TLDCON-2020

Развитие DNS как универсального инструмента публикации данных

Александр **Венедюхин**
ТЦИ

Самая привычная – A-запись:

TCINET.RU. IN A 62.76.251.7

ТЦИ

Самая привычная – A-запись:

TCINET.RU. IN A 62.76.251.7

[A]+[TCINET.RU.] ↔ 62.76.251.7

DNS позволяет хранить (и находить) пары “ключ—значение”

В общемировой распределённой БД можно размещать произвольную информацию

Удобно для многих протоколов

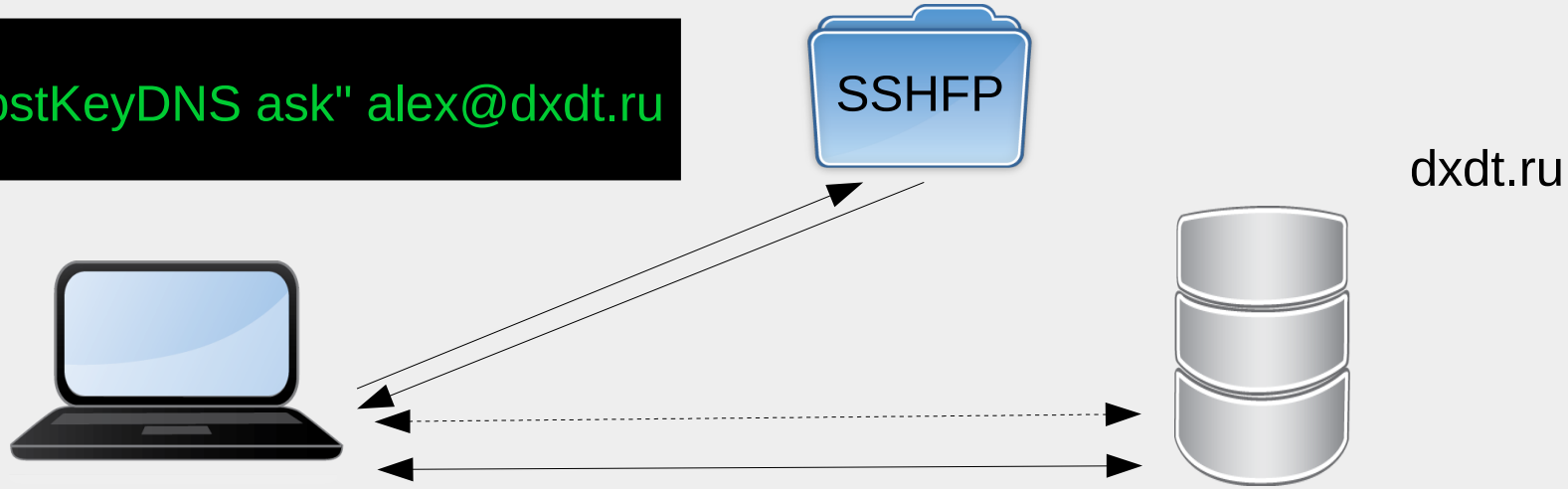
ТЦИ

Примеры (из старого):

SSHFP – отпечаток SSH-ключа хоста

(RFC 4255, 6594, 7479)

```
$ ssh -o "VerifyHostKeyDNS ask" alex@dxdt.ru
```



ТЦИ

Примеры (посвежее):

CAA – политика выпуска TLS-сертификатов

TLSA – отпечатки TLS-сертификатов/криптографических ключей

OPENPGPKEY – тоже ключи и отпечатки, email

Примеры (посвежее):

CAA

политика:
какой УЦ, для чего и почему может выпустить TLS-сертификат

ТЦИ

draft-ietf-tls-esni-07

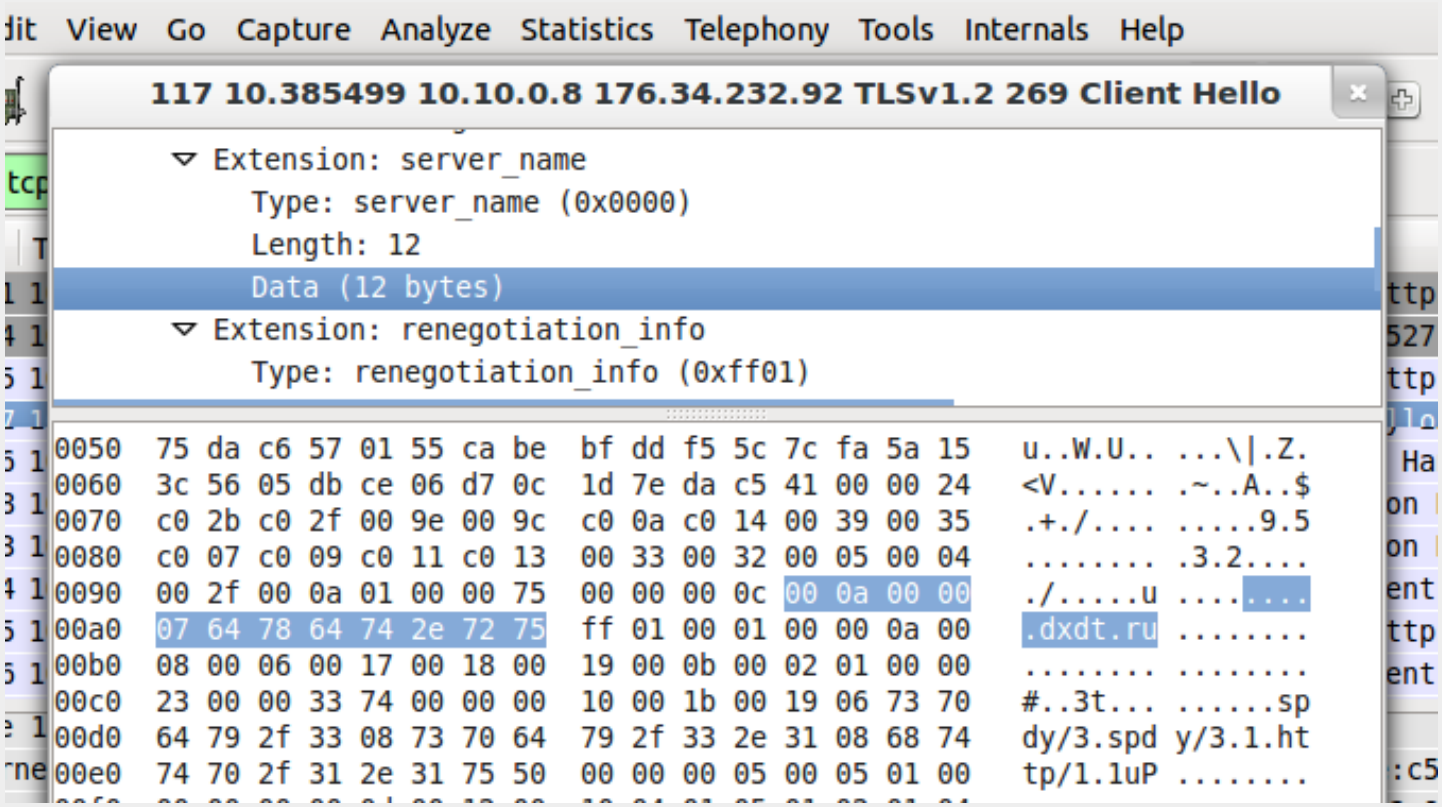
ESNI/ECH TLS Encrypted Client Hello

Проблема

TLS

Утечка: имя хоста в открытом виде

Имя хоста == доменное имя



ТЦИ

ESNI/ECH

Способы решения

TLS

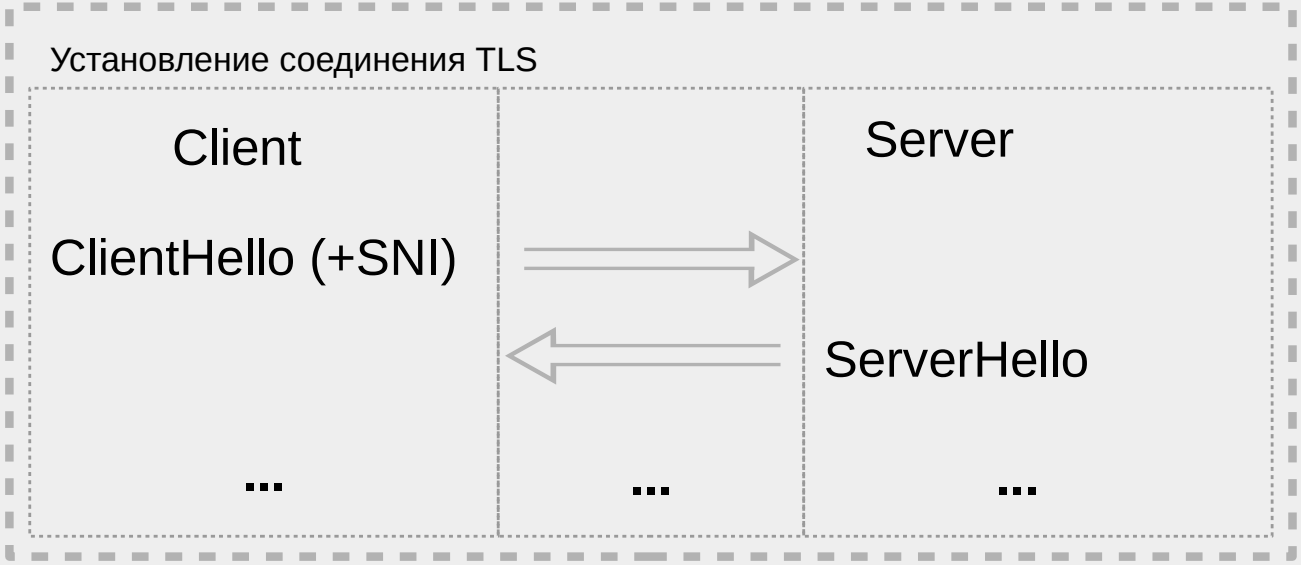
Server Name Indication (SNI) – строка с именем; можно зашифровать

ТЦИ

ESNI/ECH

TLS

Server Name Indication (SNI) – строка с именем; можно зашифровать

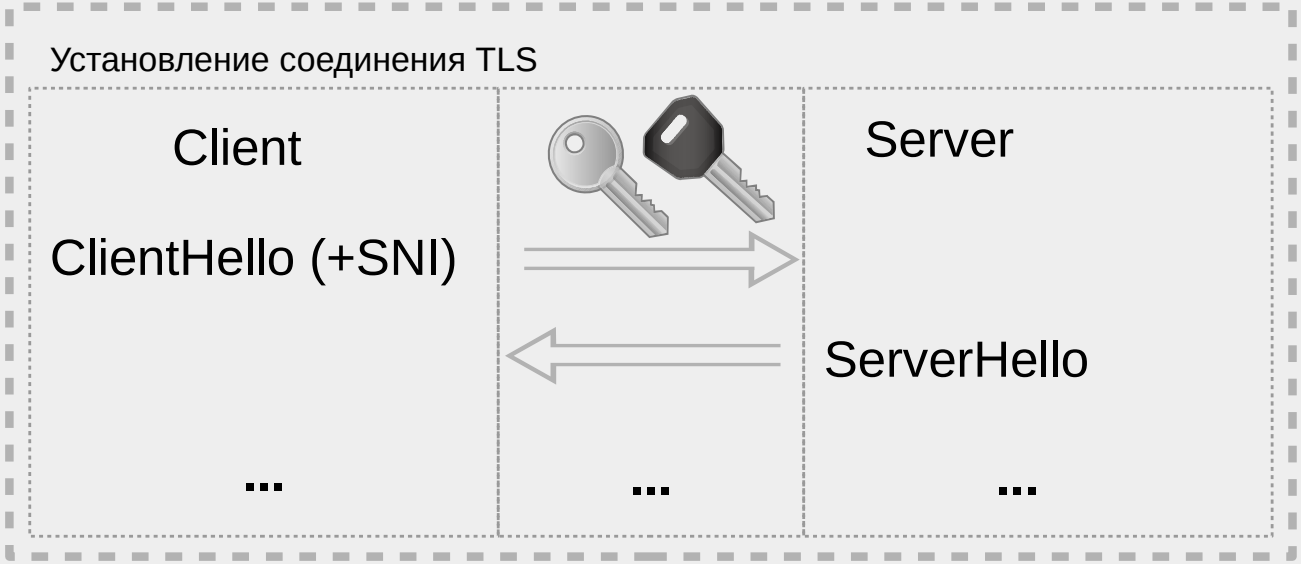


ТЦИ

ESNI/ECH

TLS

Server Name Indication (SNI) – строка с именем; можно зашифровать



ТЦИ

ESNI/ECH

TLS

Server Name Indication (SNI) – строка с именем; можно зашифровать

DNS

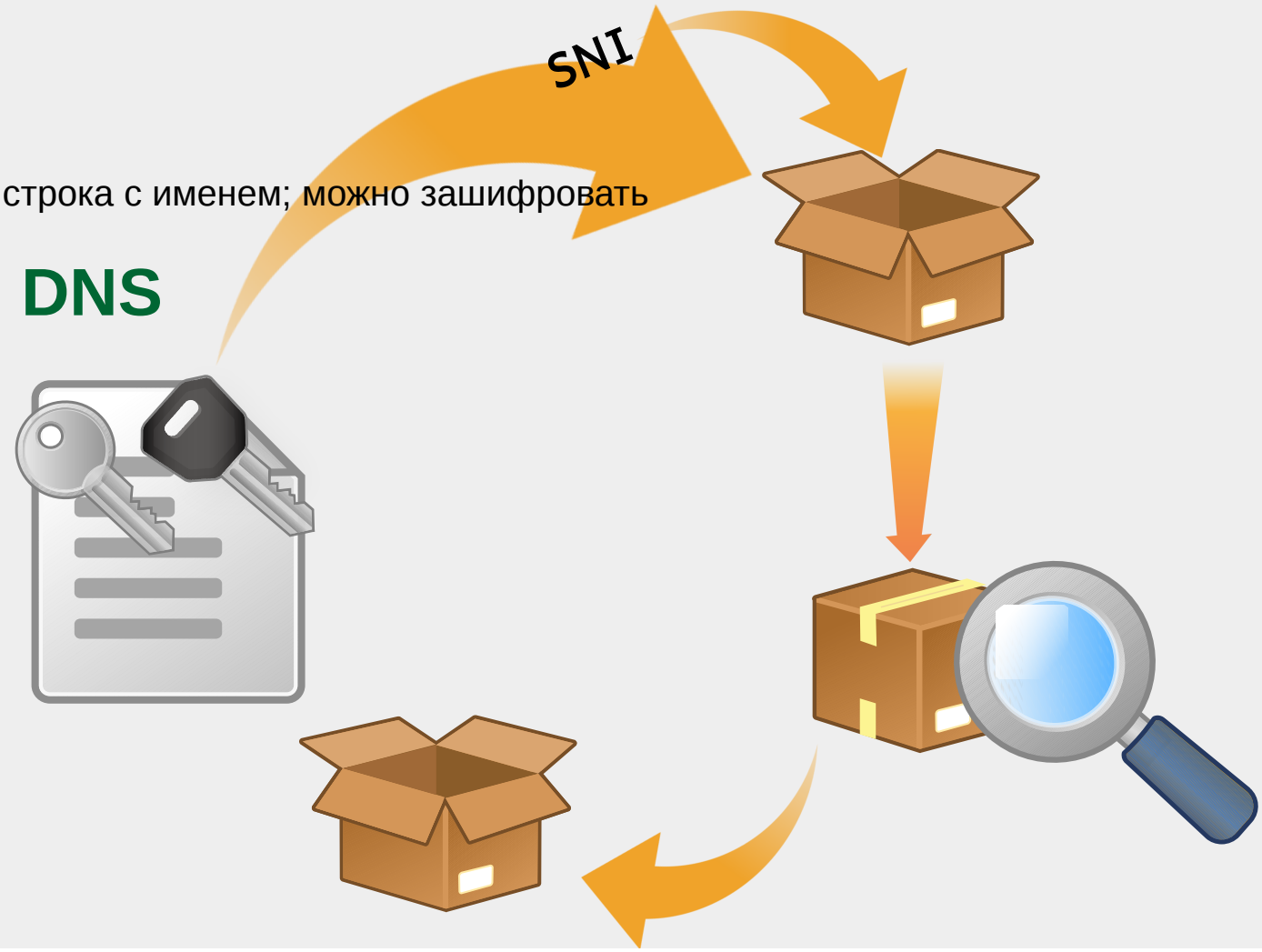
ТЦИ

ESNI/ECH

TLS

Server Name Indication (SNI) – строка с именем; можно зашифровать

DNS



ТЦИ

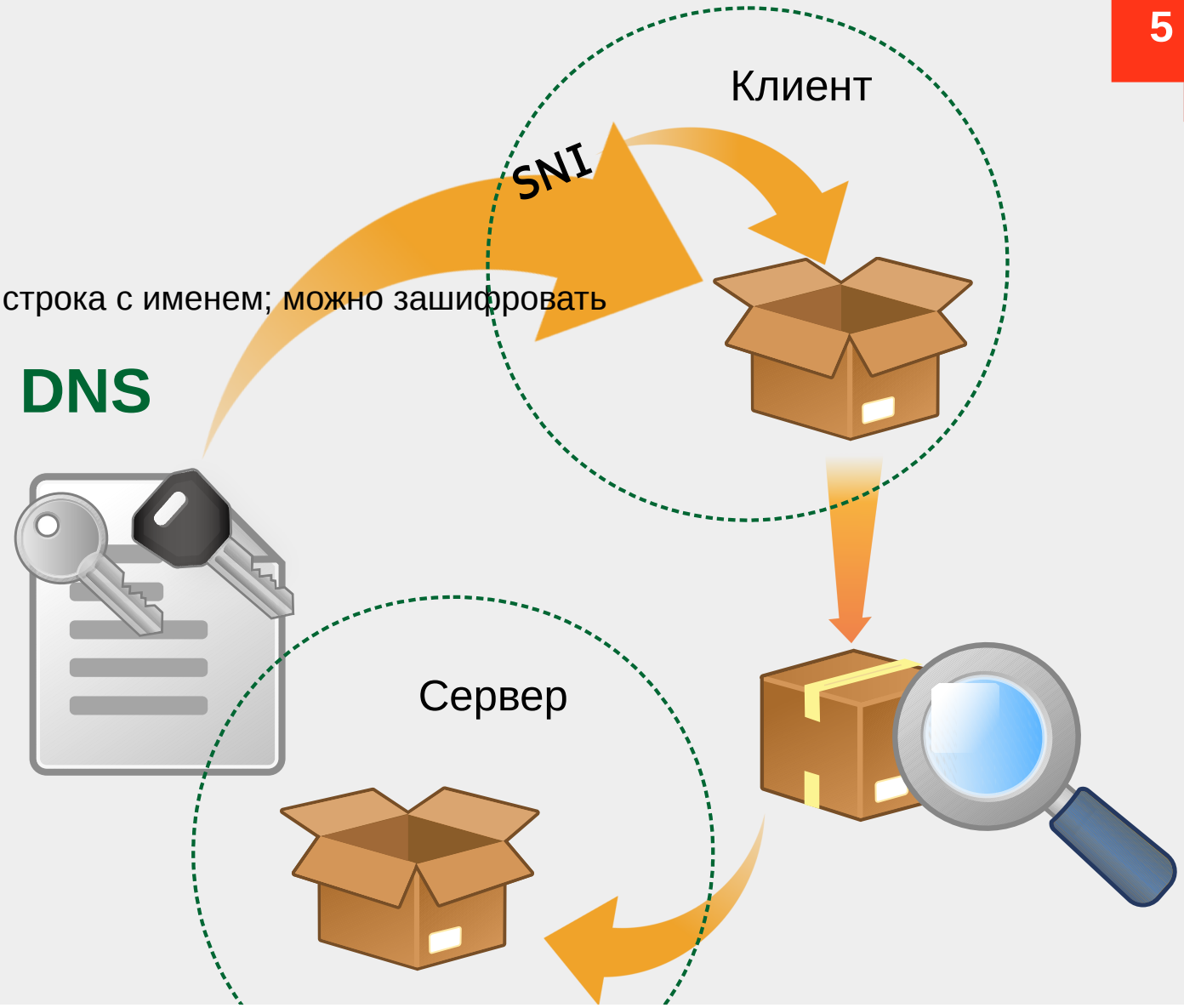
ESNI/ECH

TLS

Server Name Indication (SNI) – строка с именем; можно зашифровать

Diffie-Hellman KE

DNS



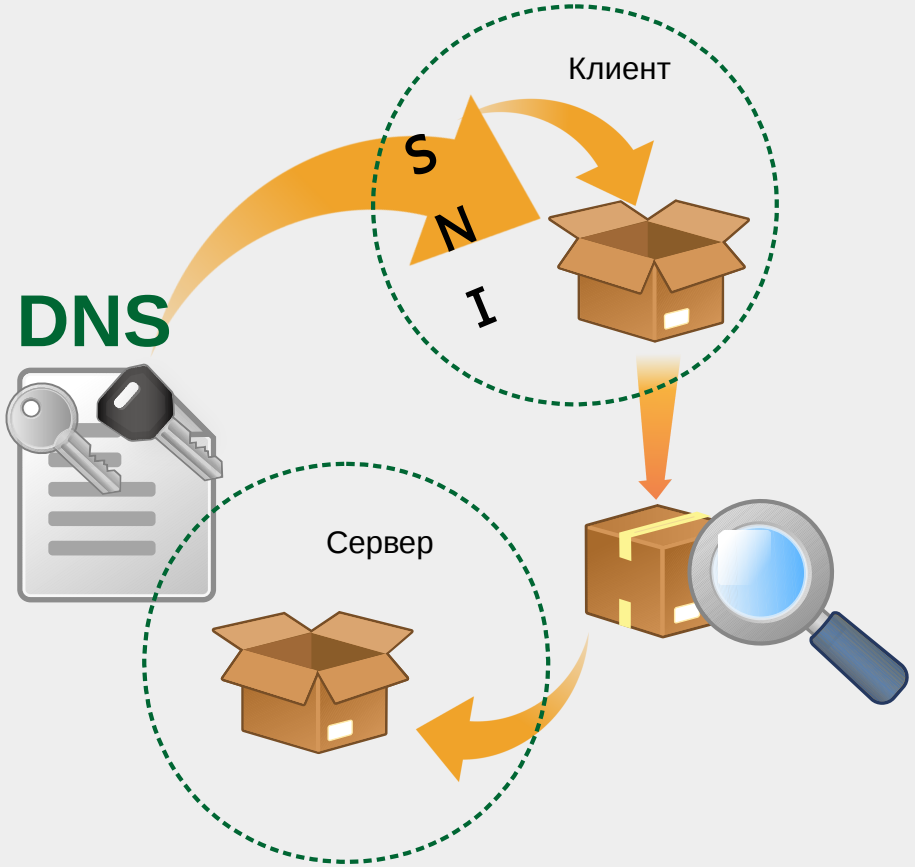
ТЦИ

ESNI/ECH

ESNI (draft) - данные в TXT-записи, строка Base64:

_esni.name.tld

IN TXT
"/wGFoqIpAIkAHQAgLukkHH6AiIAPYODmYK/6Nz3H7N58nYZyb/WG62h4TTgAGABhBLcBj0CfRsxcPdVclZGGzWPYJgryAYMY/4GILwCOTXACC6vven68udWahNDa1r6/2hRDaFATiREEqwgv1TLxwG1DRlTLaEybIljuYzacpw3mrRdUMg/NfRQHRLVaAJdqOgACEwEAgAAAABckYKDAAAAAF/0/YEAAA=="



ТЦИ

ESNI/ECH

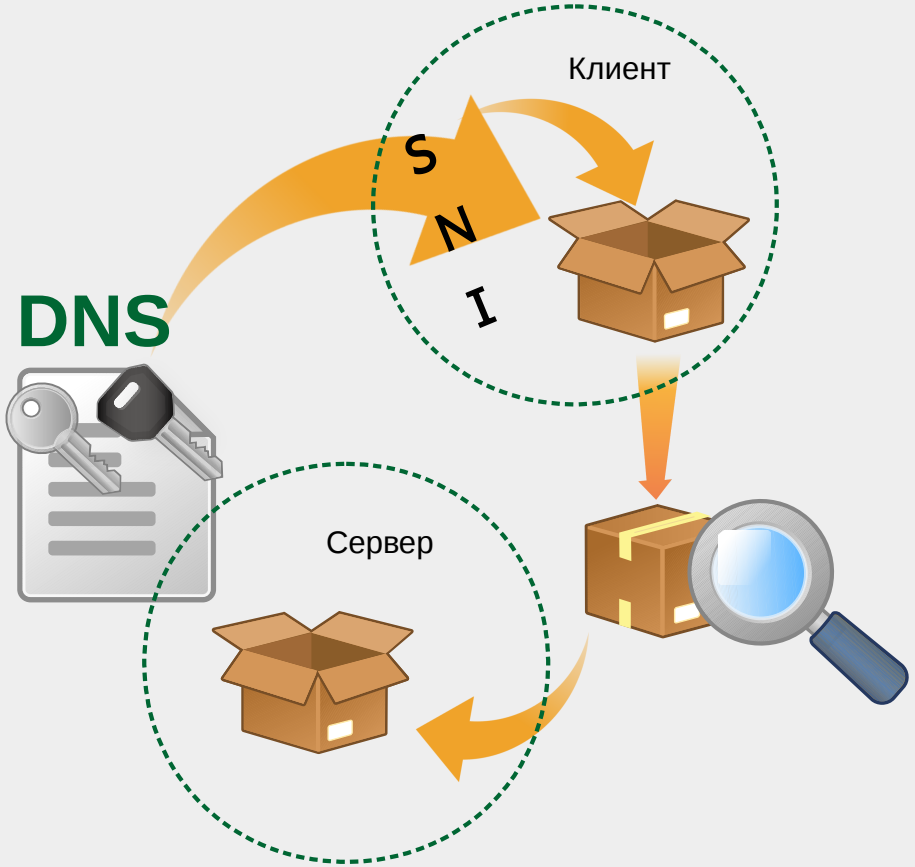
В новой версии (ECH) – зашифровывается полностью сообщение ClientHello

TLS + DNS:

Защита от утечки имени хоста в TLS

Необходимые ключи – в новой DNS-записи

Для защиты DNS - DNS-over-TLS



ТЦИ

https://statdom.ru/tld/ru/report/esnitotal/#64

Статистика ESNI в российских TLD

Домены России

ТЦИ

Русский
English

О проекте | .RU | .РФ | .SU | Сравнение отчётов

Сводный отчёт

Домены

- Общее число доменов
- Динамика изменения числа доменов
- Динамика продлений доменов
- Распределение доменов между физическими и юридическими лицами
- География распределения доменов
- Длина доменных имён
- Распределение доменов по возрасту
- Динамика продлений доменов по возрасту
- Домены, подписанные DNSSEC
- Цели использования доменов

Регистраторы

Администраторы

Серверы

Статистика по TLS

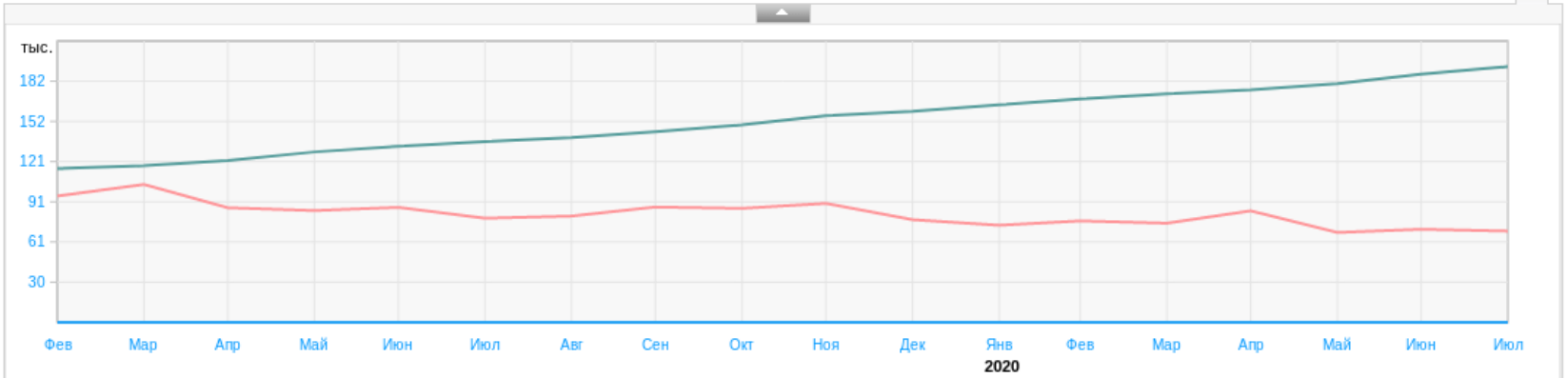
Статистика по MX

Технометрики веба

Основные показатели

Отчёт | Экспорт

фев 2019 — июл 2020



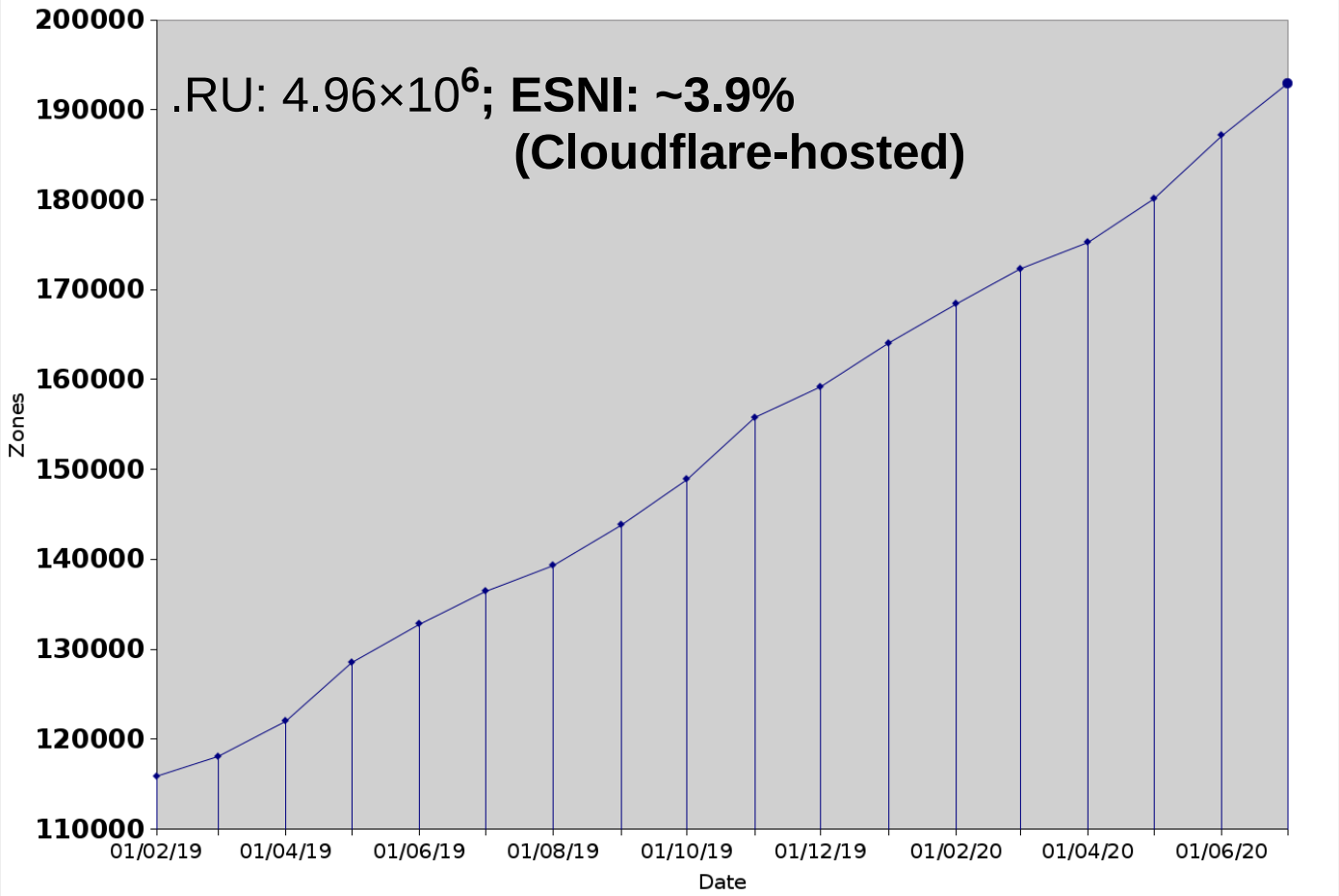
На графике: Зоны с корректной записью ESNI, число; Зоны с некорректной TXT-записью для ESNI-имени, число; Уникальные ключи протокола DH в корректных ESNI-записях, число

Выровнять столбцы

Дата	Зоны с коррек число	Зоны с некорр число	Уникальные к число
Июль 2020	192 926	68 827	5
Июнь 2020	187 115	70 201	5
Май 2020	180 101	67 780	5
Апрель 2020	175 256	84 081	5
Март 2020	172 313	74 781	5
Февраль 2020	168 431	76 514	5
Январь 2020	164 066	73 233	3

ESNI draft 2, TXT-record

ESNI in .RU (draft-2, TXT)



Июль 2020:

192926 зон .RU

DH: X25519 (100%)

AES-128-GCM **192925**

AES-256-GCM **1**

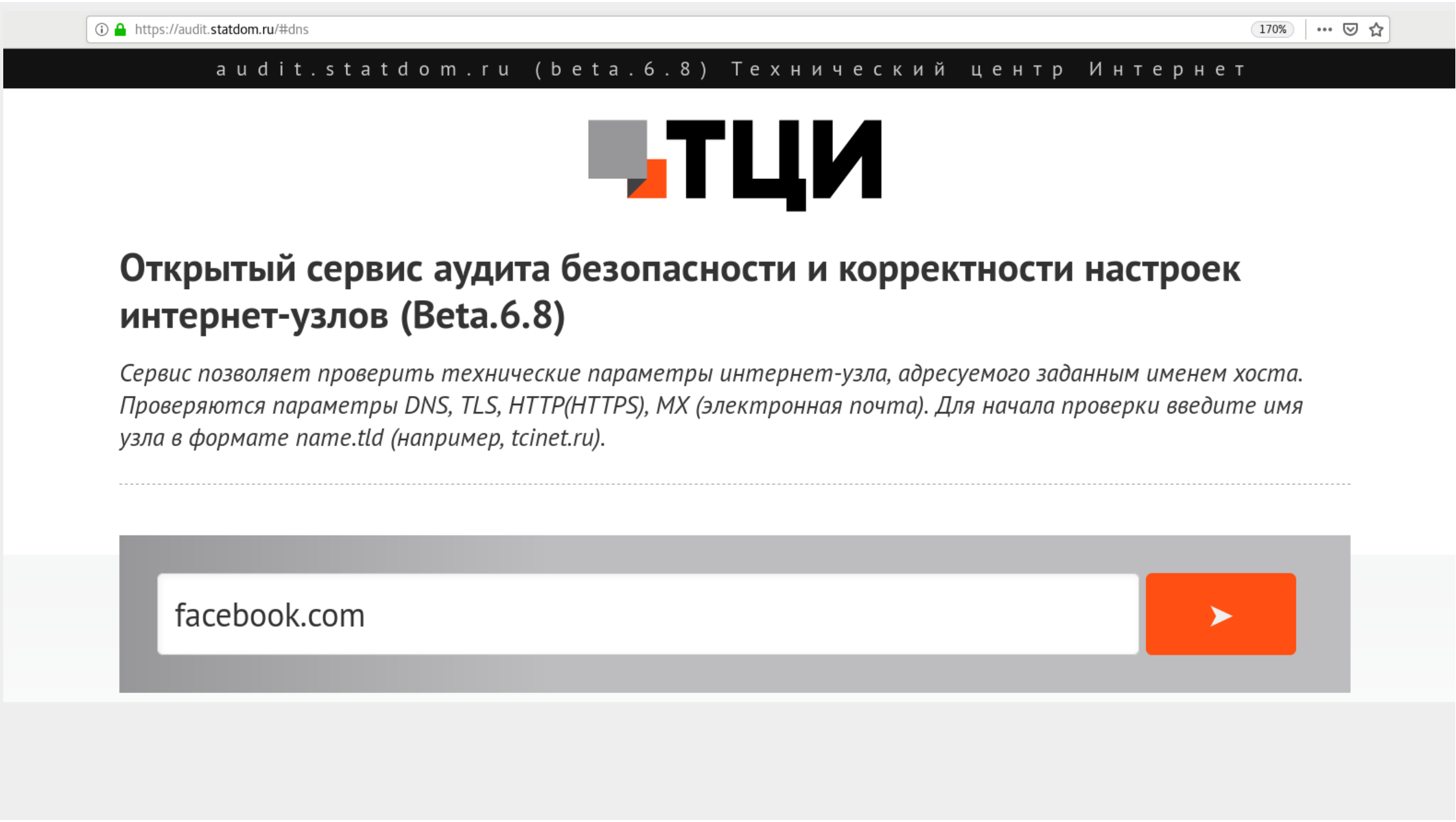
TLS (.RU): ~19%

ТЦИ

Зоны с ESNI – это зоны, размещённые на Cloudflare.

TLS для DNS “в обратную сторону” - DNS-over-TLS или DoT

ТЦИ


https://audit.statdom.ru/#dns
170%
audit.statdom.ru (beta.6.8) Технический центр Интернет
ТЦИ
Открытый сервис аудита безопасности и корректности настроек интернет-узлов (Beta.6.8)
Сервис позволяет проверить технические параметры интернет-узла, адресуемого заданным именем хоста. Проверяются параметры DNS, TLS, HTTP(HTTPS), MX (электронная почта). Для начала проверки введите имя узла в формате name.tld (например, tcinet.ru).
facebook.com

https://audit.statdom.ru/#dns 170%

Настройки DNS:

[+]

Результаты для зоны facebook.com.

Обнаружены DNS-серверы:

- c.ns.facebook.com. 185.89.218.12 SOA CAA UDP TCP **DoT**
- a.ns.facebook.com. 129.134.30.12 SOA CAA UDP TCP **DoT**
- d.ns.facebook.com. 185.89.219.12 SOA CAA UDP TCP **DoT**
- b.ns.facebook.com. 129.134.31.12 SOA CAA UDP TCP **DoT**
- c.ns.facebook.com. 2a03:2880:f1fc:c:face:b00c:0:35 SOA CAA UDP TCP **DoT**
- a.ns.facebook.com. 2a03:2880:f0fc:c:face:b00c:0:35 SOA CAA UDP TCP **DoT**
- d.ns.facebook.com. 2a03:2880:f1fd:c:face:b00c:0:35 SOA CAA UDP TCP **DoT**
- b.ns.facebook.com. 2a03:2880:f0fd:c:face:b00c:0:35 SOA CAA UDP TCP **DoT**

ТЦИ

TLDCON-2020

Развитие DNS как универсального инструмента публикации данных

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

Александр **Венедюхин**

ТЦИ

https://tcinet.ru/

This page intentionally left blank