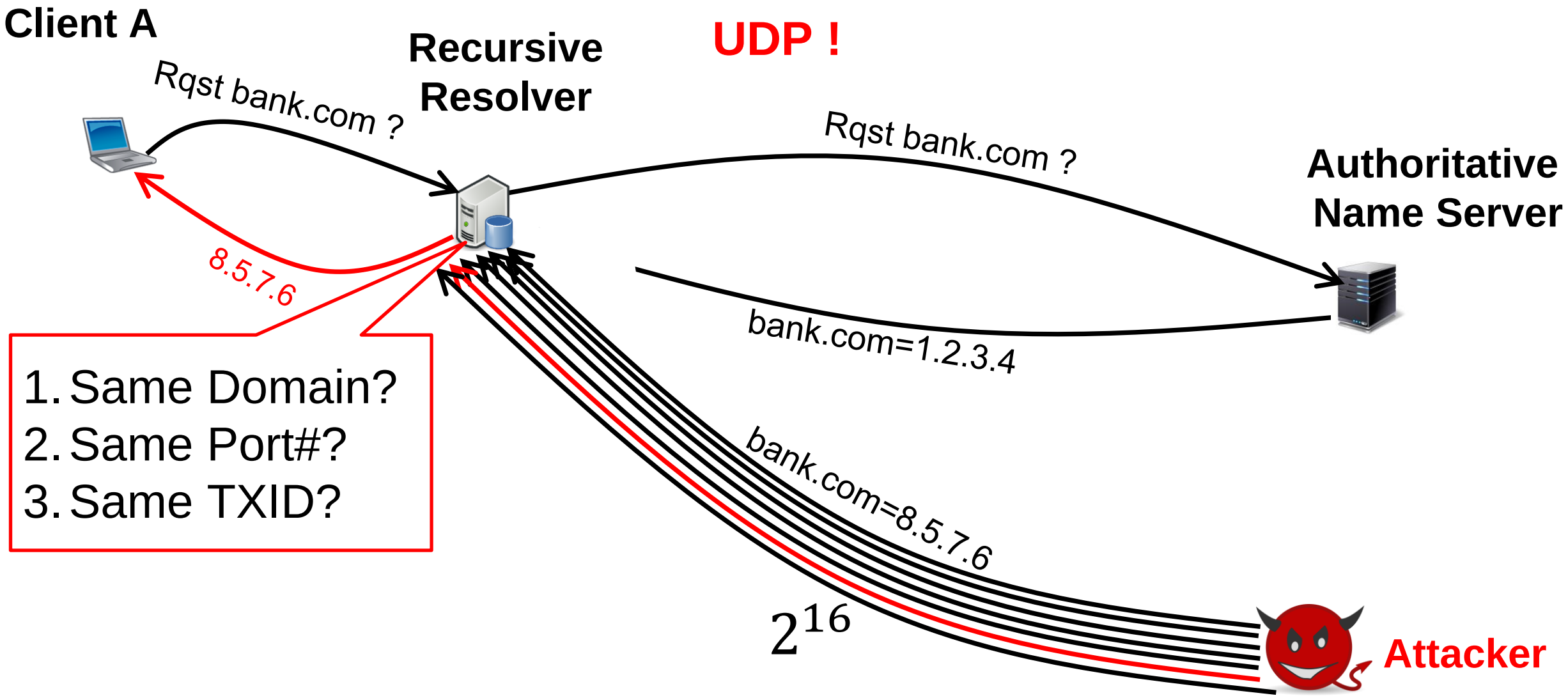
1st statistical Poisoning Attack



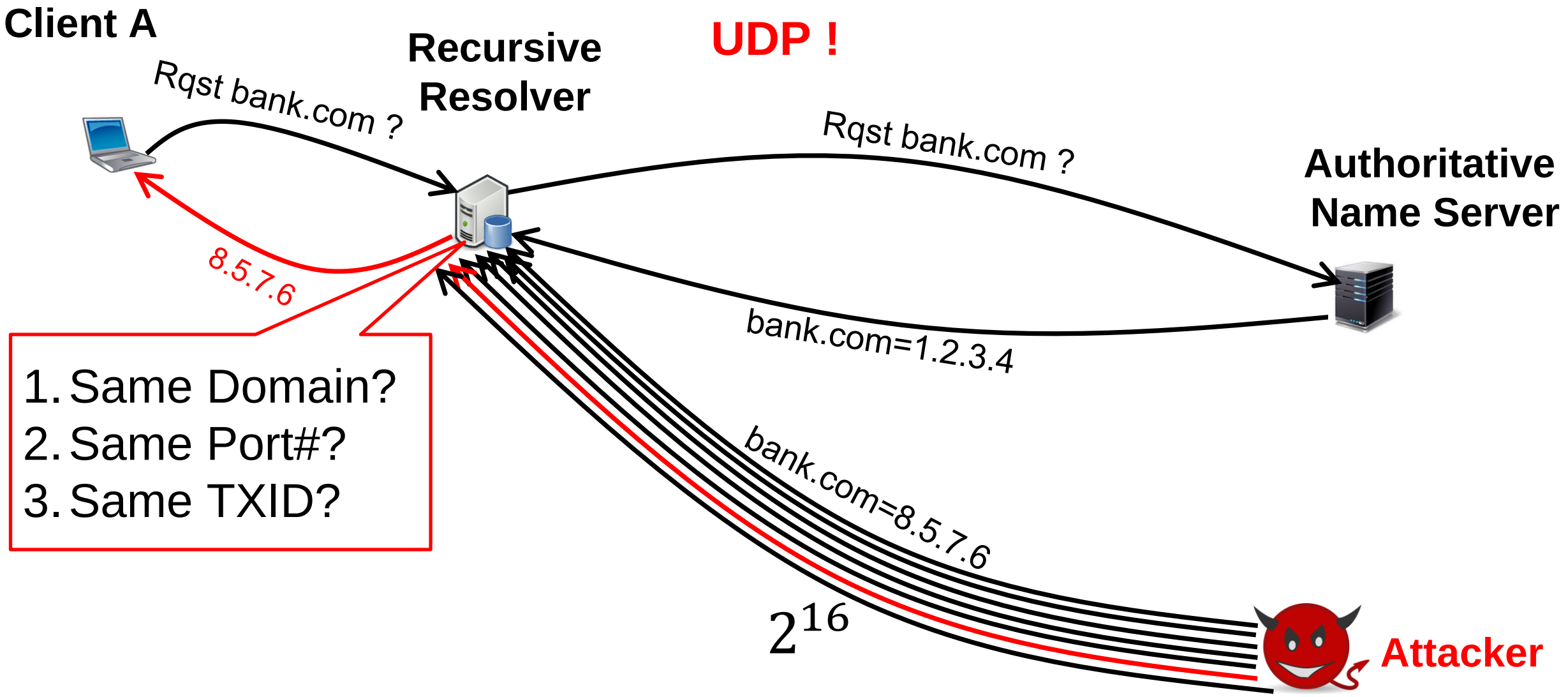
1st statistical Poisoning Attack



1st statistical Poisoning Attack

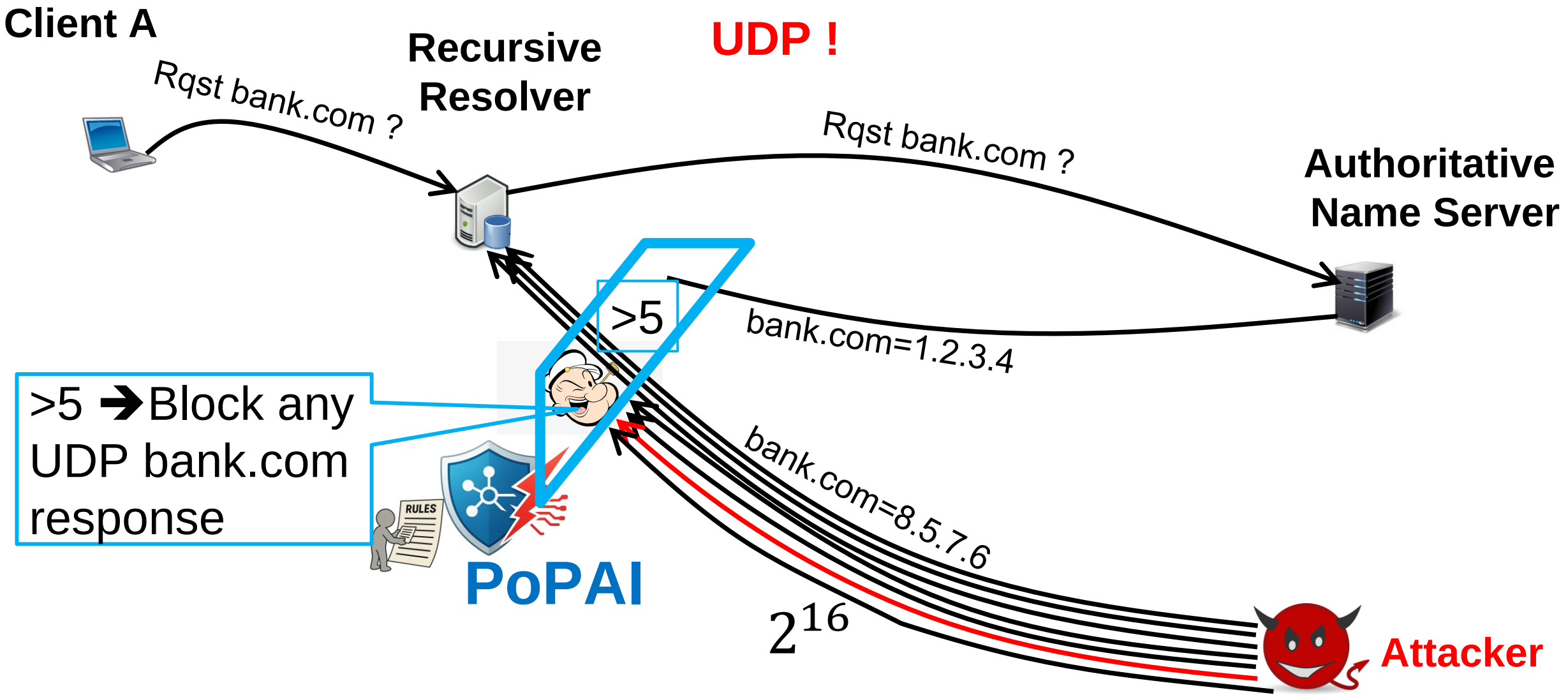


1st statistical Poisoning Attack



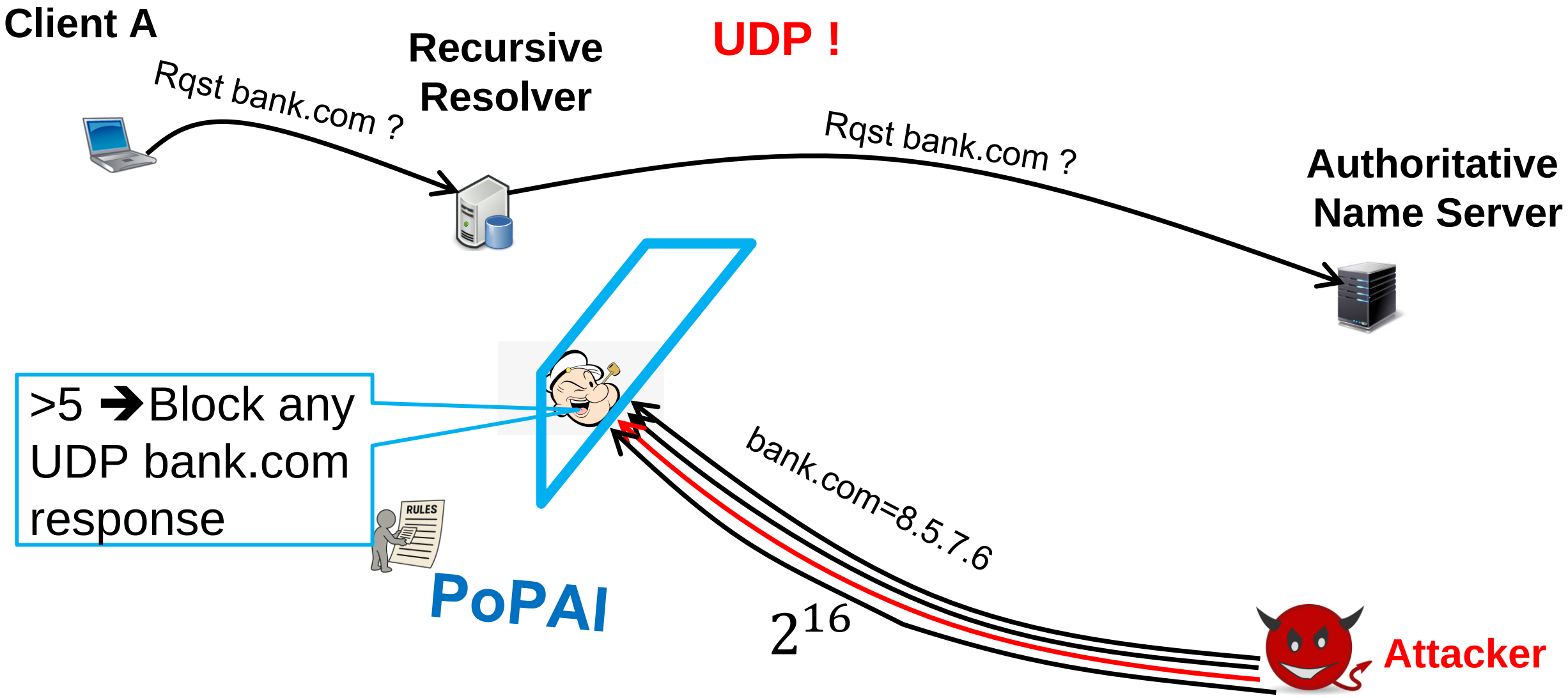
1st statistical

PoPAI Detection



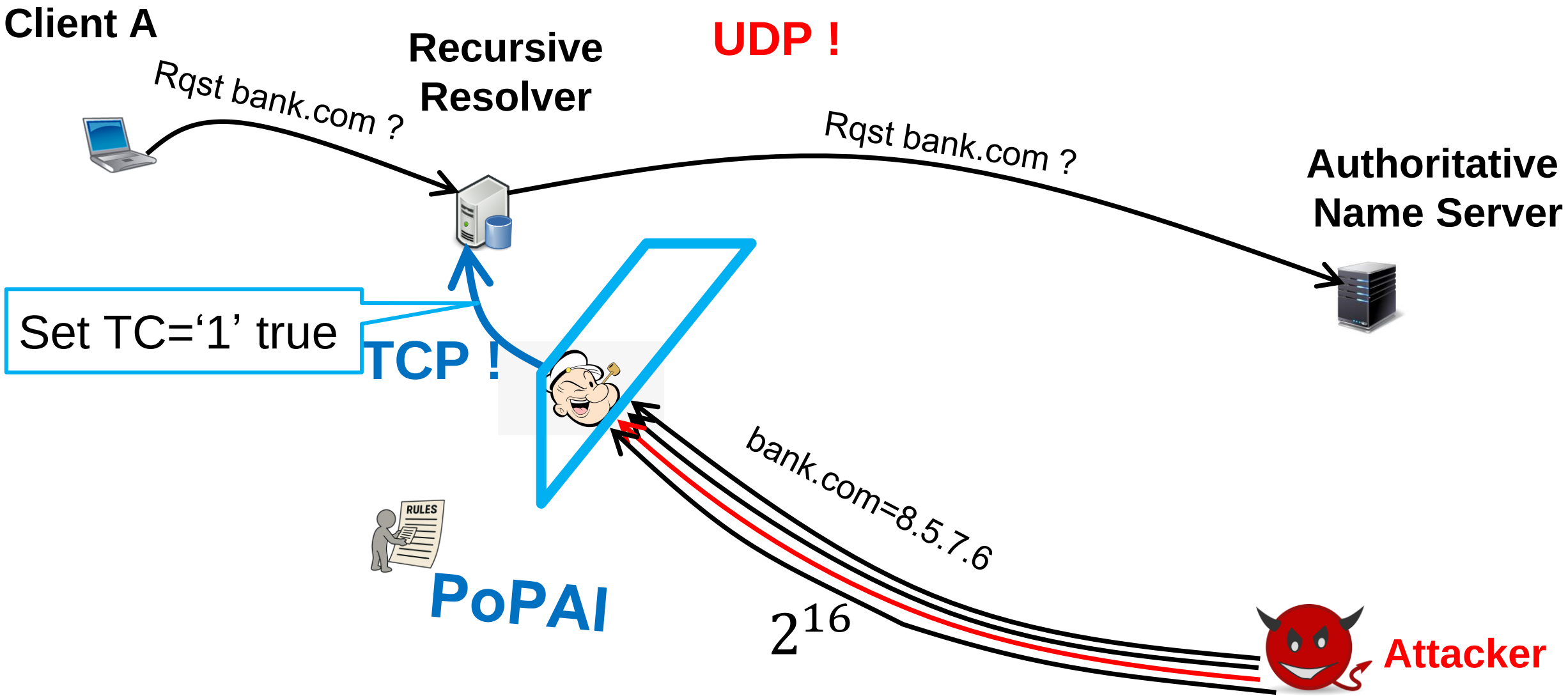
1st statistical

PoPAI Mitigation



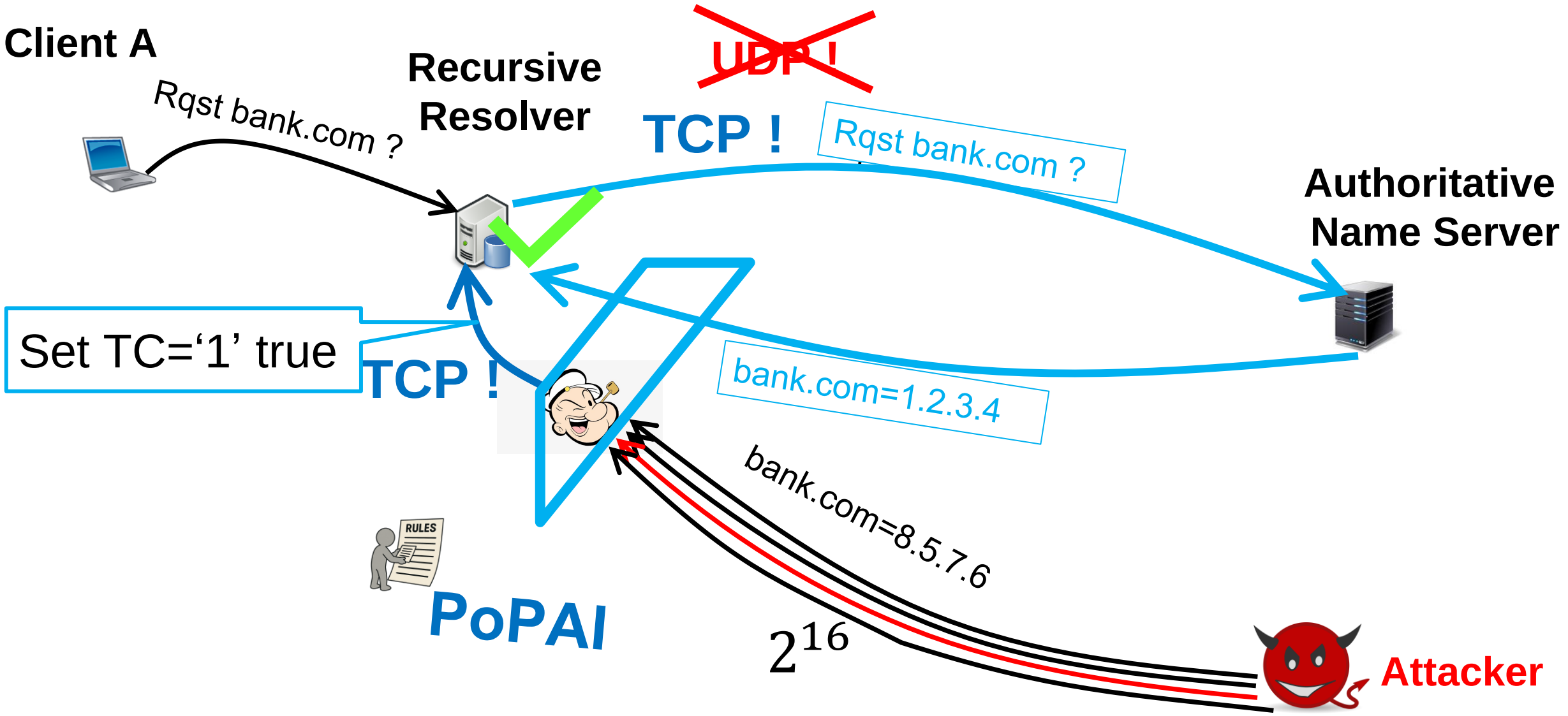
1st statistical

PoPAI Mitigation



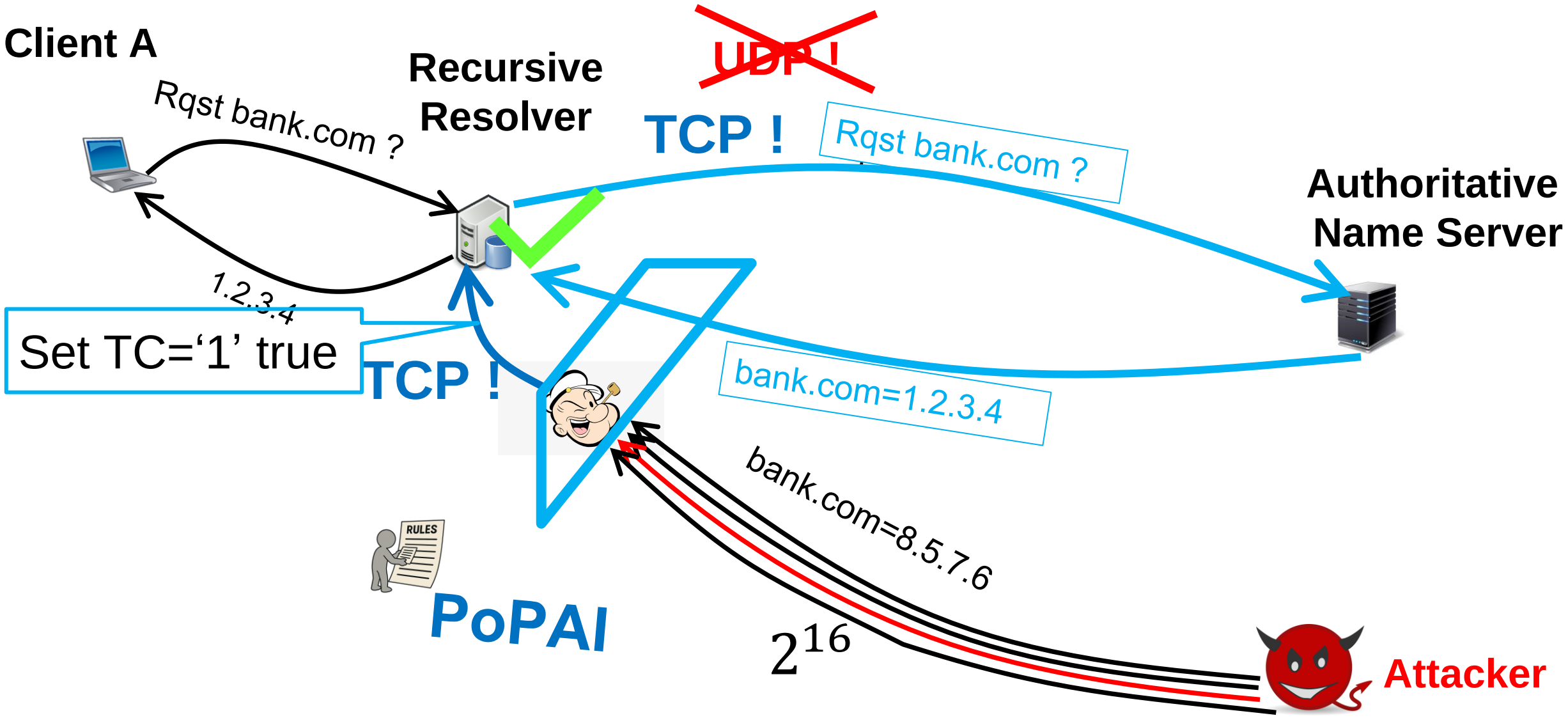
1st statistical

PoPAI Mitigation



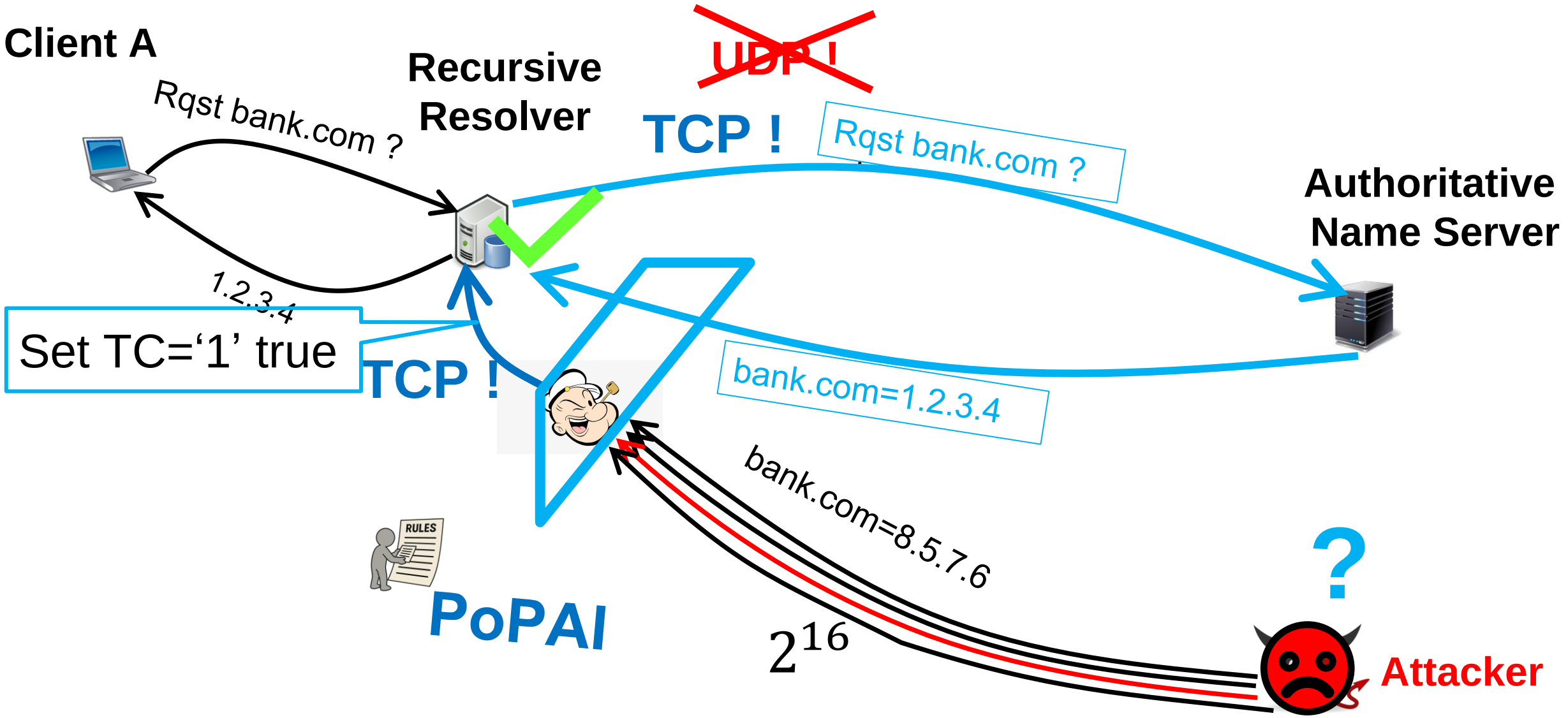
1st statistical

PoPAI Mitigation



1st statistical

PoPAI Mitigation



1st statistical

PoPAI

Statistical attacks

1st statistical

PoPAI

Statistical attacks

- **Detection: minimize false negatives (FN) & negligible false positive, 0.0076% (FP)**
  (>#5 Packets)

1st statistical

PoPAI

Statistical attacks

- **Detection:** minimize false negatives (FN) **&** negligible false positive, 0.0076% (FP)
  (>#5 Packets)
- **Mitigation:** zero FN * **&** zero FP

*Assuming resolvers respond \w TCP on TC bit
(all large ones. > 97% [Moura et.al. 21] [Bhowmick et.al.23])

1st statistical

PoPAI

Statistical attacks

- **Detection:** **minimize false negatives (FN)** **&** **negligible false positive, 0.0076% (FP)**
  (>#5 Packets)
- **Mitigation:** **zero FN** * **&** **zero FP**

==========

- All together: **zero FN**

*Assuming resolvers respond \w TCP on TC bit
(all large ones. > 97% [Moura et.al. 21] [Bhowmick et.al.23])

1st statistical

PoPAI

Statistical attacks

- **Detection:** **minimize false negatives (FN)** **&** **negligible false positive, 0.0076% (FP)**
  (>#5 Packets)
- **Mitigation:** **zero FN** * **&** **zero FP**

==========

- All together: **zero FN** **&** **negligible FP (0.0076%)**

*Assuming resolvers respond \w TCP on TC bit
(all large ones. > 97% [Moura et.al. 21] [Bhowmick et.al.23])

1st statistical

PoPAI

Statistical attacks

- **Detection:** **minimize false negatives (FN)** **&** **negligible false positive, 0.0076% (FP)**
  (>#5 Packets)
- **Mitigation:** **zero FN** * **&** **zero FP**

==========

- All together: **zero FN** **&** **negligible FP (0.0076%)**

In conclusion:

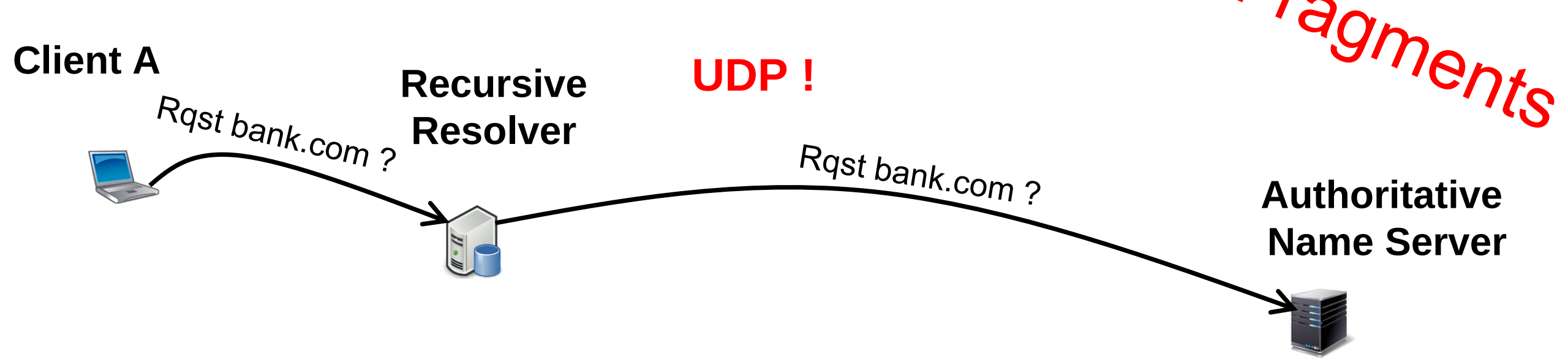
➔ Blocks 99.993% of attacks with **zero** false negatives!

➔ **Fast & efficient**

*Assuming resolvers respond \w TCP on TC bit
(all large ones. > 97% [Moura et.al. 21] [Bhowmick et.al.23])

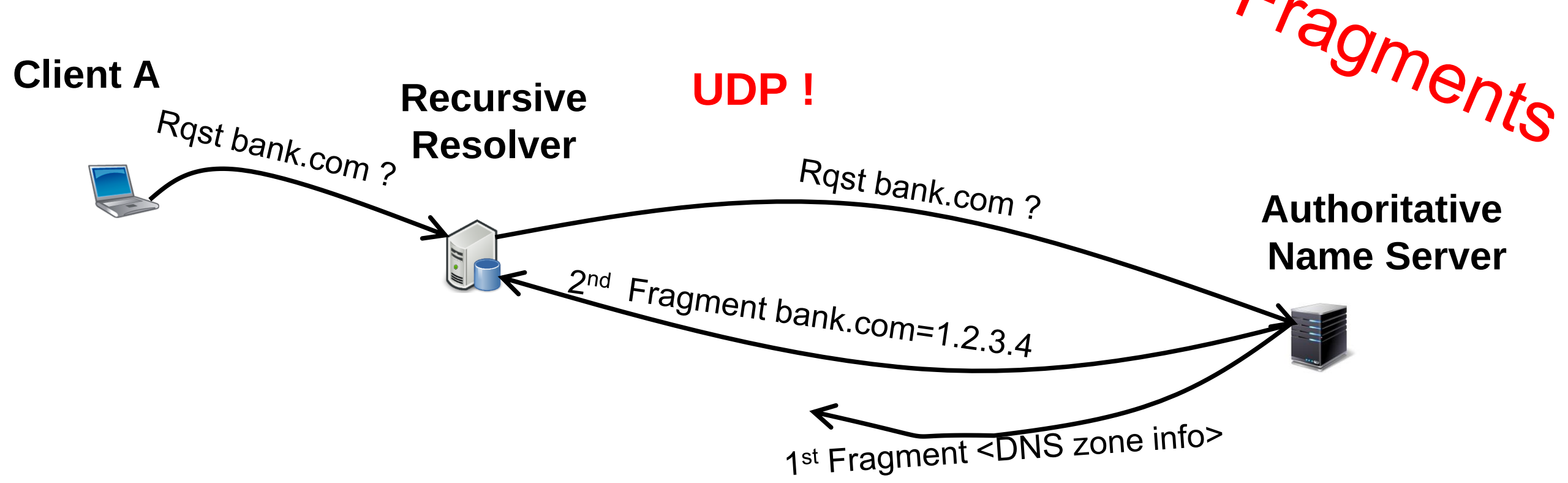
2nd Fragmentation

DNS Fragmentation Response

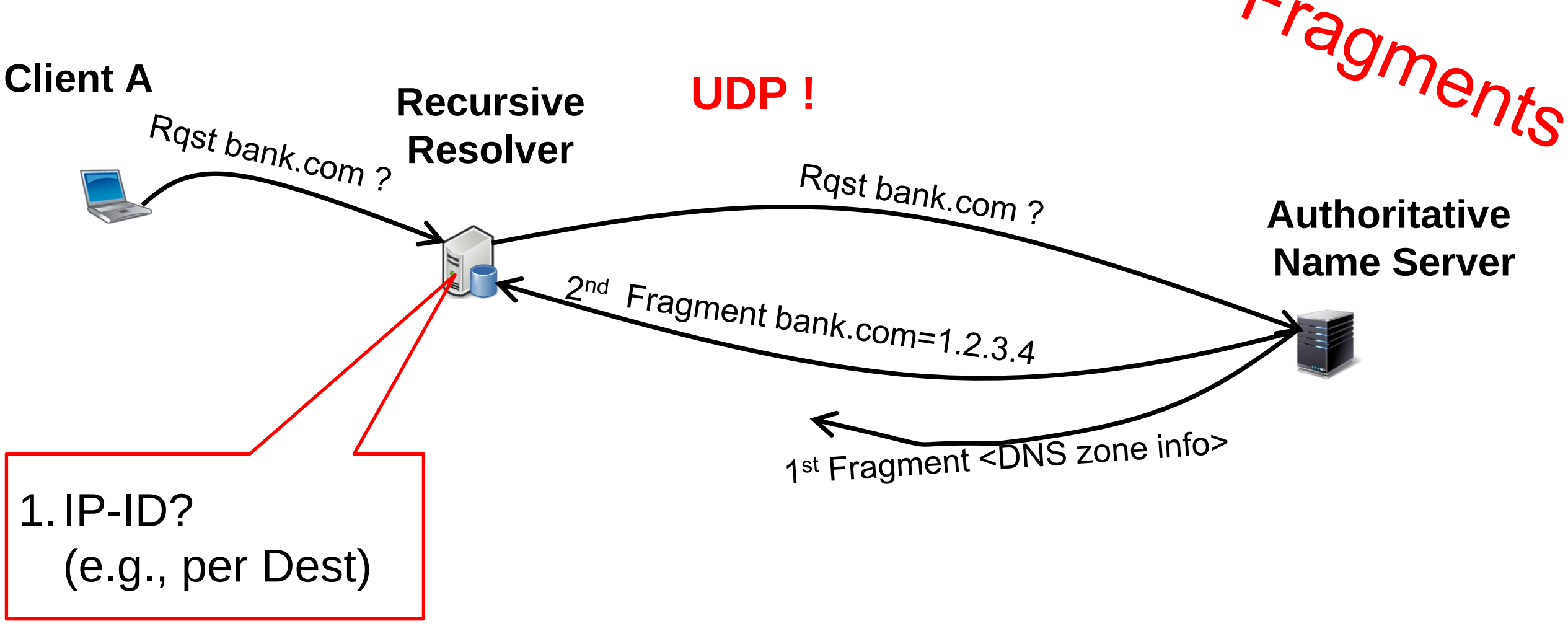


2nd Fragmentation

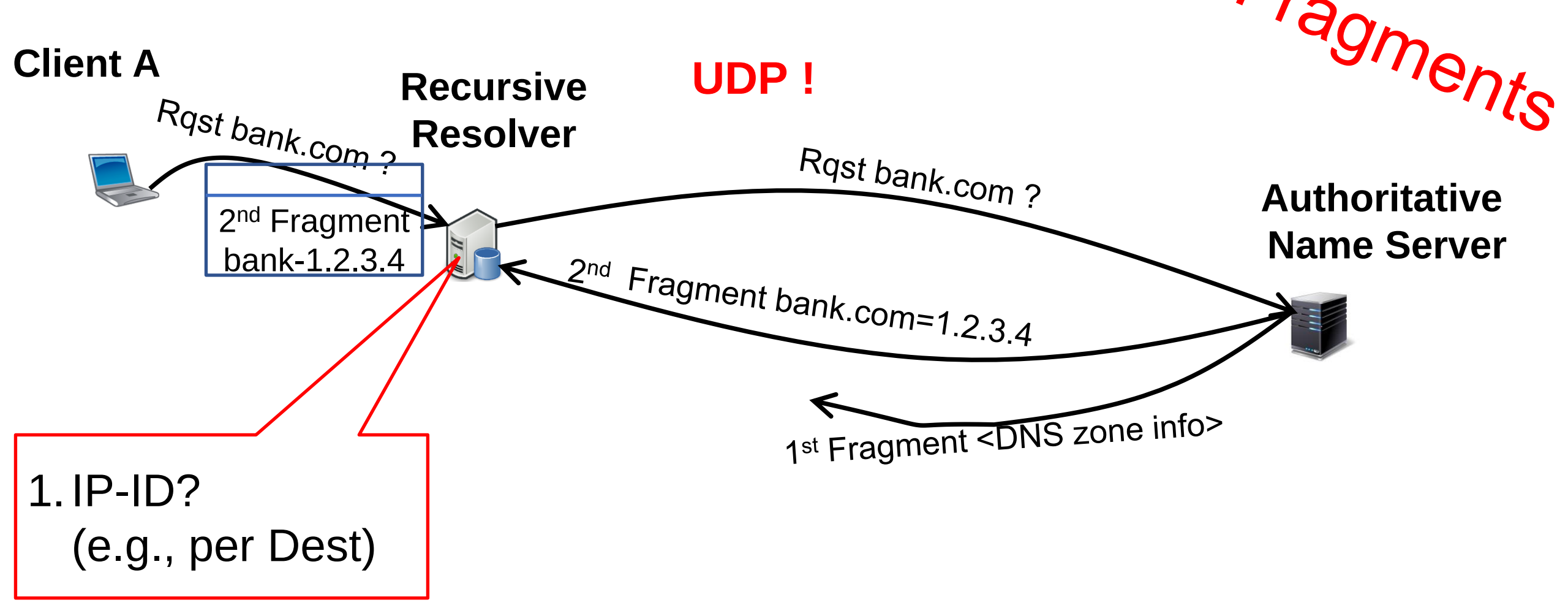
DNS Fragmentation Response



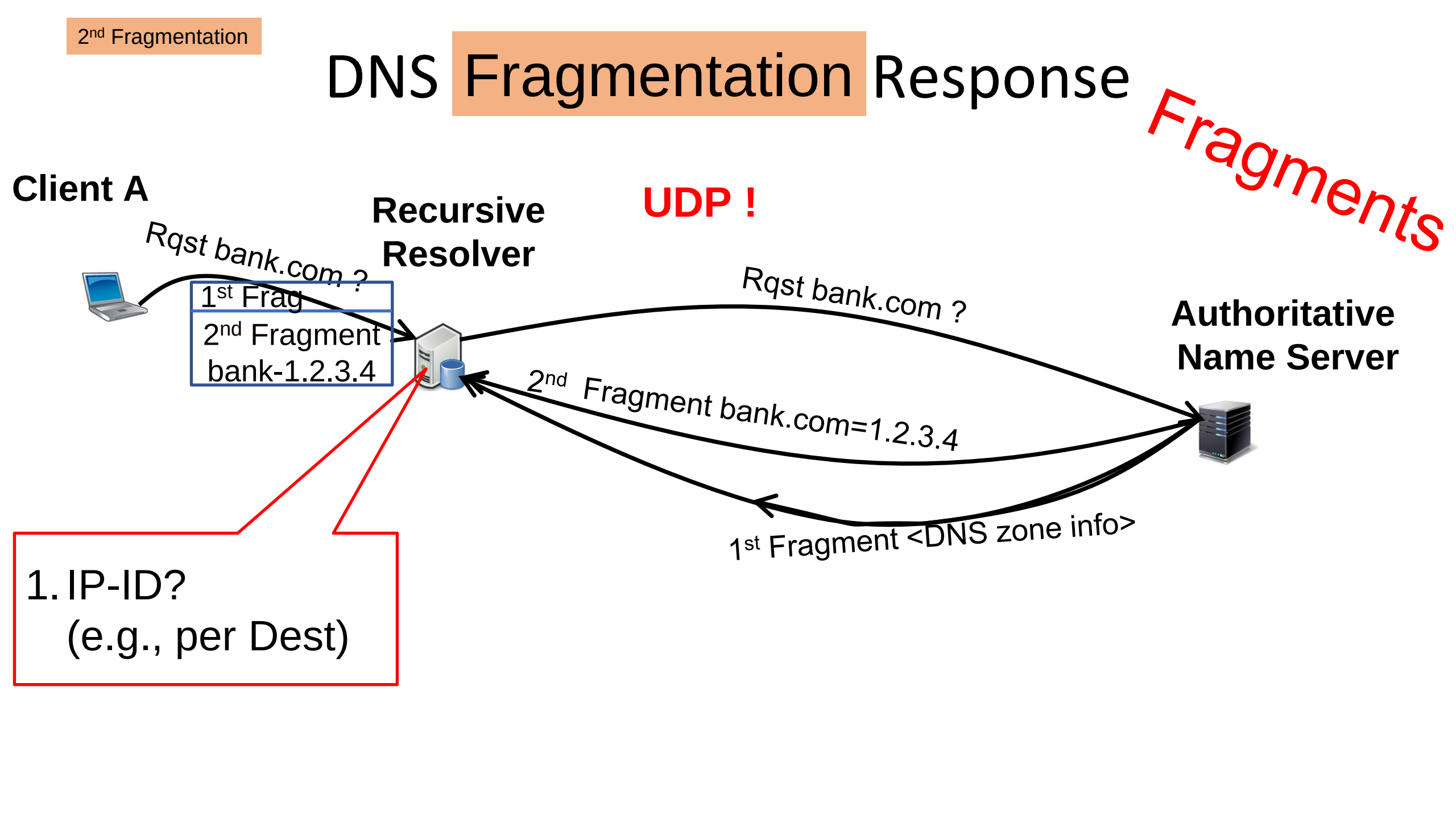
DNS Fragmentation Response



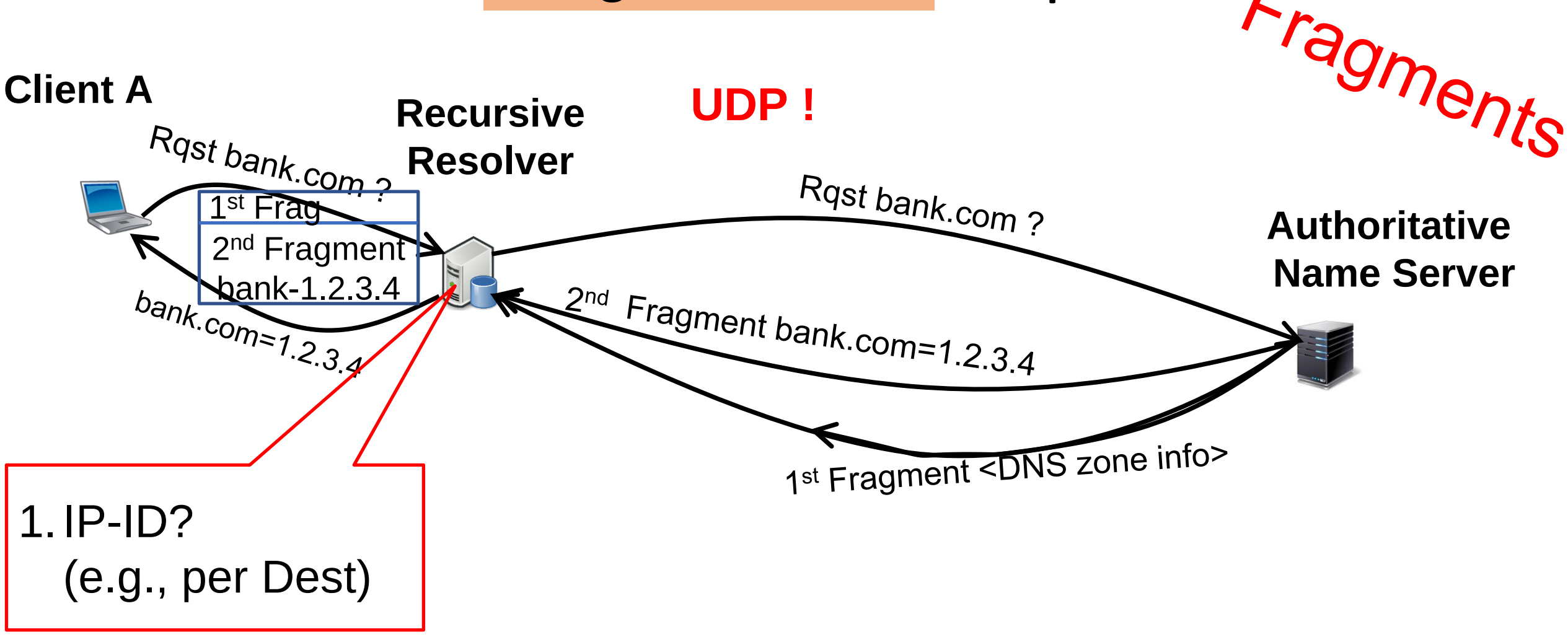
DNS Fragmentation Response



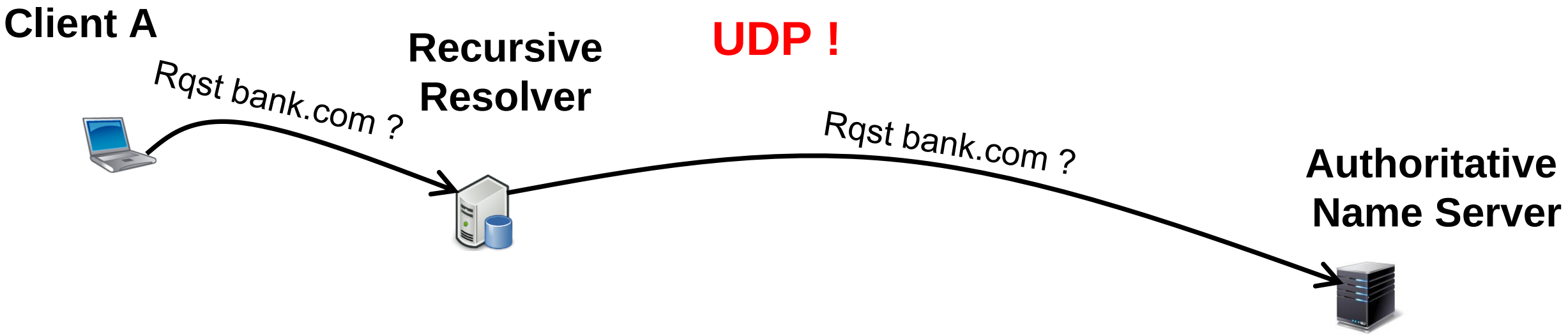
DNS Fragmentation Response



DNS Fragmentation Response

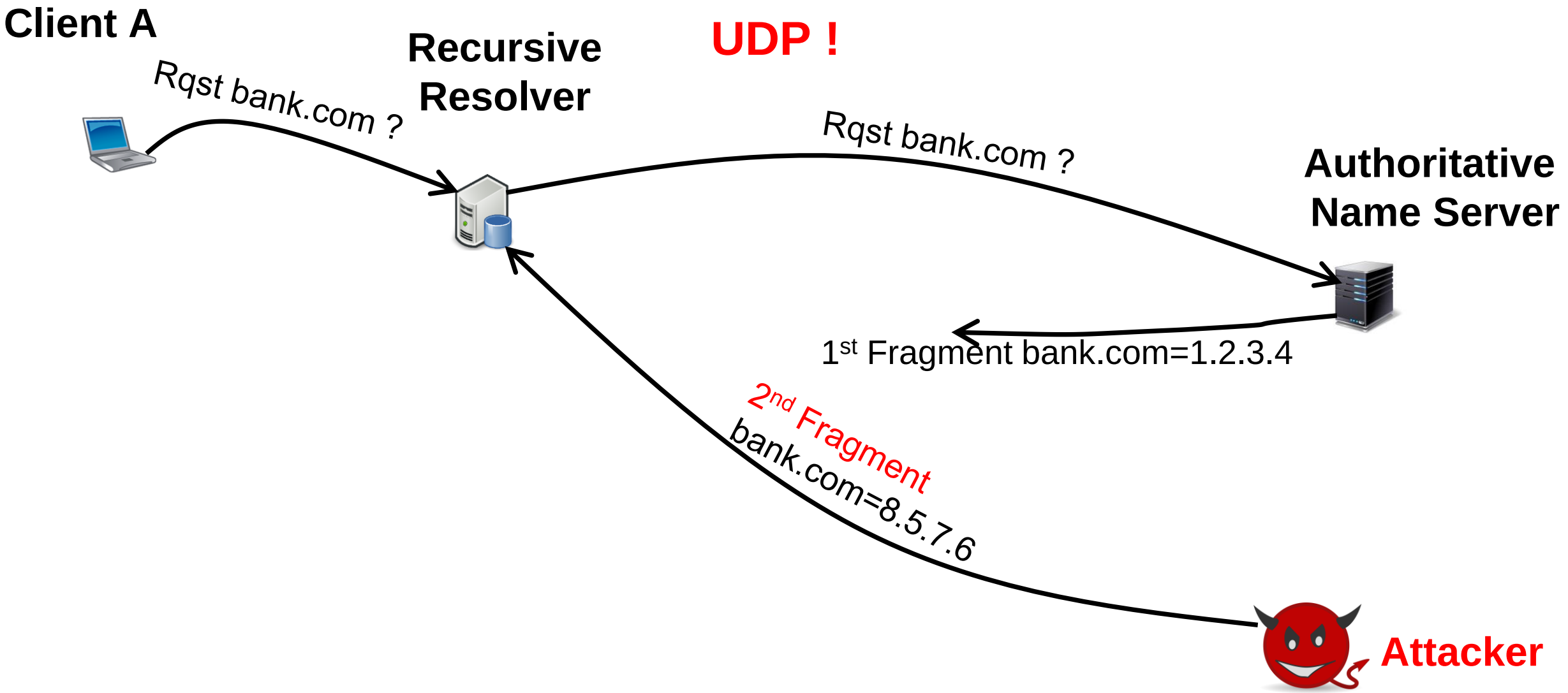


Fragmentation Poisoning Attack

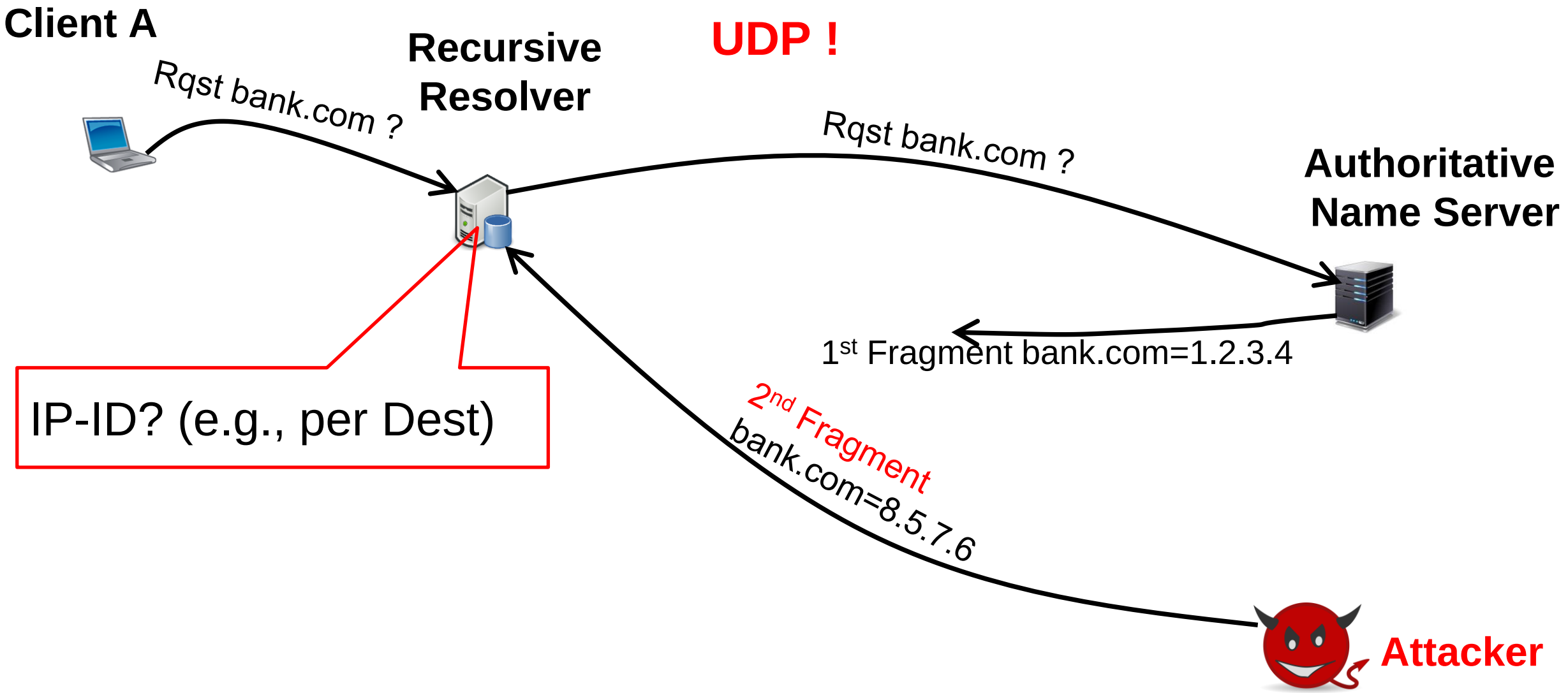


Attacker

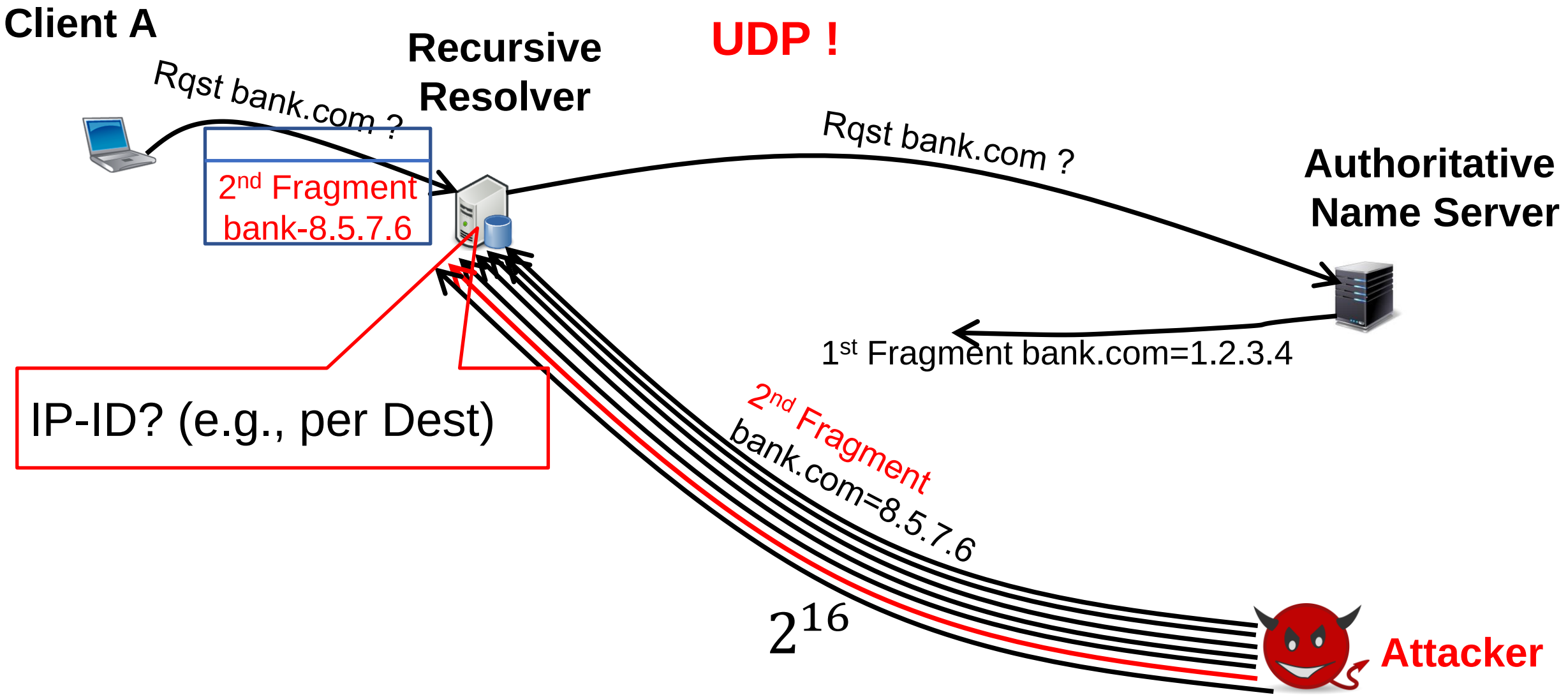
Fragmentation Poisoning Attack



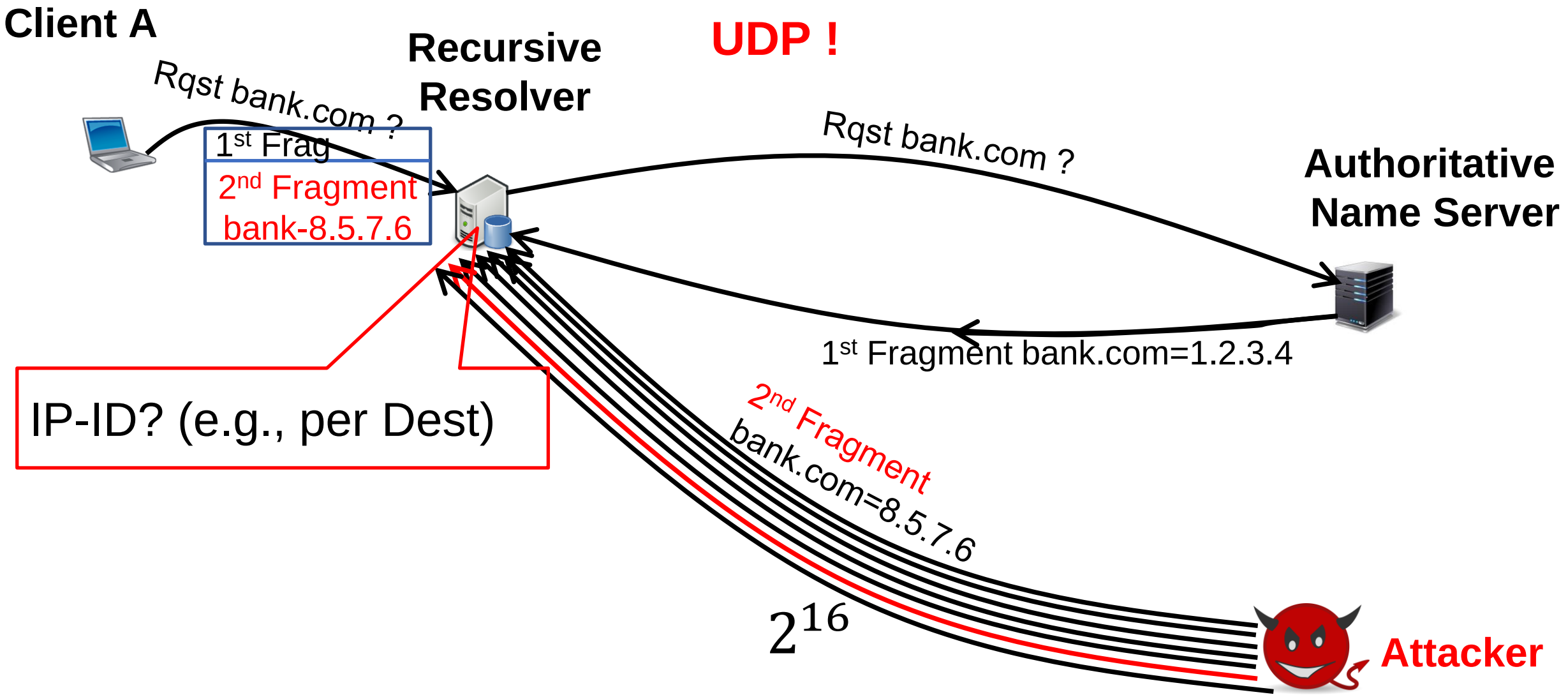
Fragmentation Poisoning Attack



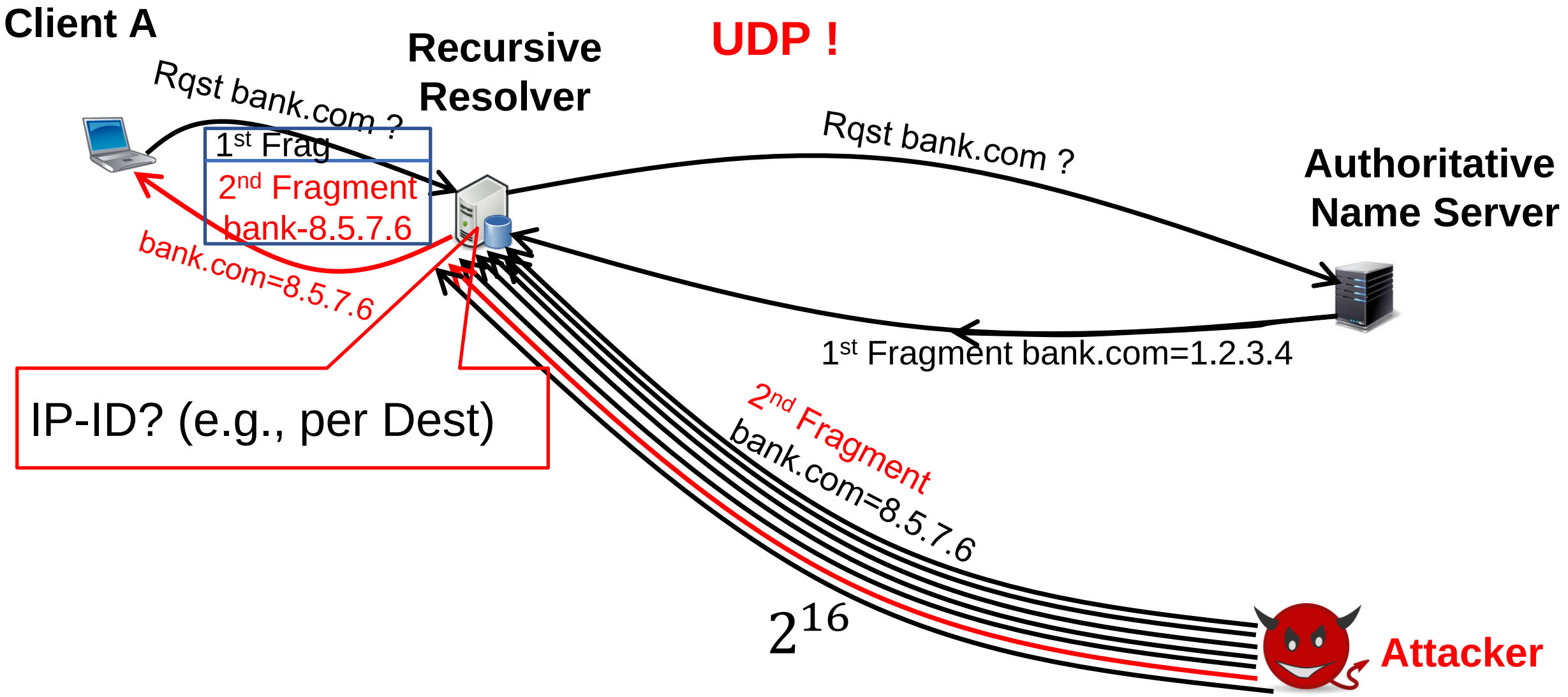
Fragmentation Poisoning Attack



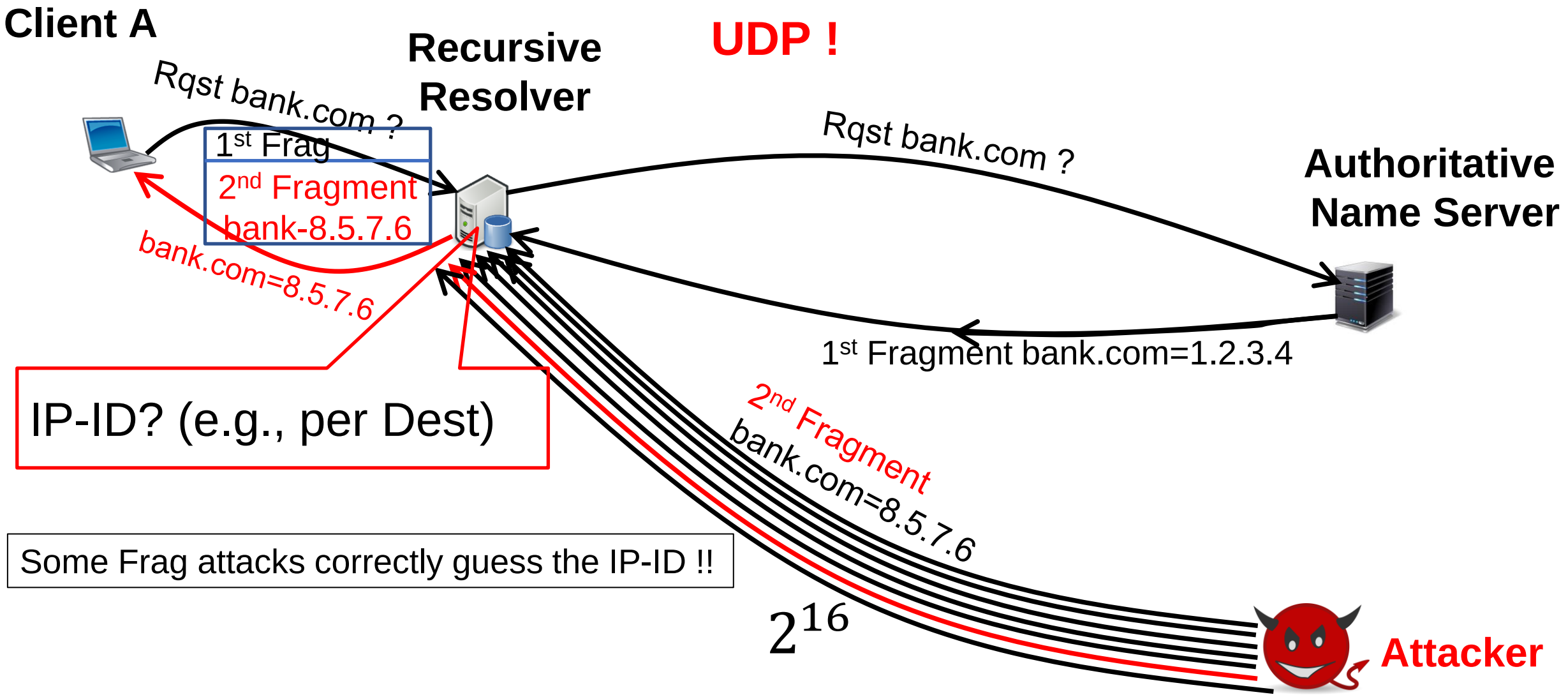
Fragmentation Poisoning Attack



Fragmentation Poisoning Attack



Fragmentation Poisoning Attack

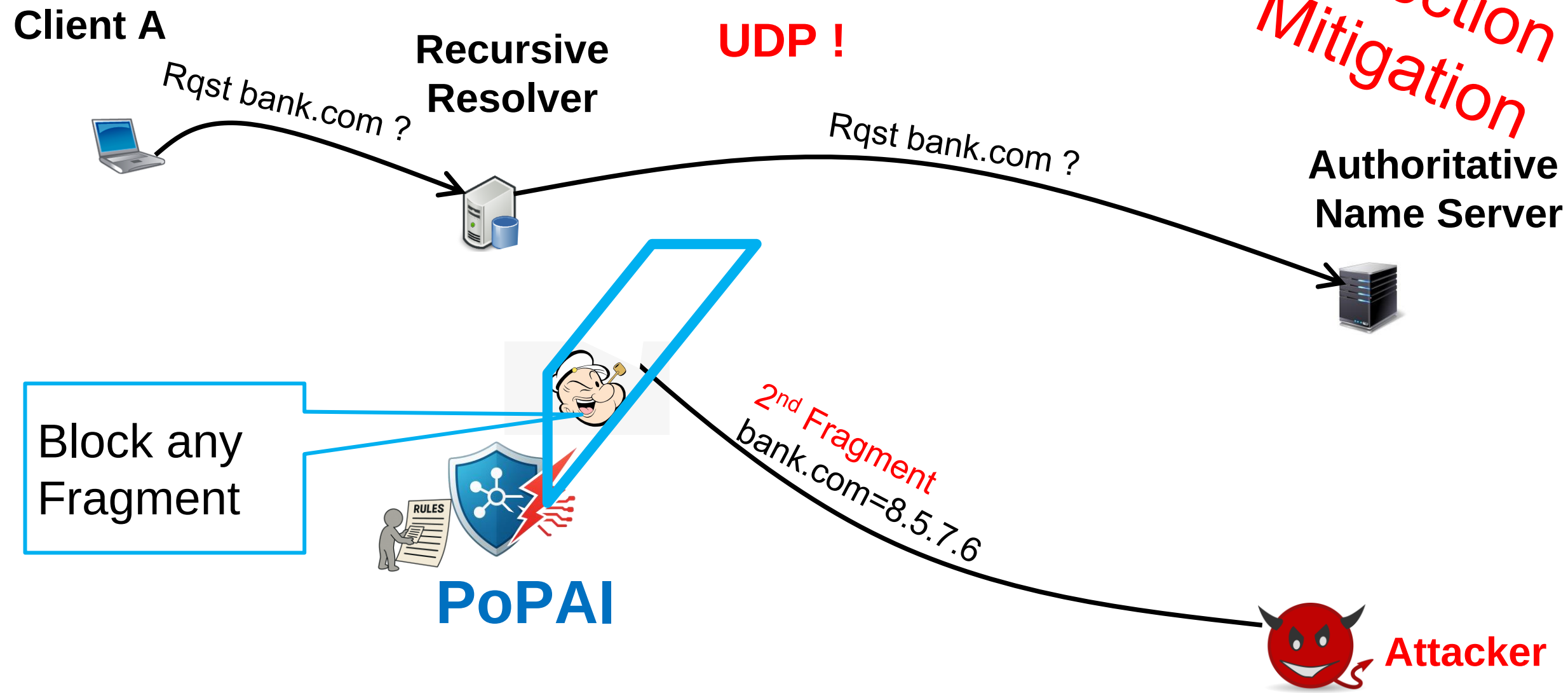


Some Frag attacks correctly guess the IP-ID !!

2nd Fragmentation

Fragmentation Poisoning Attack

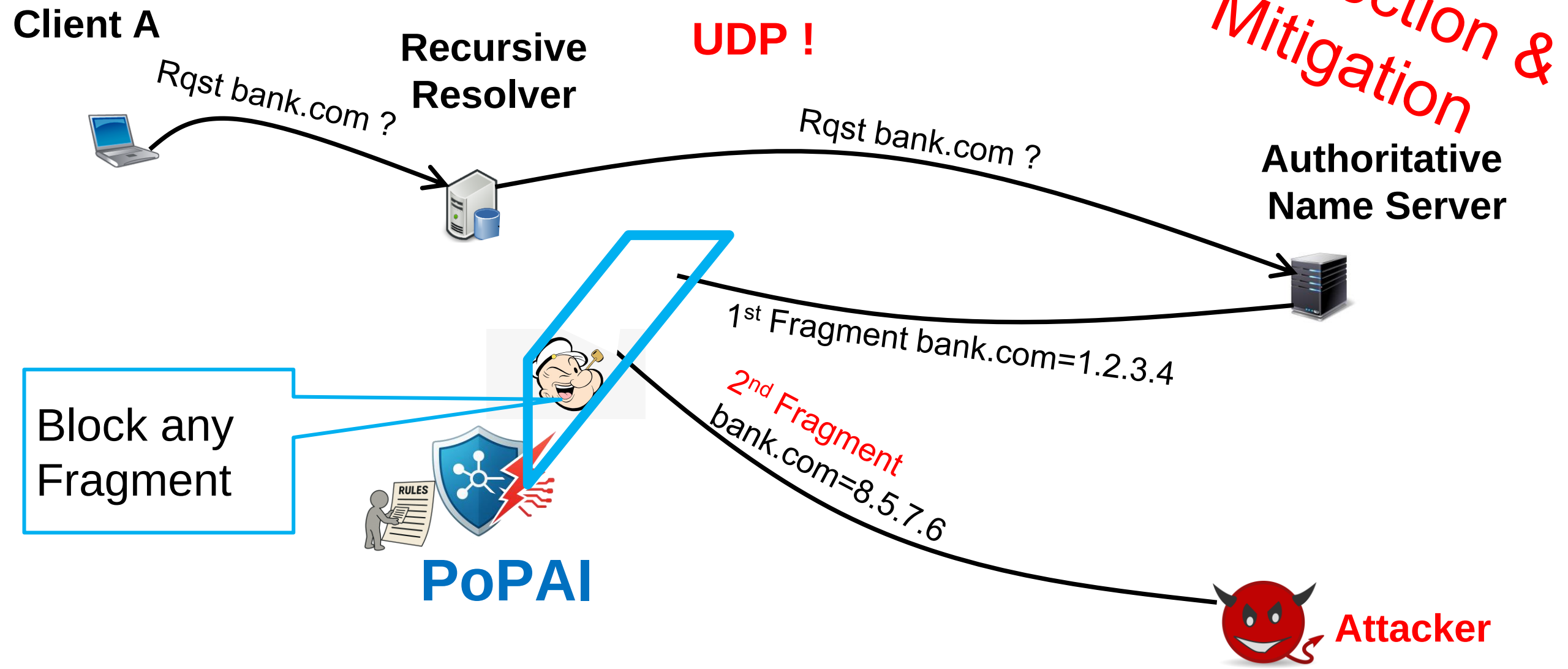
Detection & Mitigation



2nd Fragmentation

Fragmentation Poisoning Attack

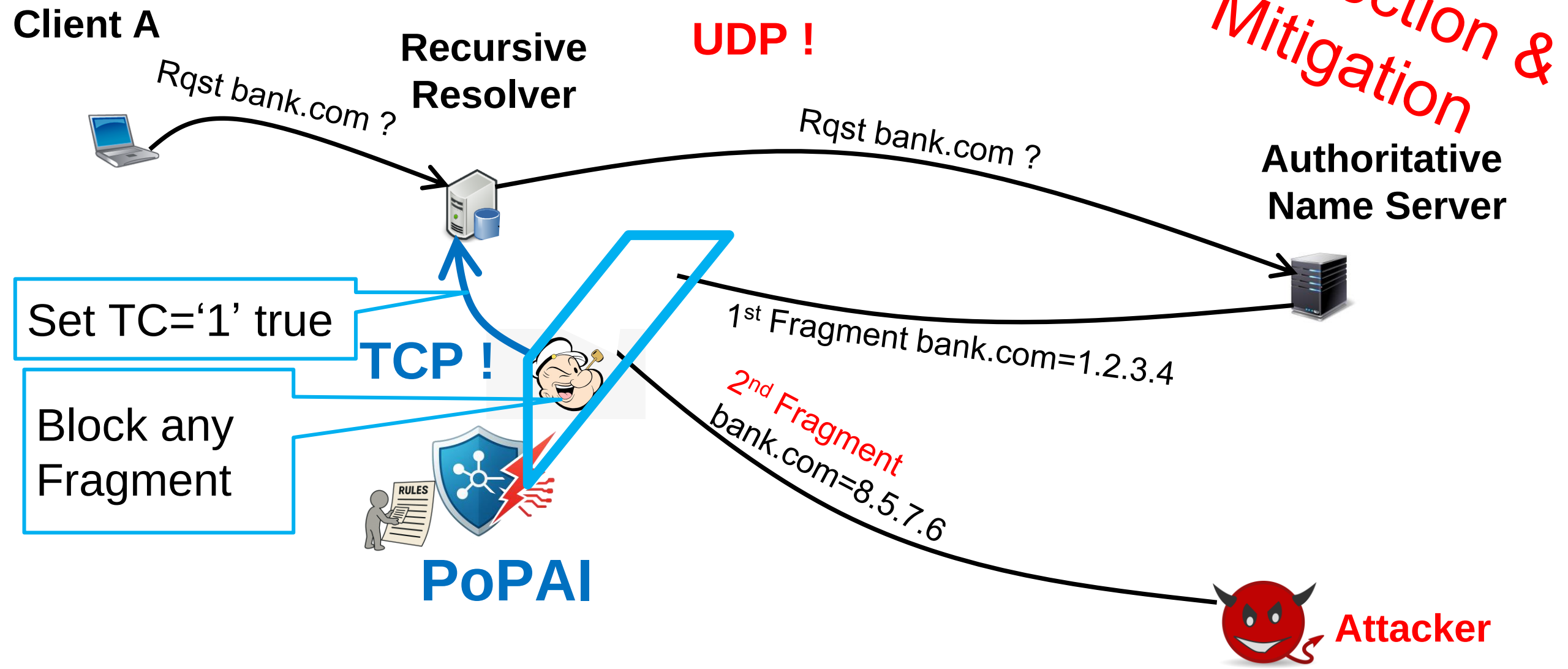
Detection & Mitigation



2nd Fragmentation

Fragmentation Poisoning Attack

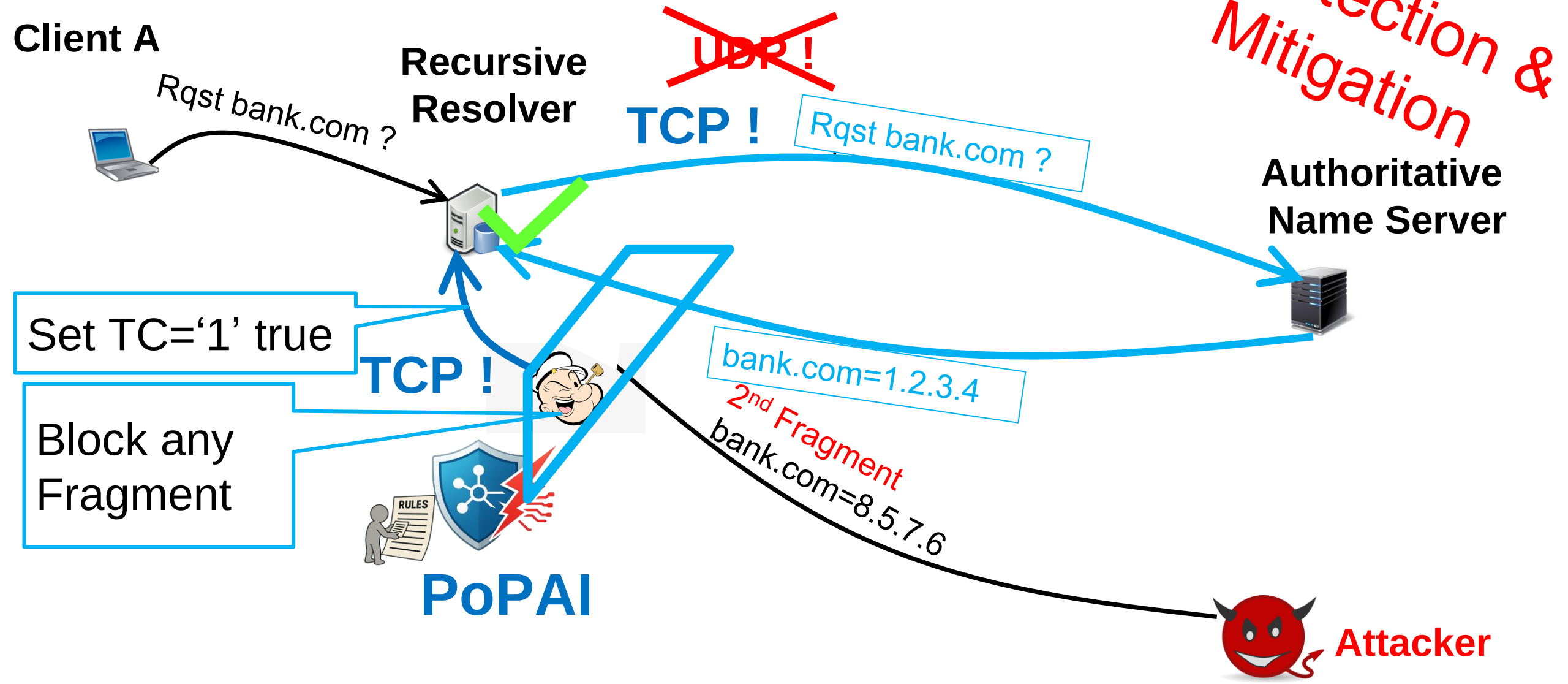
Detection & Mitigation



2nd Fragmentation

Fragmentation Poisoning Attack

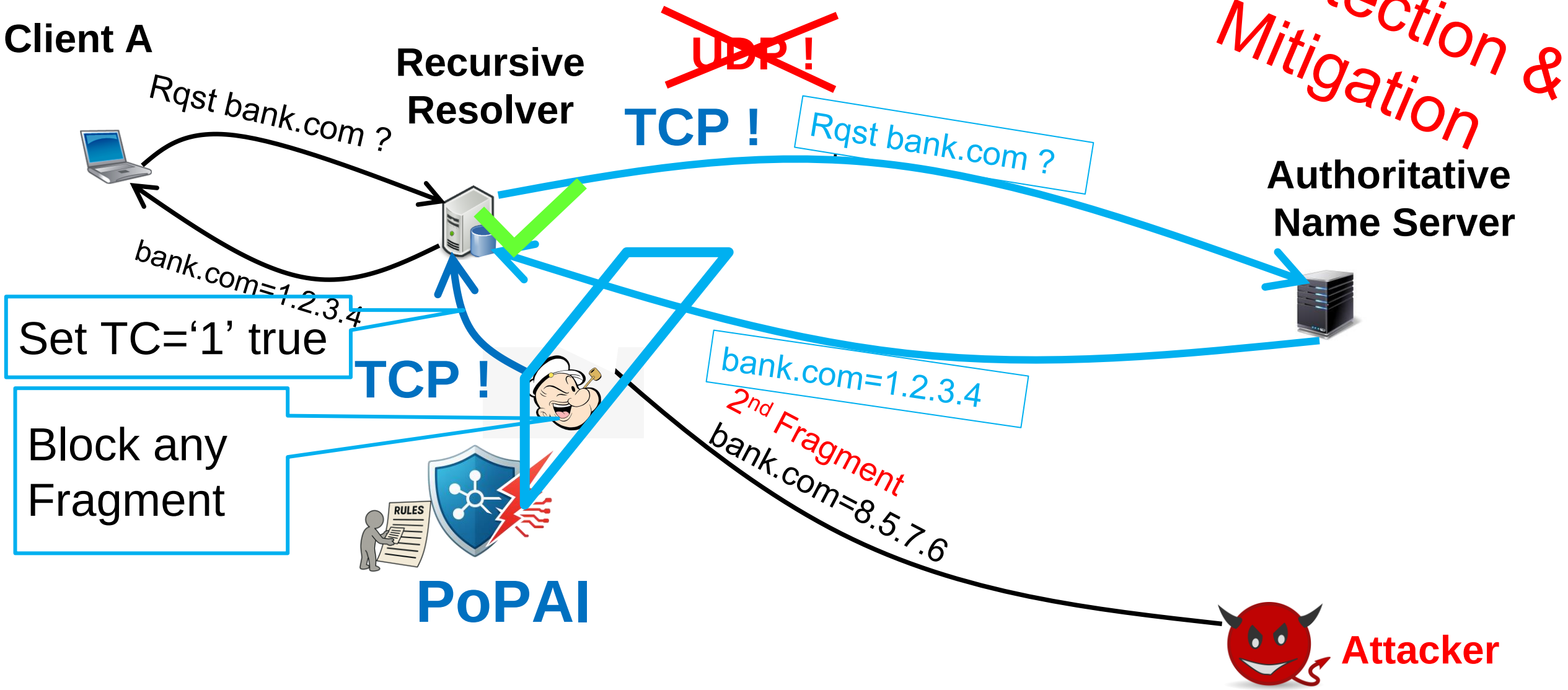
Detection & Mitigation



2nd Fragmentation

Fragmentation Poisoning Attack

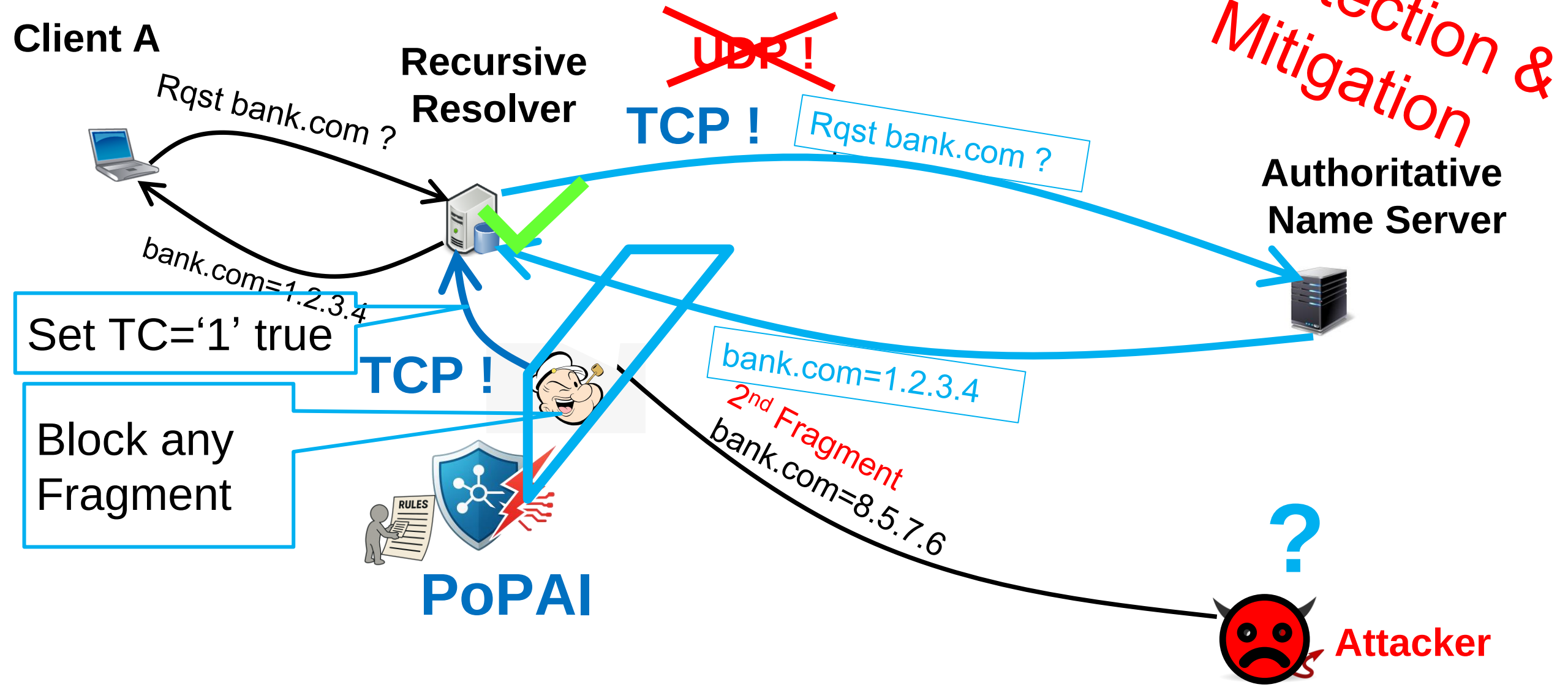
Detection & Mitigation



2nd Fragmentation

Fragmentation Poisoning Attack

Detection & Mitigation



2nd Fragmentation

PoPAI

Fragmentation attack

2nd Fragmentation

PoPAI

Fragmentation attack

- Detection: **100% false negatives (FN)** **&** **0% false positive**

2nd Fragmentation

PoPAI

Fragmentation attack

- Detection: **100% false negatives (FN)** **&** **0% false positive**
- Mitigation: **zero FN** * **&** **zero FP**

*Assuming resolvers respond \w TCP on TC bit
(all large ones. > 97% [Moura et.al. 21] [Bhowmick et.al.23])

2nd Fragmentation

PoPAI

Fragmentation attack

- Detection: 100% false negatives (FN) & 0% false positive
- Mitigation: zero FN * & zero FP

==========

- All together: zero FN

*Assuming resolvers respond \w TCP on TC bit
(all large ones. > 97% [Moura et.al. 21] [Bhowmick et.al.23])

2nd Fragmentation

PoPAI

Fragmentation attack

- Detection: 100% false negatives (FN) & 0% false positive
- Mitigation: zero FN * & zero FP

==========

- All together: zero FN & zero FP

*Assuming resolvers respond \w TCP on TC bit
(all large ones. > 97% [Moura et.al. 21] [Bhowmick et.al.23])

2nd Fragmentation

PoPAI

Fragmentation attack

- Detection: **100% false negatives (FN)** & **0% false positive**
- Mitigation: **zero FN** * & **zero FP**

==========

- All together: **zero FN** & **zero FP**

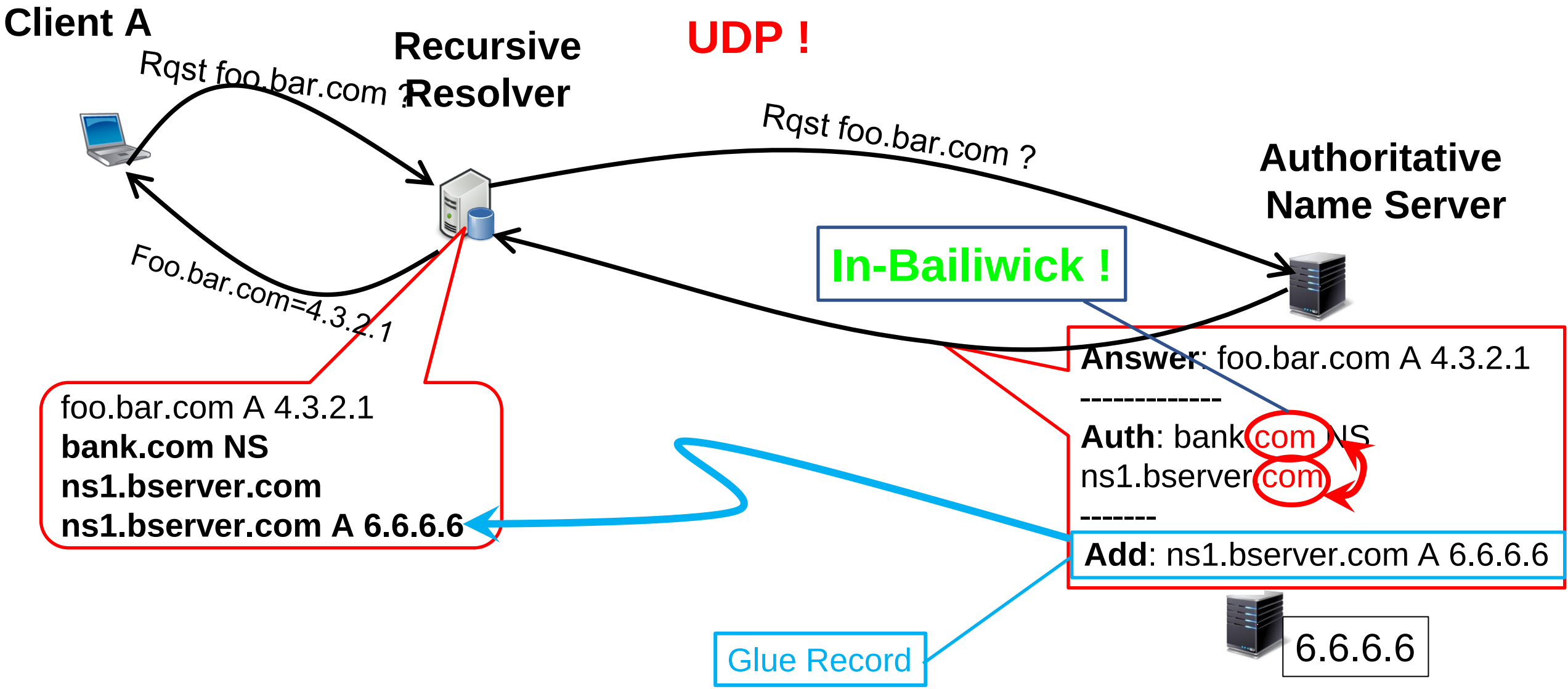
In conclusion:

➔ Blocks 100% of fragmentation attacks with **zero** false negatives!

➔ **Fast & efficient**

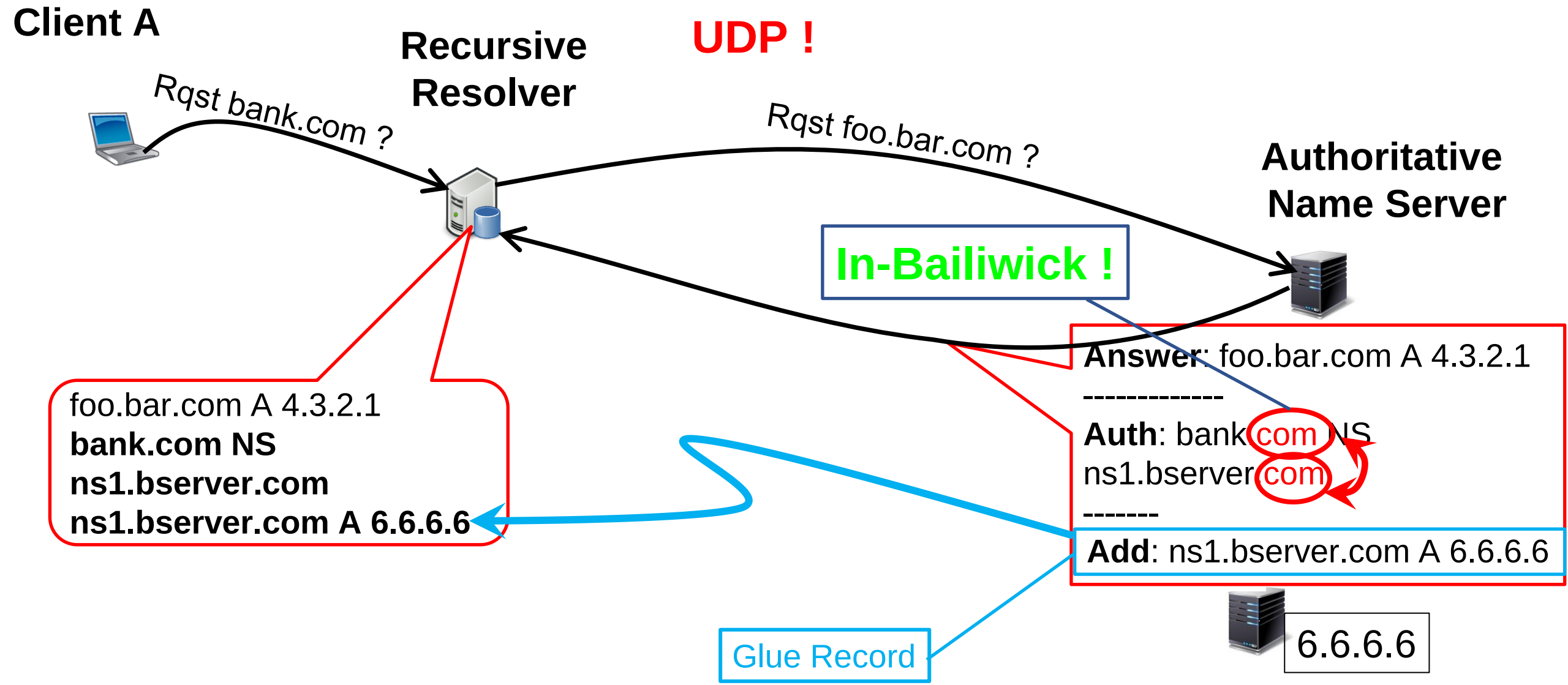
*Assuming resolvers respond \w TCP on TC bit
(all large ones. > 97% [Moura et.al. 21] [Bhowmick et.al.23])

In--Bailiwick DNS response



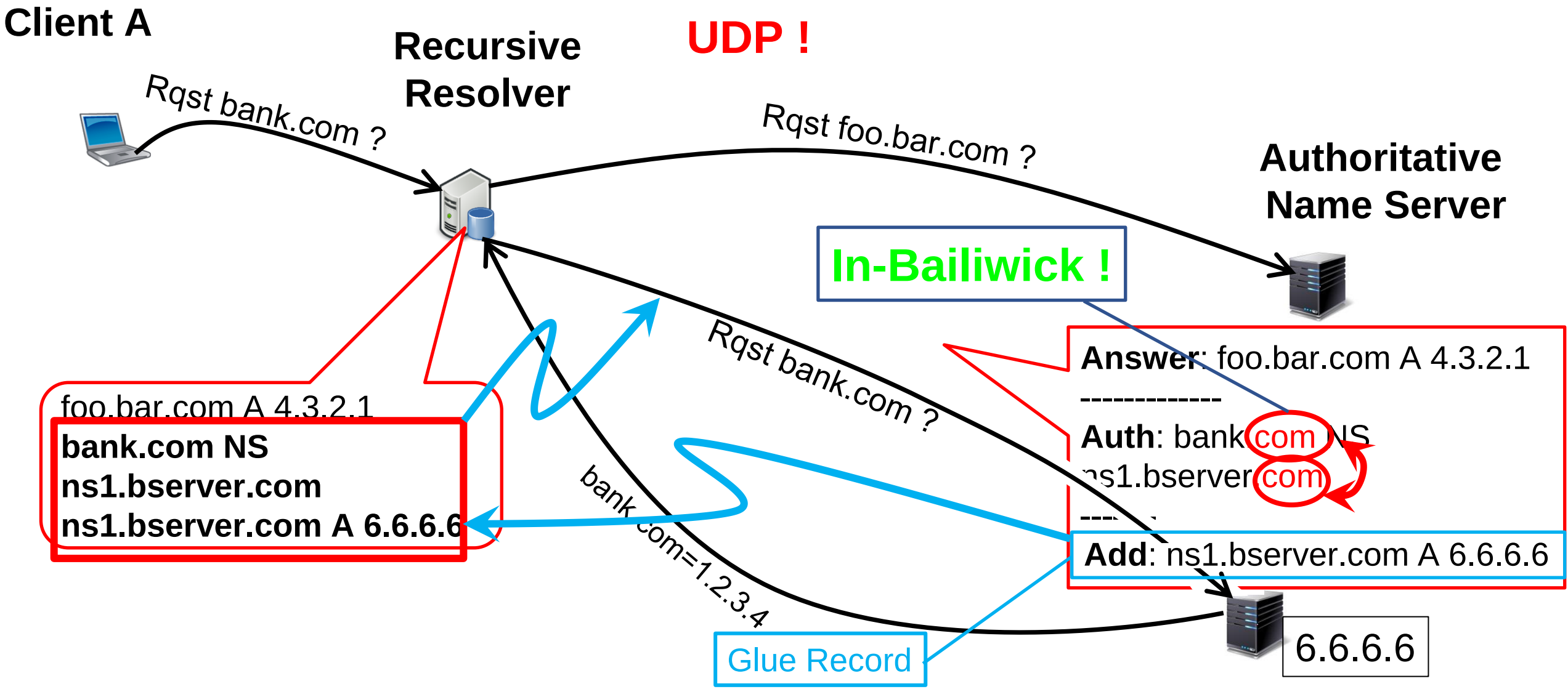
3rd Out-of-Bailiwick

In--Bailiwick DNS response



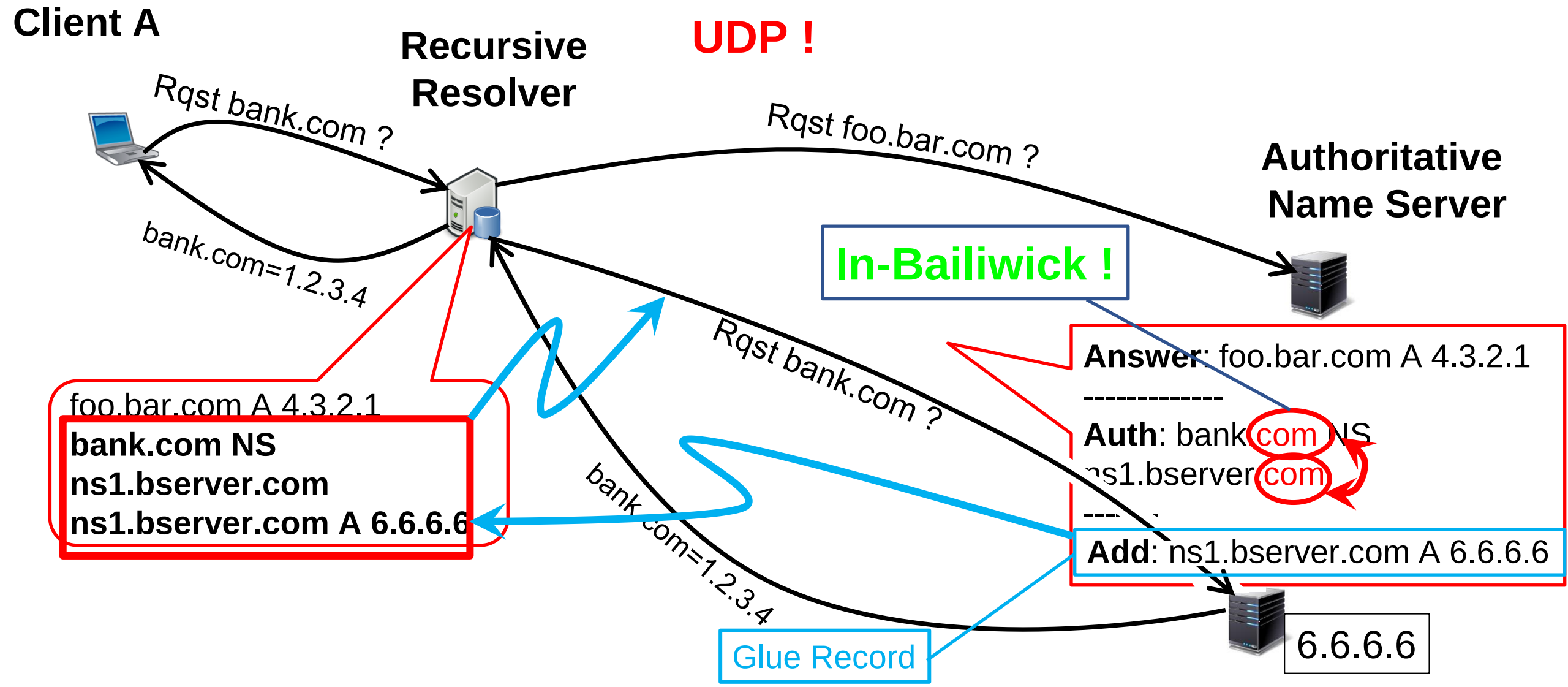
3rd Out-of-Bailiwick

In--Bailiwick DNS response



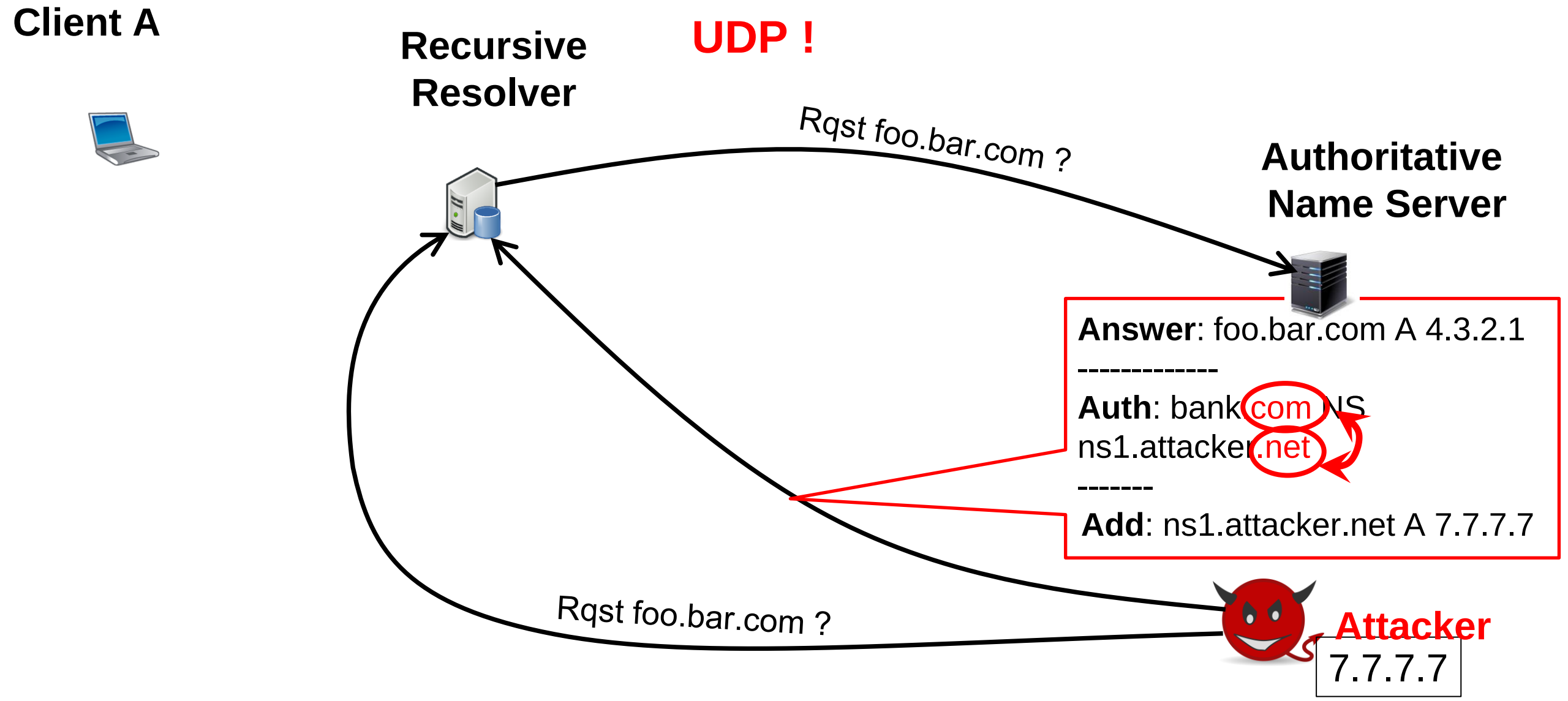
3rd Out-of-Bailiwick

In--Bailiwick DNS response



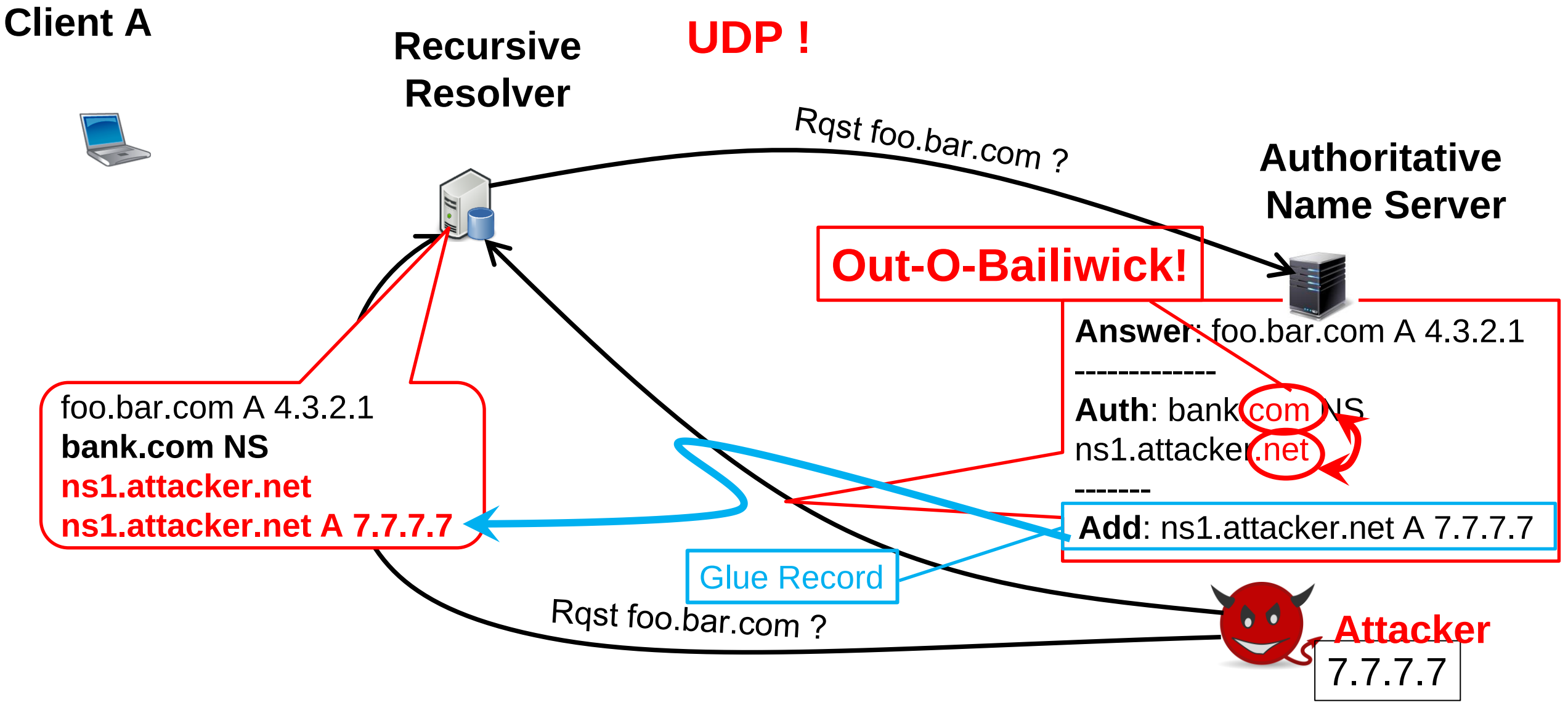
3rd Out-of-Bailiwick

Out-of-Bailiwick Poisoning Attack



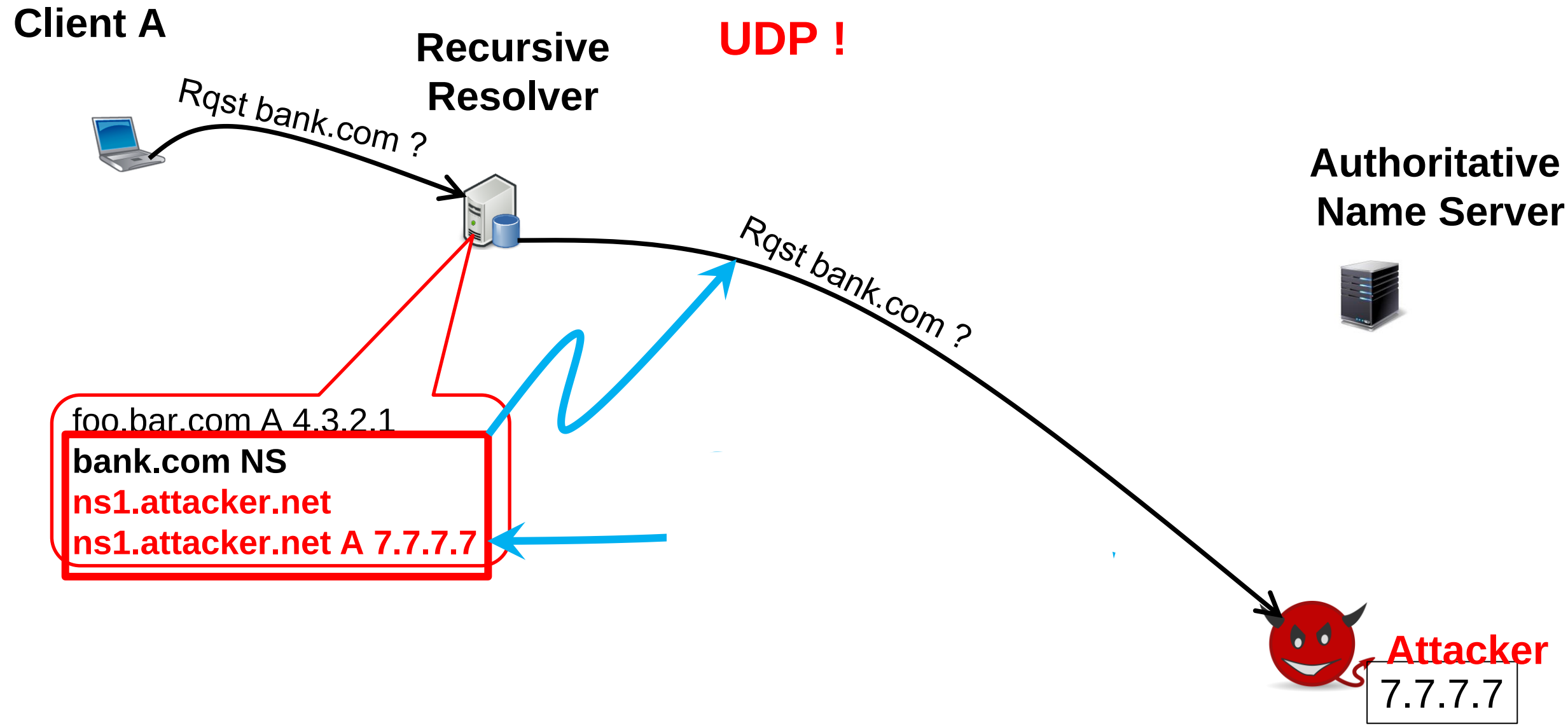
3rd Out-of-Bailiwick

Out-of-Bailiwick Poisoning Attack



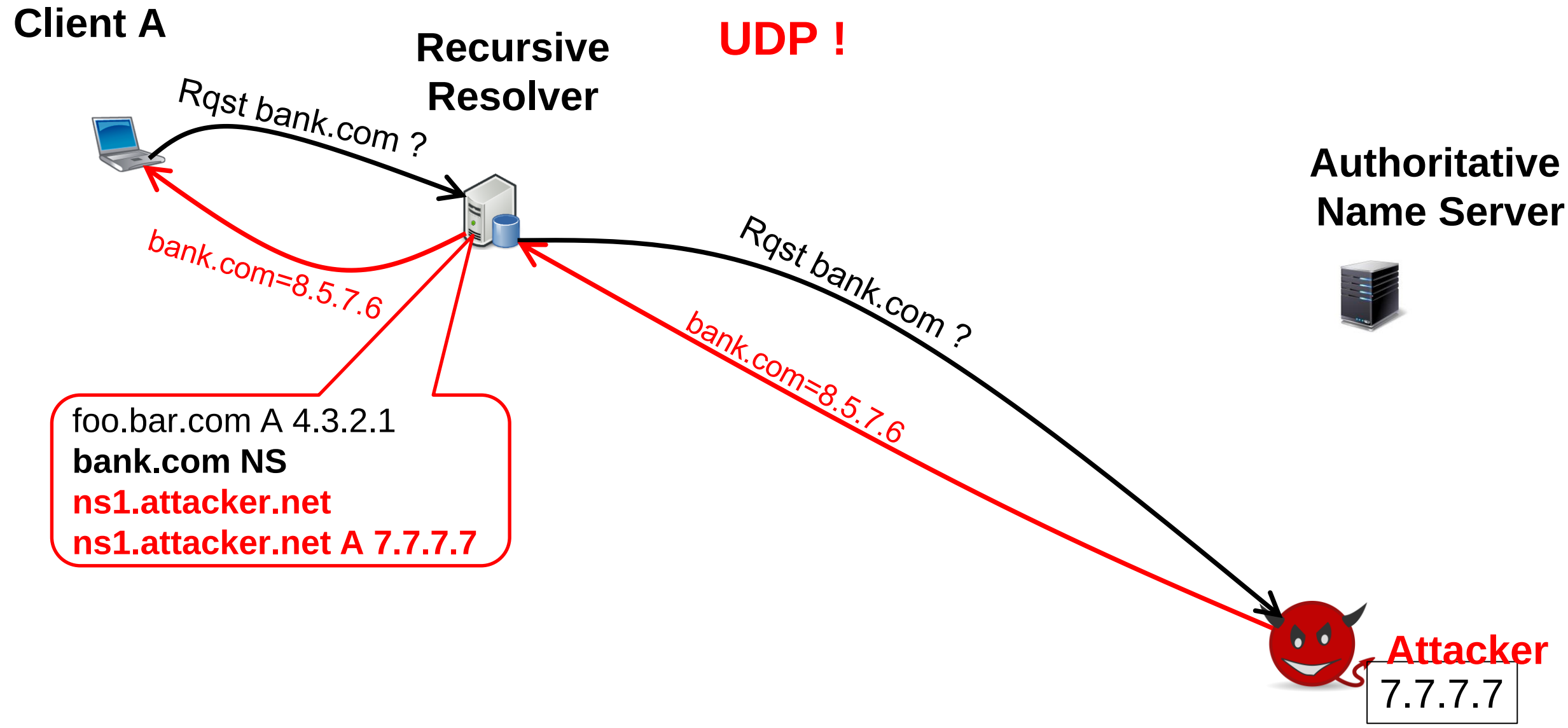
3rd Out-of-Bailiwick

Out-of-Bailiwick Poisoning Attack



3rd Out-of-Bailiwick

Out-of-Bailiwick Poisoning Attack



3rd Out-of-Bailiwick

Out-of-Bailiwick Poisoning Attack

Mitigation

Client A

Recursive Resolver

UDP !

Rqst foo.bar.com ?

Authoritative Name Server

Rqst foo.bar.com ?

Attacker

3rd Out-of-Bailiwick

Out-of-Bailiwick Poisoning Attack

Mitigation

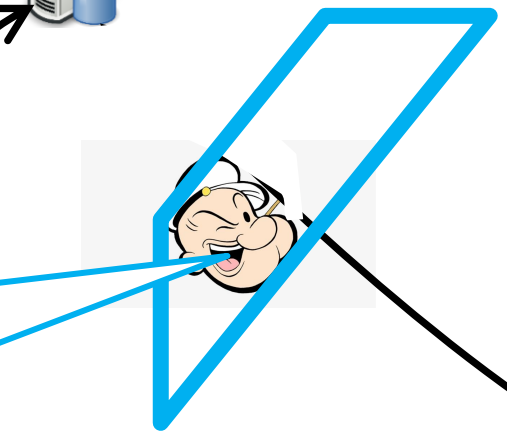
Client A

Recursive Resolver

UDP !

Rqst foo.bar.com ?

Authoritative Name Server



Drop all Out-of-Bailiwick responses

Answer: foo.bar.com A 4.3.2.1

Auth: bank.com NS ns1.attacker.net

Add: ns1.attacker.net A 7.7.7.7

Rqst foo.bar.com ?

Attacker

Detection Rule (RI3) – glue RRs outside of target domain

PoPAI Three detection rules

1st statistical

Rℓ1 >5 Catches attack after 5 packets!

- Using CMS, Minimum Memory (~4Kbit)

2nd Fragment

Rℓ2 - Fragmentation Attacks – any fragment.

3rd Out-of-Bailiwick

Rℓ3 - Out of Bailiwick Attacks – any out-of-bailiwick

= glue RRs outside the target domain

Comparison to Suricata/Snort

Suricata & Snort

Comparison to Suricata/Snort

Suricata & Snort

- Passive IDSs
- Cannot aggregate by domain name

Comparison to Suricata/Snort

Suricata & Snort

- Passive IDSs
- Cannot aggregate by domain name

POPAI detection:

- 2x – 5x faster than Suricata/Snort
- 5%–10% of packets analyzed by Suricata/Snort
- Suricata/Snort 10×–20× more False Negatives than PoPAI

Conclusions POPAI: 

- Simple Detection of DNS cache poisoning attacks (3 rules).
- Mitigation - TC Flag →TCP, Data Erasure ~0 FN, 0 FP.
- POPAI mitigates FUTURE poisoning attacks, haven’t yet seen
- POPAI mitigation works with any detection method various combinations are considered.

Thank you for listening!

- For more information
https://deepness-lab.org
yehuda.afek@gmail.com

Open Source code:
https://zenodo.org/records/15688589