Captive portal considered broken

warbiking \o/

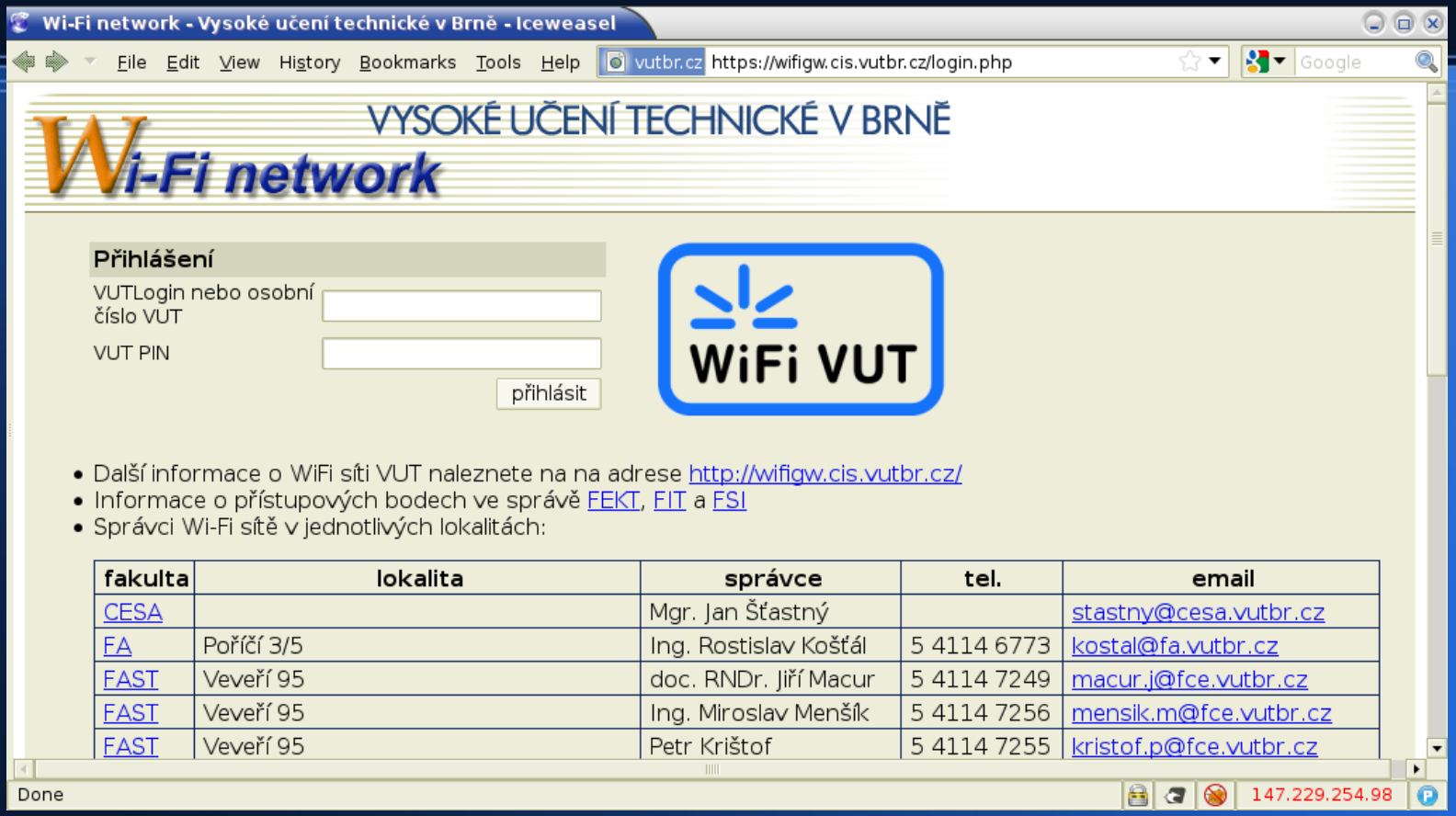
28.2. 02:39 Jenda | skóre: 60 | blog: Výlevníček | Praha
Re: Blokace internetovýc stránek
Odpovědět | Označit jako řešení | Sbalit | Výše | Link | Blokovat | Admin

> *Maximální výhoda řešení GeCon je však jeho absolutní spolehlivost filtrace a monitoringu webových stránek. Tato vlastnost je dána tím, že na koncové klienty se neinstaluje žádná aplikace, která by monitorovala ona PC a zakazovala přístup na určité stránky. Tuto funkci totiž* ***obstrává*** *samotný server, přes který probíhá veškerý obsah z internetu. Již z principu tedy není možné toto řešení nijak obejít a stává se tak 100%****-ně*** *spolehlivým.*

Vsadíme se o polárkáč, že to do deseti minut prostřelím?

Fuj, to byl hrozný sen! Zahlédl jsem v hexdumpu g!

Captive portal



- + easy to use
- - insecure, insecure, insecure

Common implementation problems

- Some ports allowed (UDP/53) 

- Plain HTTP login 

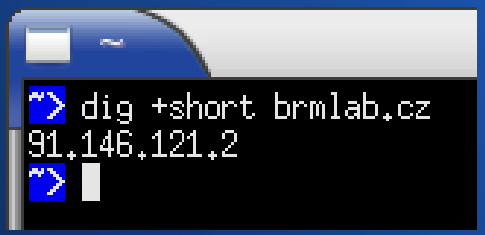
- Internal DNS queries allowed

Design flaws

- Client autentization based on MAC…
  - …MACs can be spoofed…
    - …users can be spoofed…
      - …data retention!
- Wireless traffic encryption?!

DNS tunelling

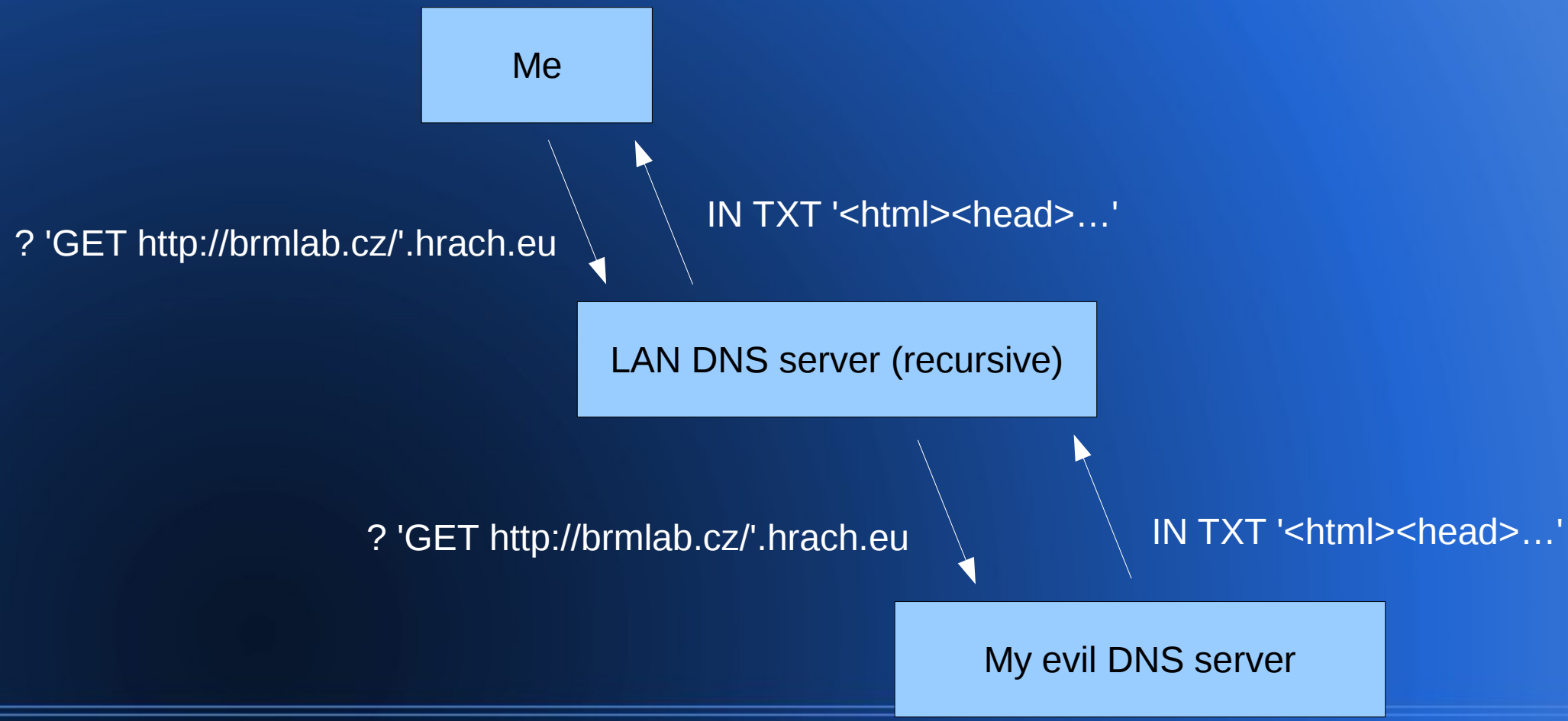
- You can push DNS queries…



- …you can push the whole Internet!

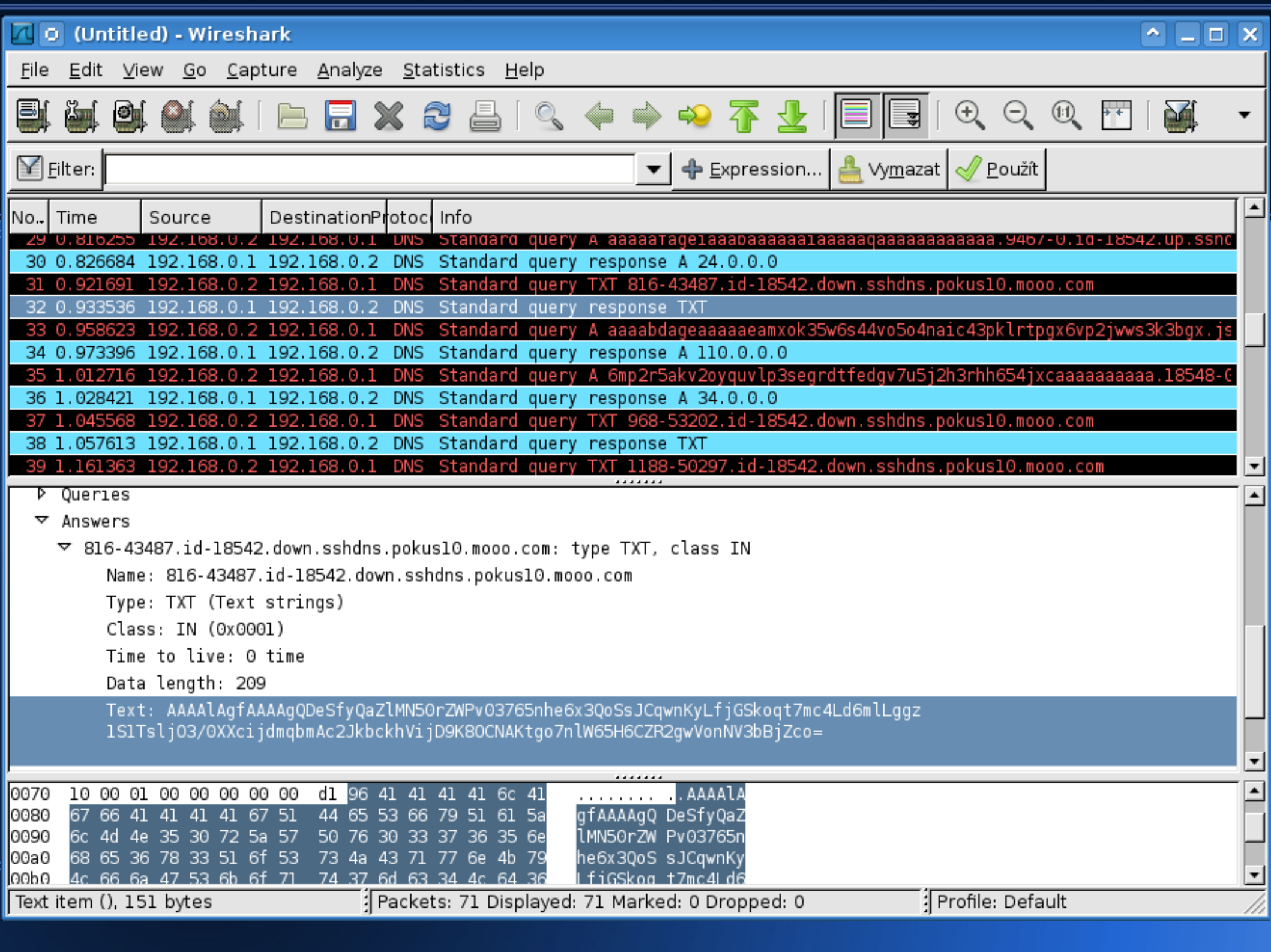
- Bypass nearly any restriction – blocked ports, L7 filters, government censorship…
  - even better than Tor or Skype
  - but requires special endpoint and is slow (~1 kB/s)

How does it work?



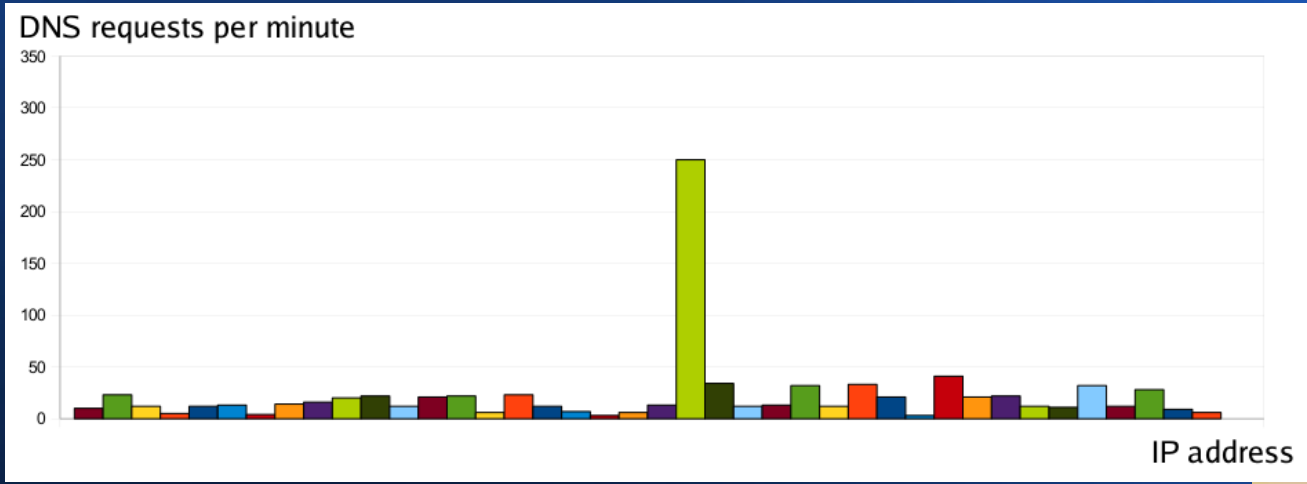
Well, the *real* implementation…

- Tunnels SSH – encryption, built-in socks proxy…
- BASE32 (case-insensitive) queries and BASE64 responses in TXT records
- Some flow control (we emulate TCP!)


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Vymazat Použít
No. Time Source DestinationProtoc Info
30 0.826684 192.168.0.1 192.168.0.2 DNS Standard query response A 24.0.0.0
31 0.921691 192.168.0.2 192.168.0.1 DNS Standard query TXT 816-43487.id-18542.down.sshdns.pokus10.mooo.com
32 0.933536 192.168.0.1 192.168.0.2 DNS Standard query response TXT
33 0.958623 192.168.0.2 192.168.0.1 DNS Standard query A aaaabdageaaaaaeamxok35w6s44vo5o4naic43pklrtpgx6vp2jwws3k3bgx.js
34 0.973396 192.168.0.1 192.168.0.2 DNS Standard query response A 110.0.0.0
35 1.012716 192.168.0.2 192.168.0.1 DNS Standard query A 6mp2r5akv2oyquvlp3segrdtfedgv7u5j2h3rhh654jxcaaaaaaaaaa.18548-0
36 1.028421 192.168.0.1 192.168.0.2 DNS Standard query response A 34.0.0.0
37 1.045568 192.168.0.2 192.168.0.1 DNS Standard query TXT 968-53202.id-18542.down.sshdns.pokus10.mooo.com
38 1.057613 192.168.0.1 192.168.0.2 DNS Standard query response TXT
39 1.161363 192.168.0.2 192.168.0.1 DNS Standard query TXT 1188-50297.id-18542.down.sshdns.pokus10.mooo.com
Queries
Answers
816-43487.id-18542.down.sshdns.pokus10.mooo.com: type TXT, class IN
Name: 816-43487.id-18542.down.sshdns.pokus10.mooo.com
Type: TXT (Text strings)
Class: IN (0x0001)
Time to live: 0 time
Data length: 209
Text: AAAAlAgfAAAAgQDeSfyQaZlMN50rZWPv03765nhe6x3QoSsJCqwnKyLfjGSkoqt7mc4Ld6mlLggz
1S1Tslj03/0XXcijdmqbmAc2JkbckhVijD9K8OCNAKtgo7nlW65H6CZR2gwVonNV3bBjZco=
0070 10 00 01 00 00 00 00 00 d1 96 41 41 41 41 6c 41 .... .AAAAlA
0080 67 66 41 41 41 41 67 51 44 65 53 66 79 51 61 5a gfAAAAgQ DeSfyQaZ
0090 6c 4d 4e 35 30 72 5a 57 50 76 30 33 37 36 35 6e lMN50rZW Pv03765n
00a0 68 65 36 78 33 51 6f 53 73 4a 43 71 77 6e 4b 79 he6x3QoS sJCqwnKy
Text item (), 151 bytes
Packets: 71 Displayed: 71 Marked: 0 Dropped: 0
Profile: Default

Oh god, I want my students (employees, citizens) to be safe!

- IDS to detect (enormous DNS traffic)



  - there are other possibilities (IP over Avian Carriers, Morse Code over ICMP…)

The ultimate solution

scissors ethernet cal

File Edit Vie

able&tbr

Přihlásit se

Google scissors ethernet cable

Vyhledávání Přibližný počet výsledků: 79 200 (0,10 s)

Bezpečné vyhledávání - mírný režim

Vše
Obrázky
Videa
Zprávy
Nákupy
Více

Všechny výsledky
Podle tématu

Libovolná velikost
Velká
Střední
Ikona
Větší než...
Přesně...

Libovolná barva
Plné barvy

http://www.google.com/imgres?hl=cs&biw=1079&bih=671&tbs=imgo:1&tbm=isch&tbnid=qWYXYUXJqzZR-M:&imgrefurl=ht...

74.125.79.102 +2

More magnets!

- http://jenda.hrach.eu/f/installfest-2010-dns-tunelovani.odp
- http://dnstunnel.de/
- http://heyoka.sourceforge.net/

UAG

(the end)