

Lab-3

1. Perform nslookup to obtain the IP address for some Australian university

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

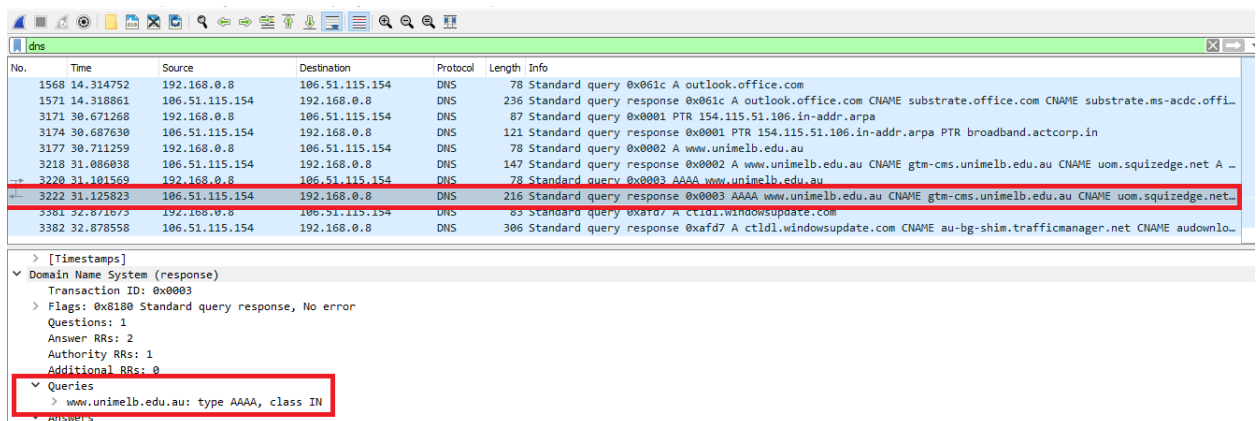
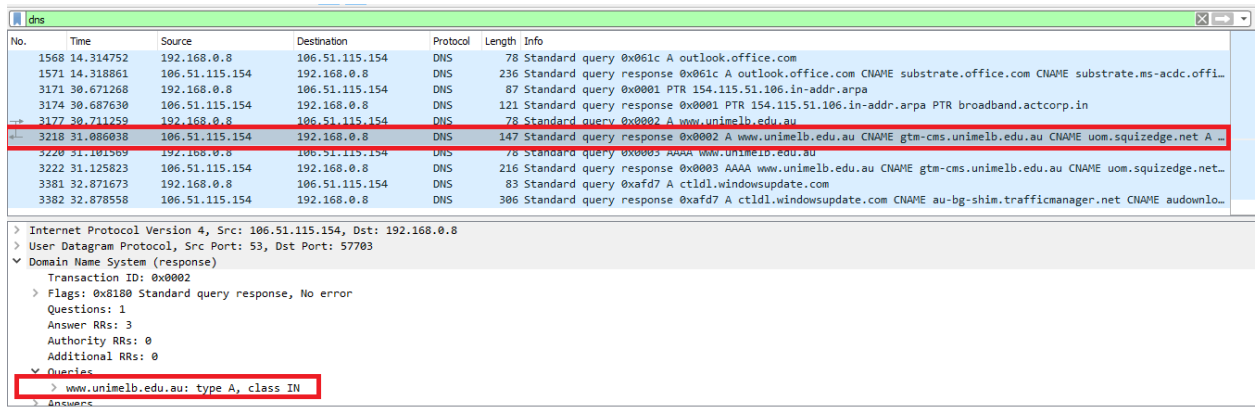
Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\Users\gurus> nslookup www.unimelb.edu.au
Server: broadband.actcorp.in
Address: 106.51.115.154

Non-authoritative answer:
Name: www.unimelb.edu.au
Address: 202.9.95.188
Aliases: www.unimelb.edu.au
          gtm-cms.unimelb.edu.au

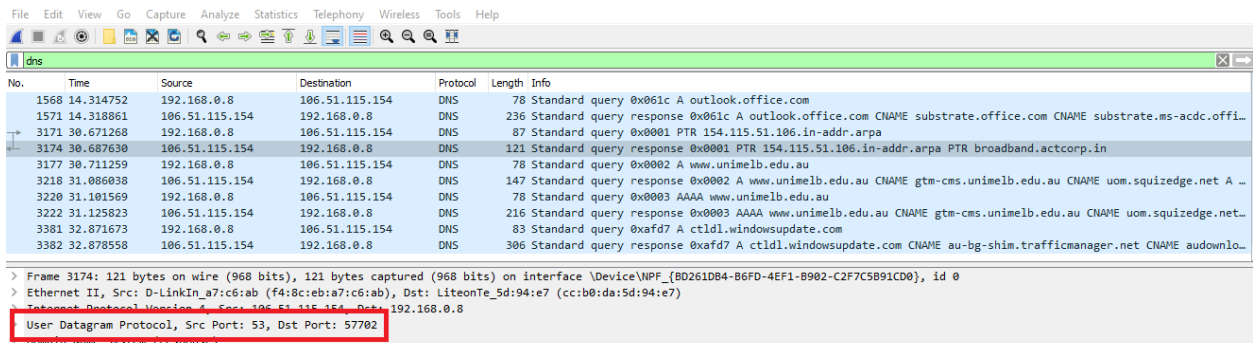
PS C:\Users\gurus>
```

2. Locate the DNS query and response in wireshark



3. Does it use TCP or UDP?

It uses UDP.



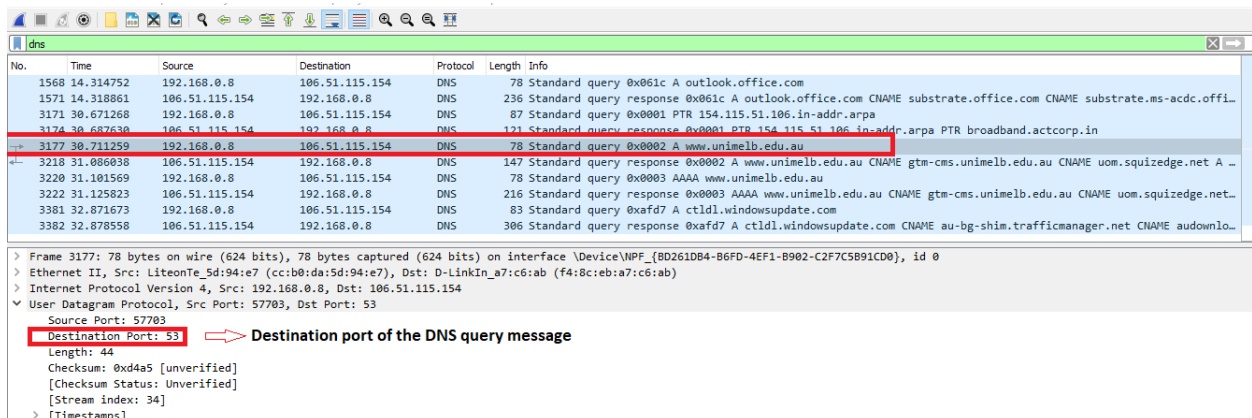
No.	Time	Source	Destination	Protocol	Length	Info
1568	14.314752	192.168.0.8	106.51.115.154	DNS	78	Standard query 0x061c A outlook.office.com
1571	14.318861	106.51.115.154	192.168.0.8	DNS	236	Standard query response 0x061c A outlook.office.com CNAME substrate.office.com CNAME substrate.ms-acdc.offi...
3171	30.671268	192.168.0.8	106.51.115.154	DNS	87	Standard query 0x0001 PTR 154.115.51.106.in-addr.arpa
3174	30.687630	106.51.115.154	192.168.0.8	DNS	121	Standard query response 0x0001 PTR 154.115.51.106.in-addr.arpa PTR broadband.actcorp.in
3177	30.711259	192.168.0.8	106.51.115.154	DNS	78	Standard query 0x0002 A www.unimelb.edu.au
3218	31.086038	106.51.115.154	192.168.0.8	DNS	147	Standard query response 0x0002 A www.unimelb.edu.au CNAME gtm-cms.unimelb.edu.au CNAME uom.squizedge.net A ...
3220	31.101569	192.168.0.8	106.51.115.154	DNS	78	Standard query 0x0003 AAAA www.unimelb.edu.au
3222	31.125823	106.51.115.154	192.168.0.8	DNS	216	Standard query response 0x0003 AAAA www.unimelb.edu.au CNAME gtm-cms.unimelb.edu.au CNAME uom.squizedge.net...
3381	32.871673	192.168.0.8	106.51.115.154	DNS	83	Standard query 0xafd7 A ctldl.windowsupdate.com
3382	32.878558	106.51.115.154	192.168.0.8	DNS	306	Standard query response 0xafd7 A ctldl.windowsupdate.com CNAME au-bg-shim.trafficmanager.net CNAME audownlo...

> Frame 3174: 121 bytes on wire (968 bits), 121 bytes captured (968 bits) on interface \Device\NPF_{BD261DB4-B6FD-4EF1-B902-C2F7C5B91CD0}, id 0
> Ethernet II, Src: D-LinkIn_a7:c6:ab (f4:8c:eb:a7:c6:ab), Dst: LiteonTe_5d:94:e7 (cc:b0:da:5d:94:e7)
> Internet Protocol Version 4, Src: 106.51.115.154, Dst: 192.168.0.8
User Datagram Protocol, Src Port: 57702, Dst Port: 57702
Domain Name System (Response)

4. What is the destination port for the DNS query message and source port of the DNS response message?

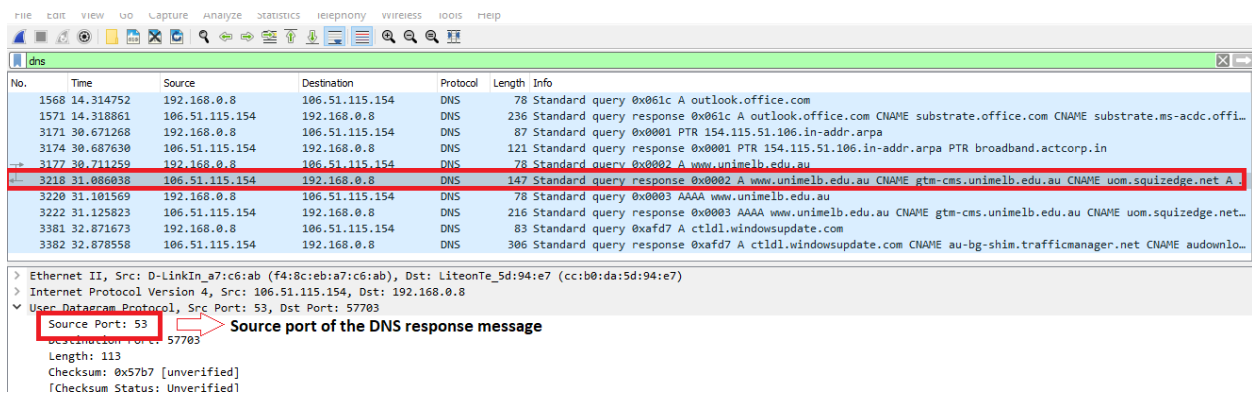
The destination port of the DNS query message is 53

The source port of the DNS response message is 53



No.	Time	Source	Destination	Protocol	Length	Info
1568	14.314752	192.168.0.8	106.51.115.154	DNS	78	Standard query 0x061c A outlook.office.com
1571	14.318861	106.51.115.154	192.168.0.8	DNS	236	Standard query response 0x061c A outlook.office.com CNAME substrate.office.com CNAME substrate.ms-acdc.offi...
3171	30.671268	192.168.0.8	106.51.115.154	DNS	87	Standard query 0x0001 PTR 154.115.51.106.in-addr.arpa
3174	30.687630	106.51.115.154	192.168.0.8	DNS	121	Standard query response 0x0001 PTR 154.115.51.106.in-addr.arpa PTR broadband.actcorp.in
3177	30.711259	192.168.0.8	106.51.115.154	DNS	78	Standard query 0x0002 A www.unimelb.edu.au
3218	31.086038	106.51.115.154	192.168.0.8	DNS	147	Standard query response 0x0002 A www.unimelb.edu.au CNAME gtm-cms.unimelb.edu.au CNAME uom.squizedge.net A ...
3220	31.101569	192.168.0.8	106.51.115.154	DNS	78	Standard query 0x0003 AAAA www.unimelb.edu.au
3222	31.125823	106.51.115.154	192.168.0.8	DNS	216	Standard query response 0x0003 AAAA www.unimelb.edu.au CNAME gtm-cms.unimelb.edu.au CNAME uom.squizedge.net...
3381	32.871673	192.168.0.8	106.51.115.154	DNS	83	Standard query 0xafd7 A ctldl.windowsupdate.com
3382	32.878558	106.51.115.154	192.168.0.8	DNS	306	Standard query response 0xafd7 A ctldl.windowsupdate.com CNAME au-bg-shim.trafficmanager.net CNAME audownlo...

> Frame 3177: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{BD261DB4-B6FD-4EF1-B902-C2F7C5B91CD0}, id 0
> Ethernet II, Src: LiteonTe_5d:94:e7 (cc:b0:da:5d:94:e7), Dst: D-LinkIn_a7:c6:ab (f4:8c:eb:a7:c6:ab)
> Internet Protocol Version 4, Src: 192.168.0.8, Dst: 106.51.115.154
User Datagram Protocol, Src Port: 57703, Dst Port: 53
Source Port: 57703
Destination Port: 53
Length: 44
Checksum: 0x4a5 [unverified]
[Checksum Status: Unverified]
[Stream Index: 34]
> [Timestamps]



No.	Time	Source	Destination	Protocol	Length	Info
1568	14.314752	192.168.0.8	106.51.115.154	DNS	78	Standard query 0x061c A outlook.office.com
1571	14.318861	106.51.115.154	192.168.0.8	DNS	236	Standard query response 0x061c A outlook.office.com CNAME substrate.office.com CNAME substrate.ms-acdc.offi...
3171	30.671268	192.168.0.8	106.51.115.154	DNS	87	Standard query 0x0001 PTR 154.115.51.106.in-addr.arpa
3174	30.687630	106.51.115.154	192.168.0.8	DNS	121	Standard query response 0x0001 PTR 154.115.51.106.in-addr.arpa PTR broadband.actcorp.in
3177	30.711259	192.168.0.8	106.51.115.154	DNS	78	Standard query 0x0002 A www.unimelb.edu.au
3218	31.086038	106.51.115.154	192.168.0.8	DNS	147	Standard query response 0x0002 A www.unimelb.edu.au CNAME gtm-cms.unimelb.edu.au CNAME uom.squizedge.net A ...
3220	31.101569	192.168.0.8	106.51.115.154	DNS	78	Standard query 0x0003 AAAA www.unimelb.edu.au
3222	31.125823	106.51.115.154	192.168.0.8	DNS	216	Standard query response 0x0003 AAAA www.unimelb.edu.au CNAME gtm-cms.unimelb.edu.au CNAME uom.squizedge.net...
3381	32.871673	192.168.0.8	106.51.115.154	DNS	83	Standard query 0xafd7 A ctldl.windowsupdate.com
3382	32.878558	106.51.115.154	192.168.0.8	DNS	306	Standard query response 0xafd7 A ctldl.windowsupdate.com CNAME au-bg-shim.trafficmanager.net CNAME audownlo...

> Ethernet II, Src: D-LinkIn_a7:c6:ab (f4:8c:eb:a7:c6:ab), Dst: LiteonTe_5d:94:e7 (cc:b0:da:5d:94:e7)
> Internet Protocol Version 4, Src: 106.51.115.154, Dst: 192.168.0.8
User Datagram Protocol, Src Port: 53, Dst Port: 57703
Source Port: 53
Destination Port: 57703
Length: 113
Checksum: 0x57b7 [unverified]
[Checksum Status: Unverified]