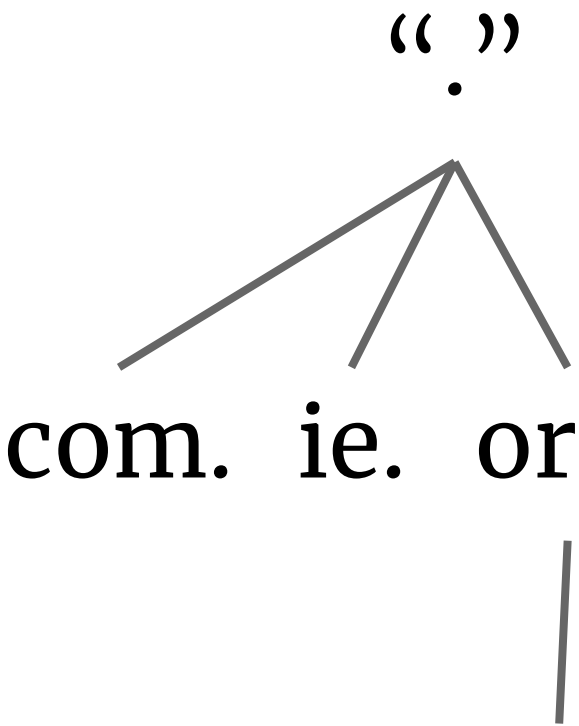
You Depend on DNS, This Is How It Works and You Won't Believe It

SREcon EMEA 2023

Philip Rowlands
Jane Street

$ ping intranet



intranet.dnsdemo.org.?
“Ask org. NS”

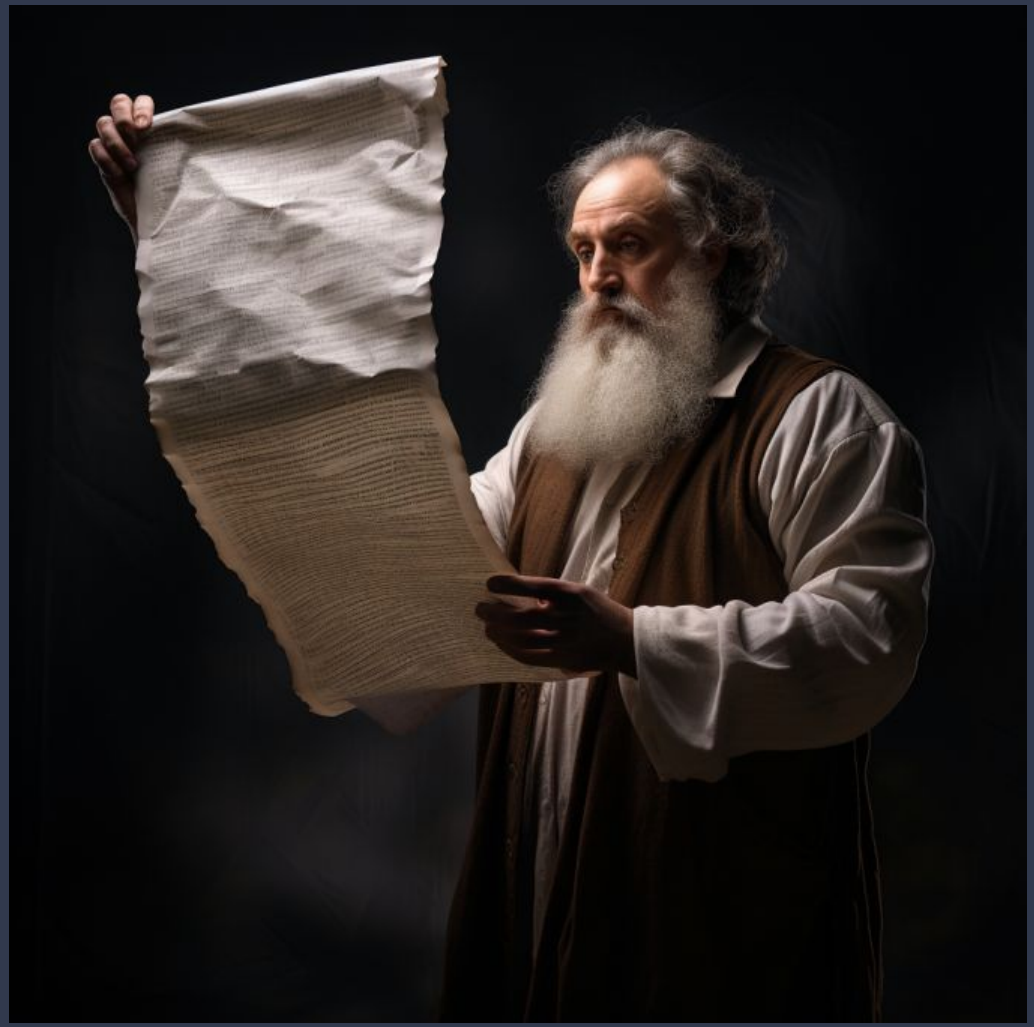
intranet.dnsdemo.org.?
“Ask dnsdemo.org. NS”

intranet.dnsdemo.org.?
“1.2.3.4”

Name this DNS pioneer?


I
dig
DNS
Microsoft

Why DNS?



```
BEGIN:
; DoD Internet Host Table
;  24-Nov-83
;
; Changes, corrections, comments or questions to (HOSTMASTER@SRI-NIC)
;
; The format of this file is documented in RFC 810, "DoD Internet
; Host Table Specification", which is available on-line at SRI-NIC
; as the file
;              [SRI-NIC]<NETINFO>RFC810.TXT
; …
HOST : 14.0.0.6 : UK-SATNET ::::
HOST : 14.0.0.7 : WISC-IBM : IBM-4341 : VM/CMS : TCP/TELNET,TCP/FTP :
HOST : 14.0.0.8 : RAND-TN : VAX-11/750 : UNIX : TCP/FTP,TCP/SMTP :
HOST : 18.2.0.7, 18.10.0.5 : MIT-BRIDGE,MIT-BR : PDP-11 : MOS : IP :
HOST : 18.10.0.6, 18.26.0.134 : MIT-SLUDGE,MIT-SL : PDP-11 : MOS : IP :
HOST : 18.26.0.8 : MIT-MELKOR,MELKOR,MEL : IBMPC : MSDOS : IP :
```

HOSTS.TXT

```
; DoD Internet Host Table
;  24-Nov-83
HOST : 18.10.0.64 : MIT-AJAX,AJAX :
HOST : 18.10.0.65 : MIT-BORAX,BORAX :
HOST : 18.10.0.66 : MIT-COMET :
HOST : 18.10.0.67 : MIT-DUTCH,DUTCH :
HOST : 18.10.0.68 : MIT-MRCLEAN,MRCLEAN :
HOST : 18.10.0.69 : MIT-BOLD,BOLD :
```

HOSTS.TXT / the naming of hosts

```
; DoD Internet Host Table
;  24-Nov-83
HOST : 18.10.0.78 : MIT-HEINEKEN,HEINEKEN :
HOST : 18.10.0.79 : MIT-OA,OA :
HOST : 18.10.0.80 : MIT-MACEWAN,MACEWAN :
HOST : 18.10.0.81 : MIT-KIRIN,KIRIN :
HOST : 18.10.0.82 : MIT-MOLSON,MOLSON :
HOST : 18.10.0.86 : MIT-MILO,MILO :
HOST : 18.10.0.87 : MIT-OPUS,OPUS :
```

HOSTS.TXT / the naming of hosts

```
com.      172800   NS   a.gtld-servers.net.
net.      172800   NS   a.gtld-servers.net.
org.      172800   NS   a0.org.afilias-nst.info.

ie.       172800   NS   a.ns.ie.
uk.       172800   NS   nsa.nic.uk.
```

https://www.internic.net/domain/root.zone

wHY tHe sArcAsTIc QUeRIes?

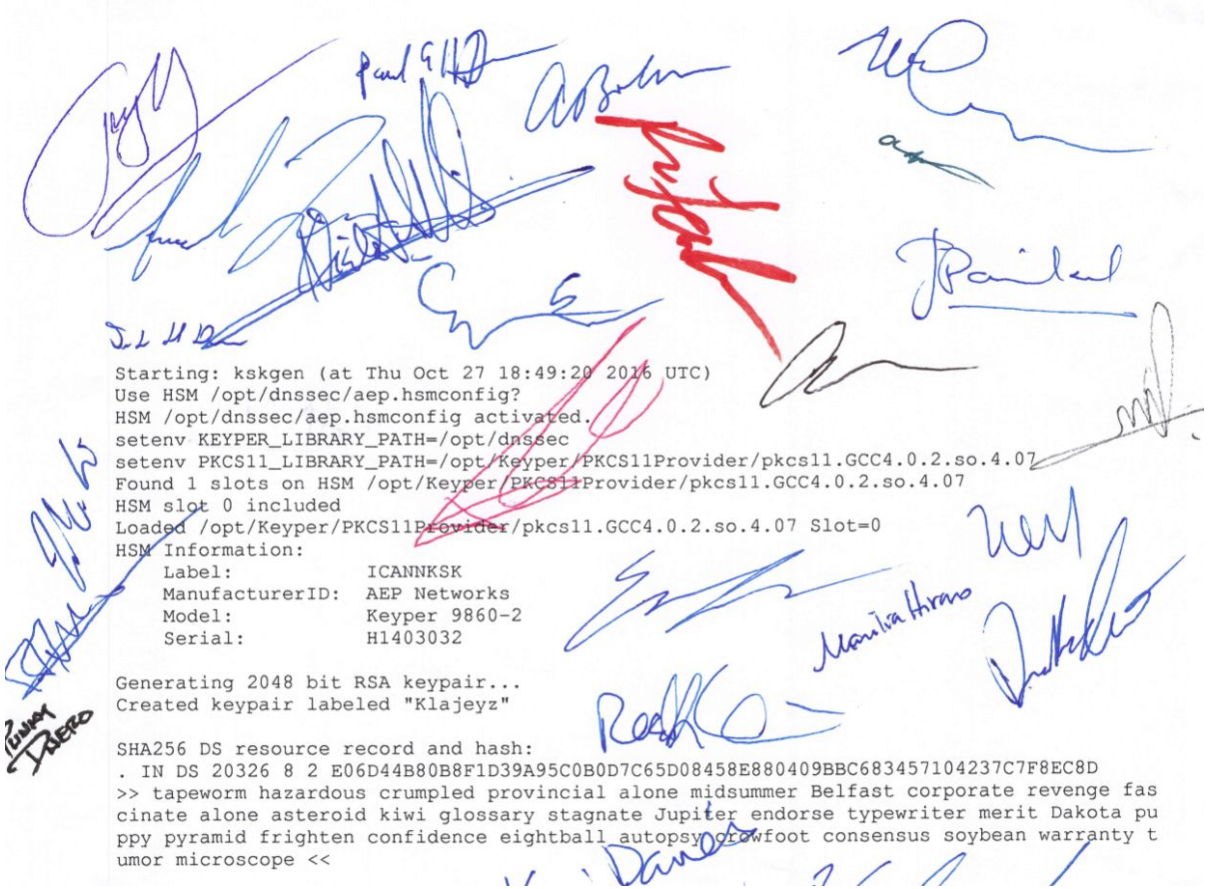
E	0x45	0x65	e
X	0x58	0x78	x
A	0x41	0x61	a
M	0x4D	0x6D	m
P	0x50	0x70	p
L	0x4C	0x6C	l
E	0x45	0x65	e
.	0x2E	0x2E	.
C	0x43	0x63	c
O	0x4F	0x6F	o
M	0x4D	0x6D	m

Equivalent DNS QNAMEs / ASCII

Why DNSSEC?

```
;; ANSWER SECTION:
blog.cloudflare.com.    300  A     104.18.28.7
blog.cloudflare.com.    300  A     104.18.29.7
blog.cloudflare.com.    300  RRSIG A          \
  13 3 300 20231011165047 20231009145047    \
  34505 blog.cloudflare.com. obPf…RUegA==
```

DNSSEC records



```
Starting: kskgen (at Thu Oct 27 18:49:20 2016 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:            ICANNKSK
    ManufacturerID:   AEP Networks
    Model:            Keyper 9860-2
    Serial:           H1403032

Generating 2048 bit RSA keypair...
Created keypair labeled "Klajeyz"

SHA256 DS resource record and hash:
. IN DS 20326 8 2 E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D
>> tapeworm hazardous crumpled provincial alone midsummer Belfast corporate revenge fas
cinate alone asteroid kiwi glossary stagnate Jupiter endorse typewriter merit Dakota pu
ppy pyramid frighten confidence eightball autopsy crowfoot consensus soybean warranty t
umor microscope <<
```

Root of all DNSSEC trust

https://www.iana.org/help/key-ceremony-attendance

Why NSEC3?

```
;; QUESTION SECTION:
;shopping.blackmonday.          A

;; AUTHORITY SECTION:
blackfriday.  86400 NSEC blockbuster. NS DS RRSIG NSEC
blackfriday.  86400 RRSIG NSEC \
  8 1 86400 20231016170000 20231003160000 \
  46780 . PpOclR7iRH…7Kqewg==

blockbuster.  86400 NSEC blog. NS DS RRSIG NSEC
blog.         86400 NSEC bloomberg. NS DS RRSIG NSEC
bloomberg.    86400 NSEC blue. NS DS RRSIG NSEC
```

NSEC signed gaps

```
;; QUESTION SECTION:
;srecon.org.                          A

;; AUTHORITY SECTION:
408au2vsicgr6gmr02fsi814qagsmddg.org. \
   3600 NSEC3 1 1 0 332539EE7F95C32A  \
   408FSNSEEIUA50H51M33JL9T42993EGD    \
   NS DS RRSIG

408au2vsicgr6gmr02fsi814qagsmddg.org. \
   3600 RRSIG NSEC3 8 2 3600          \
   20231022152320 20231001142320      \
   61110 org. D6S4sUEZ…nJXClXzRJWwS 4Lk=
```

NSEC3 signed gaps

Why so many TLDs?

dnsdemo.auto	€3873
dnsdemo.autos	€2
dnsdemo.fun	€2
dnsdemo.irish	€10
dnsdemo.management	€14
dnsdemo.pizza	€19
dnsdemo.protection	€3873

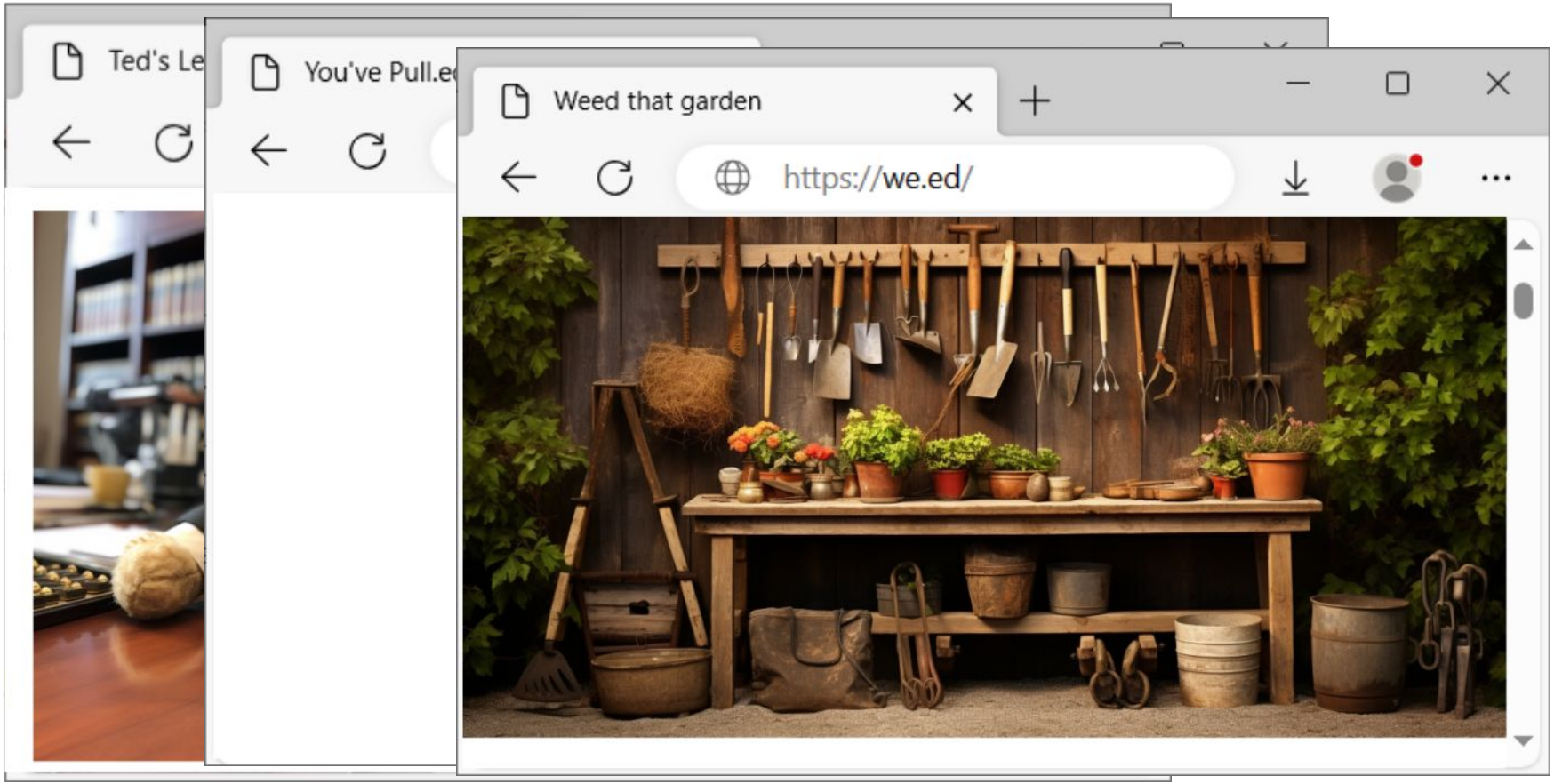
Domain registration costs

.ARPA

.GOV .EDU .COM .MIL .ORG .NET

.US .UK .IL .AU .DE .FI .FR etc.

How to make a TLD (originals)



Future .ed websites?

1988 .int
2000 .aero / .biz / .coop / .info / .museum / .name / .pro
2004 .asia / .cat / .jobs / .mobi / .tel / .travel
2011 .xxx
2012 .post

How to make a TLD (1984 - 2012)

Generic interests

.camera / .pizza / .fish / .xyz

Location themed

.london / .koeln / .africa

Brands

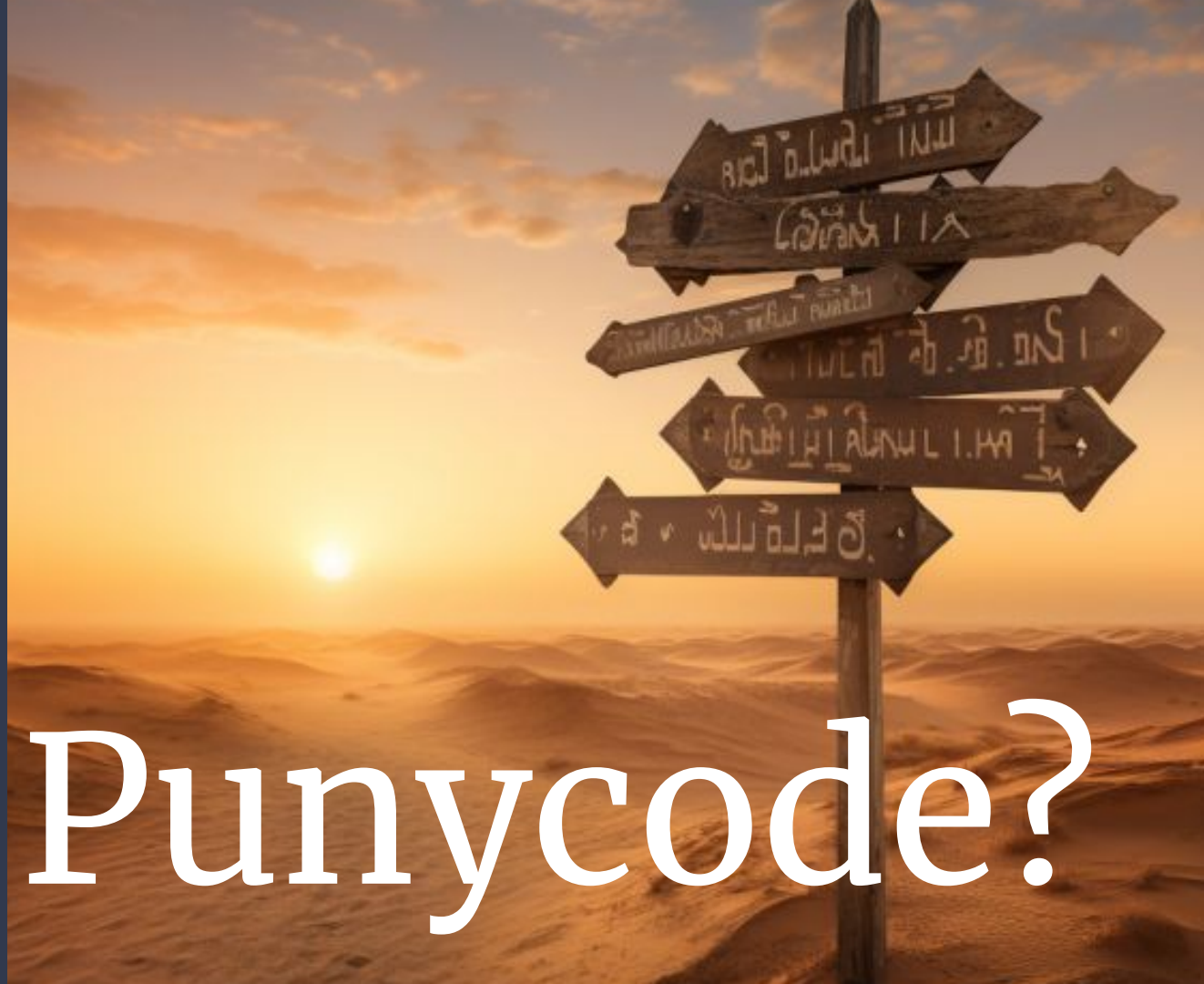
.abc / .apple / .bbc / .citadel / .google

How to make a TLD (2012 –)

.ru	Russia	.рф
.cn	China	.中国
.gr	Greece	.ελ
.il	Israel	.ישראל
.eg	Egypt	.مصر
.kr	South Korea	.한국

How to make a TLD (non-ASCII)

Why Punycode?



BaileÁthaCliath.ie ->
xn--bailethacliath-zgb.ie

телеграмм.онлайн ->
xn--80affa3aja3an.xn--80asehdb

Unicode to Punycode

```
BaileÁthaCliath
                    -> nameprep()
baileáthacliath
                    -> punycode()
bailethacliath-zgb
                    -> ASCII
                       Compatible
                       Encoding()
xn--bailethacliath-zgb
```

Unicode to Punycode

- Start with the ISO3166 “user assigned” range
  - AA, QM-QZ, XA-XZ, ZZ
- Remove any prefix already seen in use
- Remove visually similar codes
- 18 choices remain

XB XC XD XE XF XG XH XJ XK
XM XN XP XQ XR XT XW XX XY

Why “xn--”?

Trading volume on Monday 2003-02-10

IMS Hlth RX	22157
IL Tool ITW	11795
IntRectifr IRF	5742
IBM IBM	78719
IntPaper IP	16609
Interpublic IPG	34961
Inamed IMDC	1567
Informatica INFA	4357
Inktomi INKT	6085
i2 Tch ITWO	37777
IDEC Pharm IDPH	18754
Intel INTC	524545

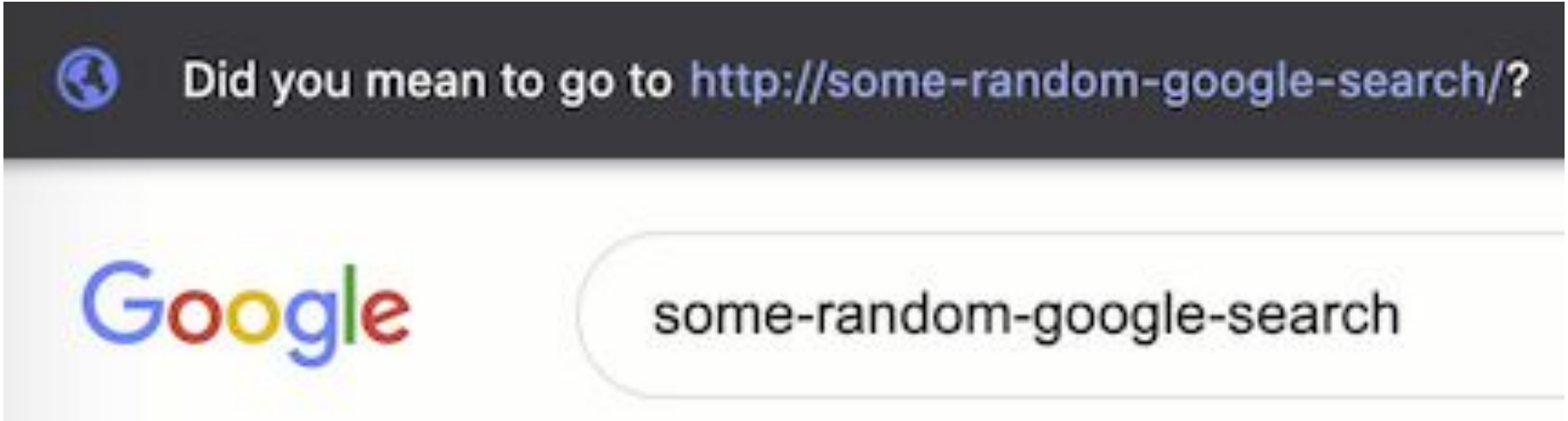
Why “xn--”?

👍.com? ❌

⛄.com? ✔

Emoji domains 🥳?

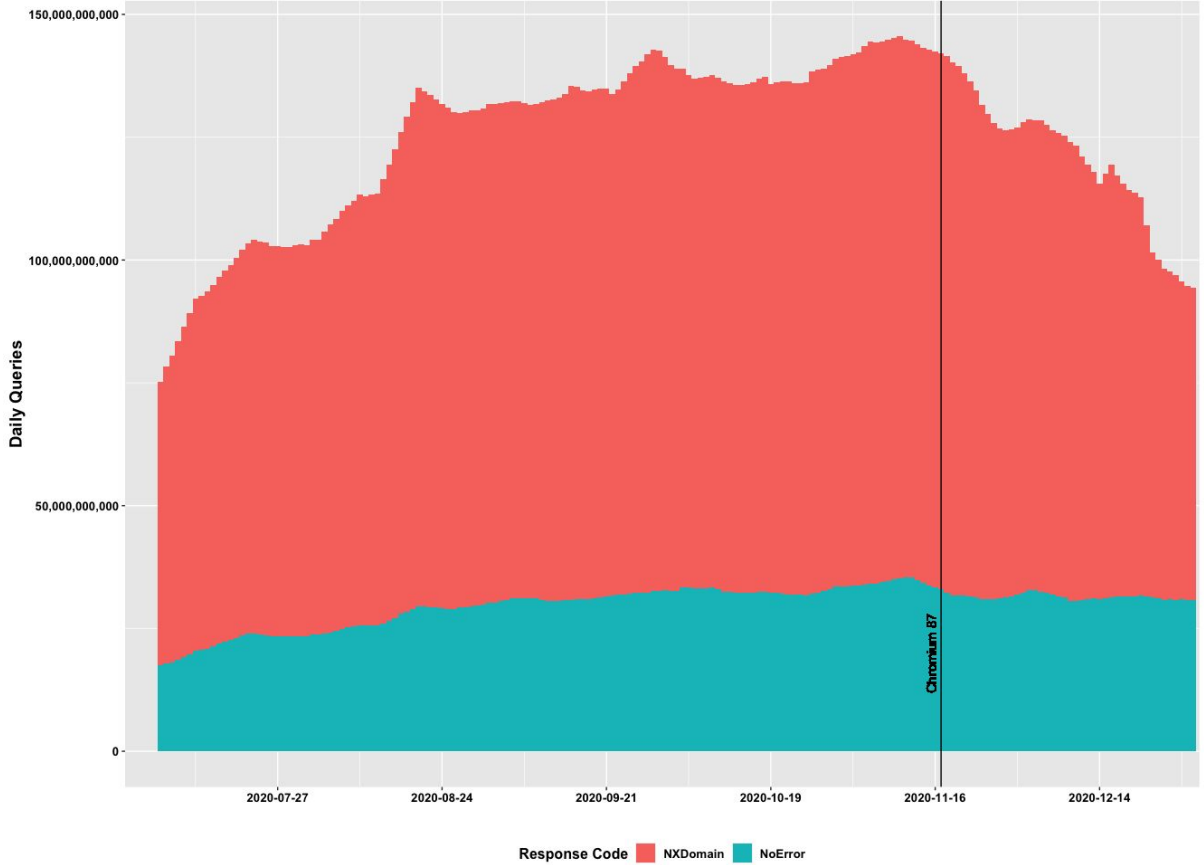
Why, Chrome? Why?


Did you mean to go to http://some-random-google-search/?
Google
some-random-google-search

Did you mean ... ?

http://rociwefoie/
http://uawfkfrefre/
http://awoimveroi/

Chrome’s random probes



Root nameserver stats, 2020

You Depend on DNS, That's (Some Of) How It Works and Did You Believe It?