Alibaba Cloud
COMPUTING FOR VALUE BEYOND COMPUTATION

Who Forged My DNS Answer?

From a Real DNS Hijacking Case

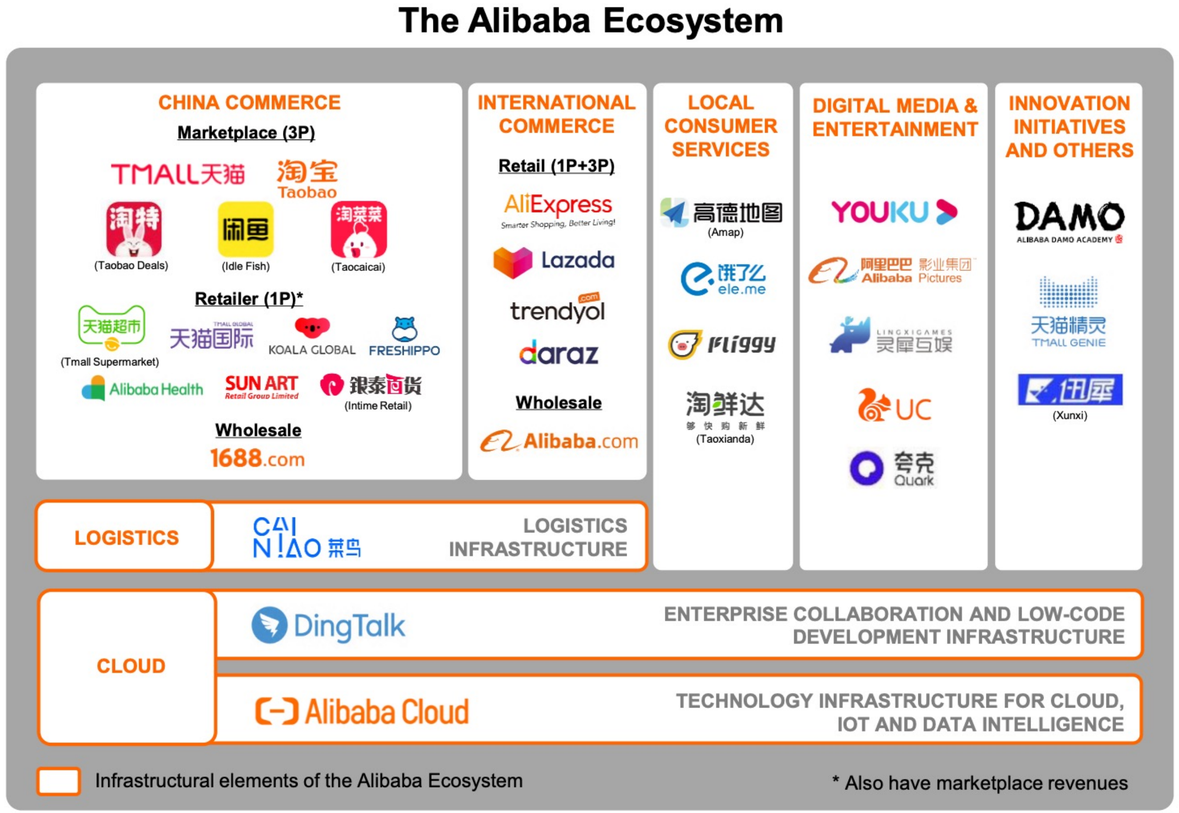
Linjian (Davey) Song

03/2024

Brief Introduction on Alibaba and DNS

Alibaba Cloud

Alibaba Group's MISSION IS TO MAKE IT EASY TO DO BUSINESS ANYWHERE



Alibaba Cloud DNS is a highly available and scalable Domain Name System (DNS) that provides managed authoritative for both public zones and private managed DNS zones

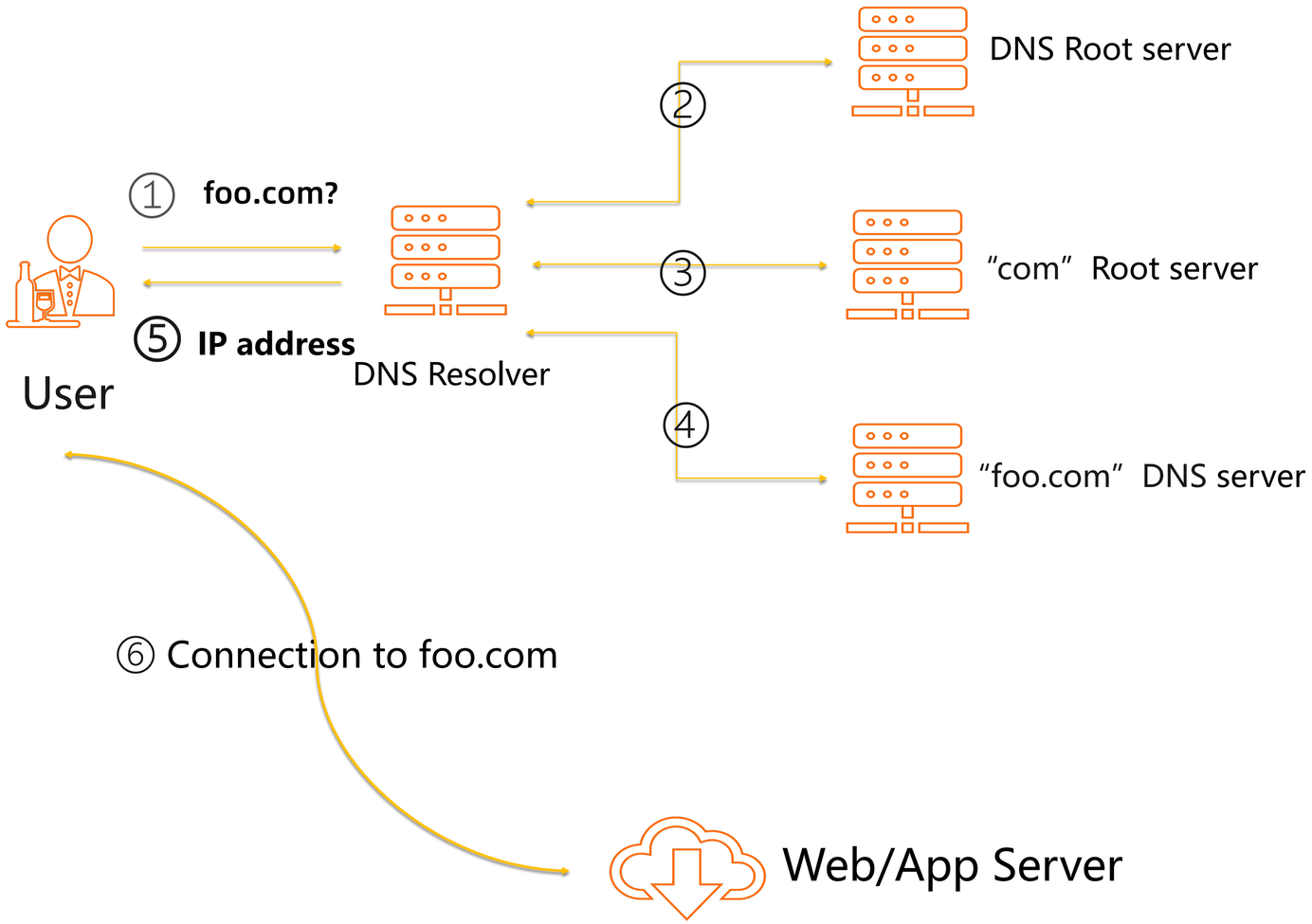



The Skyscraper and the base

- A solid and stable base is a matter most for the building
- Complicated structures and reinforced concrete with steel bars


Alibaba Cloud
DNS is the Key part of
Modern Internet Infrastructure

DNS Resolution

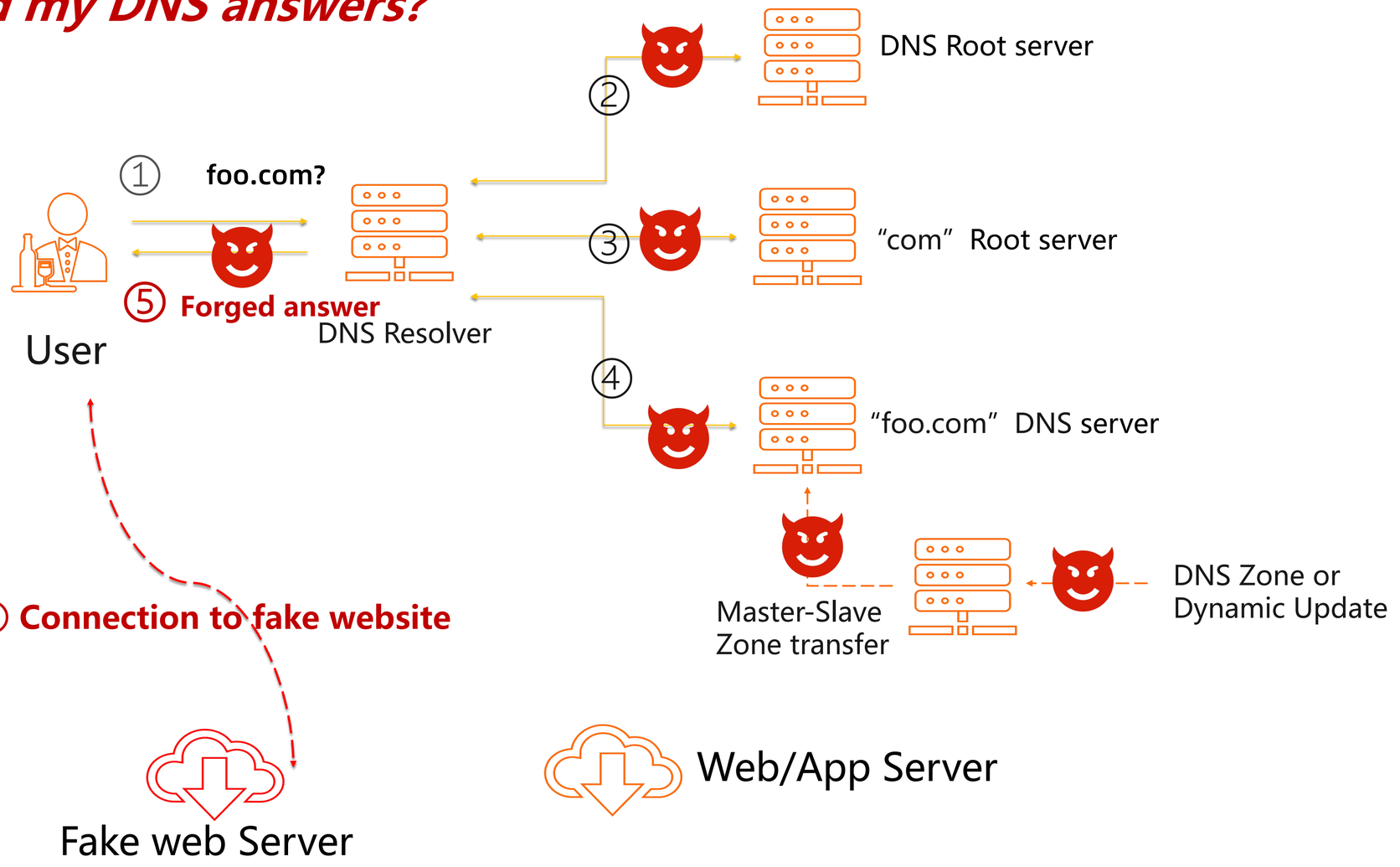


Troubleshooting DNS is very difficult

Alibaba Cloud

Who forged my DNS answers?

DNS Hijacking



A DNS Hijacking Real Case

Alibaba Cloud

DNS Hijacking Reproducing

- Probe
- Edit hosts file

DNS Hijacking Troubleshooting

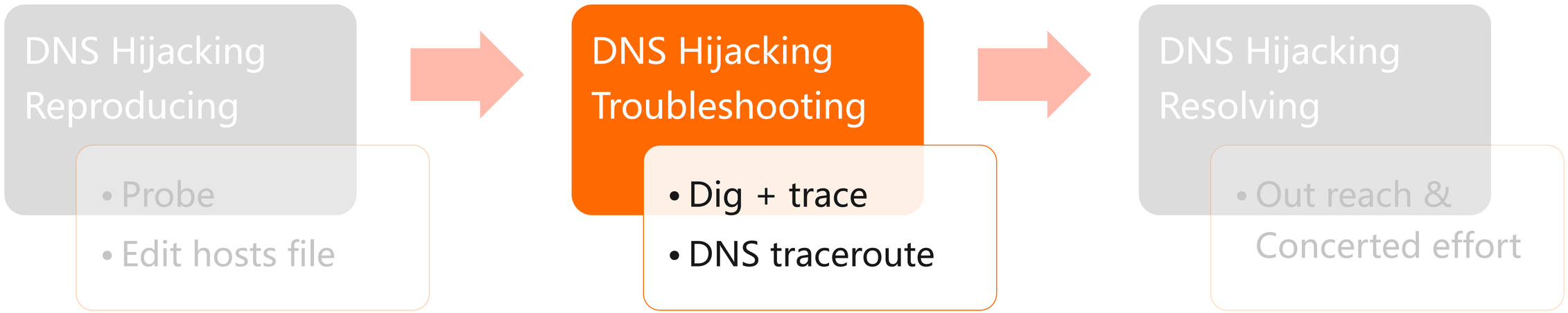
- Dig + trace
- DNS traceroute

DNS Hijacking Resolving

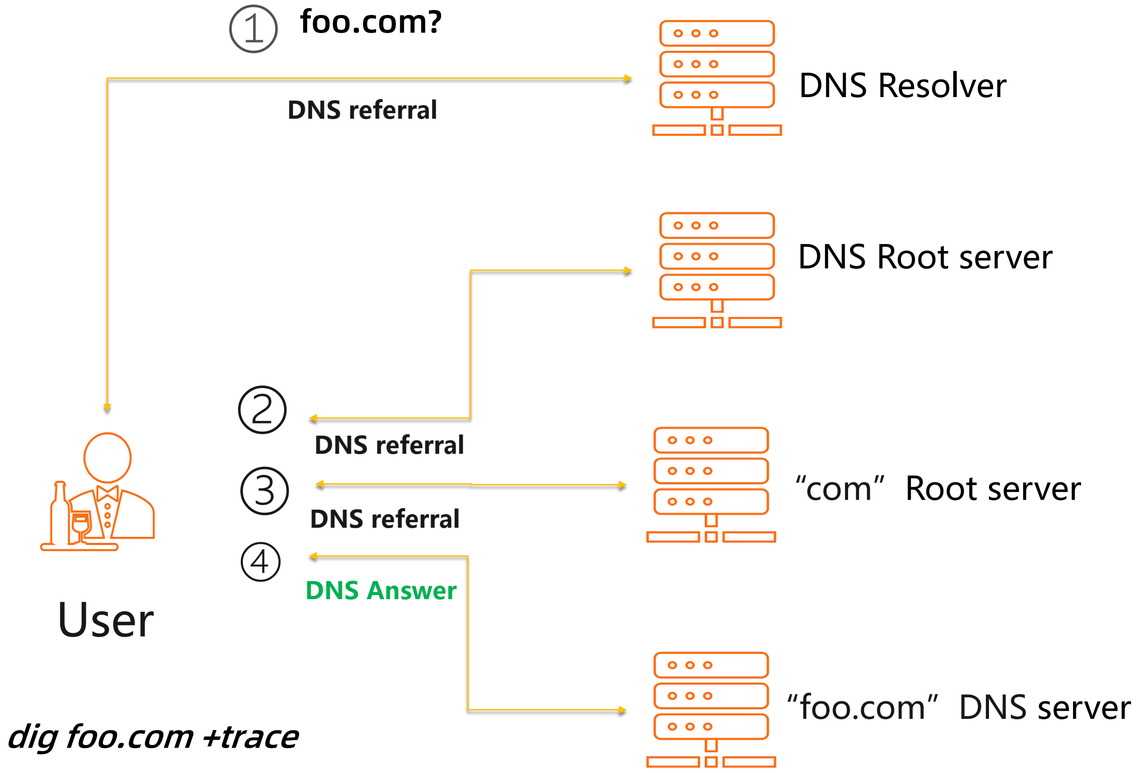
- Out reach & Concerted effort

DNS Hijacking Real Case

Alibaba Cloud

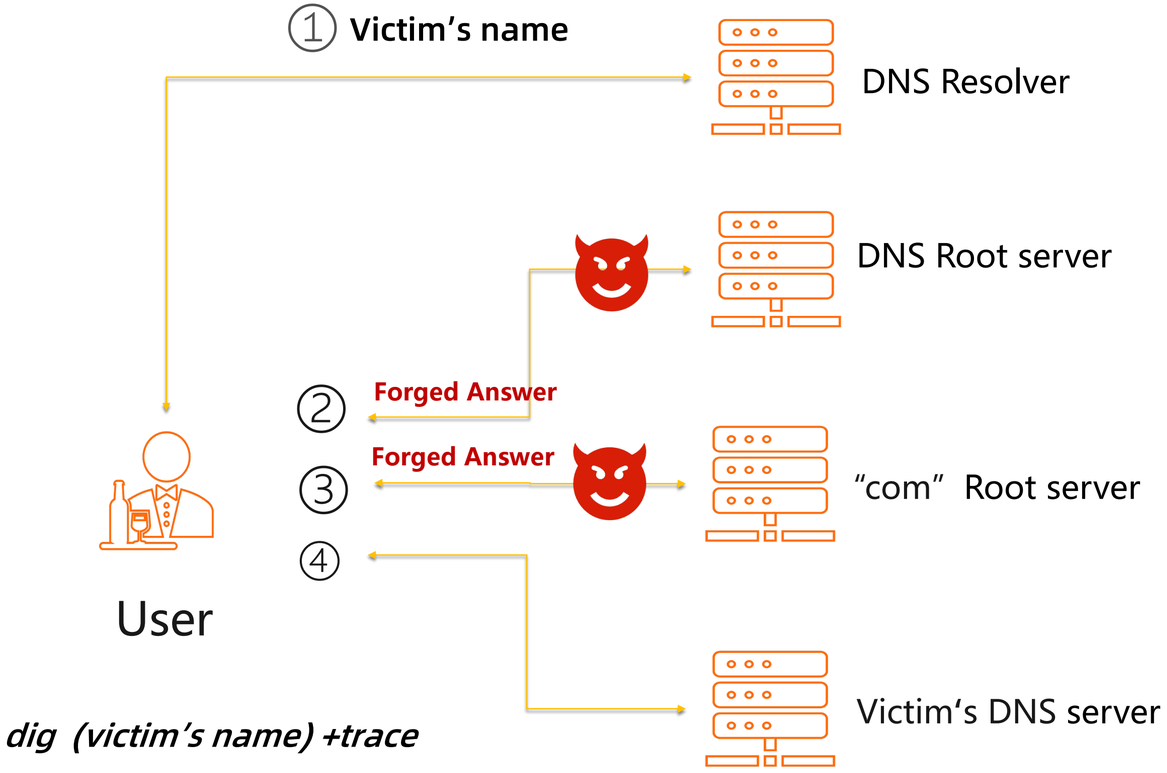


Dig +trace Command




```
songlinjian@U-93JXQXQY-2322 ~ % dig foo.com +trace

; <<>> DiG 9.10.6 <<>> foo.com +trace
;; global options: +cmd
.                       475061  IN      NS      a.root-servers.net.
.                       475061  IN      NS      b.root-servers.net.
.                       475061  IN      NS      c.root-servers.net.
.                       475061  IN      NS      d.root-servers.net.
.                       475061  IN      NS      e.root-servers.net.
.                       475061  IN      NS      f.root-servers.net.
.                       475061  IN      NS      g.root-servers.net.
.                       475061  IN      NS      h.root-servers.net.
.                       475061  IN      NS      i.root-servers.net.
.                       475061  IN      NS      j.root-servers.net.
.                       475061  IN      NS      k.root-servers.net.
.                       475061  IN      NS      l.root-servers.net.
.                       475061  IN      NS      m.root-servers.net.
.                       43061   IN      RRSIG   NS 8 0 518400 20240401050000 20240319040
000 30903 . Xg2ZlKeGlqABWOFRP6FDhvsBBIIWCb9ptHlwzkKhel3EHxdihT17YQYG fvFAPWJjPnWcbJlQeHw
rScVocUVEfDAKl85NLe/B+OUvjHw2bxjxSB0v sw7Pjp25emTPINH+dsGrzO23QB9N1hBUXNFbIp6h0wqY4Kfp1b
Hn1Op/ Sx6699J+VX0zQuTuJgs4x0TBuvPx1DGtvglHd0jJ10Dwno/X+lKWqeLy ZvSCkimA6x5WsTwwUtAm+Y2K
//nfx+jjHbzvB4NMASUTnnB2yEv6Q7e4 QdWDdJpYFfYaKlBBm62UkWLMIkJKbXqqoPv/H5+kQC2G27inzsIz9SM
D e24kug==
;; Received 747 bytes from 192.168.200.72#53(192.168.200.72) in 92 ms

com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    86400   IN      DS      19718 13 2 8ACBB0CD28F41250A80A491389424
D341522D946B0DA0C0291F2D3D7 71D7805A
com.                    86400   IN      RRSIG   DS 8 1 86400 20240401200000 202403191900
00 30903 . 3ed0I4ZvapH7crbNHXZENoCacs4oK2AxoAFWWlOdo8AjZCkwTZeO4L/z lbndTh1GwMfHPBQCd4ab
qSGWUByMKs+ELM3IdalOvjJthRbYaCyTDMKU 8gtfx71heN43fcDDeH4jbJUR9nMOCX2GqCb5P1Omf/9r1g7KENs
bcZGT YUF4ZzQCZbHloYltrH9bNxb0GNVkt01SiGKe3QEmuh0AvNYSzK9Ricqb 7HksJppp8Eu9FVWGPOy+L3LOr
tShklx3IrhWrDTezHP47ZzC/tXz3SHe AUClGdIt9t+MDwS5uZfhq5qAQSOI11/RQTysB1oN1ohFbn5W269X17rT
TyCJFQ==
;; Received 1167 bytes from 192.33.4.12#53(c.root-servers.net) in 165 ms

foo.com.                172800  IN      NS      ns1.digimedia.com.
foo.com.                172800  IN      NS      ns2.digimedia.com.
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN NSEC3 1 1 0 - CK0Q2D6NI4I7EQH8NA30NS61O48
UL8G5  NS SOA RRSIG DNSKEY NSEC3PARAM
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN RRSIG NSEC3 13 2 86400 20240325042456 202
40318031456 4534 com. mmvYdRZlvwMKhXvJLnrGnP1KI/gfF+oe3osWNb3iuZkdPxp3u9jmmn4L TlD4bvIgr
bhMm74YV2Z3Sp+iLrLOtQ==
EVHDNEB8496UATLQFALGNA815P432N23.com. 86400 IN NSEC3 1 1 0 - EVHE6HKBPNHPNF427CCGT7VU2OO
UN2QP  NS DS RRSIG
EVHDNEB8496UATLQFALGNA815P432N23.com. 86400 IN RRSIG NSEC3 13 2 86400 20240323045110 202
40316034110 4534 com. Yc8bASpmbWuxQoHJ3+RpfF/r0t5sT61Nih4jWj8KjlfQVEamXBhugVt1 B06kVem/1
CXddN/4dPm4V8xwissplg==
;; Received 471 bytes from 192.5.6.30#53(a.gtld-servers.net) in 176 ms

foo.com.                600     IN      A       34.206.39.153
foo.com.                600     IN      NS      ns1.digimedia.com.
foo.com.                600     IN      NS      ns2.digimedia.com.
;; Received 130 bytes from 23.21.243.119#53(ns2.digimedia.com) in 269 ms
```

Dig +trace Command



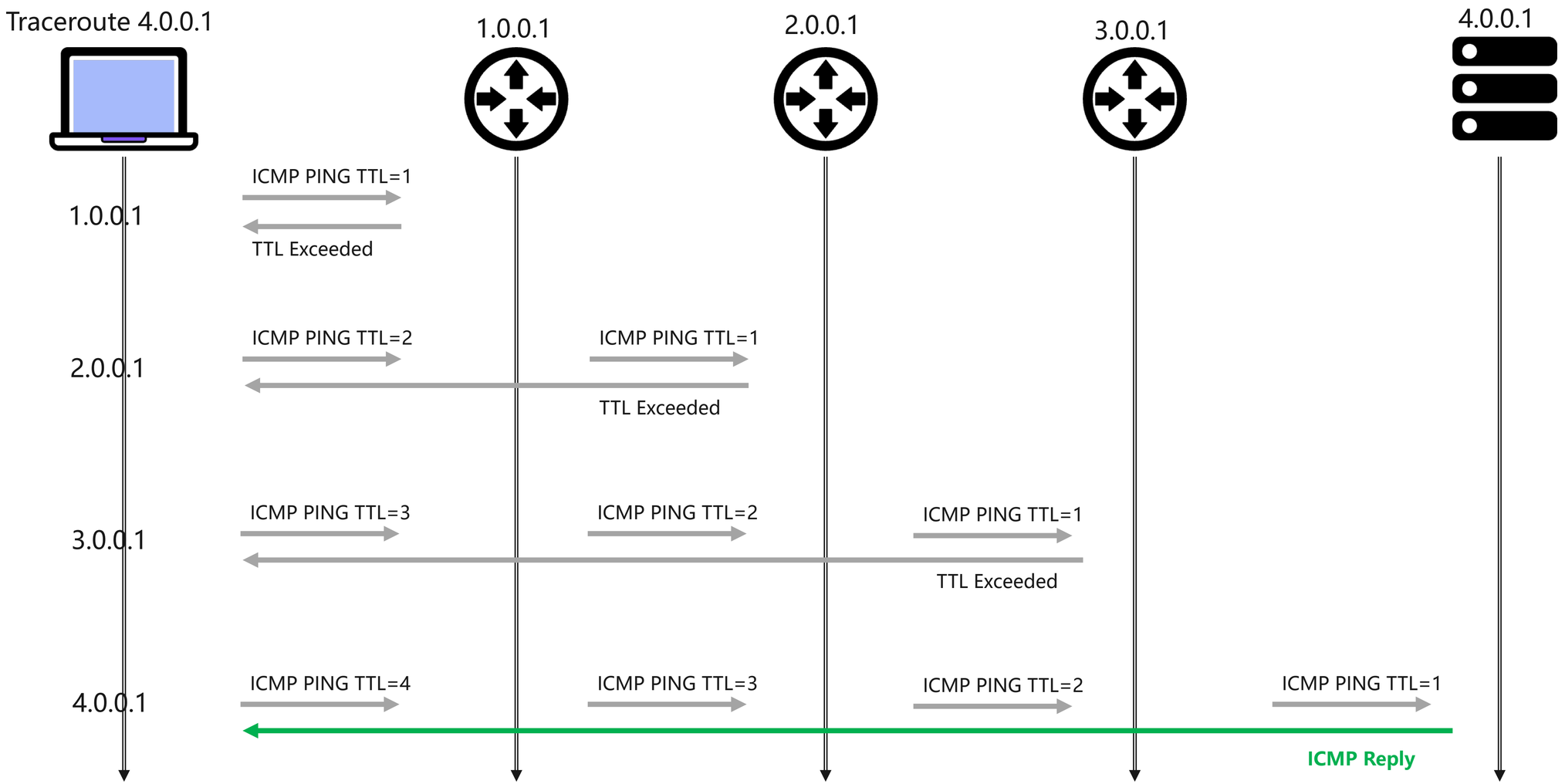
What happened in between ?

Who forged the answer?

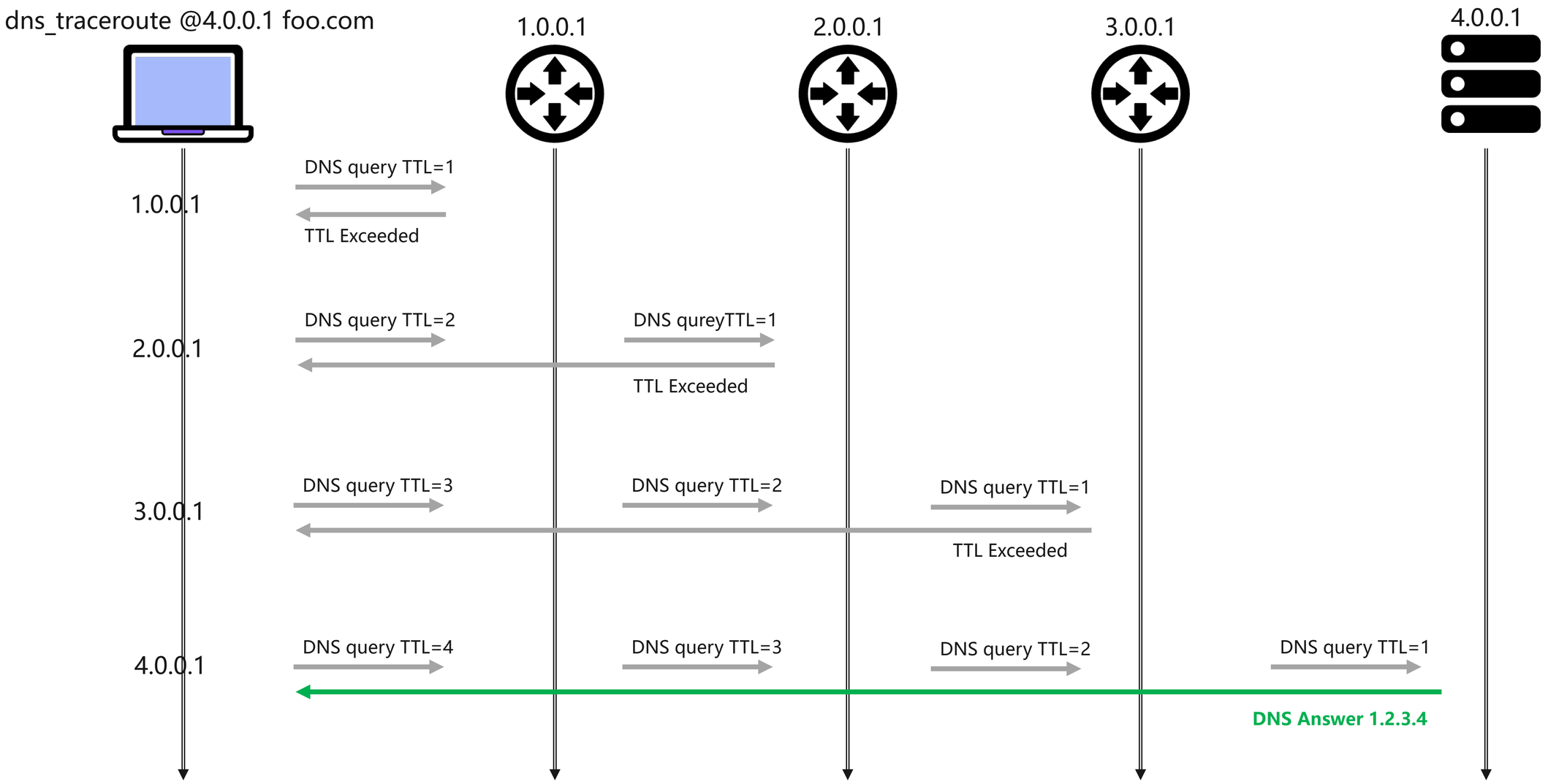
```
; <<>> DiG 9.11.19-RedHat-9.11.10-20200601113814.alios7 <<>> service.[redacted].com +trace
;; global options: +cmd
.                       2332    IN      NS      m.root-servers.net.
.                       2332    IN      NS      f.root-servers.net.
.                       2332    IN      NS      i.root-servers.net.
.                       2332    IN      NS      l.root-servers.net.
.                       2332    IN      NS      d.root-servers.net.
.                       2332    IN      NS      a.root-servers.net.
.                       2332    IN      NS      g.root-servers.net.
.                       2332    IN      NS      e.root-servers.net.
.                       2332    IN      NS      h.root-servers.net.
.                       2332    IN      NS      c.root-servers.net.
.                       2332    IN      NS      j.root-servers.net.
.                       2332    IN      NS      k.root-servers.net.
.                       2332    IN      NS      b.root-servers.net.
;; Received 239 bytes from 223.5.5.5#53(223.5.5.5) in 6 ms

service.showself.com.   7200    IN      A       156.251.239.186
;; Received 54 bytes from 192.5.5.241#53(f.root-servers.net) in 80 ms
```

```
; <<>> DiG 9.11.19-RedHat-9.11.10-20200601113814.alios7 <<>> service.[redacted].com +trace
;; global options: +cmd
.                       2821    IN      NS      a.root-servers.net.
.                       2821    IN      NS      b.root-servers.net.
.                       2821    IN      NS      c.root-servers.net.
.                       2821    IN      NS      d.root-servers.net.
.                       2821    IN      NS      e.root-servers.net.
.                       2821    IN      NS      f.root-servers.net.
.                       2821    IN      NS      g.root-servers.net.
.                       2821    IN      NS      h.root-servers.net.
.                       2821    IN      NS      i.root-servers.net.
.                       2821    IN      NS      j.root-servers.net.
.                       2821    IN      NS      k.root-servers.net.
.                       2821    IN      NS      l.root-servers.net.
.                       2821    IN      NS      m.root-servers.net.
;; Received 239 bytes from 223.5.5.5#53(223.5.5.5) in 6 ms

com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    86400   IN      DS      30909 8 2 E2D3C916F6DEEAC73294E8268FB5885
com.                    86400   IN      RRSIG   DS 8 1 86400 20231210220000 20231127210000
bJnJo+TdCx4FnUJV3ICYDJVCsuchIdWnrcx/saWjKA1 18w6y4urH3dE2ulRP+xjbRiC5yjMt8UF5IFD5xdti71w9
;; Received 1211 bytes from 192.112.36.4#53(g.root-servers.net) in 605 ms

;; expected opt record in response
service.[redacted].com. 7200    IN      A       156.251.239.186
;; Received 54 bytes from 192.33.14.30#53(b.gtld-servers.net) in 139 ms
```

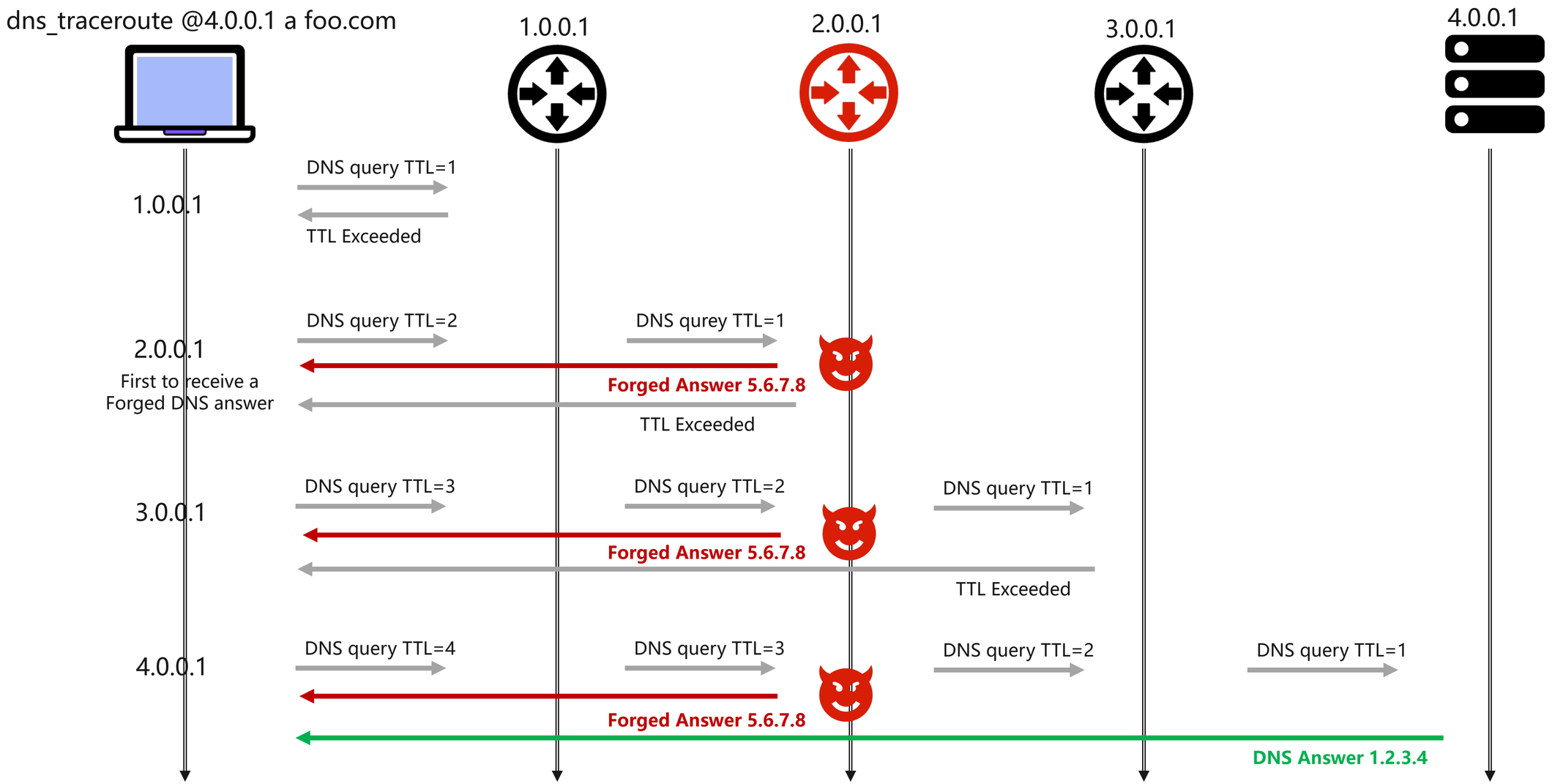
Traceroute Command (Normal response)



DNS Traceroute (Normal response)



DNS Traceroute (Forged response)



Finally, the client receives 3 forged DNS answers and 1 true DNS answer

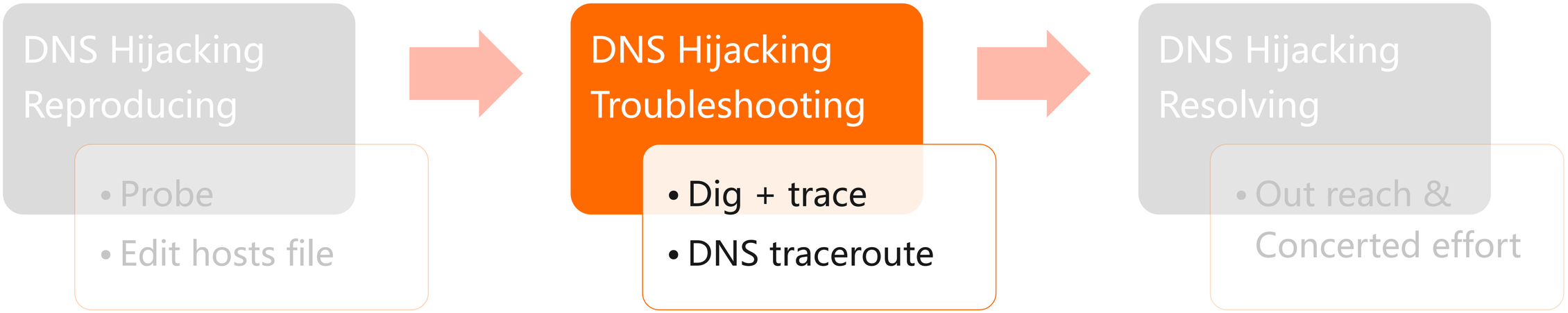
On-Path Interception Example

DNS-traceroute one victim’ s name @root server

```
listen icmp on any
listen dns on any
Sending package done,Parsing now...
Result:
1   10.123.124.62 (10.123.124.62)  9.528303ms
    10.123.120.62 (10.123.120.62)  9.377251ms
2   10.123.120.105 (10.123.120.105)  9.22598ms
    10.123.120.125 (10.123.120.125)  19.067548ms
    10.123.128.129 (10.123.128.129)  9.038707ms
3   11.88.173.145 (11.88.173.145)  8.768482ms
    11.88.173.129 (11.88.173.129)  8.680531ms
    11.88.173.237 (11.88.173.237)  8.453801ms
4   117.49.34.205 (117.49.34.205)  8.366074ms
    117.49.34.201 (117.49.34.201)  8.215159ms
    117.49.34.145 (117.49.34.145)  8.02975ms
5   117.49.34.226 (117.49.34.226)  17.909954ms
    116.251.112.109 (116.251.112.109)  17.600966ms
6   10.102.155.118 (10.102.155.118)  17.249149ms
    45.112.216.106 (45.112.216.106)  17.068307ms
7   106.39.194.1 (106.39.194.1)  17.823159ms
    106.38.196.25 (106.38.196.25)  17.687193ms
8   36.110.245.201 (36.110.245.201)  17.268574ms
10  202.97.57.157 (202.97.57.157)  36.658458ms
11  202.97.90.53 (202.97.90.53)  36.246025ms
    202.97.39.37 (202.97.39.37)  36.109253ms
    202.97.39.37 (202.97.39.37)  45.944239ms
12  202.97.43.126 (202.97.43.126)  65.46827ms
13  203.215.236.74 (203.215.236.74)  65.28509ms
    203.215.236.66 (203.215.236.66)  65.135992ms
    203.215.236.66 (203.215.236.66)  64.928742ms
14  210.173.176.242 (210.173.176.242)  64.81219ms
    210.173.176.242 (210.173.176.242)  64.637386ms
    210.173.176.242 (210.173.176.242)  64.473578ms
Received DNS response on ttl 10
;; opcode: QUERY, status: NOERROR, id: 31
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;[redacted].com.    IN      A

;; ANSWER SECTION:
[redacted].com.     60      IN      A       8.7.198.46

The following icmp time out messages match the Dns Response:
10:    202.97.57.157  36.658458ms
```

Received a forged answer and pinpoint the IP who forged it

Troubleshooting Result



- ✓ dig + trace finds specific DNS query to root/.com servers received random, forged answers which will be cached by resolvers
- ✓ dns traceroute tool prints **the path of the query forwarded** and pinpoints **IP address who forge the answer**
- ✓ dns traceroute tool also tell us it is a on-path interception. The Hijacking device responses with a forged answer in advance to the real one

WWW.ALIYUN.COM