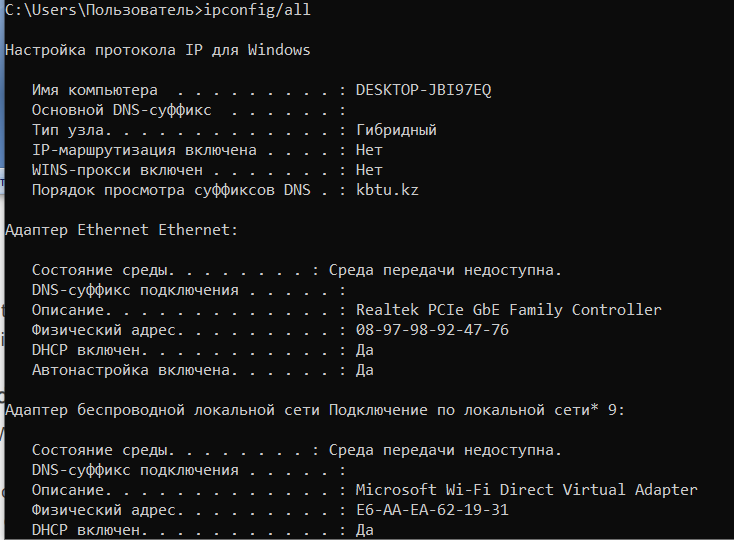
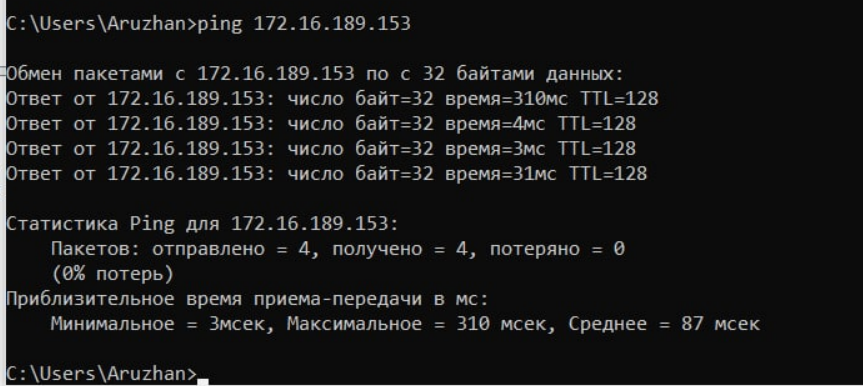
Rymbayeva Anelya, 2course, Lab2 – IT Infrastructure and Computer Networks

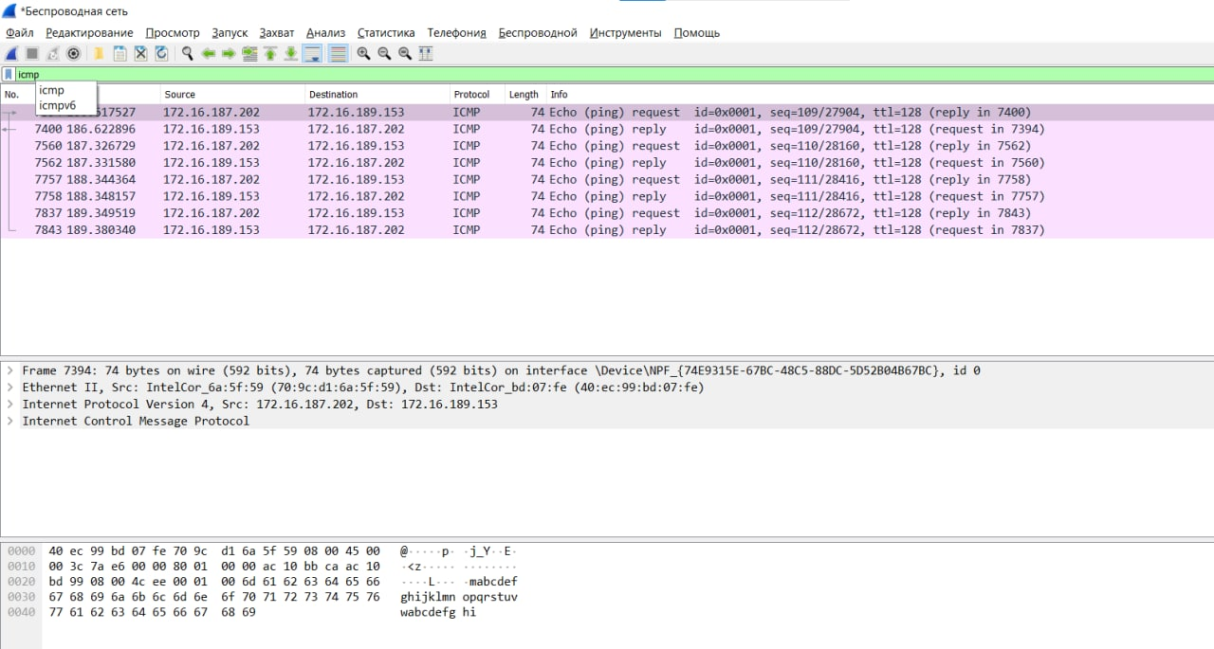
1. In a command prompt window, enter **ipconfig/all,** to the IP address of your PC interface, its description, and its MAC (physical) address.



1. Navigate to Wireshark. Double click the desired interface to start the packet capture. Make sure the desired interface has traffic.

Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol. This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN. We can apply a filter to make it easier to view and work with the data that is being captured by Wireshark. For this lab, we are only interested in displaying ICMP (ping) PDUs. Type icmp in the Filter box at the top of Wireshark and press Enter, or click the Apply button (arrow sign) to view only ICMP (ping) PDUs. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Navigate to a command prompt window and ping the IP address that you received from your team member.

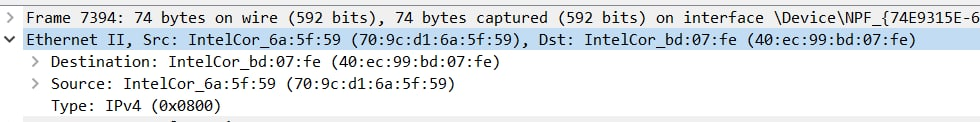




1. Click the first ICMP request PDU frames in the top section of Wireshark. Notice that the Source column has your PC IP address, and the Destination column contains the IP address of the teammate PC that you pinged.



1. With this PDU frame still selected in the top section, navigate to the middle section. Click the plus sign to the left of the Ethernet II row to view the destination and source MAC addresses.

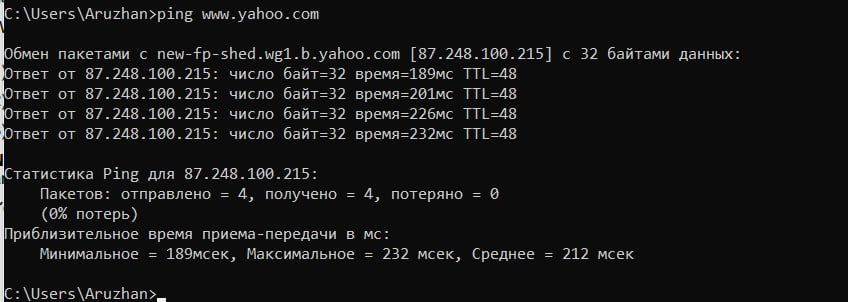


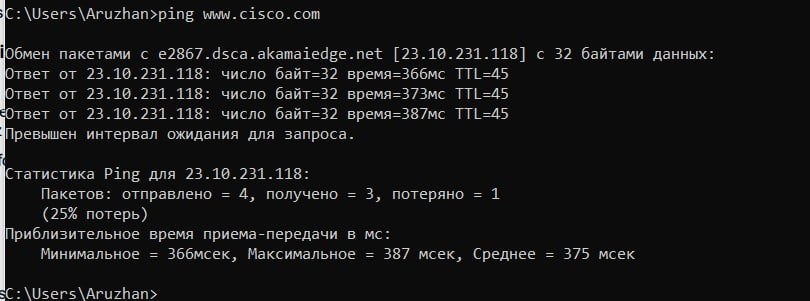
1. Does the source MAC address match your PC interface? Yes
2. Does the destination MAC address in Wireshark match your team member MAC address? Yes
3. How is the MAC address of the pinged PC obtained by your PC?

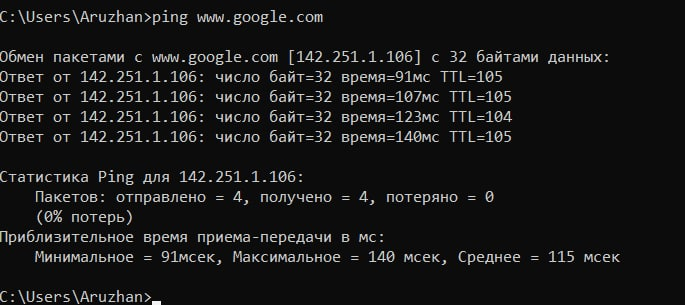
The MAC address is obtained through an ARP request/

1. With the capture active, ping the following three website URLs:

* www.yahoo.com
* [www.cisco.com](http://www.cisco.com)
* [www.google.com](http://www.google.com)







1. IP address for [**www.yahoo.com**](http://www.yahoo.com)**:** 87.248.100.215
2. MAC address for [**www.yahoo.com**](http://www.yahoo.com)**:** 74:83:c2:78:a8:8f
3. IP address for [**www.cisco.com**](http://www.cisco.com)**:** 23.10.231.118
4. MAC address for [**www.cisco.com**](http://www.cisco.com)**:** 74:83:c2:78:a8:8f
5. IP address for [**www.google.com**](http://www.google.com)**:** 142.251.1.106
6. MAC address for [**www.google.com**](http://www.google.com)**:** 74:83:c2:78:a8:8f
7. What is significant about this information? The MAC addresses of 3 sites(locations) are the same.
8. How does this information differ from the local ping information you received in Part 1?

A ping to a local host returns the MAC address of the PC NIC. A ping to a remote host returns the MAC address of the default gateway LAN interface.

1. Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?

MAC addresses for remote hosts are not known on the local network, so the MAC address of the default-gateway is used. After the packet reaches the default-gateway router, the Layer 2 information is stripped from the packet and a new Layer 2 header is attached with the destination MAC address of the next hop router.