

INTERNET 
STIFTELSEN

DNS-kurs 2024



DNS under huven

- DNS-headers
 - Statuskoder
 - Flaggor
- Hur ser verkligheten ut?
 - Hur många resolvers är för mycket?
 - Vad kan ställa till det?
- Felsökning
 - Vad behöver man tänka på?

Tillbaka till DiG

```
; <<>> DiG 9.10.6 <<>> iis.se a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42009
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::, udp: 4096
;; QUESTION SECTION:
iis.se.                IN      A

;; ANSWER SECTION:
iis.se.                77      IN      A      159.253.30.216

;; Query time: 112 msec
;; SERVER: 172.20.10.1#53(172.20.10.1)
;; WHEN: Wed Jul 15 15:29:58 CEST 2020
;; MSG SIZE rcvd: 51
```


Tillbaka till DiG

```
; <<>> DiG 9.10.6 <<>> iis.se a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42009
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::, udp: 4096
;; QUESTION SECTION:
;iis.se.                IN      A

;; ANSWER SECTION:
iis.se.                 77      IN      A      159.253.30.216

;; Query time: 112 msec
;; SERVER: 172.20.10.1#53(172.20.10.1)
;; WHEN: Wed Jul 15 15:29:58 CEST 2020
;; MSG SIZE rcvd: 51
```


Flaggor

Flagga	Om satt (bitvärde = 1)
QR	Response (om satt till 0 = Query)
AA	Authoritative Answer
TC	Truncated. (hela svaret fick inte plats)
RD	Recursion Desired (klienten ber NS agera resolver)
RA	Recursion Available (NS <u>kan</u> agera resolver)
(AD)	Authentic Data (kontrollera(d) data)
(CD)	Checking Disabled (kontrollera inte data)
(DO)	DNSSEC Data OK (klienten kan kontrollera själv)

Statuskoder

RCODE code	RCODE name	Vad det betyder
0	NOERROR	Frågan gick bra. Det behöver dock inte betyda att den efterfrågade informationen fanns
1	FORMERR	Servern kan inte tolka formatet på frågan.
2	SERVFAIL	Servern saknar eller har trasig data.
3	NXDOMAIN	Domännamnet som efterfrågas finns inte (som någon post)
4	NOTIMP	Servern stödjer inte den typen av fråga
5	REFUSED	Servern har en policy som hindrar svar.

NOERROR

```
; <<>> DiG 9.10.6 <<>> www.iis.se a @ns.nic.se
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19369
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 5
;; WARNING: recursion requested but not available
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.iis.se.                IN      A
```

```
;; ANSWER SECTION:
www.iis.se.                 60      IN      A      159.253.30.216
```



NOERROR + nodata

```
; <<>> DiG 9.10.6 <<>> www.iis.se mx @ns.nic.se +multi
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38587
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
```

```
;; QUESTION SECTION:
; www.iis.se.          IN MX
```

```
;; AUTHORITY SECTION:
iis.se.                3600 IN      SOA ns.nic.se. hostmaster.iis.se. (
                        1595416201 ; serial
                        14400      ; refresh (4 hours)
                        3600       ; retry (1 hour)
                        1814400    ; expire (3 weeks)
                        14400      ; minimum (4 hours)
                        )
```



NOERROR + nodata (referral)

```
; <<>> DiG 9.10.6 <<>> www.iis.se a @a.ns.se
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34342
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 5
;; WARNING: recursion requested but not available
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
```

```
;; QUESTION SECTION:
;www.iis.se.                IN      A
```

```
;; AUTHORITY SECTION:
iis.se.      86400 IN      NS      i.ns.se.
iis.se.      86400 IN      NS      ns3.nic.se.
iis.se.      86400 IN      NS      ns.nic.se.
```



NXDOMAIN

```
; <<>> DiG 9.10.6 <<>> vvv.iis.se a @ns.nic.se +multi
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 38587
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096

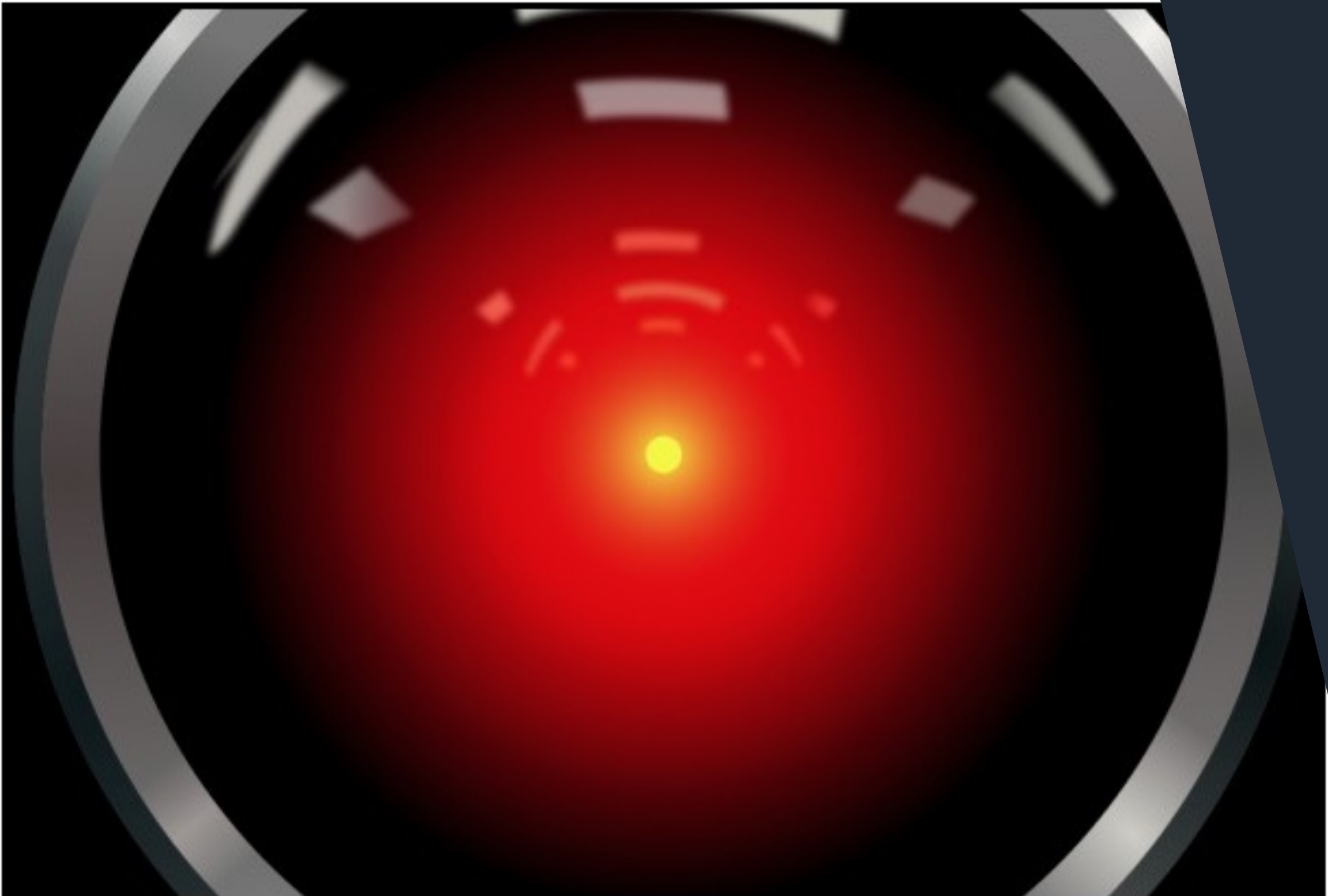
;; QUESTION SECTION:
; vvv.iis.se.          IN A

;; AUTHORITY SECTION:
iis.se.                3600 IN      SOA ns.nic.se. hostmaster.iis.se. (
                        1595416201 ; serial
                        14400   ; refresh (4 hours)
                        3600    ; retry (1 hour)
                        1814400 ; expire (3 weeks)
                        14400   ; minimum (4 hours)
                        )
```


REFUSED

```
; <<>> DiG 9.10.6 <<>> www.iis.se a @213.50.29.170
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 54213
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.iis.se.                IN      A
```



I'M SORRY, DAVE.
I'm afraid I can't do that.

DNSSEC

DNS Security Extensions

Vad är DNSSEC?

- “Skalskydd” för en domän
- Digital *signering* av DNS-data
- Ser till att DNS-datan kommer från dataägaren (source of truth) och är oförvanskad
- Är en förutsättning för andra säkerhetsmekanismer, t.ex. DANE
- OBS! Krypterar *inte* DNS-trafiken

Nya pekartyper

- RRSIG - Resource Record Signature
- DNSKEY - Kryptografisk nyckel
- DS - Delegation Signer
- NSEC - Next Secure Record
- NSEC3 - Hashad variant av NSEC
- NSEC3PARAM - Parametrar för NSEC3 hash



NSEC vs NSEC3

- NSEC
 - Underlättar zonewalking
 - Ej resurskrävande

NSEC3

- Security by obscurity
- Försvårar zonewalking, något.
- Något mer resurskrävande
- Om felkonfigurerad, mycket resurskrävande



DIG

```
; <<>> DiG 9.10.6 <<>> @1.1.1.1 www.iis.se +dnssec +qr +multi
; (1 server found)
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21601
;; flags: rd ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.iis.se.                IN A

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21601
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;www.iis.se.                IN A

;; ANSWER SECTION:
www.iis.se.                57 IN RRSIG A 5 3 60 (
                           20200805122001 20200726122001 5601 iis.se.
                           Ggw/0ovH/OEadu+6XYsuz6lU/uIO4n0H46ZB6OhmYpMM
                           7gi63wlZDIAn8lifp0ugcckL7AVB8lINOCt3RI9Tms54
                           s2axbDdiISHj9az4+raYAg+RYolAwYSkAIF2gj6vbDYt
                           uBaOjnhtfS1QGwvbqu4WNaEC2aJxVWOxTiZeWwl=
                           )
www.iis.se.                57 IN A 159.253.30.216
```




```
; <<>> DiG 9.10.6 <<>> iis.se dnskey +multi
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32298
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
;; QUESTION SECTION:
;iis.se.                IN DNSKEY

;; ANSWER SECTION:
iis.se.                 3595 IN DNSKEY 256 3 5 (
    AwEAAfOj4AyE1rcJtinMhEBOOuks0upRqKdhdVCYgMPc
    6f9ZGxf9DftnQNrtNEyBlit0Qxr3zPJG29zpr7mtjXCqO
    GNhZLJPduLqtKE6tmOLILkU+Ujv4Z0NNcjmsekPkyHQi
    dYiEyQNci01b9e1O58EddvJigzclgLqM6Jx2ALGgD6AP
    ) ; ZSK; alg = RSASHA1 ; key id = 18117

iis.se.                 3595 IN DNSKEY 257 3 5 (
    AwEAAcq5u+qe5VibnyvSnGU20panweAk2QxflGVuVQhz
    QABQV4SIdAQs+LNVHF61lcxe504jhPmjeQ656X6t+dHp
    Rz1DdPO/ukclITjIRoJHqS+XXyL6gUluZoDU+K6vpxkG
    Jx5m5n4boRTKCTUAR/9rw2+IQRRTtb6nBwsC3pmf9IIJ
    QjQMb1cQTb0UO7fYgXDZIYVul2LwGpKRrMJ6UI1nepkS
    xTMwQ4H9iKE9FhqPelpzU9dnXGtJ+ZCx9tWSZ9VsSLWB
    JtUwoE6ZfloF1ioqqxfGI9JV1/6GkDxo3pMN2edhkp8a
    qoo/R+mrJYi0vE8jbXvhZ12151DywuSxbGjAlxk=
    ) ; KSK; alg = RSASHA1 ; key id = 18937
```




```
; <<>> DiG 9.10.6 <<>> iis.se ds +multi
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25379
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 4096
;; QUESTION SECTION:
;iis.se.                IN DS

;; ANSWER SECTION:
iis.se.                 710 IN DS 18937 5 2 (
                        B5C422428DEA4137FBF15E1049A48D27FA5EADE64D2E
                        C9F3B58A994A6ABDE543 )
iis.se.                 710 IN DS 18937 5 1 (
                        10DD1EFDC7841ABFDF630C8BB37153724D70830A )
```




```
; <<>> DiG 9.10.6 <<>> vvv.iis.se a +dnssec +multi @1.1.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 61092
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
; vvv.iis.se.                IN A

;; AUTHORITY SECTION:
iis.se.                3600 IN SOA ns.nic.se. hostmaster.iis.se. (
                        1597943701 ; serial
                        14400      ; refresh (4 hours)
                        3600       ; retry (1 hour)
                        1814400    ; expire (3 weeks)
                        14400      ; minimum (4 hours)
                        )
iis.se.                3600 IN RRSIG SOA 5 2 3600 (
                        20200830161501 20200820161501 18117 iis.se.
                        CiPvtoGYMOUPmSuCpY0A1WQMnMGxnUrxWNHMYwZ/fMaJ
                        iexs2Q2UULvewRTz3h33noEYLq6DkBp9tCMP7W2lvGoz
                        HHJ41/409FnF4H1CgGtC+pNohMqWsn/rjY36xvcf1uGs
                        YE55MXSg7P2xy+Sk1GGpycxaBpHqblvM2am6oVI= )
vpn2.iis.se.          14400 IN NSEC watcher.iis.se. A RRSIG NSEC
vpn2.iis.se.          14400 IN RRSIG NSEC 5 3 14400 (
                        20200830161501 20200820161501 18117 iis.se.
                        tpyOsU2FoOsXC/7f9j35dsfmBnf22ovB8946ZPwrKWrV
                        cqJsjtHra8BQBdYD9xCF13VxiysXYn3Fvb50lx8AIN4
                        qXfqroIMlk9AQdhtJJJoILFXbVsFs3qrH72N3GIOXI+kh
                        9JDxTQUkGKrWMIpcKZ5aGEQ9z3hbLj2JOU59/40= )
```



Kryptografiska signaturer

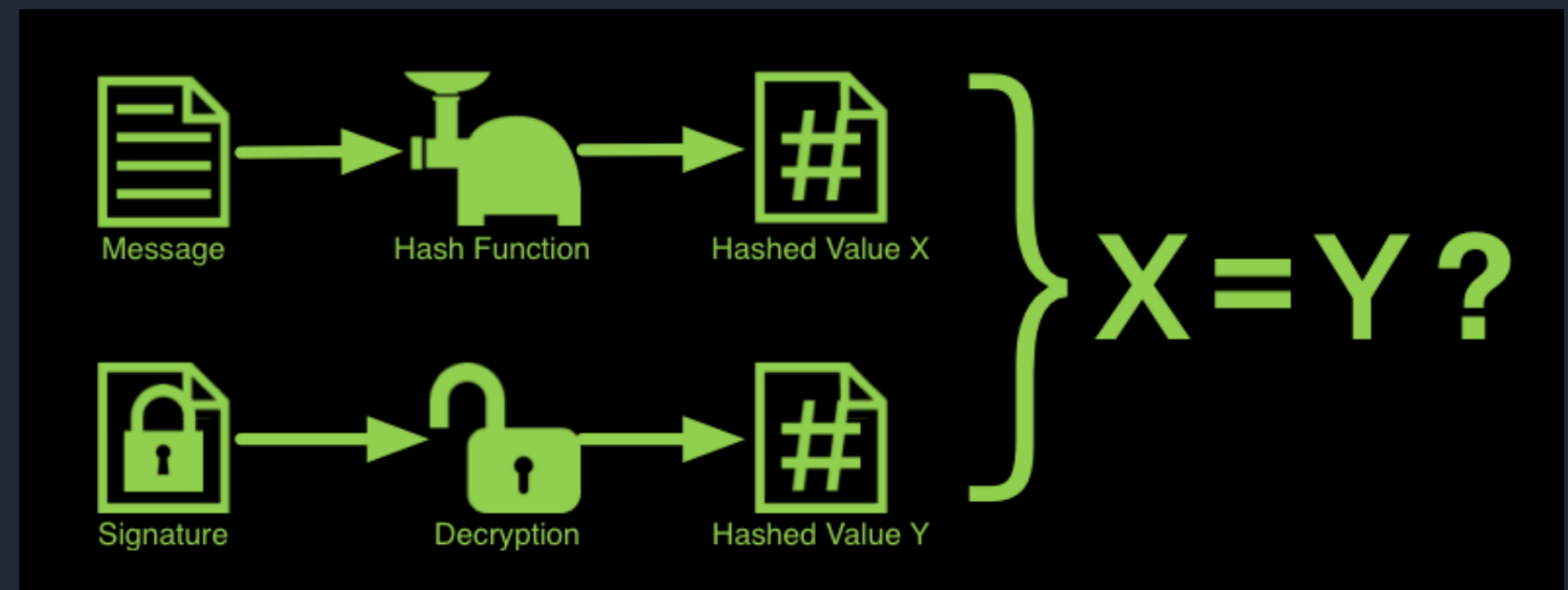
- Asymetrisk kryptering (PGP, SSH, TLS)
- Nyckelpar som genereras tillsammans
- En nyckel hålls hemlig, den andra sprids fritt (privat/publik)
- En nyckel *kan inte* dekryptera det den krypterat
- Endast *den andra* nyckeln i nyckelparet kan det

Kryptografiska signaturer

Generera:



Verifiera:



Nyttan med hash

Input

Digest

Fox

cryptographic
hash
function

DFCD 3454 BBEA 788A 751A
696C 24D9 7009 CA99 2D17

The red fox
jumps over
the blue dog

cryptographic
hash
function

0086 46BB FB7D CBE2 823C
ACC7 6CD1 90B1 EE6E 3ABC

The red fox
jumps over
the blue dog

cryptographic
hash
function

8FD8 7558 7851 4F32 D1C6
76B1 79A9 0DA4 AEFE 4819

The red fox
jumps over
the blue dog

cryptographic
hash
function

FCD3 7FDB 5AF2 C6FF 915F
D401 C0A9 7D9A 46AF FB45

The red fox
jumps over
the blue dog

cryptographic
hash
function

8ACA D682 D588 4C75 4BF4
1799 7D88 BCF8 92B9 6A6C

Föräldrason

DS

KSK

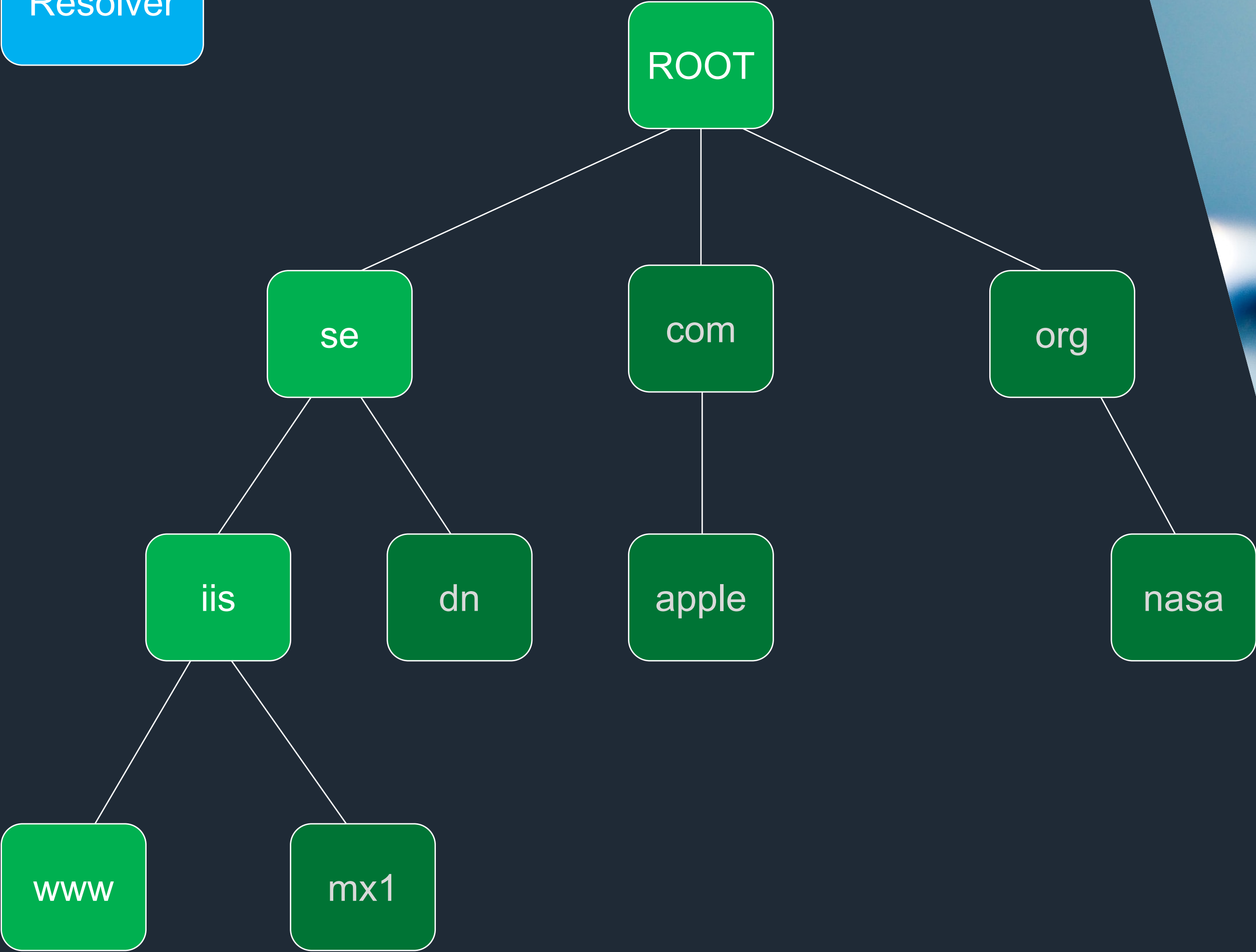
Barnzon

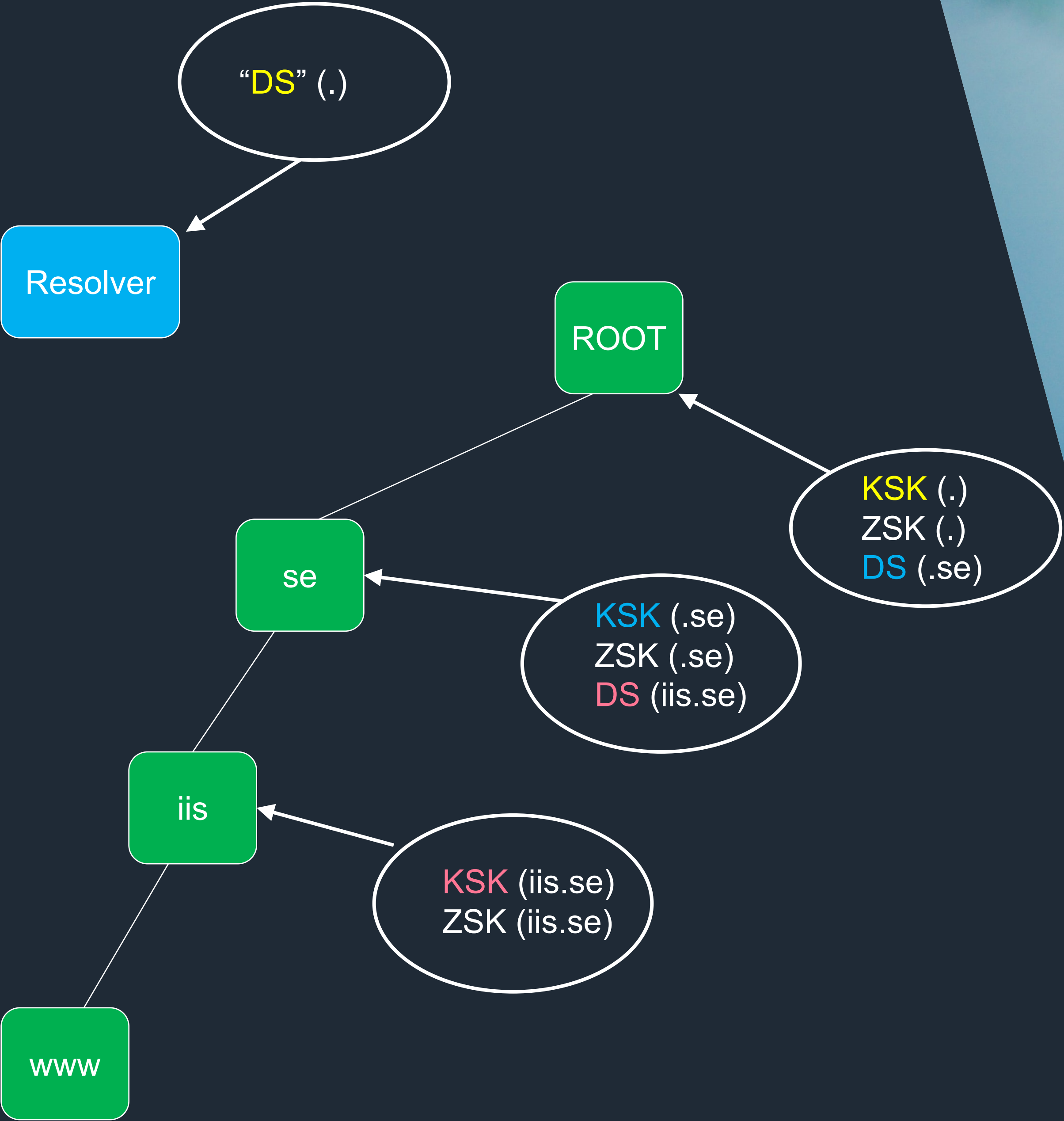
ZSK

Perake i zonen
(t.ex. en DS-post)



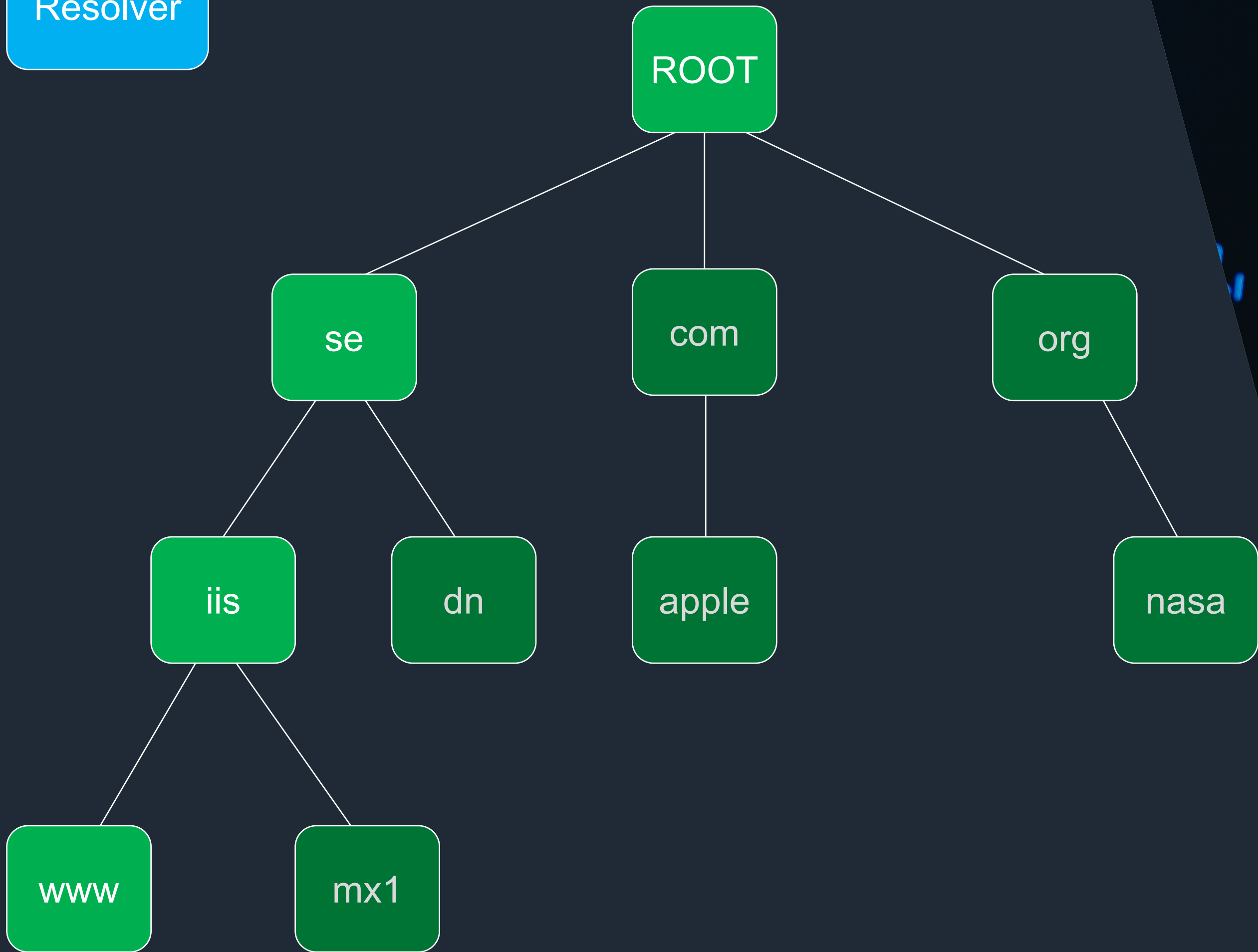
Resolver





www.iis.se?

Resolver



www.iis.se?

Resolver

ROOT

se

com

org

iis

dn

apple

nasa

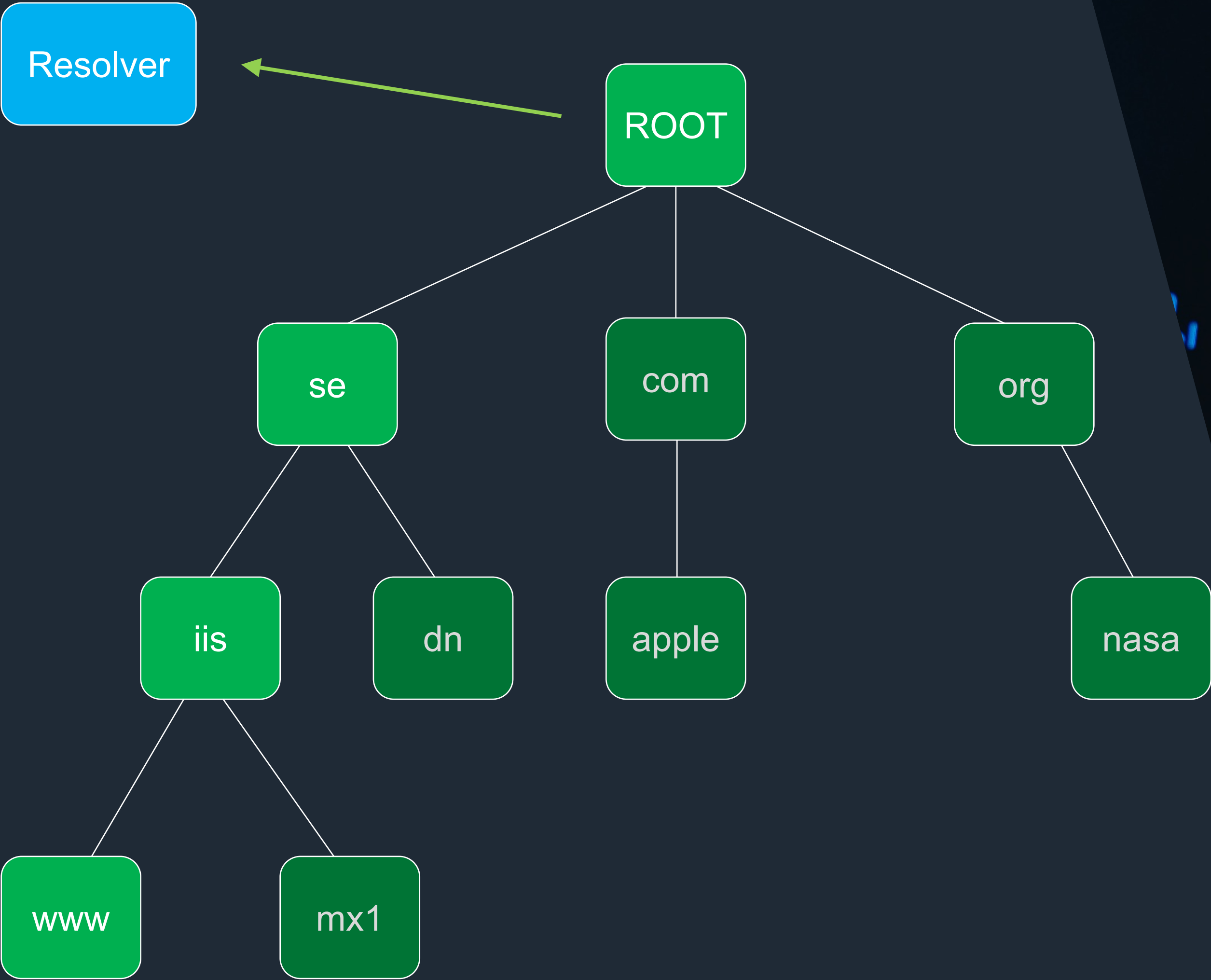
www

mx1



Utan DNSSEC

¯_ (ツ) _/¯



```
:: global options: +cmd
:: Got answer:
:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55630
:: flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 21
:: WARNING: recursion requested but not available

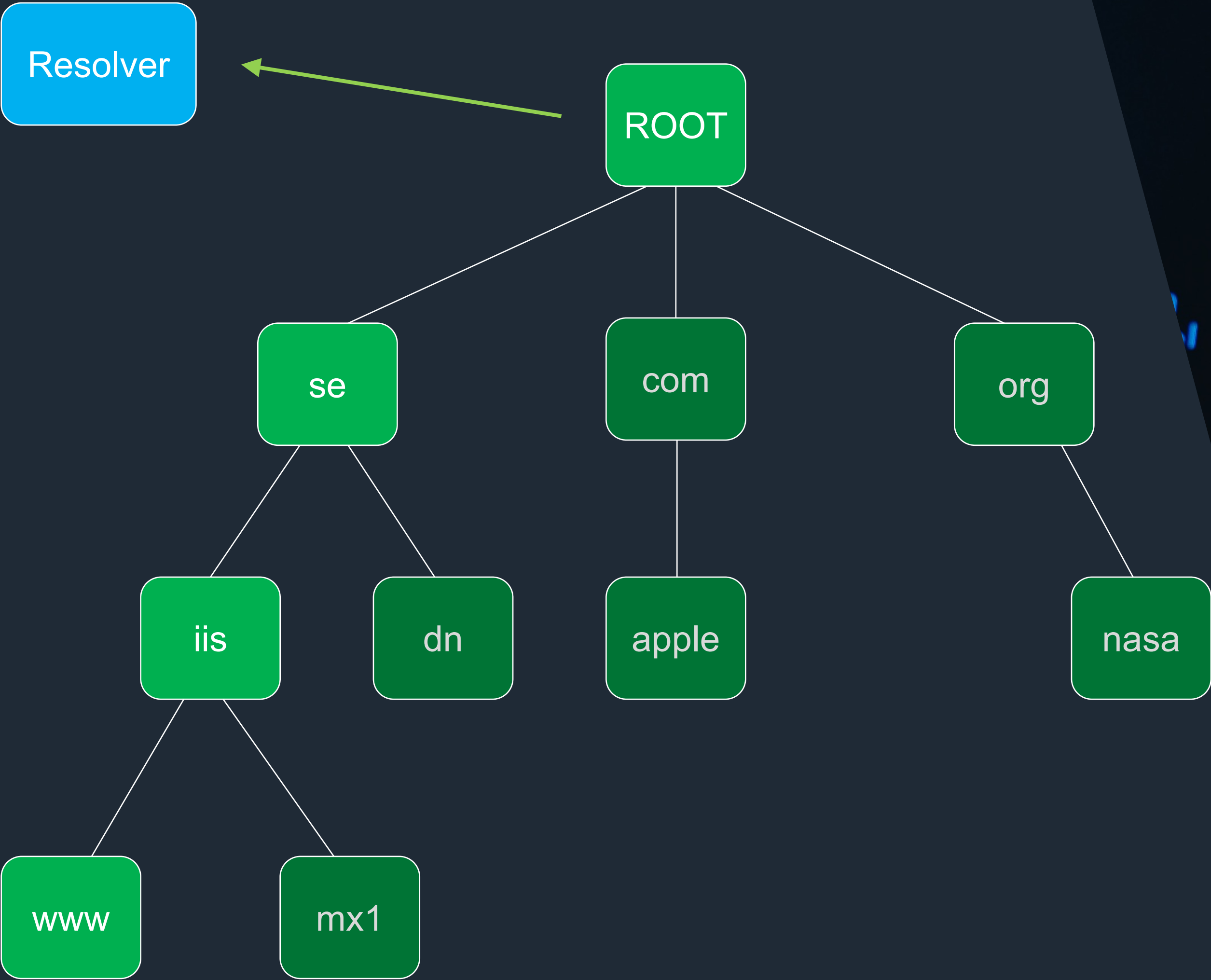
:: OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 1232
:: QUESTION SECTION:
;www.iis.se.          IN      A

:: AUTHORITY SECTION:
se.                  172800   IN      NS      a.ns.se.
se.                  172800   IN      NS      b.ns.se.
se.                  172800   IN      NS      c.ns.se.
...

:: ADDITIONAL SECTION:
a.ns.se.             172800   IN      A        192.36.144.107
b.ns.se.             172800   IN      A        192.36.133.107
c.ns.se.             172800   IN      A        192.36.135.107
...
a.ns.se.             172800   IN      AAAA     2a01:3f0:0:301::53
b.ns.se.             172800   IN      AAAA     2001:67c:254c:301::53
c.ns.se.             172800   IN      AAAA     2001:67c:2554:301::53
...
```


Med DNSSEC

¯_ (ツ) _/¯



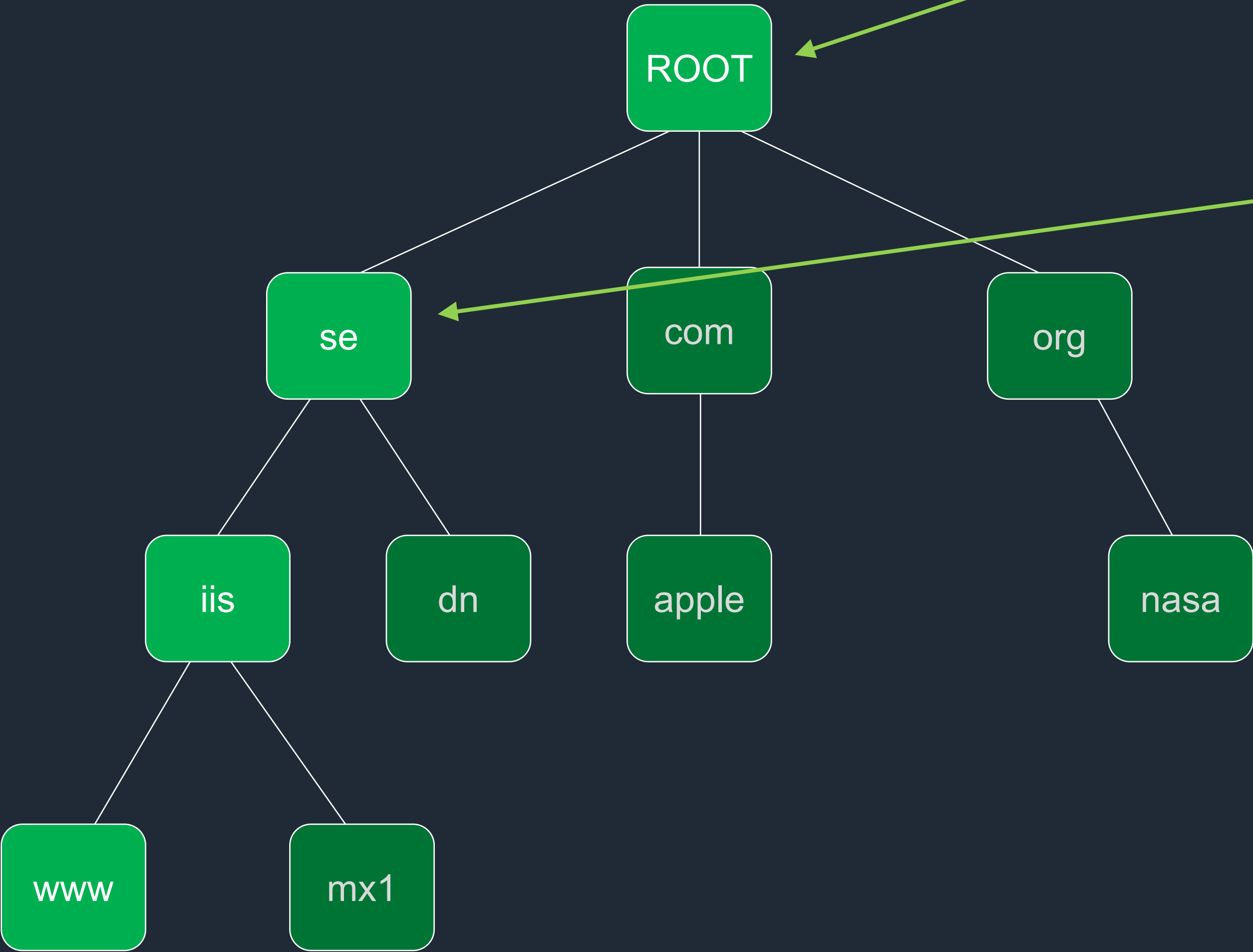
```
; <<>> DiG 9.10.6 <<>> @a.root-servers.net www.iis.se a +dnssec +multi
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26669
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 12, ADDITIONAL: 21
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.iis.se.          IN A

;; AUTHORITY SECTION:
se.                  172800 IN NS x.ns.se.
se.                  172800 IN NS y.ns.se.
se.                  172800 IN NS i.ns.se.
...
se.                  86400 IN DS 59407 8 2 (
                        67A8E06FCEFD9397F77F26C41ADE4EC142F299BCFA1
                        827F0EF8FD87F2F63022 )
se.                  86400 IN RRSIG DS 8 1 86400 (
                        20200927050000 20200914040000 46594 .
                        dakIVy9yYAfUgqHeCveKYJiD78TKb+fZqkTupVUITXGk
                        smJ+kCk1Kmv+ZpNR2ikvfrVxwwCcp5HCGW5yol8RZjtF
                        e1GdPxI+AxqwsZvvdRhLVcX0JLthylj0mK+WWjOYVYT1
                        DOobuhJV+0KhyHJcdNpZWf2bebS7aaEK7/Geedmb1U85
                        g0NLkUf0tZQnRA7fMVhSfU/ZxRjb+O+E+rCR/hi85RQC
                        jPYuVwKe01sqnKYpoDqlf9mG0fSdUDf5G0nyc/RjCB1H
                        dGxiMvRB6Cxi9fDAy49FuAtOrH+7DBKJCpqRWjS50DPw
                        gy1ZZlcr/YTer87W9JwqC2P8mq8f0LxOBg== )
...

```


Med DNSSEC



```
se.      86400 IN DS 59407 8 2 (
        67A8E06FCEFDD9397F77F26C41ADE4EC142F299BCFA1
        827F0EF8FD87F2F63022 )
```

```
:: ANSWER SECTION:
se.      3600 IN      DNSKEY 257 3 8 (
        AwEAAccqQMsh1rhvB3IWXmWZpCrug9MEGCKGteLIvwp
        yHeHgeBBm3M0p5FV9ImquvxFcNbd6Eey3Vf8SzoTodZ3
        YrGF9WFve7bmie2MIBhFDoCep16v9lon0ZsKrOvoCkPb
        TT0iFCdrbdyikYcCfvvh303anvQeTCf3jy+bHOTleaqV
        aNRJiGv5NBsPKpfnnqBpqqKyZymSpwQXHtTeyv7iWwGI
        3cfP3U6sp711WvKkXy7Y2Djnc5T5owHWUy1ZPI4s+9Dt
        uC2A9AWhOpDicguHYRfmyscjCbPOB8/tO5j+uECo67i7
        JjsiLjQTRyHuigUUBRag3Z3FaTXZBg/myaoUL0U=
        ) ; KSK; alg = RSASHA256 ; key id = 59407
se.      3600 IN      DNSKEY 256 3 8 (
        AwEAAayMZyxKcMdYA/I5OZwSGrMCpqwLcVTNXs94pVcr
        4Q2R9Xn3q1B/ccuyKI5IDq1cG7+ap4RD2iotGln2kWIX
        wQQAfLofh+ebAqngO0CLSKx/QvdjmHtNzS6EDCL6o+6r
        yabAcRpqsJbM3uw4f3RlswNXVNI7bx6iF5iu+ZhZ+zVd
        UcluO2Zlhy2AVYmne+Cq9bFpDbkrafsik0z8XjfbhWOa
        suLqwrL4QXBSvgegKVOrBD7/gfByboDw/wl5QDwK9yb6
        tr4G12TKIRFZqG8PYEyUG740UbhfvZRb0sJnRzO/yZ57
        i6vJyoVWovfpyn/3E9Tr3yQv0cc8CoboTNmTek=
        ) ; ZSK; alg = RSASHA256 ; key id = 2418
...
```


DNSSEC i praktiken

- Vad behöver man?
- Vad händer?
- Vem gör vad?
- Vad kan gå fel?



Vad behöver man?

- Namnserver att serva zonen (duh!)
- Signeringsmotor
 - Separat (OpenDNSSEC)
 - Integrerad (Knot, BIND, PowerDNS)
- Nyckelhanterare
 - HSM
 - SoftHSM (= nyckel på disk med PKCS #11 interface)
 - Följer vanligtvis med DNSSEC-kapabel namnserver
- Rätt tid!
 - NTP
 - Både för authoritative och resolver

```
31 del
32 self.file = None
33 self.fingerprints = set()
34 self.logdups = True
35 self.debug = debug
36 self.logger = logging.getLogger(__name__)
37 if path:
38     self.file = open(os.path.join(path, "zone.fingerprints"), "a")
39     self.file.seek(0)
40     self.fingerprints.update(e.request_fingerprint() for e in zone.entries)
41
42 @classmethod
43 def from_settings(cls, settings):
44     debug = settings.getbool("debug", False)
45     return cls(job_dir(settings), debug)
46
47 def request_seen(self, request):
48     fp = self.request_fingerprint(request)
49     if fp in self.fingerprints:
50         return True
51     self.fingerprints.add(fp)
52     if self.file:
53         self.file.write(fp + os.linesep)
54
55 def request_fingerprint(self, request):
56     return request_fingerprint(request)
```




Vad händer?

- DNSKEY record set läggs till i zonen
- (CDS/CDNSKEY läggs till i zonen)
- Zondata sorteras
- NSEC genereras
 - eller NSEC3, för de med den läggningen...
- Signaturer för record set genereras
- DS record läggs in i föräldrazonen
 - Skickas in med EPP
 - Hämtas av föräldrazonen (CDS/CDNSKEY)

Vem gör vad?

Exempel för en .se-domän

Registrant

- Önskar få sina domäner signerade.
 - Gnäll / hot / mutor

Registrar

- Skickar in DS-record via EPP

DNS-operator

- Hanterar nycklar
- Signerar zonen

Registry

- Publicerar DS



Vad kan gå fel?

- Trasiga signaturer
 - Utgången
 - Felaktig/saknad ZSK
 - Algoritm som resolvern inte förstår
- Trasig NSEC(3)
- Ingen DNSKEY som matchar DS
 - (Om DS saknas räknas zonen som osignerad, oavsett om ser finns nycklar / signaturer)

Felsökning DNSSEC

Grundläggande felavgränsning

- Hur vet man att DNSSEC är boven?
- Vad kan man göra åt det?

Felsökning DNSSEC

```
; <<>> DiG 9.10.6 <<>> @1.1.1.1 trasigdnssec.se soa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 13348
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
```


Felsökning DNSSEC

```
; <<>> DiG 9.10.6 <<>> @1.1.1.1 trasigdnssec.se soa +cd +multi
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36657
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
```

1

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;trasigdnssec.se.      IN      SOA
```

```
;; ANSWER SECTION:
trasigdnssec.se. 300 IN SOA ns.nic.se. hostmaster.iis.se. (
                        1489498801 ; serial
                        10800      ; refresh (3 hours)
                        3600       ; retry (1 hour)
                        86400      ; expire (1 day)
                        3600
```


Felsökning DNSSEC

```
; <<>> DiG 9.10.6 <<>> @1.1.1.1 trasigdnssec.se ds +dnssec +multi
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24605
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;trasigdnssec.se.IN DS

;; ANSWER SECTION:
trasigdnssec.se. 3600 IN      DS 44809 5 1 (
    E47802BAF4D673CF34C4CC5CC5ACFA4D17D136B7 )
trasigdnssec.se. 3600 IN      DS 44809 5 2 (
    33B50DFC93B9F29DA03CDFAC208770816EC3F052E679
    8F620F1CD05625094179 )
trasigdnssec.se. 3600 IN      RRSIG DS 8 2 3600 (
    20201129130817 20201116041101 2418 se.
    jV5aFDhex9FQALN8XrRwyyTeeRLshOoDAodoihCk8AR0
    e2tZGONIFI69Ry72kYFOyJrHsk3j5dxhBfB97dGgSC84
    V/3v1h2cKzxd3RNm1y5JVPUnwdPWym7r4bpbk6oYZtA7V
    A1ZqbFS2focCWmA6pgPub5Gb9Q/zpgehqy1SV7nAm4zC
    dzFGjP8Wp8fodmbTVZeqoKgb2C9r49aoS+VY766wuh3L
    xeC7qFluyG8Dsd6vgNvl9Htg+tY8lxCVF08kSGCBHsQ4
    4M49crrah/8PB4BwLiRTiMu1zYNLQrzw8o7G78EeoUeA
    HfiY3YwVrECstnr09kXJBTD6gEFEhefMrQ== )
```



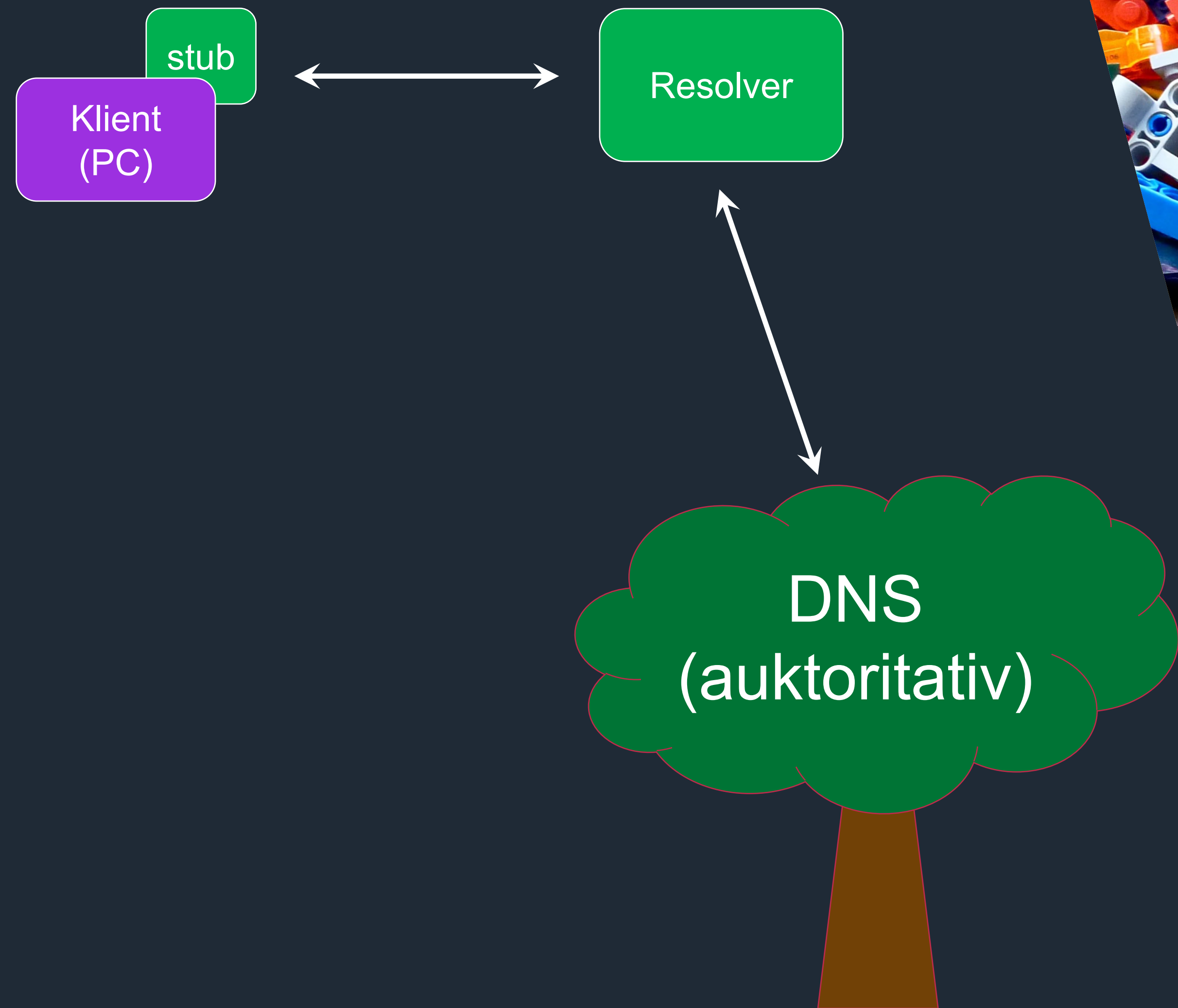

Andra verktyg

- DNSVIZ
 - dnsviz.net
- ZONEMASTER
 - zonemaster.se
 - zonemaster.net

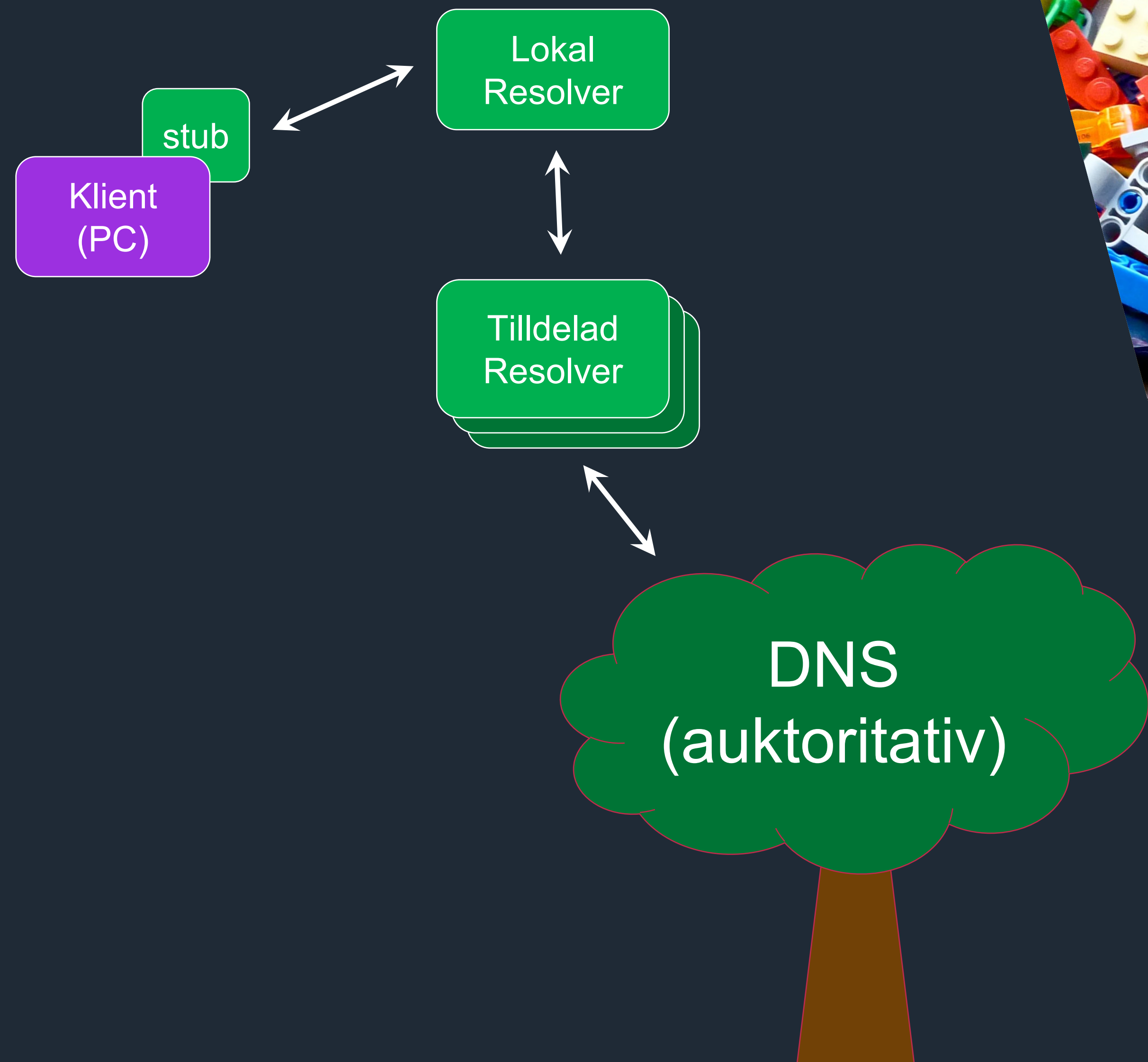
Resolving

- Resolvers är också DNS-servrar
- Men de har en annan roll än de auktoritativa namnservrarna
- Auktoritativa namnservrar äger zondata för sina domäner och svarar bara på förfrågningar för dessa
- Resolvers äger ingen zondata, men försöker ta reda på den för att ge svar
- Resolvers traverserar domänträdet tills de får ett svar eller ett fel

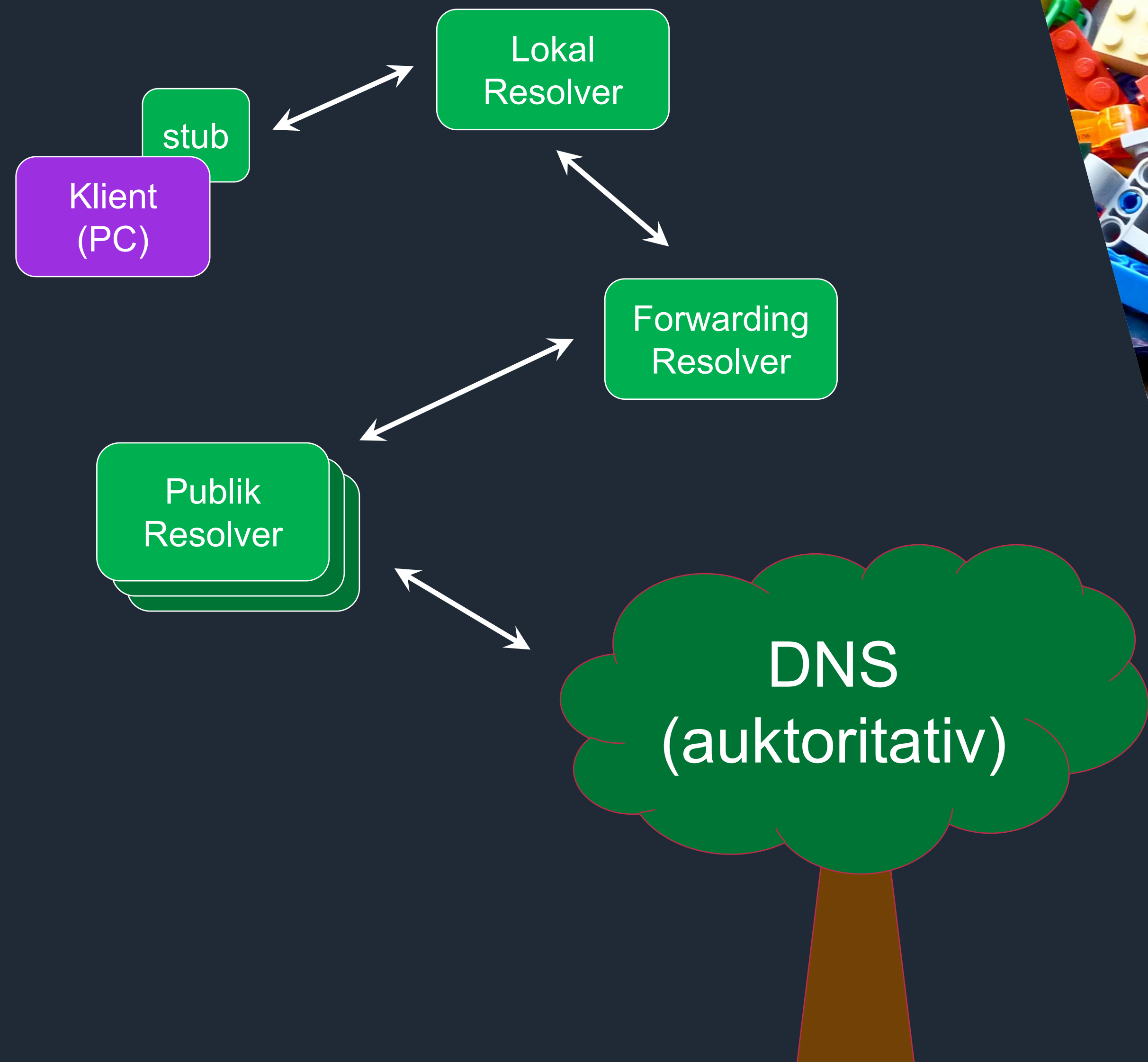
Den stökiga verkligheten



Den stökiga verkligheten



Den stökiga verkligheten



Den stökiga verkligheten

Variabler att ta hänsyn till

- Flera resolvers i kedjan
- Anycast
- Lastdelning
- Separat cache
- Delad cache
- Olika policys för bl.a. cache



Felsökning med DIG

- Vad får du för statuskod?
- Vad säger dig den övriga informationen i headern?
- Vilken server frågar du?
 - En resolver?
 - Din default-resolver?
 - Öppen resolver?
 - Annan resolver?
 - Den auktoritativa namnservern?
- Blir det någon skillnad om du frågar en annan server?
- Hur långt kan du följa stegen i DNS-trädet?

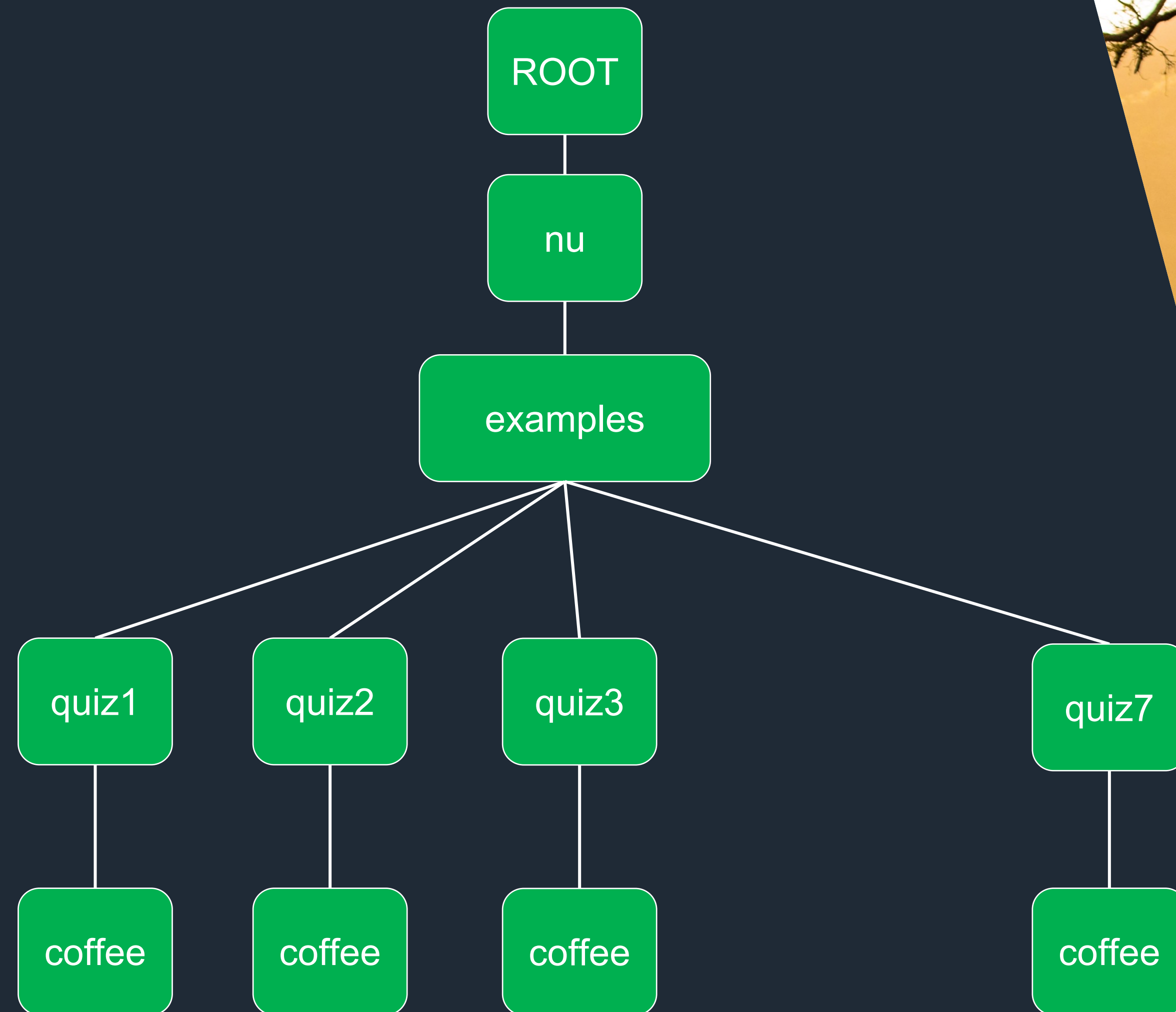
DIG quiz!

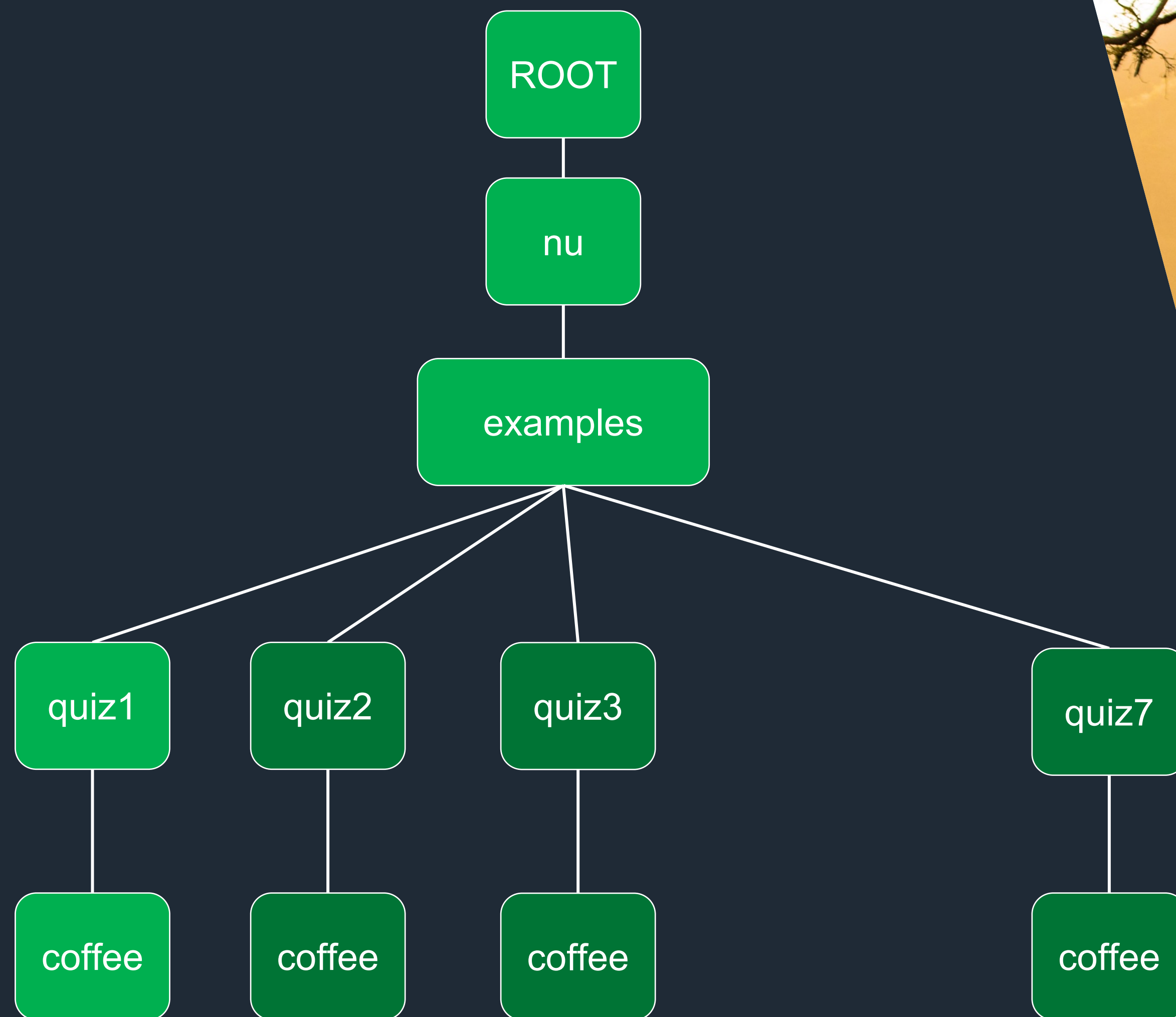
1. a. Vilken zon tillhör coffee.quiz1.examples.nu?
b. Vilken zon är *förälder* till zonen i fråga a?
2. a. Vilken zon tillhör coffee.quiz7.examples.nu?
b. Vilken zon är *förälder* till zonen i fråga a?
3. Hur ser man att så är fallet i fråga 1 och 2
4. Hur tog du reda på informationen för frågorna 1 och 2?
(Vad ställde du för frågor och till vilka namnservrar?)
5. Vad är fel med:
 - a. quiz2.examples.nu?
 - b. quiz3.examples.nu?
 - c. quiz5.examples.nu?

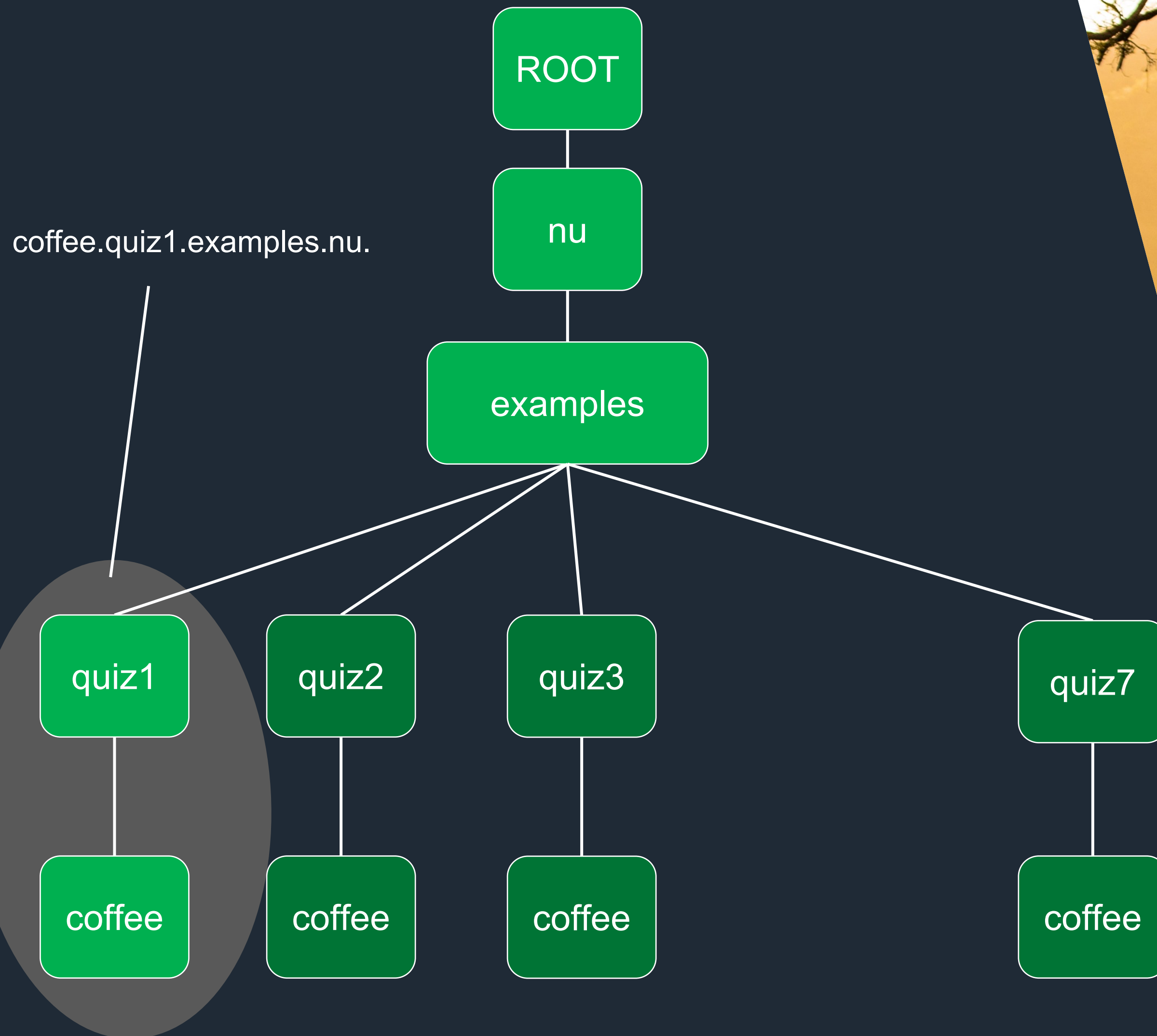


Lösningar





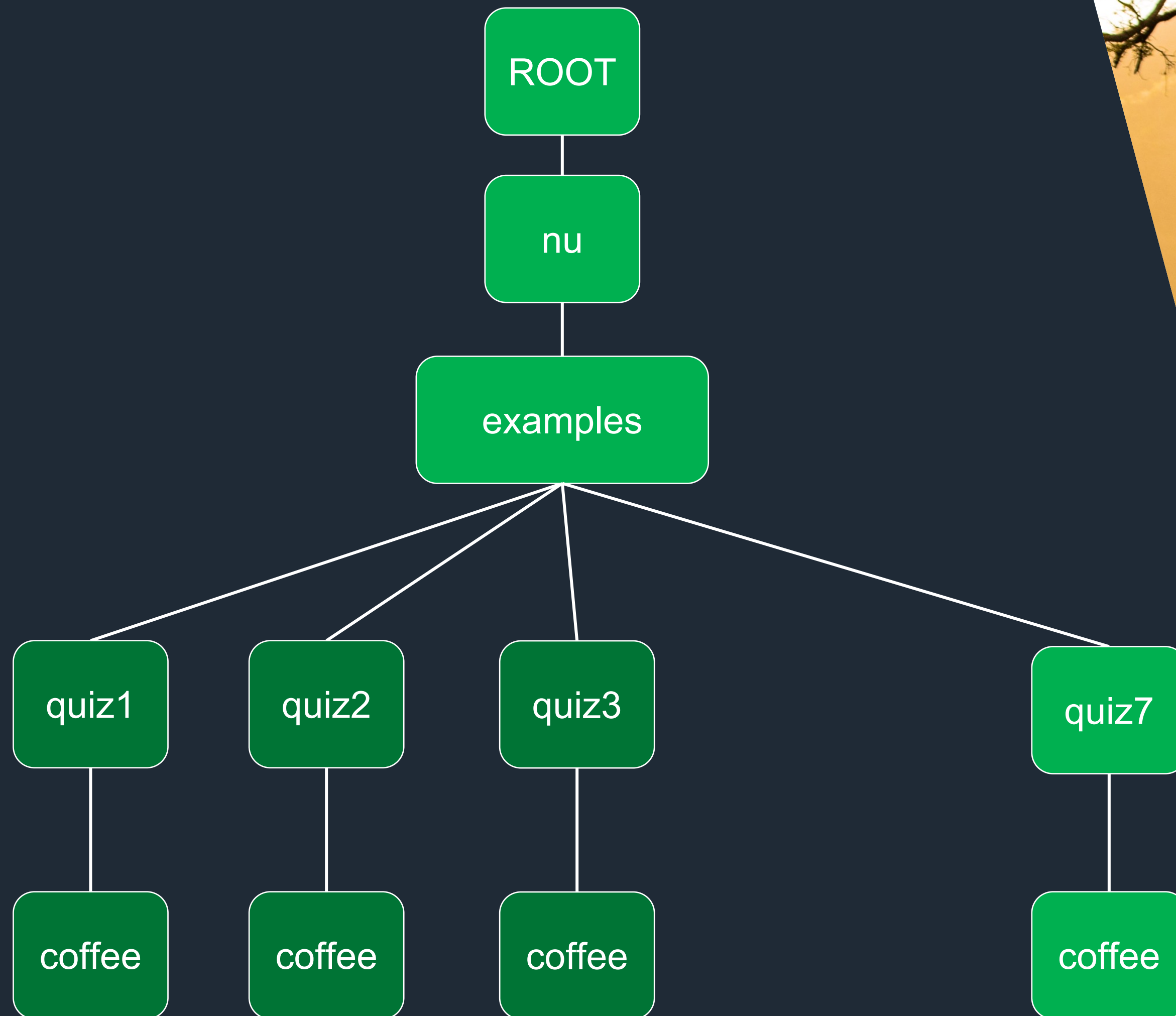


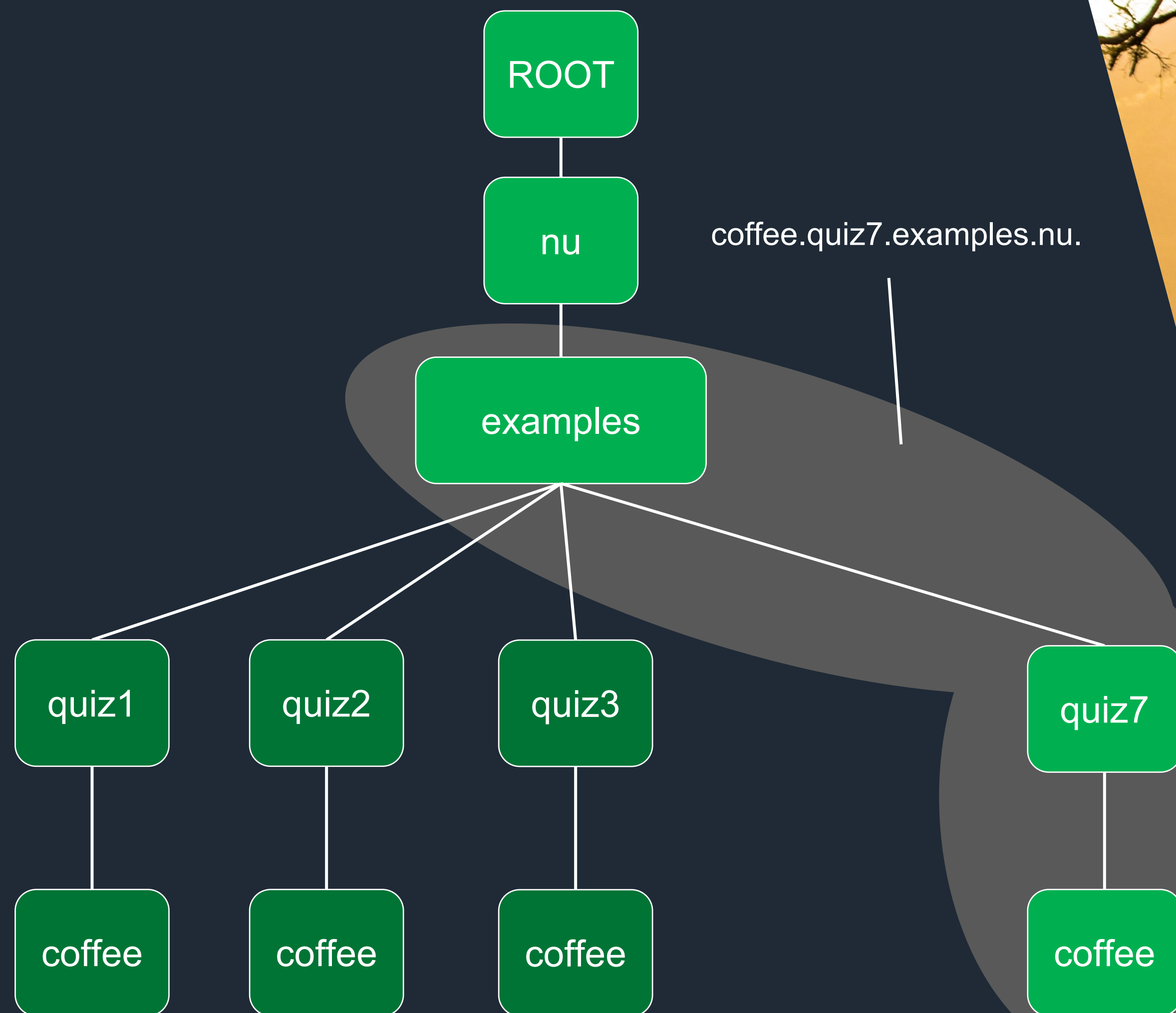


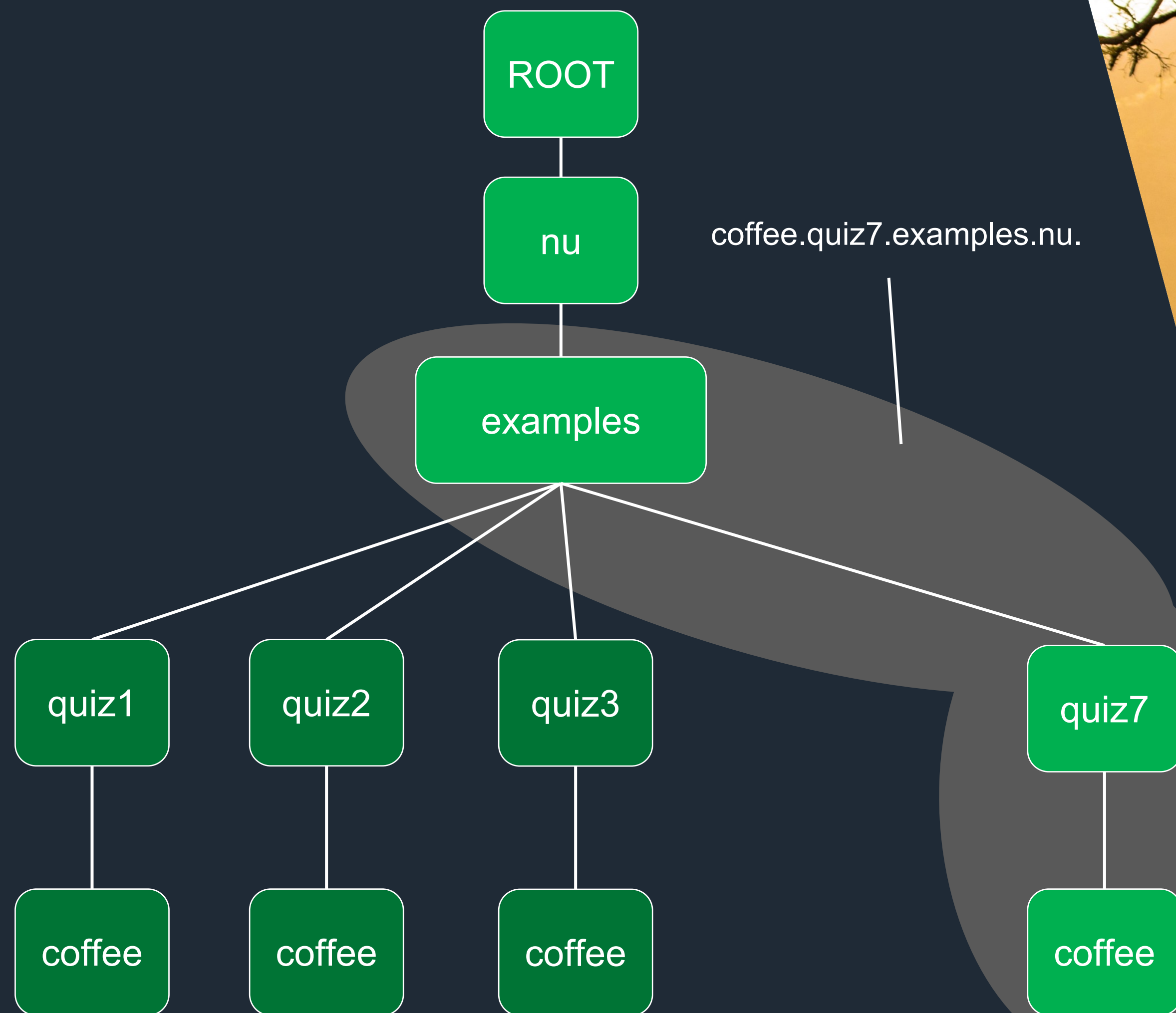
```
; <<>> DiG 9.10.6 <<>> @ns1.quiz1.examples.nu coffee.quiz1.examples.nu a
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20419
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::, udp: 1232
;; QUESTION SECTION:
;coffee.quiz1.examples.nu.    IN    A
```

```
;; ANSWER SECTION:
coffee.quiz1.examples.nu. 3600    IN    A    7.3.3.1
```

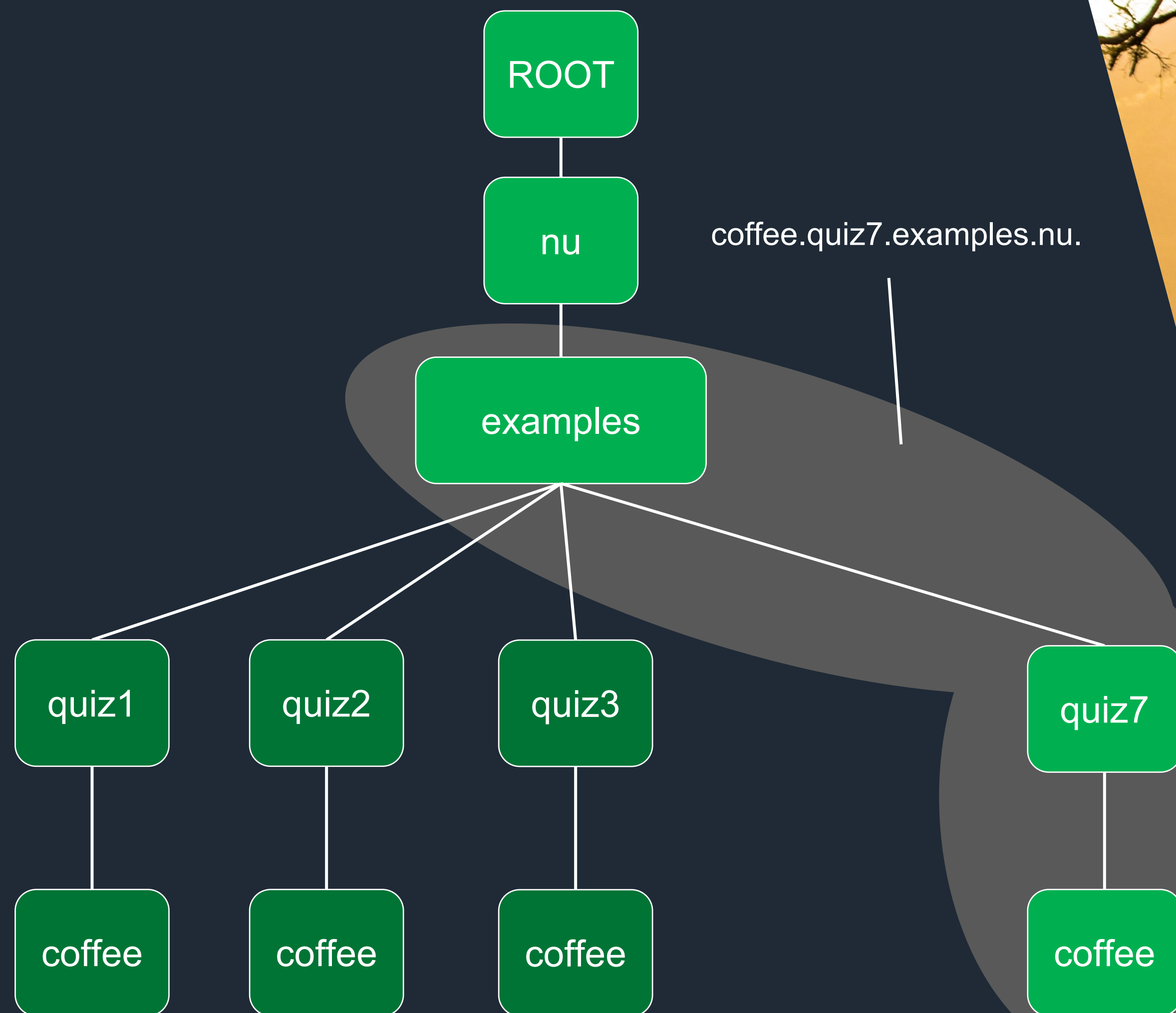




```
; <<>> DiG 9.10.6 <<>> @ns1.examples.nu coffee.quiz7.examples.nu a
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14300
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::, udp: 1232
;; QUESTION SECTION:
;coffee.quiz7.examples.nu.      IN      A
```

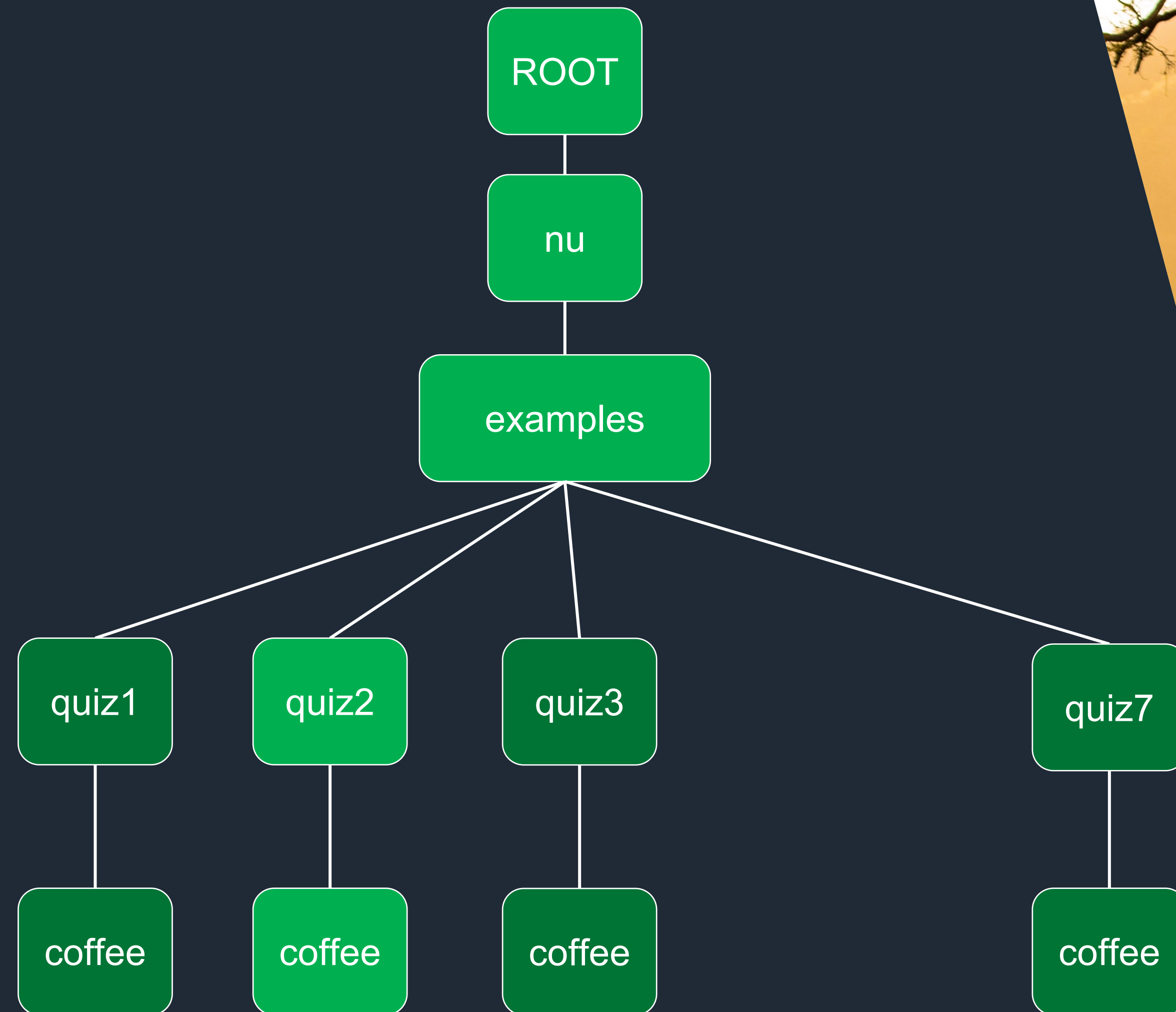
```
;; ANSWER SECTION:
coffee.quiz7.examples.nu. 3600      IN      A      1.3.3.7
```

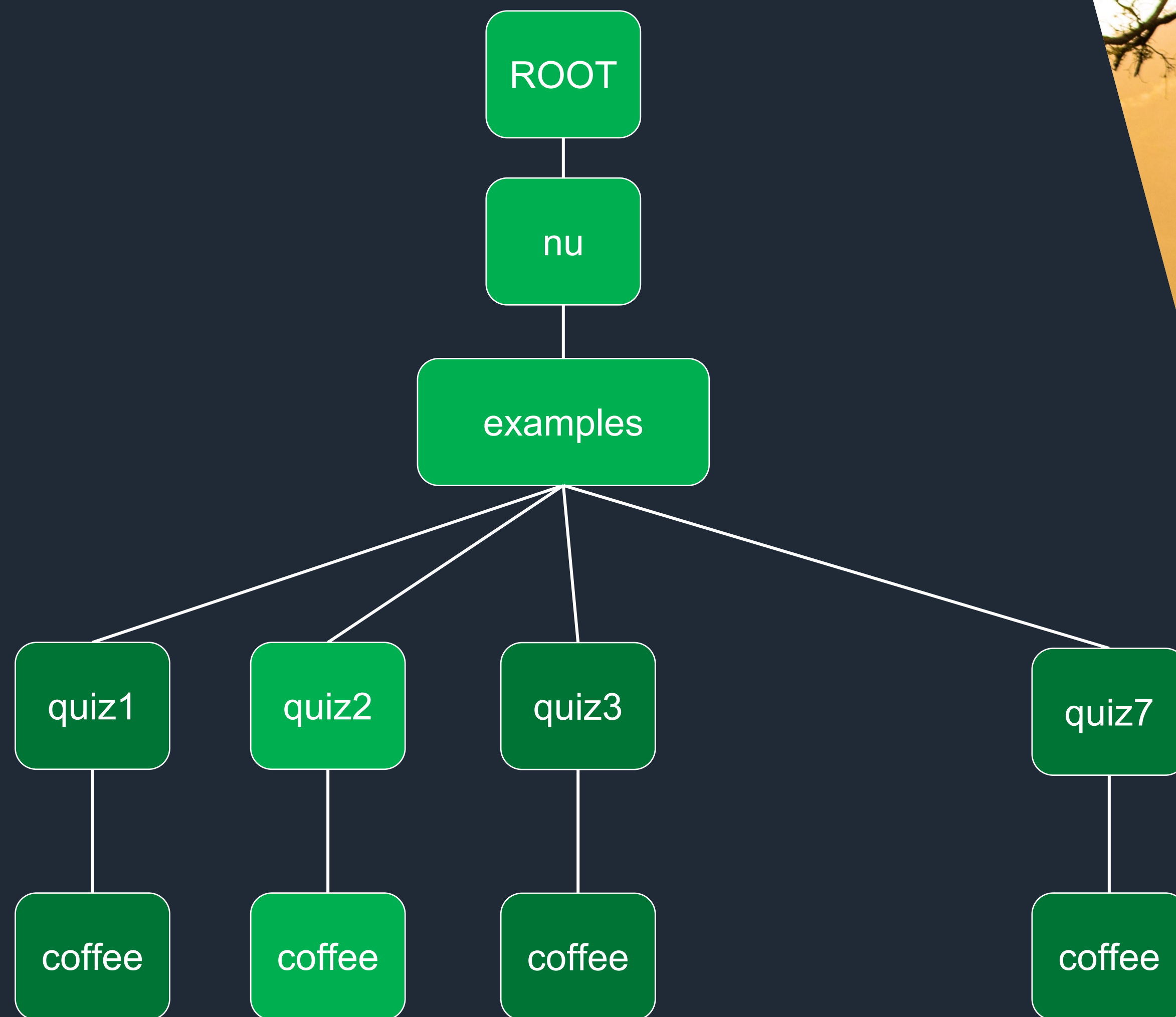



```
; <<>> DiG 9.10.6 <<>> @ns1.examples.nu quiz7.examples.nu any
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44096
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::, udp: 1232
;; QUESTION SECTION:
;quiz7.examples.nu.          IN      ANY

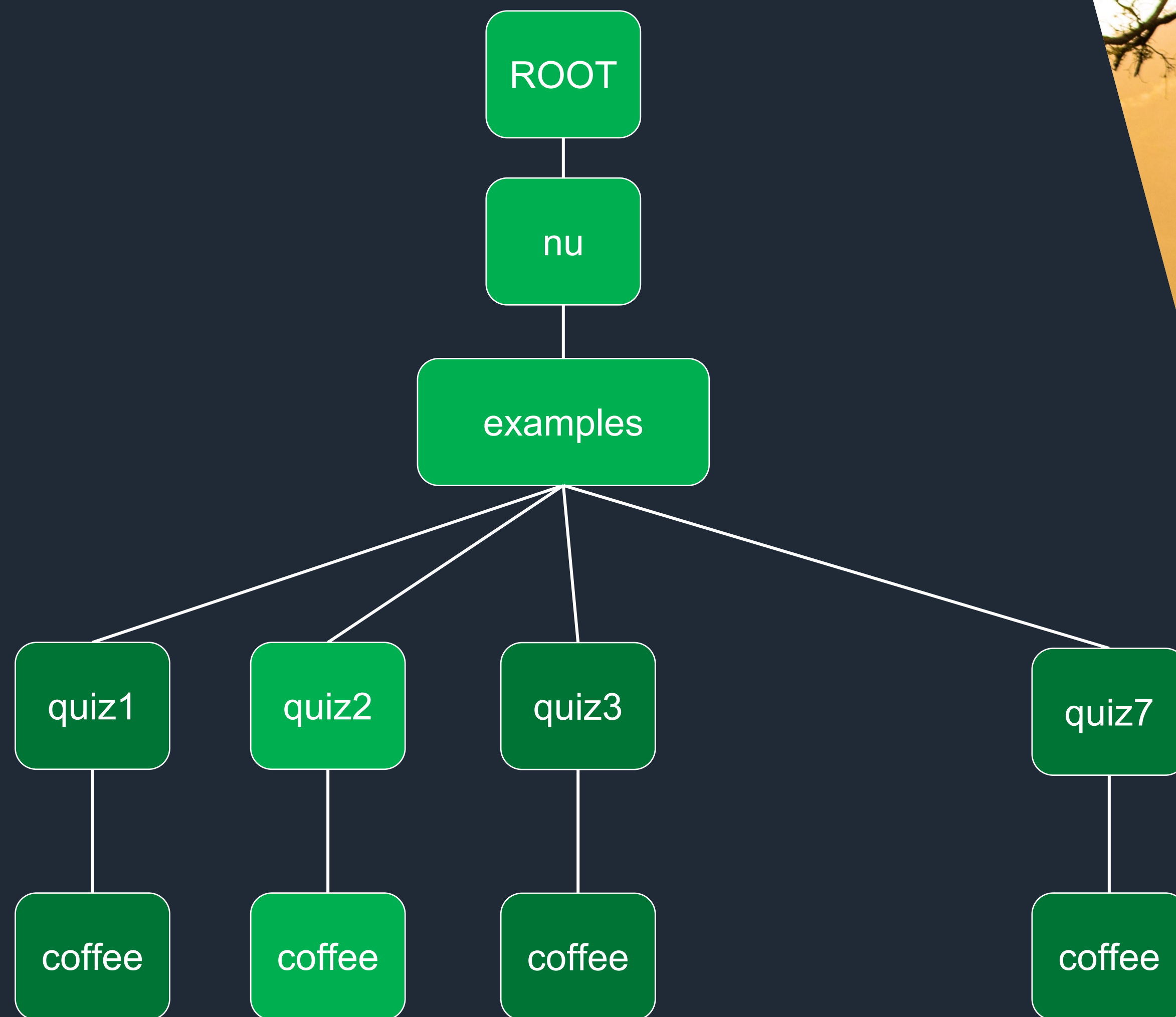
;; AUTHORITY SECTION:
examples.nu.                 3600 IN      SOA ns1.examples.nu. dns.iis.se. (
                                1597409128 ; serial
                                14400   ; refresh (4 hours)
                                3600    ; retry (1 hour)
                                604800   ; expire (1 week)
                                3600     ; minimum (1 hour)
                                )
```



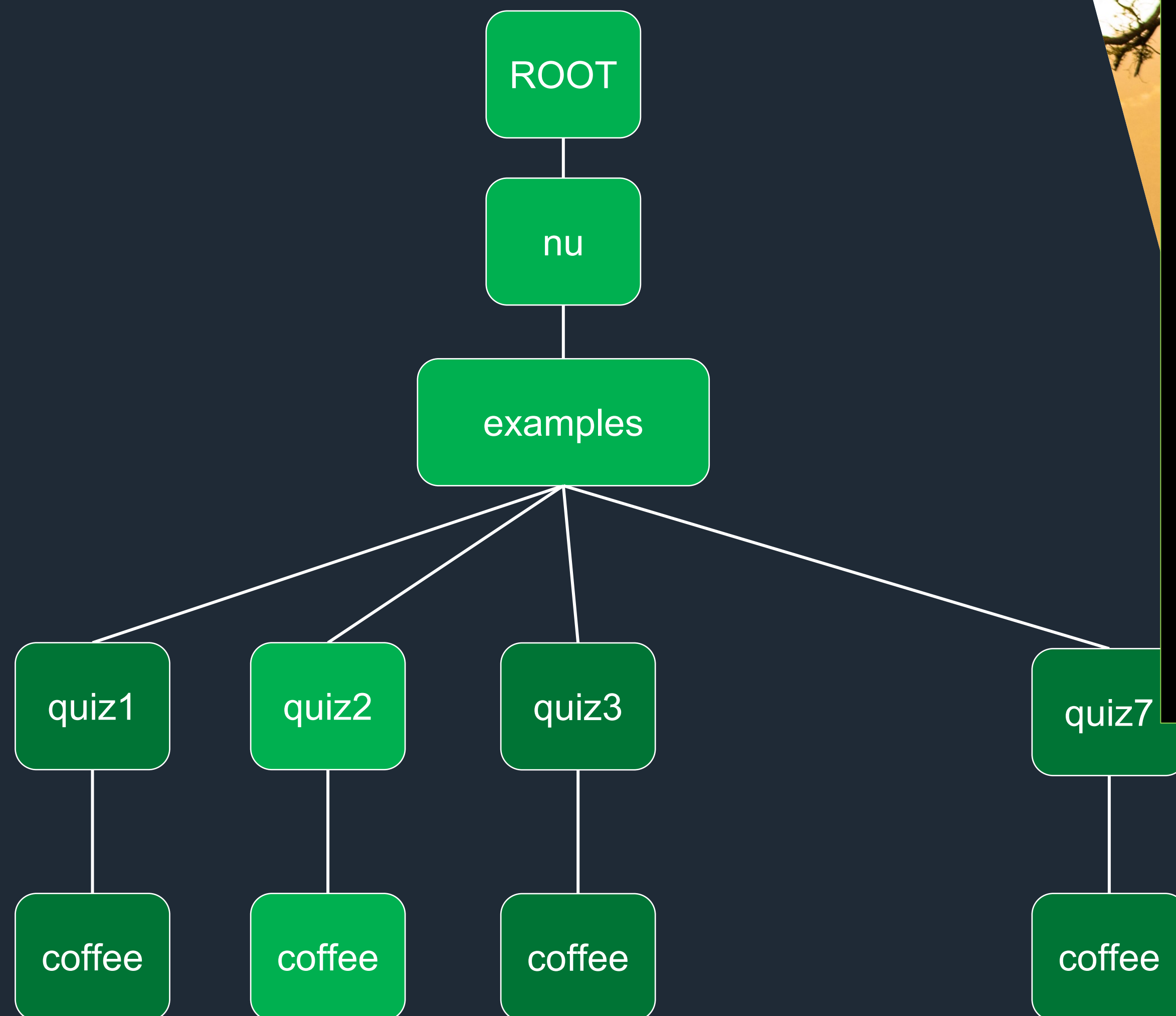
```
; <<>> DiG 9.10.6 <<>> quiz2.examples.nu soa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 65433
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 4096
;; QUESTION SECTION:
;quiz2.examples.nu.      IN      SOA
```

```
; <<>> DiG 9.10.6 <<>> @1.1.1.1 quiz2.examples.nu soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 38289
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::, udp: 1232
; OPT=15: 00 16 61 74 20 64 65 6c 65 67 61 74 69 6f 6e 20 71 75 69 7a 32 2e 65 78
61 6d 70 6c 65 73 2e 6e 75 2e ("..at delegation quiz2.examples.nu.")
; OPT=15: 00 18 ("..")
;; QUESTION SECTION:
;quiz2.examples.nu.          IN      SOA
```

```
; <<>> DiG 9.10.6 <<>> quiz2.examples.nu soa @ns1.examples.nu
```

```
:: global options: +cmd
```

```
:: Got answer:
```

```
:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21950
```

```
:: flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 5
```

```
:: WARNING: recursion requested but not available
```

```
:: OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags:: udp: 1232
```

```
:: QUESTION SECTION:
```

```
;quiz2.examples.nu.          IN      SOA
```

```
:: AUTHORITY SECTION:
```

```
quiz2.examples.nu.    3600 IN    NS    ns1.quiz2.examples.nu.
```

```
quiz2.examples.nu.    3600 IN    NS    ns2.quiz2.examples.nu.
```

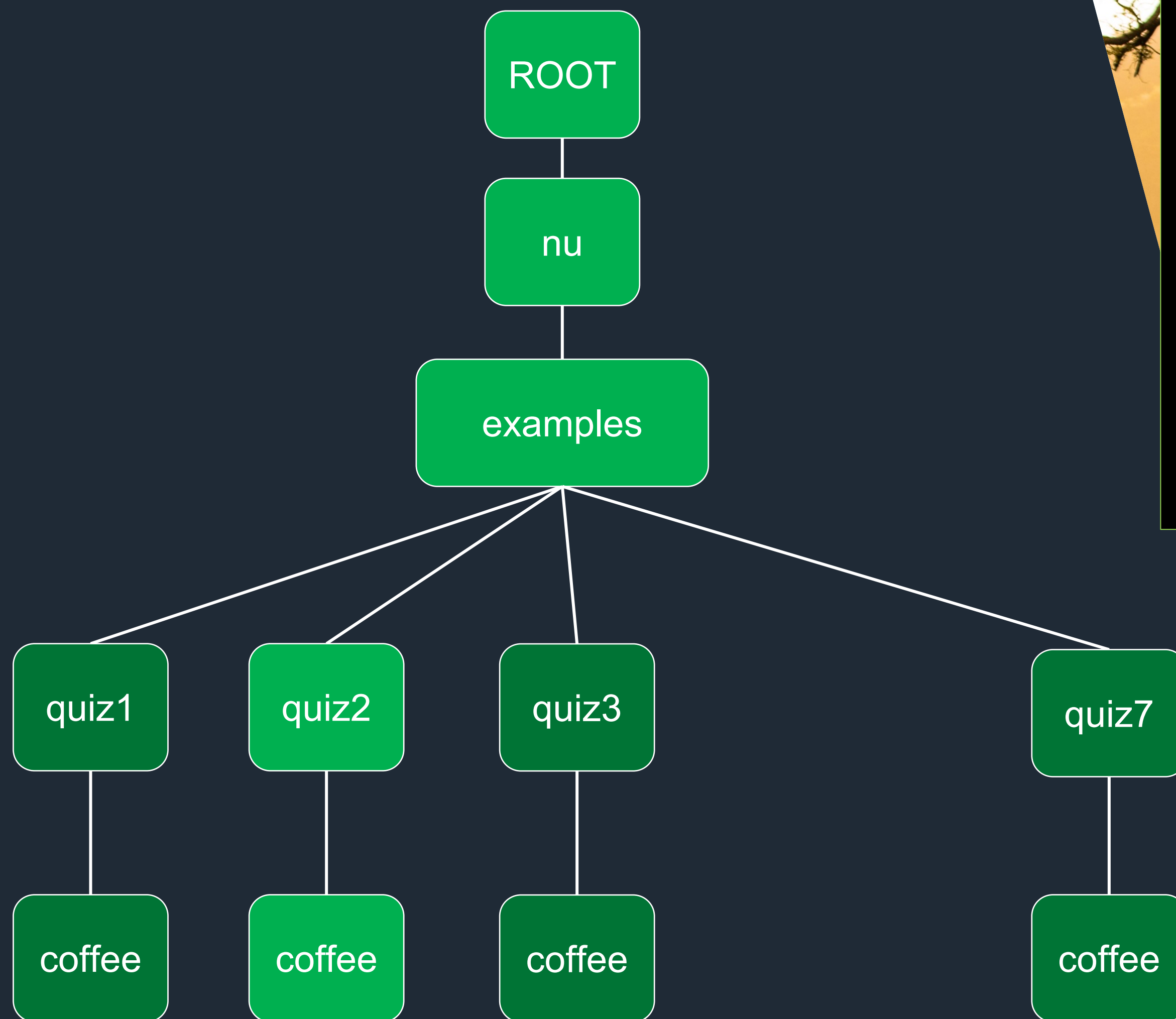
```
:: ADDITIONAL SECTION:
```

```
ns1.quiz2.examples.nu. 3600 IN    A      3.249.243.22
```

```
ns1.quiz2.examples.nu. 3600 IN    AAAA2a05:d018:bca:9d01:a5a5:65f2:b701:582e
```

```
ns2.quiz2.examples.nu. 3600 IN    A      13.53.192.161
```

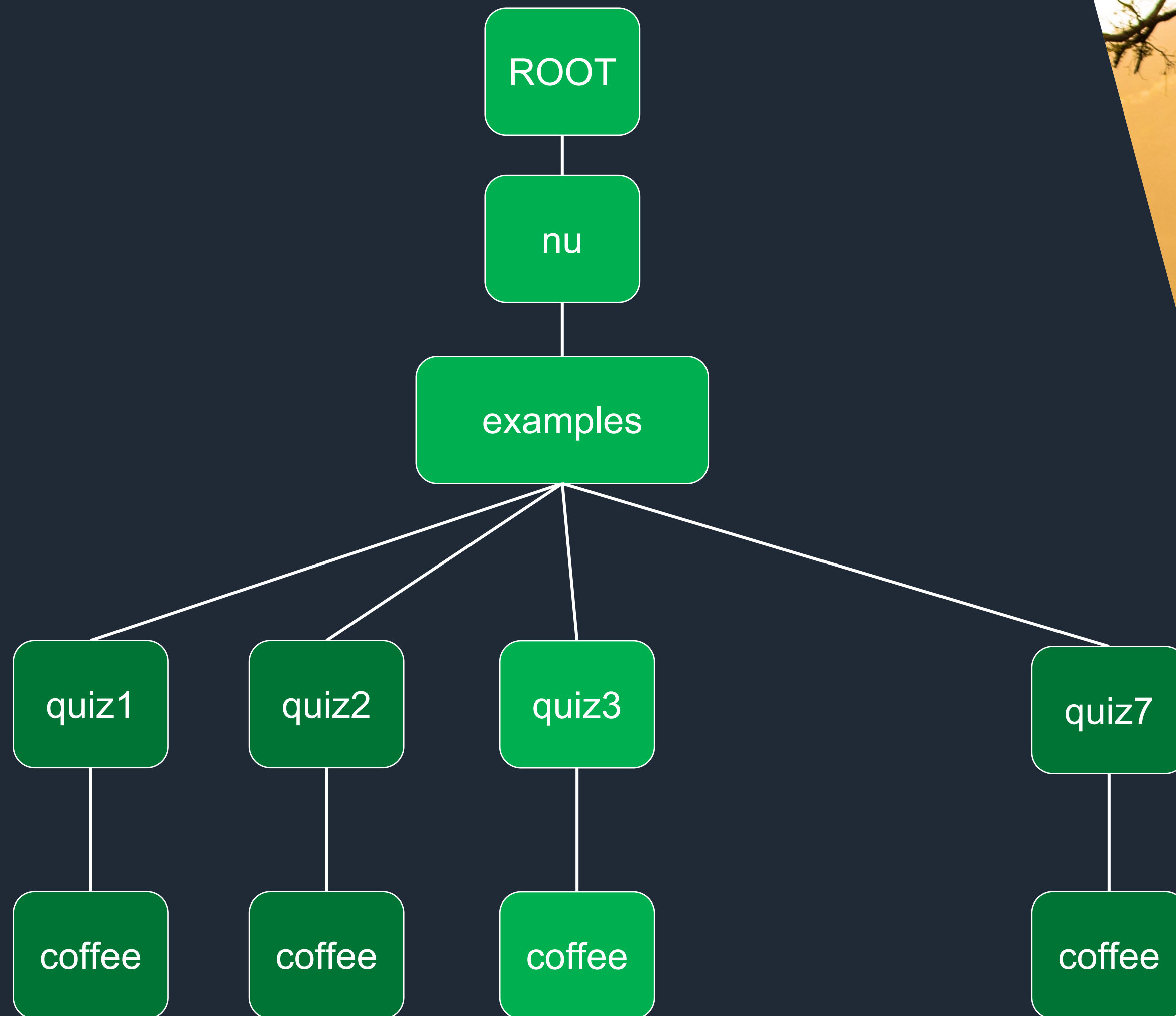
```
ns2.quiz2.examples.nu. 3600 IN    AAAA2a05:d016:163:703:f411:4efd:3a13:3815
```

```
; <<>> DiG 9.10.6 <<>> quiz2.examples.nu soa @3.249.243.22
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 14709
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

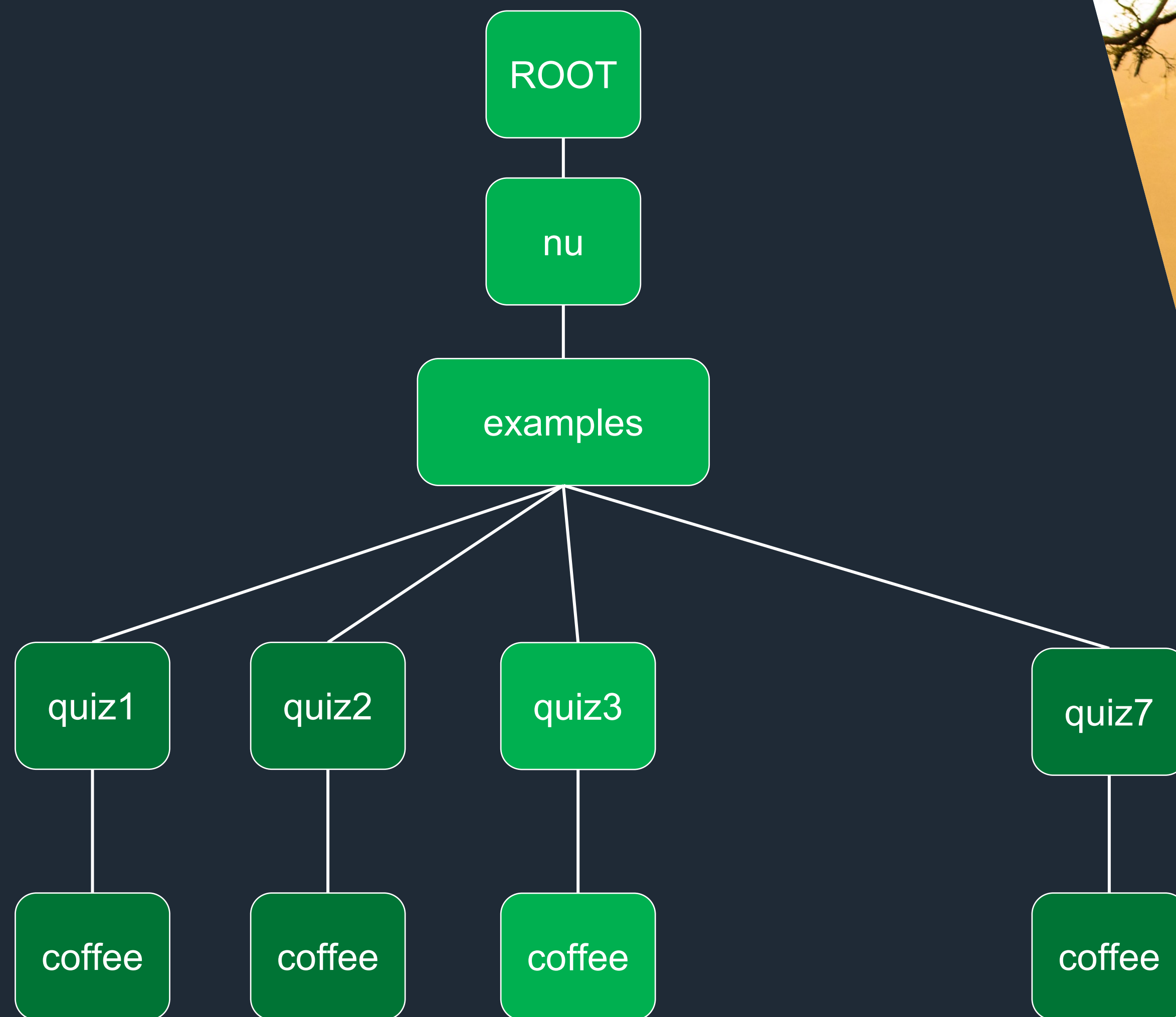
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:: udp: 1232
;; QUESTION SECTION:
;;quiz2.examples.nu.          IN      SOA

;; Query time: 39 msec
;; SERVER: 3.249.243.22#53(3.249.243.22)
;; WHEN: Mon Oct 26 18:08:20 CET 2020
;; MSG SIZE rcvd: 46
```

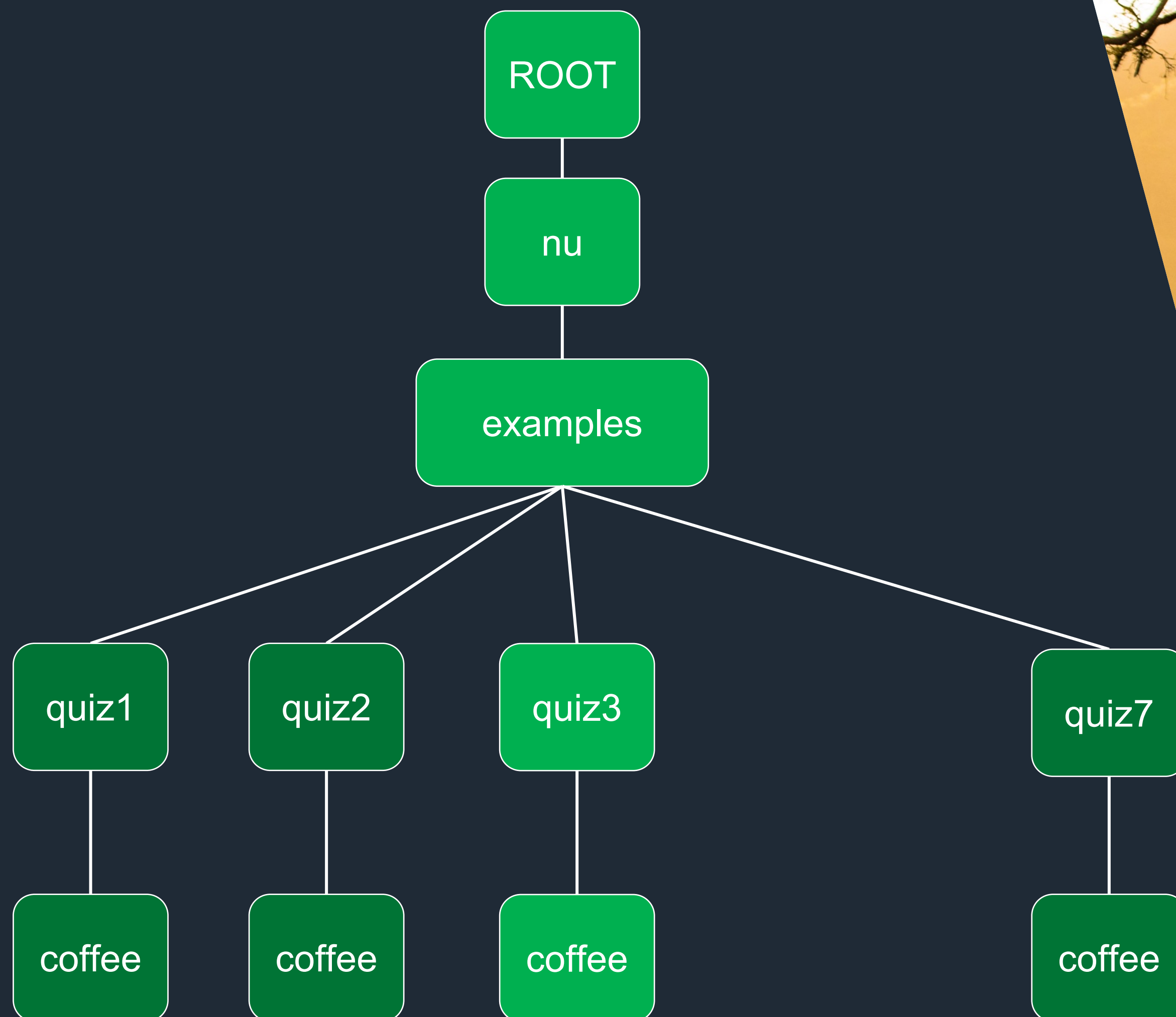
```
; <<>> DiG 9.10.6 <<>> quiz3.examples.nu soa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 40199
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 4096
;; QUESTION SECTION:
;quiz3.examples.nu.      IN      SOA
```

```
; <<>> DiG 9.10.6 <<>> @1.1.1.1 quiz3.examples.nu soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 55496
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::, udp: 1232
; OPT=15: 00 16 61 74 20 64 65 6c 65 67 61 74 69 6f 6e 20 71 75 69 7a 33 2e 65 78
61 6d 70 6c 65 73 2e 6e 75 2e ("..at delegation quiz3.examples.nu.")
;; QUESTION SECTION:
;quiz3.examples.nu.          IN      SOA
```

```
; <<>> DiG 9.10.6 <<>> quiz3.examples.nu soa @ns1.examples.nu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12113
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 5
;; WARNING: recursion requested but not available
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 1232
;; QUESTION SECTION:
;quiz3.examples.nu.      IN      SOA
```

```
;; AUTHORITY SECTION:
quiz3.examples.nu.      3600 IN    NS     ns1.quiz3.examples.nu.
quiz3.examples.nu.      3600 IN    NS     ns2.quiz3.examples.nu.
```

```
;; ADDITIONAL SECTION:
ns1.quiz3.examples.nu.  3600 IN    A       127.0.0.1
ns1.quiz3.examples.nu.  3600 IN    AAAA    ::1
ns2.quiz3.examples.nu.  3600 IN    A       127.0.0.2
ns2.quiz3.examples.nu.  3600 IN    AAAA    ::2
```