Advanced IPv6 Network Reconnaissance

Fernando Gont

SI6 NETWORKS

IPv6 Business Conference
Zürich, Switzerland. June 16, 2016

About...

- Security Researcher and Consultant at SI6 Networks
- Published:
  - 25 IETF RFCs (13 on IPv6)
  - 10+ active IETF Internet-Drafts
- Author of the SI6 Networks' IPv6 toolkit
  - http://www.si6networks.com/tools/ipv6toolkit
- I have worked on security assessment of communication protocols for:
  - UK NISCC (National Infrastructure Security Co-ordination Centre)
  - UK CPNI (Centre for the Protection of National Infrastructure)
- More information at: http://www.gont.com.ar

Introduction

- IPv6 changes the “Network Reconnaissance” game
- Brute force address scanning attacks undesirable (if at all possible)
- Security guys need to evolve in how they do net reconnaissance
    - Pentests/audits
    - Deliberate attacks
- Network reconnaissance support in security tools has traditionally been **very poor**

What we have done

- Research on IPv6 network reconnaissance
  - Much of it published in IETF RFC 7707 (“Network Reconnaissance in IPv6 Networks”) -- new RFC!
- SI6 Networks' IPv6 Toolkit
  - Free, open-source, portable IPv6 toolkit
  - https://www.si6networks.com/tools/ipv6toolkit

IPv6 Address Scanning

Dismantling a Myth

IPv6 host scanning attacks

"Thanks to the increased IPv6 address space, IPv6 host scanning attacks are unfeasible. Scanning a /64 would take 500.000.000 years"

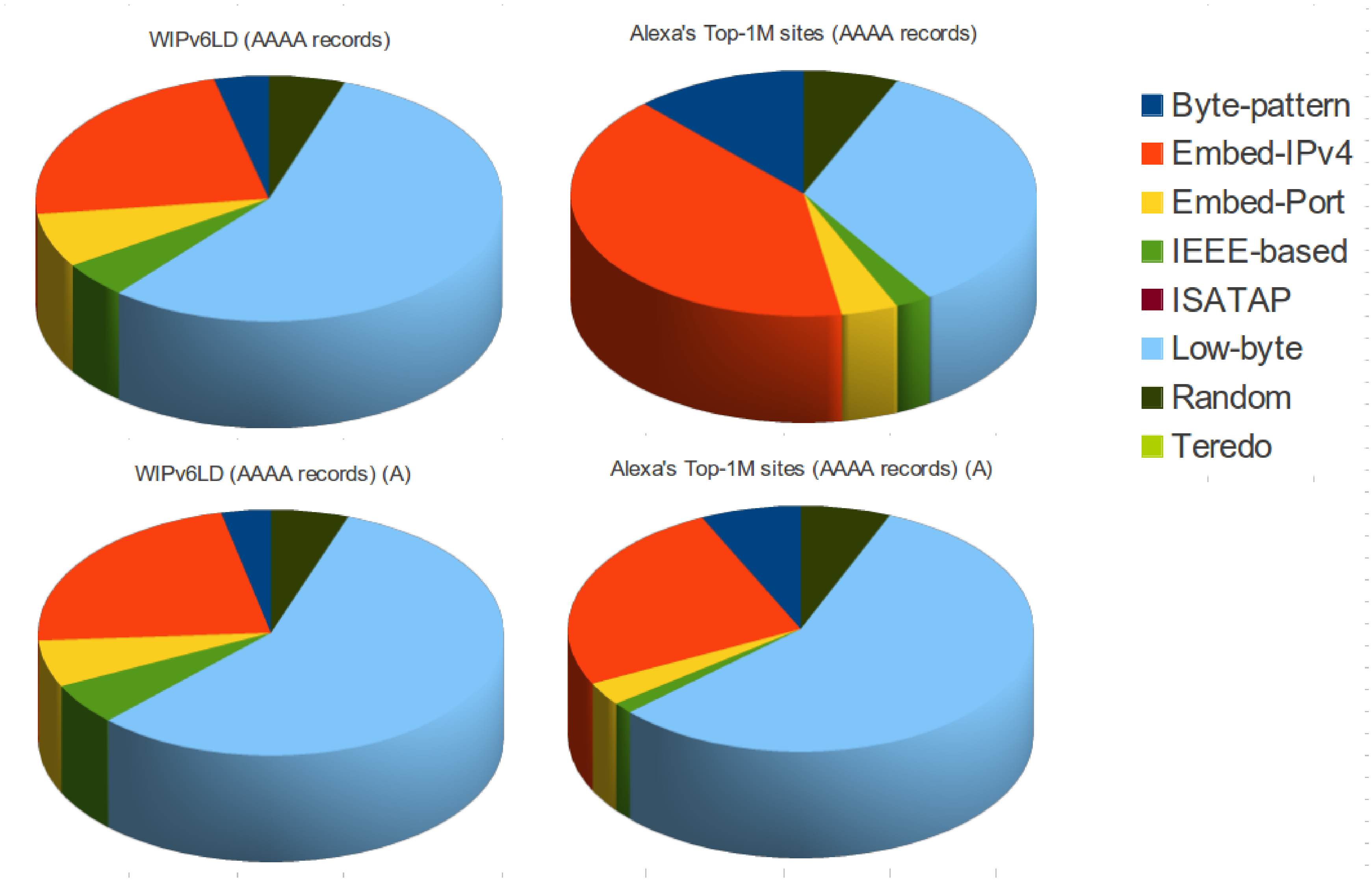
– Urban legend

Is the search space for a /64 really 2^{64} addresses?

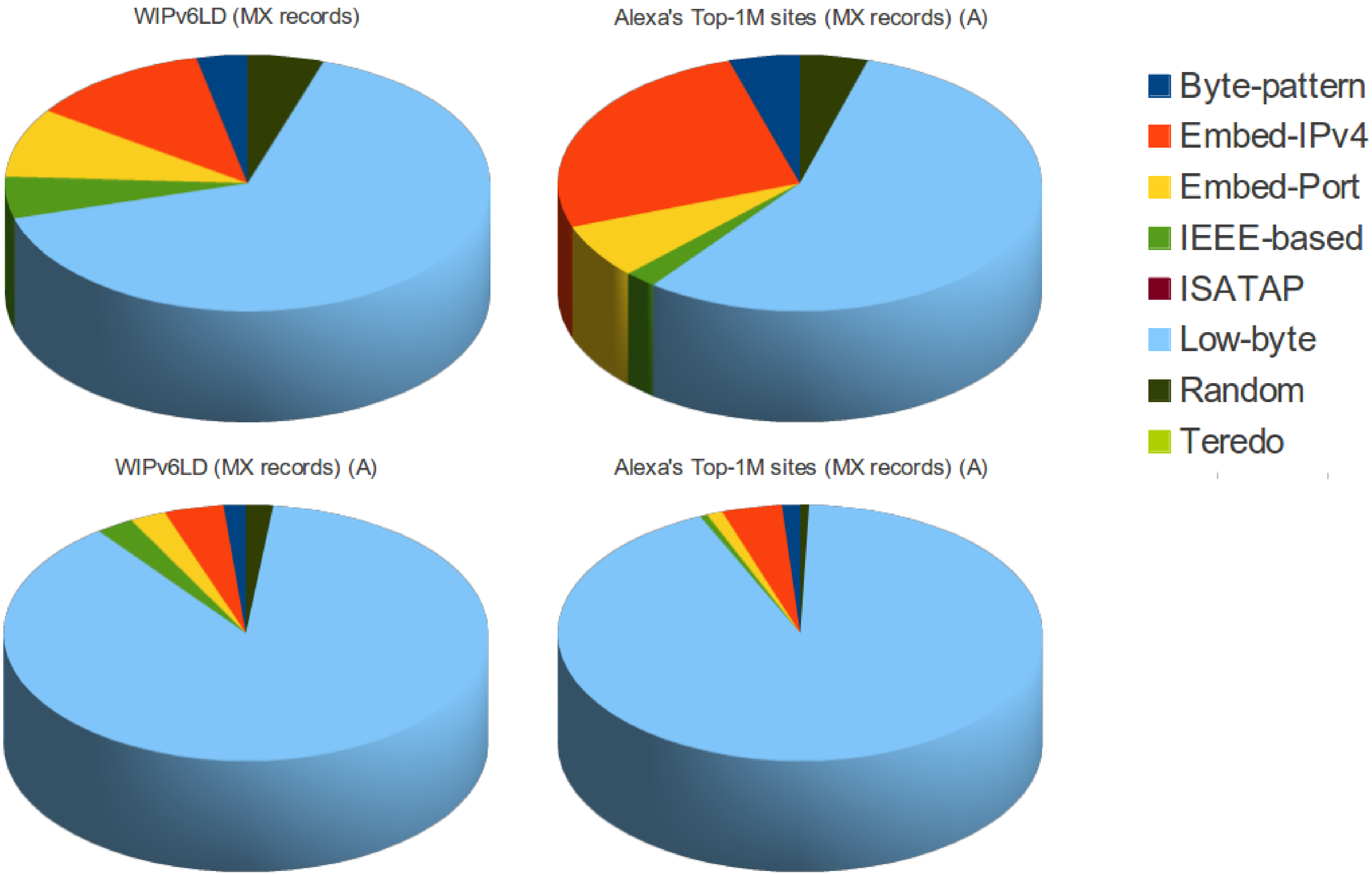
Our experiment

- Find “a considerable number of IPv6 nodes” for address analysis:
  - Alexa Top-1M sites -> **`script6`** -> **`addr6`**
  - World IPv6 Launch Day site -> **`script6`** -> **`addr6`**
- For each domain:
  - AAAA records
  - NS records -> AAAA records
  - MX records -> AAAA records
- What did we find?

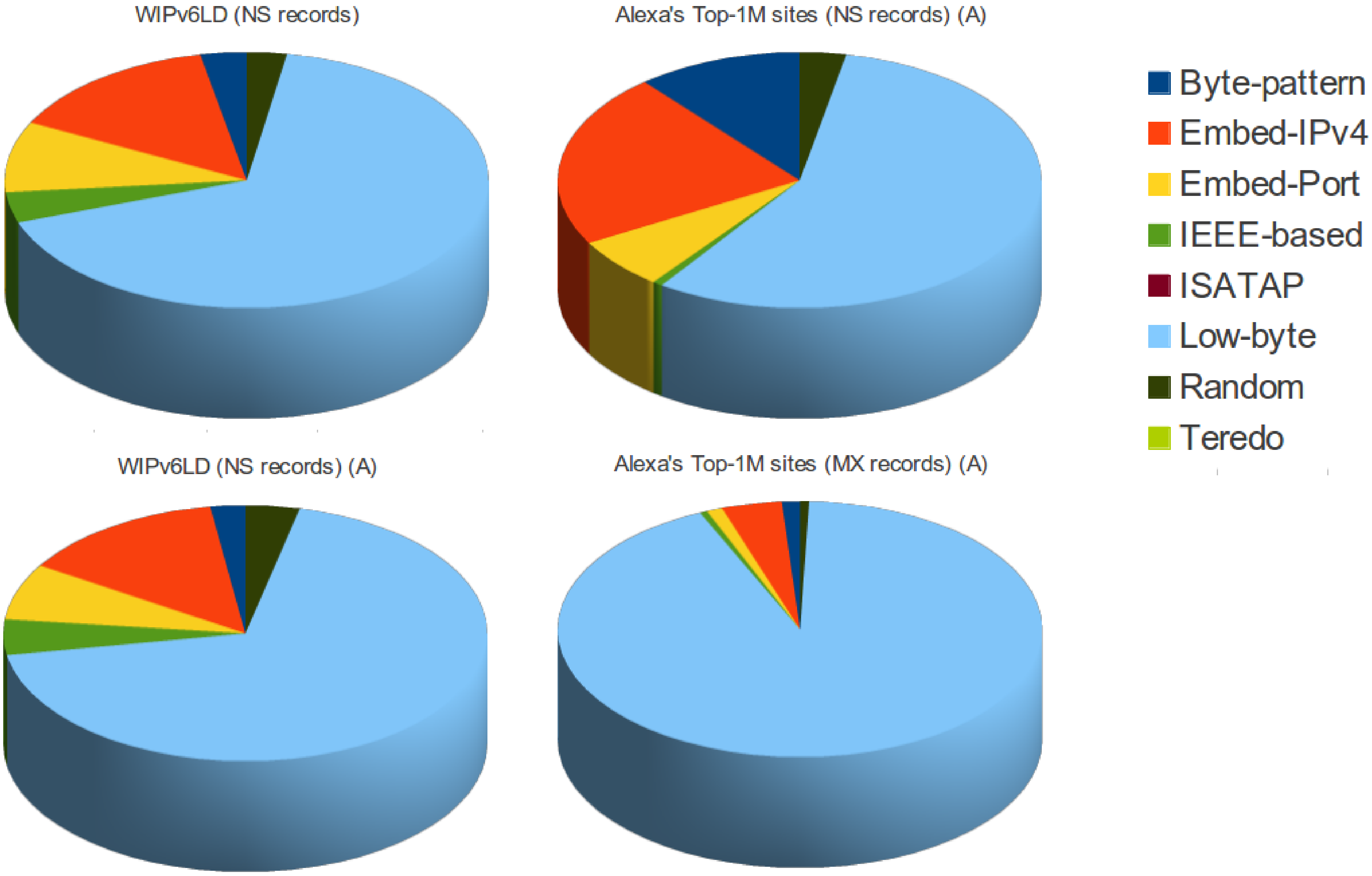
IPv6 address distribution for the web



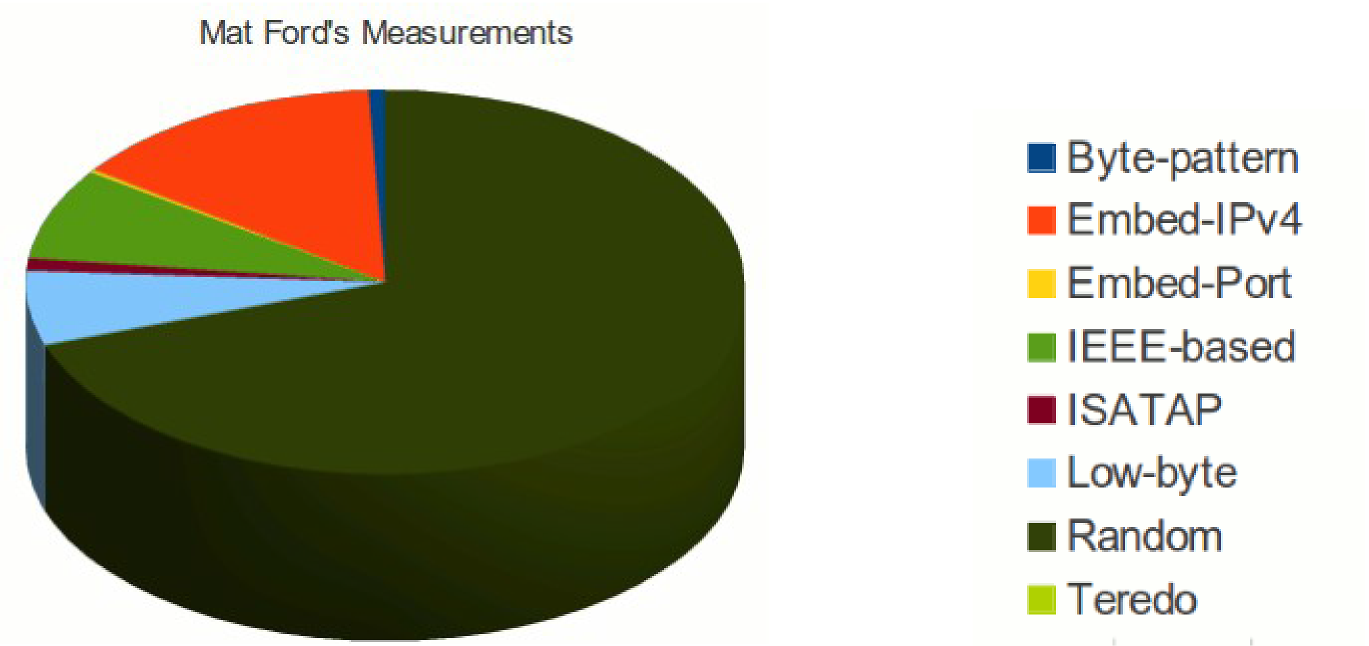
IPv6 address distribution for mail servers



IPv6 address distribution for the DNS



Client addresses



- Caveats:
  - Graphic illustrates IID types used for outgoing connections.
  - No data about IID types used for stable addresses when RFC4941 is employed.

Source: <http://www.internetsociety.org/blog/2013/05/ipv6-address-analysis-privacy-transition-out>

Some take-aways from our study

- Server addresses clearly do follow patterns
  - The majority of addresses follow patterns with a small search space
- Passive measurements on client addresses are of little use
  - Due to IPv6 temporary addresses (RFC4941)

IPv6 Addressing Scanning

Leveraging Address Patterns

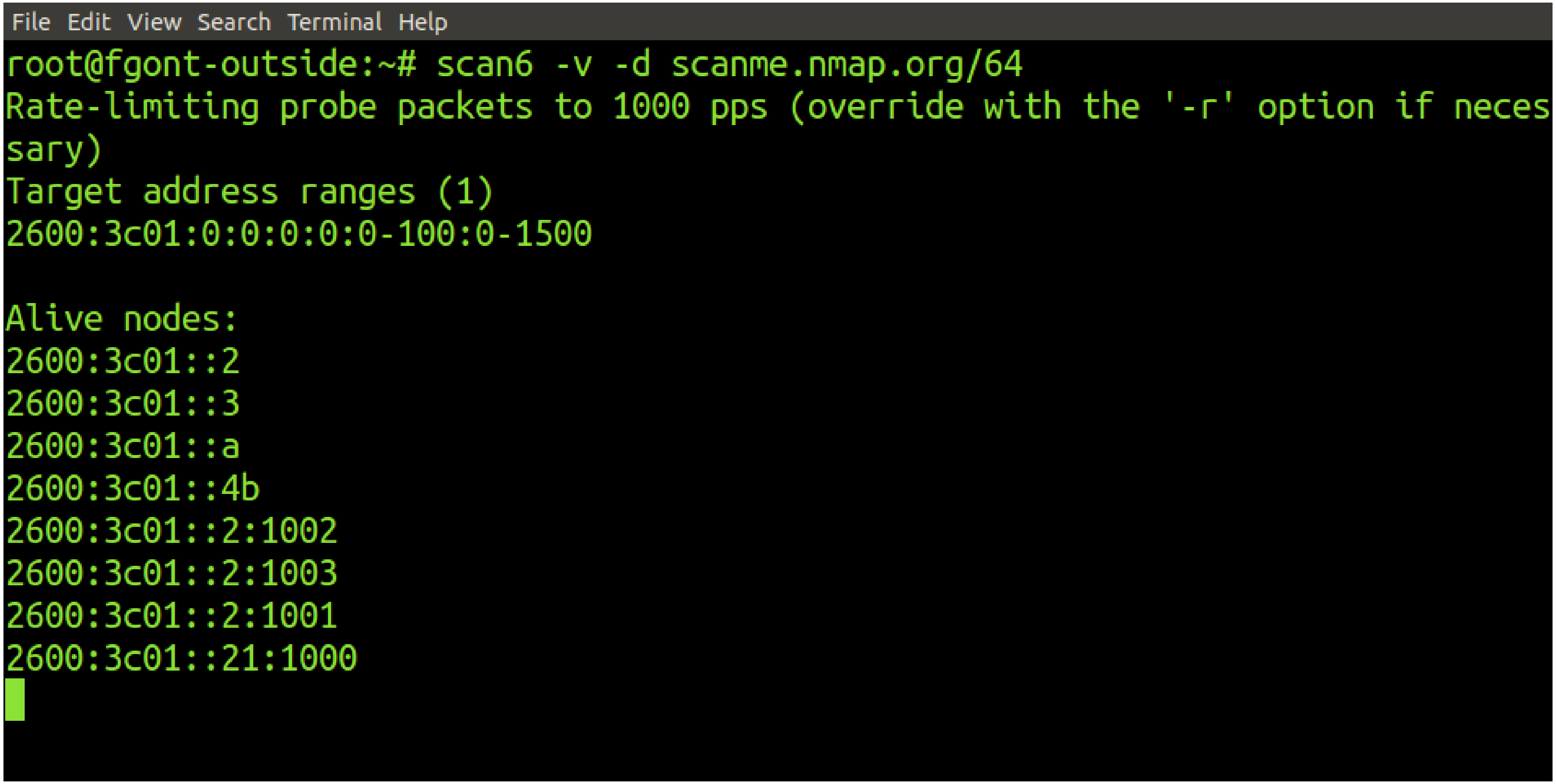
scan6: Smart IPv6 address scanning

- **`scan6`** of the SI6 Networks' IPv6 Toolkit is probably the most comprehensive address scanner to date
- It can "automagically" detect address patterns and target only the corresponding search space
- How to employ "smart" scanning:

```
sudo scan6 -d DOMAIN/64 -v

sudo scan6 -d ADDRESS/64 -v
```

scan6: Smart IPv6 address scanning (II)



```
root@fgont-outside:~# scan6 -v -d scanme.nmap.org/64
Rate-limiting probe packets to 1000 pps (override with the '-r' option if neces
sary)
Target address ranges (1)
2600:3c01:0:0:0:0-100:0-1500

Alive nodes:
2600:3c01::2
2600:3c01::3
2600:3c01::a
2600:3c01::4b
2600:3c01::2:1002
2600:3c01::2:1003
2600:3c01::2:1001
2600:3c01::21:1000
```

IPv6 Addressing Scanning

The low-hanging fruit

Overview

- Leverage IPv6 all-nodes link-local multicast address
- Employ multiple probe types:
  - Normal multicasted ICMPv6 echo requests (don't work for Windows)
  - Unrecognized options of type 10xxxxxx
- Combine learned IIDs with known prefixes to learn all addresses
- Example:

  ```
  # scan6 -i eth0 -L
  ```

Working with IPv6 addresses

`addr6` to the rescue!

Introduction

- Given a set of IPv6 address, you may want to:
  - Discard duplicate addresses
  - Discard addresses of specific scope
  - Analyze the address type
  - Produce statistics
- We created `addr6` for that!

Filtering IPv6 addresses

- addr6 has a number of features to filter IPv6 addresses
- Filter duplicate addresses:

```
cat LIST.TXT | addr6 -i -q
```

- Accept (or block) specific prefixes:

```
cat LIST.TXT | addr6 -i --accept 2001:db8::/16
cat LIST.TXT | addr6 -i --block 2001:db8::/16
```

- Accept (or block) address types:

```
cat LIST.TXT | addr6 -i --accept-type TYPE
cat LIST.TXT | addr6 -i --block-type TYPE
```

  - Types: unicast, unspec, multicast

Filtering IPv6 addresses (II)

- Accept (or block) address scopes:

```
cat LIST.TXT | addr6 -i --accept-scope SCOPE
cat LIST.TXT | addr6 -i --block-scope SCOPE
```

  - Scopes: interface, link, admin, site, local, global...

- Accept (or block) unicast address types:

```
cat LIST.TXT | addr6 -i --accept-utype TYPE
cat LIST.TXT | addr6 -i --block-utype TYPE
```

  - Types: loopback, ipv4-compat, ipv4-mapped, link-local, site-local, unique-local, 6to4, teredo, global

Producing statistics

- The addr6 tool can produce statistics based on a group of IPv6 addresses
- Example:

```
cat LIST.TXT | addr6 -i -s
```

IPv6 Extension Headers

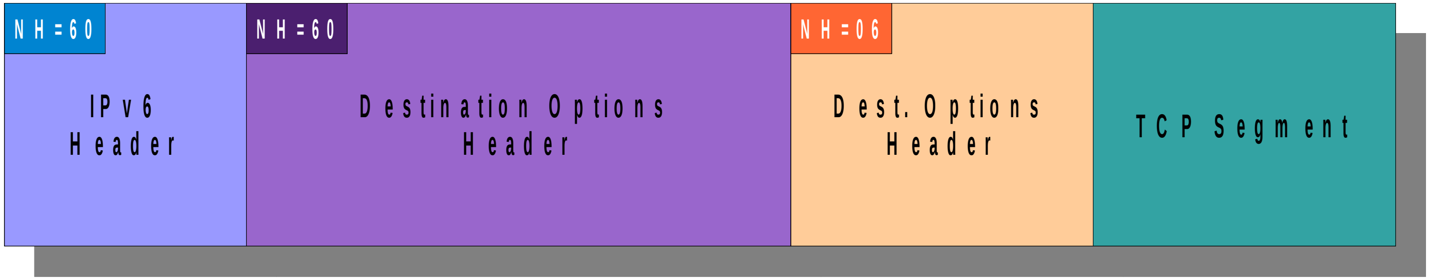
In Network Reconnaissance

IPv6 Extension Headers

Overview

General IPv6 packet format

- Consists of an IPv6 header chain and an (optional) payload
- Each Extension Header is typically encoded as TLV (Type-Length-Value)
- Any number of instances of any number of different headers are allowed
- Each header may contain an arbitrary number of options



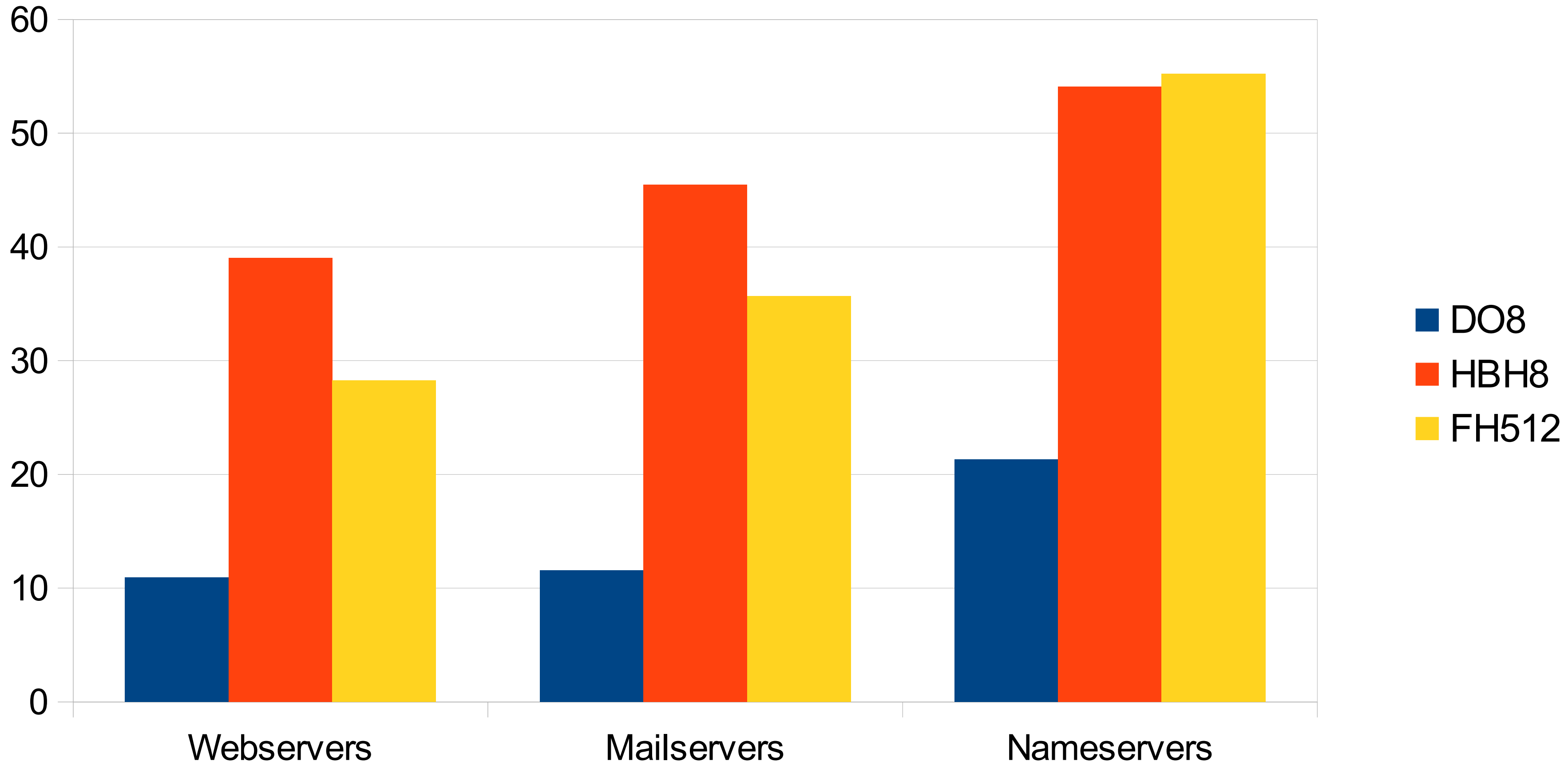
Processing the IPv6 header chain

- Implications for inspecting “boxes”:
  - Large number of headers/options may have a negative impact on performance
  - Many routers can only look into a few dozen bytes into the packet
  - It becomes harder (if at all possible) to enforce layer-4 ACLs
  - Fragmentation represents similar challenge as in IPv4
- Potential benefits for network reconnaissance:
  - Evasion

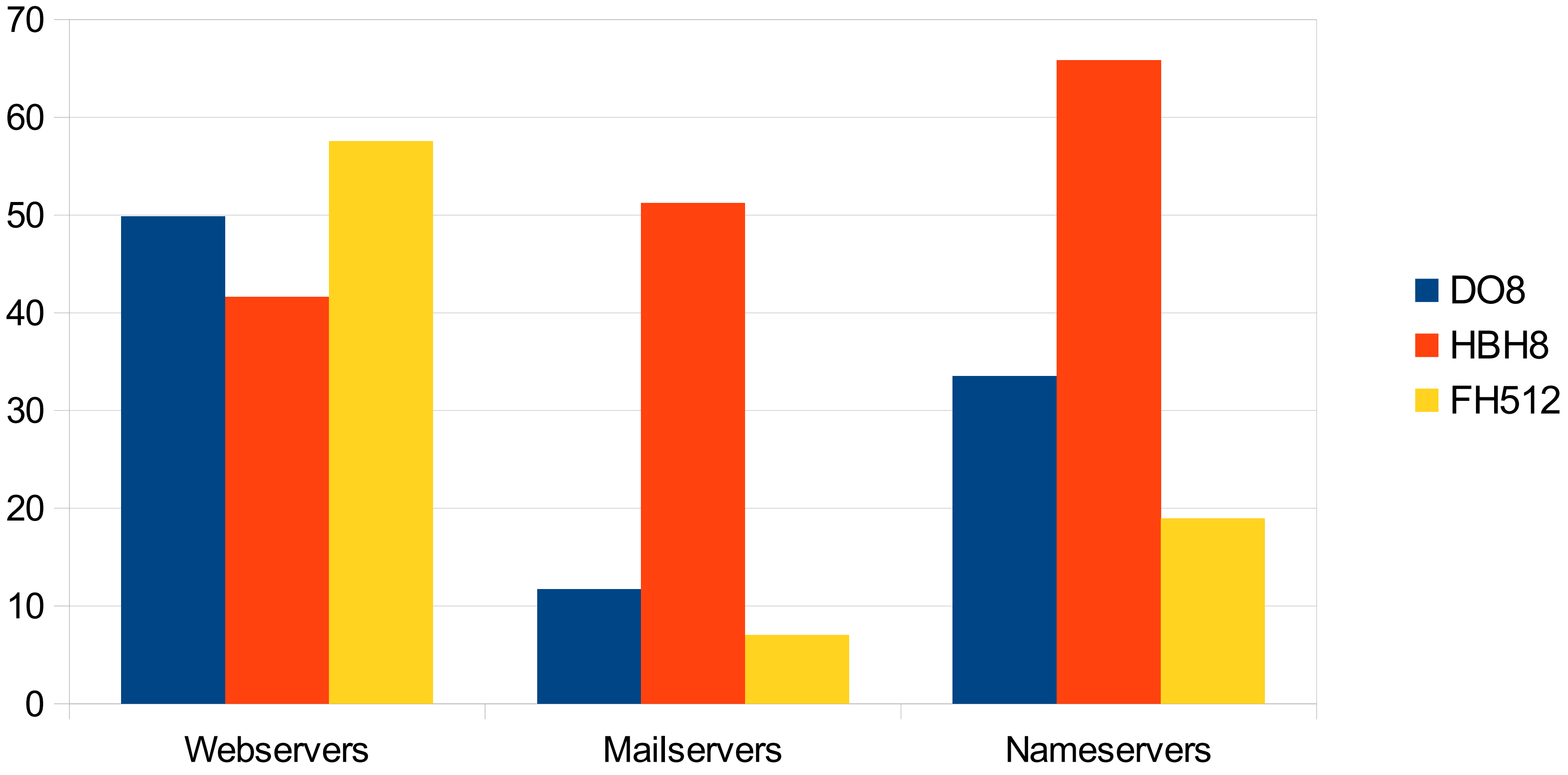
IPv6 Extension Headers

In The Real World

Alexa dataset: Packet Drop rate



Alexa dataset: Drops by diff. AS



So... what does this all mean?

- IPv6 EHs “not that cool” for evasion or reconnaissance

  ...at least when doing remote IPv6 network reconnaissance!

IPv6 Extension Headers

Use in network reconnaissance

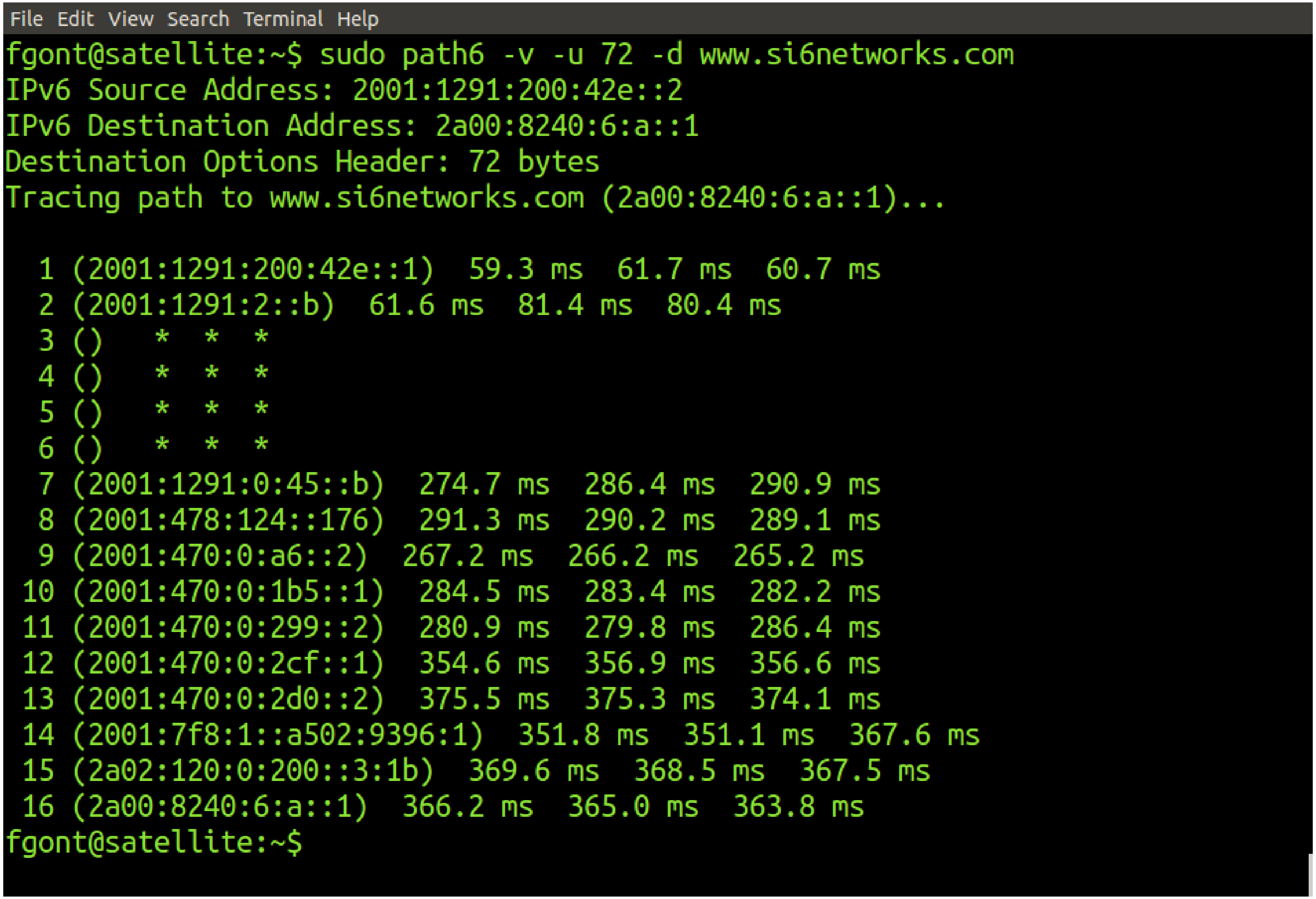
path6: An EH-enabled traceroute

- How far do your IPv6 EH-enabled packets get?
- No existing traceroute tool supported IPv6 extension headers
- Hence we produced our path6 tool
  - Supports IPv6 Extension Headers
  - Can employ TCP, UDP, or ICMPv6 probes
  - It's faster ;-)
- Example:

```
# path6 -u 100 -d fc00:1::1
```

Dst Opt Hdr

path6: An EH-enabled traceroute (II)



```
fgont@satellite:~$ sudo path6 -v -u 72 -d www.si6networks.com
IPv6 Source Address: 2001:1291:200:42e::2
IPv6 Destination Address: 2a00:8240:6:a::1
Destination Options Header: 72 bytes
Tracing path to www.si6networks.com (2a00:8240:6:a::1)...

  1 (2001:1291:200:42e::1)  59.3 ms  61.7 ms  60.7 ms
  2 (2001:1291:2::b)  61.6 ms  81.4 ms  80.4 ms
  3 ()   *  *  *
  4 ()   *  *  *
  5 ()   *  *  *
  6 ()   *  *  *
  7 (2001:1291:0:45::b)  274.7 ms  286.4 ms  290.9 ms
  8 (2001:478:124::176)  291.3 ms  290.2 ms  289.1 ms
  9 (2001:470:0:a6::2)  267.2 ms  266.2 ms  265.2 ms
 10 (2001:470:0:1b5::1)  284.5 ms  283.4 ms  282.2 ms
 11 (2001:470:0:299::2)  280.9 ms  279.8 ms  286.4 ms
 12 (2001:470:0:2cf::1)  354.6 ms  356.9 ms  356.6 ms
 13 (2001:470:0:2d0::2)  375.5 ms  375.3 ms  374.1 ms
 14 (2001:7f8:1::a502:9396:1)  351.8 ms  351.1 ms  367.6 ms
 15 (2a02:120:0:200::3:1b)  369.6 ms  368.5 ms  367.5 ms
 16 (2a00:8240:6:a::1)  366.2 ms  365.0 ms  363.8 ms
fgont@satellite:~$
```

blackhole6: Finding IPv6 blackholes

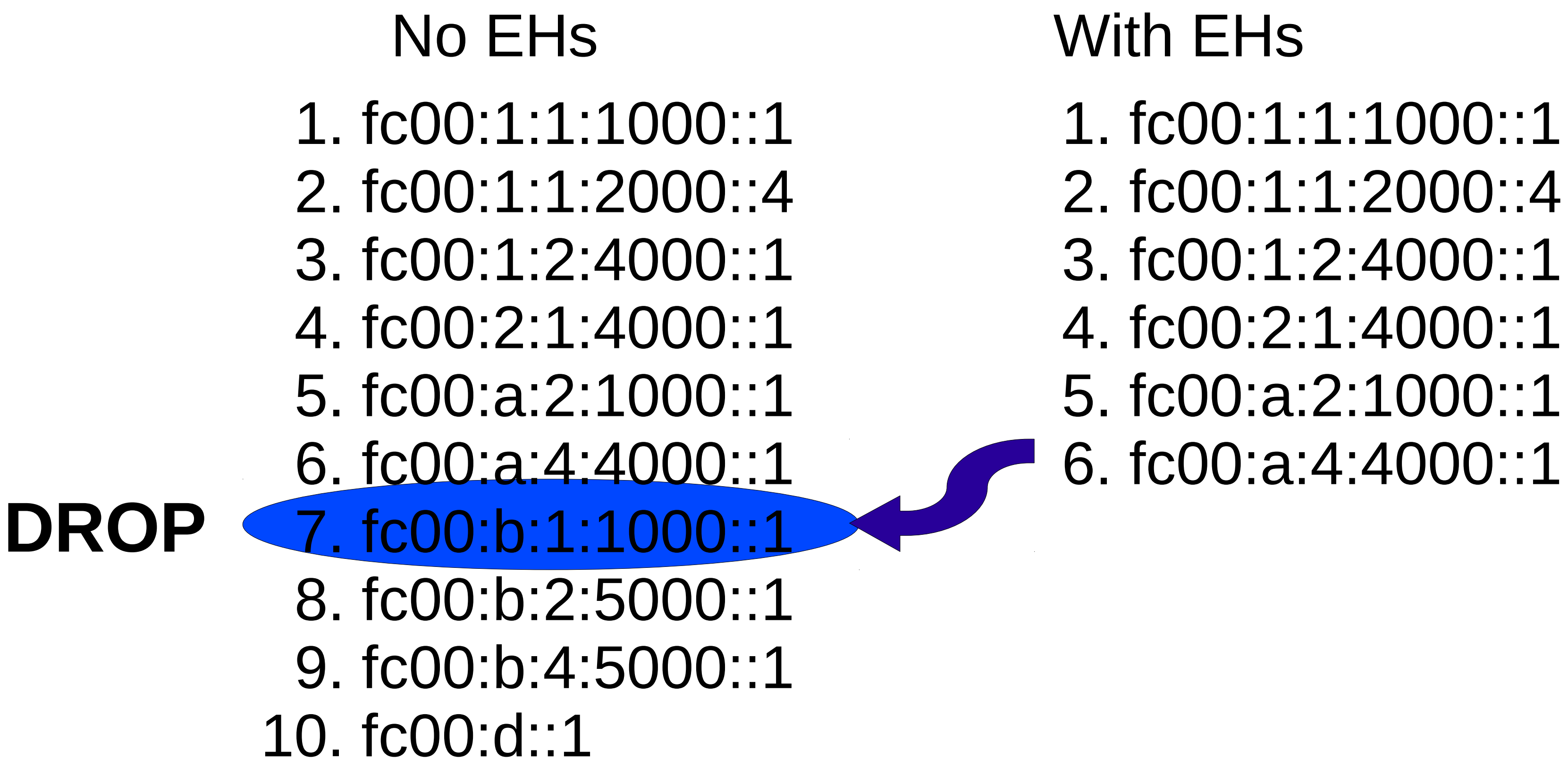
- How it works?
  - path6 without EHs + path6 with EHs + a little bit of magic

```
fgont@satellite:~$ sudo blackhole6 www.google.com do8
SI6 Networks IPv6 Toolkit v2.0
blackhole6: A tool to find IPv6 blackholes
Tracing www.google.com (2607:f8b0:400b:807::1012)...

Dst. IPv6 address: 2607:f8b0:400b:807::1012 (AS15169 - GOOGLE - Google
Inc.,US)
Last node (no EHs): 2607:f8b0:400b:807::1012 (AS15169 - GOOGLE - Google
Inc.,US) (13 hop(s))
Last node (DO 8): 2001:5a0:12:100::72 (AS6453 - AS6453 - TATA
COMMUNICATIONS (AMERICA) INC,US) (7 hop(s))
Dropping node: 2001:4860:1:1:0:1935:0:75 (AS15169 - GOOGLE - Google
Inc.,US || AS15169 - GOOGLE - Google Inc.,US)
```

blackhole6: Methodology

- Given the output of path6 for no-EH and EHs:



No EHs

1. fc00:1:1:1000::1
2. fc00:1:1:2000::4
3. fc00:1:2:4000::1
4. fc00:2:1:4000::1
5. fc00:a:2:1000::1
6. fc00:a:4:4000::1
7. fc00:b:1:1000::1
8. fc00:b:2:5000::1
9. fc00:b:4:5000::1
10. fc00:d::1

With EHs

1. fc00:1:1:1000::1
2. fc00:1:1:2000::4
3. fc00:1:2:4000::1
4. fc00:2:1:4000::1
5. fc00:a:2:1000::1
6. fc00:a:4:4000::1

DROP

Port scanning

The basics

IPv6-based TCP/UDP port scanning

- **`scan6`** incorporates all known TCP and UDP port-scanning techniques
- Specifying a protocol and port range:

```
--port-scan {tcp,udp}:port_low[-port_hi]
```

- Specifying a TCP scan type:

```
--tcp-scan-type {syn,fin,null,xmas,ack}
```

- Example:

```
--port-scan tcp:1-1024 --tcp-scan-type syn
```

TCP/UDP most popular ports

- scan6 can target the most frequently open ports
- All top ports for all protocols:

```
--port-scan all:top:all
```

- Top N of all protocols:

```
--port-scan all:top:N
```

- All TCP top ports:

```
--port-scan tcp:top:all
```

- Top N TCP ports

```
--port-scan tcp:top:N
```

Network Reconnaissance

Obtaining AS-related Info

Obtaining AS-related info

- Given an IPv6 address, the corresponding AS identifies the corresponding organization, e.g.
  - who should I contact when an IPv6 address is attacking me?
  - who should I contact when a given router is dropping my packets?
- script6 can query AS-related information:

```
script6 get-as

script6 get-asn
```

DNS for IPv6 Network Reconnaissance

Introduction

- Most of this ground is well-known from the IPv4-world:
  - DNS zone transfers
  - DNS bruteforcing
  - etc.
- DNS reverse-mappings particularly useful for “address scanning”

Get domains and IPv6 addresses

- script6 can do batch-processing of domain names
- Get IPv6 addresses:

```
$ cat domains.txt | script6 get-aaaa
```

- Get nameserver addresses:

```
$ cat domains.txt | script6 get-ns | script6
get-aaaa
```

- Get mailserver addresses:

```
$ cat domains.txt | script6 get-mx | script6
get-aaaa
```

Bruteforce domain names

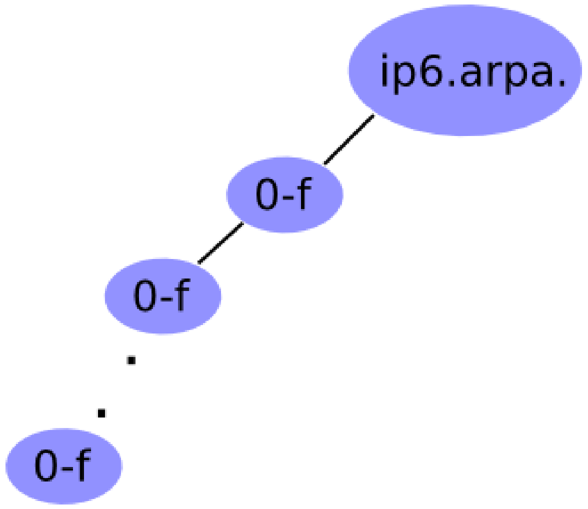
- script6 can bruteforce domain names and get the corresponding AAAA records
- For a single domain:

```
$ script6 get-bruteforce-aaaa DOMAIN
```

- Pipelined:

```
$ cat domains.txt | script6 get-bruteforce-aaaa
```

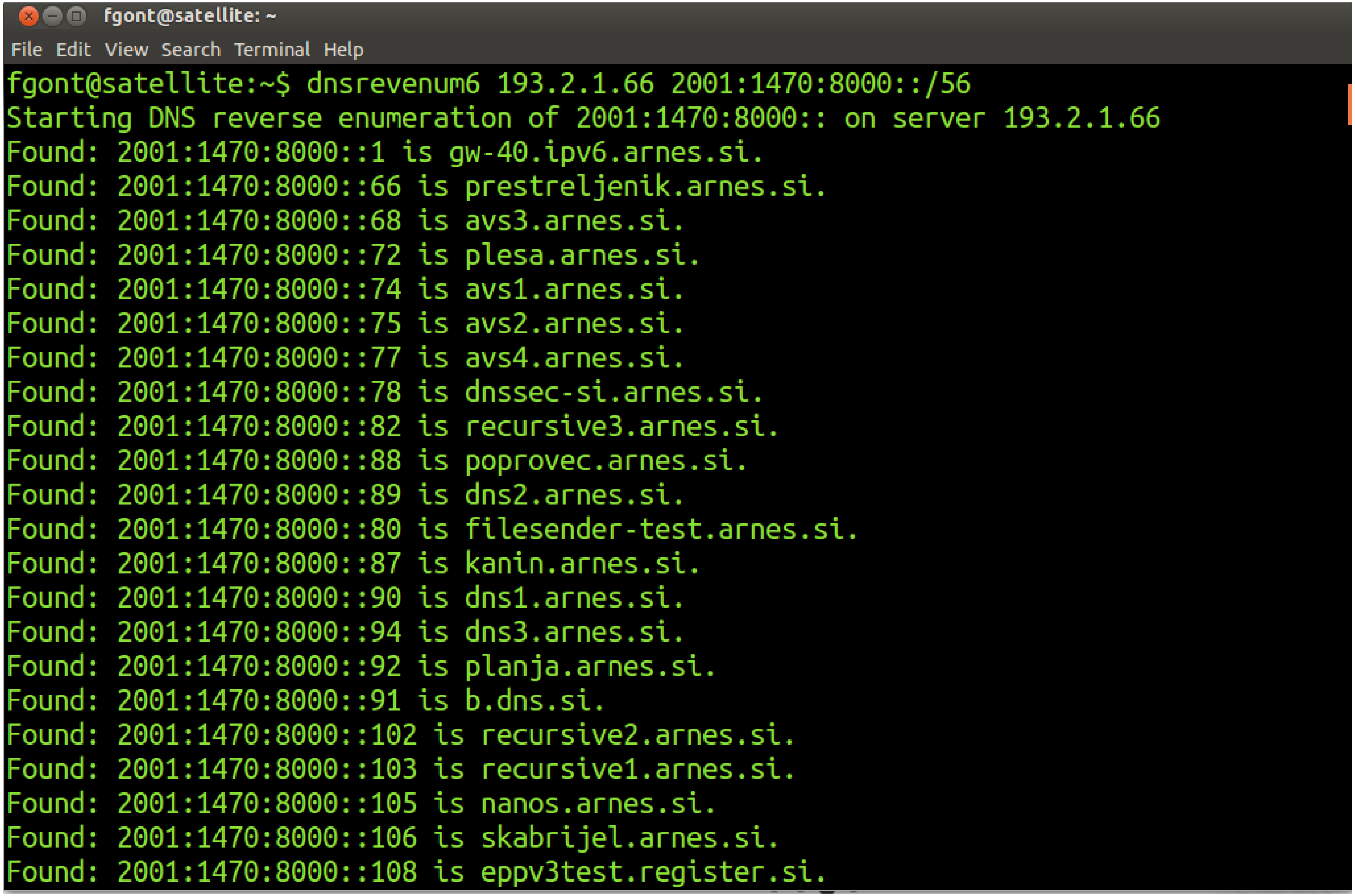
IPv6 DNS reverse mappings



- Technique:
  - Given a zone X.ip6.arpa., try the labels [0-f].X.ip6.arpa.
  - If an NXDOMAIN is received, that part of the "tree" should be ignored
  - Otherwise, if NOERROR is received, "walk" that part of the tree
- Example (using `dnsrevenum6` from **THC-IPv6**):

```
$ dnsrevenum6 DNSSERVER IPV6PREFIX
```

THC-IPv6's dnsrevenum6



```
fgont@satellite:~$ dnsrevenum6 193.2.1.66 2001:1470:8000::/56
Starting DNS reverse enumeration of 2001:1470:8000:: on server 193.2.1.66
Found: 2001:1470:8000::1 is gw-40.ipv6.arnes.si.
Found: 2001:1470:8000::66 is prestreljenik.arnes.si.
Found: 2001:1470:8000::68 is avs3.arnes.si.
Found: 2001:1470:8000::72 is plesa.arnes.si.
Found: 2001:1470:8000::74 is avs1.arnes.si.
Found: 2001:1470:8000::75 is avs2.arnes.si.
Found: 2001:1470:8000::77 is avs4.arnes.si.
Found: 2001:1470:8000::78 is dnssec-si.arnes.si.
Found: 2001:1470:8000::82 is recursive3.arnes.si.
Found: 2001:1470:8000::88 is poprovec.arnes.si.
Found: 2001:1470:8000::89 is dns2.arnes.si.
Found: 2001:1470:8000::80 is filesender-test.arnes.si.
Found: 2001:1470:8000::87 is kanin.arnes.si.
Found: 2001:1470:8000::90 is dns1.arnes.si.
Found: 2001:1470:8000::94 is dns3.arnes.si.
Found: 2001:1470:8000::92 is planja.arnes.si.
Found: 2001:1470:8000::91 is b.dns.si.
Found: 2001:1470:8000::102 is recursive2.arnes.si.
Found: 2001:1470:8000::103 is recursive1.arnes.si.
Found: 2001:1470:8000::105 is nanos.arnes.si.
Found: 2001:1470:8000::106 is skabrijel.arnes.si.
Found: 2001:1470:8000::108 is eppv3test.register.si.
```

Caveats for DNS reverse mappings

- Some DNS software responds with NOERROR for ENT (Empty Non-Terminals)
  - Please see draft-ietf-dnsop-nxdomain-cut

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com

Thanks to all our Sponsors

Infoblox®
CONTROL YOUR NETWORK

f5®

SWITCH

DIGICOMP

eb-Qual

itrain
THE ESSENCE OF IT

Sunny Connection

BLUECAT

asecus
securing your business

flowdays
achieving more together