

# Using Wireshark

---

## Introduction to Wireshark (version 3.x)

Wireshark is a software protocol analyser, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "**captures**" each protocol data unit (PDU) and can decode and analyse its content according to the appropriate RFC or other specifications.

## Objectives

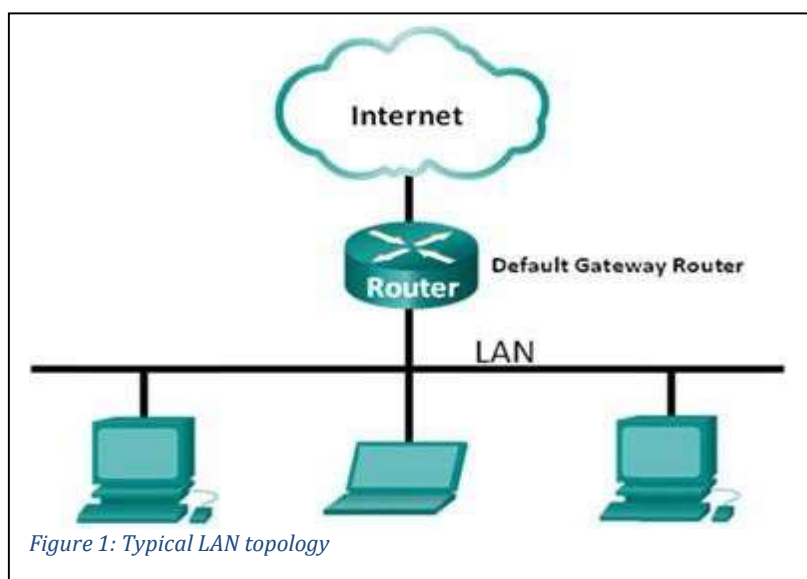
In this tutorial, you will capture and analyse local ICMP data in network traffic and determine the IP and MAC address information in the captured data.

## Analysing local ICMP traffic

One of the most commonly used types of ICMP, and the easiest to manually test, is known as "PING". Ping is similar in concept to the idea of sonar pings that are often seen in submarine films. In sonar, a pressure (sound) wave is sent out and reflects back (echos) from any object in the path. Time difference tells you how far away the object is. In data networks several Packet INternet Groper (ping) Echo Requests are sent to a target to determine if it exists, the target should then reply back with the same number of Echo Replies. The number of packets returned and time taken can indicate several things including the network distance to the target and the consistency / reliability of the network path.

In this tutorial, you will ping another PC on the LAN (illustrated in Figure 1) and capture **ICMP requests and replies** using Wireshark. You will also look inside the packets captured for specific information. This analysis will also give a first look at packet headers and their relevance to network data transport.

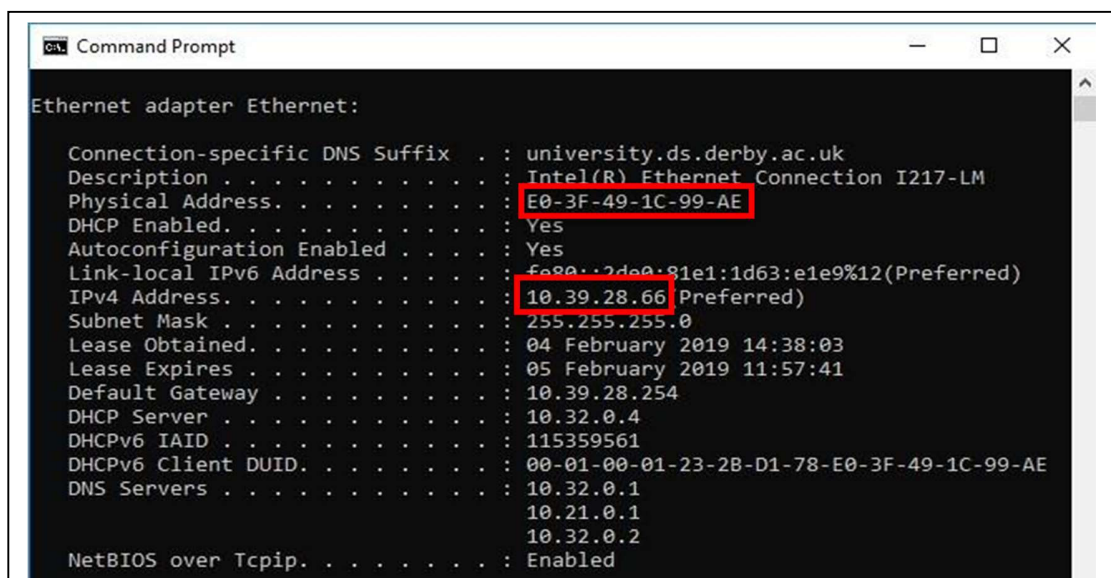
You can conduct this experiment on either the small or large PC but you must ensure that you and your "classmate" are using the same type, i.e both using small or both using large.



### Step 1: Retrieve your PC's interface addresses.

For this lab, you will need to retrieve your PC's IP address and its network interface card (NIC) physical address, also called the MAC address.

- Open a command prompt window: **Start → cmd (select Command Prompt)**
- Type **ipconfig /all**, and then press **Enter**.
- Note your PC interface's IPv4 address and MAC (physical) address as shown in Figure 2. Also note down your "default gateway" address



```

Command Prompt

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : university.ds.derby.ac.uk
    Description . . . . . : Intel(R) Ethernet Connection I217-LM
    Physical Address. . . . . : E0-3F-49-1C-99-AE
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::2de0:81e1:1d63:e1e9%12(Preferred)
    IPv4 Address. . . . . : 10.39.28.66 (Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : 04 February 2019 14:38:03
    Lease Expires . . . . . : 05 February 2019 11:57:41
    Default Gateway . . . . . : 10.39.28.254
    DHCP Server . . . . . : 10.32.0.4
    DHCPv6 IAID . . . . . : 115359561
    DHCPv6 Client DUID. . . . . : 00-01-00-01-23-2B-D1-78-E0-3F-49-1C-99-AE
    DNS Servers . . . . . : 10.32.0.1
                           10.21.0.1
                           10.32.0.2
    NetBIOS over Tcpip. . . . . : Enabled
  
```

Figure 2: Output of command ipconfig /all

- Ask a classmate for their PC IPv4 address and, in return, provide your PC IPv4 address. If you are working from home, you will be able to use the "Default

Gateway” address obtained at the previous stage or if you are really brave (and know how to find it) you could use the wifi address of your smartphone, tablet or smart tv (the default gateway address should be the same for all of them)

The “default gateway” is the address of router that connects you to your Internet Service Provider (ISP)

## Step 2: Start Wireshark and begin capturing data.

On your PC, **launch Wireshark** and after the tool starts, click on the **Local Area Connection**. If you are using a wireless network connection, chose the appropriate interface name. Begin a capture

Information will start scrolling down the top section in Wireshark. The data lines will appear in different colours based on protocol, as shown in Figure 3. For a home network, there should be minimal traffic in this window unless you are actively uploading, downloading or MS are sending you an update.

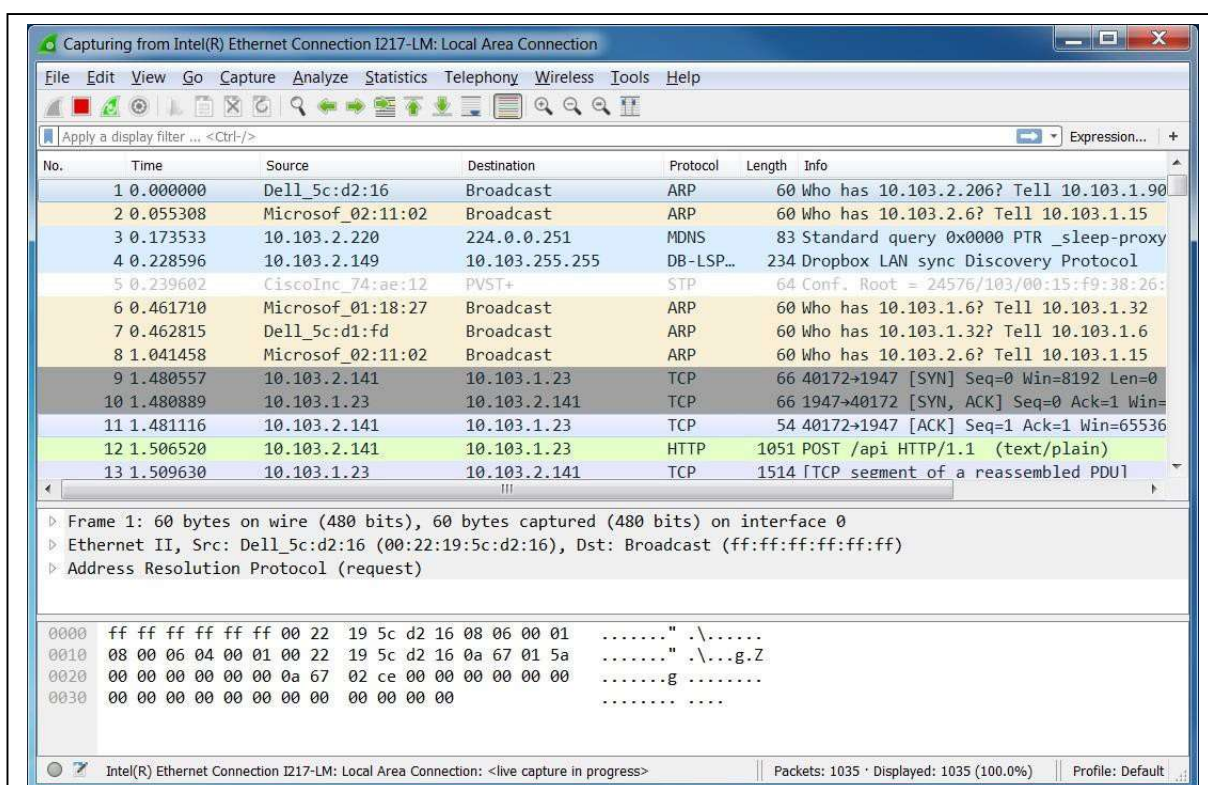


Figure 3: Live capture of the selected interface

This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN / WLAN.

Since we are only interested in displaying ICMP (ping) PDUs, you should apply a filter as discussed in the previous tutorial. An example of the required filtering is illustrated in Figure 4.

Note: PDU is a generic term used for any type of data, technically we are looking at IP packets (or IP datagrams).

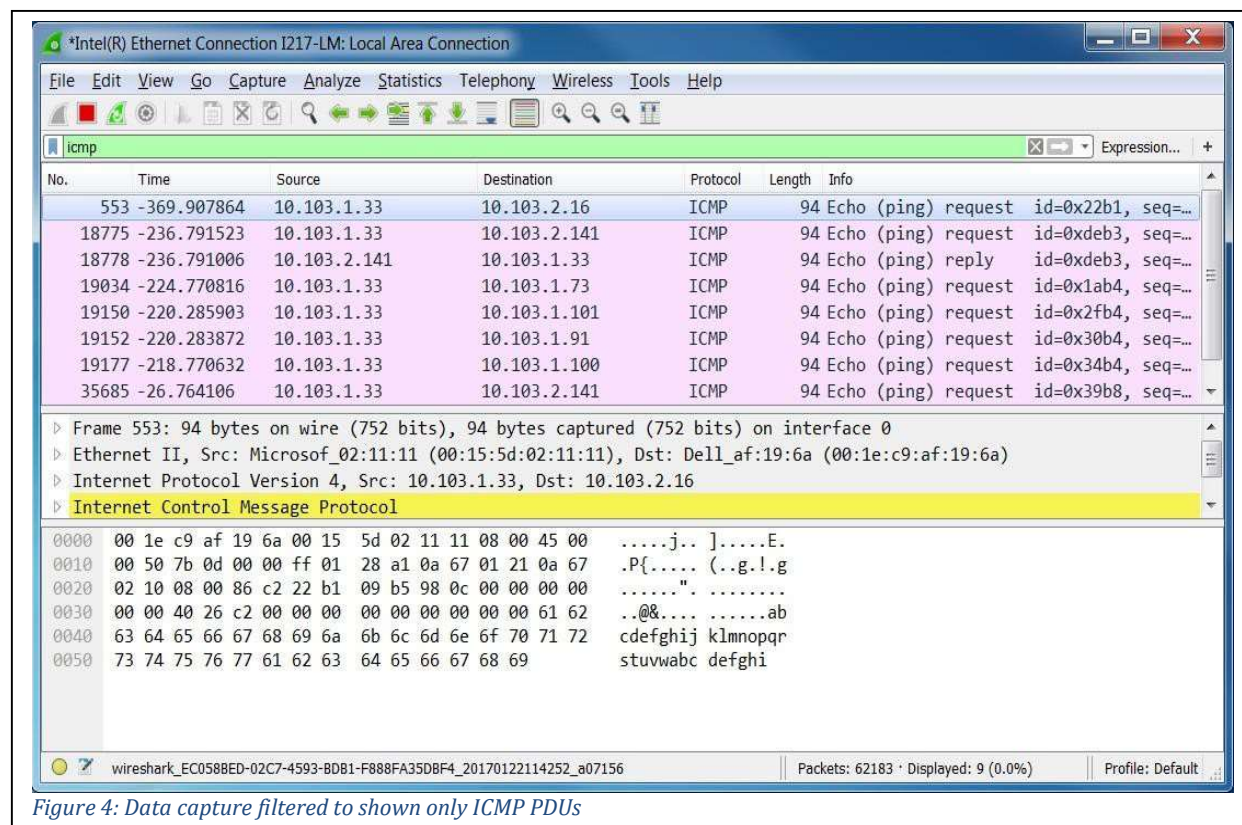


Figure 4: Data capture filtered to shown only ICMP PDUs

This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Make sure you go to the last packet captured – you can do that in several ways: via the **Go** menu, use the key combination **Ctrl+End** or scroll to the end of the capture.

Bring forward the command prompt window that you opened earlier and ping the IP address that you received from a colleague (or the default gateway address, or the tv address etc) – refer to Figure 5. Simply type the word “ping” followed by the IPv4 address.

Ping is quite clever, try this later if you wish, type “ping www.microsoft .com”, “ping www.derby.ac.uk” or “ping udo.derby.ac.uk”. If you try this and you are not sure what the results are telling you, it will become clearer later in the course.



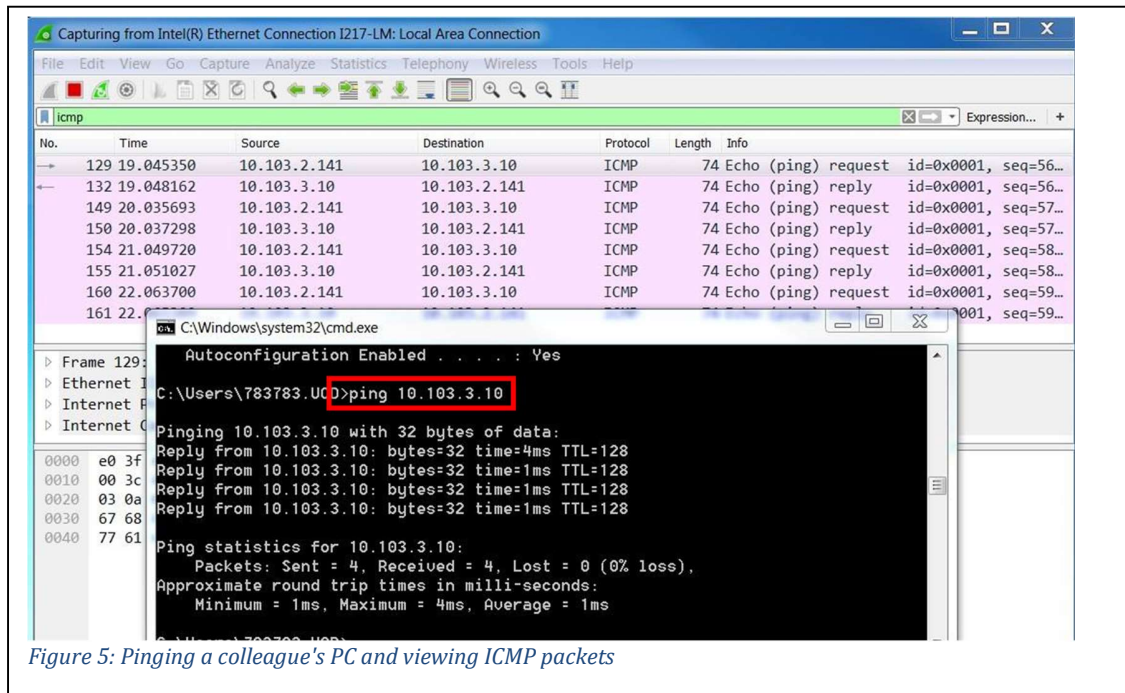


Figure 5: Pinging a colleague's PC and viewing ICMP packets

Notice that you start seeing data related to this ping appearing in the top window of Wireshark again.

Stop capturing data by clicking the **Stop Capture** icon which is now red.

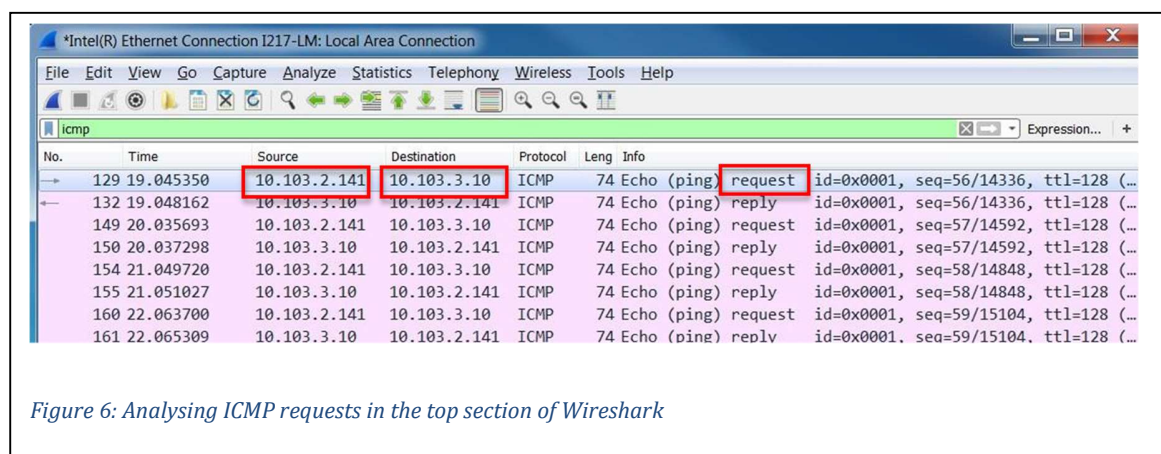
### Step 3: Examine the captured data.

In Step 3, examine the data that was generated by the ping requests to your colleague's PC and respective replies. As you know, Wireshark data is displayed in three sections:

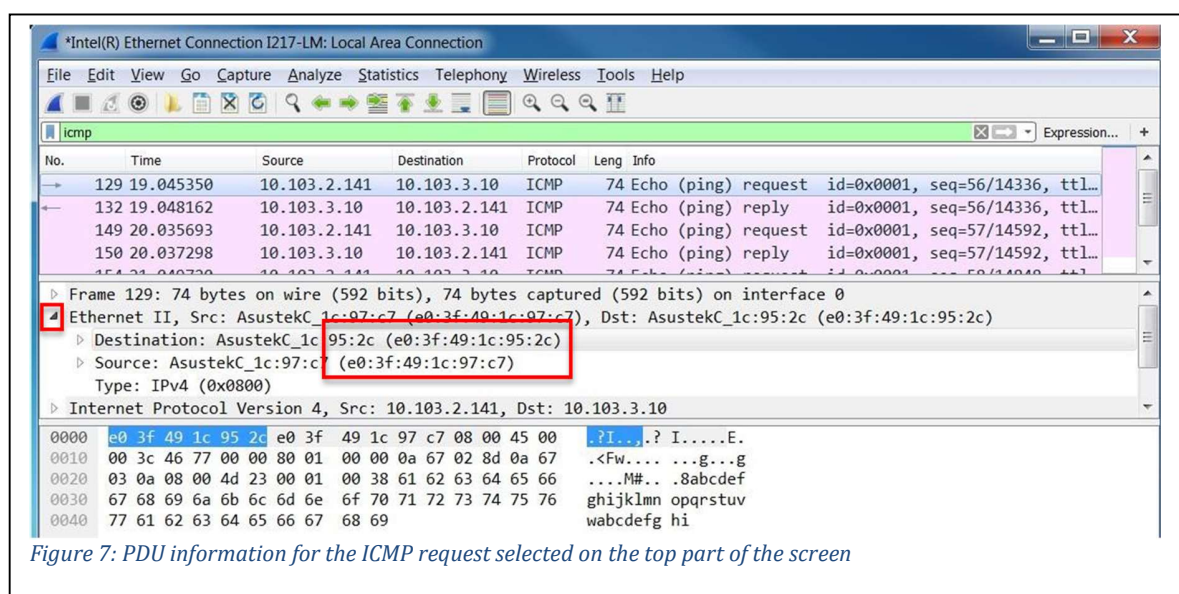
1. The **top section** displays the list of **PDU frames** captured with a summary of the IP packet information listed.
2. The **middle section** lists **PDU information for the frame** selected in the top part of the screen and separates a captured PDU frame by its protocol layers.
3. The **bottom section** displays the **raw data** of each layer for the selected frame. The raw data is displayed in both hexadecimal and ASCII formats.

*Click on an ICMP request PDU frame in the top section of Wireshark. Notice that the Source column has your PC's IP address, and the Destination contains the IP address of the colleague's PC / gateway that you pinged. Refer to*

Figure 6.



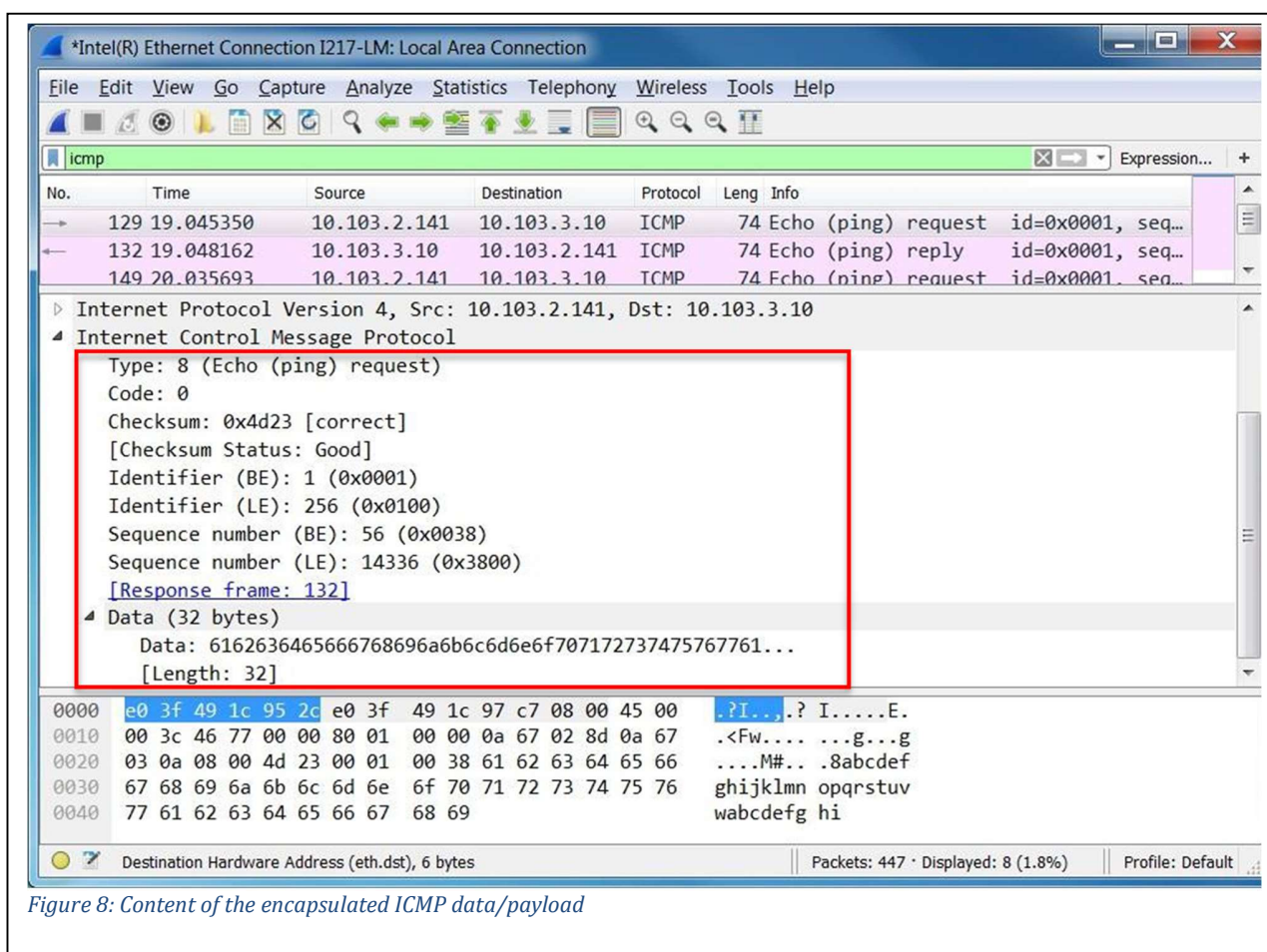
With this PDU frame still selected in the top section, navigate to the middle section. Click the **right arrow** of the Ethernet II row (highlighted in Figure 7) to view the Destination and Source MAC addresses (see Figure 7).



- Does the Source MAC address match your PC's interface?
- Does the Destination MAC address match the MAC address that of your colleague's?
- How is the MAC address of the pinged PC obtained by your PC?

If you want, you can save this capture via the **File → Save As** option from the menu or simply close it without saving via **File → Close, Continue without Saving**.

**Note:** You can (and we will) analyse this much further as indicated in Figure 8, this has only been an introduction.



Read this link for further information about remote ICMP request/reply:

[https://en.wikiversity.org/wiki/Wireshark/IPv4\\_remote](https://en.wikiversity.org/wiki/Wireshark/IPv4_remote)

## References

- Wireshark website <https://www.wireshark.org/>
- Cisco Networking academy: Lab - Using Wireshark to View Network Traffic