Lying Makes Negative Answers Cheaper

Dani Grant | dani@cloudflare.com | @thedanigrant

57 Billion Record Sets

CloudFlare Daily Signature Count

NXDOMAIN

Name does not exist.

```
dig bogus.ietf.org
```

SOA

```
ietf.org. 1179 IN SOA ns0.amsl.com. glen.amsl.com. 1200000325 1800 1800 604800
1800
```

SOA

```
ietf.org. 1179 IN SOA ns0.amsl.com. glen.amsl.com. 1200000325 1800 1800 604800
1800
```

SOA RRSIG

```
ietf.org. 1179 IN   RRSIG     SOA 5 2 1800 20170308083354 20160308073501 40452
ietf.org. S0gIjTnQGA6TyIBjCeBXL4ip8aEQEgg2y+kCQ3sLtFa3oNy9vj9kj4aP
8EVu4oIexr8X/i9L8Oj5ec4HOrQoYsMGObRUG0FGT0MEbxepi+wWrfed
vD/3mq8KZg/pj6TQAKebeSQGkmb8y9eP0PdWdUi6EatH9ZY/tsoiKyqg
U4vtq9sWZ/4mH3xfhK9RBI4M7XIXsPX+biZoik6aOt4zSWR5WDq27pXI
0l+BLzZb72C7McT4PlBiF+U86OngBlGxVBnILyW2aUisi2LY6KeO5AmK
WNT0xHWe5+JtPD5PgmSm46YZ8jMP5mH4hSYr76jqwvlCtXvq8XgYQU/P QyuCpQ==
```

SOA

```
ietf.org. 1179 IN SOA ns0.amsl.com. glen.amsl.com. 1200000325 1800 1800 604800
1800
```

SOA RRSIG

```
ietf.org. 1179 IN   RRSIG     SOA 5 2 1800 20170308083354 20160308073501 40452
ietf.org. S0gIjTnQGA6TyIBjCeBXL4ip8aEQEgg2y+kCQ3sLtFa3oNy9vj9kj4aP
8EVu4oIexr8X/i9L8Oj5ec4HOrQoYsMGObRUG0FGT0MEbxepi+wWrfed
vD/3mq8KZg/pj6TQAKebeSQGkmb8y9eP0PdWdUi6EatH9ZY/tsoiKyqg
U4vtq9sWZ/4mH3xfhK9RBI4M7XIXsPX+biZoik6aOt4zSWR5WDq27pXI
0l+BLzZb72C7McT4PlBiF+U86OngBlGxVBnILyW2aUisi2LY6KeO5AmK
WNT0xHWe5+JtPD5PgmSm46YZ8jMP5mH4hSYr76jqwvlCtXvq8XgYQU/P QyuCpQ==
```

NSEC

```
www.apps.ietf.org. 1062 IN NSEC cloudflare-verify.ietf.org. A RRSIG NSEC
```

CLOUDFLARE

SOA

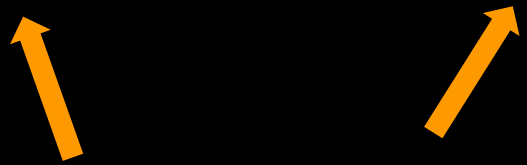
```
ietf.org. 1179 IN SOA ns0.amsl.com. glen.amsl.com. 1200000325 1800 1800 604800
1800
```

SOA RRSIG

```
ietf.org. 1179 IN   RRSIG     SOA 5 2 1800 20170308083354 20160308073501 40452
ietf.org. S0gIjTnQGA6TyIBjCeBXL4ip8aEQEgg2y+kCQ3sLtFa3oNy9vj9kj4aP
8EVu4oIexr8X/i9L8Oj5ec4HOrQoYsMGObRUG0FGT0MEbxepi+wWrfed
vD/3mq8KZg/pj6TQAKebeSQGkmb8y9eP0PdWdUi6EatH9ZY/tsoiKyqg
U4vtq9sWZ/4mH3xfhK9RBI4M7XIXsPX+biZoik6aOt4zSWR5WDq27pXI
0l+BLzZb72C7McT4PlBiF+U86OngBlGxVBnILyW2aUisi2LY6KeO5AmK
WNT0xHWe5+JtPD5PgmSm46YZ8jMP5mH4hSYr76jqwvlCtXvq8XgYQU/P QyuCpQ==
```

NSEC

```
www.apps.ietf.org. 1062 IN NSEC cloudflare-verify.ietf.org. A RRSIG NSEC
```



bogus.ietf.org is between these two names

CLOUDFLARE

SOA

```
ietf.org. 1179 IN SOA ns0.amsl.com. glen.amsl.com. 1200000325 1800 1800 604800
1800
```

SOA RRSIG

```
ietf.org. 1179 IN   RRSIG     SOA 5 2 1800 20170308083354 20160308073501 40452
ietf.org. S0gIjTnQGA6TyIBjCeBXL4ip8aEQEgg2y+kCQ3sLtFa3oNy9vj9kj4aP
8EVu4oIexr8X/i9L8Oj5ec4HOrQoYsMGObRUG0FGT0MEbxepi+wWrfed
vD/3mq8KZg/pj6TQAKebeSQGkmb8y9eP0PdWdUi6EatH9ZY/tsoiKyqg
U4vtq9sWZ/4mH3xfhK9RBI4M7XIXsPX+biZoik6aOt4zSWR5WDq27pXI
0l+BLzZb72C7McT4PlBiF+U86OngBlGxVBnILyW2aUisi2LY6KeO5AmK
WNT0xHWe5+JtPD5PgmSm46YZ8jMP5mH4hSYr76jqwvlCtXvq8XgYQU/P QyuCpQ==
```

NSEC

```
www.apps.ietf.org. 1062 IN NSEC cloudflare-verify.ietf.org. A RRSIG NSEC
```

NSEC RRSIG

```
www.apps.ietf.org. 1062 IN RRSIG NSEC 5 4 1800 20170308083322 20160308073501
40452 ietf.org. NxmjhCkTtoiolJUow/OreeBRxTtf2AnIPM/r2p7oS/hNeOdFI9tpgGQY
g0lTOYjcNNoIoDB/r56Kd+5wtuaKT+xsYiZ4K413I+cmrNQ+6oLT+Mz6
Kfzvo/TcrJD99PVAYIN1MwzO42od/vi/juGkuKJVcCzrBKNHCZqu7clu
mU3DEqbQQT2O8dYIUjLlfom1iYtZZrfuhB6FCYFTRd3h8OLfMhXtt8f5
8Q/XvjakiLqov1blZAK229I2qgUYEhd77n2pXV6SJuOKcSjZiQsGJeaM
wIotSKa8EttJELkpNAUkN9uXfhU+WjouS1qzgyWwbf2hdgsBntKP9his 9MfJNA==
```

CLOUDFLARE

SOA

```
ietf.org. 1179 IN SOA ns0.amsl.com. glen.amsl.com. 1200000325 1800 1800 604800
1800
```

SOA RRSIG

```
ietf.org. 1179 IN   RRSIG     SOA 5 2 1800 20170308083354 20160308073501 40452
ietf.org. S0gIjTnQGA6TyIBjCeBXL4ip8aEQEgg2y+kCQ3sLtFa3oNy9vj9kj4aP
8EVu4oIexr8X/i9L8Oj5ec4HOrQoYsMGObRUG0FGT0MEbxepi+wWrfed
vD/3mq8KZg/pj6TQAKebeSQGkmb8y9eP0PdWdUi6EatH9ZY/tsoiKyqg
U4vtq9sWZ/4mH3xfhK9RBI4M7XIXsPX+biZoik6aOt4zSWR5WDq27pXI
0l+BLzZb72C7McT4PlBiF+U86OngBlGxVBnILyW2aUisi2LY6KeO5AmK
WNT0xHWe5+JtPD5PgmSm46YZ8jMP5mH4hSYr76jqwvlCtXvq8XgYQU/P QyuCpQ==
```

NSEC

```
www.apps.ietf.org. 1062 IN NSEC cloudflare-verify.ietf.org. A RRSIG NSEC
```

NSEC RRSIG

```
www.apps.ietf.org. 1062 IN RRSIG NSEC 5 4 1800 20170308083322 20160308073501
40452 ietf.org. NxmjhCkTtoiolJUow/OreeBRxTtf2AnIPM/r2p7oS/hNeOdFI9tpgGQY
g0lTOYjcNNoIoDB/r56Kd+5wtuaKT+xsYiZ4K413I+cmrNQ+6oLT+Mz6
Kfzvo/TcrJD99PVAYIN1MwzO42od/vi/juGkuKJVcCzrBKNHCZqu7clu
mU3DEqbQQT2O8dYIUjLlfom1iYtZZrfuhB6FCYFTRd3h8OLfMhXtt8f5
8Q/XvjakiLqov1blZAK229I2qgUYEhd77n2pXV6SJuOKcSjZiQsGJeaM
wIotSKa8EttJELkpNAUkN9uXfhU+WjouS1qzgyWwbf2hdgsBntKP9his 9MfJNA==
```

I ran out of space, continuing on the next page


SOA
SOA RRSIG
NSEC
NSEC RRSIG

NSEC

```
ietf.org. 1062 IN NSEC ietf1._domainkey.ietf.org. A NS SOA MX TXT AAAA RRSIG
NSEC DNSKEY SPF
```

SOA | SOA RRSIG | NSEC | NSEC RRSIG

NSEC

```
ietf.org. 1062 IN NSEC ietf1._domainkey.ietf.org. A NS SOA MX TXT AAAA RRSIG
NSEC DNSKEY SPF
```

*.ietf.org would exist between these names

CLOUDFLARE

SOA | SOA RRSIG | NSEC | NSEC RRSIG

NSEC

```
ietf.org. 1062 IN NSEC ietf1._domainkey.ietf.org. A NS SOA MX TXT AAAA RRSIG
NSEC DNSKEY SPF
```

NSEC RRSIG

```
ietf.org. 1062 IN RRSIG NSEC 5 2 1800 20170308083303 20160308073501 40452 ietf.
org. homg5NrZIKo0tR+aEp0MVYYjT7J/KGTKP46bJ8eeetbq4KqNvLKJ5Yig
ve4RSWFYrSARAmbi3GIFW00P/dFCzDNVlMWYRbcFUt5NfYRJxg25jy95
yHNmInwDUnttmzKuBezdVVvRLJY3qSM7S3VfI/b7n6++ODUFcsL88uNB
V6bRO6FOksgE1/jUrtz6/lEKmodWWI2goFPGgmgihqLR8ldv0Dv7k9vy
Ao1uunP6kDQEj+omkICFHaT/DBSSYq59DVeMAAcfDq2ssbr4p8hUoXiB
tNlJWEubMnHi7YmLSgby+m8b97+8b6qPe8W478gAiggsNjc2gQSKOOXH EejOSA==
```

CLOUDFLARE

for the wildcard

for the previous and next name

```
ietf.org. 1179 IN SOA ns0.amsl.com. glen.amsl.com. 1200000325 1800 1800 604800 1800

ietf.org.    1179   IN    RRSIG  SOA 5 2 1800 20170308083354 20160308073501 40452 ietf.org.
S0gIjTnQGA6TyIBjCeBXL4ip8aEQEgg2y+kCQ3sLtFa3oNy9vj9kj4aP 8EVu4oIexr8X/i9L8Oj5ec4HOrQoYsMGObRUG0FGT0MEbxepi+wWrfed
vD/3mq8KZg/pj6TQAKebeSQGkmb8y9eP0PdWdUi6EatH9ZY/tsoiKyqg U4vtq9sWZ/4mU3xfhK9RBI4M7XIXsPX+biZoik6aOt4zSWR5WDq27pXI
0l+BLzZb72C7McT4PlBiF+U86OngBlGxVBnILyW2aUisi2LY6Ko5[illegible]5PgmSm46YZ8jMP5mH4hSYr76jqwvlCtXvq8XgYQU/P
QyuCpQ==

www.apps.ietf.org. 106[illegible]

www.apps.ietf.org. 1062[illegible]501 40452 ietf.org.
NxmjhCkTtoiolJUow/OreeB[illegible]r56Kd+5wtuaKT+xsYiZ4K413I+cmrNQ+6oLT+Mz6
Kfzvo/TcrJD99PVAYIN1Mwz[illegible]jLlfom1iYtZZrfuhB6FCYFTRd3h8OLfMhXtt8f5
8Q/XvjakiLqov1blZAK229I2[illegible]sKa8EttJELkpNAUkN9uXfhU+WjouS1qzgyWwbf2hdgsBntKP9his
9MfJNA==

ietf.org. 1062 IN NSEC ietf1._domainkey.ietf.org. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY SPF

ietf.org. 1062 IN RRSIG NSEC 5 2 1800 20170308083303 20160308073501 40452 ietf.org.
homg5NrZIKo0tR+aEp0MVYYjT7J/KGTKP46bJ8eeetbq4KqNvLKJ5Yig ve4RSWFYrSARAmbi3GIFW00P/dFCzDNVlMWYRbcFUt5NfYRJxg25jy95
yHNmInwDUnttmzKuBezdVVvRLJY3qSM7S3VfI/b7n6++ODUFcsL88uNB V6bRO6FOksgE1/jUrtz6/lEKmodWWI2goFPGgmgihqLR8ldv0Dv7k9vy
Ao1uunP6kDQEj+omkICFHaT/DBSSYq59DVeMAAcfDq2ssbr4p8hUoXiB tNlJWEubMnHi7YmLSgby+m8b97+8b6qPe8W478gAiggsNjc2gQSKOOXH
EejOSA==
```

1096 BYTES!!

CLOUDFLARE

Some of you may have realized...

- You can “walk” a zone by looking up the next names in NSEC
- You will learn all the names in a zone

Zone Walking

ietf.org NSEC:

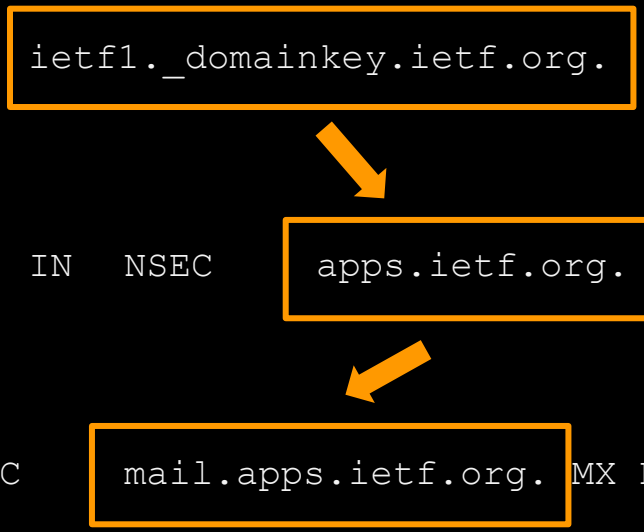
```
ietf.org.        1799 IN  NSEC    ietf1._domainkey.ietf.org. A NS SOA MX
TXT AAAA RRSIG NSEC DNSKEY SPF
```

ietf1._domainkey.ietf.org NSEC:

```
ietf1._domainkey.ietf.org. 1799   IN   NSEC    apps.ietf.org. TXT RRSIG
NSEC
```

apps.ietf.org. NSEC:

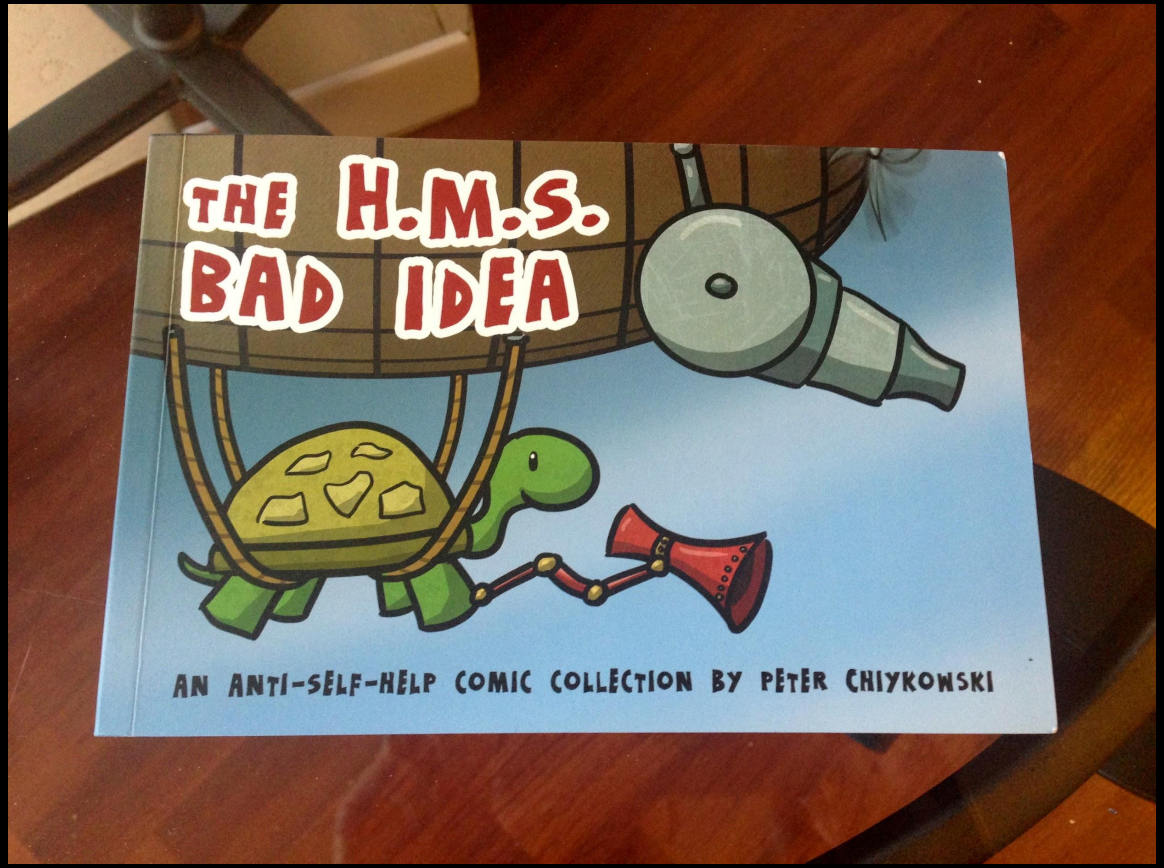
```
apps.ietf.org.       1799 IN  NSEC    mail.apps.ietf.org. MX RRSIG NSEC
```



This was in the *plan.*

“The complete NXT chains specified in this document enable a resolver to obtain, by successive queries chaining through NXTs, all of the names in a zone.”

– RFC2535


THE H.M.S.
BAD IDEA
AN ANTI-SELF-HELP COMIC COLLECTION BY PETER CHIYKOWSKI

CLOUDFLARE

NSEC3 To The Rescue

```
hp9pfrp9ussvle9s5d1oir5n2cfe6qv5.icann.org. 3599 IN NSEC3 1 0 5
2C21FAE313005174 HPF52CF3IK019R1OCDAS1A1FFHLVAB7H A NS SOA MX TXT AAAA
RRSIG DNSKEY NSEC3PARAM
```

hashed

```
6rmo7l6664ki2heho7jtih1lea9k6los.icann.org. 3599 IN NSEC3 1 0 5
2C21FAE313005174 6S2J9F2OI56GPVEIH3KBKJGGCL21SKKL A RRSIG
```

hashed

```
uik932halksloj7g5ejes298hgekcs37.icann.org. 3599 IN NSEC3 1 0 5
2C21FAE313005174 UIMS82AKS3[illegible]K1RVLV3TRUN9RDJ1JM33 A RRSIG
```

hashed

CLOUDFLARE

NSEC3 To The Rescue

```
hp9pfrp9ussvle9s5d1oir5n2cfe6qv5.icann.org. 3599 IN  NSEC3 1 0 5
2C21FAE313005174 HPF52CF3IK019R1OCDAS1A1FFHLVAB7H A NS SOA MX TXT AAAA
RRSIG DNSKEY NSEC3PARAM
```

hashed

```
6rmo7l6664ki2heho7jtih1lea9k6los.icann.org. 3599 IN  NSEC3 1 0 5
2C21FAE313005174 6S2J9F2OI56GPVEIH3KBKJGGCL21SKKL A RRSIG
```

hashed

```
uik932halksloj7g5ejes298hgekcs37.icann.org. 3599 IN  NSEC3 1 0 5
2C21FAE313005174 UIMS82AKS3I3K1RVLV3TRUN9RDJ1JM33 A RRSIG
```

hashed

Close to being *almost* a good plan

1. Still, giant answers
2. Not bulletproof, still can find names on a zone by dictionary attack

Two problems with negative answers

1. Requires authoritative server to return previous and next name
2. 2 NSEC + 2 NSEC RRSIG or 3 NSEC3 + 3 NSEC3 RRSIG to say one thing

The trouble with previous and next name.

The trouble with previous + next name

1. Expensive
2. Leak information

CloudFlare DNS

- In house built DNS server written in Go
- No zone files, instead SQL database of DNS records
- Previous and next name would require sorted search of the DB

RFC4470 White Lies

- Randomly generate previous and next name for NSEC
- Helps prevent zone walking and extra database lookups
- Still, two separately signed NSEC records to say one thing

CLOUDFLARE

```
dig missing.cloudflare.com
```

```
missing.cloudflare.com.    3599    IN    NSEC    \000.missing.cloudflare.
com. RRSIG NSEC
```

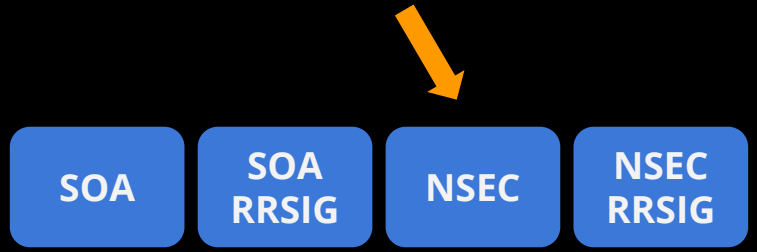
NSEC directly on the missing name.
Means we do not need additional NSEC for wildcard.

```
dig missing.cloudflare.com

missing.cloudflare.com.    3599    IN    NSEC    \000.missing.cloudflare.
com. RRSIG NSEC
```

Return \000.[name]. as the next name.
Saves a DB lookup.

Just one NSEC



```
 cloudflare.com.                 1799    IN      SOA     ns3.cloudflare.com. dns.cloudflare.com. 2020742566 10000 2400 604800 3600
blog.cloudflare.com.    3599    IN      NSEC    \000.blog.cloudflare.com. RRSIG NSEC
cloudflare.com.                 1799    IN      RRSIG   SOA 13 2 86400 20160220230013 20160218210013 35273 cloudflare.com. kgjtJDuuNC/yX8yWQpol4ZUUr8s8yAXZi26KWBI6S3HDtry2t6LnP1ou
QK10Ut7DXO/XhyZddRBVj3pIpWYdBQ==
blog.cloudflare.com.    3599    IN      RRSIG   NSEC 13 3 3600 20160220230013 20160218210013 35273 cloudflare.com. 8BKAAS8EXNJbm8DxEI1OOBba8KaiimIuB47mPlteiZf3sVLGN1edsrXE
+q+pHaSHEfYG5mHfCBJrbi6b3EoXOw==
```

Black Lies: 357 bytes

NODATA

Name exists, type does not.

```
dig ds apps.ietf.org

apps.ietf.org.          1799 IN   NSEC     mail.apps.ietf.org. MX RRSIG NSEC
```

DS does not exist on apps.ietf.org but these types do.

Problems with NODATA

- Inefficient: Search for all the types that do exist, *just* to say the queried type does not exist.

CLOUDFLARE

CloudFlare Lies To You

We set *all* the types, *but not* the type you asked for.

DNS Shotgun

When you ask for TXT:

```
blog.cloudflare.com.  3599 IN  NSEC \000.blog.cloudflare.com. A WKS HINFO MX
~~TXT~~ AAAA LOC SRV CERT SSHFP IPSECKEY RRSIG NSEC TLSA HIP OPENPGPKEY SPF
```

When you ask for MX:

```
blog.cloudflare.com.  3599 IN  NSEC \000.blog.cloudflare.com. A WKS HINFO  ~~MX~~
TXT AAAA LOC SRV CERT SSHFP IPSECKEY RRSIG NSEC TLSA HIP OPENPGPKEY SPF
```

How is this possibly standards compliant?

(You may be wondering)

Black Lies + DNS Shotgun are “compliant”

- RFC4470 (White Lies) allows us to randomly generate next names in NSEC.
- The NSEC for the wildcard does not apply if there’s an NSEC record on the queried name.
- Setting many record types in NSEC for NODATA is okay. Domains are constantly changing, it’s feasible that the domain changed in between two queries.
- Internet Draft for Black Lies: https://tools.ietf.org/html/draft-valsorda-dnsop-black-lies

Questions?

@thedanigrant | dani@cloudflare.com