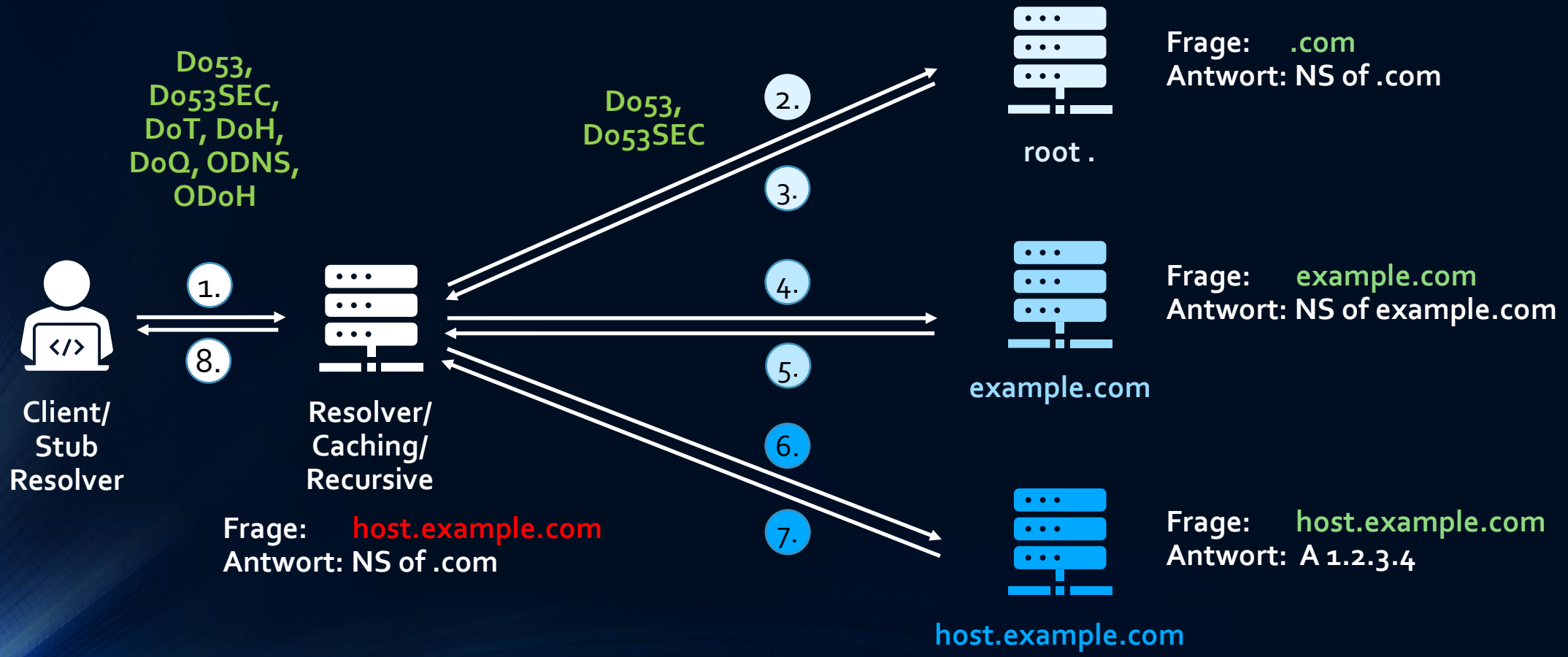
Hyper-local root DNS

JÖRG BACKSCHUES - 6. DDI USER GROUP 12/2022

DNS-Server & Client

- **Authoritative DNS-Server**
  - verantwortlich für eine bestimmte Zone
    (z.B. Zone "net" oder Zone "backschues.net")
  - verwaltet die Resource Records (RR) für eine bestimmte Zone
- **non-authoritative / recursive / caching DNS-Server**
  - holt sich Resource Records von den verschiedenen authoritative DNS-Servern der einzelnen Zonen, setzt sie zusammen und gibt sie an den Sub Resolver eines Clients weiter
  - rekursive Vorgehensweise: 1. TLD 2. (Sub-) Domains … X. Hostname
- **Client Sub Resolver**
  - eigentlicher Empfänger der DNS-Informationen (RRs)

Namesauflösung



Analyse einer DNS-Infrastruktur

- Wo befinden sich authoritative / recursive DNS-Server?
- Klassifizierung von Clients (Applikationen / Benutzer)
- Welche RRs benötigt ein Client (split-horizon DNS Situation) ?
- Welcher Client fragt welchen DNS-Server ab?
- Welche RRs werden von den Clients abgefragt?
  (Chromium based browsers & DNS <https://brainattic.in/blog/2020/06/03/chromium-based-browsers-dns/>)

Anfragen beim DNS root

RFC 6761 name	As of Nov 2022	Past 3 months	Historic Low	Historic High
LOCAL	8.745%	7.280%	2.360%	8.069%
TEST	0.653%	0.235%	0.008%	0.345%
LOCALHOST	0.519%	0.525%	0.206%	0.561%
INVALID	0.359%	0.373%	0.191%	0.485%
ONION	0.012%	0.012%	0.002%	0.017%

RFC 6761 Special-Use Domain Names

EXAMPLE

Frequently used string	As of Nov 2022	Past 3 months	Historic Low	Historic High
INTERNAL	4.468%	3.969%	0.301%	4.058%
HOME	1.731%	1.626%	1.515%	4.279%
CTC	1.200%	1.130%	0.000%	1.156%
DHCP	1.196%	1.328%	0.206%	1.618%
BBROUTER	1.077%	1.069%	0.000%	1.443%
LAN	0.871%	0.681%	0.469%	1.306%
WIFI	0.554%	0.495%	0.000%	0.578%

(root Server Statistiken: <https://ithi.research.icann.org/graph-m3.html>)

Performance & Privacy

- **Query Time**
  - NXDOMAIN

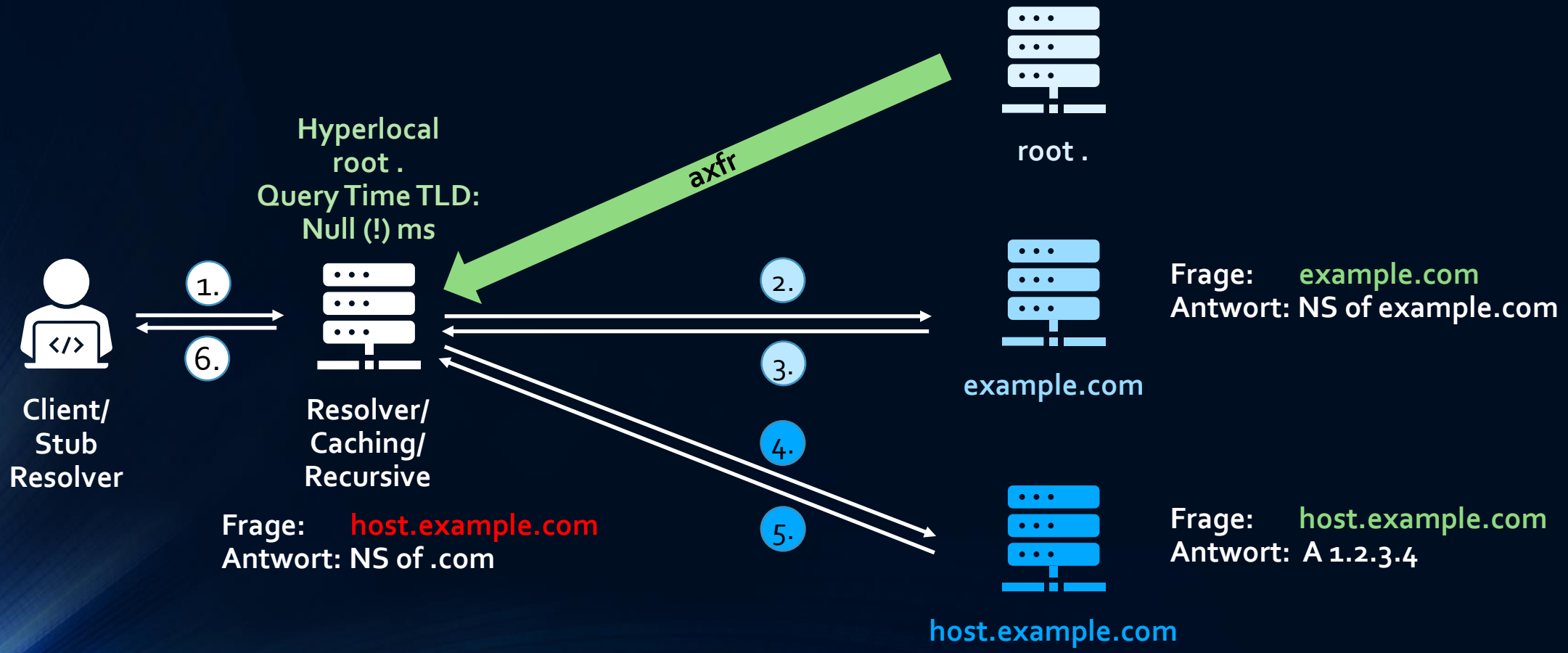
```
dig thisdoesnotexsists @b.root-servers.net
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 46293
[…]
;; Query time: 16 msec
;; SERVER: 2001:500:200::b#53(2001:500:200::b)
[…]
```

- **Special-Use Domain Names / Leaked strings**
  - Auswertung von (evtl. internen) Anfragen möglich

Historie Hyperlocal DNS

- **RFC 7706 (obsolet): Decreasing Access Time to Root Servers by Running One on Loopback (November 2015)**
  - „longer-than-desired round-trip times […]“
  - “Some DNS recursive resolver operators want to prevent snooping of requests sent to DNS root servers by third parties”
- **RFC 8806: Running a Root Server Local to a Resolver (Juni 2020)**
  - „Added the idea that a recursive resolver using this design might switch to using the normal (remote) root servers if the local root server fails.“
  - „Refreshed the list of where one can get copies of the root zone.”
  - “Added examples of other resolvers and updated the existing examples.“

Hyperlocal root DNS



Performance & Privacy

- **Query Time**
  - NXDOMAIN

```
dig thisdoesnotexsists @10.64.64.1
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 16394
[…]
;; Query time: 0 msec
;; SERVER: 10.64.64.1#53(10.64.64.1)
[…]
```

- **Special-Use Domain Names / Leaked strings**
  - (Interne) Anfragen werden bereits vom lokalen Resolver beantwortet.

Referenz Umsetzung bind

- bind 9.14 basierend auf fest integrierter IANA root zone Daten

```
zone "." {
    type mirror;
};
```

- Bind 9.12

```
zone "." {
    type slave;
    file "/var/cache/bind/slave/db.root";
    notify no;
    masters {
       199.9.14.201;    # b.root-servers.net
       2001:500:200::b; # b.root-servers.net
       [...]
    };
};
```

(RFC 8806 <https://www.rfc-editor.org/rfc/rfc8806>)

Referenz Umsetzung unbound

- **unbound 1.8**

```
auth-zone:
name: "."
    master: 199.9.14.201    # b.root-servers.net
    master: 192.33.4.200::b # b.root-servers.net
    [...]
    fallback-enabled: yes
    for-downstream: no
    for-upstream: yes
```

(RFC 8806 <https://www.rfc-editor.org/rfc/rfc8806>)

Referenz Umsetzung Windows Server

- **Windows 2012**

  (RFC 8806 <https://www.rfc-editor.org/rfc/rfc8806>)

Betrieb eines Hyperlocal root DNS

- **Monitoring**
  - Überwachung der AXFRs,
  - Monitoring SOA der lokale Kopie der root Zone
- **Statistik**
  - in der Regel 1-3 neue Versionen der root Zone pro Tag
  - aktuell ca. 1,7 MB Größe
  - ca. 1500 TLDs
- **Verfügbarkeit & Zuverlässigkeit**
  - unbound Setup: innerhalb der letzten 3 Jahre stabil

(Geoff Huston: Expanding the DNS Root: Hyperlocal vs NSEC Caching <https://www.potaroo.net/ispcol/2019-04/root.html>)

Hyperlocal DNS abseits von root Zone

- **DNS Open Zone Data**
  - Estonia
  - France
  - Slovakia
  - Switzerland
  - Sweden and Niue
- **Sinnhaftigkeit?**
  - Zuverlässigkeit der AXFRs
  - Größe der Zonen ca. 5 GB

(DNS open zone data <https://jpmens.net/2021/05/18/dns-open-zone-data/>)

Einsatz eines Hyperlocal root DNS

- **Empfehlung: Netze mit Endbenutzern/-Geräten**
  - Access Netze (z.B. WLAN)
  - Browser-Sessions
  - unkontrollierte Abfragen an den DNS
- **eher nicht: Netze mit Servern & Applikationen**
  - Netze mit Server & Applikationen
  - kontrollierte Abfragen an den DNS
  - Risiko-Minimierung, dass root Zone nicht zur Verfügung steht.

Vielen Dank!

OFFEN FÜR FRAGEN & DISKUSSION