



POPAL: (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 **2023**
November 6, 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](#)]

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

poisoning bugs hits Symantec

COLA

The financial sector has emerged as the impact of DNS attacks. **2023**

GlobalData | GlobalData Thematic Intelligence **November 6, 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 Prevention by Authentication & Integrity

- 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	<i>S</i>	\checkmark 2^{16}	<i>Rl1</i>
Klein, Amit [42] 2007	<i>S</i>	\checkmark >100	<i>Rl1</i>
Kaminsky, Dan [13] 2008	<i>S</i>	\checkmark $200 \cdot q$	<i>Rl1</i>
Herzberg et al. [18] 2012	<i>S</i>	\checkmark 2^{16}	<i>Rl1</i>
Herzberg et al. [18] 2012	<i>SFrag</i>	\checkmark 2^{16}	<i>Rl2</i>
Herzberg et al. [43] 2013	<i>BFrag</i>	\checkmark 1	<i>Rl2</i>
Herzberg et al. [44] 2013	<i>SFrag</i>	\checkmark $\sim 2^{11}$	<i>Rl2</i>
Herzberg et al. [45] 2013	<i>S, SFrag</i>	\checkmark 2^{16}	<i>Rl1</i>
Zheng et al. [46] 2020	<i>BFrag</i>	\checkmark 1	<i>Rl2</i>
Man et al. [47] 2020	<i>S</i>	\checkmark 2^{16}	<i>Rl1</i>
Dai et al. [48] 2021	<i>SFrag</i>	\checkmark 64	<i>Rl1</i>
Klein et al. [49] 2021	<i>S</i>	\checkmark 2^{16}	<i>Rl1</i>
Jeitner et al. [50] 2022	<i>S</i>	\checkmark 2^{16}	<i>Rl1</i>
Jeitner et al. [50] 2022	<i>S</i>	\checkmark 2^{16}	<i>Rl1</i>
Li et al. [17] 2023	<i>SOoB</i>	\checkmark 2^{16}	<i>Rl3</i>
Heftring et al. [51] 2023	<i>SFrag</i>	\checkmark 2^{16}	<i>Rl2</i>
Li et al. [22] 2024	<i>S</i>	\checkmark 2^{16}	<i>Rl1</i>

Past



Mitigated CVEs

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

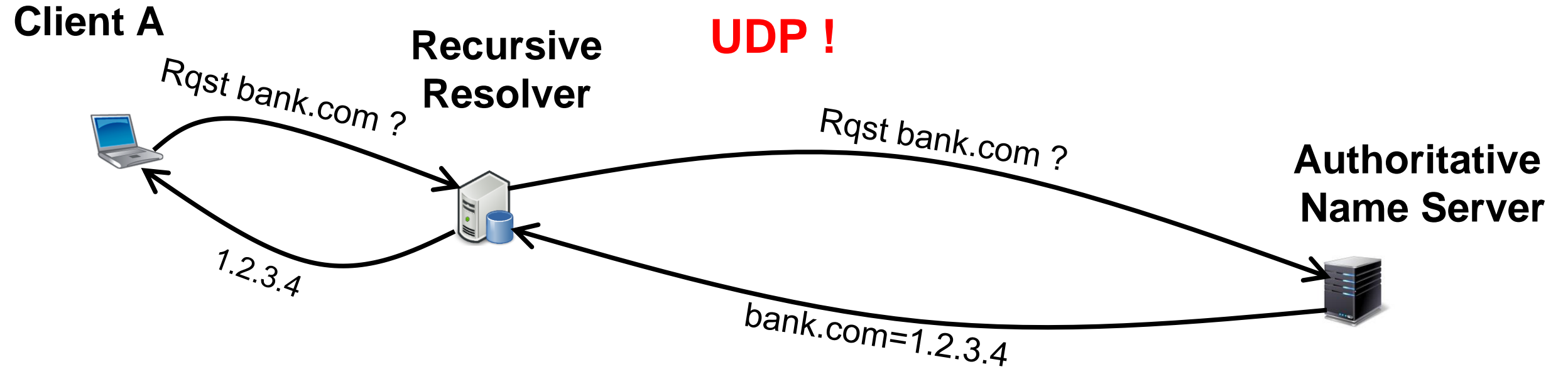
PoPAI

Past & Future

- Mythos-ready for the DNS Vulnerability Storm
- disclosure \leftrightarrow exploitation time is shrinking!



High level DNS request



1st statistical Poisoning Attack

Client A



Rqst bank.com ?

Recursive Resolver



UDP !

Rqst bank.com ?

Authoritative Name Server

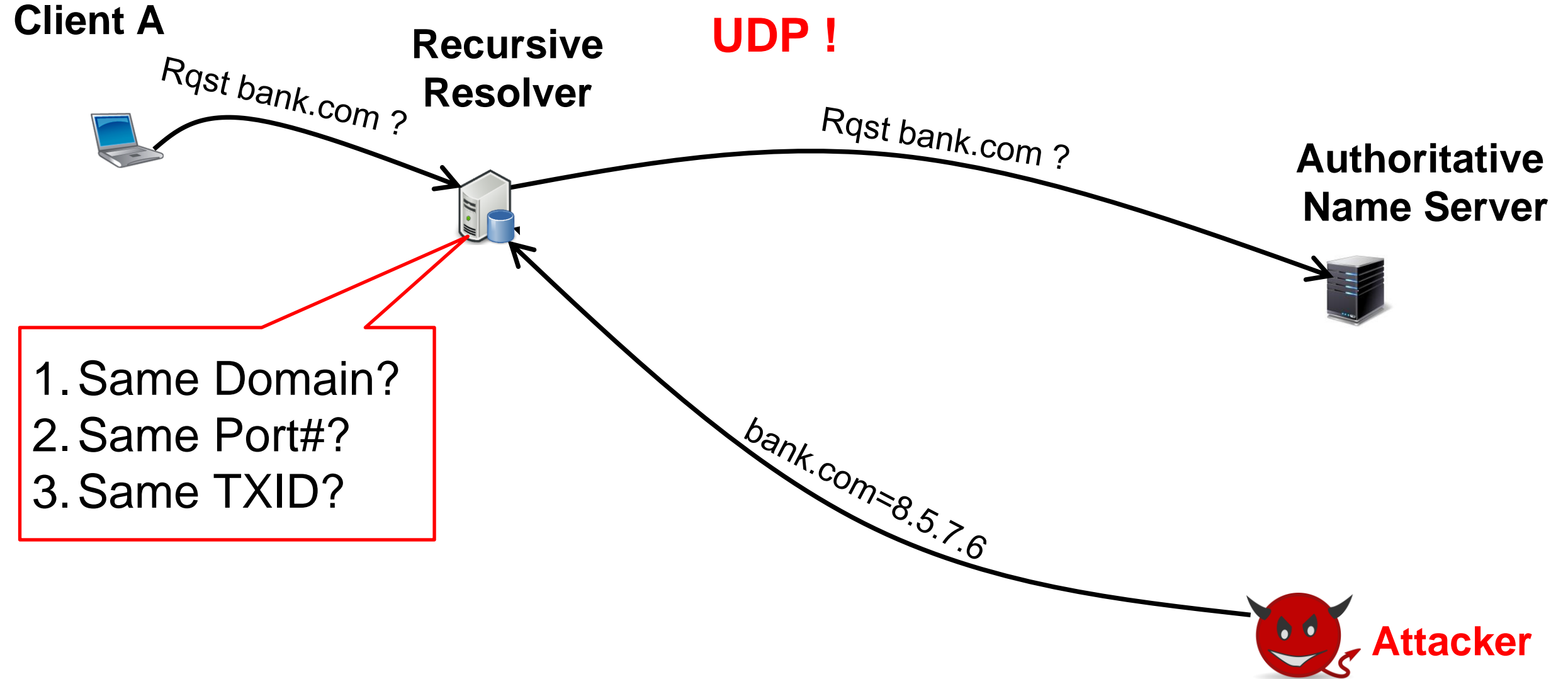


- 1. Same Domain?
- 2. Same Port#?
- 3. Same TXID?

bank.com=8.5.7.6



Attacker



1st statistical Poisoning Attack

Client A



Rqst bank.com ?

Recursive
Resolver



UDP !

Rqst bank.com ?

Authoritative
Name Server



2.3.4

bank.com=8.5.7.6



Attacker

- 1. Same Domain?
- 2. Same Port#?
- 3. Same TXID?

1st statistical Poisoning Attack

Client A



Rqst bank.com ?

Recursive Resolver



UDP !

Rqst bank.com ?

Authoritative Name Server



2.3.4

bank.com=8.5.7.6



Attacker

- 1. Same Domain?
- 2. Same Port#?
- 3. Same TXID?

1st statistical Poisoning Attack

Client A



Rqst bank.com ?

Recursive
Resolver



UDP !

Rqst bank.com ?

Authoritative
Name Server



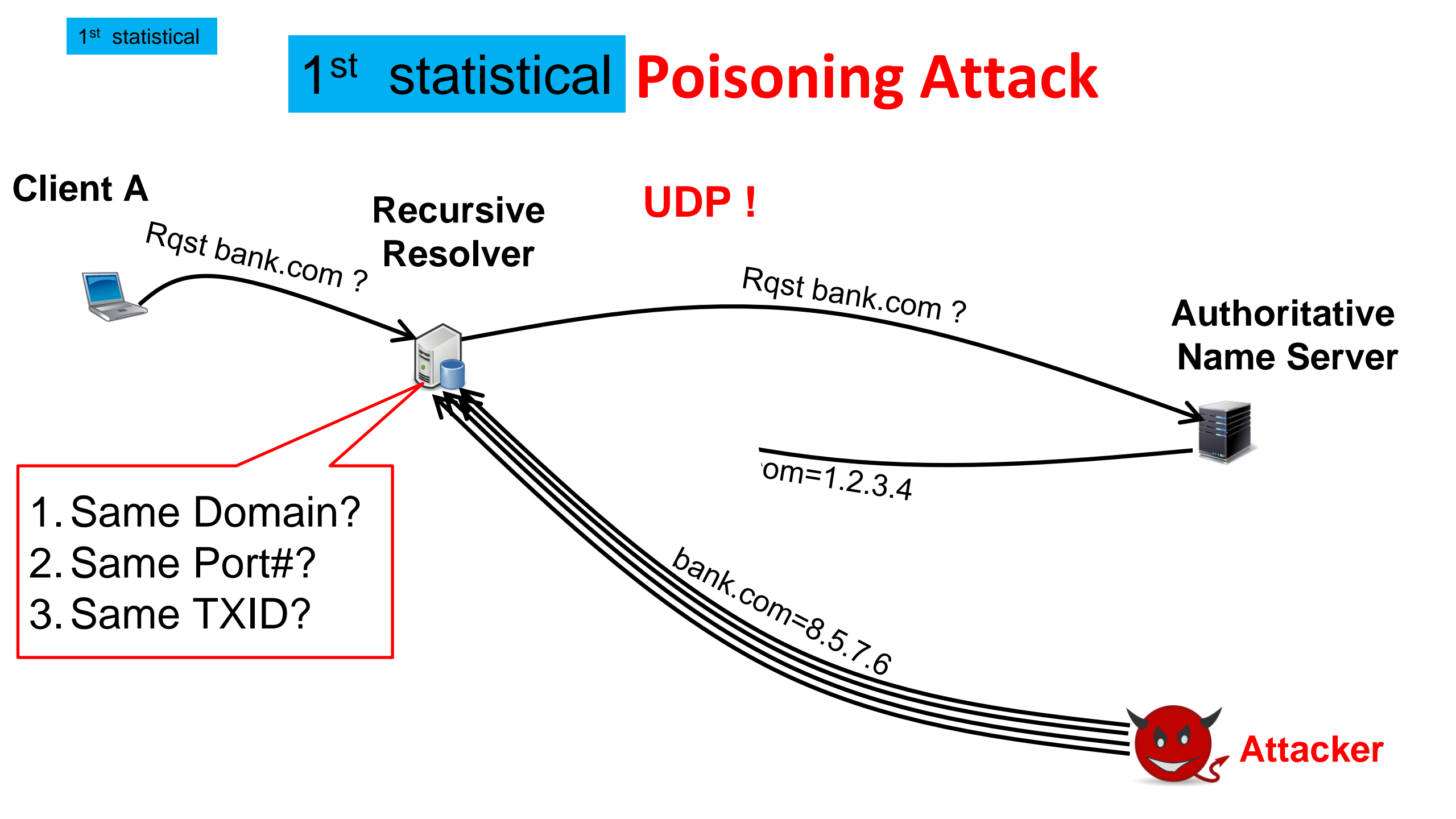
om=1.2.3.4

bank.com=8.5.7.6

- 1. Same Domain?
- 2. Same Port#?
- 3. Same TXID?



Attacker



1st statistical Poisoning Attack

UDP !

Client A

Recursive Resolver

Authoritative Name Server



Rqst bank.com ?

Rqst bank.com ?

8.5.7.6

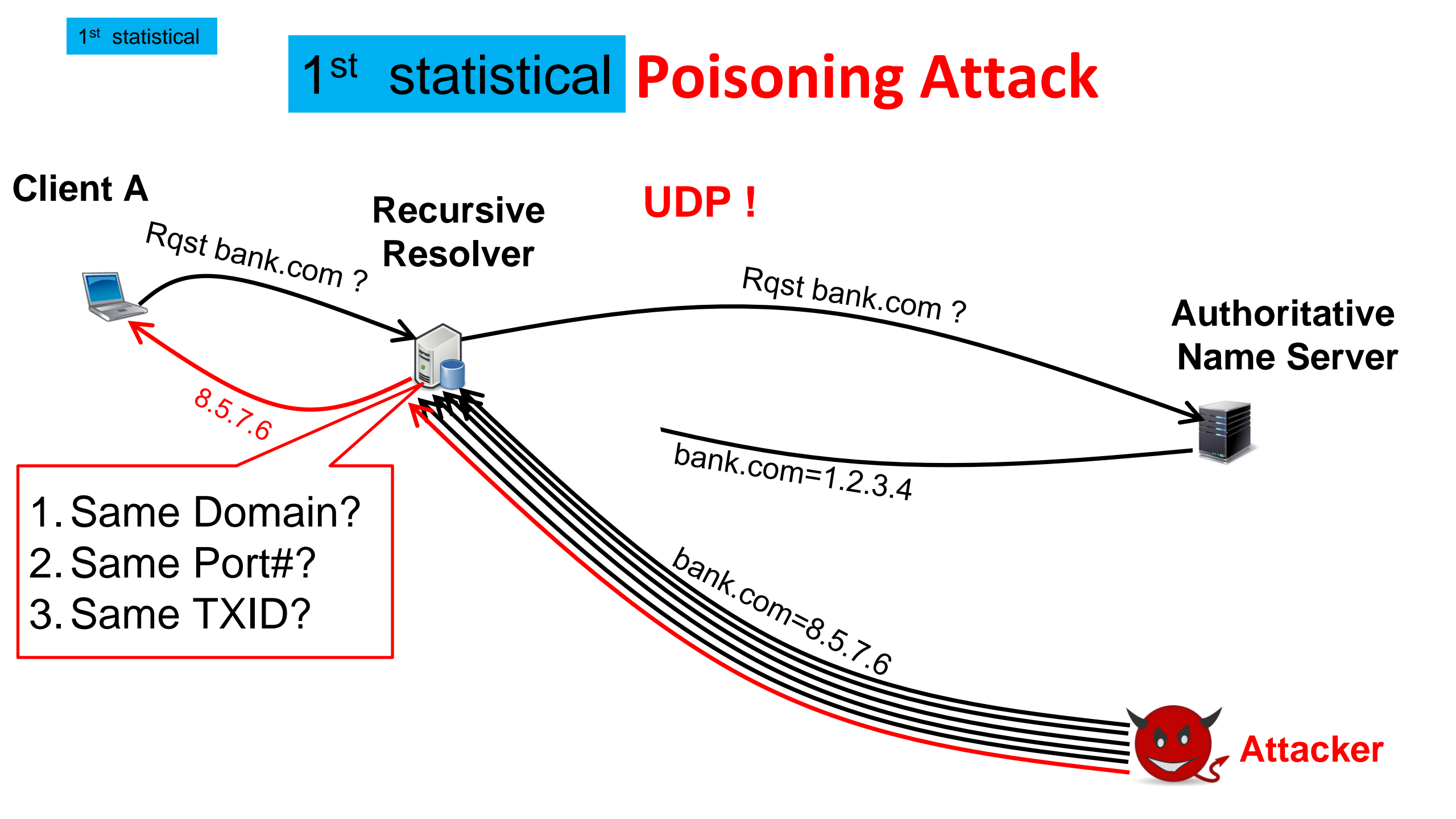
bank.com=1.2.3.4

bank.com=8.5.7.6

- 1. Same Domain?
- 2. Same Port#?
- 3. Same TXID?



Attacker



1st statistical Poisoning Attack

Client A

Recursive Resolver

UDP !

Authoritative Name Server

Rqst bank.com ?

Rqst bank.com ?

8.5.7.6

bank.com=1.2.3.4

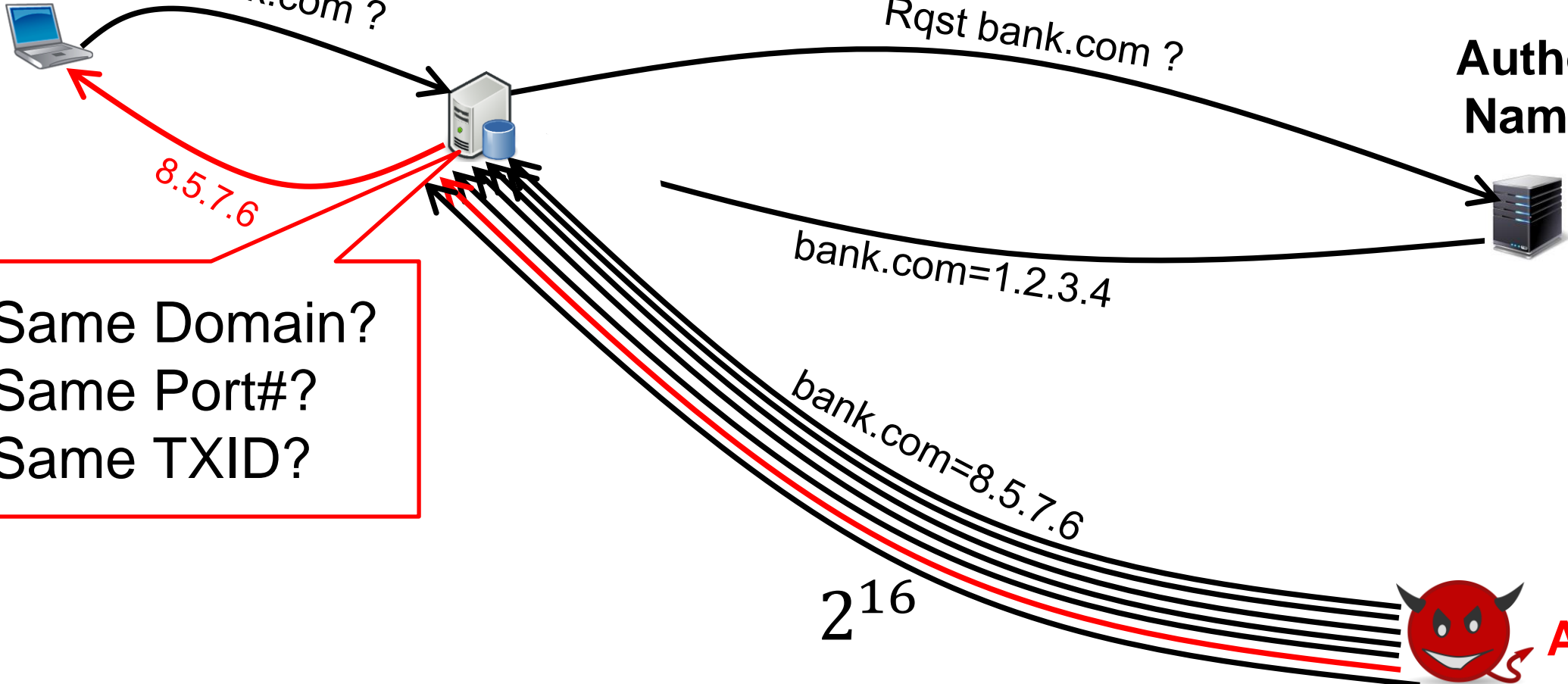
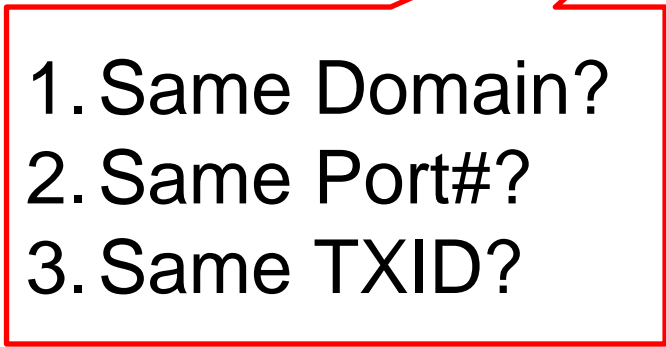
bank.com=8.5.7.6

2^{16}



Attacker

- 1. Same Domain?
- 2. Same Port#?
- 3. Same TXID?



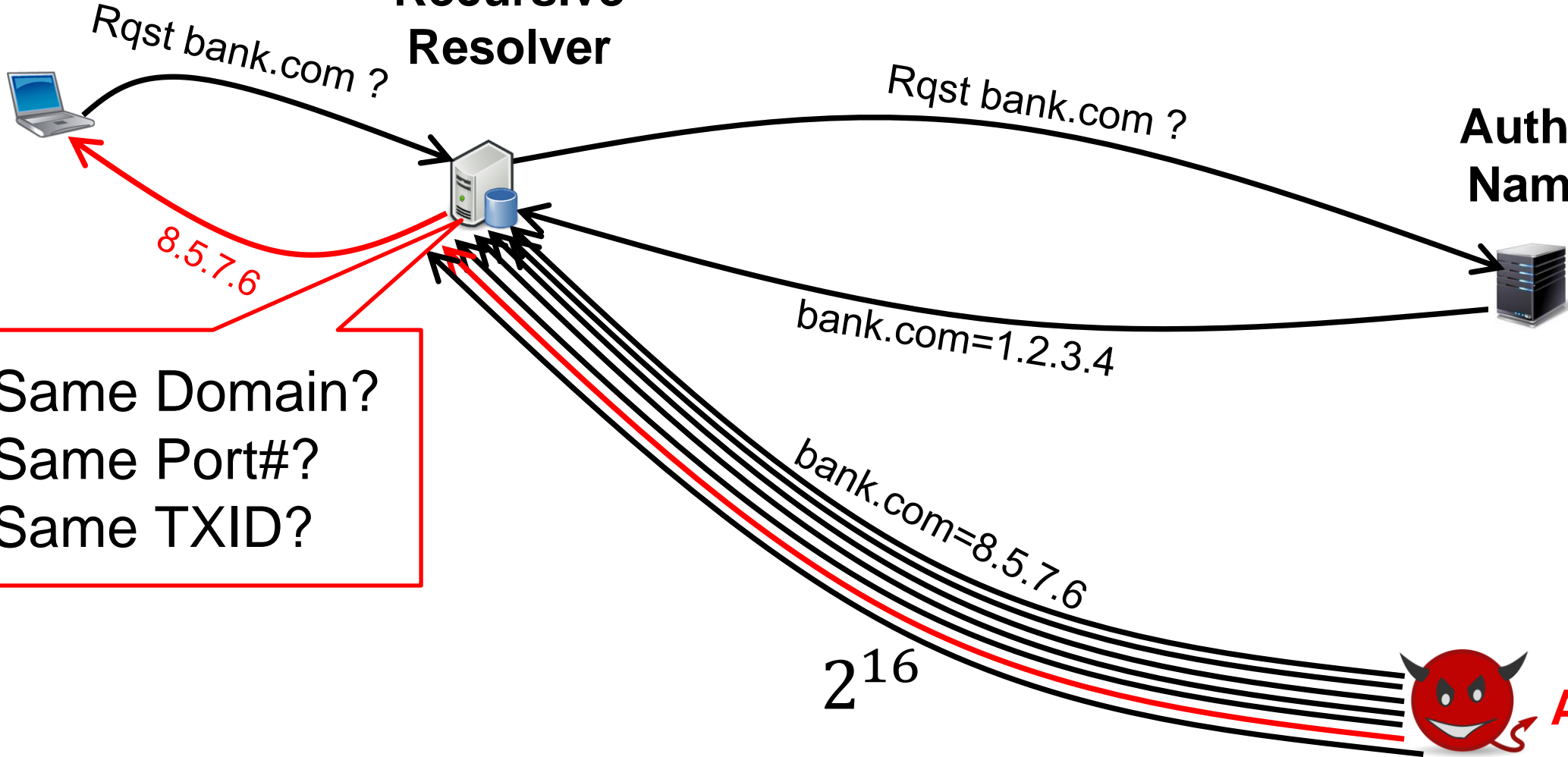
1st statistical Poisoning Attack

Client A

Recursive Resolver

UDP !

Authoritative Name Server



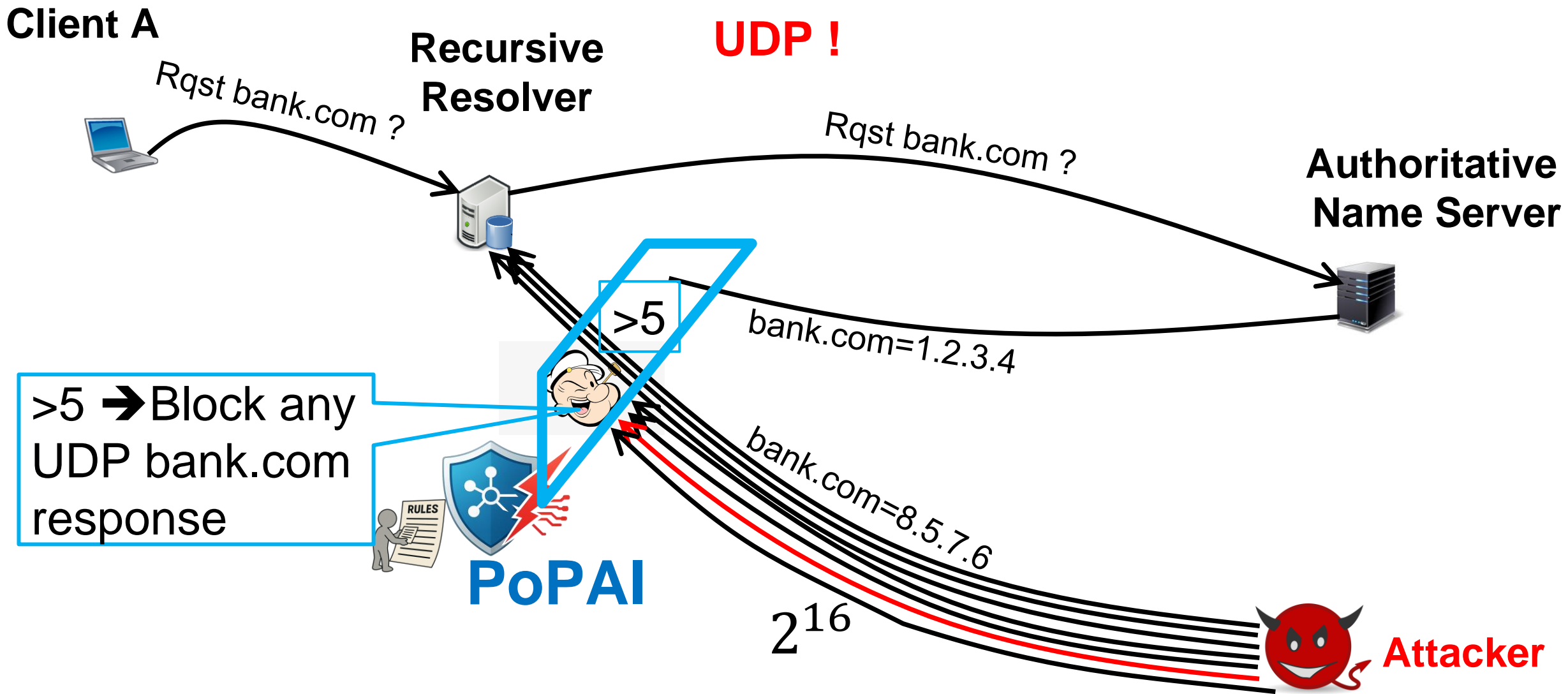
- 1. Same Domain?
- 2. Same Port#?
- 3. Same TXID?

2^{16}



Attacker

PoPAI Detection



UDP !

>5 → Block any UDP bank.com response

PoPAI

Attacker

PoPAI Mitigation

Client A



Rqst bank.com ?

Recursive Resolver



UDP !

Rqst bank.com ?

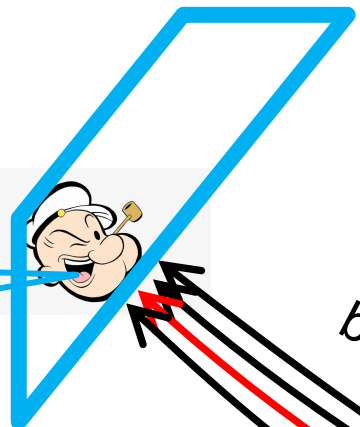
Authoritative Name Server



>5 → Block any UDP bank.com response



PoPAI

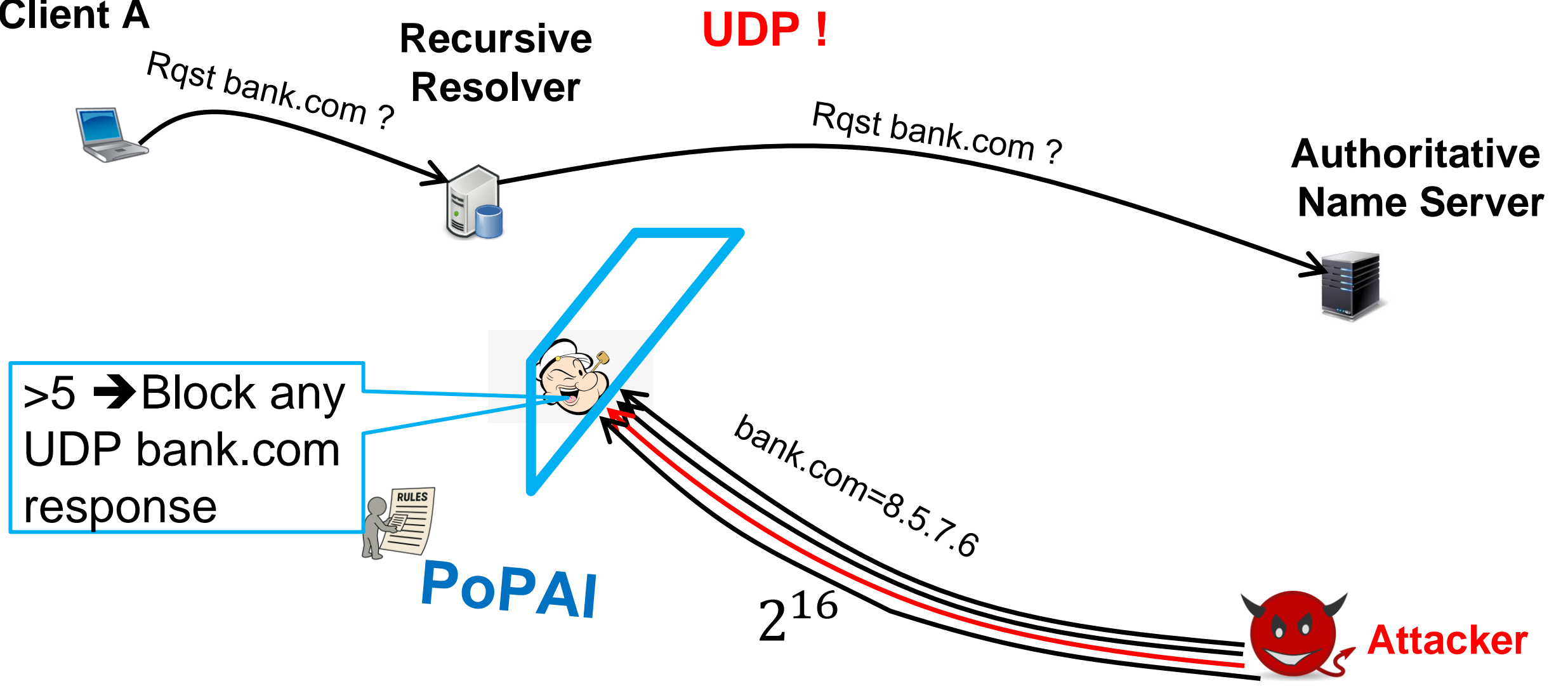


bank.com=8.5.7.6

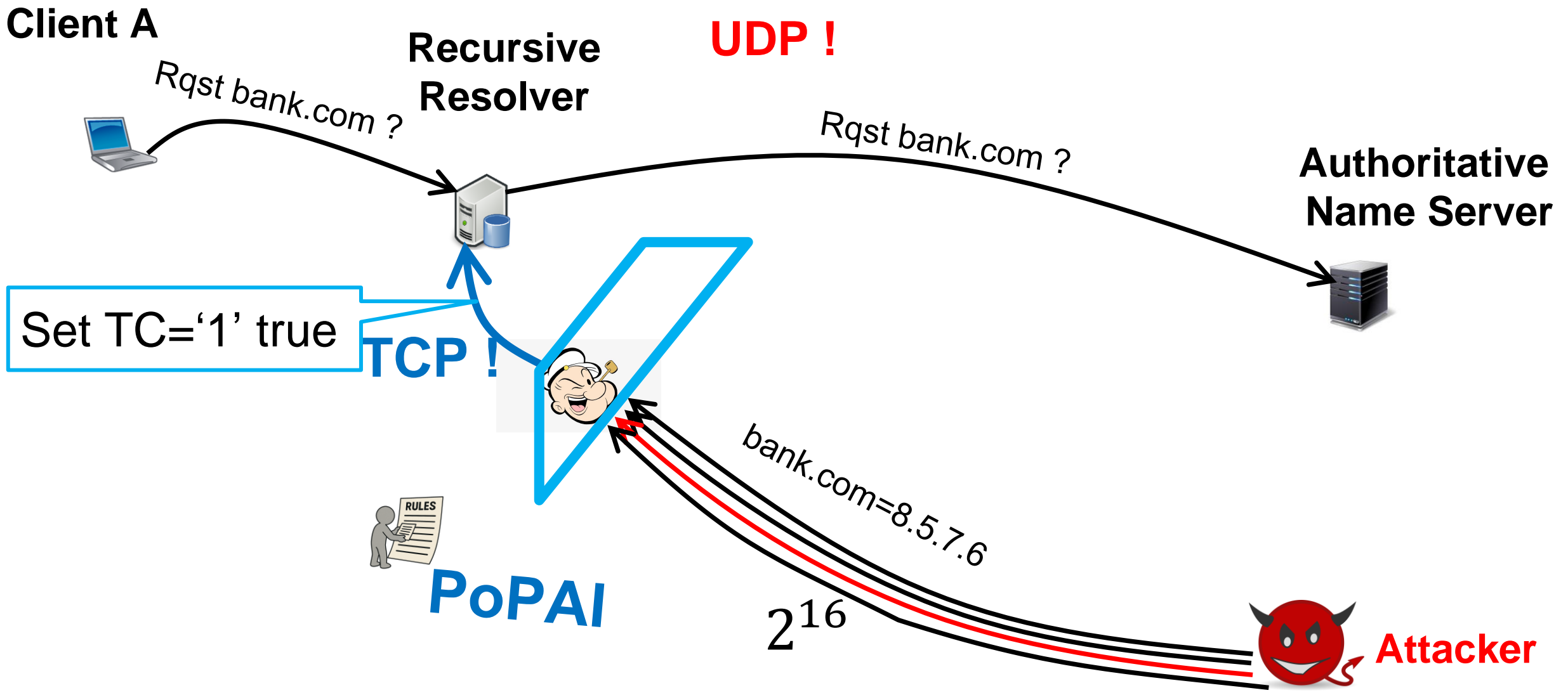
2¹⁶



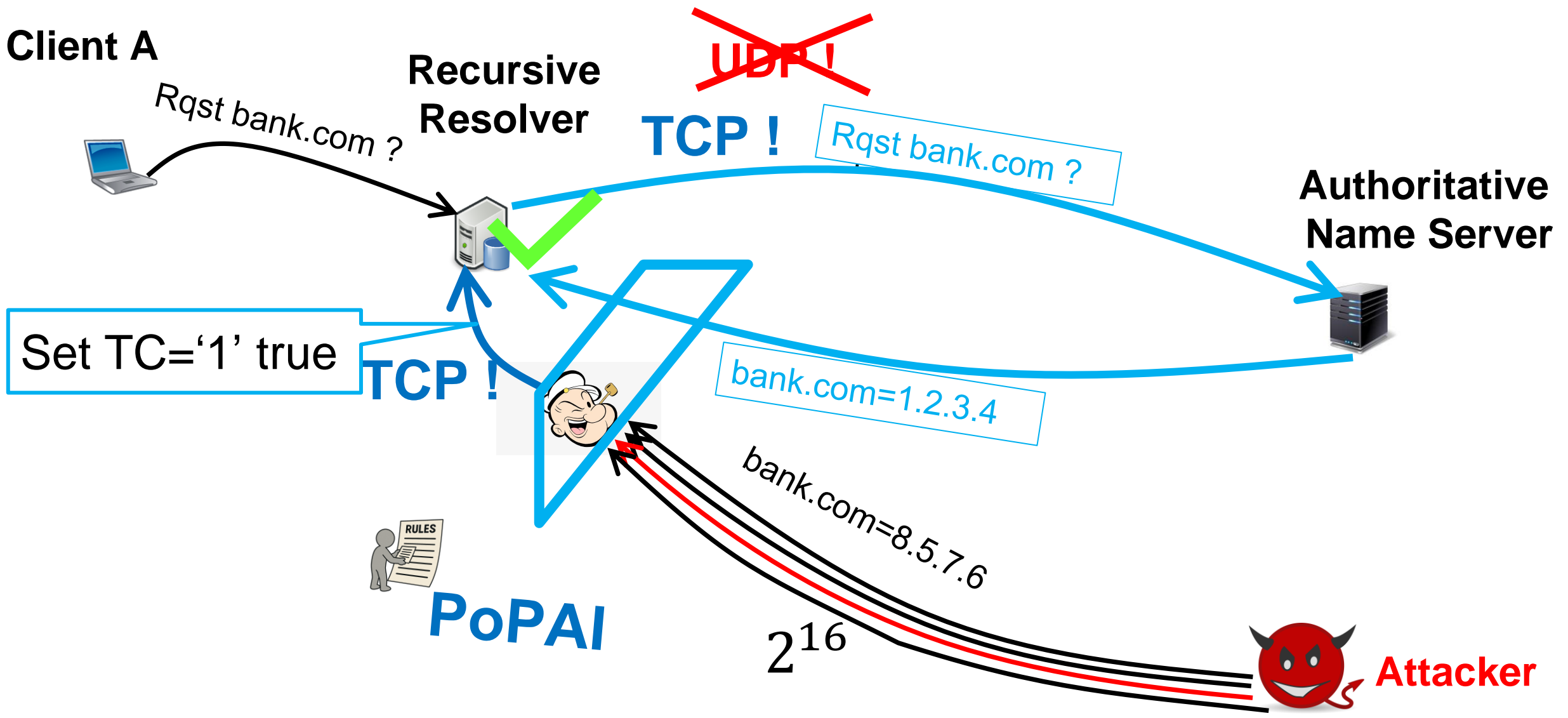
Attacker



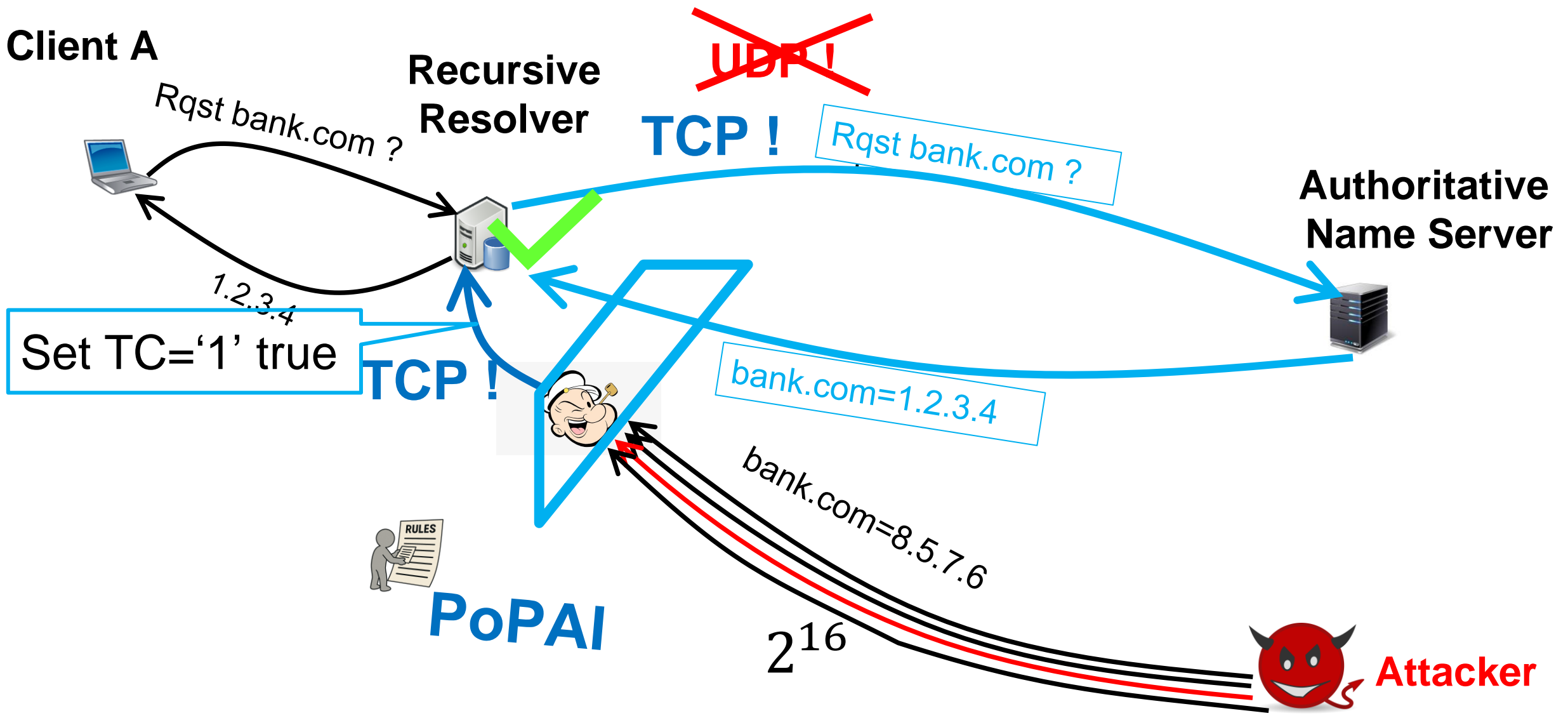
PoPAI Mitigation



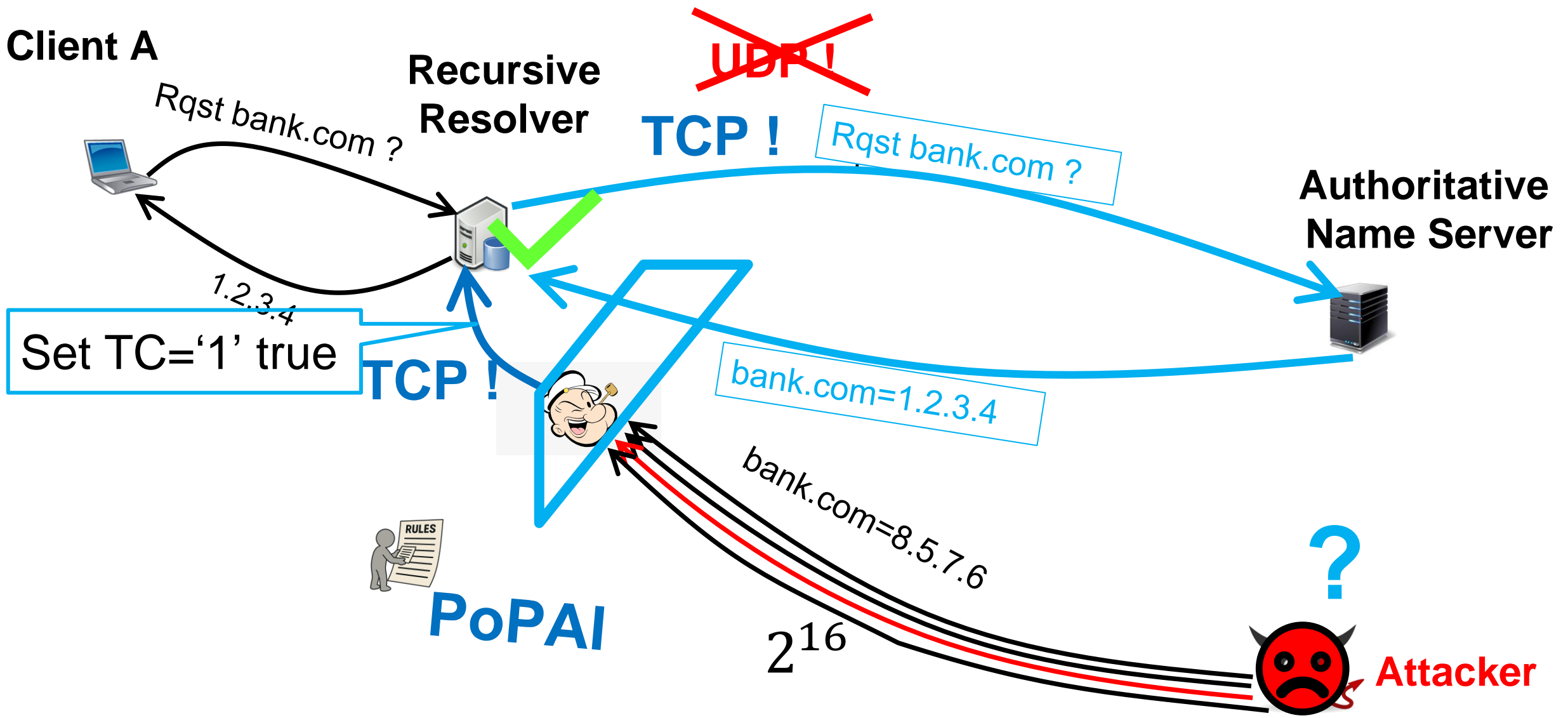
PoPAI Mitigation



PoPAI Mitigation



PoPAI Mitigation



Client A

Recursive Resolver

~~UDP !~~

TCP !

Rqst bank.com ?

Authoritative Name Server

Set TC='1' true

TCP !

bank.com=1.2.3.4



bank.com=8.5.7.6



PoPAI

2^{16}



Attacker

?

PoPAI

Statistical attacks

PoPAI

Statistical attacks

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

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])

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])

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])

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])

DNS Fragmentation Response

Fragmentation

Client A



Recursive Resolver



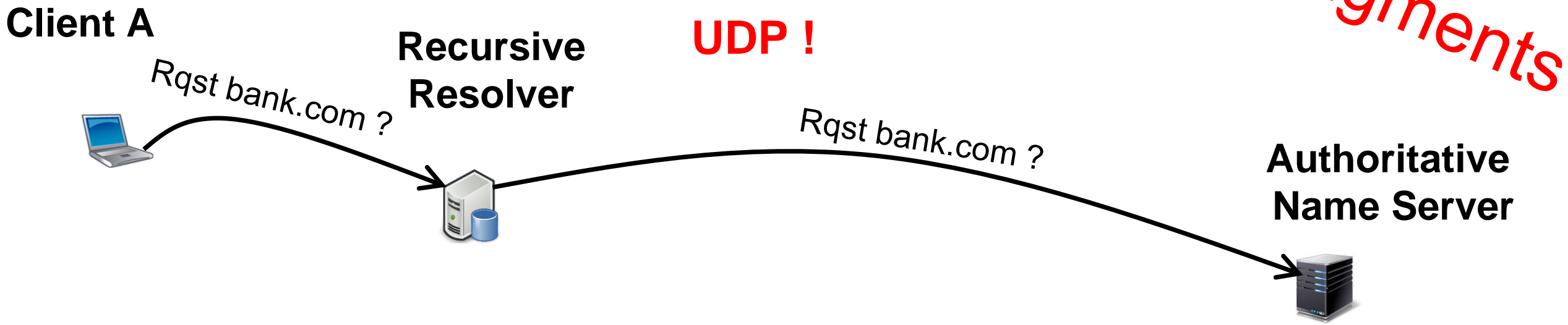
UDP !

Authoritative Name Server



Rqst bank.com ?

Rqst bank.com ?



DNS Fragmentation Response

Fragments

UDP !

Client A



Recursive Resolver



Authoritative Name Server

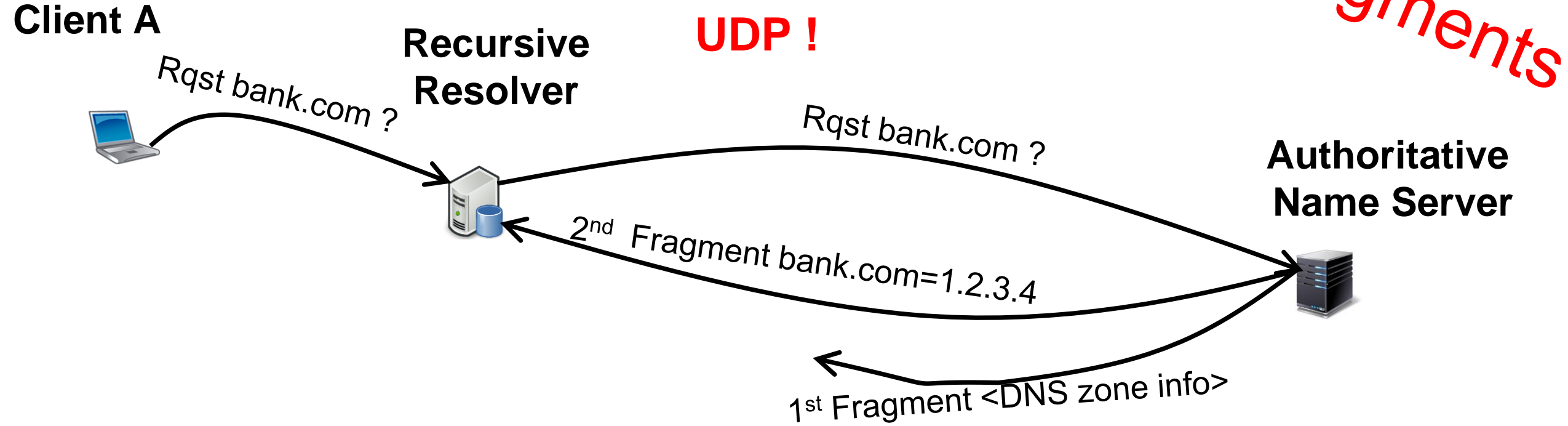


Rqst bank.com ?

Rqst bank.com ?

2nd Fragment bank.com=1.2.3.4

1st Fragment <DNS zone info>



DNS Fragmentation Response

Fragments

UDP !

Client A



Rqst bank.com ?

Recursive Resolver



UDP !

Rqst bank.com ?

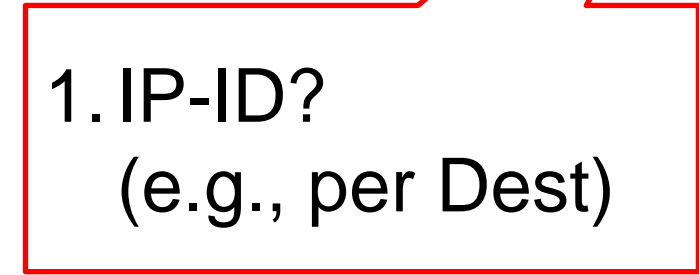
Authoritative Name Server



2nd Fragment bank.com=1.2.3.4

1st Fragment <DNS zone info>

1. IP-ID?
(e.g., per Dest)



2nd Fragmentation

DNS Fragmentation Response

Fragmentation

UDP !

Client A

Recursive Resolver

Authoritative Name Server



Rqst bank.com ?

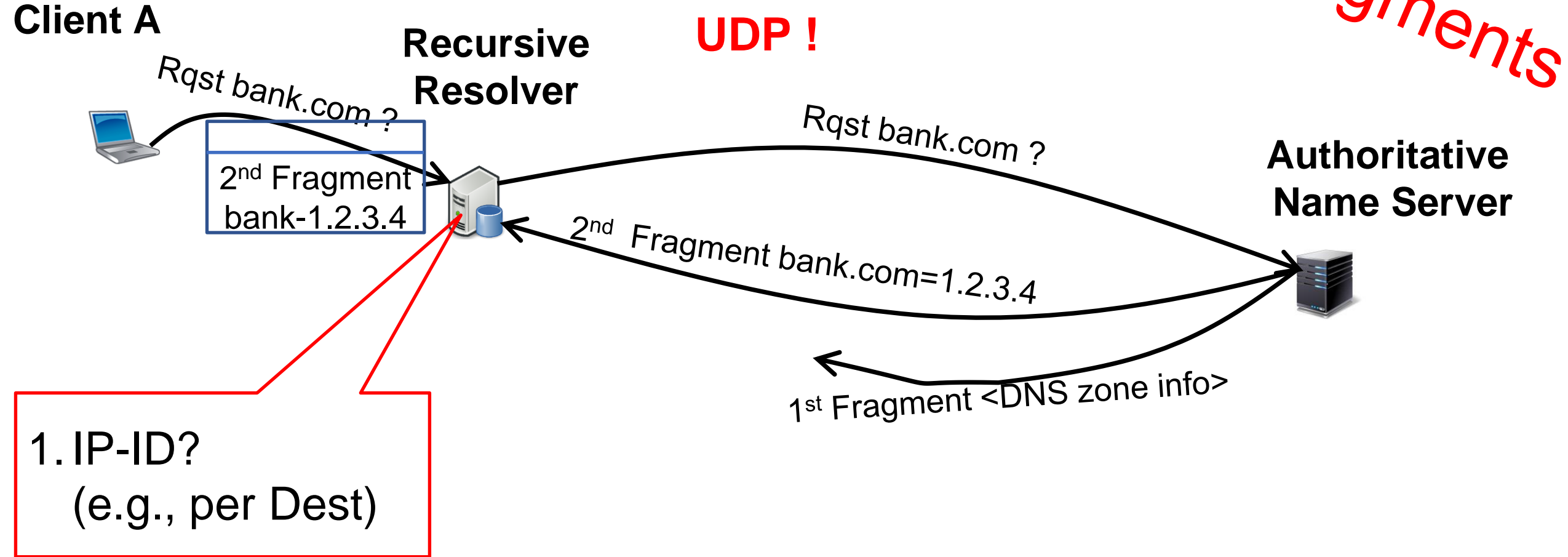
2nd Fragment
bank-1.2.3.4

Rqst bank.com ?

2nd Fragment bank.com=1.2.3.4

1st Fragment <DNS zone info>

1. IP-ID?
(e.g., per Dest)



DNS Fragmentation Response

Fragments

UDP !

Client A

Recursive Resolver

Authoritative Name Server



Rqst bank.com ?

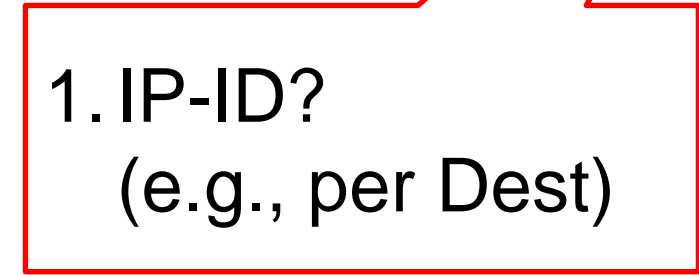
1st Frag
2nd Fragment
bank-1.2.3.4

Rqst bank.com ?

2nd Fragment bank.com=1.2.3.4

1st Fragment <DNS zone info>

1. IP-ID?
(e.g., per Dest)



DNS Fragmentation Response

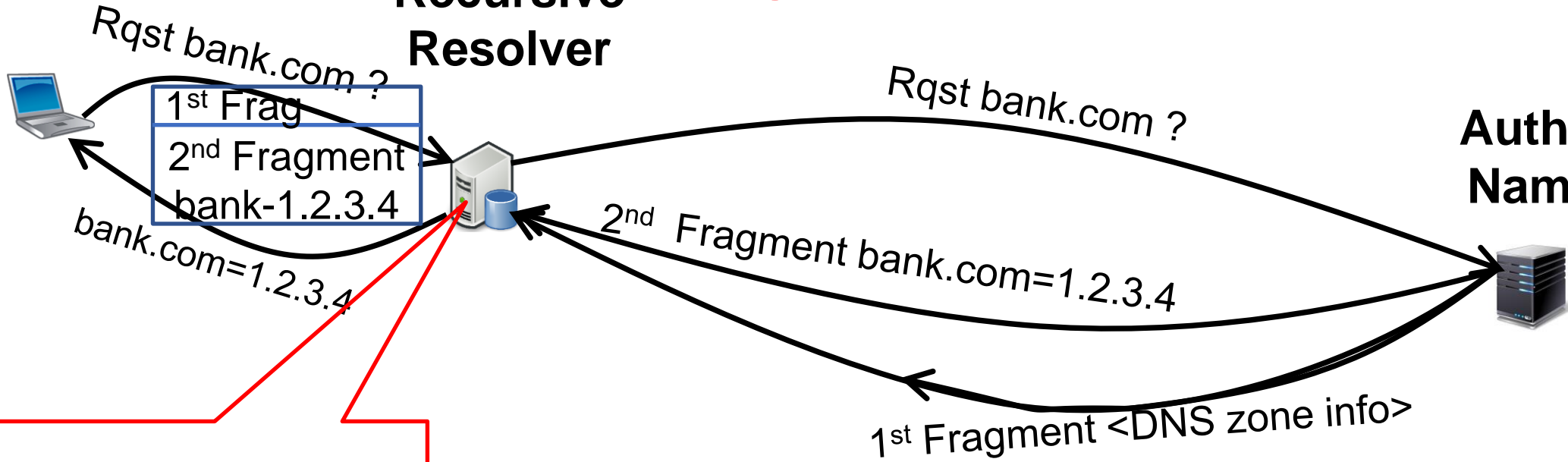
Fragments

UDP !

Client A

Recursive Resolver

Authoritative Name Server



1. IP-ID?
(e.g., per Dest)

Fragmentation Poisoning Attack

Client A



Rqst bank.com ?

**Recursive
Resolver**



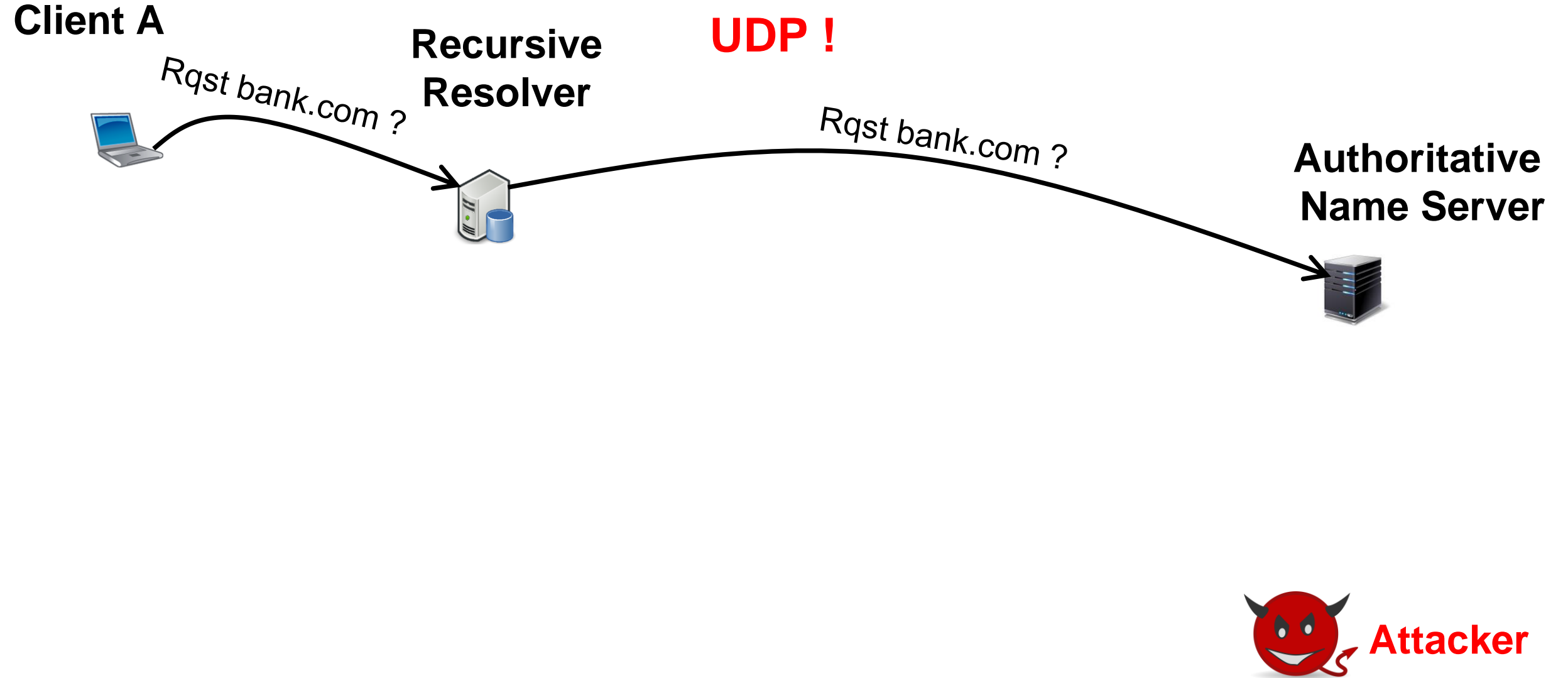
UDP !

Rqst bank.com ?

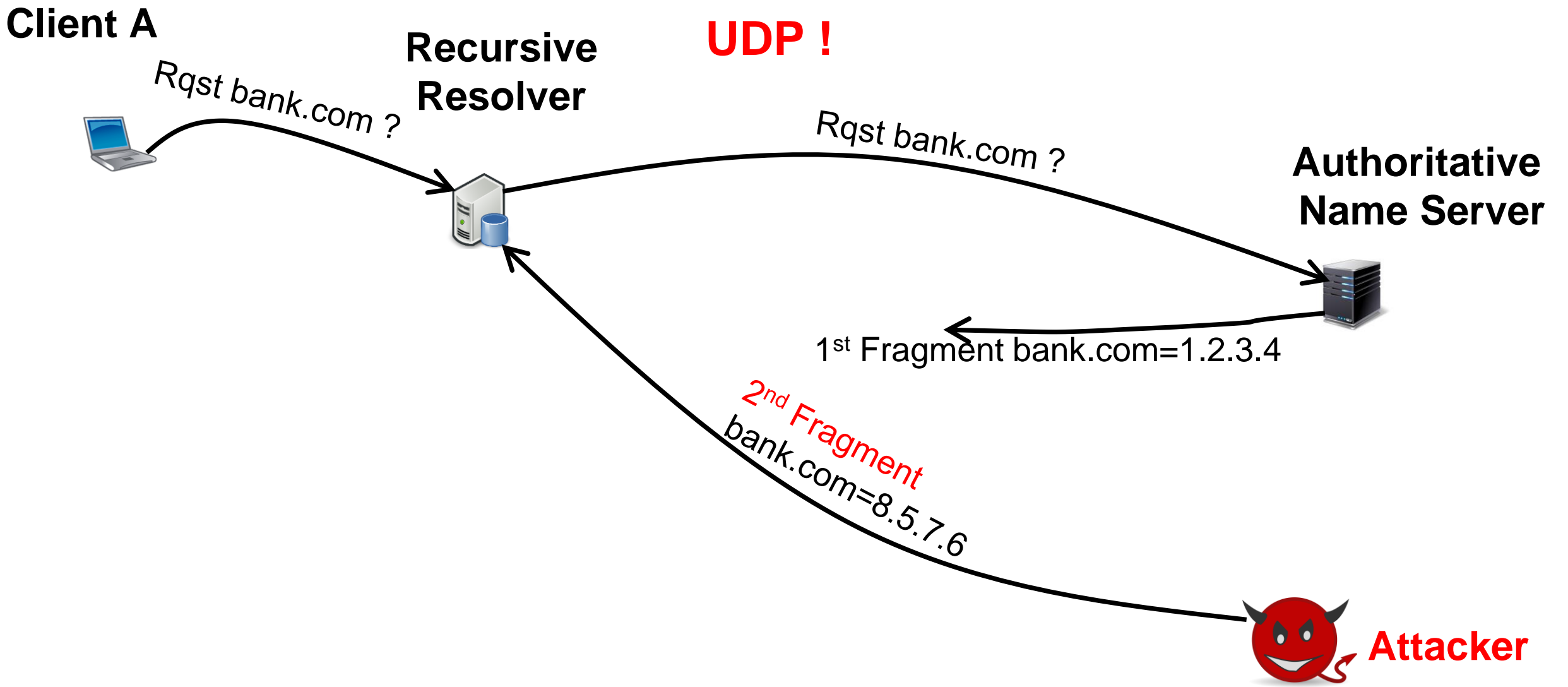
**Authoritative
Name Server**



Attacker



Fragmentation Poisoning Attack



Fragmentation Poisoning Attack

Client A



Rqst bank.com ?

Recursive Resolver



UDP !

Rqst bank.com ?

Authoritative Name Server



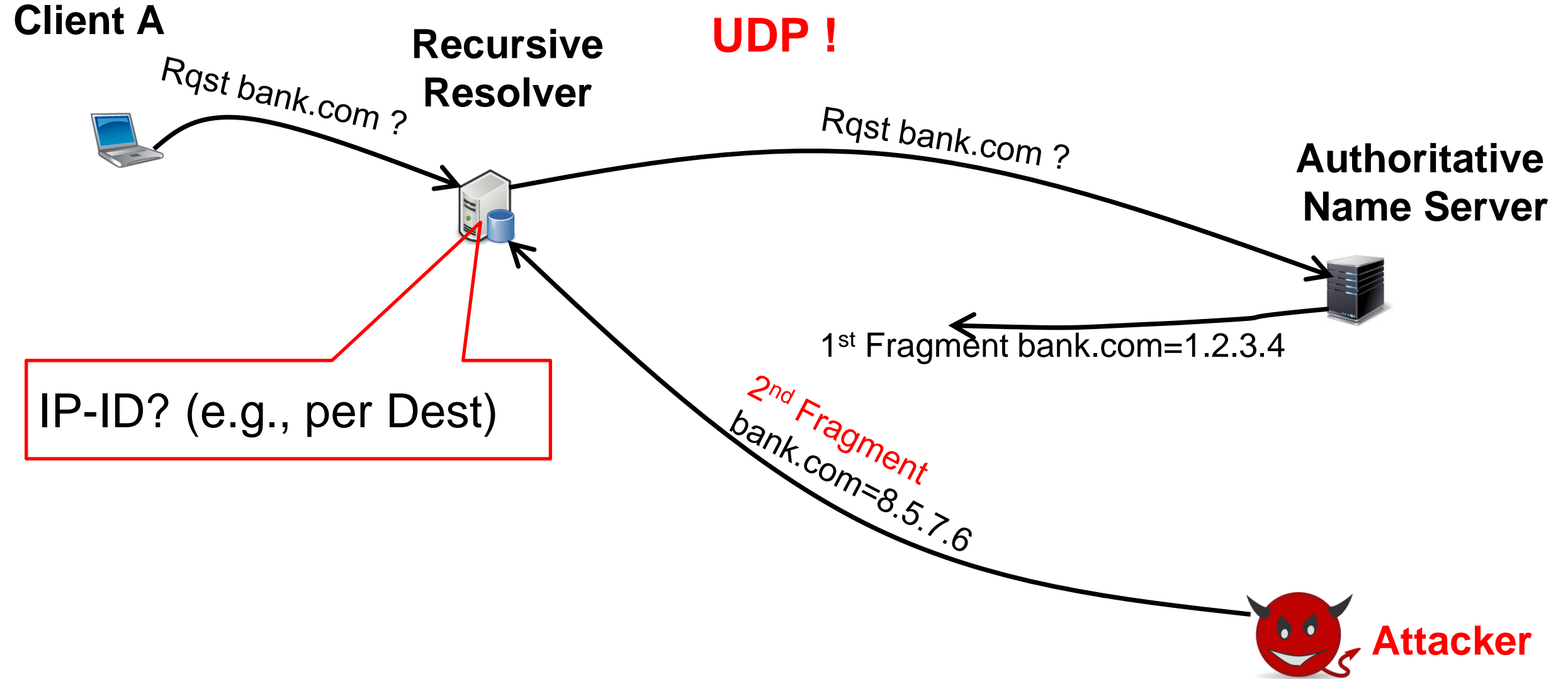
1st Fragment bank.com=1.2.3.4

2nd Fragment
bank.com=8.5.7.6

IP-ID? (e.g., per Dest)



Attacker



Fragmentation Poisoning Attack

Client A

Recursive Resolver

UDP !

Authoritative Name Server



Rqst bank.com ?

2nd Fragment
bank-8.5.7.6



Rqst bank.com ?



1st Fragment bank.com=1.2.3.4

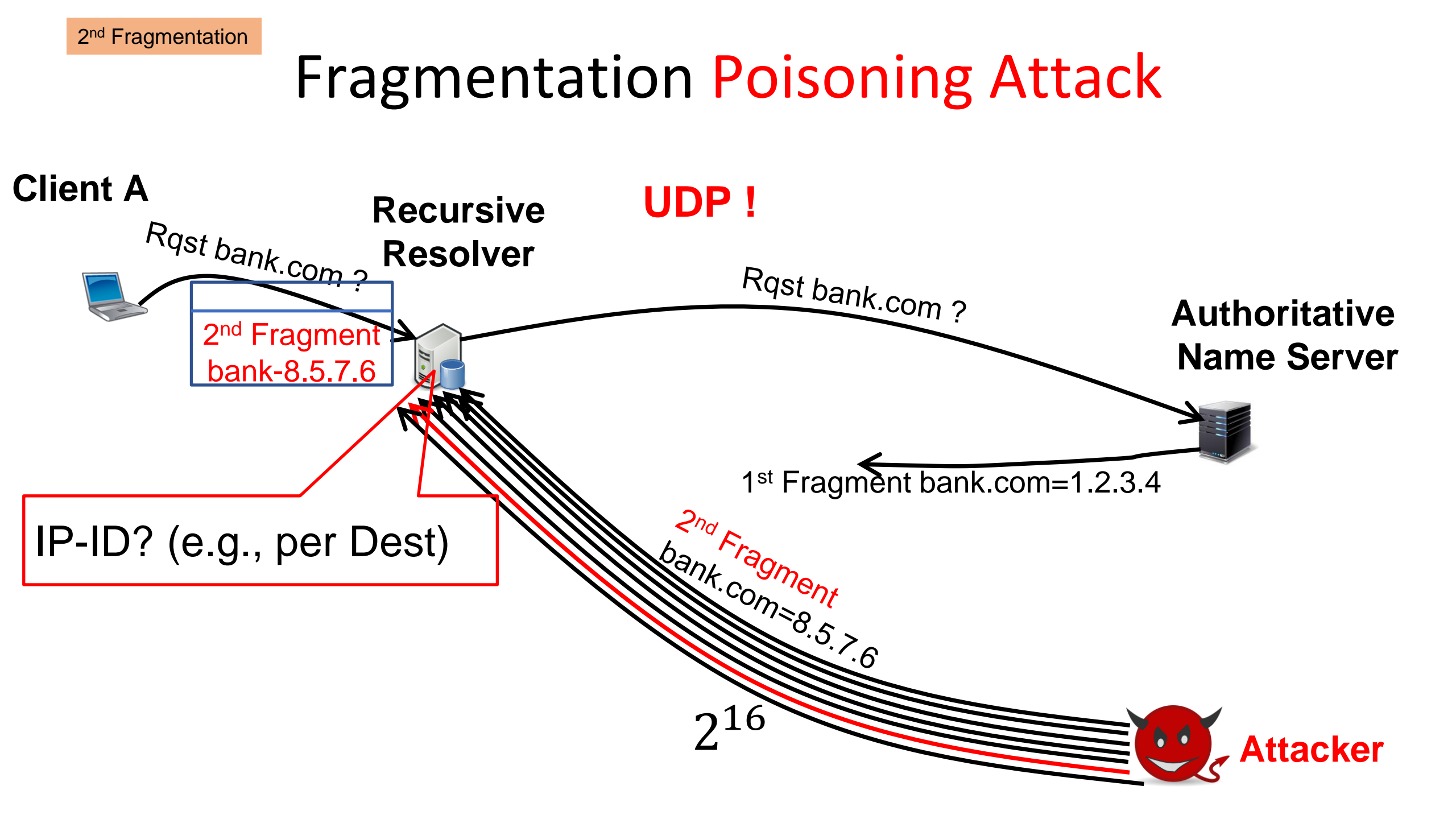
IP-ID? (e.g., per Dest)

2nd Fragment
bank.com=8.5.7.6

2¹⁶



Attacker



Fragmentation Poisoning Attack

Client A



Rqst bank.com ?

1st Frag
2nd Fragment
bank-8.5.7.6

Recursive Resolver



UDP !

Rqst bank.com ?

Authoritative Name Server



1st Fragment bank.com=1.2.3.4

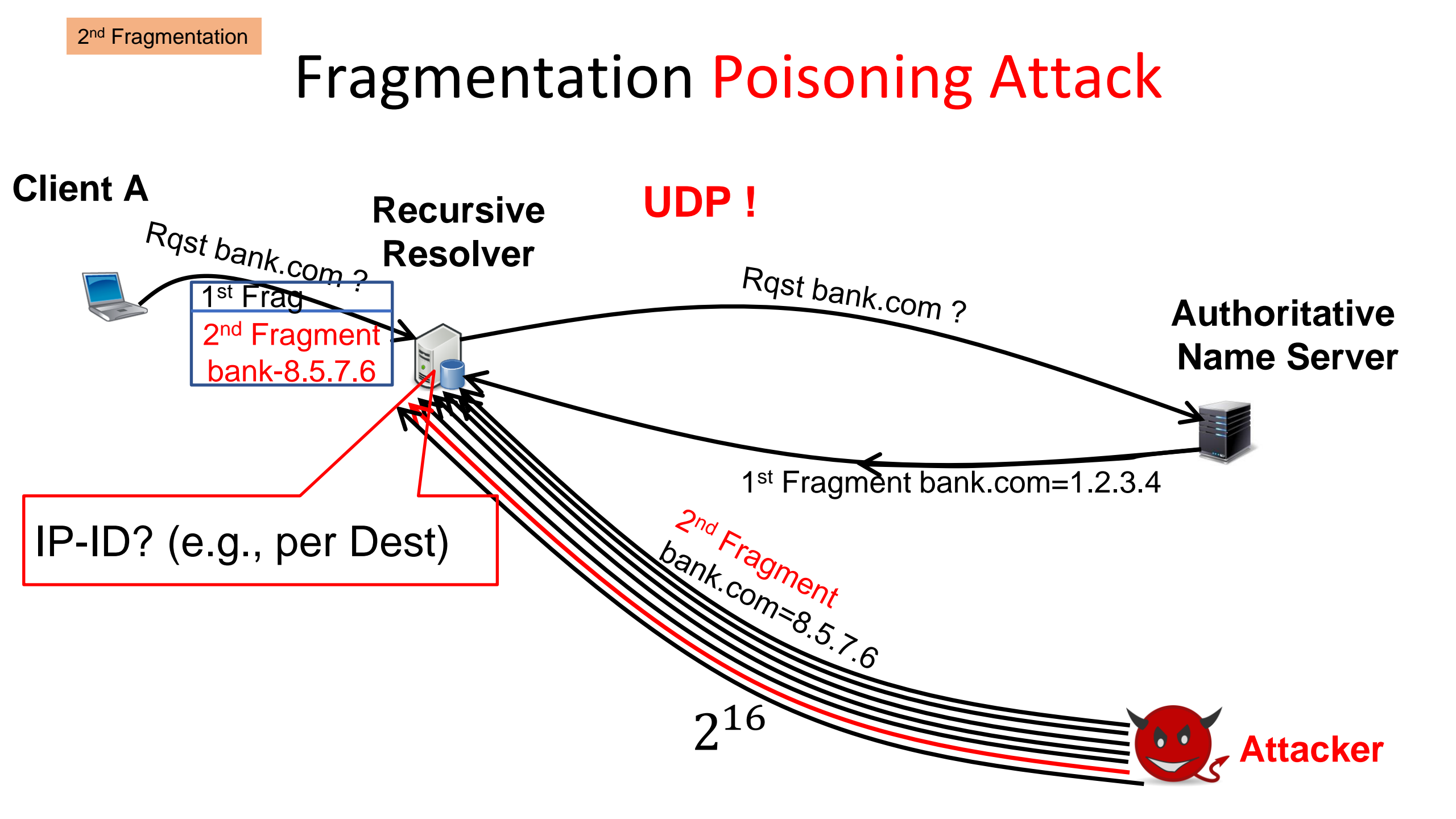
2nd Fragment
bank.com=8.5.7.6

2^{16}



Attacker

IP-ID? (e.g., per Dest)



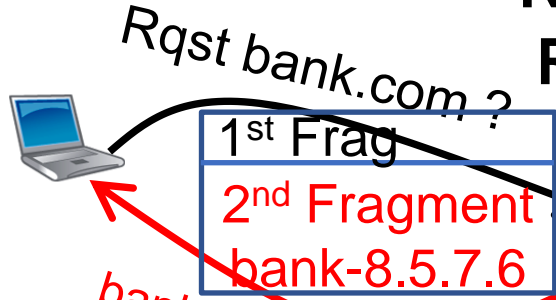
Fragmentation Poisoning Attack

Client A

Recursive Resolver

UDP !

Authoritative Name Server



bank.com=8.5.7.6

IP-ID? (e.g., per Dest)



Rqst bank.com ?



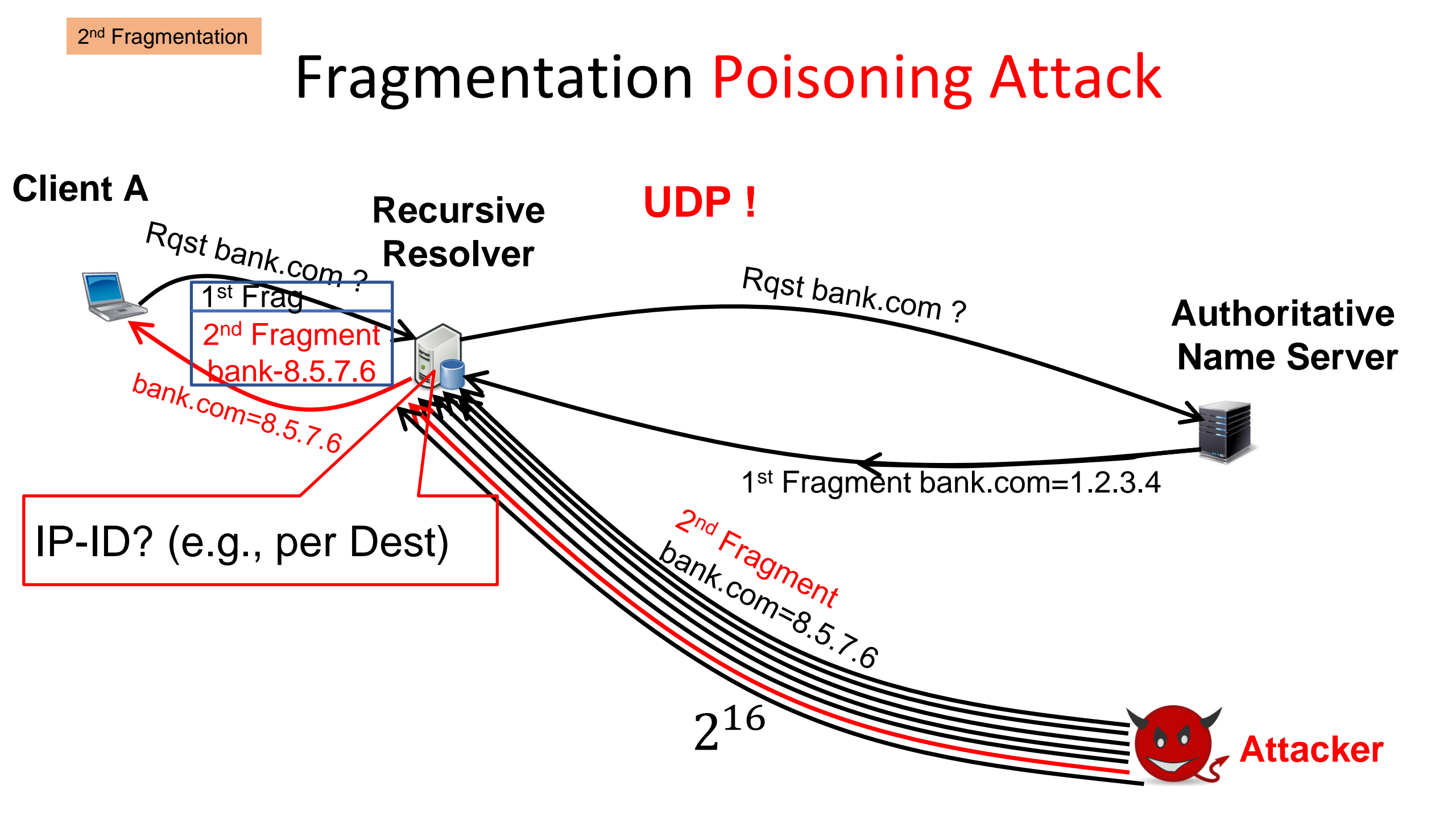
1st Fragment bank.com=1.2.3.4

2nd Fragment
bank.com=8.5.7.6

2^{16}



Attacker



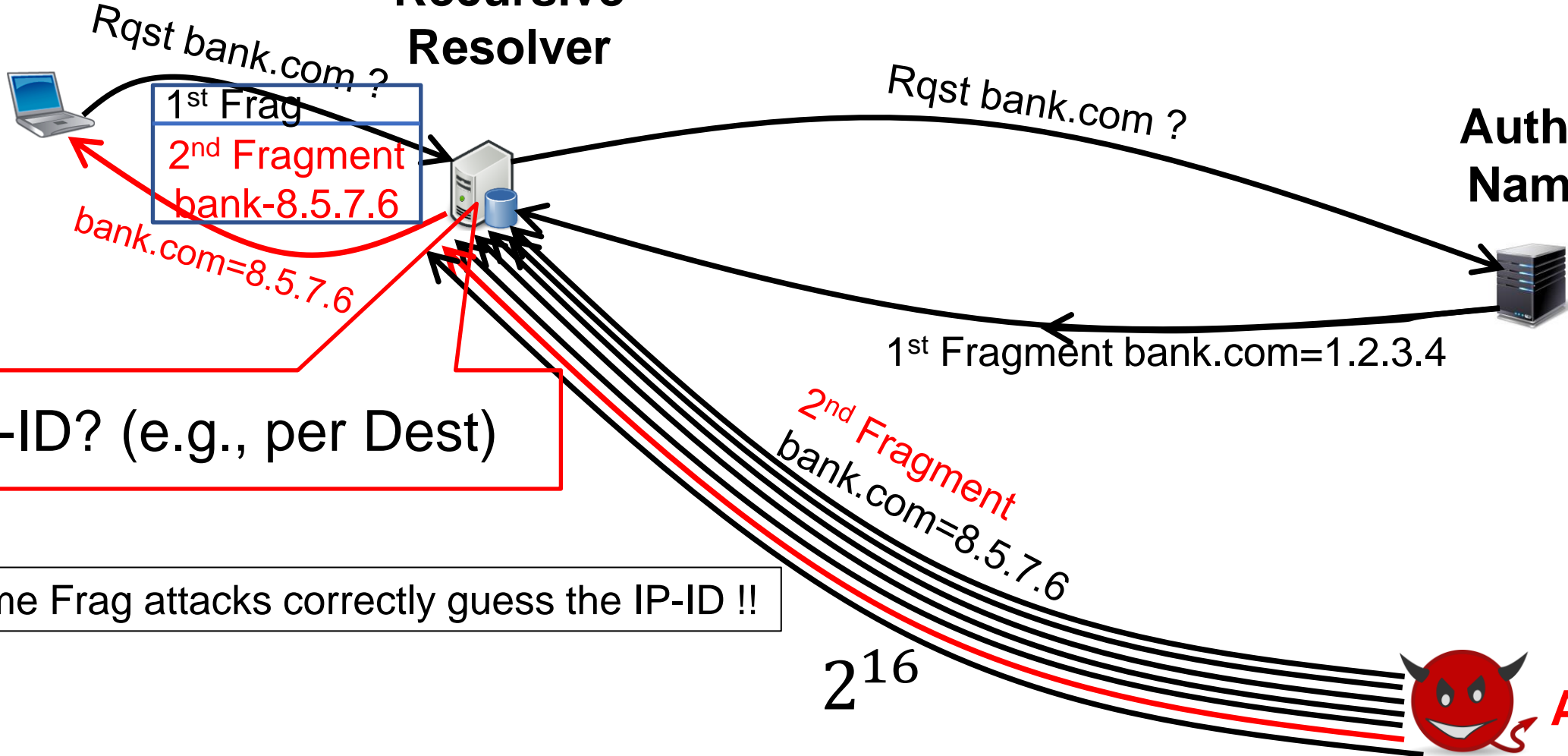
Fragmentation Poisoning Attack

Client A

Recursive Resolver

UDP !

Authoritative Name Server



IP-ID? (e.g., per Dest)

Some Frag attacks correctly guess the IP-ID !!

Fragmentation Poisoning Attack

Detection & Mitigation

UDP !

Client A

Recursive Resolver

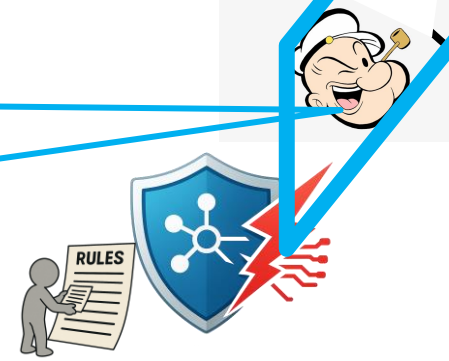
Authoritative Name Server



Rqst bank.com ?

Rqst bank.com ?

Block any Fragment

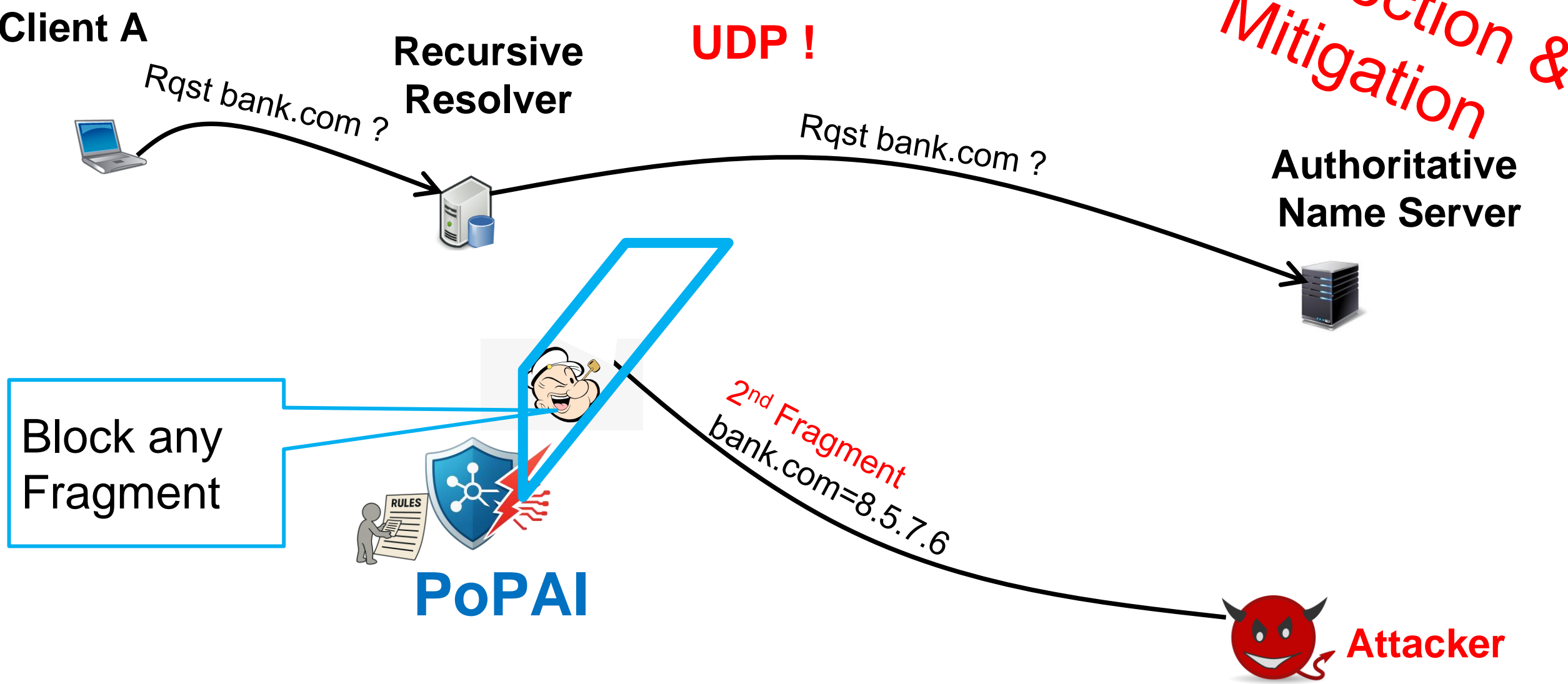


PoPAI

2nd Fragment
bank.com=8.5.7.6



Attacker



Fragmentation Poisoning Attack

Detection & Mitigation

UDP !

Client A

Recursive Resolver

Authoritative Name Server



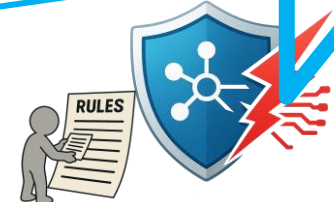
Rqst bank.com ?

Rqst bank.com ?

1st Fragment bank.com=1.2.3.4

2nd Fragment
bank.com=8.5.7.6

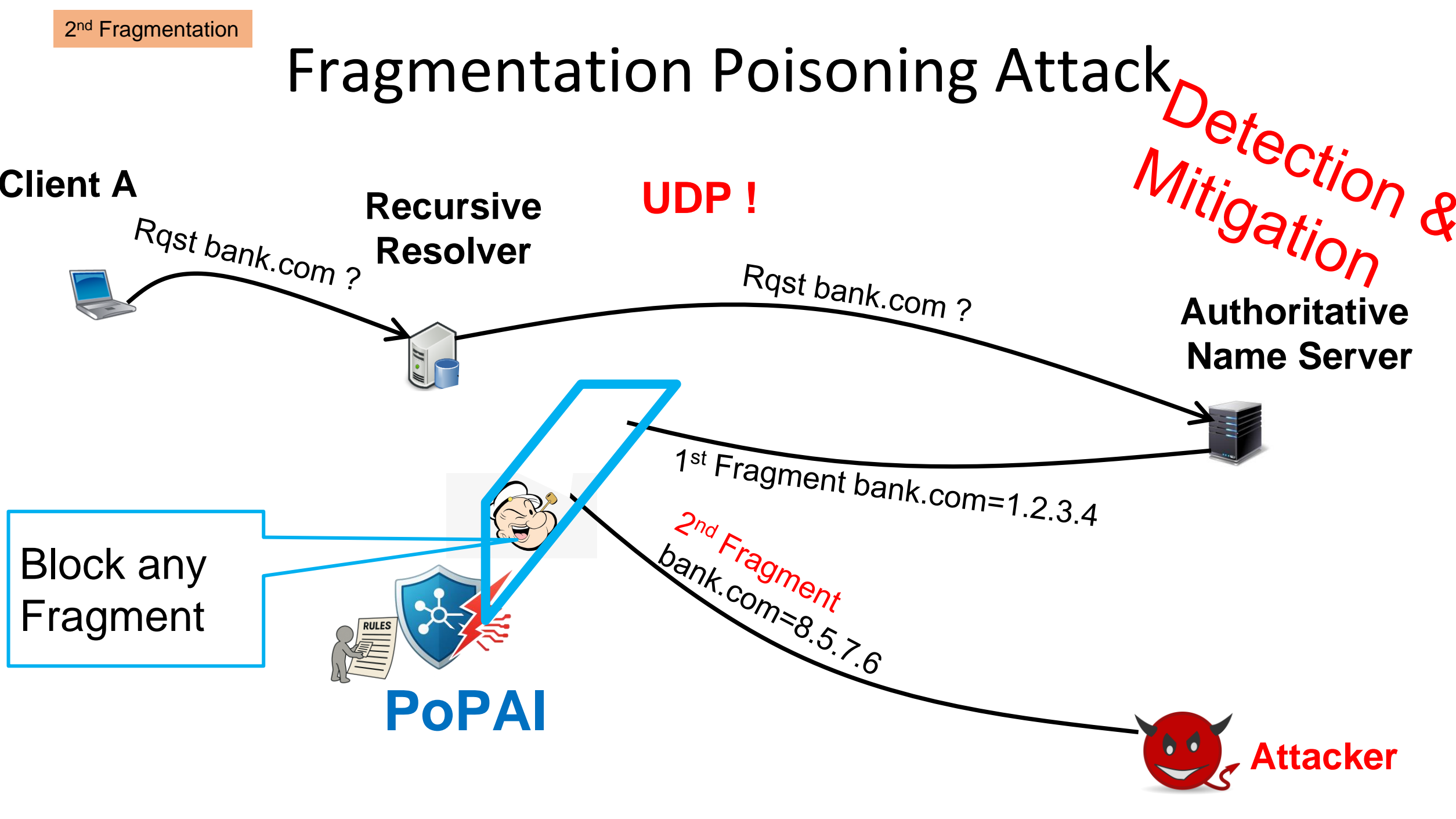
Block any Fragment



PoPAI



Attacker



Fragmentation Poisoning Attack

Detection & Mitigation

UDP !

TCP !

PoPAI

Client A

Recursive Resolver

Authoritative Name Server

Attacker

Rqst bank.com ?

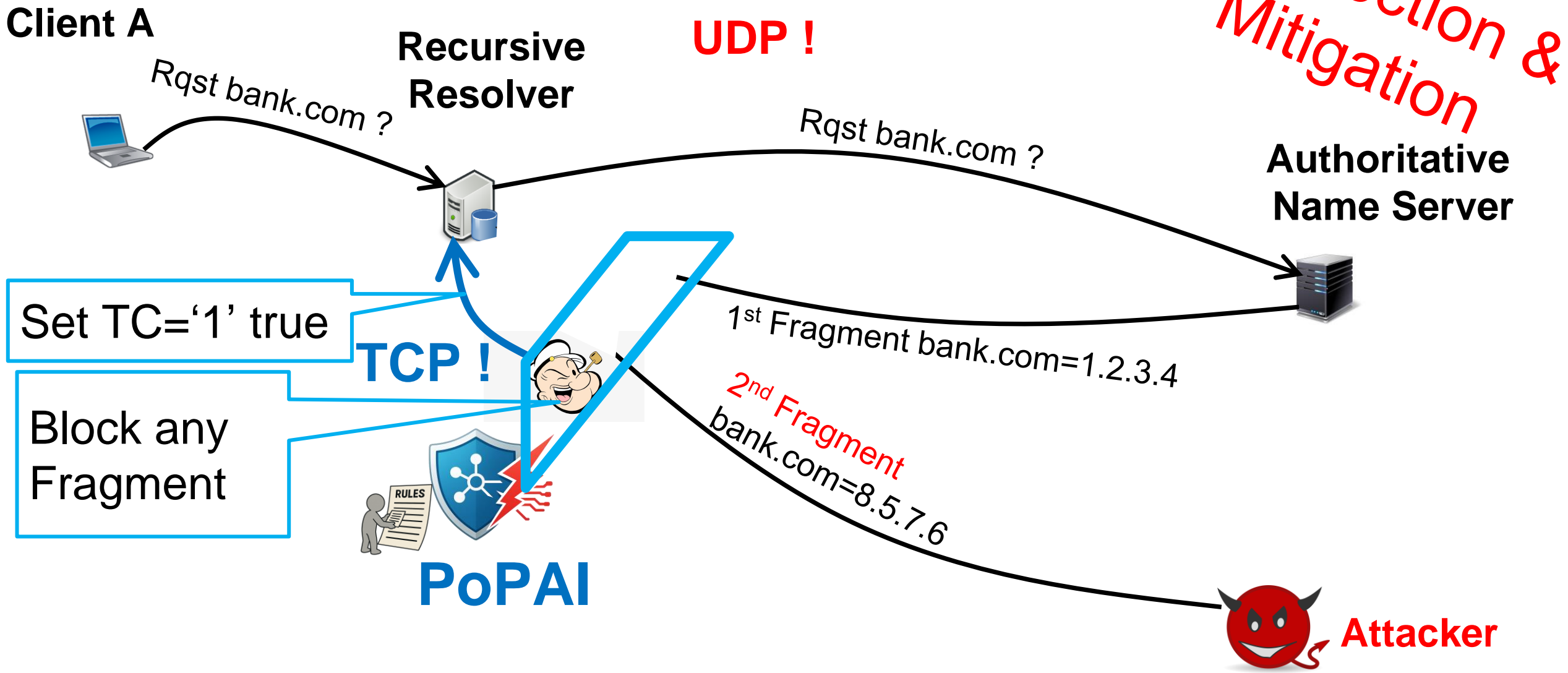
Rqst bank.com ?

1st Fragment bank.com=1.2.3.4

2nd Fragment
bank.com=8.5.7.6

Set TC='1' true

Block any
Fragment



Fragmentation Poisoning Attack

Detection & Mitigation

Client A



Rqst bank.com ?

Recursive Resolver



~~UDP !~~
TCP !

Rqst bank.com ?

Authoritative Name Server



Set TC='1' true

TCP !

Block any Fragment



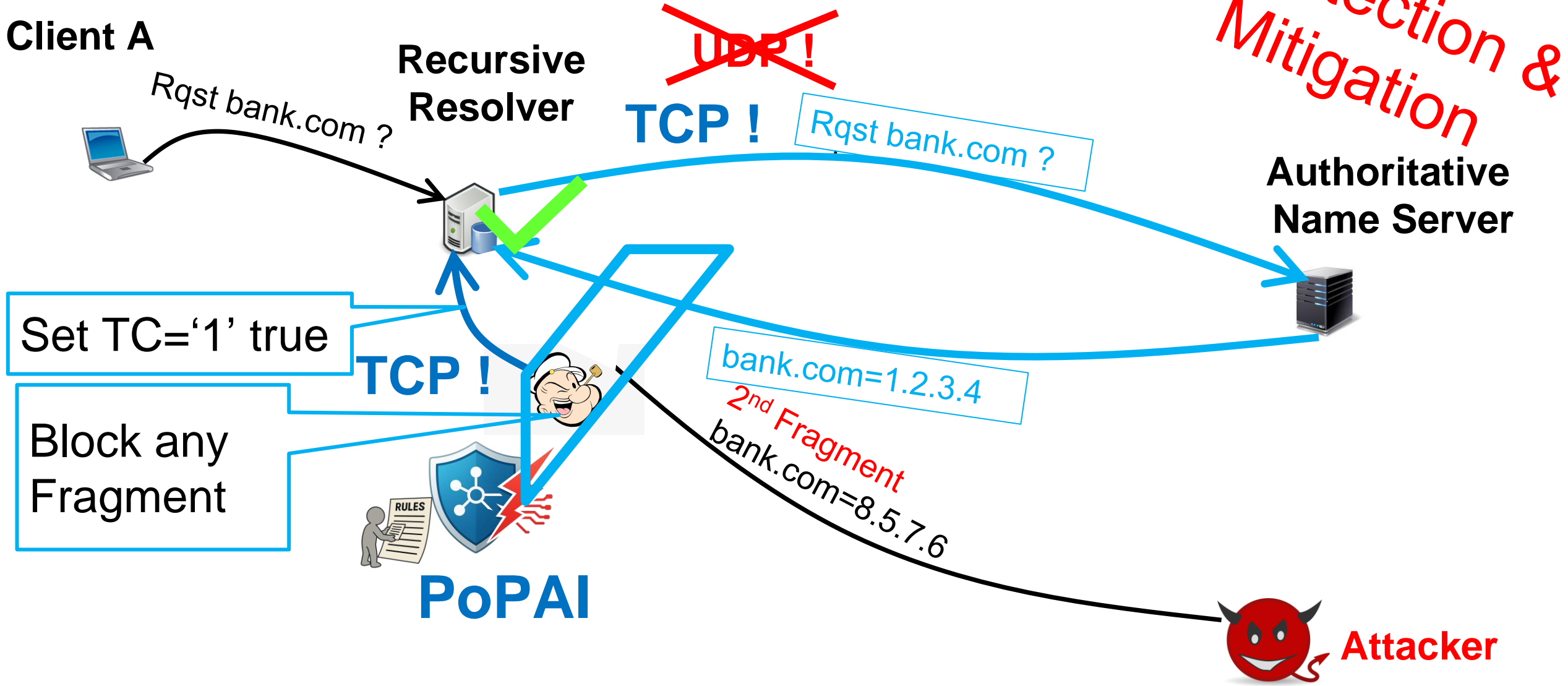
PoPAI

bank.com=1.2.3.4

2nd Fragment
bank.com=8.5.7.6



Attacker



Fragmentation Poisoning Attack

Detection & Mitigation

Client A

Recursive Resolver

~~UDP!~~
TCP!
Rqst bank.com ?

Authoritative Name Server



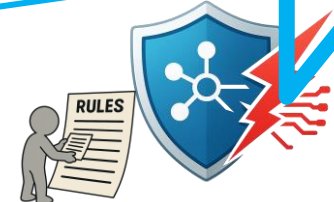
Rqst bank.com ?

bank.com=1.2.3.4

Set TC='1' true

TCP!

Block any Fragment



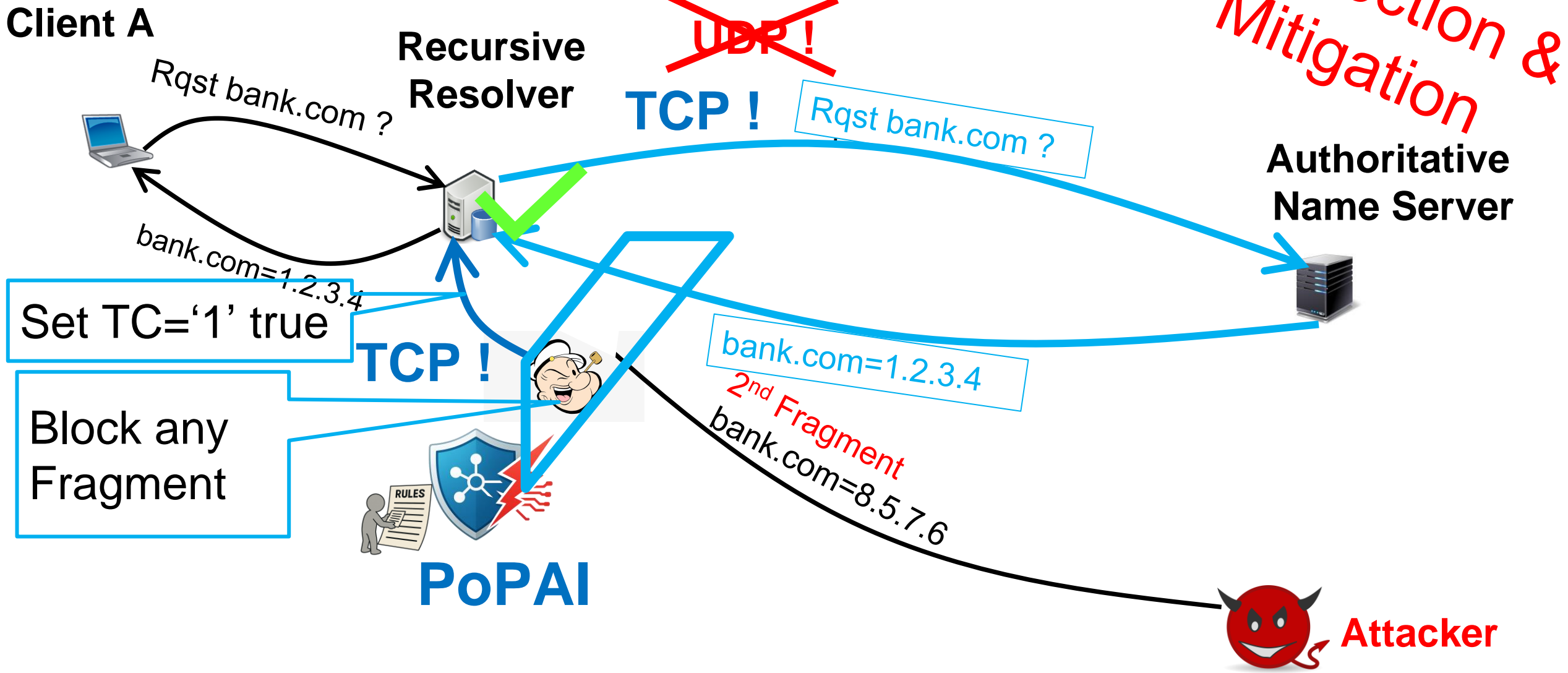
PoPAI

bank.com=1.2.3.4

2nd Fragment
bank.com=8.5.7.6



Attacker



Fragmentation Poisoning Attack

Detection & Mitigation

Client A

Recursive Resolver

~~UDP!~~

TCP!

Rqst bank.com ?

Authoritative Name Server



Rqst bank.com ?

bank.com=1.2.3.4

Set TC='1' true

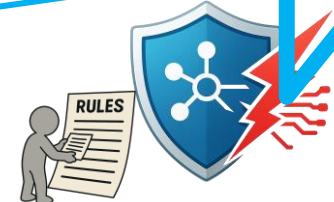
TCP!

Block any Fragment



bank.com=1.2.3.4

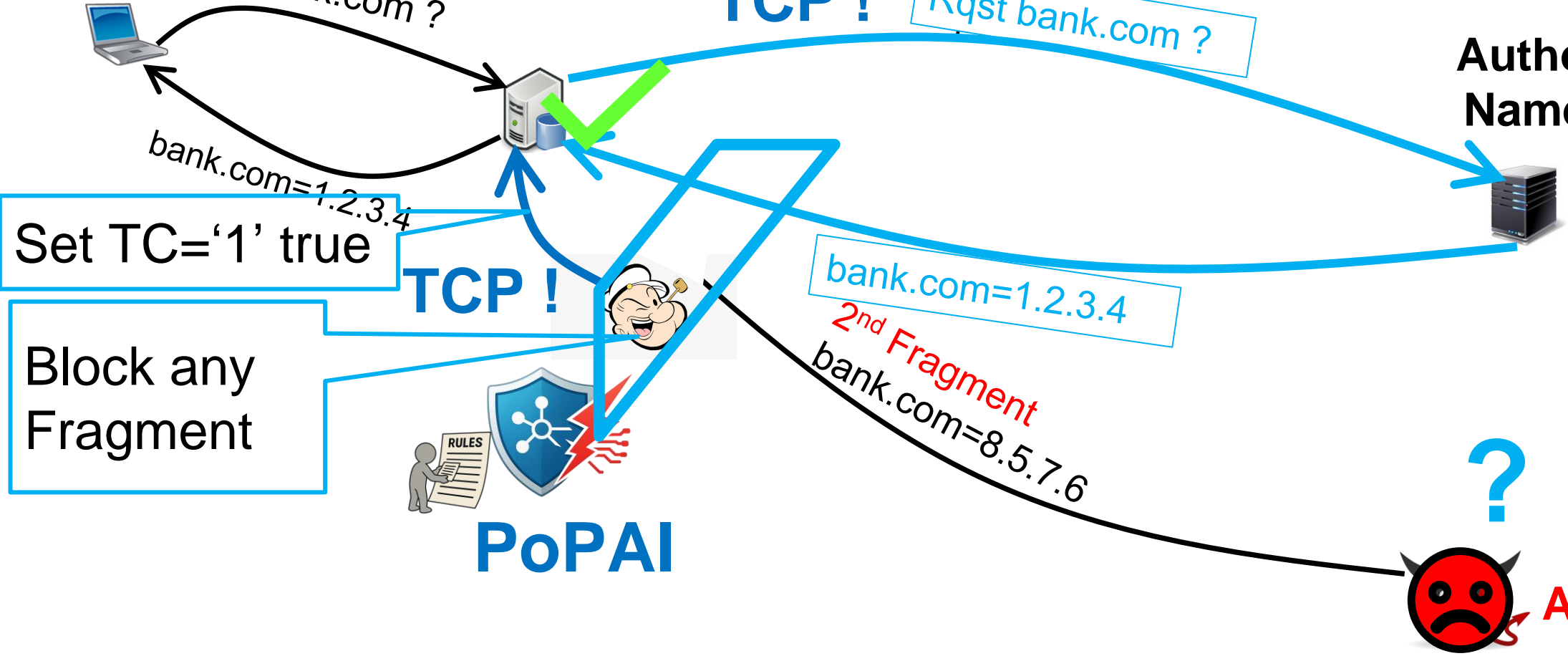
2nd Fragment
bank.com=8.5.7.6



PoPAI



Attacker



PoPAI

Fragmentation attack

PoPAI

Fragmentation attack

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

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])

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])

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])

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

Client A

Recursive Resolver

UDP !

Authoritative Name Server

In-Bailiwick !

Rqst foo.bar.com ?

Rqst foo.bar.com ?

Foo.bar.com=4.3.2.1

Answer: foo.bar.com A 4.3.2.1

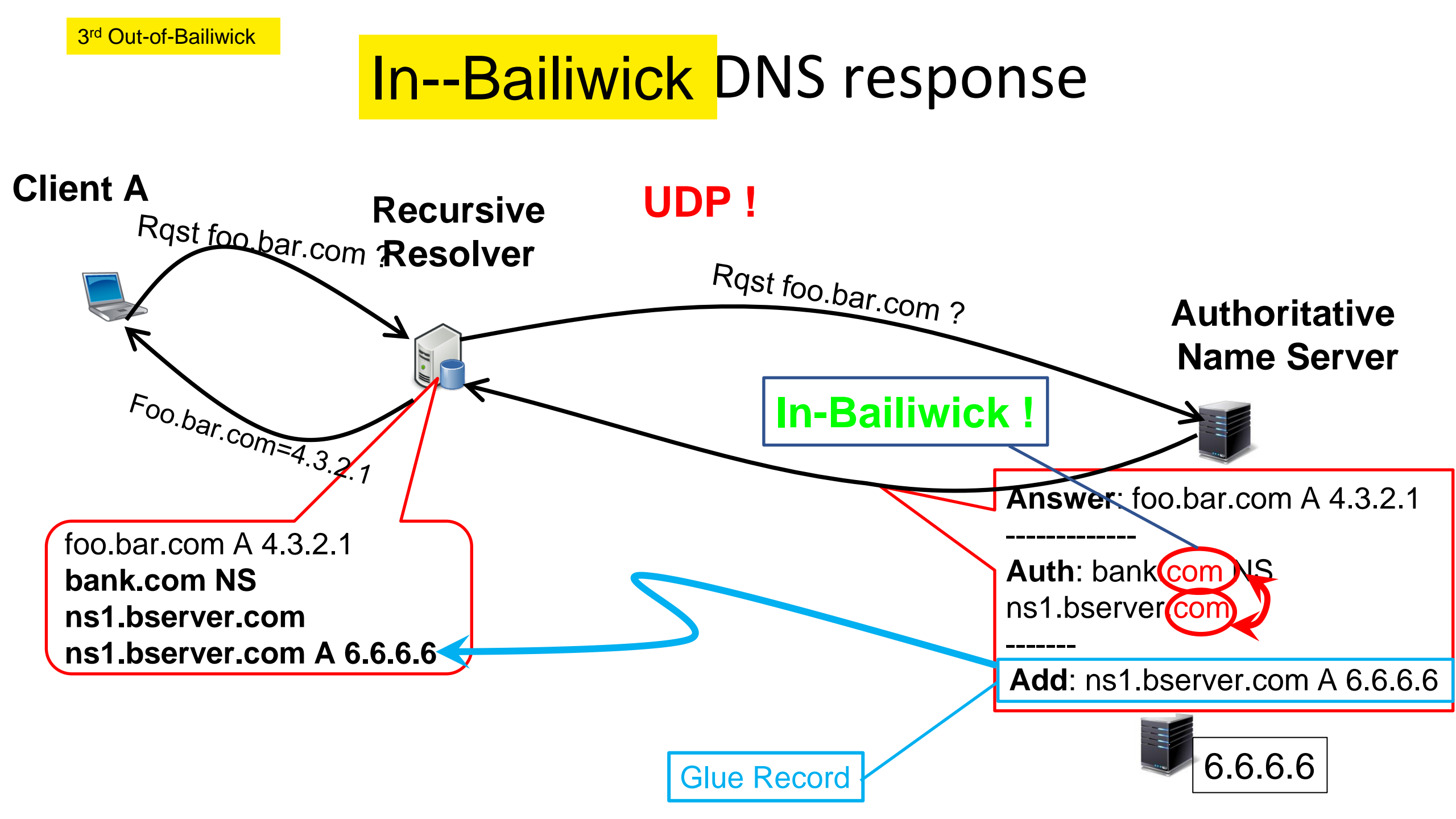
foo.bar.com A 4.3.2.1
bank.com NS
ns1.bserver.com
ns1.bserver.com A 6.6.6.6

Auth: bank.com NS
ns1.bserver.com

Add: ns1.bserver.com A 6.6.6.6

Glue Record

6.6.6.6



In--Bailiwick DNS response

Client A



Rqst bank.com ?

Recursive Resolver



UDP !

Rqst foo.bar.com ?

Authoritative Name Server



In-Bailiwick !

foo.bar.com A 4.3.2.1
bank.com NS
ns1.bserver.com
ns1.bserver.com A 6.6.6.6

Answer: foo.bar.com A 4.3.2.1

Auth: bank.com NS
ns1.bserver.com

Add: ns1.bserver.com A 6.6.6.6

Glue Record



6.6.6.6

In--Bailiwick DNS response

Client A

Recursive Resolver

UDP !

Authoritative Name Server

In-Bailiwick !

foo.bar.com A 4.3.2.1
bank.com NS
ns1.bserver.com
ns1.bserver.com A 6.6.6.6

Answer: foo.bar.com A 4.3.2.1

Auth: bank.com NS
ns1.bserver.com

Add: ns1.bserver.com A 6.6.6.6

Glue Record

6.6.6.6

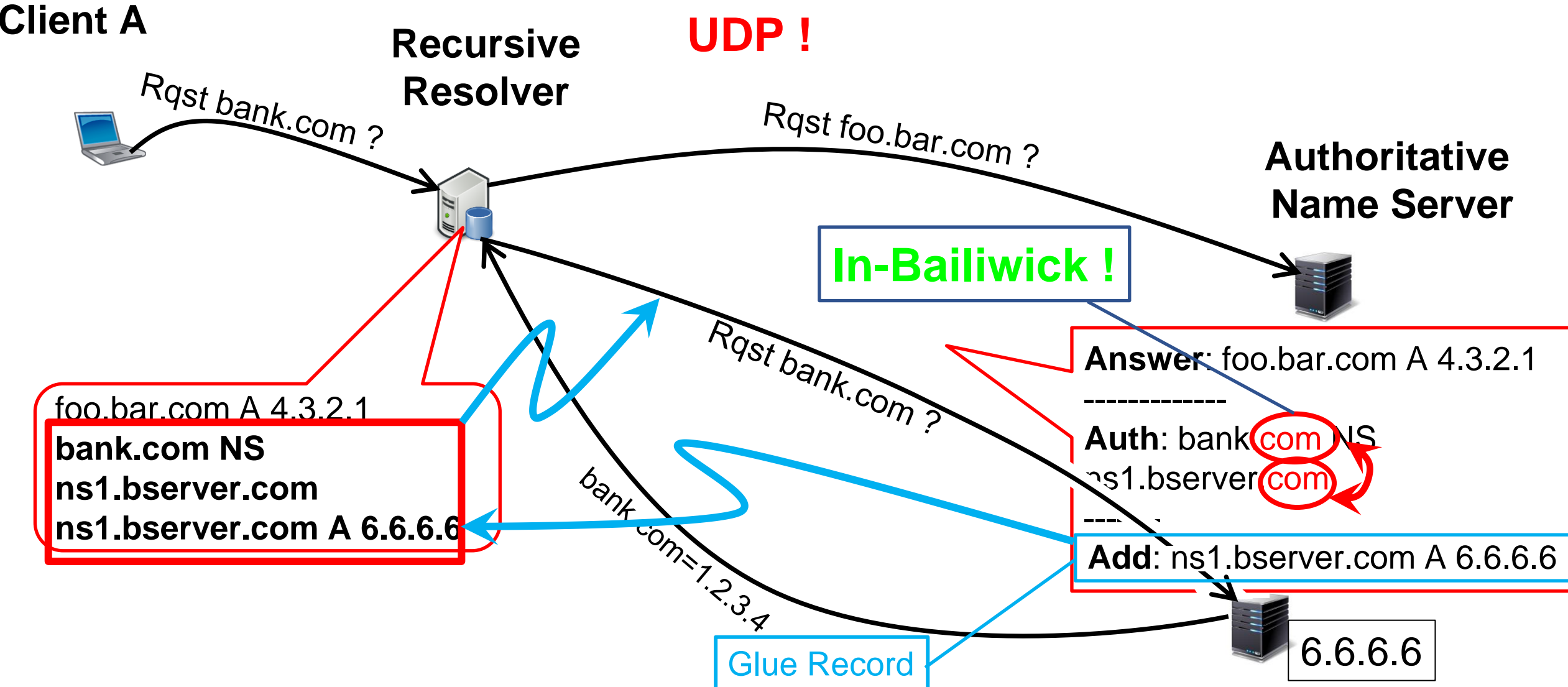


Rqst bank.com ?

Rqst foo.bar.com ?

Rqst bank.com ?

bank.com=1.2.3.4



In--Bailiwick DNS response

Client A

Recursive Resolver

UDP !

Authoritative Name Server

In-Bailiwick !

foo.bar.com A 4.3.2.1
bank.com NS
ns1.bserver.com
ns1.bserver.com A 6.6.6.6

Answer: foo.bar.com A 4.3.2.1

Auth: bank.com NS
ns1.bserver.com

Add: ns1.bserver.com A 6.6.6.6

Glue Record

6.6.6.6



Rqst bank.com ?

Rqst foo.bar.com ?

bank.com=1.2.3.4

Rqst bank.com ?

bank.com=1.2.3.4

Answer: foo.bar.com A 4.3.2.1

Auth: bank.com NS
ns1.bserver.com

Add: ns1.bserver.com A 6.6.6.6

6.6.6.6

Out-of-Bailiwick Poisoning Attack

Client A



Recursive Resolver

UDP !

Rqst foo.bar.com ?

Authoritative Name Server



Answer: foo.bar.com A 4.3.2.1

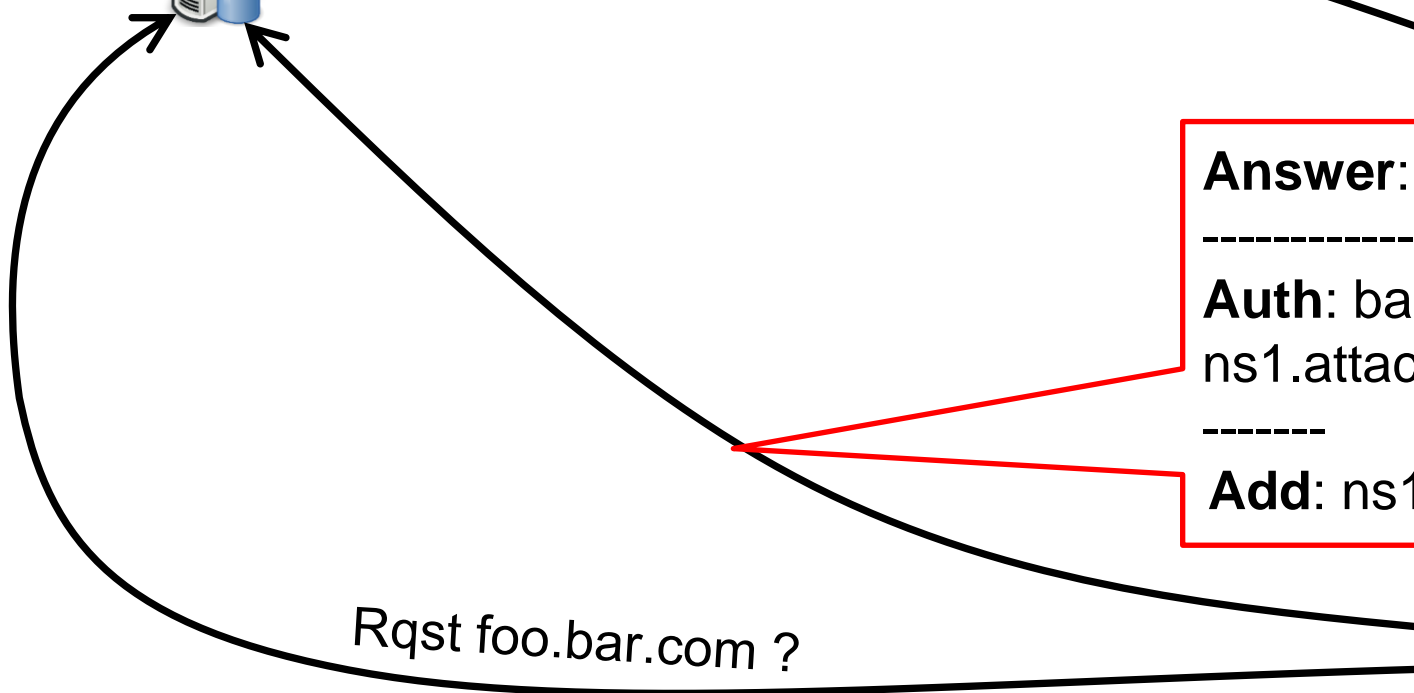
Auth: bank.com NS
ns1.attacker.net

Add: ns1.attacker.net A 7.7.7.7

Rqst foo.bar.com ?



Attacker
7.7.7.7



Out-of-Bailiwick Poisoning Attack

Client A



Recursive Resolver

UDP !

Rqst foo.bar.com ?

Authoritative Name Server

Out-O-Bailiwick!

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

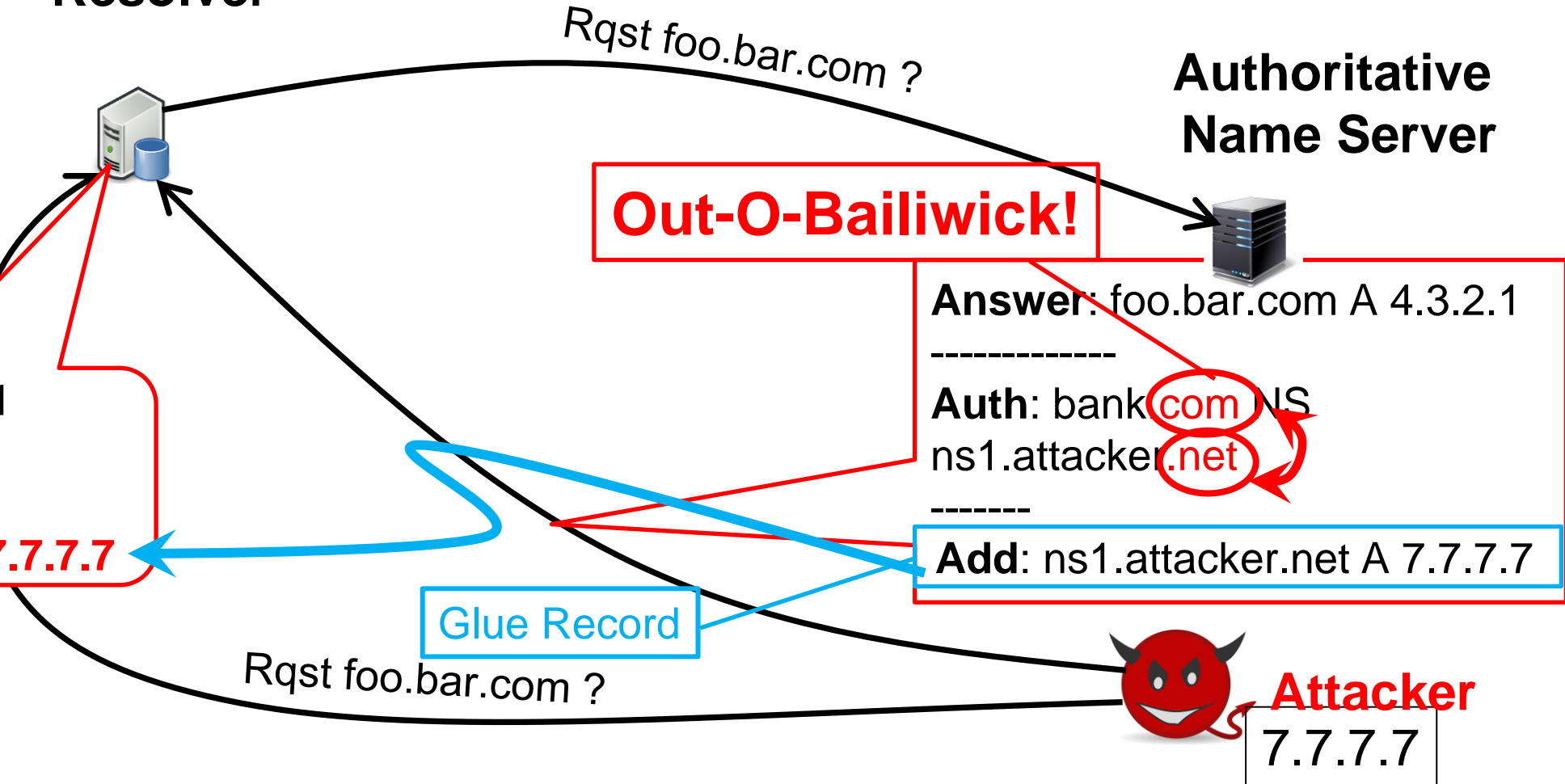
foo.bar.com A 4.3.2.1
bank.com NS
ns1.attacker.net
ns1.attacker.net A 7.7.7.7

Glue Record

Rqst foo.bar.com ?



Attacker
7.7.7.7



Out-of-Bailiwick Poisoning Attack

Client A



Rqst bank.com ?

Recursive Resolver



UDP !

Rqst bank.com ?

Authoritative Name Server

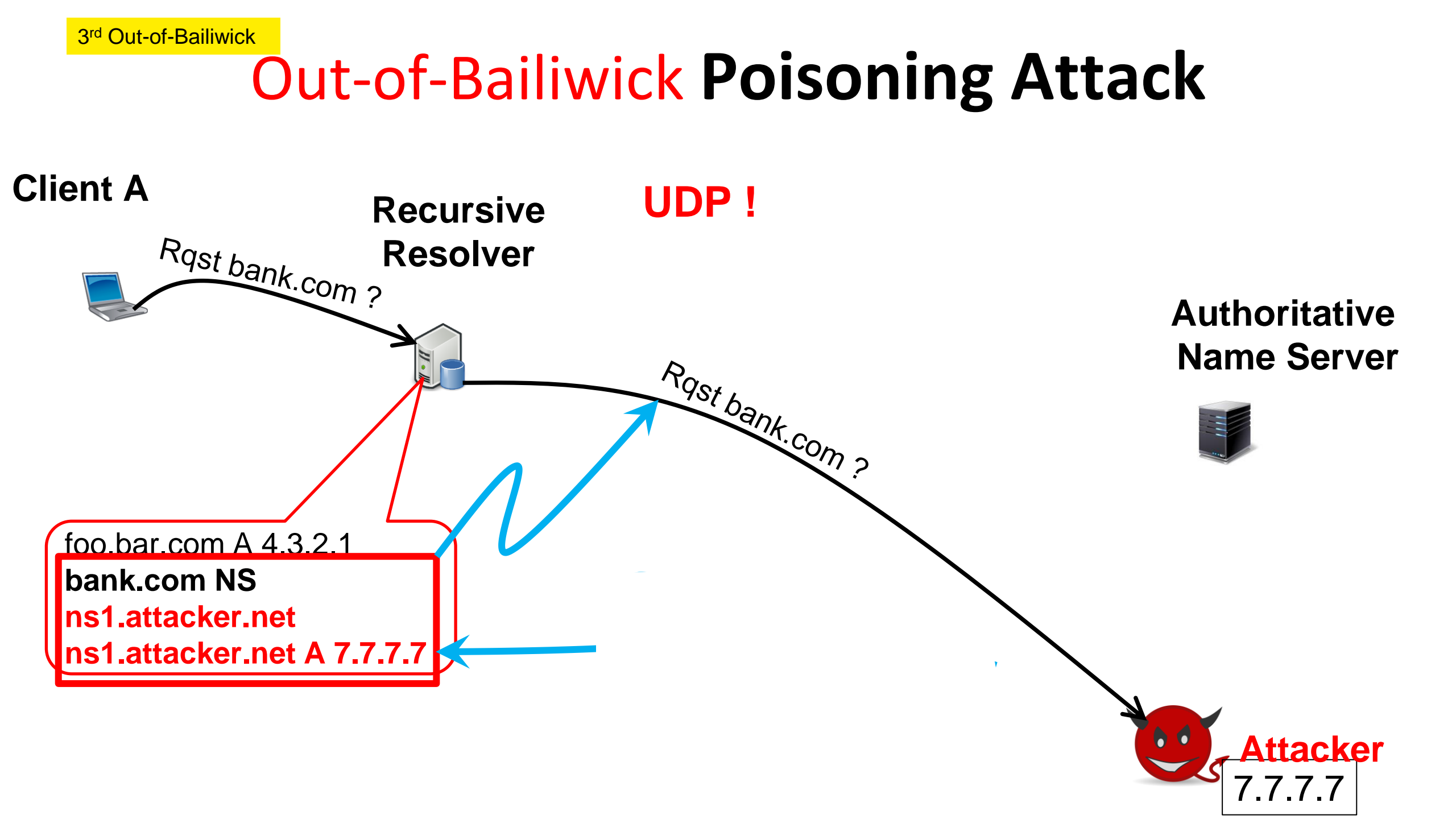


foo.bar.com A 4.3.2.1
bank.com NS
ns1.attacker.net
ns1.attacker.net A 7.7.7.7



Attacker

7.7.7.7



Out-of-Bailiwick Poisoning Attack

Client A

Recursive
Resolver

UDP !

Authoritative
Name Server



Rqst bank.com ?

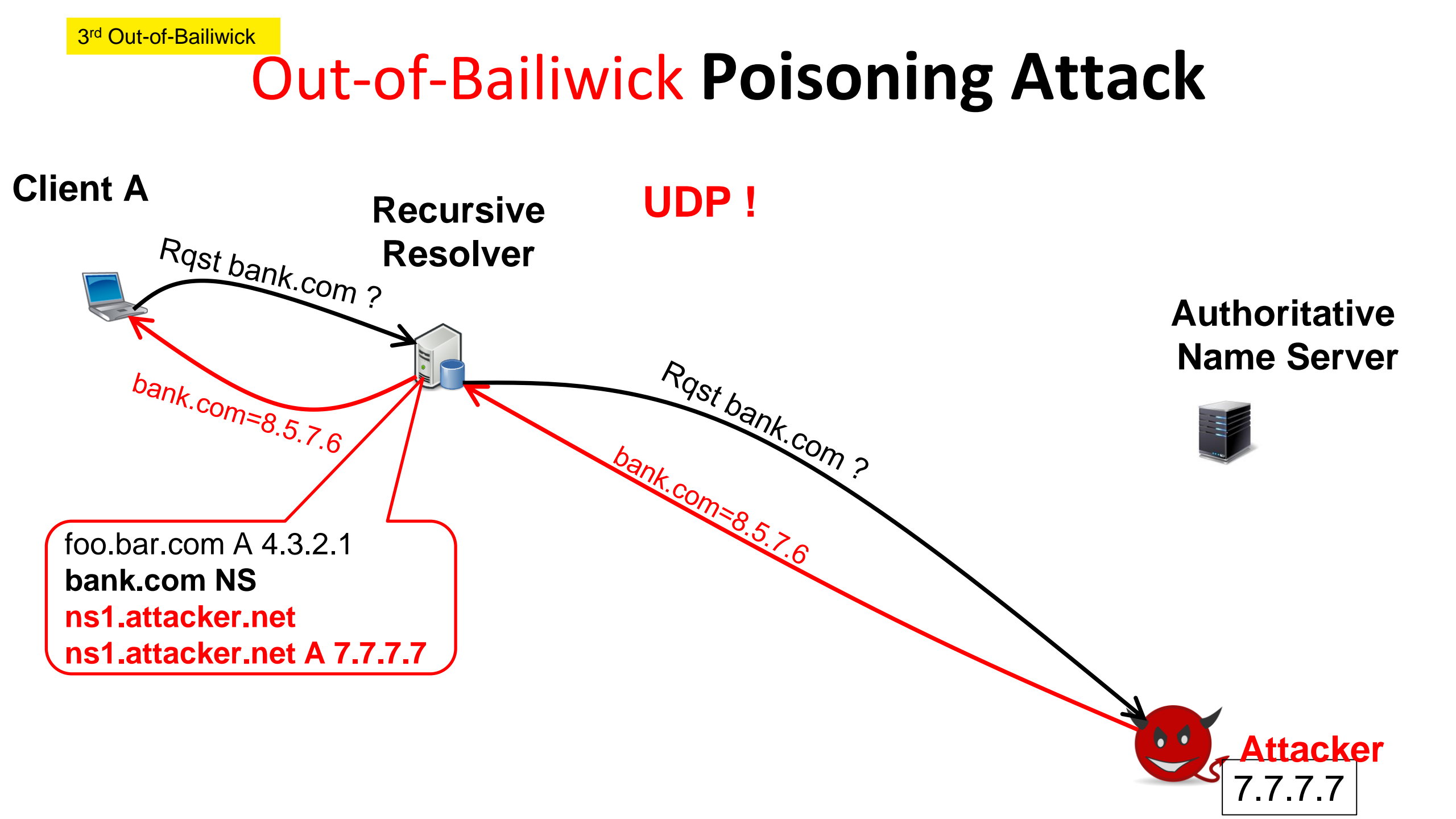
Rqst bank.com ?

bank.com=8.5.7.6

bank.com=8.5.7.6

foo.bar.com A 4.3.2.1
bank.com NS
ns1.attacker.net
ns1.attacker.net A 7.7.7.7

Attacker
7.7.7.7



Out-of-Bailiwick Poisoning Attack

Mitigation

Client A



Recursive Resolver



UDP !

Rqst foo.bar.com ?

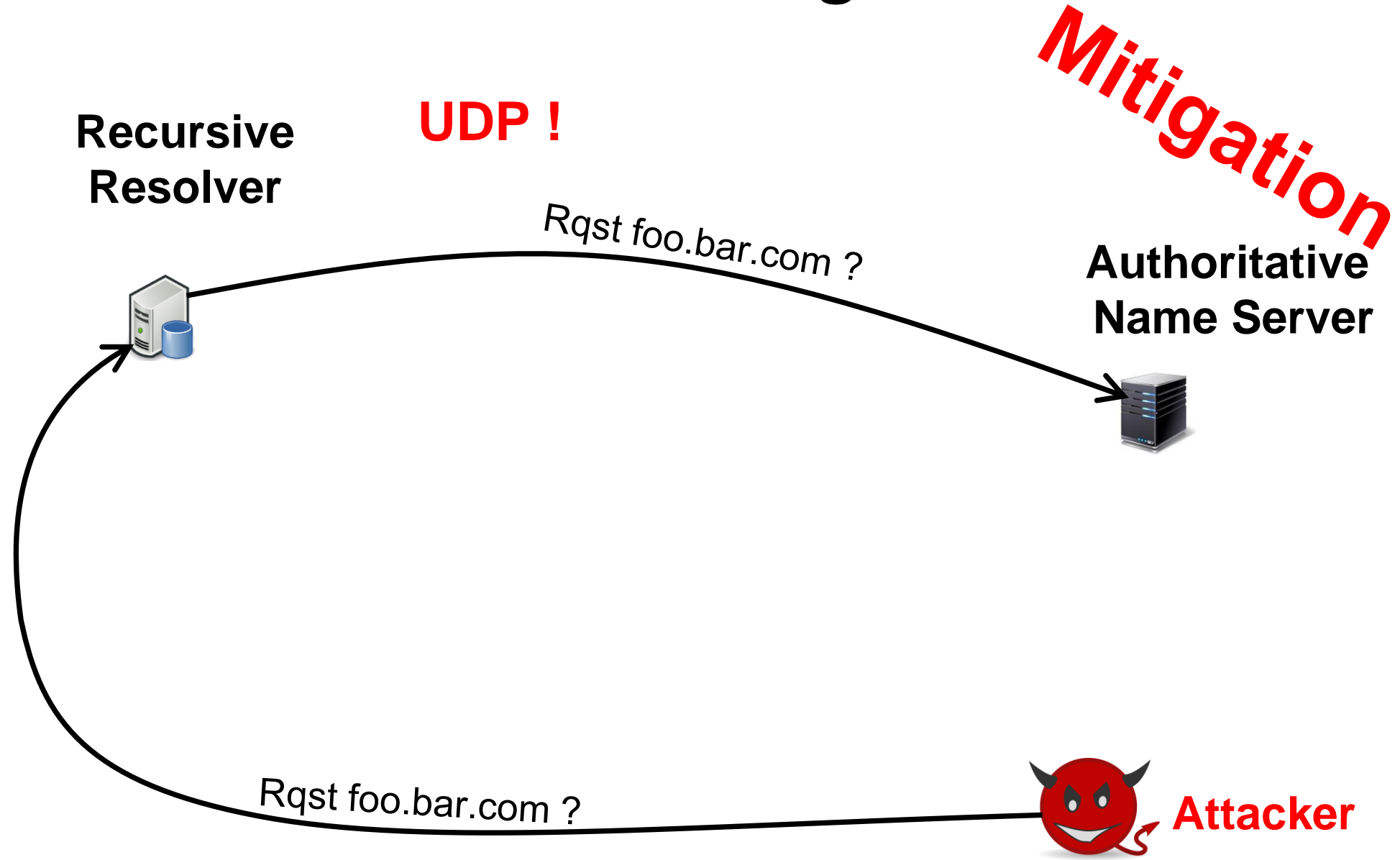
Authoritative Name Server



Rqst foo.bar.com ?



Attacker



Out-of-Bailiwick Poisoning Attack

Mitigation

Client A



Recursive Resolver

UDP !

Authoritative Name Server

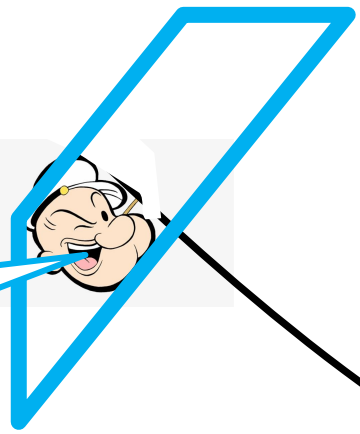
Rqst foo.bar.com ?

```

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

```

Drop all Out-of-Bailiwick responses



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



POPAL detection:

- 2x – 5x faster than Suricata/Snort
- 5%–10% of packets analyzed by Suricata/Snort
- Suricata/Snort 10x–20x 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>