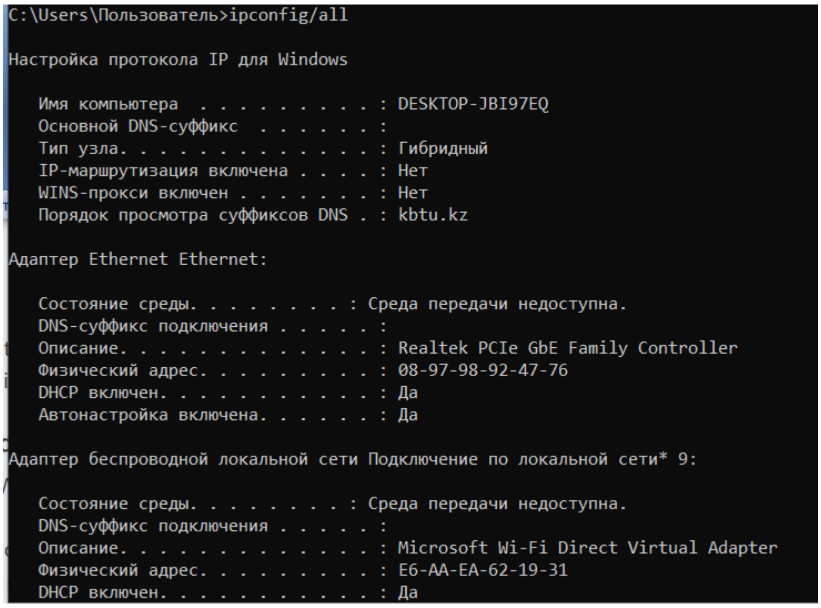
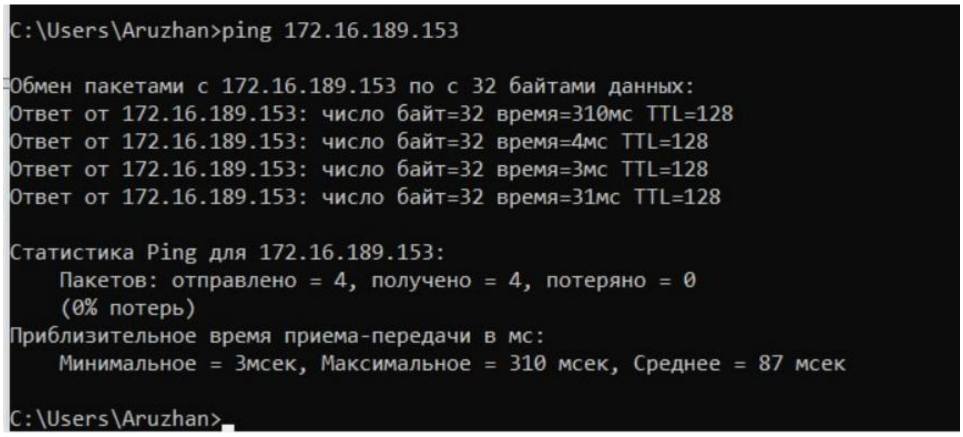
Rymbayeva Anelya, 2 course, Lab2 – IT Infrastructure and Computer Networks

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

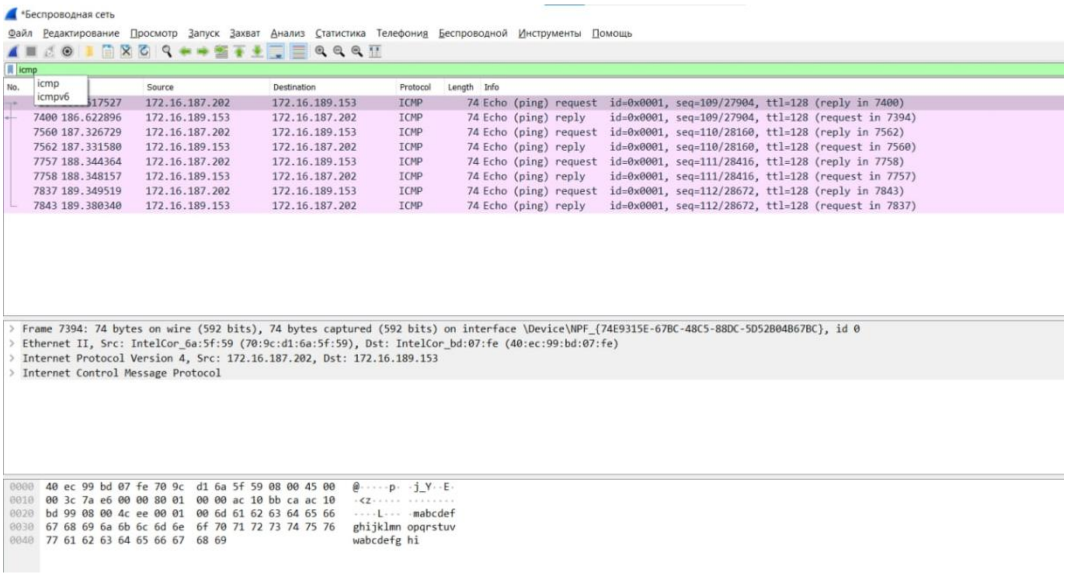


```
C:\Users\Пользователь>ipconfig/all

Настройка протокола IP для Windows

   Имя компьютера  . . . . . . . . . : DESKTOP-JBI97EQ
   Основной DNS-суффикс  . . . . . . :
   Тип узла. . . . . . . . . . . . . : Гибридный
   IP-маршрутизация включена . . . . : Нет
   WINS-прокси включен . . . . . . . : Нет
   Порядок просмотра суффиксов DNS . : kbtu.kz

Адаптер Ethernet Ethernet:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Физический адрес. . . . . . . . . : 08-97-98-92-47-76
   DHCP включен. . . . . . . . . . . : Да
   Автонастройка включена. . . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 9:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Физический адрес. . . . . . . . . : E6-AA-EA-62-19-31
   DHCP включен. . . . . . . . . . . : Да
```

2. 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.



```
C:\Users\Aruzhan>ping 172.16.189.153

Обмен пакетами с 172.16.189.153 по с 32 байтами данных:
Ответ от 172.16.189.153: число байт=32 время=310мс TTL=128
Ответ от 172.16.189.153: число байт=32 время=4мс TTL=128
Ответ от 172.16.189.153: число байт=32 время=3мс TTL=128
Ответ от 172.16.189.153: число байт=32 время=31мс TTL=128

Статистика Ping для 172.16.189.153:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 310 мсек, Среднее = 87 мсек

C:\Users\Aruzhan>
```



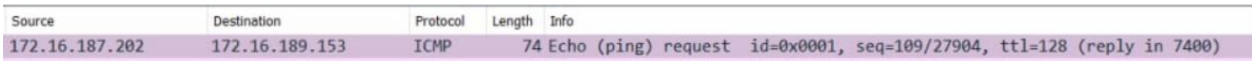
*Беспроводная сеть
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
icmp
icmp
icmpv6

```
No.          Source           Destination      Protocol  Length  Info
     17527   172.16.187.202   172.16.189.153   ICMP      74 Echo (ping) request  id=0x0001, seq=109/27904, ttl=128 (reply in 7400)
7400 186.622896 172.16.189.153 172.16.187.202  ICMP      74 Echo (ping) reply    id=0x0001, seq=109/27904, ttl=128 (request in 7394)
7560 187.326729 172.16.187.202 172.16.189.153  ICMP      74 Echo (ping) request  id=0x0001, seq=110/28160, ttl=128 (reply in 7562)
7562 187.331580 172.16.189.153 172.16.187.202  ICMP      74 Echo (ping) reply    id=0x0001, seq=110/28160, ttl=128 (request in 7560)
7757 188.344364 172.16.187.202 172.16.189.153  ICMP      74 Echo (ping) request  id=0x0001, seq=111/28416, ttl=128 (reply in 7758)
7758 188.348157 172.16.189.153 172.16.187.202  ICMP      74 Echo (ping) reply    id=0x0001, seq=111/28416, ttl=128 (request in 7757)
7837 189.349519 172.16.187.202 172.16.189.153  ICMP      74 Echo (ping) request  id=0x0001, seq=112/28672, ttl=128 (reply in 7843)
7843 189.380340 172.16.189.153 172.16.187.202  ICMP      74 Echo (ping) reply    id=0x0001, seq=112/28672, ttl=128 (request in 7837)
```

```
> Frame 7394: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{74E9315E-67BC-48C5-88DC-5D52B04B67BC}, id 0
> Ethernet II, Src: IntelCor_6a:5f:59 (70:9c:d1:6a:5f:59), Dst: IntelCor_bd:07:fe (40:ec:99:bd:07:fe)
> Internet Protocol Version 4, Src: 172.16.187.202, Dst: 172.16.189.153
> Internet Control Message Protocol
```

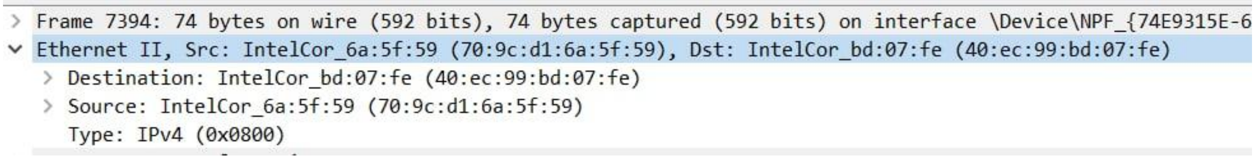
```
0000  40 ec 99 bd 07 fe 70 9c  d1 6a 5f 59 08 00 45 00   @·····p· ·j_Y··E·
0010  00 3c 7a e6 00 00 80 01  00 00 ac 10 bb ca ac 10   ·<z····· ········
0020  bd 99 08 00 4c ee 00 01  00 6d 61 62 63 64 65 66   ····L··· ·mabcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

3. 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.



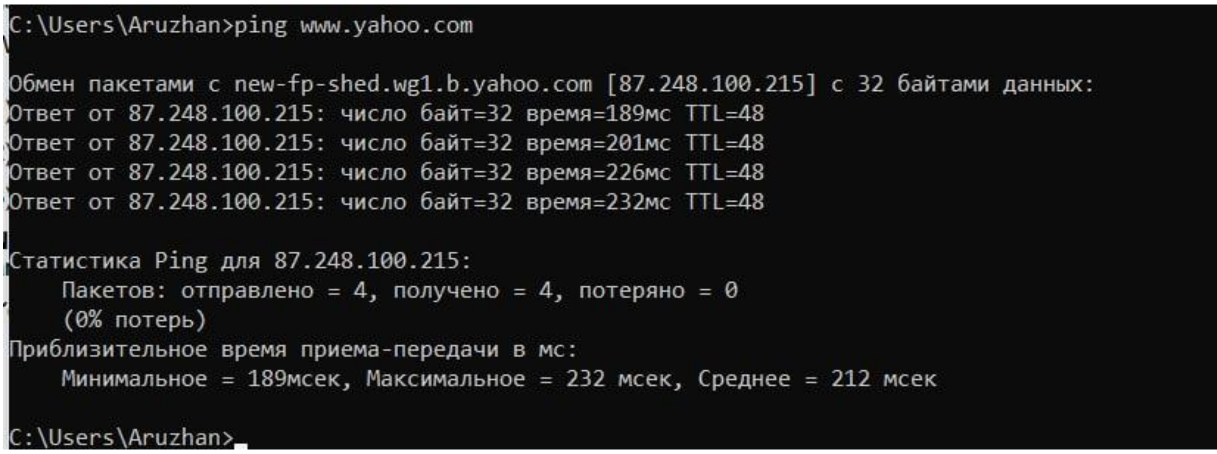
```
Source           Destination      Protocol  Length  Info
172.16.187.202   172.16.189.153   ICMP      74 Echo (ping) request  id=0x0001, seq=109/27904, ttl=128 (reply in 7400)
```

4. 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.

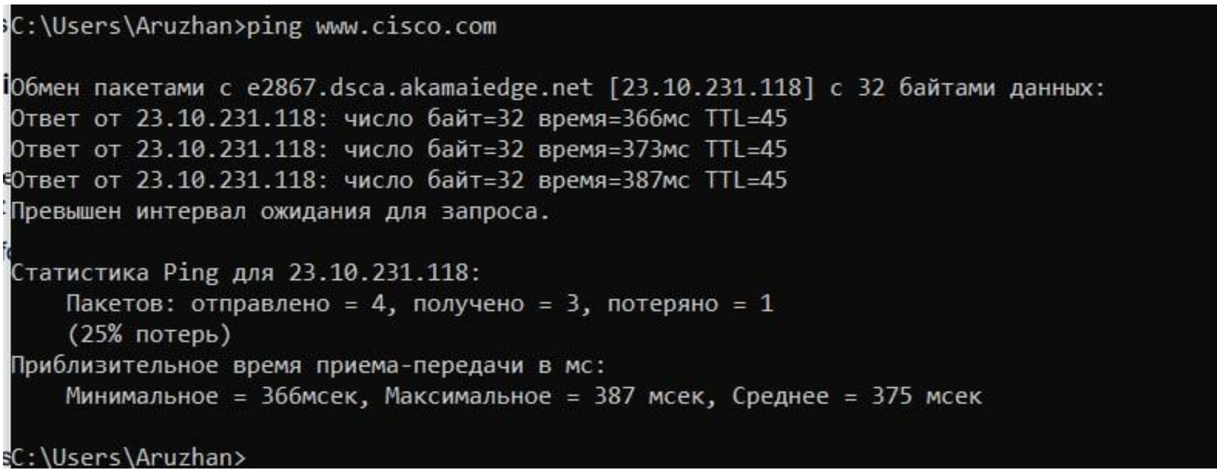


```
> Frame 7394: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{74E9315E-6
v Ethernet II, Src: IntelCor_6a:5f:59 (70:9c:d1:6a:5f:59), Dst: IntelCor_bd:07:fe (40:ec:99:bd:07:fe)
  > Destination: IntelCor_bd:07:fe (40:ec:99:bd:07:fe)
  > Source: IntelCor_6a:5f:59 (70:9c:d1:6a:5f:59)
    Type: IPv4 (0x0800)
```

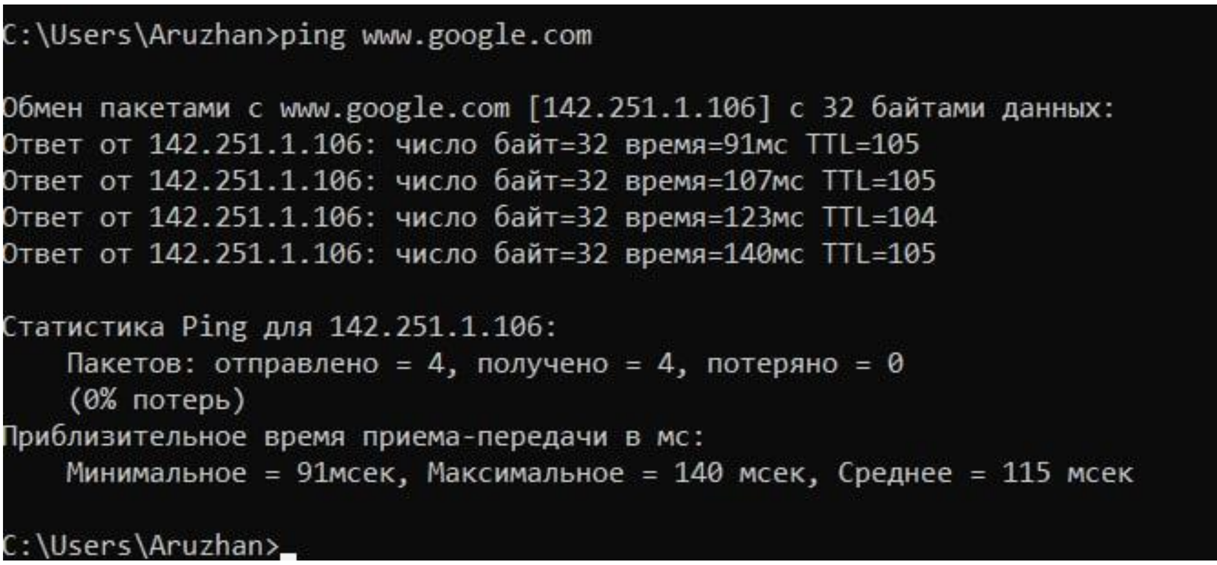
5. Does the source MAC address match your PC interface? Yes
6. Does the destination MAC address in Wireshark match your team member MAC address? Yes
7. How is the MAC address of the pinged PC obtained by your PC?
   The MAC address is obtained through an ARP request/
8. With the capture active, ping the following three website URLs:
   - www.yahoo.com
   - www.cisco.com
   - www.google.com



```
C:\Users\Aruzhan>ping www.yahoo.com

Обмен пакетами с new-fp-shed.wg1.b.yahoo.com [87.248.100.215] с 32 байтами данных:
Ответ от 87.248.100.215: число байт=32 время=189мс TTL=48
Ответ от 87.248.100.215: число байт=32 время=201мс TTL=48
Ответ от 87.248.100.215: число байт=32 время=226мс TTL=48
Ответ от 87.248.100.215: число байт=32 время=232мс TTL=48

Статистика Ping для 87.248.100.215:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 189мсек, Максимальное = 232 мсек, Среднее = 212 мсек

C:\Users\Aruzhan>
```



```
C:\Users\Aruzhan>ping www.cisco.com

Обмен пакетами с e2867.dsca.akamaiedge.net [23.10.231.118] с 32 байтами данных:
Ответ от 23.10.231.118: число байт=32 время=366мс TTL=45
Ответ от 23.10.231.118: число байт=32 время=373мс TTL=45
Ответ от 23.10.231.118: число байт=32 время=387мс TTL=45
Превышен интервал ожидания для запроса.

Статистика Ping для 23.10.231.118:
    Пакетов: отправлено = 4, получено = 3, потеряно = 1
    (25% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 366мсек, Максимальное = 387 мсек, Среднее = 375 мсек

C:\Users\Aruzhan>
```



```
C:\Users\Aruzhan>ping www.google.com

Обмен пакетами с www.google.com [142.251.1.106] с 32 байтами данных:
Ответ от 142.251.1.106: число байт=32 время=91мс TTL=105
Ответ от 142.251.1.106: число байт=32 время=107мс TTL=105
Ответ от 142.251.1.106: число байт=32 время=123мс TTL=104
Ответ от 142.251.1.106: число байт=32 время=140мс TTL=105

Статистика Ping для 142.251.1.106:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 91мсек, Максимальное = 140 мсек, Среднее = 115 мсек

C:\Users\Aruzhan>
```

9. IP address for **www.yahoo.com:** 87.248.100.215
10. MAC address for **www.yahoo.com:** 74:83:c2:78:a8:8f
11. IP address for **www.cisco.com:** 23.10.231.118
12. MAC address for **www.cisco.com:** 74:83:c2:78:a8:8f
13. IP address for **www.google.com:** 142.251.1.106
14. MAC address for **www.google.com:** 74:83:c2:78:a8:8f
15. What is significant about this information? The MAC addresses of 3 sites(locations) are the same.
16. 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.
17. 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.