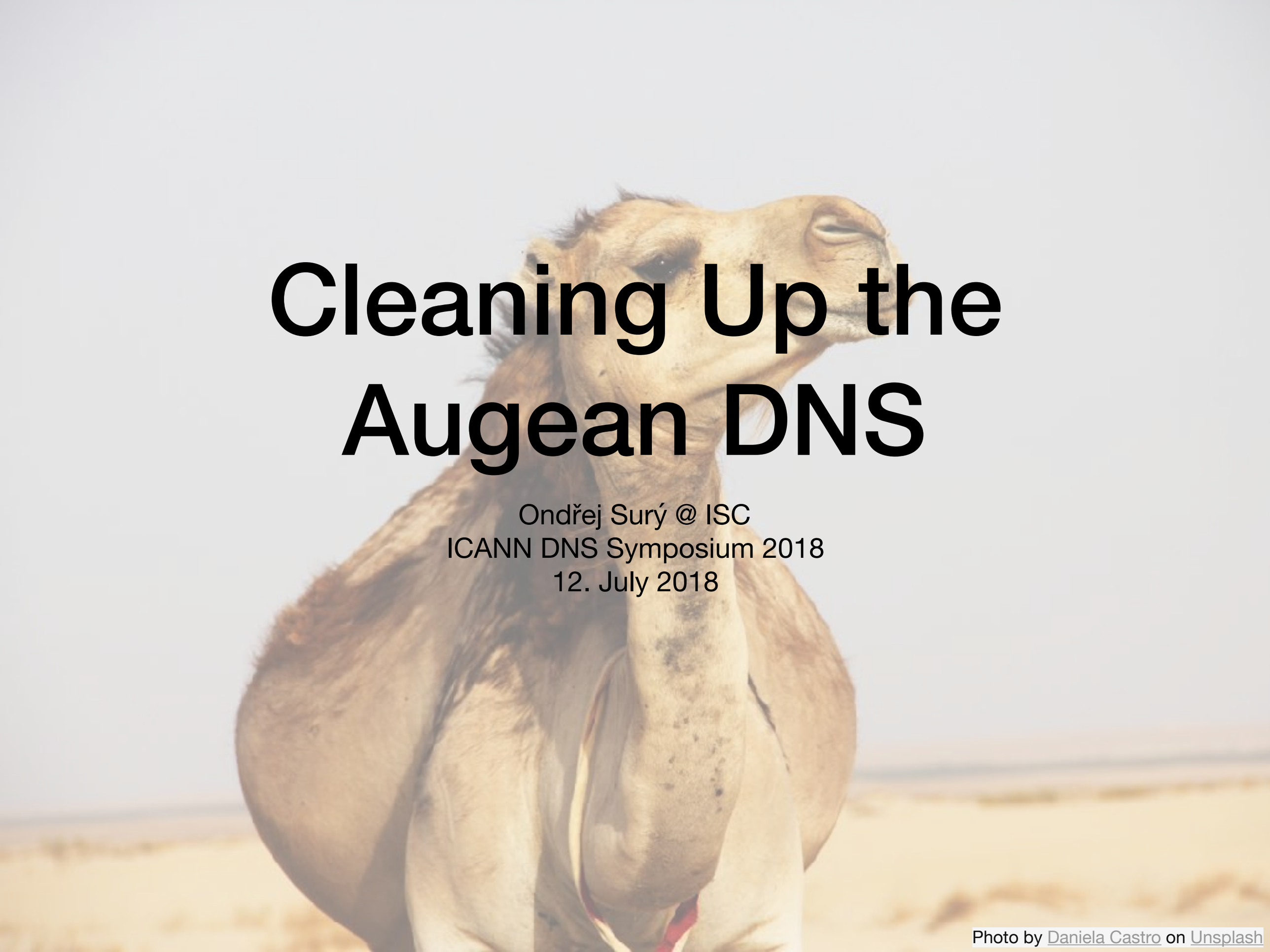
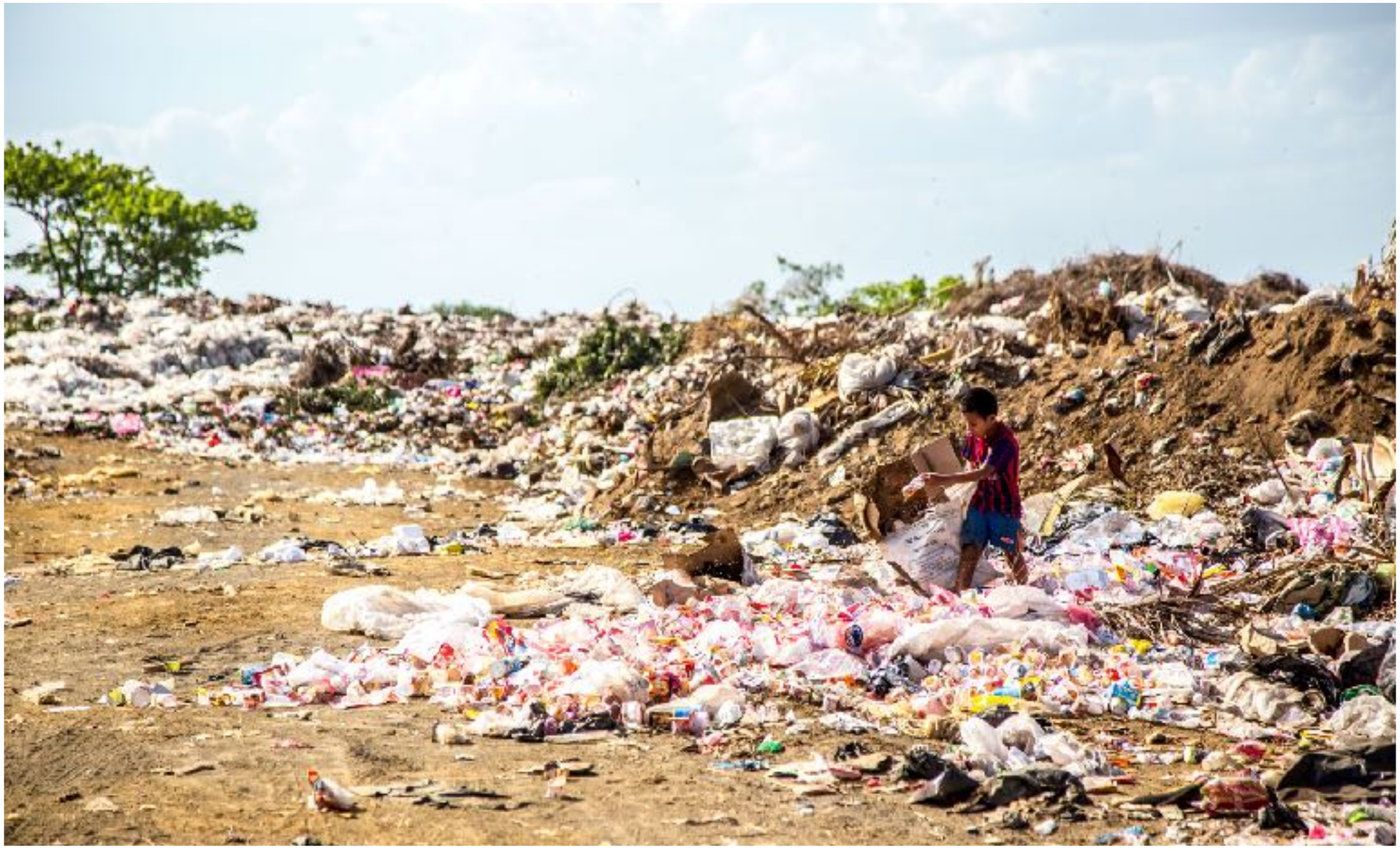
Cleaning Up the Augean DNS

Ondřej Surý @ ISC

ICANN DNS Symposium 2018

12. July 2018





DNS

Everything but a kitchensink

Photo by Hermes Rivera on Unsplash

The Great Ancient DNS Quiz

- Use the back of your schedule to answer your questions
- You can form a group or play on your own
- Put your name on your form
- When done answering, hand the form to your neighbour
- We’ll the go over the answers
- Sometimes more answers are correct
- A point is scored for each correct answer
- No points are scored if there is a wrong answer

1

What is MAILA resource record type?

A. Not an actual RRTYPE

B. Query type which returns MB, MG, MR and MINFO records

C. Query type which returns MF and MD records

D. Word “MAILER” in #gangsta grammar

2

What is WKS resource record type?

A. A Workstation Resource Record

B. A Well-Known Service Description record

C. They serve no known useful function, except internally among LISP machines

D. Caused by alcohol abuse

3

What is MAILB resource record type?

A. Not formally obsoleted

B. Query type which returns MB, MG, MR and MINFO records

C. Query type which returns MF and MD records

D. Inspiration for the “You’ve Got Mail” movie

4

NULL resource record?

A. Has RDATA that’s 65535 octets or less

B. Has RDATA that’s NULL (0 octets)

C. Not allowed in master files

D. Declared EXPERIMENTAL in RFC1035

5

GSS-TSIG?

A. Uses SIG(0) to establish secret keys

B. Used to establish security context

C. Uses TKEY to establish secret keys

D. The server MUST not generate a signed response to an unsigned request under any circumstances.

6

What is TKEY resource record?

A. Uses Elliptic-curve Diffie-Hellman for key-exchange

B. Uses Diffie-Hellman key-exchange

C. Misspelled T-KEY, a rapper and hip-hop artist

D. Secret Key Establishment for DNS

7

What does “Transactional Security” in IANA DNSSEC table means?

A. Algorithm can be used for DNS over TLS

B. Has a meaning only in DNSKEY records

C. Algorithm can be used for SIG(0)

D. Has a meaning only in KEY records

8

What is the reasonable default EDNS(0) size?

A. 4096

B. Slightly less than 1280 (IPv6 minimum fragment size)

C. Around 1500 (ethernet frame size)

D. Only Geoff Huston knows

9

What is RP resource record?

A. Reverse Proxy record

B. Responsible Person record

C. RP records are used in IPoAC

D. None of the above

10

Why 512 octets was chosen as maximum DNS msg size?

A. To mess with future generations

B. To be less than minimum IPv4 fragment

C. To be less than minimum IPv4 packet size

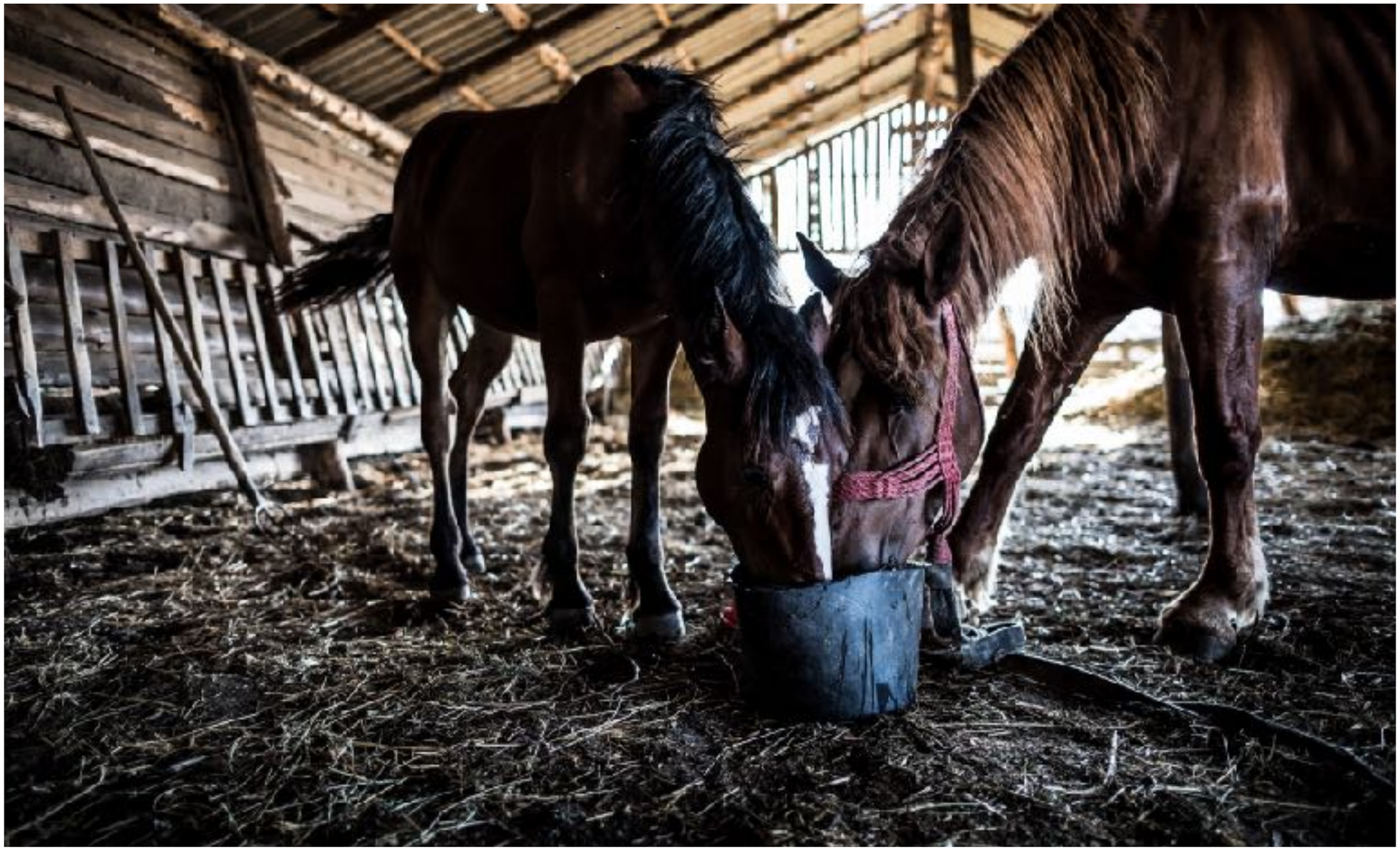
D. 512 octets should be enough for everyone

Answers

Photo by Edwin Andrade on Unsplash

Correct Answers

1. A,C
2. B,C
3. A,B
4. A,C,D
5. B,C
6. B,D
7. C,D
8. D, and maybe B
9. B
10. C



Cleaning the DNS Stables

Photo by Alex Blăjan on Unsplash

DNS Protocol Development

- We constantly add new things

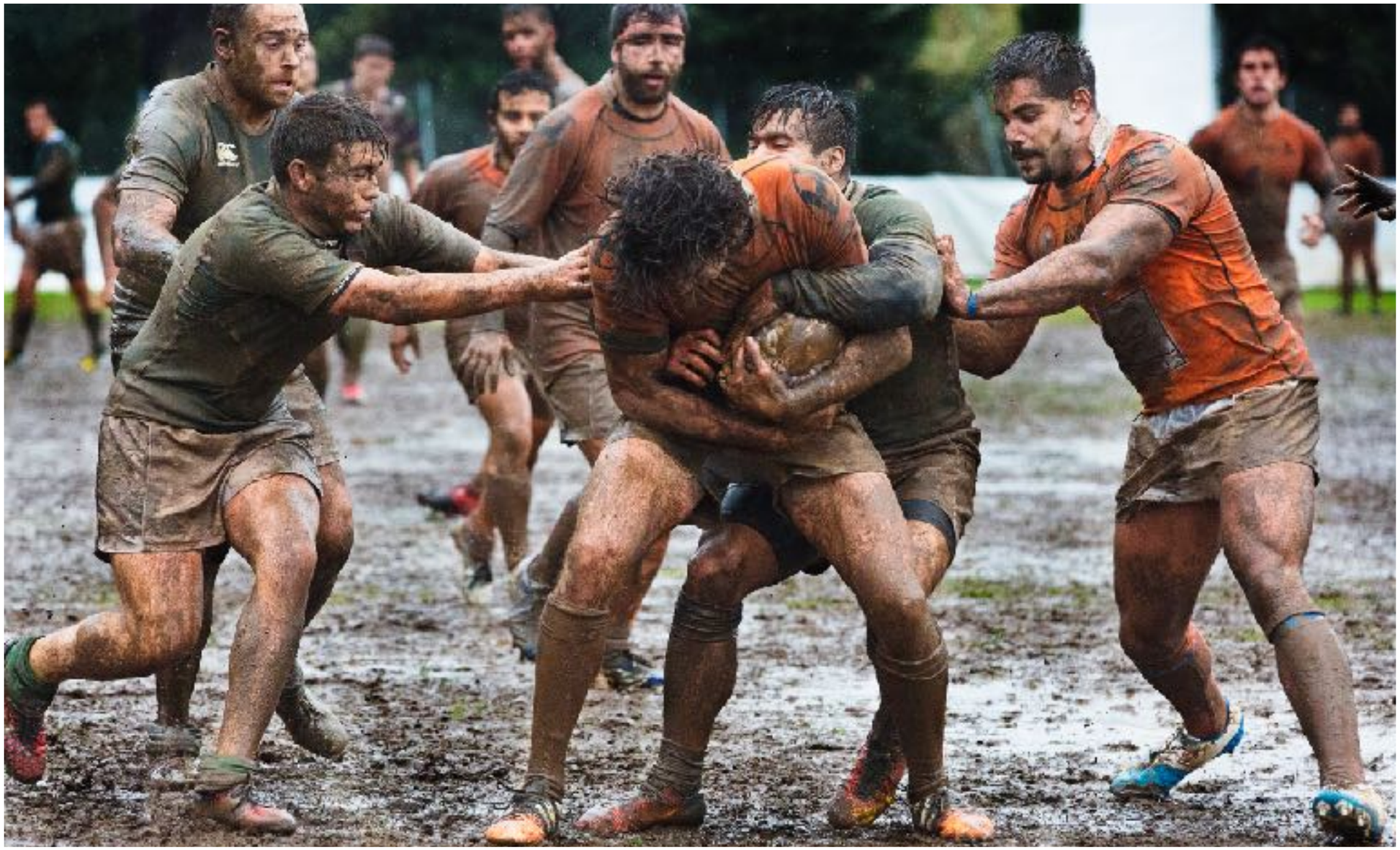
- We (almost) never remove things

Refactoring DNS Protocol

- Why old stuff never gets removed?
  - It’s not **fun** (refactoring never is)
  - There are no **counters** for features
  - People **might** be using this or that
  - It’s not a **problem**

Next steps?

- Actually rewrite the foundation RFCs
  - RFC 1034, 1035, 1183, 2181, …
  - Bit by bit
- Start deprecating the features / records that nobody use
- Improve existing (but perhaps less used) features
  - Add ECDH to GSS-TSIG and remove DH
  - Define transactional security for ECC algorithms
  - Find new innovative ways to use SIG(0) or deprecate it



Discussion

Photo by Quino Al on Unsplash