Lab Exercise – DNS

Objective

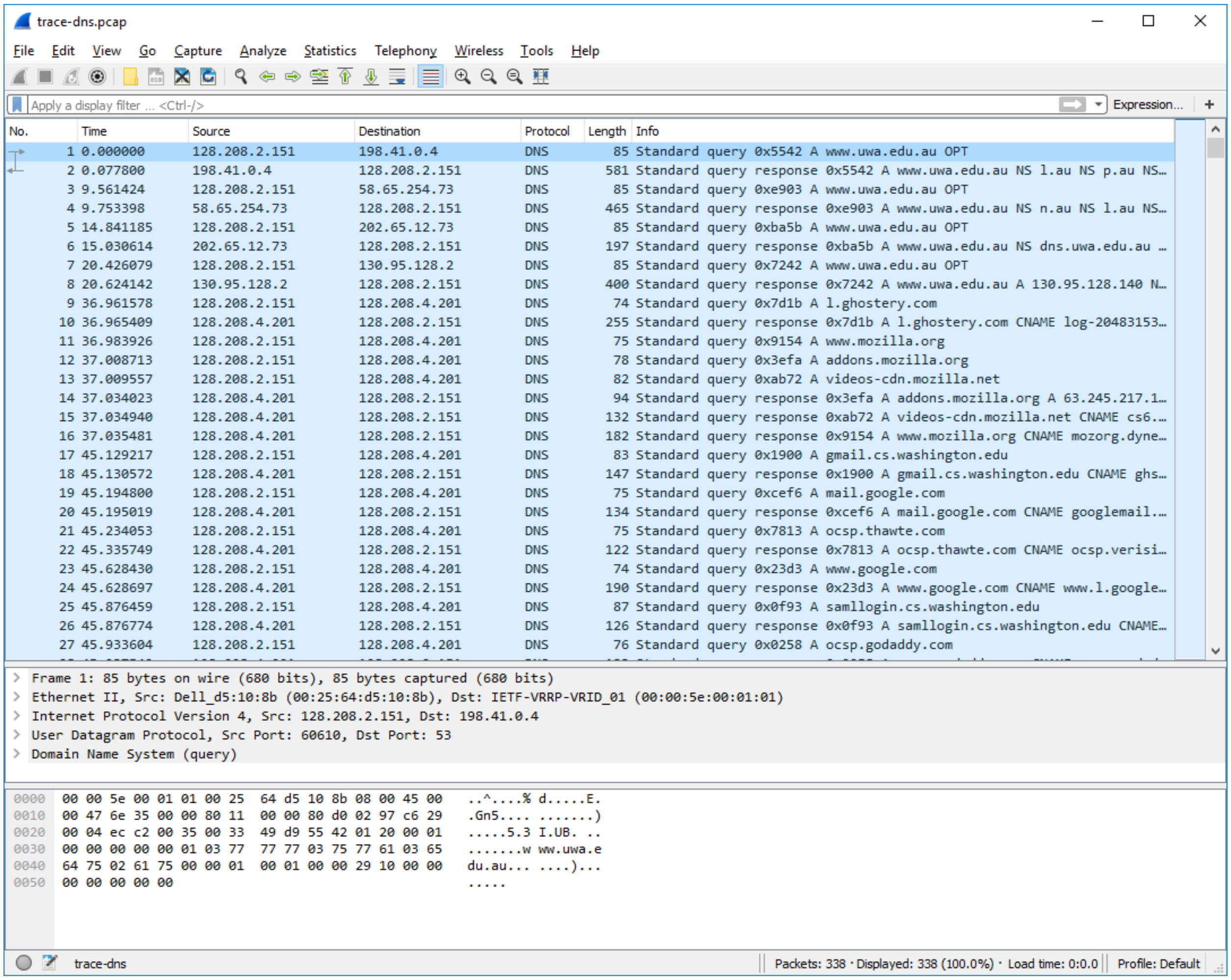
DNS (Domain Name System) is the system & protocol that translates domain names to IP addresses.

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://kevincurran.org/com320/labs/wireshark/trace-dns.pcap

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


trace-dns.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
trace-dns
Packets: 338 · Displayed: 338 (100.0%) · Load time: 0:0.0
Profile: Default

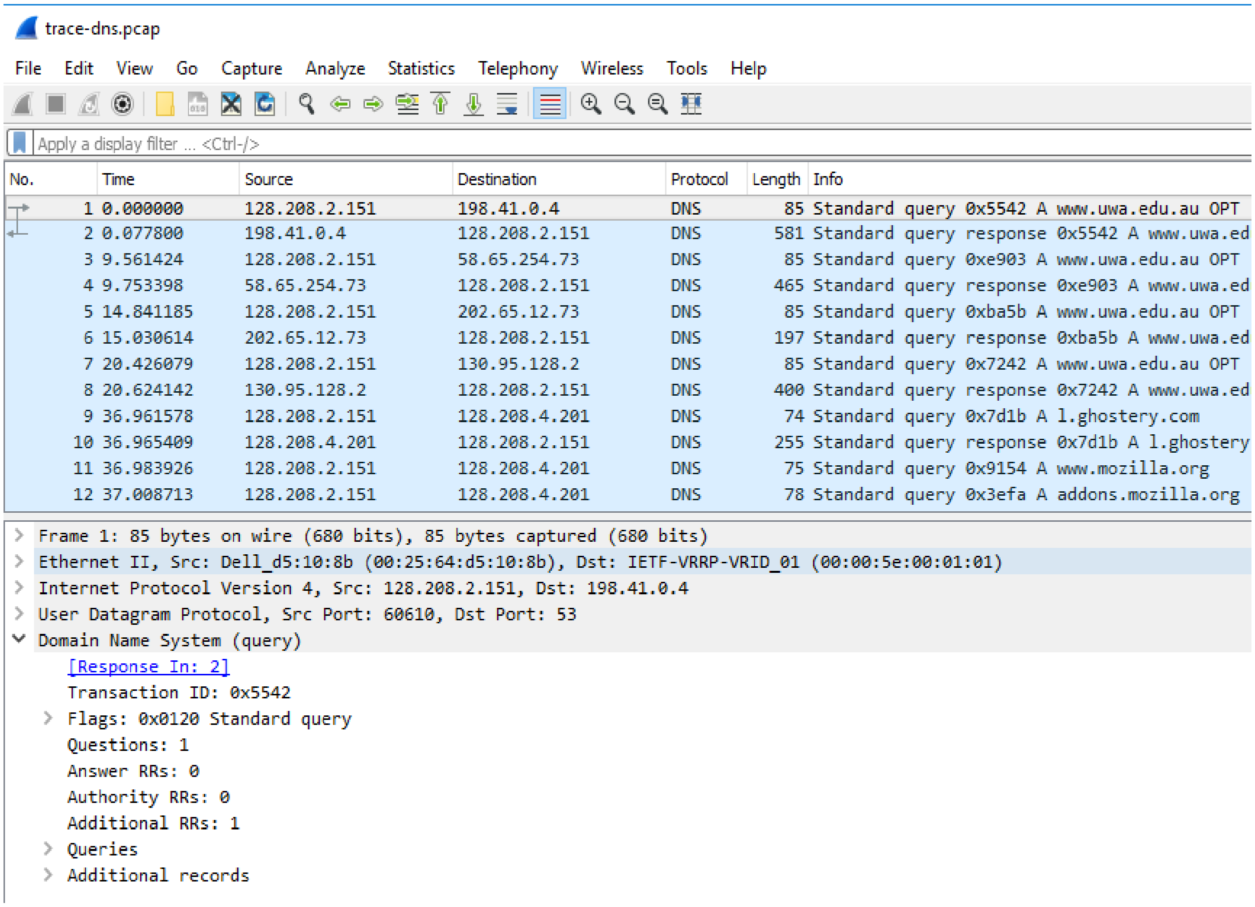
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	128.208.2.151	198.41.0.4	DNS	85	Standard query 0x5542 A www.uwa.edu.au OPT
2	0.077800	198.41.0.4	128.208.2.151	DNS	581	Standard query response 0x5542 A www.uwa.edu.au NS l.au NS p.au NS…
3	9.561424	128.208.2.151	58.65.254.73	DNS	85	Standard query 0xe903 A www.uwa.edu.au OPT
4	9.753398	58.65.254.73	128.208.2.151	DNS	465	Standard query response 0xe903 A www.uwa.edu.au NS n.au NS l.au NS…
5	14.841185	128.208.2.151	202.65.12.73	DNS	85	Standard query 0xba5b A www.uwa.edu.au OPT
6	15.030614	202.65.12.73	128.208.2.151	DNS	197	Standard query response 0xba5b A www.uwa.edu.au NS dns.uwa.edu.au …
7	20.426079	128.208.2.151	130.95.128.2	DNS	85	Standard query 0x7242 A www.uwa.edu.au OPT
8	20.624142	130.95.128.2	128.208.2.151	DNS	400	Standard query response 0x7242 A www.uwa.edu.au A 130.95.128.140 N…
9	36.961578	128.208.2.151	128.208.4.201	DNS	74	Standard query 0x7d1b A l.ghostery.com
10	36.965409	128.208.4.201	128.208.2.151	DNS	255	Standard query response 0x7d1b A l.ghostery.com CNAME log-20483153…
11	36.983926	128.208.2.151	128.208.4.201	DNS	75	Standard query 0x9154 A www.mozilla.org
12	37.008713	128.208.2.151	128.208.4.201	DNS	78	Standard query 0x3efa A addons.mozilla.org
13	37.009557	128.208.2.151	128.208.4.201	DNS	82	Standard query 0xab72 A videos-cdn.mozilla.net
14	37.034023	128.208.4.201	128.208.2.151	DNS	94	Standard query response 0x3efa A addons.mozilla.org A 63.245.217.1…
15	37.034940	128.208.4.201	128.208.2.151	DNS	132	Standard query response 0xab72 A videos-cdn.mozilla.net CNAME cs6.…
16	37.035481	128.208.4.201	128.208.2.151	DNS	182	Standard query response 0x9154 A www.mozilla.org CNAME mozorg.dyne…
17	45.129217	128.208.2.151	128.208.4.201	DNS	83	Standard query 0x1900 A gmail.cs.washington.edu
18	45.130572	128.208.4.201	128.208.2.151	DNS	147	Standard query response 0x1900 A gmail.cs.washington.edu CNAME ghs…
19	45.194800	128.208.2.151	128.208.4.201	DNS	75	Standard query 0xcef6 A mail.google.com
20	45.195019	128.208.4.201	128.208.2.151	DNS	134	Standard query response 0xcef6 A mail.google.com CNAME googlemail.…
21	45.234053	128.208.2.151	128.208.4.201	DNS	75	Standard query 0x7813 A ocsp.thawte.com
22	45.335749	128.208.4.201	128.208.2.151	DNS	122	Standard query response 0x7813 A ocsp.thawte.com CNAME ocsp.verisi…
23	45.628430	128.208.2.151	128.208.4.201	DNS	74	Standard query 0x23d3 A www.google.com
24	45.628697	128.208.4.201	128.208.2.151	DNS	190	Standard query response 0x23d3 A www.google.com CNAME www.l.google…
25	45.876459	128.208.2.151	128.208.4.201	DNS	87	Standard query 0x0f93 A samllogin.cs.washington.edu
26	45.876774	128.208.4.201	128.208.2.151	DNS	126	Standard query response 0x0f93 A samllogin.cs.washington.edu CNAME…
27	45.933604	128.208.2.151	128.208.4.201	DNS	76	Standard query 0x0258 A ocsp.godaddy.com

```
> Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits)
> Ethernet II, Src: Dell_d5:10:8b (00:25:64:d5:10:8b), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 128.208.2.151, Dst: 198.41.0.4
> User Datagram Protocol, Src Port: 60610, Dst Port: 53
> Domain Name System (query)
```

```
0000  00 00 5e 00 01 01 00 25  64 d5 10 8b 08 00 45 00   ..^....% d.....E.
0010  00 47 6e 35 00 00 80 11  00 00 80 d0 02 97 c6 29   .Gn5.... .......)
0020  00 04 ec c2 00 35 00 33  49 d9 55 42 01 20 00 01   .....5.3 I.UB. ..
0030  00 00 00 00 00 01 03 77  77 77 03 75 77 61 03 65   .......w ww.uwa.e
0040  64 75 02 61 75 00 00 01  00 01 00 00 29 10 00 00   du.au... ....)...
0050  00 00 00 00 00                                     .....
```

Figure 3: DNS traffic

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.



```
No.  Time       Source         Destination    Protocol Length Info
   1 0.000000   128.208.2.151  198.41.0.4     DNS        85 Standard query 0x5542 A www.uwa.edu.au OPT
   2 0.077800   198.41.0.4     128.208.2.151  DNS       581 Standard query response 0x5542 A www.uwa.ed
   3 9.561424   128.208.2.151  58.65.254.73   DNS        85 Standard query 0xe903 A www.uwa.edu.au OPT
   4 9.753398   58.65.254.73   128.208.2.151  DNS       465 Standard query response 0xe903 A www.uwa.ed
   5 14.841185  128.208.2.151  202.65.12.73   DNS        85 Standard query 0xba5b A www.uwa.edu.au OPT
   6 15.030614  202.65.12.73   128.208.2.151  DNS       197 Standard query response 0xba5b A www.uwa.ed
   7 20.426079  128.208.2.151  130.95.128.2   DNS        85 Standard query 0x7242 A www.uwa.edu.au OPT
   8 20.624142  130.95.128.2   128.208.2.151  DNS       400 Standard query response 0x7242 A www.uwa.ed
   9 36.961578  128.208.2.151  128.208.4.201  DNS        74 Standard query 0x7d1b A l.ghostery.com
  10 36.965409  128.208.4.201  128.208.2.151  DNS       255 Standard query response 0x7d1b A l.ghostery
  11 36.983926  128.208.2.151  128.208.4.201  DNS        75 Standard query 0x9154 A www.mozilla.org
  12 37.008713  128.208.2.151  128.208.4.201  DNS        78 Standard query 0x3efa A addons.mozilla.org
```

```
> Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits)
> Ethernet II, Src: Dell_d5:10:8b (00:25:64:d5:10:8b), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
> Internet Protocol Version 4, Src: 128.208.2.151, Dst: 198.41.0.4
> User Datagram Protocol, Src Port: 60610, Dst Port: 53
v Domain Name System (query)
    [Response In: 2]
    Transaction ID: 0x5542
  > Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  > Queries
  > Additional records
```

Figure 1: Trace of DNS traffic showing the details of the DNS header

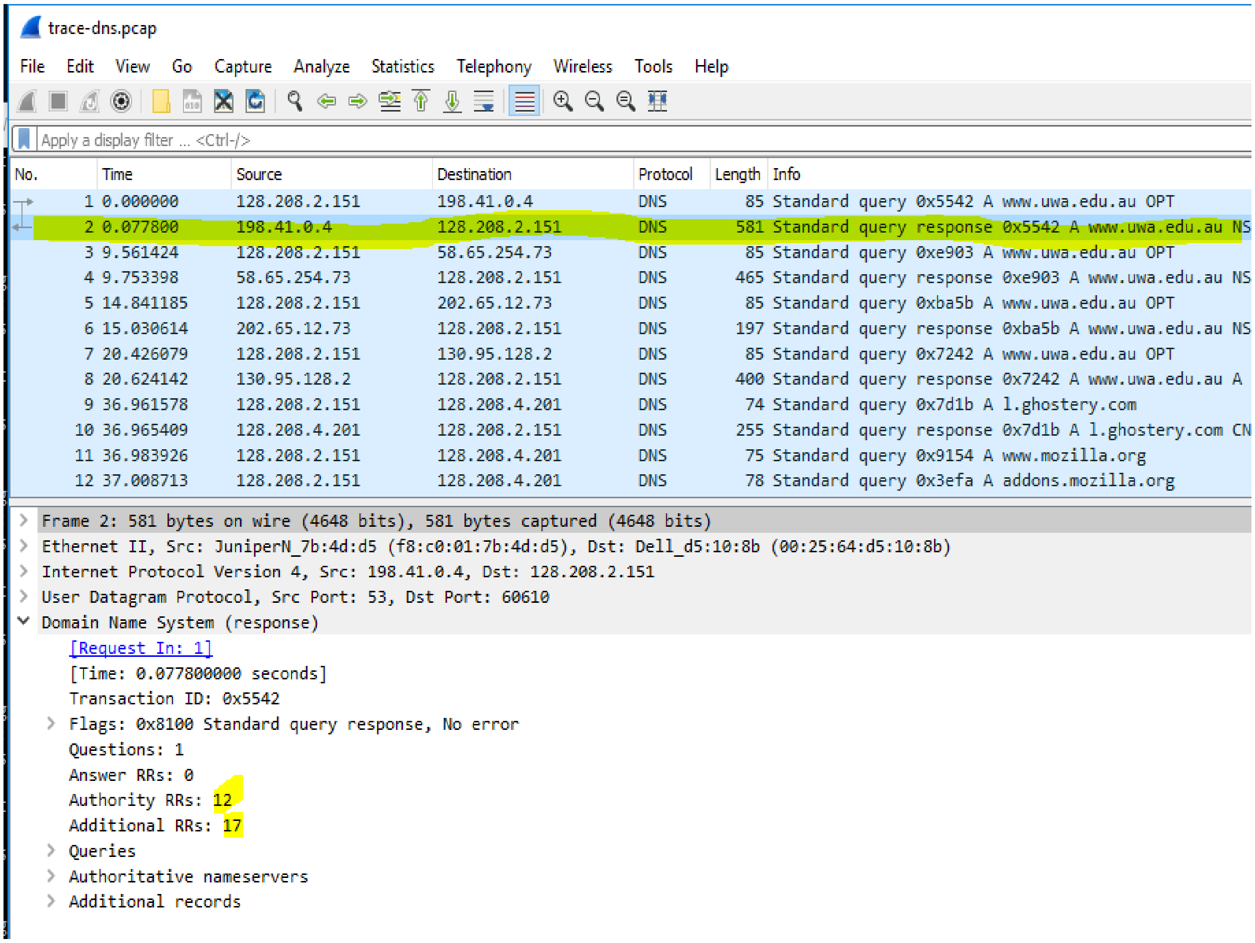
Look for the following details:

- 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.)


trace-dns.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source          Destination     Protocol  Length  Info
    1 0.000000    128.208.2.151   198.41.0.4      DNS         85 Standard query 0x5542 A www.uwa.edu.au OPT
    2 0.077800    198.41.0.4      128.208.2.151   DNS        581 Standard query response 0x5542 A www.uwa.edu.au NS
    3 9.561424    128.208.2.151   58.65.254.73    DNS         85 Standard query 0xe903 A www.uwa.edu.au OPT
    4 9.753398    58.65.254.73    128.208.2.151   DNS        465 Standard query response 0xe903 A www.uwa.edu.au NS
    5 14.841185   128.208.2.151   202.65.12.73    DNS         85 Standard query 0xba5b A www.uwa.edu.au OPT
    6 15.030614   202.65.12.73    128.208.2.151   DNS        197 Standard query response 0xba5b A www.uwa.edu.au NS
    7 20.426079   128.208.2.151   130.95.128.2    DNS         85 Standard query 0x7242 A www.uwa.edu.au OPT
    8 20.624142   130.95.128.2    128.208.2.151   DNS        400 Standard query response 0x7242 A www.uwa.edu.au A
    9 36.961578   128.208.2.151   128.208.4.201   DNS         74 Standard query 0x7d1b A l.ghostery.com
   10 36.965409   128.208.4.201   128.208.2.151   DNS        255 Standard query response 0x7d1b A l.ghostery.com CN
   11 36.983926   128.208.2.151   128.208.4.201   DNS         75 Standard query 0x9154 A www.mozilla.org
   12 37.008713   128.208.2.151   128.208.4.201   DNS         78 Standard query 0x3efa A addons.mozilla.org
```

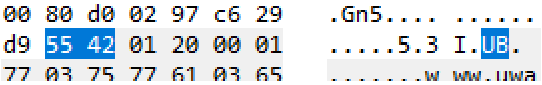
```
> Frame 2: 581 bytes on wire (4648 bits), 581 bytes captured (4648 bits)
> Ethernet II, Src: JuniperN_7b:4d:d5 (f8:c0:01:7b:4d:d5), Dst: Dell_d5:10:8b (00:25:64:d5:10:8b)
> Internet Protocol Version 4, Src: 198.41.0.4, Dst: 128.208.2.151
> User Datagram Protocol, Src Port: 53, Dst Port: 60610
v Domain Name System (response)
    [Request In: 1]
    [Time: 0.077800000 seconds]
    Transaction ID: 0x5542
  > Flags: 0x8100 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 12
    Additional RRs: 17
  > Queries
  > Authoritative nameservers
  > Additional records
```

Figure 2: First DNS response – packet #2

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.

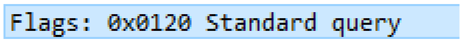
The Transaction ID is 16 bits long, which makes collisions unlikely.



```
00 80 d0 02 97 c6 29   .Gn5.... ......
d9 55 42 01 20 00 01   .....5.3 I.UB.
77 03 75 77 61 03 65   .......w ww.uwa
```

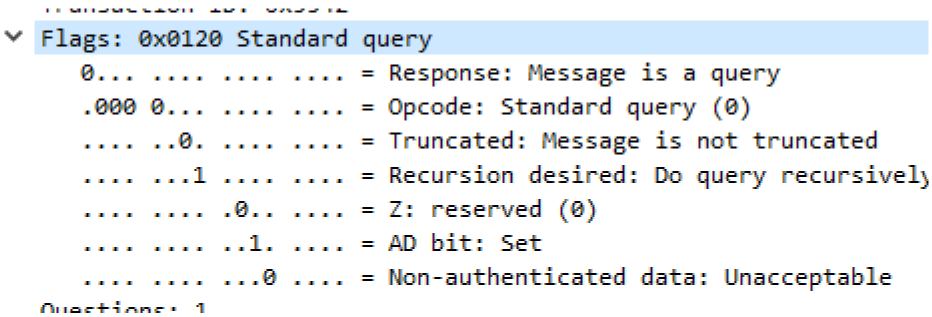
Since the host computer is setting this value, it can use all 2^16 choices before repeating. This means that 2^16 query/response pairs would need to be outstanding at the same time to cause a collision. For a normal computer, this is an extremely or implausibly high DNS workload.

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



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

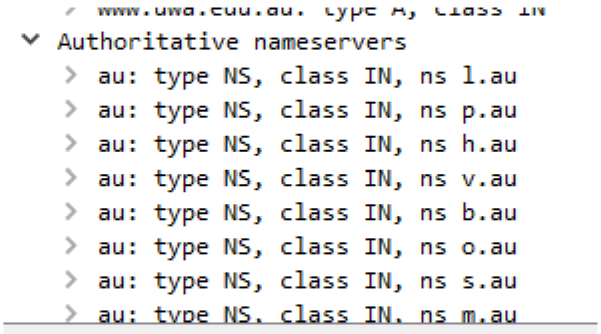
The DNS header is 12 bytes long.



```
Transaction ID: 0x5542
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
```

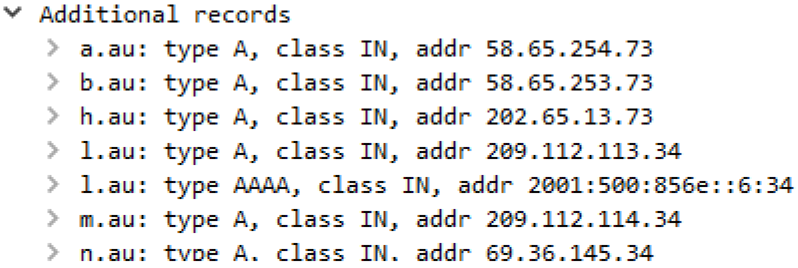
The initial response should have provided another nameserver one step closer to the nameserver, but not the final answer. You will find that it includes the original query in its Query section. It will also include records with both the name of the nameservers to contact next, and the IP addresses of 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.



```
  > www.uwa.edu.au: type A, class IN
v Authoritative nameservers
  > au: type NS, class IN, ns l.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.



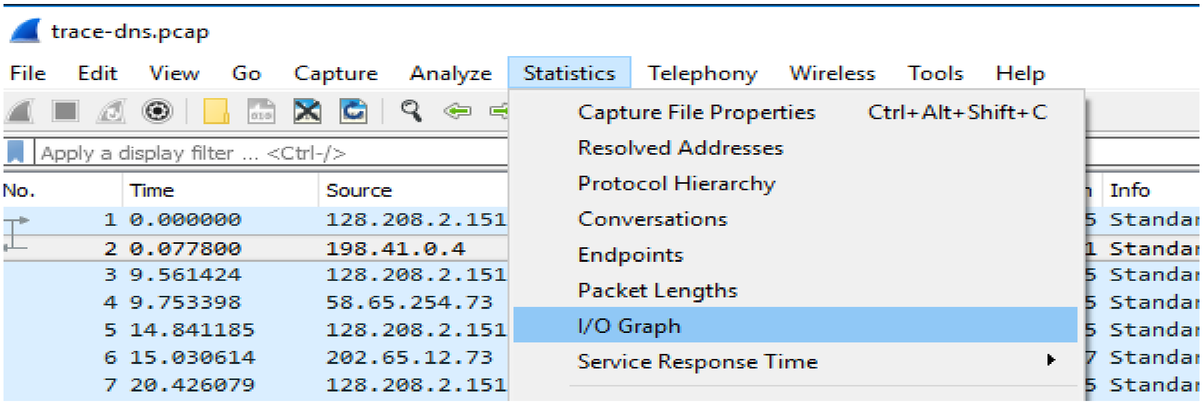
```
v Additional records
  > a.au: type A, class IN, addr 58.65.254.73
  > b.au: type A, class IN, addr 58.65.253.73
  > h.au: type A, class IN, addr 202.65.13.73
  > l.au: type A, class IN, addr 209.112.113.34
  > l.au: type AAAA, class IN, addr 2001:500:856e::6:34
  > m.au: type A, class IN, addr 209.112.114.34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

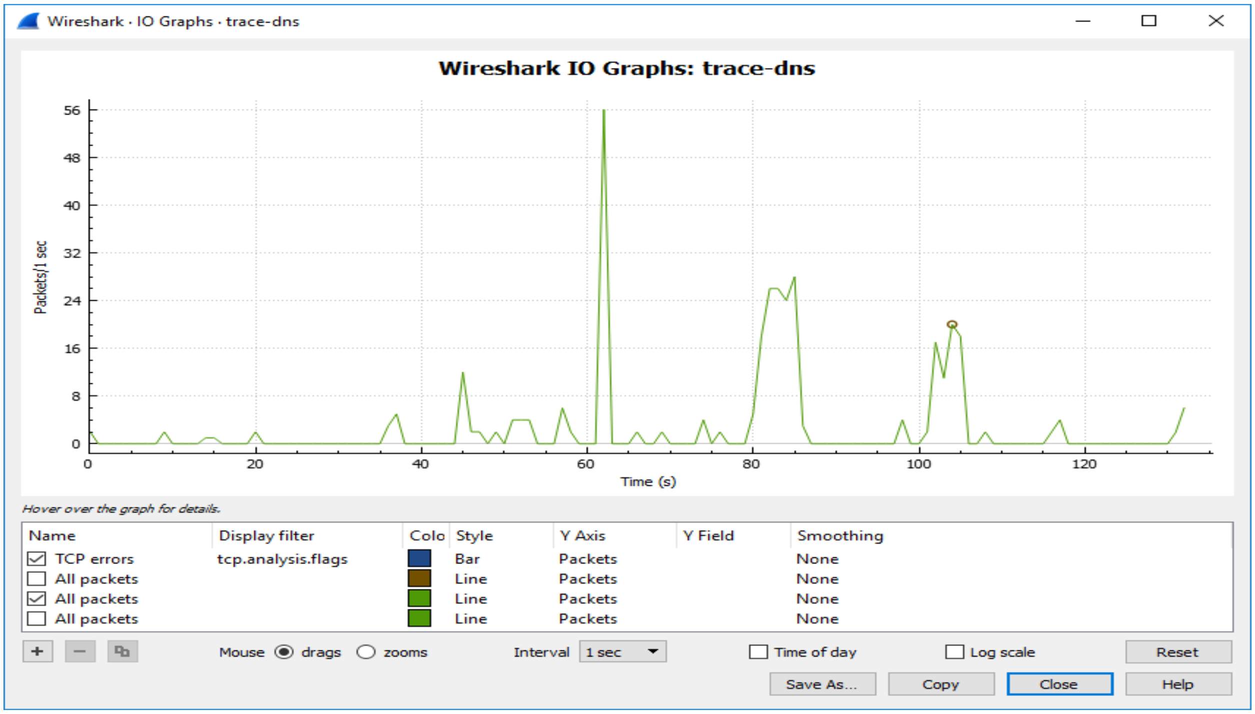
To conclude this lab, we will look at the DNS response time of the DNS queries. This is a normal DNS usage, in which a computer sends a single query and receives the answer in the response. The response time is the delay between when the computer sends the query to the local nameserver and when it receives 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.



No.	Time	Source	Info
1	0.000000	128.208.2.151	Standar
2	0.077800	198.41.0.4	Standar
3	9.561424	128.208.2.151	Standar
4	9.753398	58.65.254.73	Standar
5	14.841185	128.208.2.151	Standar
6	15.030614	202.65.12.73	Standar
7	20.426079	128.208.2.151	Standar

By default, this graph shows the rate of packets over time (See below)

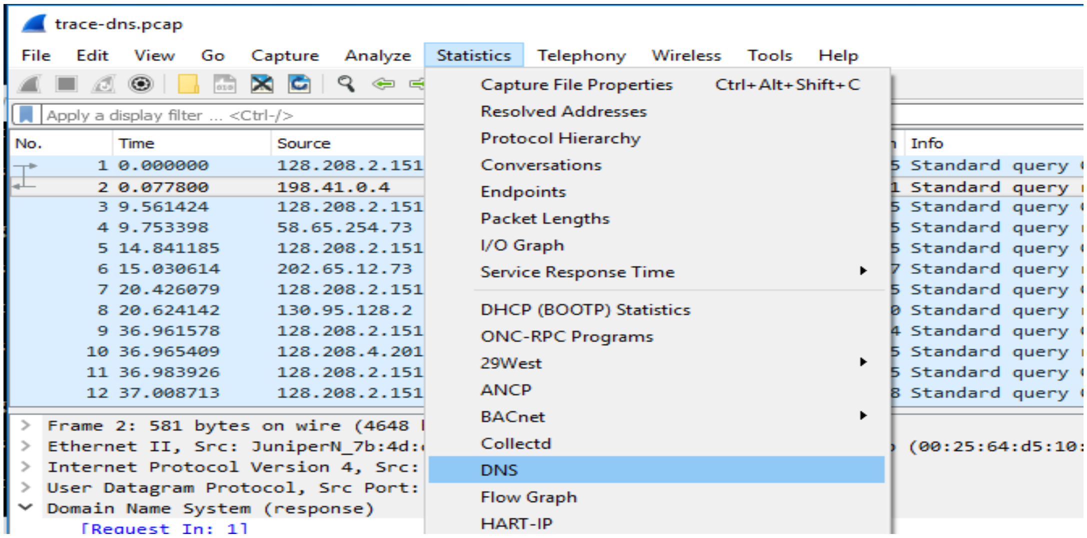


Hover over the graph for details.

Name	Display filter	Colo	Style	Y Axis	Y Field	Smoothing
☑ TCP errors	tcp.analysis.flags	🟦	Bar	Packets		None
☐ All packets		🟫	Line	Packets		None
☑ All packets		🟩	Line	Packets		None
☐ All packets		🟩	Line	Packets		None

Mouse ● drags ○ zooms Interval 1 sec ☐ Time of day ☐ Log scale

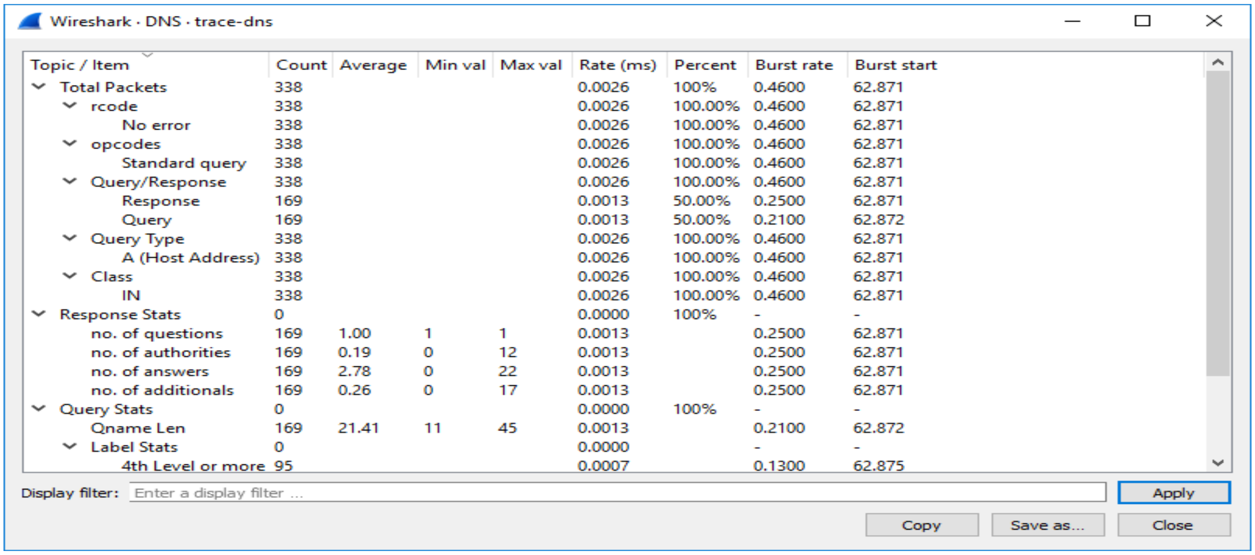
We can also choose Statistics → DNS as shown below.



No.	Time	Source	Info
1	0.000000	128.208.2.151	Standard query
2	0.077800	198.41.0.4	Standard query
3	9.561424	128.208.2.151	Standard query
4	9.753398	58.65.254.73	Standard query
5	14.841185	128.208.2.151	Standard query
6	15.030614	202.65.12.73	Standard query
7	20.426079	128.208.2.151	Standard query
8	20.624142	130.95.128.2	Standard query
9	36.961578	128.208.2.151	Standard query
10	36.965409	128.208.4.201	Standard query
11	36.983926	128.208.2.151	Standard query
12	37.008713	128.208.2.151	Standard query

```
> Frame 2: 581 bytes on wire (4648 
> Ethernet II, Src: JuniperN_7b:4d:                    (00:25:64:d5:10:
> Internet Protocol Version 4, Src:
> User Datagram Protocol, Src Port:
v Domain Name System (response)
     [Request In: 1]
```

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.



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Total Packets	338				0.0026	100%	0.4600	62.871
rcode	338				0.0026	100.00%	0.4600	62.871
No error	338				0.0026	100.00%	0.4600	62.871
opcodes	338				0.0026	100.00%	0.4600	62.871
Standard query	338				0.0026	100.00%	0.4600	62.871
Query/Response	338				0.0026	100.00%	0.4600	62.871
Response	169				0.0013	50.00%	0.2500	62.871
Query	169				0.0013	50.00%	0.2100	62.872
Query Type	338				0.0026	100.00%	0.4600	62.871
A (Host Address)	338				0.0026	100.00%	0.4600	62.871
Class	338				0.0026	100.00%	0.4600	62.871
IN	338				0.0026	100.00%	0.4600	62.871
Response Stats	0				0.0000	100%	-	-
no. of questions	169	1.00	1	1	0.0013		0.2500	62.871
no. of authorities	169	0.19	0	12	0.0013		0.2500	62.871
no. of answers	169	2.78	0	22	0.0013		0.2500	62.871
no. of additionals	169	0.26	0	17	0.0013		0.2500	62.871
Query Stats	0				0.0000	100%	-	-
Qname Len	169	21.41	11	45	0.0013		0.2100	62.872
Label Stats	0				0.0000		-	-
4th Level or more	95				0.0007		0.1300	62.875

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.