

## Lab 8. ICMP

### Lab Objective:

Learn how to recognize an ICMP packet.

### Lab Purpose:

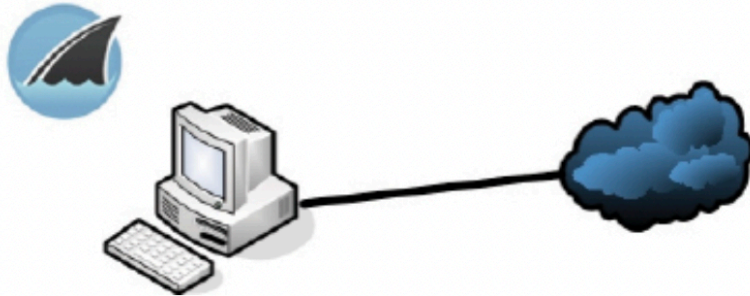
The Internet Control Message Protocol is used by network devices to report on the reliability and send error messages. It is different from most of the other protocols within TCP/IP inasmuch as it isn't used to transport data. You will use ICMP when you ping other devices.

### 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 pinging a website name.



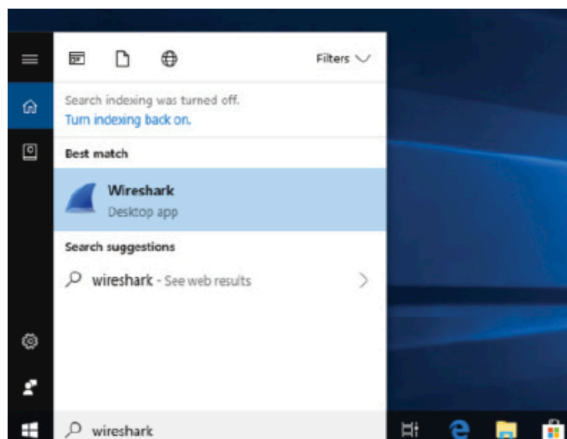
### Lab Walkthrough:

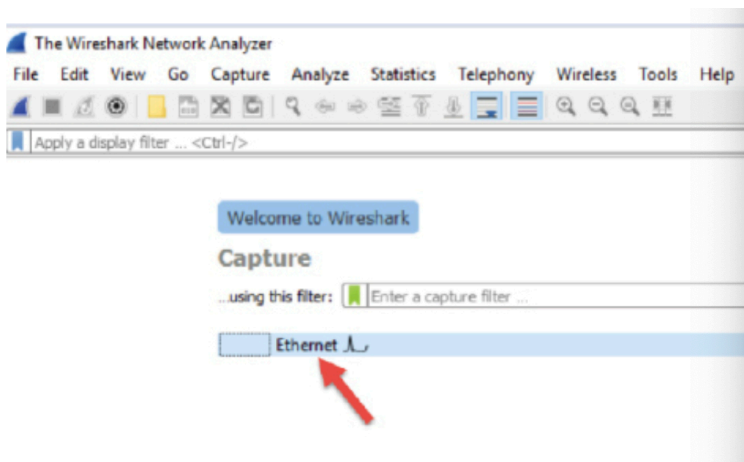
#### Task 1:

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.

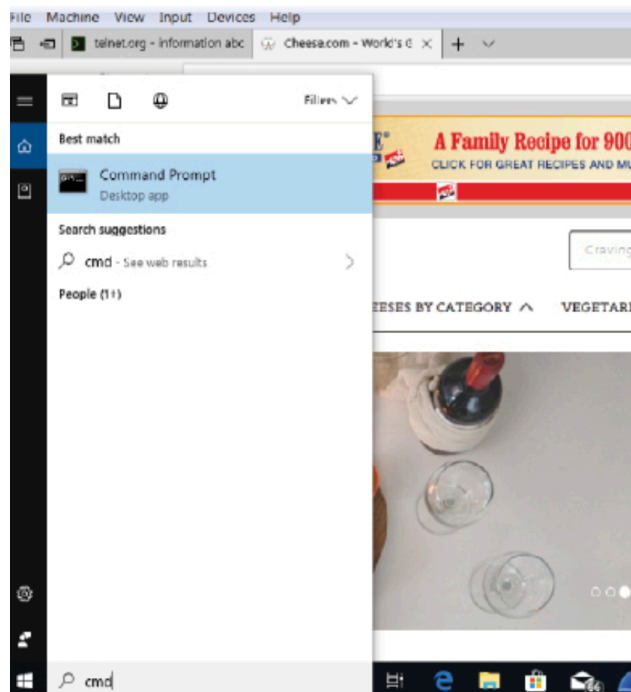
The screenshot shows the Wireshark Network Analyzer interface with a list of captured network packets. The table below represents the data shown in the packet list pane.

No.	Time	Source	Destination	Protocol	Length	Info
3	17.365843	192.168.0.1	10.0.2.15	DNS	151	Standard query response 0x164 No such name A wpad.localdomain SOA a.root
4	21.240300	10.0.2.15	10.0.2.255	BROADCAST	250	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enu
5	23.614756	10.0.2.15	52.230.04.217	TLSv1	187	Application Data
6	23.615004	52.230.04.217	10.0.2.15	TCP	60	443 → 49726 [ACK] Seq=1 Ack=54 Win=65535 Len=0
7	23.611621	52.230.04.217	10.0.2.15	TLSv1	224	Application Data, Application Data
8	23.605095	10.0.2.15	52.230.04.217	TCP	54	49726 → 443 [ACK] Seq=54 Ack=171 Win=62800 Len=0
9	35.366279	105.254.191.195	10.0.2.15	TLSv1.2	247	Application Data
10	35.366716	10.0.2.15	105.254.191.195	TLSv1.2	877	Application Data
11	35.368874	105.254.191.195	10.0.2.15	TCP	60	443 → 49874 [ACK] Seq=194 Ack=824 Win=65535 Len=0

Below the packet list, the packet details pane shows the following information for the selected packet (Frame 1):

- Frame 1: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface 0
- Ethernet II, Src: PcsCompu\_07:00:50 (00:00:27:07:00:50), Dst: IPvdcast\_01:00:02 (02:03:00:01:00:02)
- Internet Protocol Version 6, Src: fe80::54b2:5b3e:5dc2:1fb13, Dst: ff02::1:2
- User Datagram Protocol, Src Port: 546, Dst Port: 547
- DHCPv6

**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).

```
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\paulw>ping cisco.com

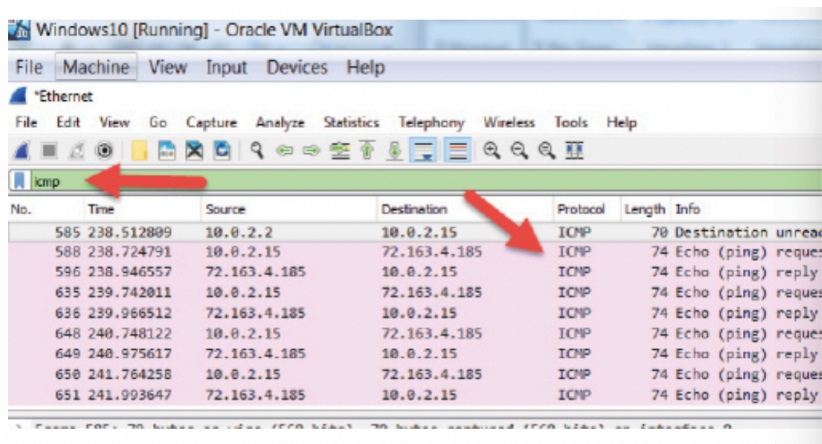
Pinging cisco.com [72.163.4.185] with 32 bytes of data:
Reply from 72.163.4.185: bytes=32 time=221ms TTL=237
Reply from 72.163.4.185: bytes=32 time=224ms TTL=237
Reply from 72.163.4.185: bytes=32 time=227ms TTL=237
Reply from 72.163.4.185: bytes=32 time=229ms TTL=237

Ping statistics for 72.163.4.185:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 221ms, Maximum = 229ms, Average = 225ms

C:\Users\paulw>
```

### 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.

```
> Internet Protocol Version 4, Src: 72.163.4.185, Dst: 10.0.2.15
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x555a [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 1 (0x0001)
  Sequence number (LE): 256 (0x0100)
  [Request frame: 300]
  [Response time: 221.766 ms]
  ▼ Data (32 bytes)
    Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
    [Length: 32]
```

### Talk 8:

You will find the time to live (TTL) field in the IP header.

```
▼ Internet Protocol Version 4, Src: 72.163.4.185, Dst: 10.0.2.15
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0x4dc4 (19908)
  > Flags: 0x0000
  Time to live: 237
  Protocol: ICMP (1)
  Header checksum: 0x2692 [validation disabled]
  [Header checksum status: Unverified]
  Source: 72.163.4.185
```

### Note:

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