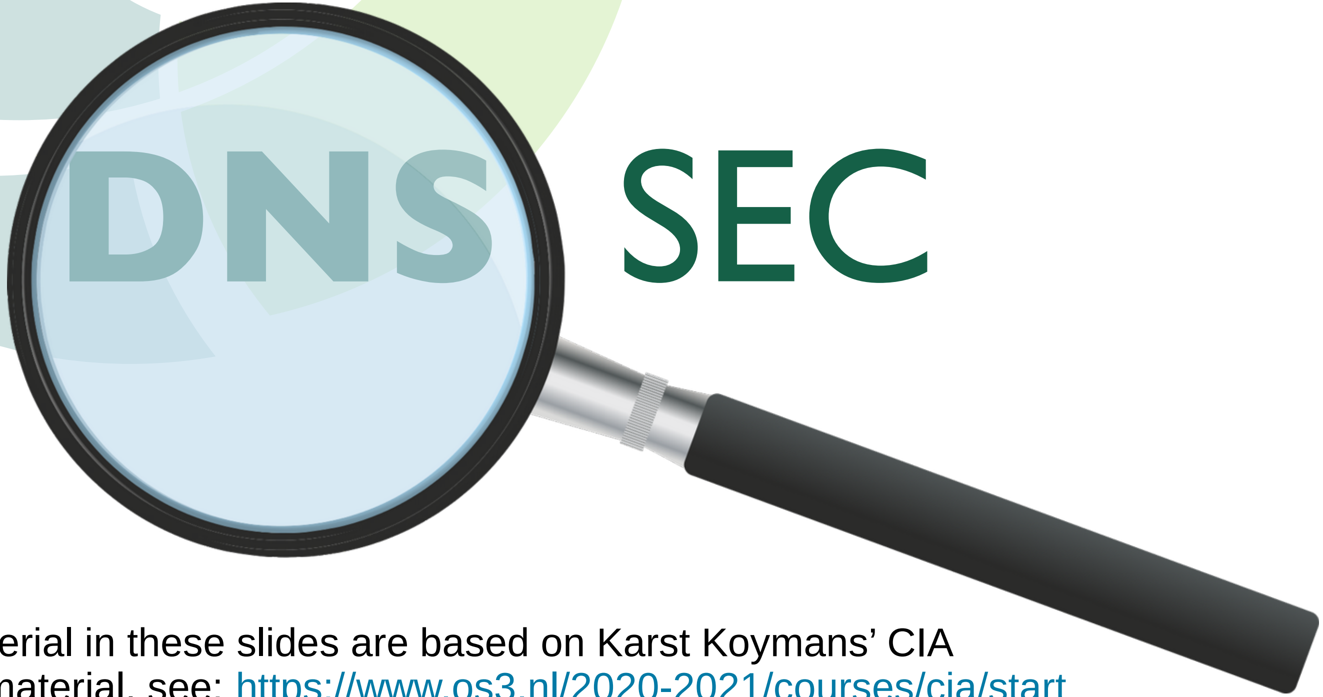
ยินดีต้อนรับสู่

CYBER SECURITY WORKSHOP



DNS SEC

Bangkok
8-9 May 2019

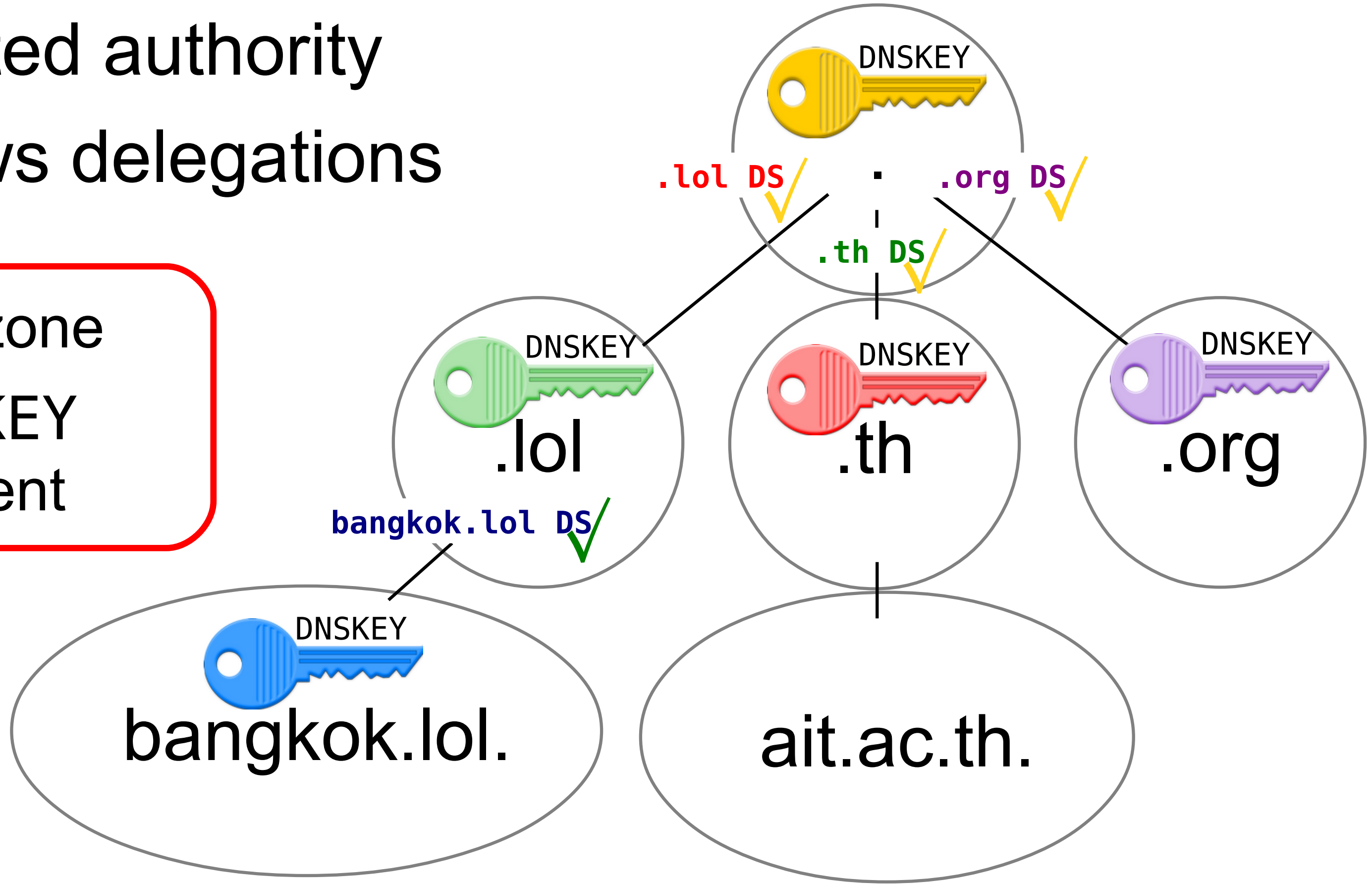
The material in these slides are based on Karst Koymans’ CIA course material, see: https://www.os3.nl/2020-2021/courses/cia/start

DNS Security Extensions (DNSSEC)

Chain of Trust

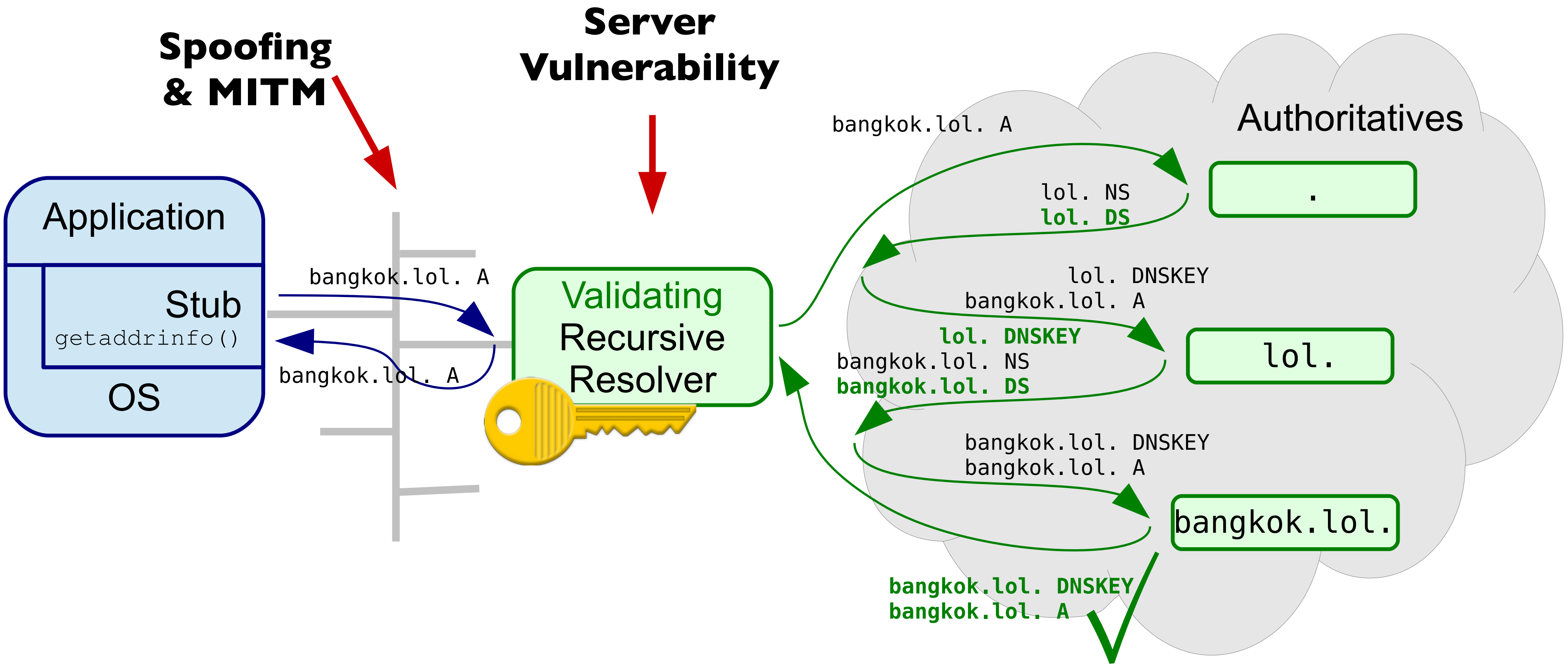
- Zones with distributed authority
- Chain of trust follows delegations

DNSKEY	Public key of zone
DS	Hash of DNSKEY signed by parent



DNS Security Extensions (DNSSEC)

Validation



DNS Security Extensions (DNSSEC)

Properties

- DNSSEC gives you
  - Authenticity - *You can prove the origin*
  - Integrity - *Detect alteration*
- DNSSEC does **not** give you
  - Confidentiality - Anyone *can read it*

DNS Security Extensions (DNSSEC)

History

- Original spec January 1997(RFC2065)
- Revised spec March 1999 (RFC2535)
- “Final” spec March 2005
  - DNSSEC-bis (RFC4033, 4034 and 4035)
- “Final” addition from February 2008
  - NSEC3 (RFC5155)
- Root zone signed 15 July 2010

DNSSEC Resource records

- To build the Chain of Trust
  - DNSKEY
    - Public key for the zone at the Apex
    - Used to verify signatures in the zone
    - Root DNSKEYs are well known
  - DS
    - Delegation signer
    - DNSKEY with a DS in the parent: Secure Entry Point (SEP)
  - RRSIG
    - Resource Record (set) SIGnature

DNSSEC Resource records

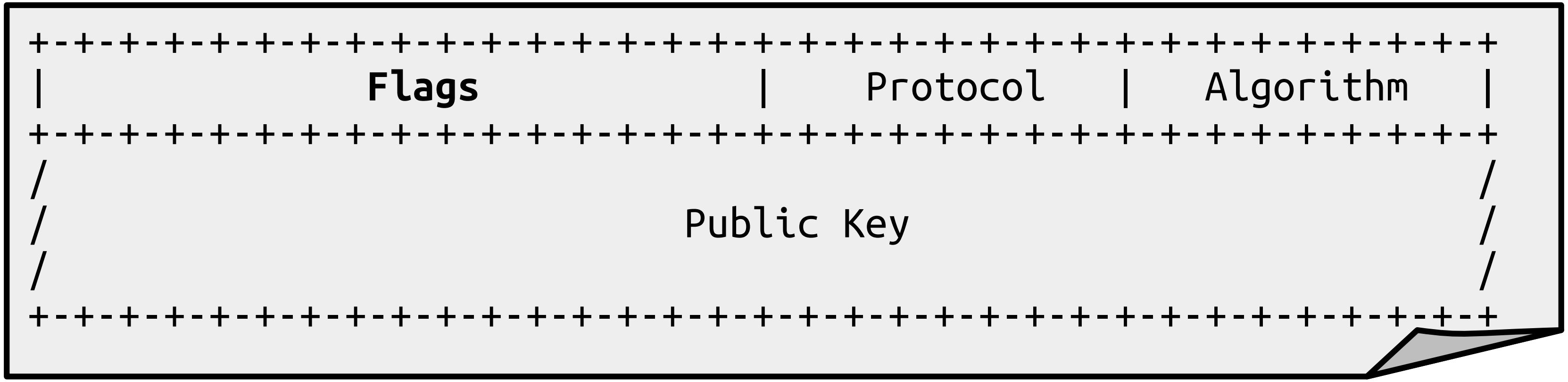
DNSKEY

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Flags            |    Protocol   |   Algorithm   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                                               /
/                            Public Key                         /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
example.com. 86400 IN DNSKEY 256 3 5 ( AQPSKmynfzW4kyBv015MUG2DeIQ3
                                       Cbl+BBZH4b/0PY1kxkmvHjcZc8no
                                       kfzj31GajIQKY+5CptLr3buXA10h
                                       WqTkF7H6RfoRqXQeogmMHfpftf6z
                                       Mv1LyBUgia7za6ZEzOJBOztyvhjL
                                       742iU/TpPSEDhm2SNKLijfUppn1U
                                       aNvv4w==  )
```

DNSSEC Resource records

DNSKEY – Flags



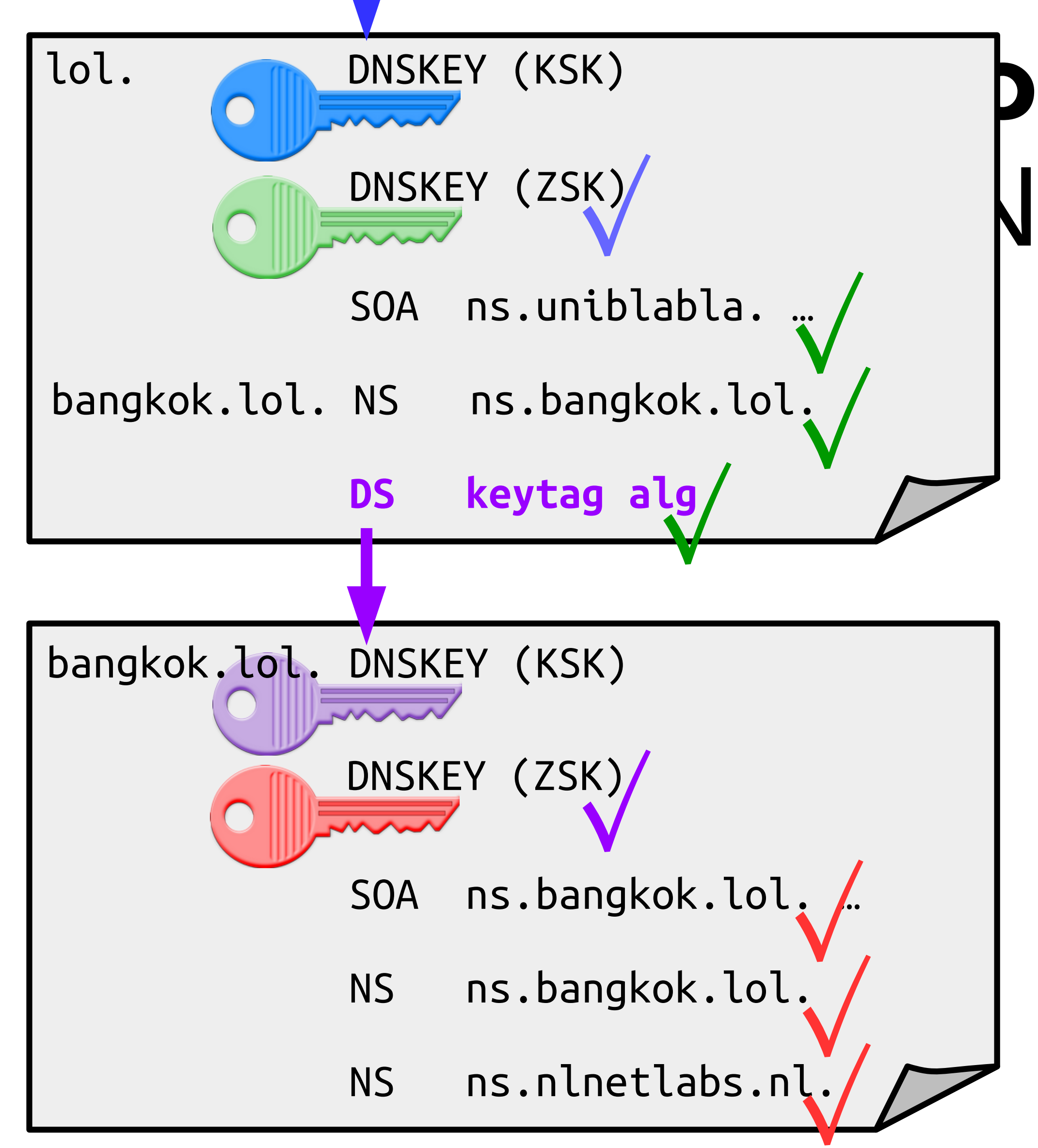
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Flags            |    Protocol   |   Algorithm   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                                               /
/                            Public Key                         /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- 256 – Zone Signing Key (ZSK)
- 257 – Key Signing Key (KSK)
  - Only used to sign the DNSKEY RRset
- 385 – Revoked Key Signing Key (RFC5011)

ource records

NSKEY – Flags

- 256 – Zone Signing Key (ZSK)
- 257 – Key Signing Key (KSK)



lol. DNSKEY (KSK)

DNSKEY (ZSK)

SOA ns.uniblabla. …

bangkok.lol. NS ns.bangkok.lol.

DS keytag alg

bangkok.lol. DNSKEY (KSK)

DNSKEY (ZSK)

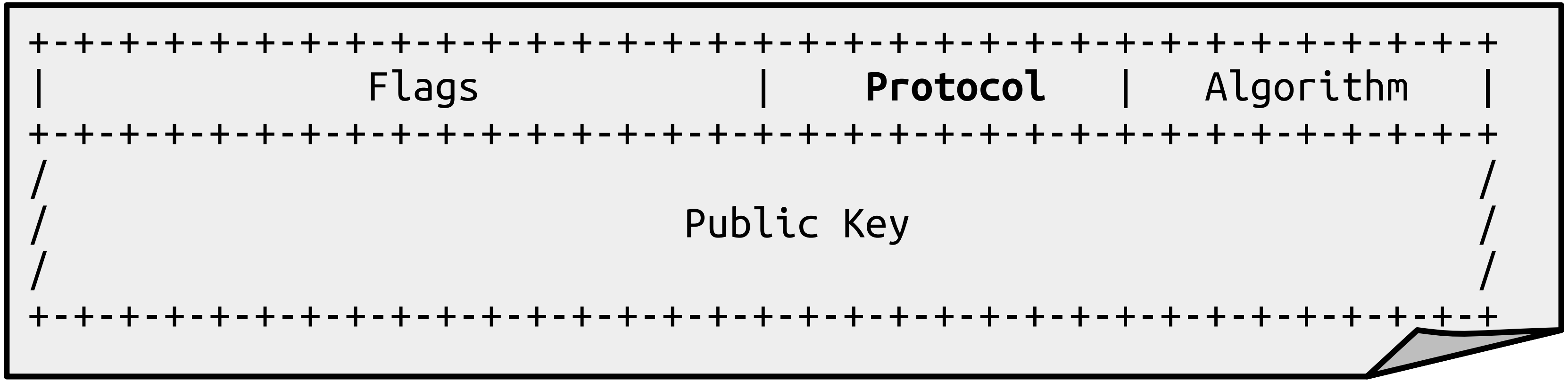
SOA ns.bangkok.lol. …

NS ns.bangkok.lol.

NS ns.nlnetlabs.nl.

DNSSEC Resource records

DNSKEY – Protocol



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Flags            |    Protocol   |   Algorithm   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                                               /
/                            Public Key                         /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- 3

DNSSEC Resource records

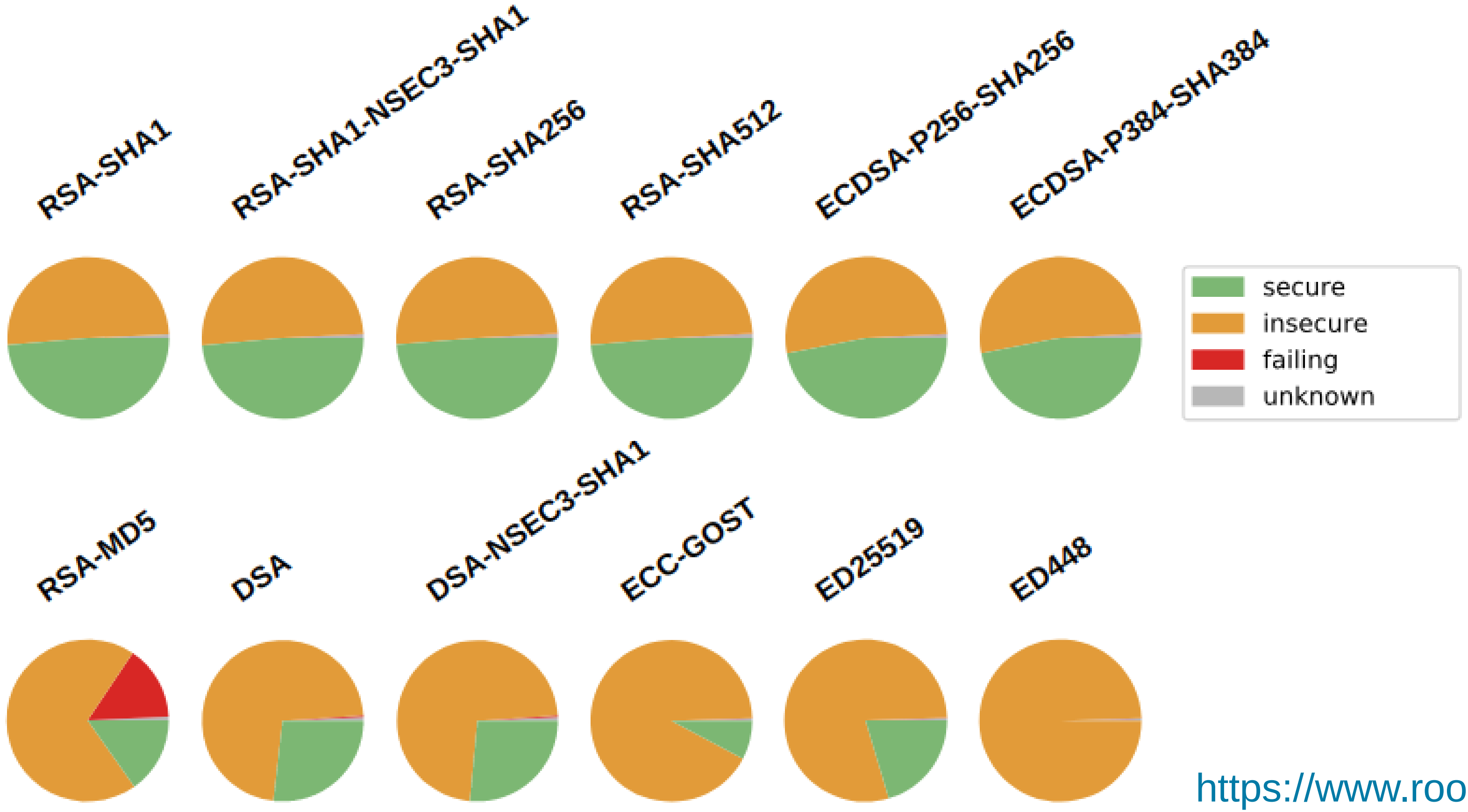
DNSKEY – Algorithm

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Flags            |    Protocol   |   Algorithm   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                                               /
/                            Public Key                         /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

~~1~~	~~RSA/MD5~~
3	DSA/SHA1
5	RSA/SHA1
6	DSA-NSEC3-SHA1
7	RSASHA1-NSEC3-SHA1
8	RSA/SHA-256

10	RSA/SHA-512
12	GOST R 34.10-200
13	**ECDSA Curve P-256 with SHA-256**
14	ECDSA Curve P-384 with SHA-384
15	Ed25519
16	Ed448

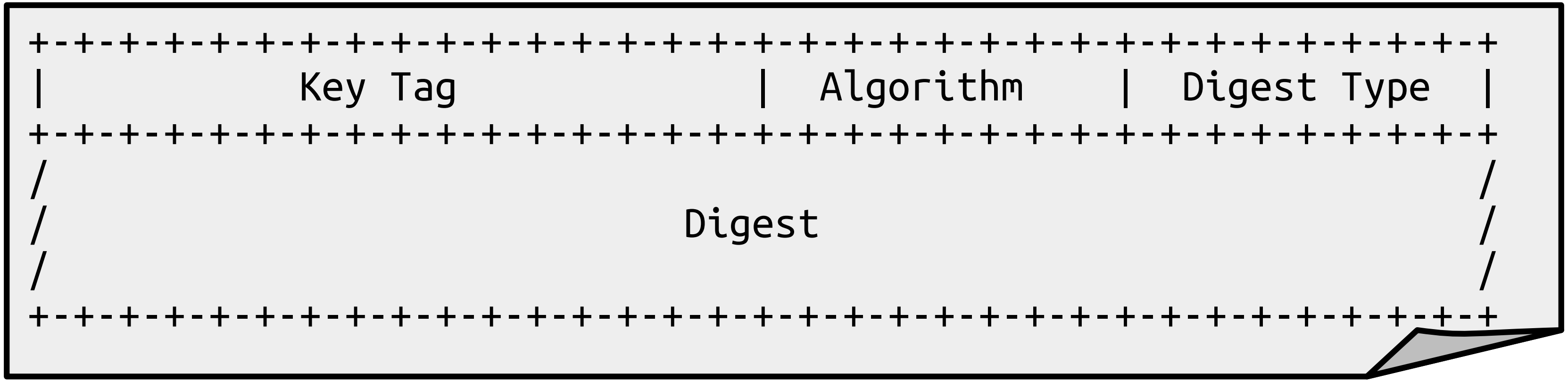
DNSSEC Resource records
DNSKEY – Algorithm



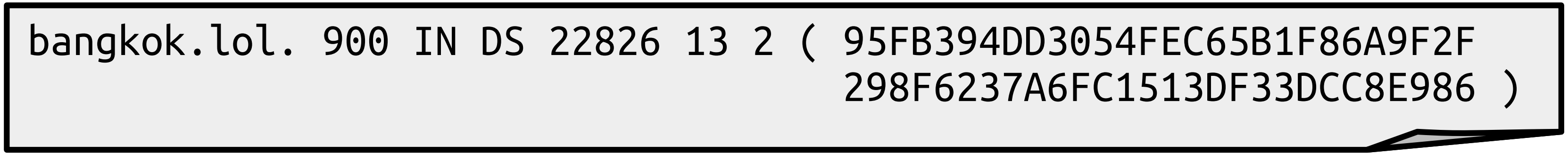
https://www.rootcanary.org/

DNSSEC Resource records

DS



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Key Tag             |  Algorithm    |  Digest Type  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                                               /
/                            Digest                             /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



```
bangkok.lol. 900 IN DS 22826 13 2 ( 95FB394DD3054FEC65B1F86A9F2F
                                    298F6237A6FC1513DF33DCC8E986 )
```

DNSSEC Resource records

DS – Key Tag

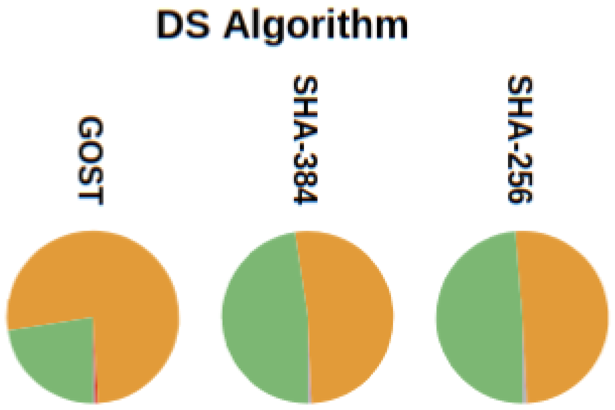
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Key Tag             |  Algorithm    |  Digest Type  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                                               /
/                            Digest                             /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
uint32_t keytag (uint8_t key[], size_t keysize)
{
        uint32_t ac;
        size_t i;

        for ( ac = 0, i = 0; i < keysize; ++i )
                ac += (i & 1) ? key[i] : key[i] << 8;
        ac += (ac >> 16) & 0xFFFF;
        return ac & 0xFFFF;
}
```

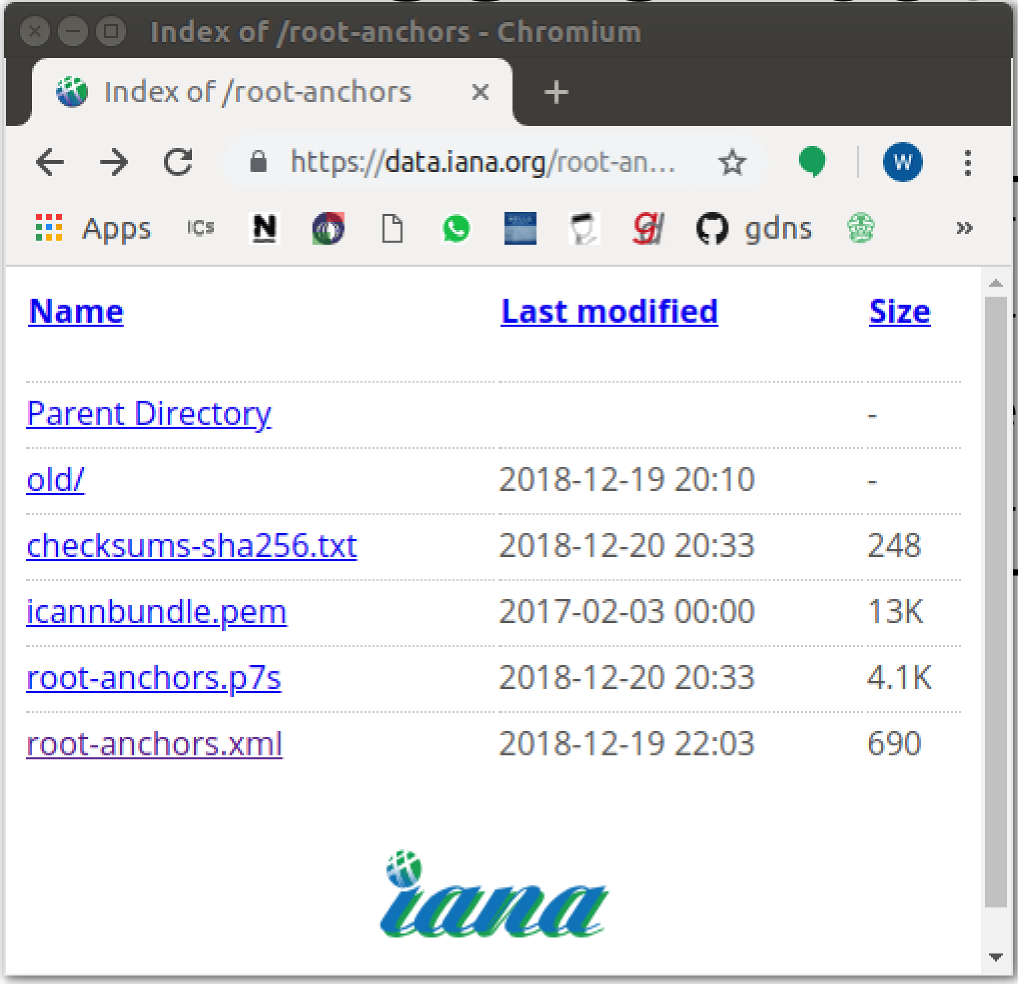
DNSSEC Resource records

DS – Digest Type

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Key Tag             |  Algorithm    |  Digest Type  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                                               /
/                            Digest                             /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



DNSSEC Resource records — Digest Type



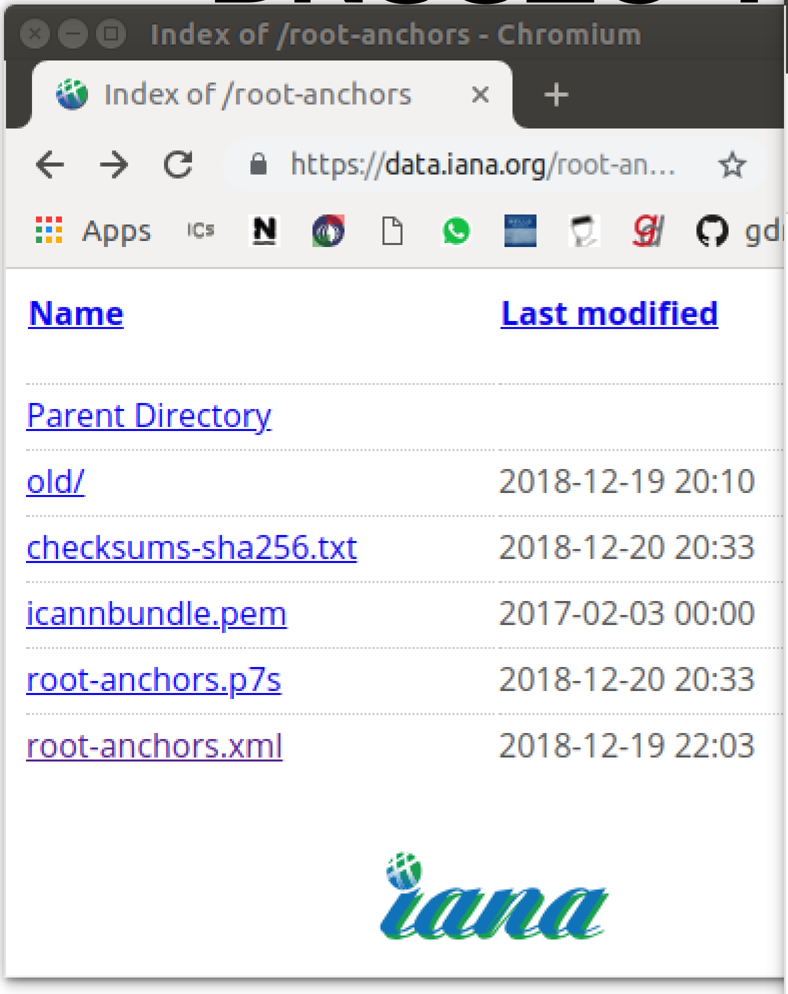
Index of /root-anchors - Chromium
Index of /root-anchors
https://data.iana.org/root-an...
Apps
gdns
iana

Name	Last modified	Size
Parent Directory		-
old/	2018-12-19 20:10	-
checksums-sha256.txt	2018-12-20 20:33	248
icannbundle.pem	2017-02-03 00:00	13K
root-anchors.p7s	2018-12-20 20:33	4.1K
root-anchors.xml	2018-12-19 22:03	690

```
-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  Algorithm        |  Digest Type  |
-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                /
st                              /
                                /
-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

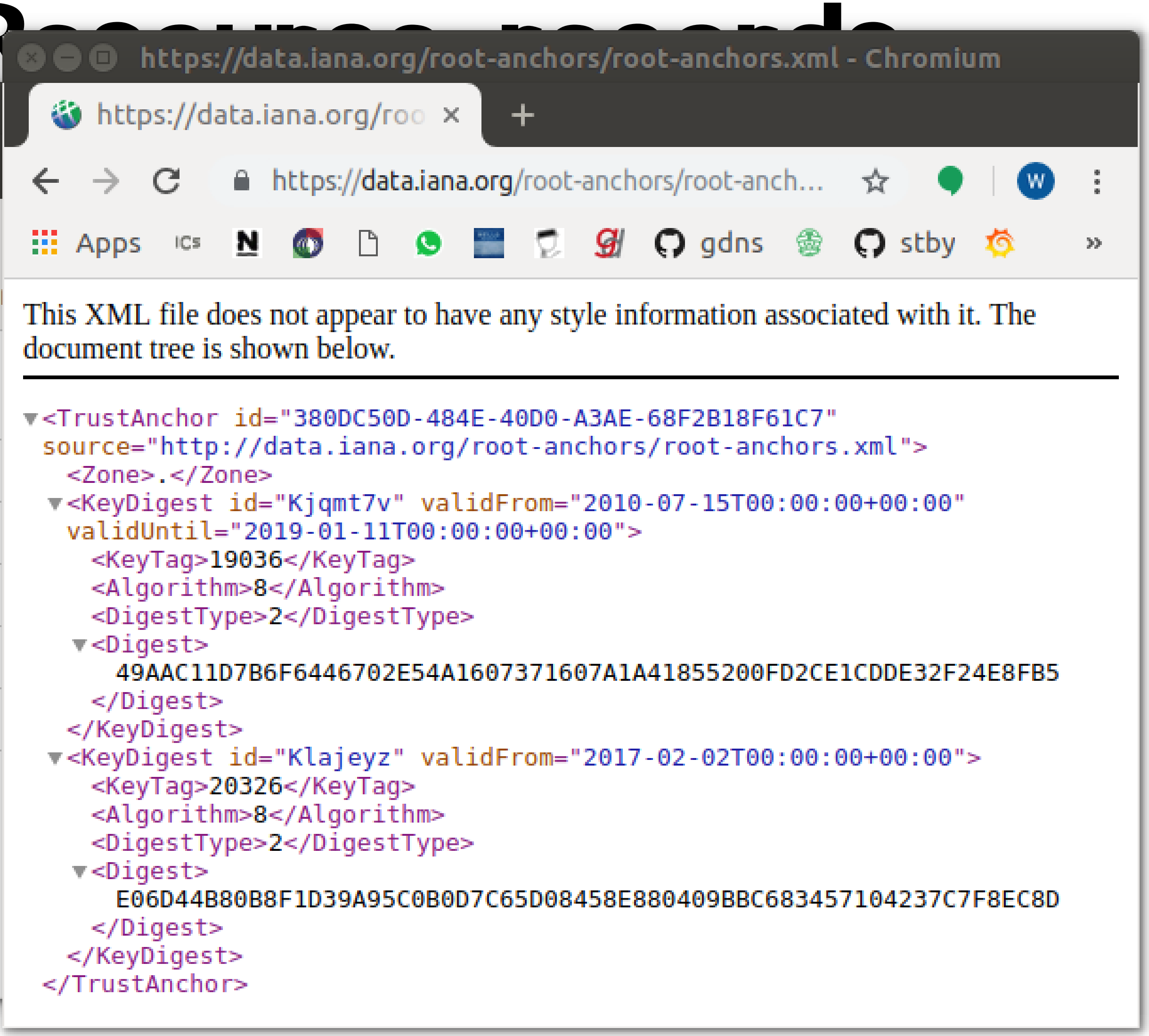
RFC7958

DNSSEC Resource records



Index of /root-anchors - Chromium
Index of /root-anchors
https://data.iana.org/root-an...
Apps

Name	Last modified
Parent Directory	
old/	2018-12-19 20:10
checksums-sha256.txt	2018-12-20 20:33
icannbundle.pem	2017-02-03 00:00
root-anchors.p7s	2018-12-20 20:33
root-anchors.xml	2018-12-19 22:03



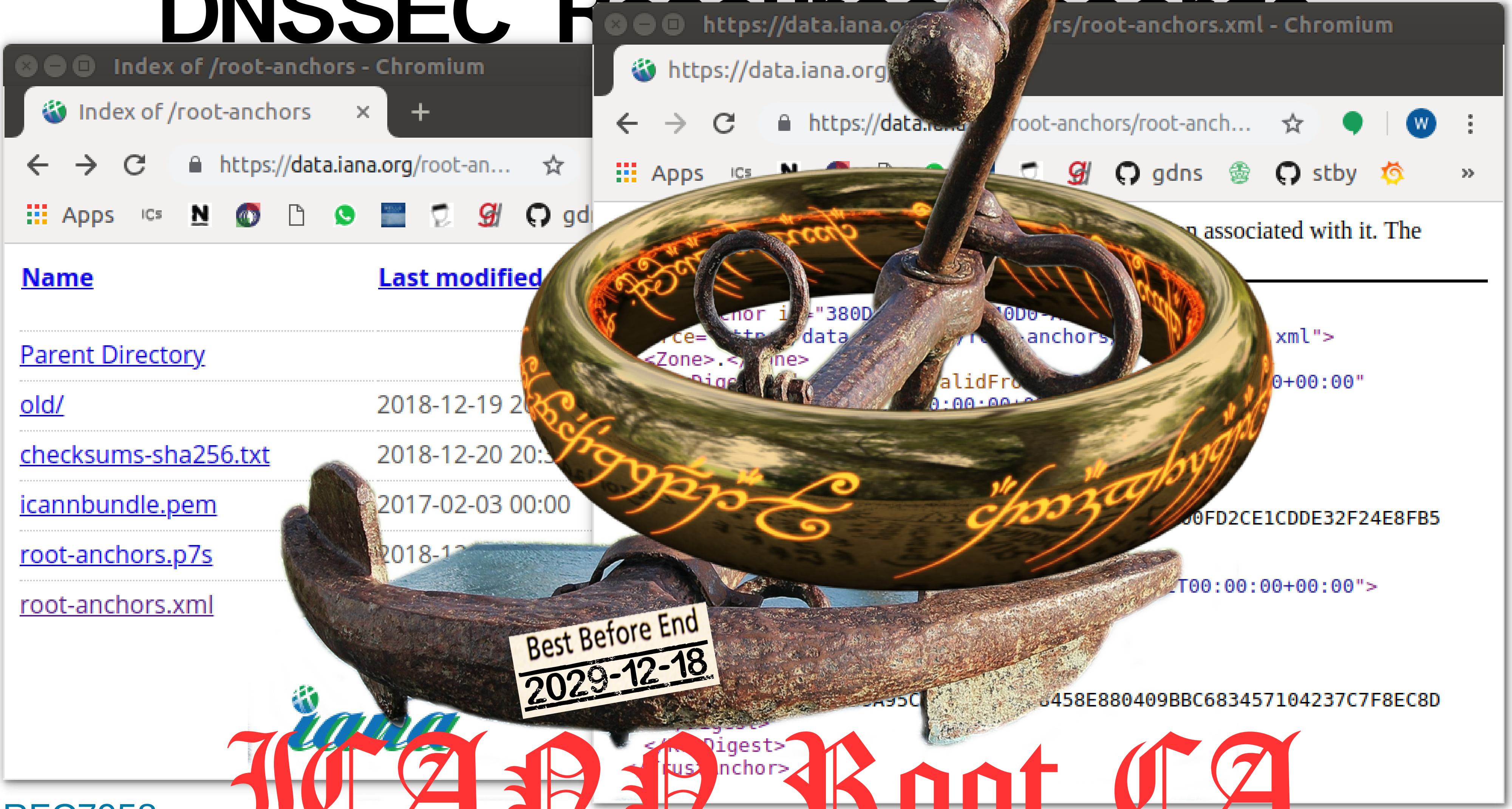
https://data.iana.org/root-anchors/root-anchors.xml - Chromium
https://data.iana.org/roo
https://data.iana.org/root-anchors/root-anch...
Apps
gdns
stby

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<TrustAnchor id="380DC50D-484E-40D0-A3AE-68F2B18F61C7"
 source="http://data.iana.org/root-anchors/root-anchors.xml">
   <Zone>.</Zone>
  ▼<KeyDigest id="Kjqmt7v" validFrom="2010-07-15T00:00:00+00:00"
   validUntil="2019-01-11T00:00:00+00:00">
     <KeyTag>19036</KeyTag>
     <Algorithm>8</Algorithm>
     <DigestType>2</DigestType>
    ▼<Digest>
       49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
     </Digest>
   </KeyDigest>
  ▼<KeyDigest id="Klajeyz" validFrom="2017-02-02T00:00:00+00:00">
     <KeyTag>20326</KeyTag>
     <Algorithm>8</Algorithm>
     <DigestType>2</DigestType>
    ▼<Digest>
       E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
     </Digest>
   </KeyDigest>
 </TrustAnchor>
```

RFC7958

DNSSEC R



Index of /root-anchors - Chromium
Index of /root-anchors
https://data.iana.org/root-an…
Apps
https://data.iana.o rs/root-anchors.xml - Chromium
https://data.iana.org
https://data.iana root-anchors/root-anch…
Apps
gdns
stby
Best Before End
2029-12-18

Name	Last modified
Parent Directory	
old/	2018-12-19 2
checksums-sha256.txt	2018-12-20 20:
icannbundle.pem	2017-02-03 00:00
root-anchors.p7s	2018-1
root-anchors.xml	

n associated with it. The

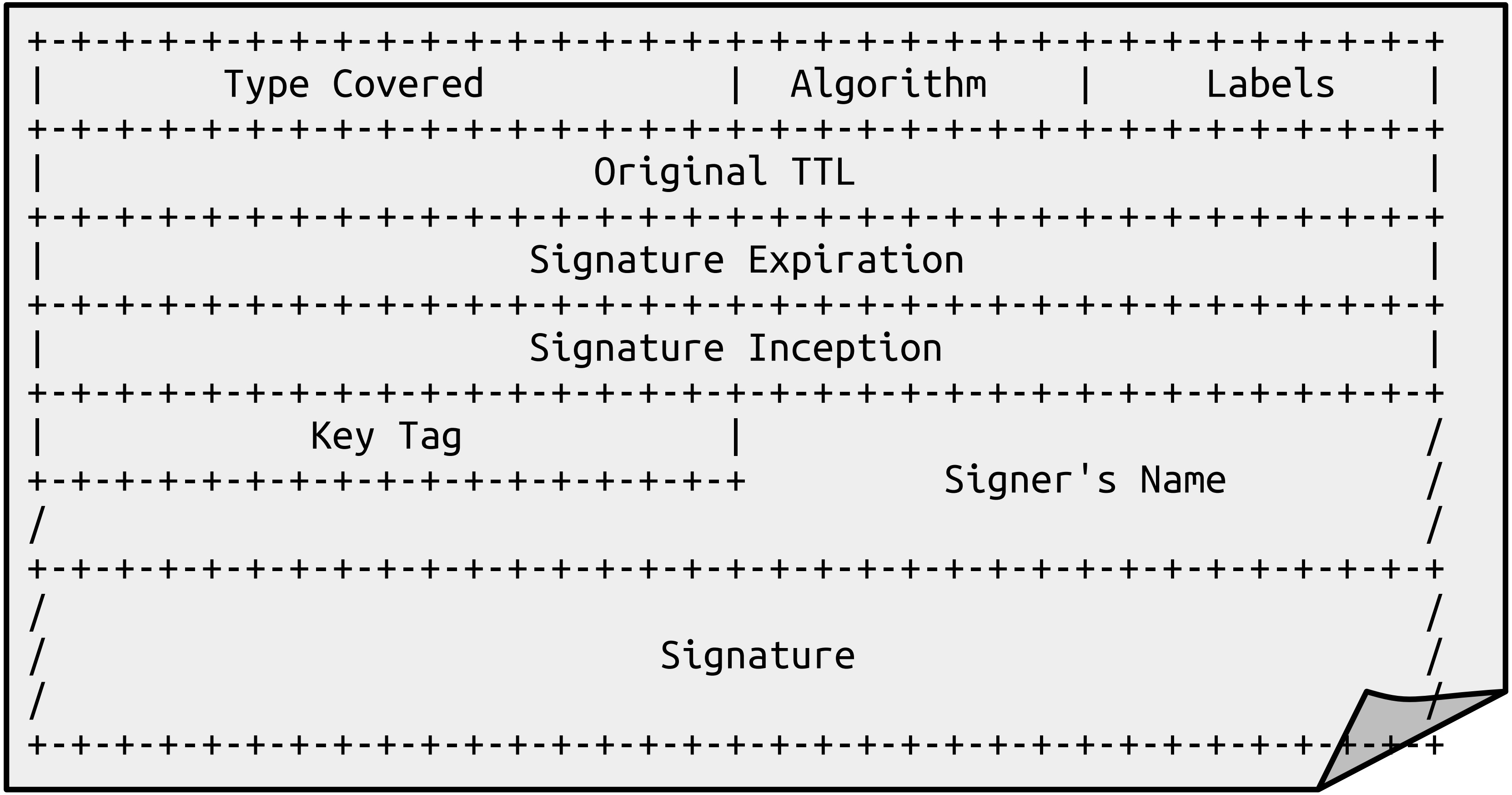
```
  nchor i ="380D      0D0-
  ce= http  data     anchors    xml">
<Zone>.</  ne>
  Dige
                alidFro           0+00:00"
              0:00:00+
                                 0FD2CE1CDDE32F24E8FB5
                                 T00:00:00+00:00">
        A95C          458E880409BBC683457104237C7F8EC8D
      igest>
</   Digest>
   rust anchor>
```

ICANN Root CA

RFC7958

DNSSEC Resource records

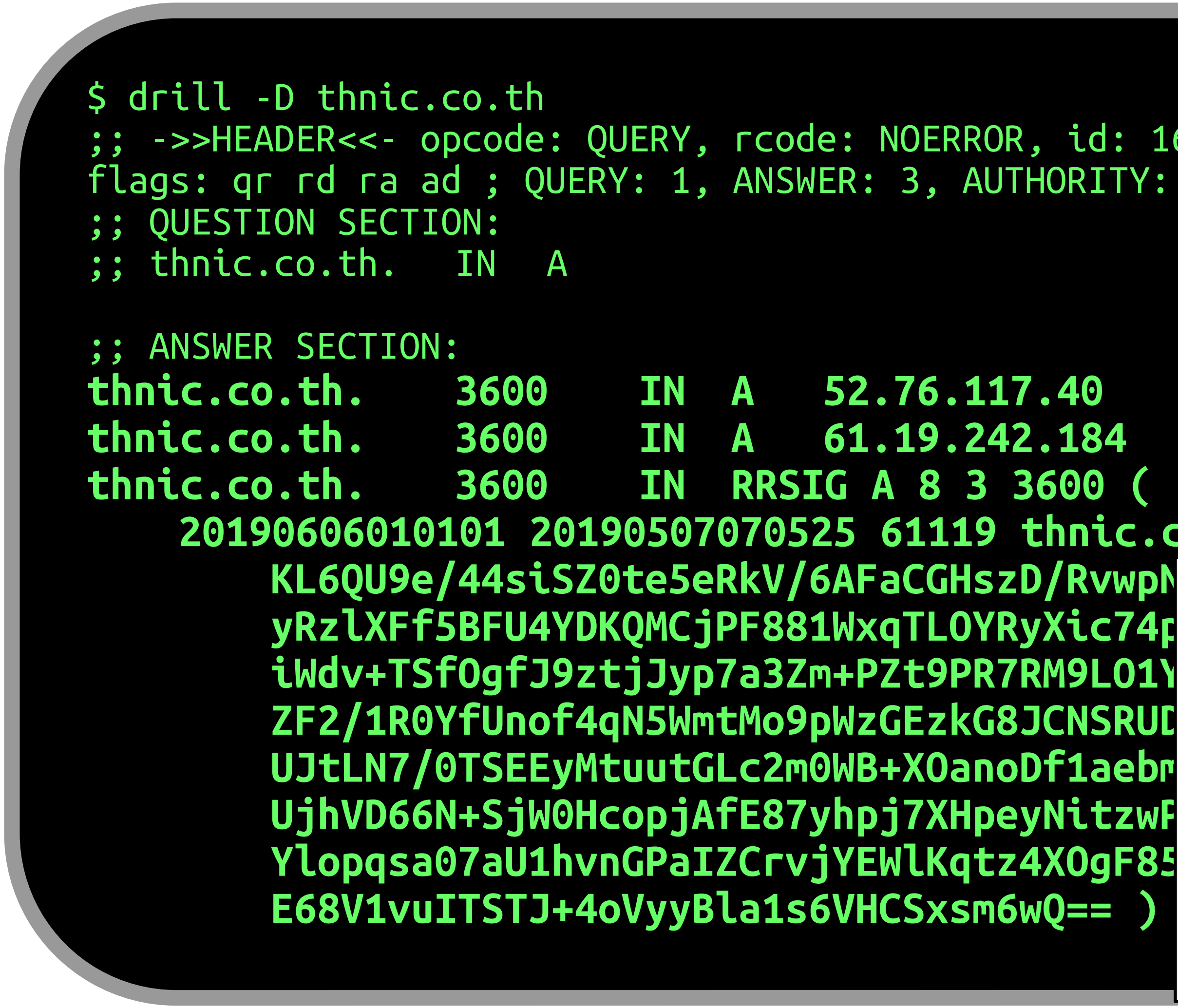
RRSIG



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Type Covered           |  Algorithm    |     Labels    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Original TTL                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Signature Expiration                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Signature Inception                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Key Tag            |                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+         Signer's Name         /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                                               /
/                            Signature                          /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

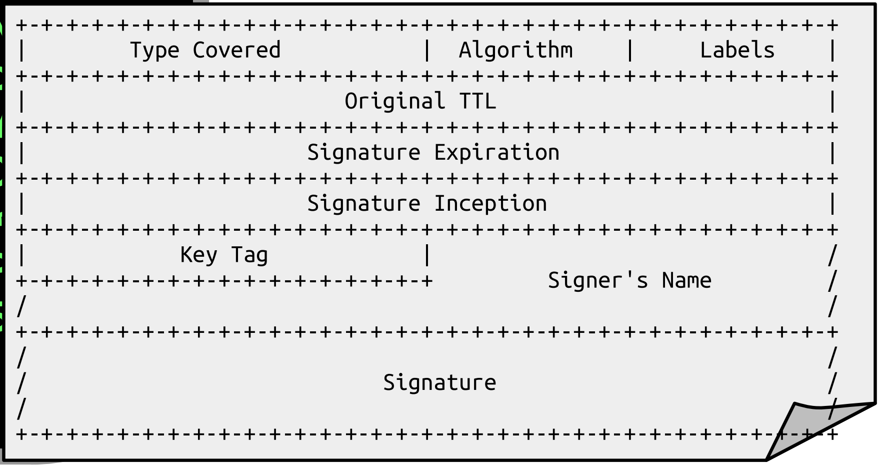
DNSSEC Resource records

RRSIG



```
$ drill -D thnic.co.th
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 16
flags: qr rd ra ad ; QUERY: 1, ANSWER: 3, AUTHORITY:
;; QUESTION SECTION:
;; thnic.co.th.   IN   A

;; ANSWER SECTION:
thnic.co.th.    3600    IN  A   52.76.117.40
thnic.co.th.    3600    IN  A   61.19.242.184
thnic.co.th.    3600    IN  RRSIG A 8 3 3600 (
    20190606010101 20190507070525 61119 thnic.co.th.
        KL6QU9e/44siSZ0te5eRkV/6AFaCGHszD/RvwpN
        yRzlXFf5BFU4YDKQMCjPF881WxqTLOYRyXic74p
        iWdv+TSfOgfJ9ztjJyp7a3Zm+PZt9PR7RM9LO1Y
        ZF2/1R0YfUnof4qN5WmtMo9pWzGEzkG8JCNSRUD
        UJtLN7/0TSEEyMtuutGLc2m0WB+XOanoDf1aebm
        UjhVD66N+SjW0HcopjAfE87yhpj7XHpeyNitzwP
        Ylopqsa07aU1hvnGPaIZCrvjYEWlKqtz4XOgF85
        E68V1vuITSTJ+4oVyyBla1s6VHCSxsm6wQ== )
```

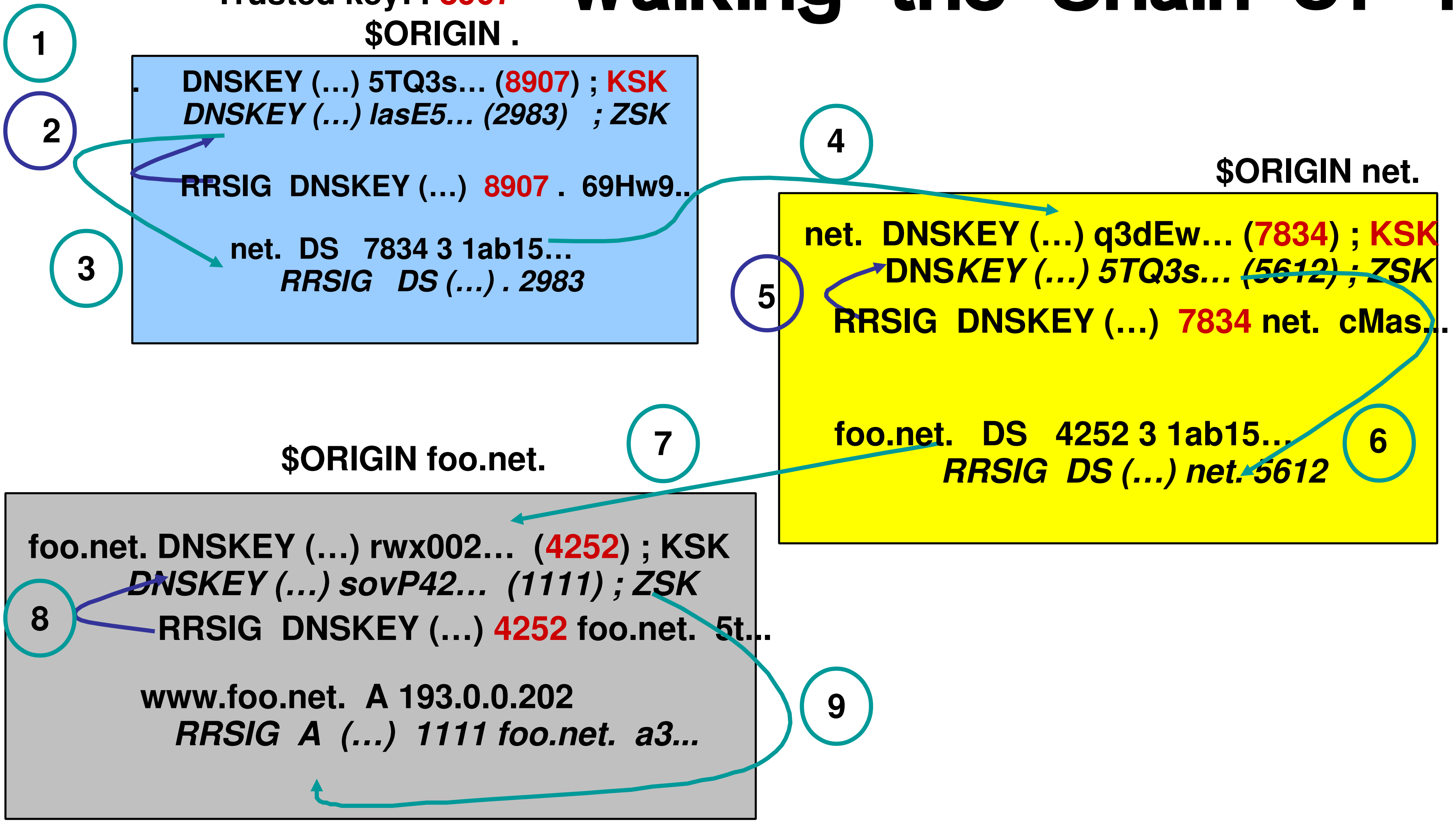
- Signature is over the RRset
- Why?



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Type Covered           |  Algorithm    |     Labels    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Original TTL                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Signature Expiration                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Signature Inception                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Key Tag            |                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+         Signer's Name         /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                                               /
/                            Signature                          /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Walking the Chain of Trust

Locally configured
Trusted key: . 8907



$ORIGIN .

```
.    DNSKEY (…) 5TQ3s… (8907) ; KSK
     DNSKEY (…) lasE5… (2983)   ; ZSK

     RRSIG  DNSKEY (…)  8907 .  69Hw9…

        net.  DS   7834 3 1ab15…
             RRSIG   DS (…) . 2983
```

$ORIGIN net.

```
net.  DNSKEY (…) q3dEw… (7834) ; KSK
      DNSKEY (…) 5TQ3s… (5612) ; ZSK
  RRSIG  DNSKEY (…)  7834 net.  cMas…

  foo.net.   DS   4252 3 1ab15…
           RRSIG  DS (…) net. 5612
```

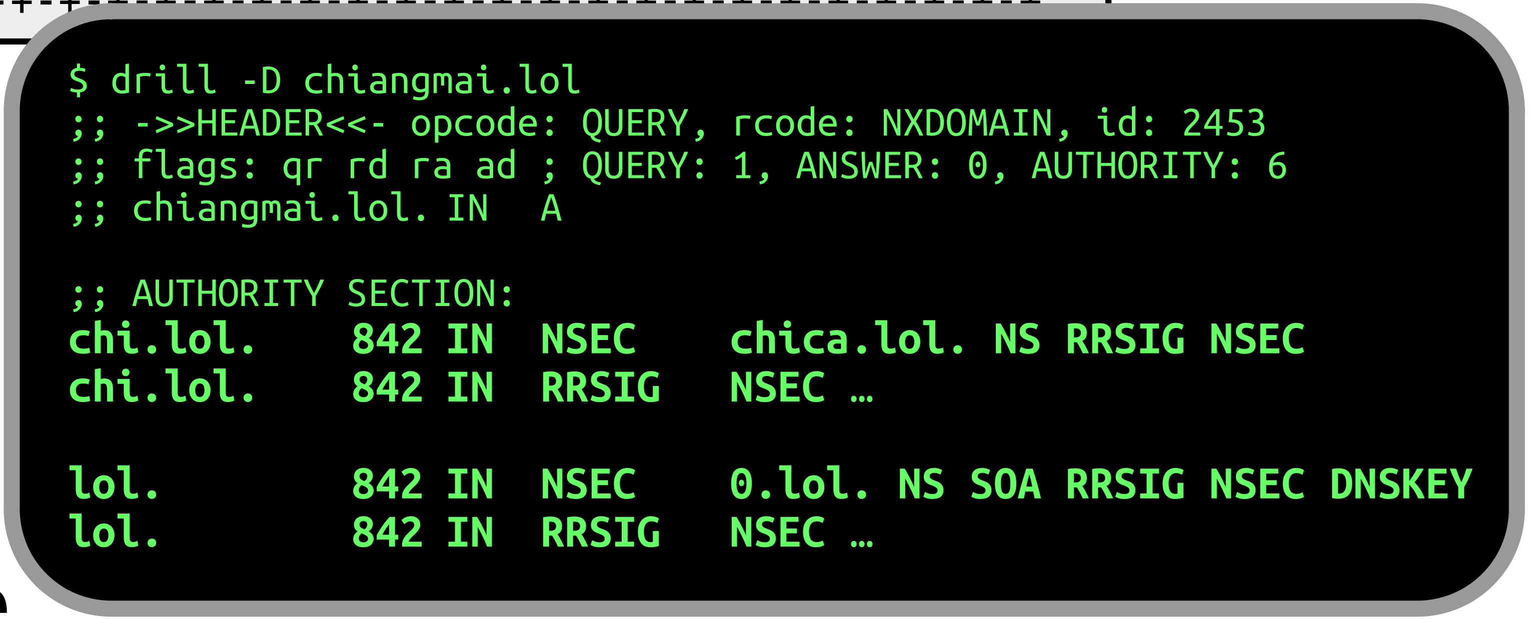
$ORIGIN foo.net.

```
foo.net. DNSKEY (…) rwx002…  (4252) ; KSK
         DNSKEY (…) sovP42…  (1111) ; ZSK
          RRSIG  DNSKEY (…) 4252 foo.net.  5t…

         www.foo.net.  A 193.0.0.202
           RRSIG  A  (…)  1111 foo.net.  a3…
```

DNSSEC Resource records

NSEC

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                      Next Domain Name                         /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                        Type Bit Maps                          /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



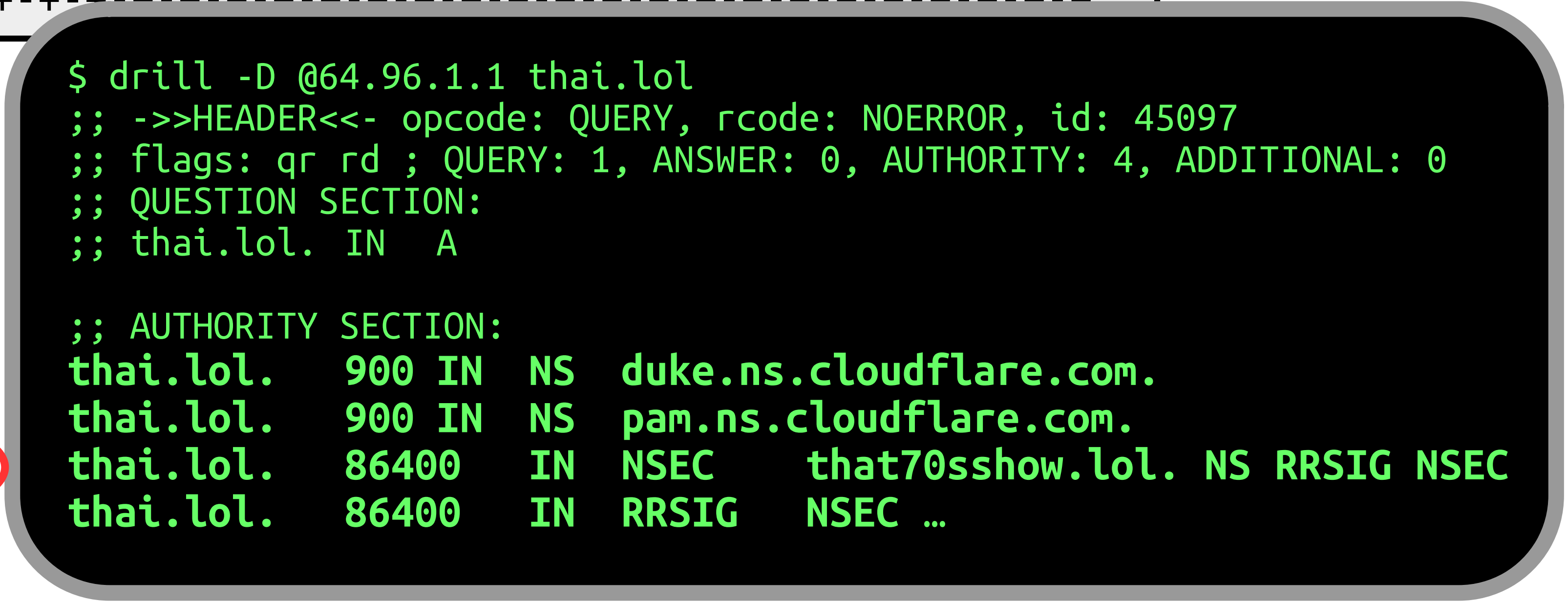
```
$ drill -D chiangmai.lol
;; ->>HEADER<<- opcode: QUERY, rcode: NXDOMAIN, id: 2453
;; flags: qr rd ra ad ; QUERY: 1, ANSWER: 0, AUTHORITY: 6
;; chiangmai.lol. IN   A

;; AUTHORITY SECTION:
chi.lol.     842 IN  NSEC    chica.lol. NS RRSIG NSEC
chi.lol.     842 IN  RRSIG   NSEC …

lol.         842 IN  NSEC    0.lol. NS SOA RRSIG NSEC DNSKEY
lol.         842 IN  RRSIG   NSEC …
```

- Next SECure
- There is nothing between chi.lol. and chica.lol.

DNSSEC Resource records

NSEC

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                      Next Domain Name                         /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                       Type Bit Maps                           /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



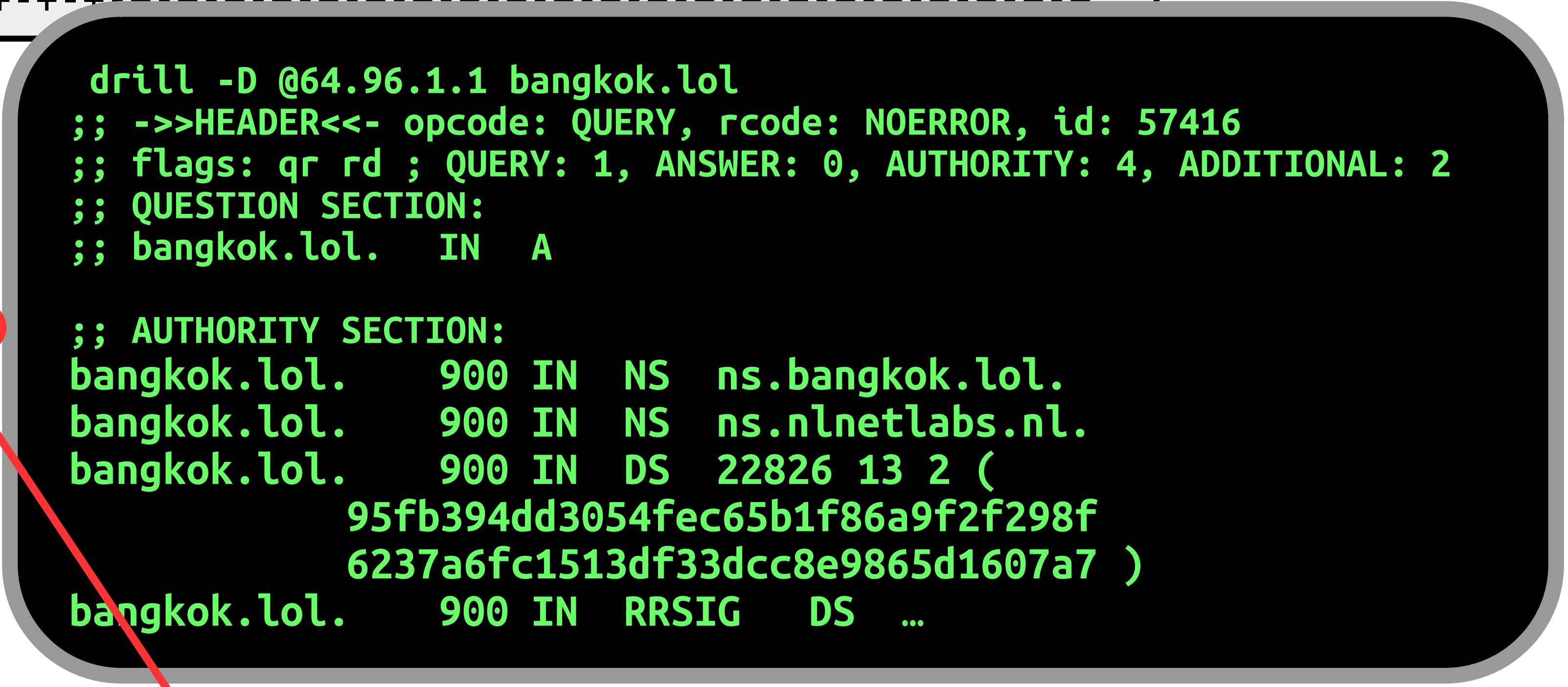
```
$ drill -D @64.96.1.1 thai.lol
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 45097
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 0
;; QUESTION SECTION:
;; thai.lol.  IN   A

;; AUTHORITY SECTION:
thai.lol.   900 IN  NS  duke.ns.cloudflare.com.
thai.lol.   900 IN  NS  pam.ns.cloudflare.com.
thai.lol.   86400   IN  NSEC    that70sshow.lol. NS RRSIG NSEC
thai.lol.   86400   IN  RRSIG   NSEC …
```

- **Secure**
- Insecure
- **BOGUS**
- Indeterminate

DNSSEC Resource records

NSEC

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                      Next Domain Name                         /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                       Type Bit Maps                           /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



```
 drill -D @64.96.1.1 bangkok.lol
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 57416
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 2
;; QUESTION SECTION:
;; bangkok.lol.    IN    A

;; AUTHORITY SECTION:
bangkok.lol.    900 IN  NS  ns.bangkok.lol.
bangkok.lol.    900 IN  NS  ns.nlnetlabs.nl.
bangkok.lol.    900 IN  DS  22826 13 2 (
             95fb394dd3054fec65b1f86a9f2f298f
             6237a6fc1513df33dcc8e9865d1607a7 )
bangkok.lol.    900 IN  RRSIG   DS  …
```

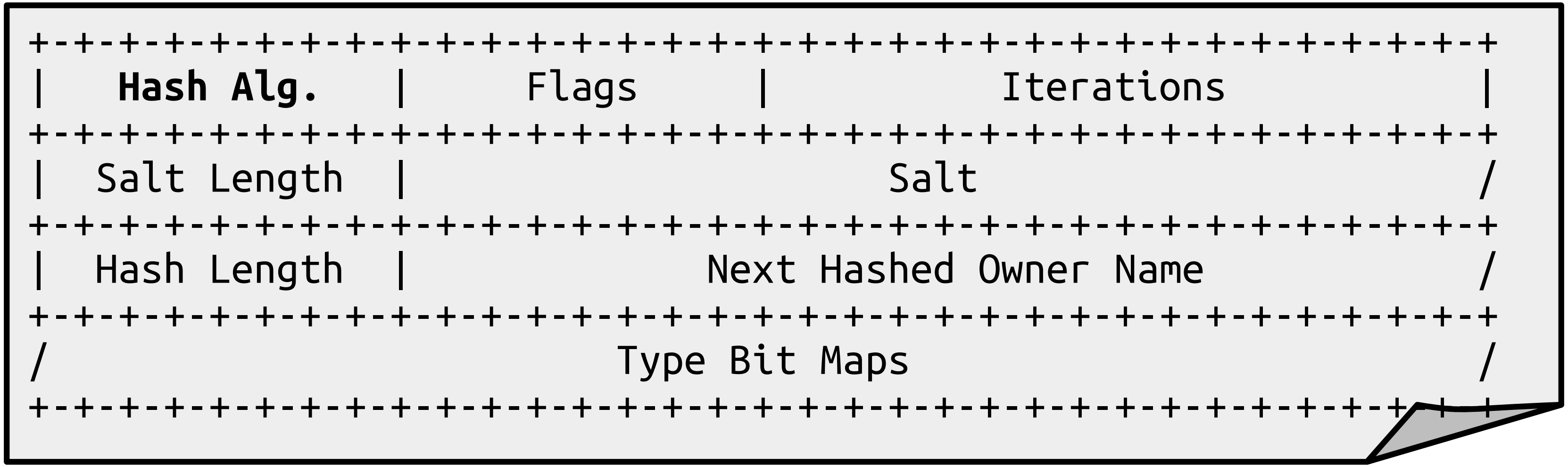
- Secure
- Insecure
- BOGUS
- Indeterminate

- Iff child has matching DNSKEY

RFC5155

DNSSEC Resource records

NSEC3



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Hash Alg.   |     Flags     |          Iterations           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Salt Length  |                     Salt                      /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Hash Length  |             Next Hashed Owner Name            /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                         Type Bit Maps                         /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

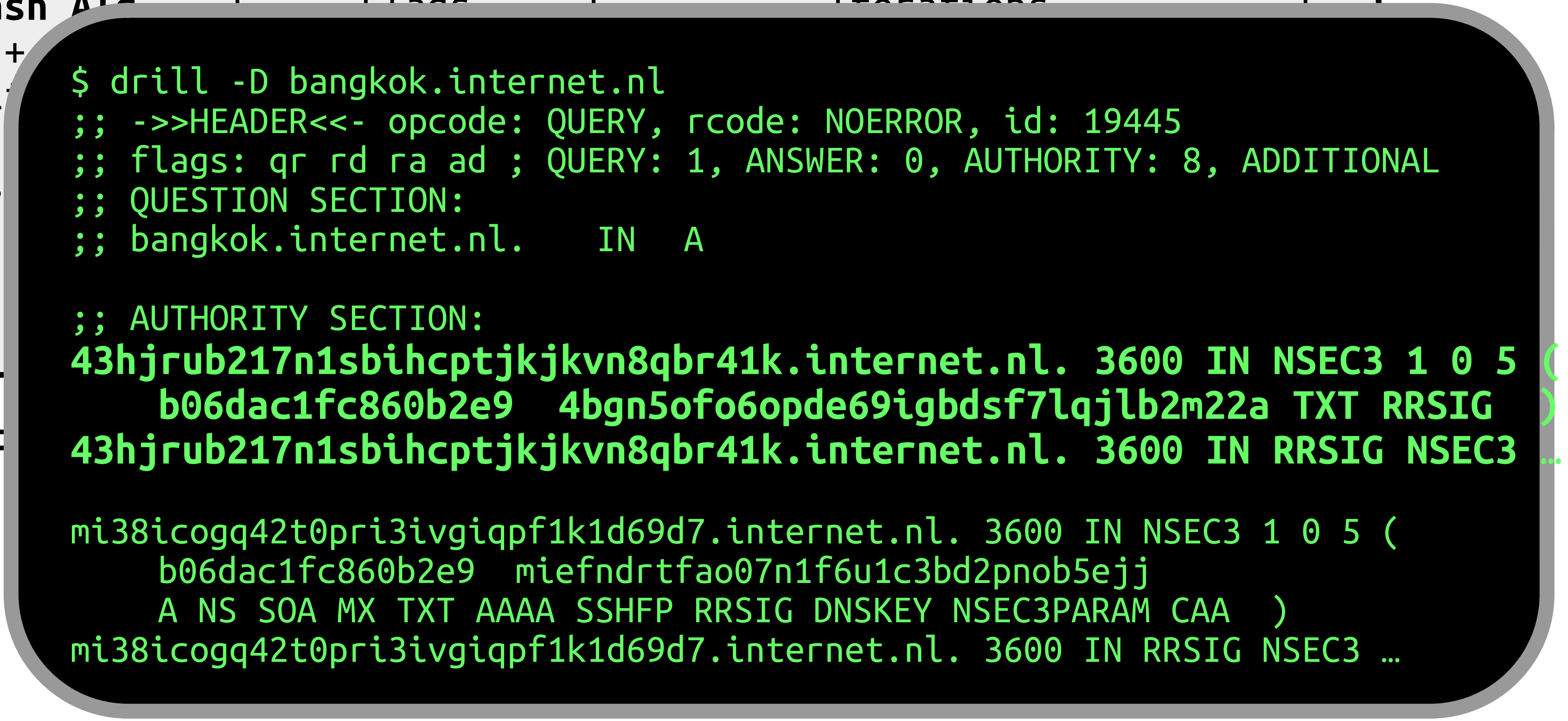
1 = SHA1

DNSSEC Resource records

NSEC3

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Hash Alg    |     Flags     |          Iterations           |
+-+-+-+-+
|  Sal
+-+-+-+-
|  Has
+-+-+-+-
/
+-+-+-+-
```

- 1 =

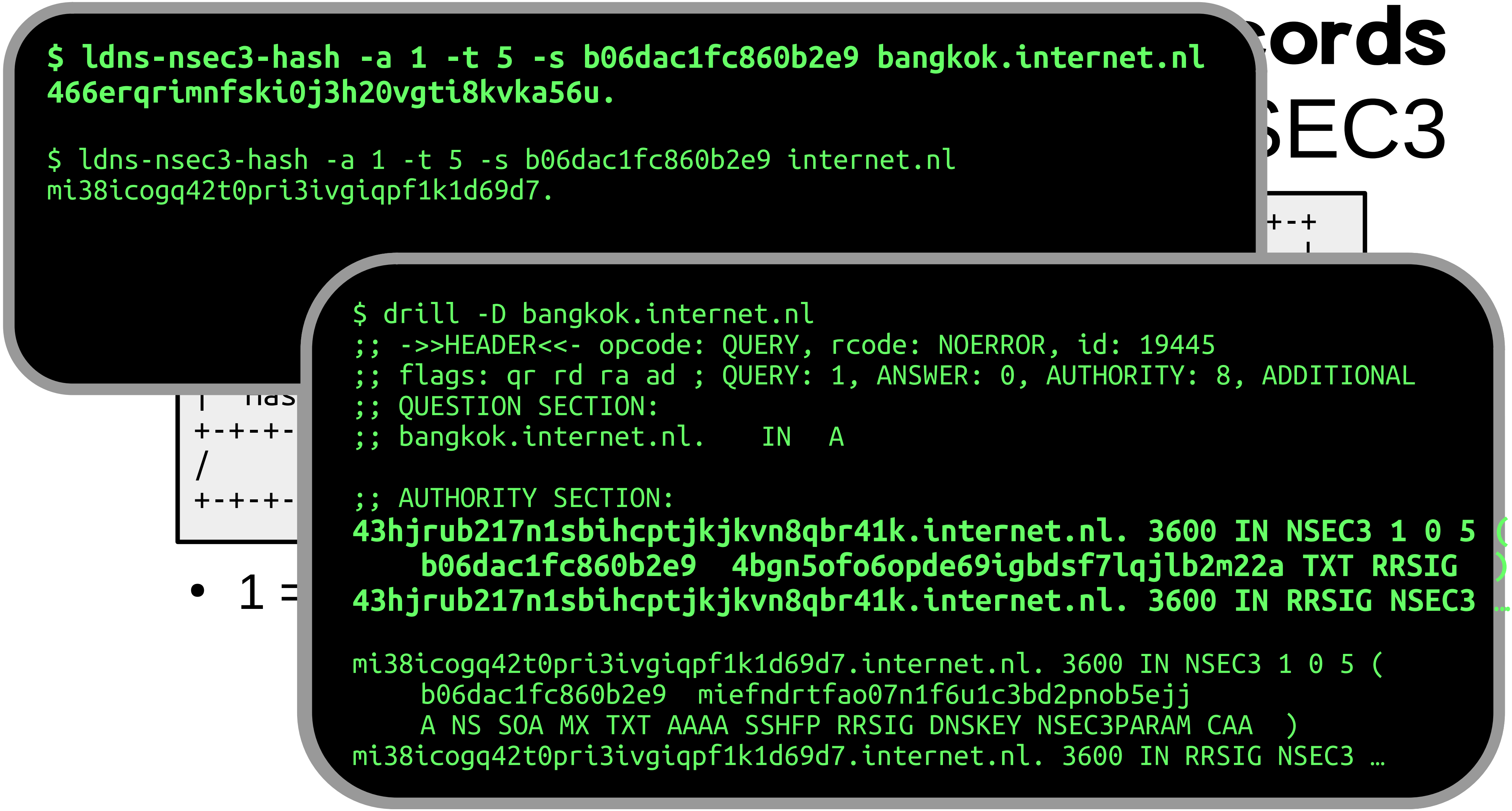


```
$ drill -D bangkok.internet.nl
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 19445
;; flags: qr rd ra ad ; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL
;; QUESTION SECTION:
;; bangkok.internet.nl.    IN   A

;; AUTHORITY SECTION:
43hjrub217n1sbihcptjkjkvn8qbr41k.internet.nl. 3600 IN NSEC3 1 0 5 (
    b06dac1fc860b2e9  4bgn5ofo6opde69igbdsf7lqjlb2m22a TXT RRSIG )
43hjrub217n1sbihcptjkjkvn8qbr41k.internet.nl. 3600 IN RRSIG NSEC3 …

mi38icogq42t0pri3ivgiqpf1k1d69d7.internet.nl. 3600 IN NSEC3 1 0 5 (
    b06dac1fc860b2e9  miefndrtfao07n1f6u1c3bd2pnob5ejj
    A NS SOA MX TXT AAAA SSHFP RRSIG DNSKEY NSEC3PARAM CAA  )
mi38icogq42t0pri3ivgiqpf1k1d69d7.internet.nl. 3600 IN RRSIG NSEC3 …
```

…cords
…SEC3

```
+-+
|
|  has
+-+-+-
/
+-+-+-
```

- 1 =

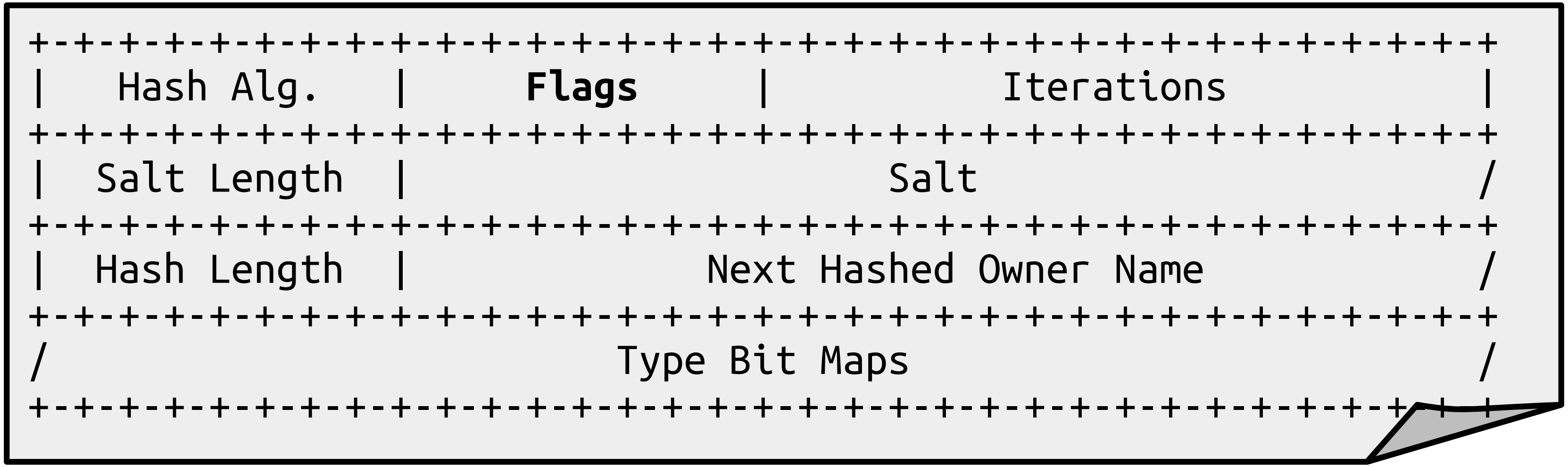


```
$ ldns-nsec3-hash -a 1 -t 5 -s b06dac1fc860b2e9 bangkok.internet.nl
466erqrimnfski0j3h20vgti8kvka56u.

$ ldns-nsec3-hash -a 1 -t 5 -s b06dac1fc860b2e9 internet.nl
mi38icogq42t0pri3ivgiqpf1k1d69d7.
```

```
$ drill -D bangkok.internet.nl
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 19445
;; flags: qr rd ra ad ; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL
;; QUESTION SECTION:
;; bangkok.internet.nl.    IN   A

;; AUTHORITY SECTION:
43hjrub217n1sbihcptjkjkvn8qbr41k.internet.nl. 3600 IN NSEC3 1 0 5 (
    b06dac1fc860b2e9  4bgn5ofo6opde69igbdsf7lqjlb2m22a TXT RRSIG  )
43hjrub217n1sbihcptjkjkvn8qbr41k.internet.nl. 3600 IN RRSIG NSEC3 …

mi38icogq42t0pri3ivgiqpf1k1d69d7.internet.nl. 3600 IN NSEC3 1 0 5 (
    b06dac1fc860b2e9  miefndrtfao07n1f6u1c3bd2pnob5ejj
    A NS SOA MX TXT AAAA SSHFP RRSIG DNSKEY NSEC3PARAM CAA  )
mi38icogq42t0pri3ivgiqpf1k1d69d7.internet.nl. 3600 IN RRSIG NSEC3 …
```

DNSSEC Resource records

NSEC3

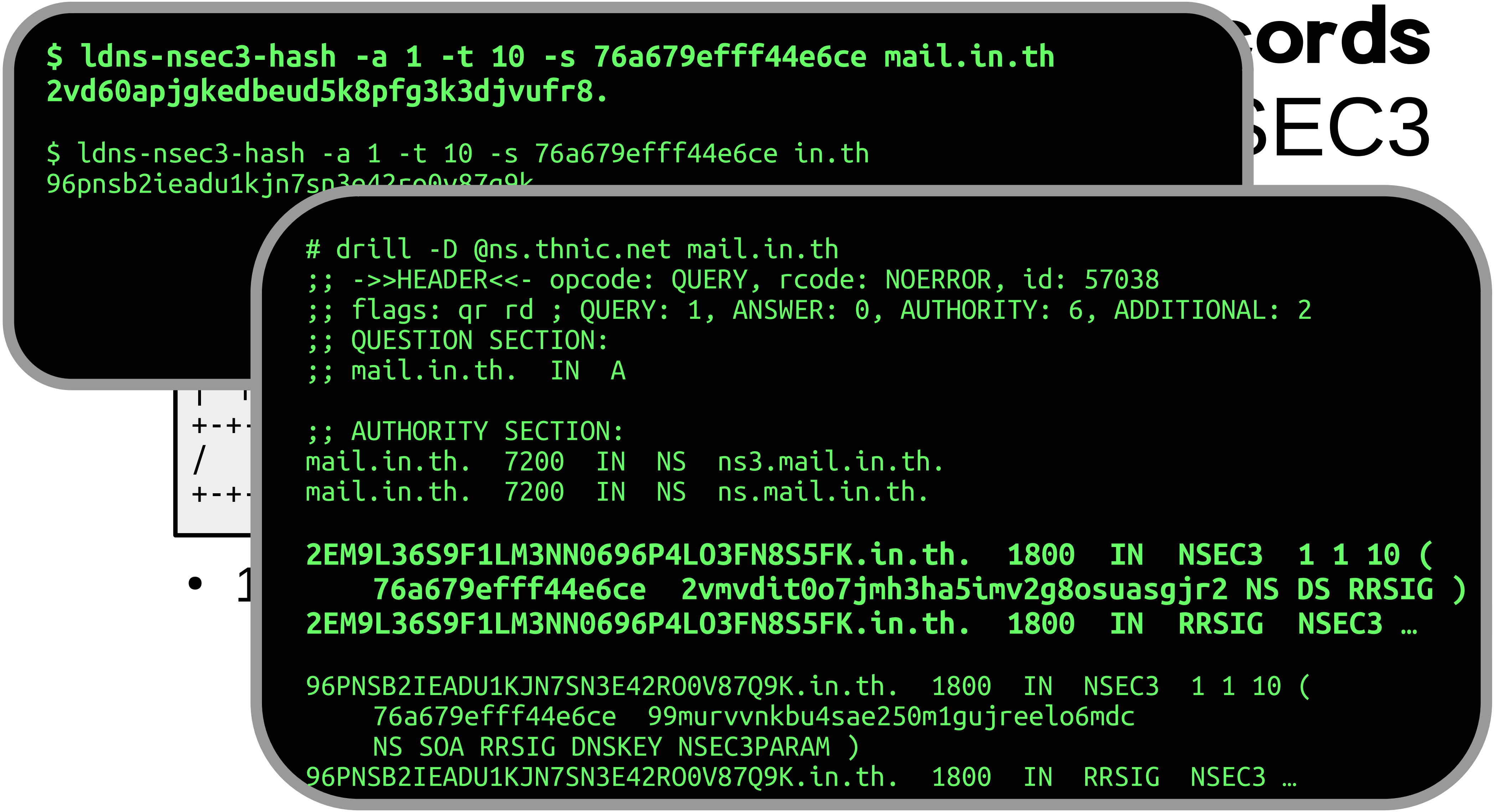


```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Hash Alg.   |     Flags     |          Iterations           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Salt Length  |                     Salt                      /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Hash Length  |             Next Hashed Owner Name            /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                         Type Bit Maps                         /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- 1 = Opt-out

cords

SEC3



```
$ ldns-nsec3-hash -a 1 -t 10 -s 76a679efff44e6ce mail.in.th
2vd60apjgkedbeud5k8pfg3k3djvufr8.

$ ldns-nsec3-hash -a 1 -t 10 -s 76a679efff44e6ce in.th
96pnsb2ieadu1kjn7sn3e42ro0v87q9k
```

```
# drill -D @ns.thnic.net mail.in.th
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 57038
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 2
;; QUESTION SECTION:
;; mail.in.th.   IN   A

;; AUTHORITY SECTION:
mail.in.th.  7200  IN  NS  ns3.mail.in.th.
mail.in.th.  7200  IN  NS  ns.mail.in.th.

2EM9L36S9F1LM3NN0696P4LO3FN8S5FK.in.th.  1800  IN  NSEC3  1 1 10 (
    76a679efff44e6ce  2vmvdit0o7jmh3ha5imv2g8osuasgjr2 NS DS RRSIG )
2EM9L36S9F1LM3NN0696P4LO3FN8S5FK.in.th.  1800  IN  RRSIG  NSEC3 …

96PNSB2IEADU1KJN7SN3E42RO0V87Q9K.in.th.  1800  IN  NSEC3  1 1 10 (
    76a679efff44e6ce  99murvvnkbu4sae250m1gujreelo6mdc
    NS SOA RRSIG DNSKEY NSEC3PARAM )
96PNSB2IEADU1KJN7SN3E42RO0V87Q9K.in.th.  1800  IN  RRSIG  NSEC3 …
```

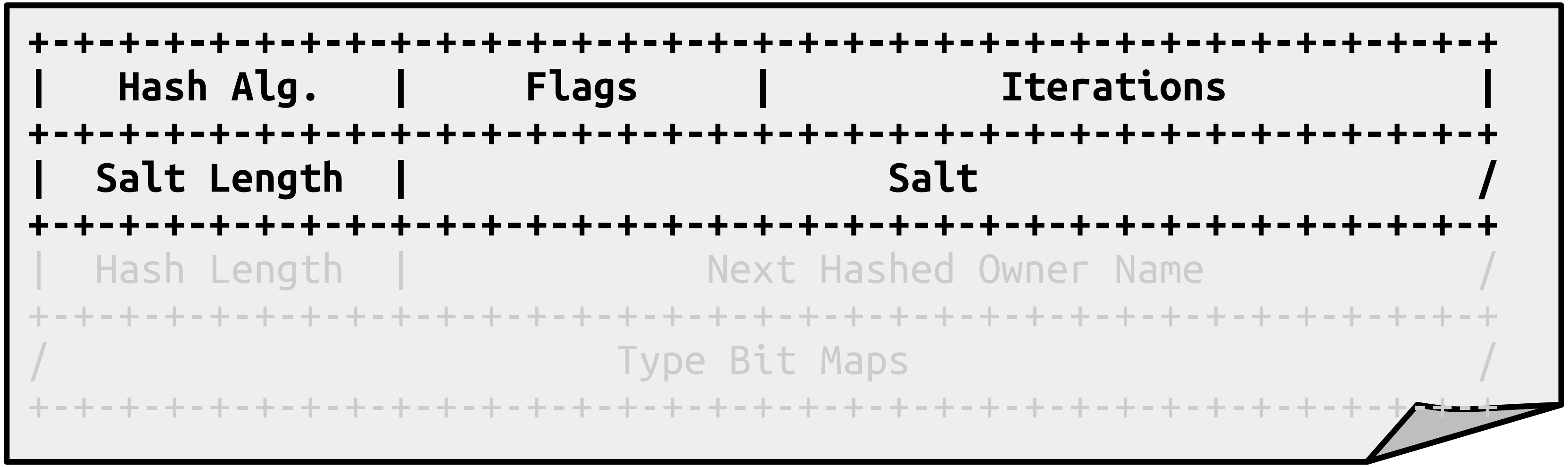
```
+-+-
/
+-+-
```

- 1

RFC5155

DNSSEC Resource records

NSEC3PARAM



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Hash Alg.   |     Flags     |          Iterations           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Salt Length  |                     Salt                      /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Hash Length  |             Next Hashed Owner Name            /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                         Type Bit Maps                         /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Lab time!

- Hands on: http://bangkok.lol/
- 6. Signing your zone the primitive way

Photo by Alex Kondratiev on Unsplash