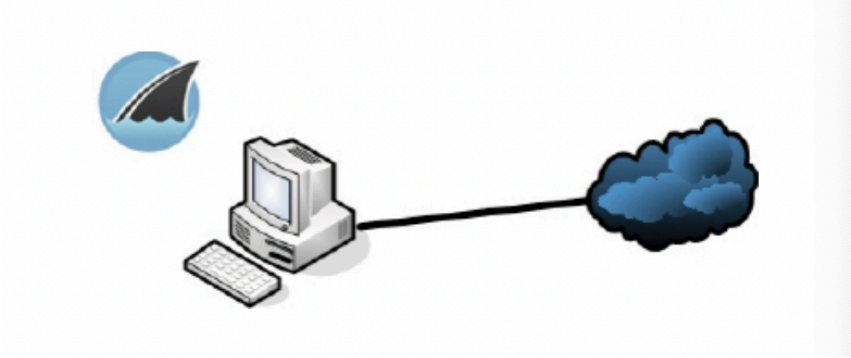
Lab 7. UDP

Lab Objective:
Learn how to recognize a TCP packet.

Lab Purpose:
UDP is used by many services and protocols, such as RIP, DNS, SNMP, and DHCP, and routing protocols, such as RIP.
It offers low overhead but with no guarantee of delivery.
There are no acknowledgements: the packets are numbered and sent, but that's it.

Lab Tool:
Wireshark
Putty
Google

Lab Topology:
Run Wireshark.
You need to be able to get out to the internet because we will be checking for a DNS lookup for a website.

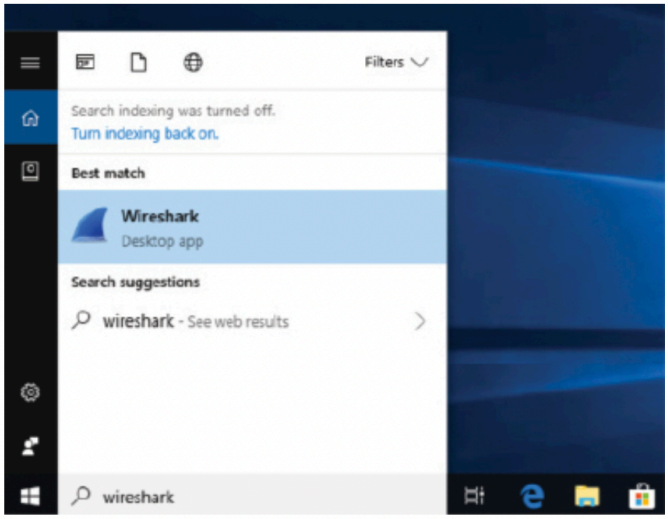


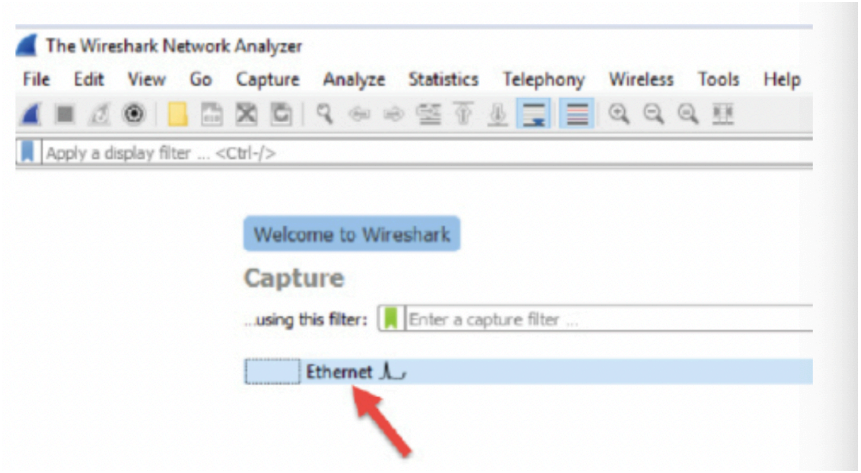
Lab Walkthrough::

Task 1:
Install Wireshark if not yet installed.

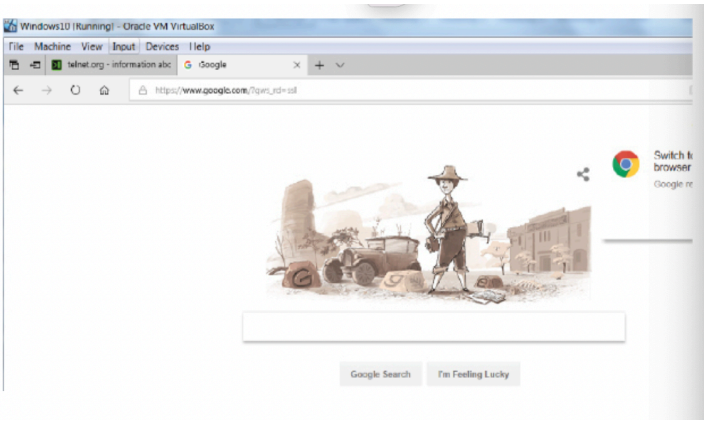
Task 2:
Open a web browser, but don't input any URL yet.

Task 3:
Boot Wireshark on your PC and check the correct interface is the one being monitored. Click on the interface name to open the capture window.
Note that mine says "Ethernet", but your device configuration and hardware will differ and so you may see "En0", "WiFi", or something else.

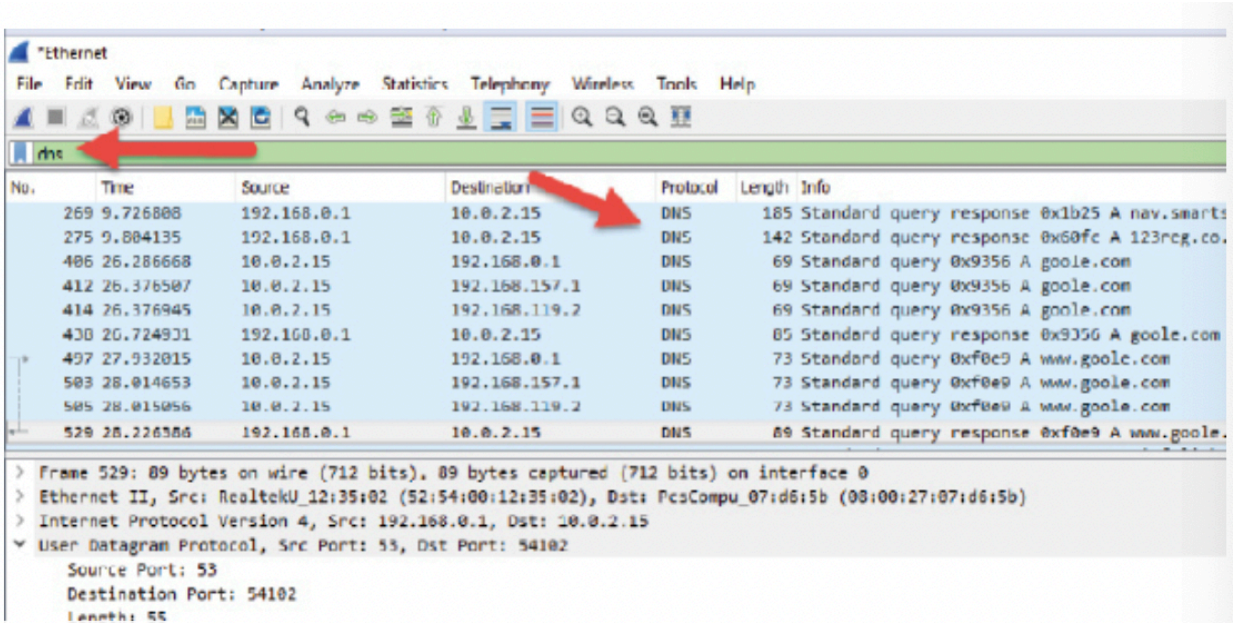




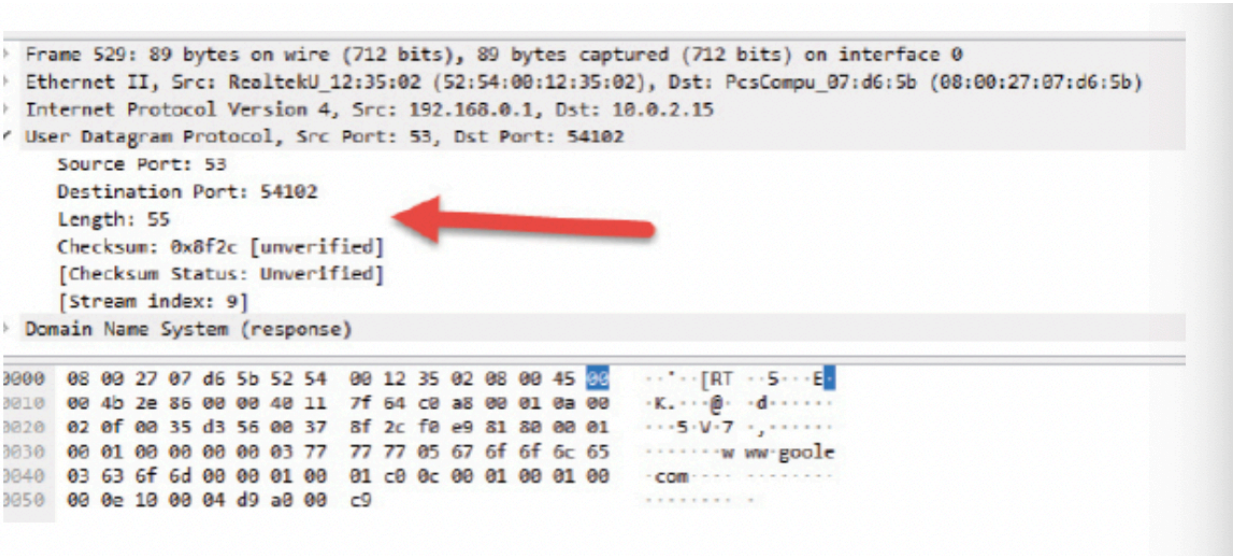
Task 4:
Browse to a website which isn't in your local cache. You want to prompt a DNS lookup (because it used UDP). I've never used this virtual machine, so any URL will work for me because my DNS cache is empty. - There will have to be a name lookup performed (generating traffic on Wireshark).



Task 5:
Go to Wireshark. Stop the captures by pressing the red square. Then use the filter bar to search for DNS. For some reason, you have to use lowercase for the search.

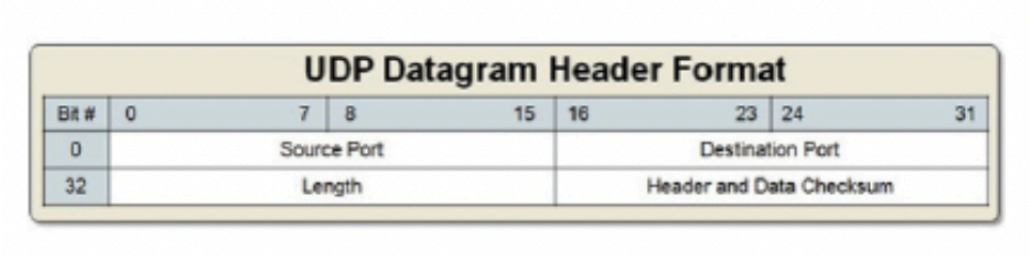


Task 6:
Click on one for the DNS entries and drill into the packet capture. Check the entries against the UDP image below.
Note that we are missing many of the TCP fields, such as sequence number and flags.



Task 7:
UDP does have a checksum for error checking, but that's about it. Check the above packet capture for the checksum fields.

Task 8:
You can use the below image as a reference to check the UDP fields.



UDP Datagram Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	

Note: Some protocols, such as DNS, will use UDP to start but then move to TCP if there is no response or for zone transfers, so bear that in mind.