Lab Exercise – DNS

Objective
DNS (Domain Name System) is the system & protocol that translates domain names to IP addresses.

Step 1: Analyse the supplied DNS Trace

Here we examine the supplied trace of a browser making DNS requests as follows.

Open the trace from here: https://kevincuran.com/320/labs/wireshark/trace-dns.pcap

1. You should see a screen as below showing just the DNS traffic which is normally carried on UDP port 53.

![Figure 3: DNS traffic](image-url)
To explore the details of DNS packets, select the first DNS query & expand its Domain Name System block (by using the “+” expander or icon). Your display should be similar to the one shown in the figure, with a series of packets with protocol DNS. We have selected the first DNS message.

Look for the following details:

- The DNS block follows the IP and UDP blocks. This is because DNS messages are carried in UDP segments within IP packets. You will see that the UDP port used by a nameserver is 53.
- The DNS header starts with a Transaction ID that is used to link a request and the corresponding reply – they both carry the same Transaction ID.
- Next come a set of flags that you can expand. They indicate whether the DNS message is a query or response, amongst other details.
- Then come the number of query, answer, authority and additional records. These fields conclude the header.
- After the DNS header, the remainder of the message consists of the indicated number of query, answer, authority and additional records. Often there will be only one query – for the IP address of the domain name we are seeking – but there may be many of the other records. These records are grouped in sections, such as the Authority section for all of the authority records. Each query has a Type code that indicates the kind of record sought, whether an IP address or other-
wise. Each of the other records also has a Type code that indicates whether it carries an IP address of a host, the name of a nameserver, or something else. The format of an individual record depends on its type. The entire DNS message is designed to fit within one UDP message.

- Wireshark may show other information, such as the number of the packet that carries the response to this request or the response time for the DNS exchange, but this is derived information. It is not actually carried on any packet.

*Repeat the above to look at a DNS response.* You should see a larger set of records in this message; while DNS queries mostly serve to carry the query, DNS responses often return a set of useful information (see below for the records in the second packet #2.)

![Figure 2: First DNS response – packet #2](image-url)
Step 2: Details of DNS Messages

Select the first DNS query packet in your trace, with the first several packets corresponding to earlier `dig` commands. To check, see if there are several queries that list the domain you chose in the Info column, each followed by a response.

The Transaction ID is 16 bits long, which makes collisions unlikely.

```
00 80 d0 02 97 c5 29 .Gn5.... ......  
d9 55 42 01 20 00 01 ....5.3 IJR. 
77 03 75 77 61 03 65 ..........W IyA
```

Since the host computer is setting this value, it can use all $2^{16}$ choices before repeating. This means that $2^{16}$ query/response pairs would need to be outstanding at the same time to cause a collision. For a normal computer, this is an extremely or implausibly high DNS workload.

The first flag bit signifies query or response. A “0” indicates a query, and hence a “1” a response.

```
Flags: 0x0120  Standard query
```

The DNS header is 12 bytes long.

```
Transaction: 1          0x0002
   Flags: 0x0120  Standard query
   0... .... .... .... = Response: Message is a query
   .000 0... .... .... = Opcode: Standard query (0)
   .... .0. .... .... = Truncated: Message is not truncated
   .... 1 .... .... = Recursion desired: Do query recursively
   .... .... .0. .... = Z: reserved (0)
   .... .... .1. .... = AD bit: Set
   .... .... ....0 .... = Non-authenticated data: Unacceptable
Questions: 1
```
The initial response should have provided another nameserver one step closer to the nameserver, but not the final answer. You will find that it includes the original query in its Query section. It will also include records with both the name of the nameservers to contact next, and the IP addresses of those nameservers. The final response in this series will include the IP address of the domain name – this is the answer to the query.

The names of name servers are carried in the Authority section in an NS (NameServer) record.

```
;;authority
www.uno.edu.au. type A, class IN

;Authoritative nameservers
au: type NS, class IN, ns 1.au
au: type NS, class IN, ns p.au
au: type NS, class IN, ns h.au
au: type NS, class IN, ns v.au
au: type NS, class IN, ns b.au
au: type NS, class IN, ns o.au
au: type NS, class IN, ns s.au
au: type NS, class IN, ns m.au
```

The IP addresses of the name servers are carried in the Additional section. The Type of record is A, for an IPv4 address, or AAAA for an IPv6 address.

```
;Additional records
a.au: type A, class IN, addr 58.65.254.73
b.au: type A, class IN, addr 58.65.253.73
h.au: type A, class IN, addr 202.65.13.73
l.au: type A, class IN, addr 209.112.113.34
l.au: type AAAA, class IN, addr 2001:500:856e::6:34
m.au: type A, class IN, addr 209.112.114.34
n.au: type A, class IN, addr 69.36.145.34
```

The IP address of the queried domain name is carried in the Answer section (in an A or AAAA record.)
**Step 3: DNS Response Time**

To conclude this lab, we will look at the DNS response time of the DNS queries. This is a normal DNS usage, in which a computer sends a single query and receives the answer in the response. The response time is the delay between when the computer sends the query to the local nameserver and when it receives the response from the local nameserver. This time includes the time taken by the local nameserver to contact remote nameservers, if the answer is not cached. Since this response time can delay connections to sites, it should be as small as possible.

*Proceed as follows to generate an “IO Graph” of the DNS response times.* IO graphs are a standard feature of Wireshark available under the Statistics menu. Select it now.

By default, this graph shows the rate of packets over time (See below)
We can also choose Statistics → DNS as shown below.

![Image of Wireshark DNS trace]

We expect that you will see many small DNS response times, and a scattering of larger DNS response times. In our graph, most times are very small, likely because the correct answer is cached by the local nameserver. In some cases, however, there is a longer delay of hundreds of milliseconds as remote nameservers must be queried. You can click a point on the graph to be taken to the nearest point in the trace if there is a feature you would like to investigate.

![Image of Wireshark DNS statistics]

If you look over the DNS traffic caused by your browser, you are likely to see a greater range of behaviors than in the DNS traffic caused by the `dig` commands. This behavior might include new types of records, such as CNAME (canonical name, to provide information about aliases when one machine is known by multiple names), answers that indicate that a name does not exist, and so forth.