NAME

dnstop − displays various tables of DNS traffic on your network

SYNOPSIS

dnstop [**−aps**] [**−b** *expression*] [**−i** *address*] [**−f** *filter*] [*device*] [*savefile*]

DESCRIPTION

dnstop is a small tool to listen on *device* or to parse the file *savefile* and collect and print statistics on the local network's DNS traffic. You must have read access to `/dev/bpf*`.

COMMAND LINE OPTIONS

The options are as follows:

−a anonymize addresses

−b *expression*
BPF filter expression
(default: udp dst port 53 and udp[10:2] & 0x8000 = 0)

−i *address*
ignore select addresses

−p Do not put the interface into promiscuous mode.

−s collect second-level domain statistics

−t collect third-level domain statistics

−f input filter name

The "unknown-tlds" filter includes only queries for TLDs that are bogus. Useful for identifying hosts/servers that leak queries for things like "localhost" or "workgroup."

The "A-for-A" filter includes only A queries for names that are already IP addresses. Certain Microsoft Windows DNS servers have a known bug that forward these queries.

The "rfc1918-ptr" filter includes only PTR queries for addresses in RFC1918 space. These should never leak from inside an organization.

savefile
a captured network trace in **pcap** format

device
ethernet device (ie fxp0)

RUN TIME OPTIONS

While running, the following options are available to alter the display:

s display the source address table

d display the destination address table

t display the breakdown of query types seen

o display the breakdown of opcodes seen

1 show the TLD table

2	show the SLD table
3	show the 3LD table
@	show the SLD+source table
#	show the 3LD+source table
ˆR	reset the counters
ˆX	exit the program
?	help

NON-INTERACTIVE MODE

If stdout is not a tty, **dnstop** runs in non-interactive mode. In this case, you must supply a savefile for reading, instead of capturing live packets. After reading the entire savefile, **dnstop** prints the top 50 entries for each table.

AUTHORS

Duane Wessels (wessels@measurement-factory.com)
Mark Foster (mark@foster.cc)
Jose Nazario (jose@monkey.org)
Sam Norris <@ChangeIP.com>
http://dnstop.measurement-factory.com/

BUGS

Unless compiled with -DUSE_PPP the program will not correctly decode PPP frames.