**Lab 8. ICMP**

**Lab Objective:**

Learn how to recognize an ICMP packet.

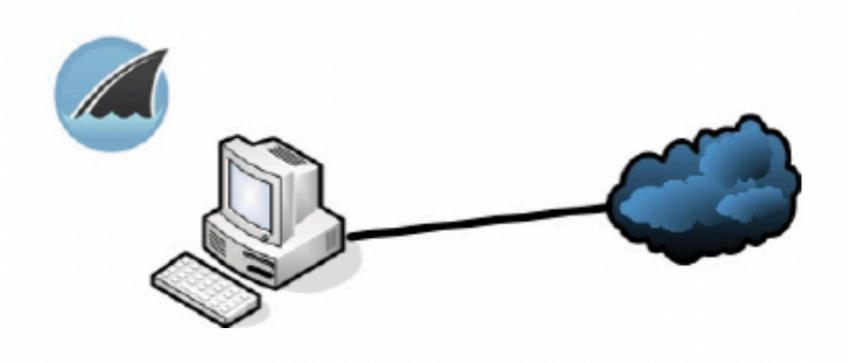
**Lab Purpose:**

The Internet Control Message Protocol is used by network devices to report on the reliability and send error messages. It is different from most of the other protocols within TCP/IP inasmuch as it isn't used to transport data. You will use ICMP when you ping other devices.

**Lab Tool:**

Wireshark on our PC.

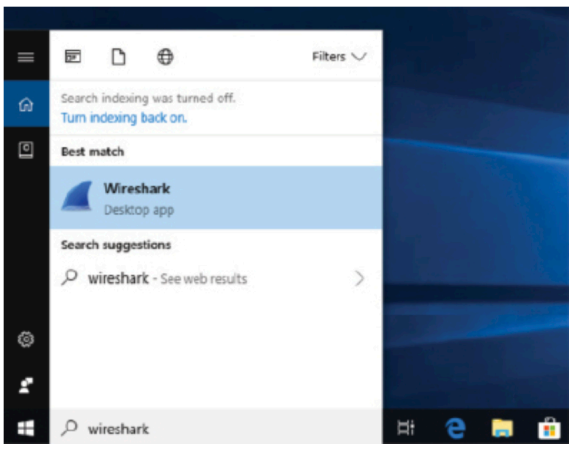
**Lab Topology:**
Run Wireshark on your home PC. You need to be able to get out to the internet because we will be pining a website name.

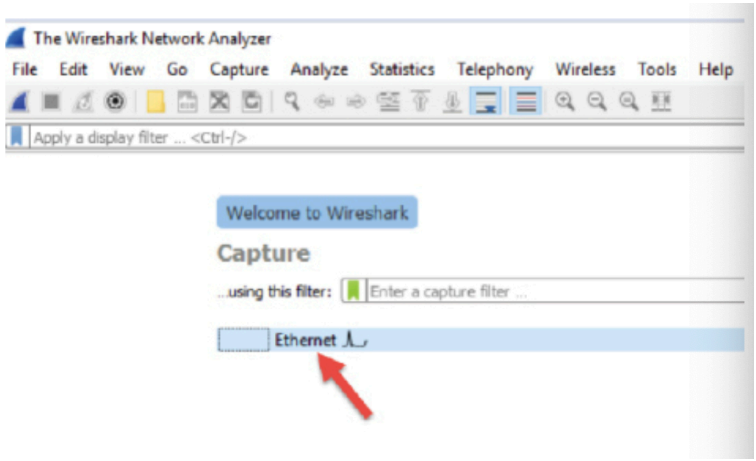


**Lab Walkthrough:**

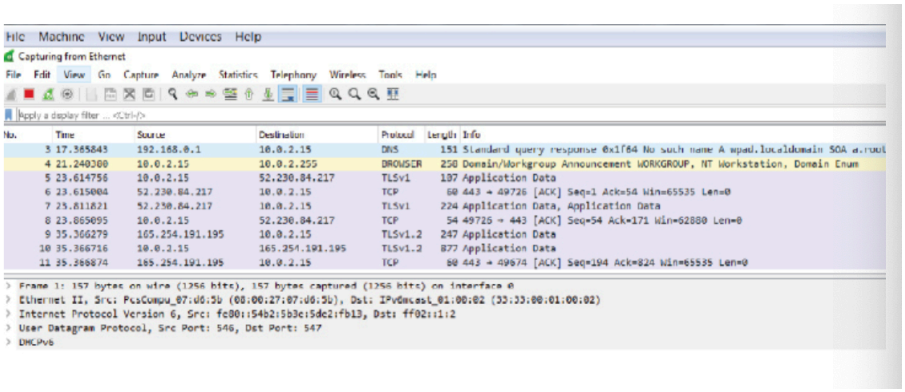
**Task 1:**
Install Wireshark on our PC if you do not have it yet.

**Task 2:**
Boot Wireshark on your PC (or your virtual PC if you are using one) and check the correct interface is the one being monitored. Click on the interface name to open the capture window.

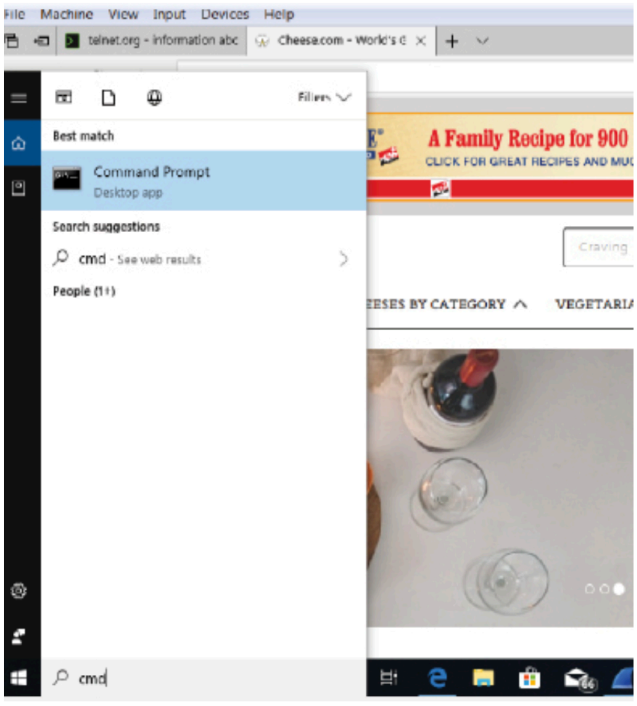





**Task 3:**
Ensure Wireshark is capturing general network traffic.

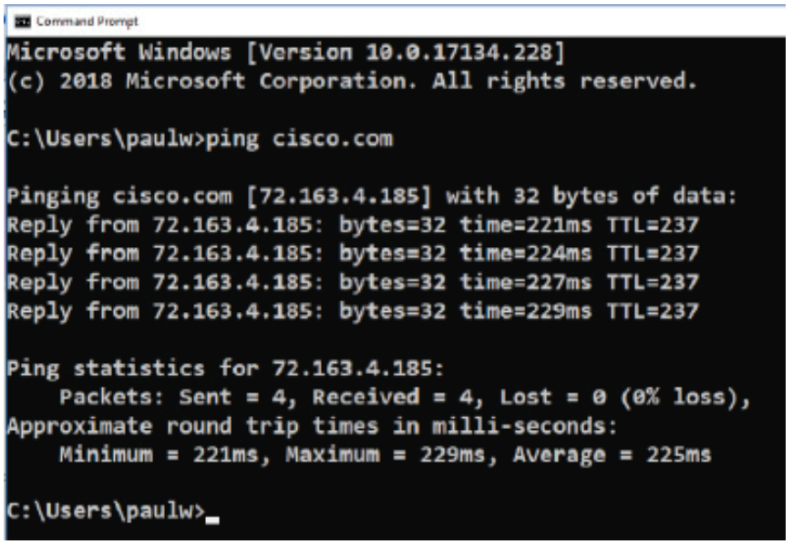



**Task 4:**
Open a command line window by typing ‘cmd’ in the search bar.

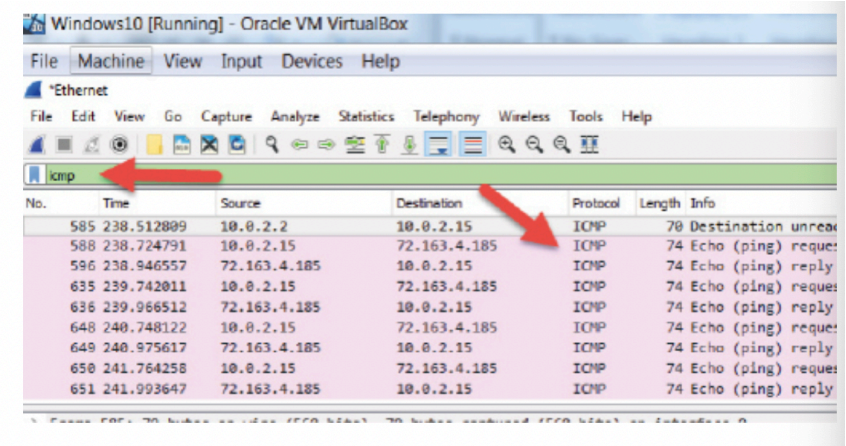


**Task 5:**

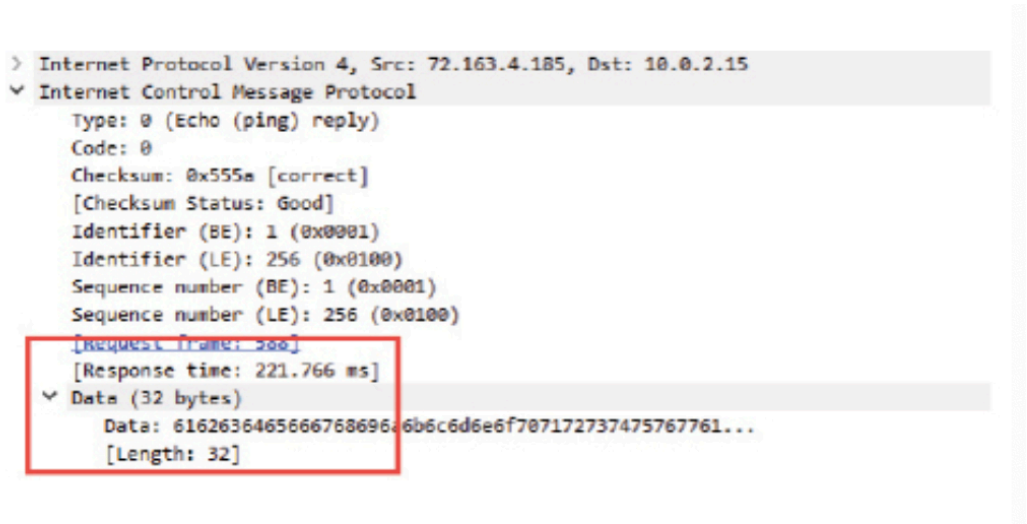
Ping a common URL, such as cisco.com. Many sites will block ICMP, so find one which doesn't (or ping an internal machine on your network).



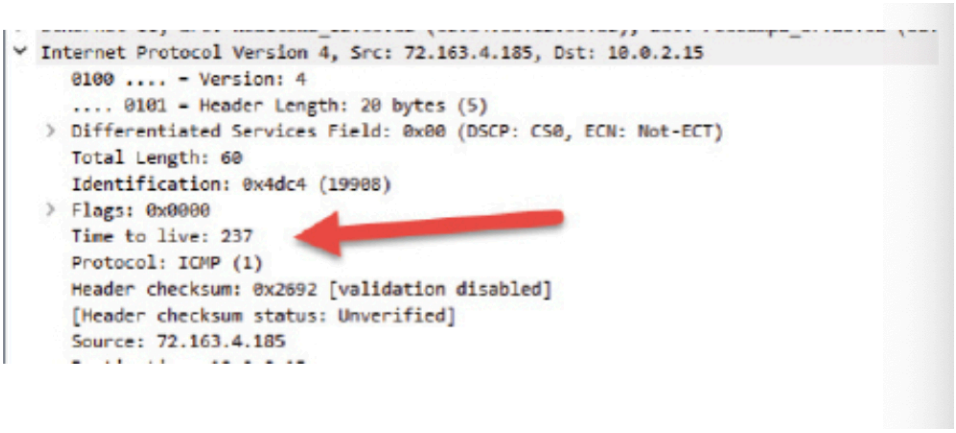

**Task 6:**
Use the Wireshark filter bar to narrow down results and use ICMP traffic. It only works if you type in lowercase.



**Task 7:**
Note that ping uses ICMP echo request and echo reply packets. Compare the other fields with the command line output. You should be able to identify the response time, length, etc.




**Talk 8:**
You will find the time to live (TTL) field in the IP header.




**Note:**
You can use sniffers to really dig into the packet contents to understand the protocols and services in great detail.