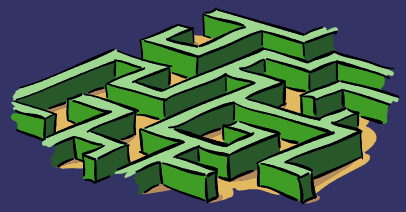
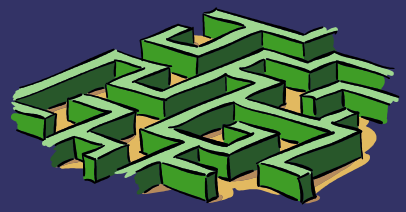
DNSCAP

Paul Vixie, ISC
with
Duane Wessels, Measurement Factory
July 2007



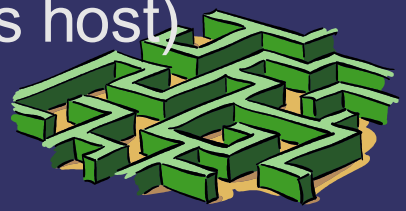
Things TCPDUMP Won't Do

- Close/reopen output files on a set schedule
- Search by DNS message type
- Select by DNS initiator or responder
- Listen to multiple interfaces
- Dump messages in DiG (text) format
- Select messages using regular expressions



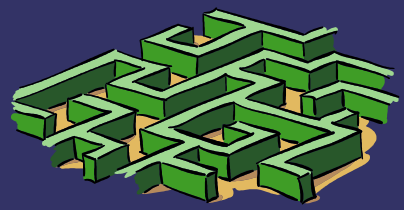
Output File Scheduling

- Motivations:
  - hourly (or some interval) output files
  - megapacket (or some other size) output files
- Mechanisms:
  - "**-b** *xxx*" option sets output file base name
  - files are called *xxx*.$*seconds*.$*microseconds*
    - (e.g., **pcap-f-sfo2.1184962119.000433**)
  - also, "**-k gzip**" would fork/exec a gzip command with the file name as its argument, on close
    - (usually -k refers to a more complex script that's also capable of scp'ing the new file to an analysis host)



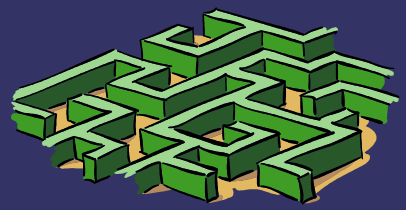
Searching by DNS Msg Type

- Motivations:
  - sometimes we only want queries, or updates, or (someday) notifies
  - sometimes we only want initiations, or responses
  - sometimes we want errors, sometimes not
- Mechanisms:
  - "**-m** [**quir**]" selects queries, updates, initiations, responses
  - "**-e** [**yn**]" selects noerrors, errors
  - multiple types can be selected



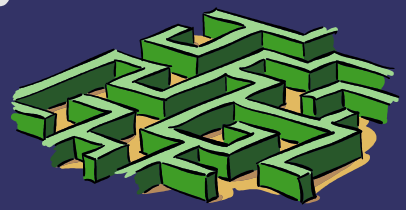
Selecting Initiators & Responders

- Motivation:
  - The BPF pattern for “all messages for which host *xxx* is the initiator” is quite complex
  - Some user mode filtering is also required
- Mechanisms:
  - “-q *xxx*” adds host *xxx* to the list of interesting initiators
  - “-r *yyy*” adds host *yyy* to the list of interesting responders
  - both sides of selected transactions are selected



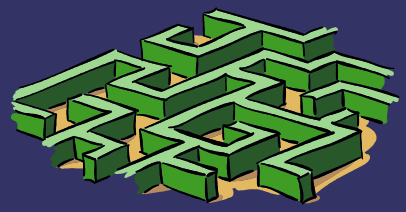
Multiple Interfaces

- Motivations:
  - on multihomed hosts and monitoring clusters, DNS packet data can appear on more than one network interface
  - on Linux, there's a pseudointerface called “all” that sometimes matches expectations
- Mechanisms:
  - “**-i** *ifname*” can be specified more than once
  - each one opens a separate *bpf* file descriptor
  - output packets are interspersed, mostly in order of receipt



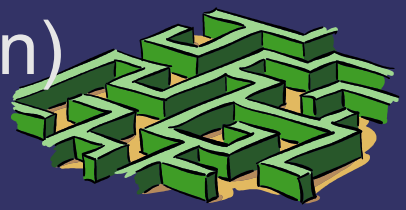
Dumping in DiG Format

- Motivations:
  - often we want to see the full DNS message in presentation (text) format
  - TCPDUMP only shows a one-line summary
- Mechanisms:
  - "**-g**" sends DiG-like output to *stderr*
- Design Notes:
  - *stdout* already reserved for binary *pcap* output
  - we might someday also teach DiG to read *pcap*



Regular Expression Searching

- Motivations:
  - for security work, it's often desirable to select DNS messages based on regular expressions
  - post-processing DiG-style output is painful
- Mechanisms:
  - "**-x** *pat*" adds to a list of patterns which must match the presentation form of the *qname* or of one of the answer, authority, or additional RRs
  - "**-n**" reverses the sense of all "**-x**", so, messages must not match
  - (this is per-message not per-transaction)



Status

- DNSCAP RC5 is available via anoncvs, see http://public.oarci.net/tools/dnscap/
- Have delayed the “final release” while the command line syntax evolves and settles
- It's time to declare that it's finished, and focus on other work (NCAP)
- These features and ideas should be revisited as part of a larger NCAP toolworks