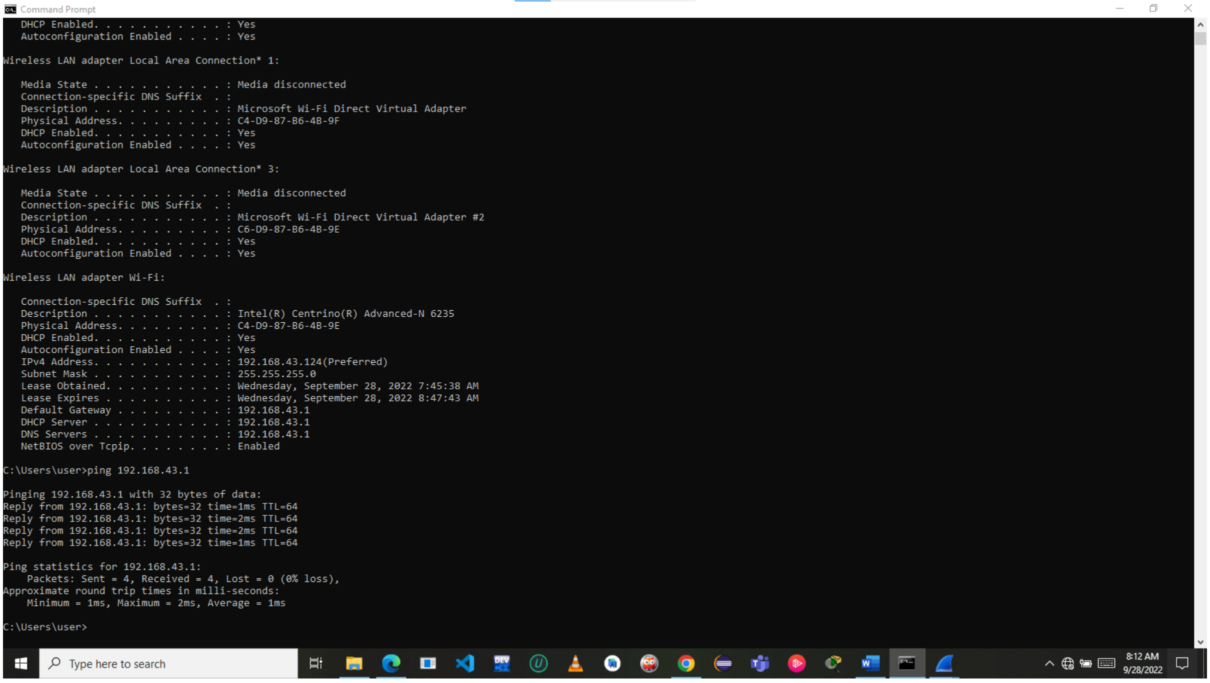
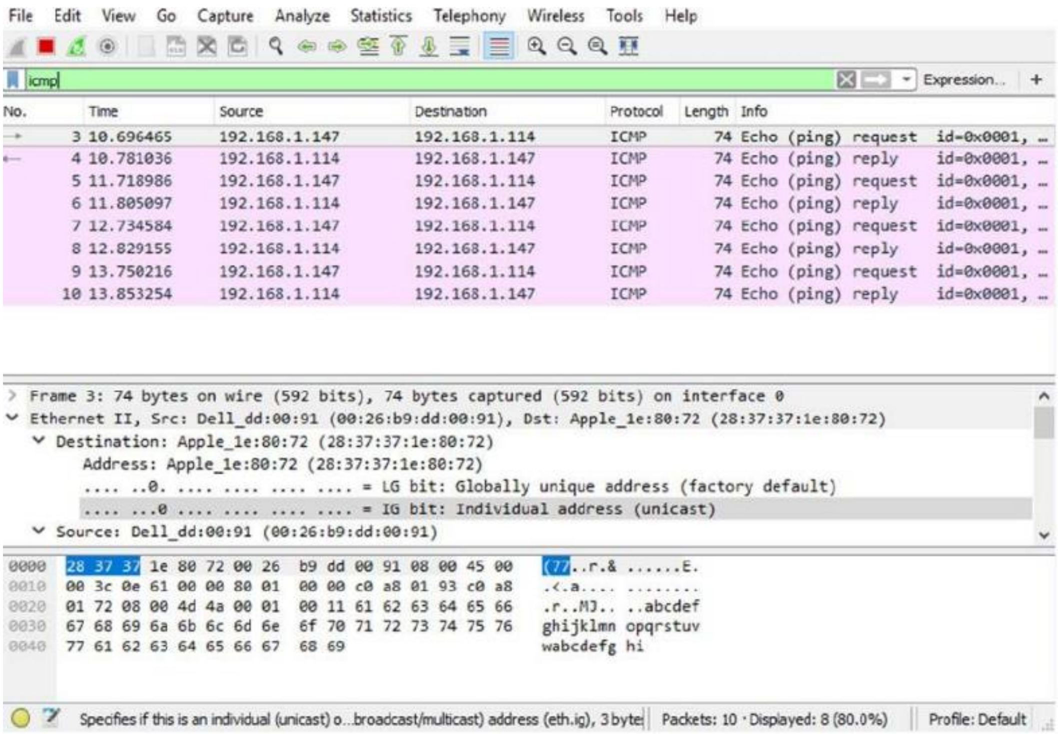
Wireshark to View Network Traffic

Examining and analyzing the data from the remote hosts.



```
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : C4-D9-87-B6-4B-9F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : C6-D9-87-B6-4B-9E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6235
   Physical Address. . . . . . . . . : C4-D9-87-B6-4B-9E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.43.124(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, September 28, 2022 7:45:38 AM
   Lease Expires . . . . . . . . . . : Wednesday, September 28, 2022 8:47:43 AM
   Default Gateway . . . . . . . . . : 192.168.43.1
   DHCP Server . . . . . . . . . . . : 192.168.43.1
   DNS Servers . . . . . . . . . . . : 192.168.43.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\user>ping 192.168.43.1

Pinging 192.168.43.1 with 32 bytes of data:
Reply from 192.168.43.1: bytes=32 time=1ms TTL=64
Reply from 192.168.43.1: bytes=32 time=2ms TTL=64
Reply from 192.168.43.1: bytes=32 time=2ms TTL=64
Reply from 192.168.43.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.43.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\user>
```



icmp

No.	Time	Source	Destination	Protocol	Length	Info
3	10.696465	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, …
4	10.781036	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, …
5	11.718986	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, …
6	11.805097	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, …
7	12.734584	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, …
8	12.829155	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, …
9	13.750216	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, …
10	13.853254	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, …

```
> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
v Ethernet II, Src: Dell_dd:00:91 (00:26:b9:dd:00:91), Dst: Apple_1e:80:72 (28:37:37:1e:80:72)
  v Destination: Apple_1e:80:72 (28:37:37:1e:80:72)
      Address: Apple_1e:80:72 (28:37:37:1e:80:72)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Dell_dd:00:91 (00:26:b9:dd:00:91)
```

```
0000  28 37 37 1e 80 72 00 26  b9 dd 00 91 08 00 45 00   (77..r.& ......E.
0010  00 3c 0e 61 00 00 80 01  00 00 c0 a8 01 93 c0 a8   .<.a.... ........
0020  01 72 08 00 4d 4a 00 01  00 11 61 62 63 64 65 66   .r..MJ.. ..abcdef
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
```

Specifies if this is an individual (unicast) o...broadcast/multicast) address (eth.ig), 3 byte | Packets: 10 · Displayed: 8 (80.0%) | Profile: Default

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.

Does the source MAC address match your PC interface?

Yes

Does the destination MAC address in Wireshark match your team member MAC address?

Yes

How is the MAC address of the pinged PC obtained by your PC?

The MAC address is obtained through an ARP request.

IP address for www.yahoo.com: 98.137.246.7

MAC address for www.yahoo.com: C4-D9-87-B6-4B-9E

IP address for www.cisco.com: 96.7.79.147

MAC address for www.cisco.com: C4-D9-87-B6-4B-9E

IP address for www.google.com: 172.217.14.100

MAC address for www.google.com: C4-D9-87-B6-4B-9E

The IP addresses vary but MAC addresses for all three locations are the same.

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.