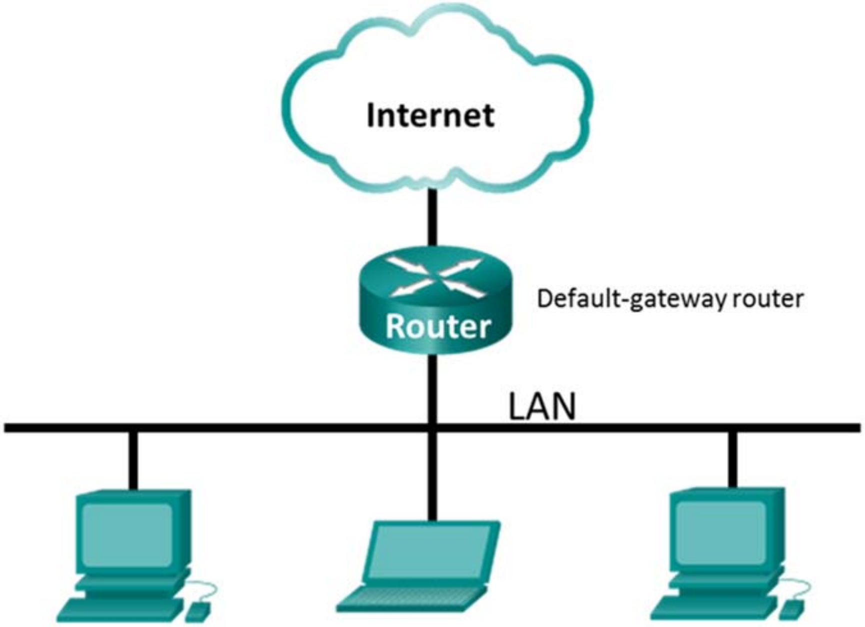
Lab – Address Resolution Protocol (ARP)

Topology



Objectives

Part 1: Download and Install Wireshark

Part 2: Capture and Analyze ARP Data in Wireshark

- Start and stop data capture of ping traffic to remote hosts.
- Locate the IPv4 and MAC address information in captured PDUs.
- Analyze the content of the ARP messages exchanged between devices on the LAN.

Part 3: View the ARP cache entries on the PC

- Access the Windows Command Prompt.
- Use the Windows **arp** command to view the local ARP table cache on the PC.

Background / Scenario

Address Resolution Protocol (ARP) is used by TCP/IP to map a Layer 3 IPv4 address to a Layer 2 MAC address.   When an Ethernet frame is transmitted on the network, it must have a destination MAC address. To dynamically discover the MAC address of a known destination, the source device broadcasts an ARP request on the local network. The device that is configured with the destination IPv4 address responds to the request with an ARP reply and the MAC address is recorded in the ARP cache.

Every device on the LAN maintains its own ARP cache. The ARP cache is a small area in RAM that holds the ARP responses. Viewing an ARP cache on a PC displays the IPv4 address and the MAC address of each device on the LAN with which the PC has exchanged ARP messages.

Wireshark is a software protocol analyzer, 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 analyze its content according to the appropriate protocol specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs in the Cisco courses for data analysis and troubleshooting. This lab provides instructions for downloading and installing Wireshark, although it may already be installed. In this lab, you will use Wireshark to capture ARP exchanges on the local network.

Required Resources

- 1 Windows 10 PC with Internet access
- Additional PC(s) on a local-area network (LAN) will be used to reply to **ping** requests. If no additional PCs are on the LAN, the default gateway address will be used to reply to the **ping** requests.

Part 1: Download and Install Wireshark

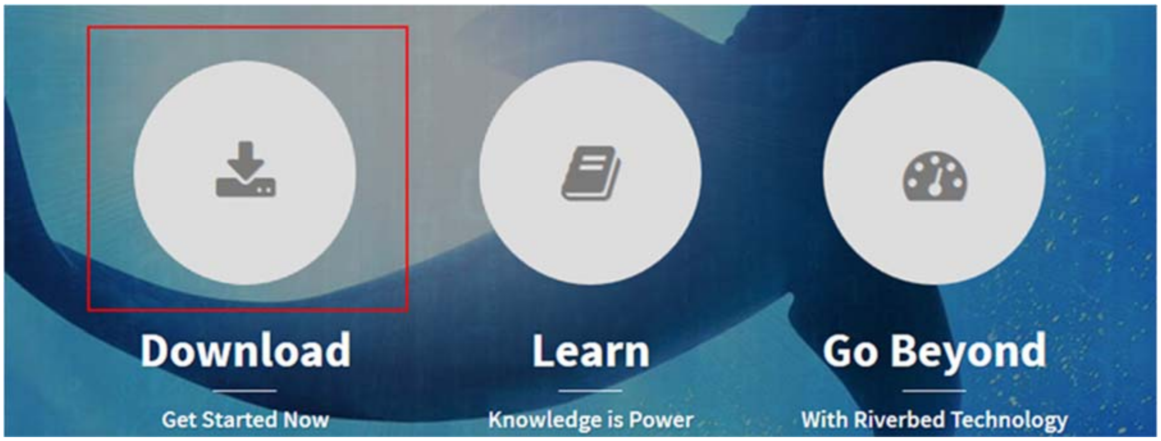
Wireshark has become the industry standard packet-sniffer program used by network engineers. This open source software is available for many different operating systems, including Windows, Mac, and Linux.

If Wireshark is already installed on your PC, you can skip Part 1 and go directly to Part 2. If Wireshark is not installed on your PC, check with your instructor about your academy's software download policy.

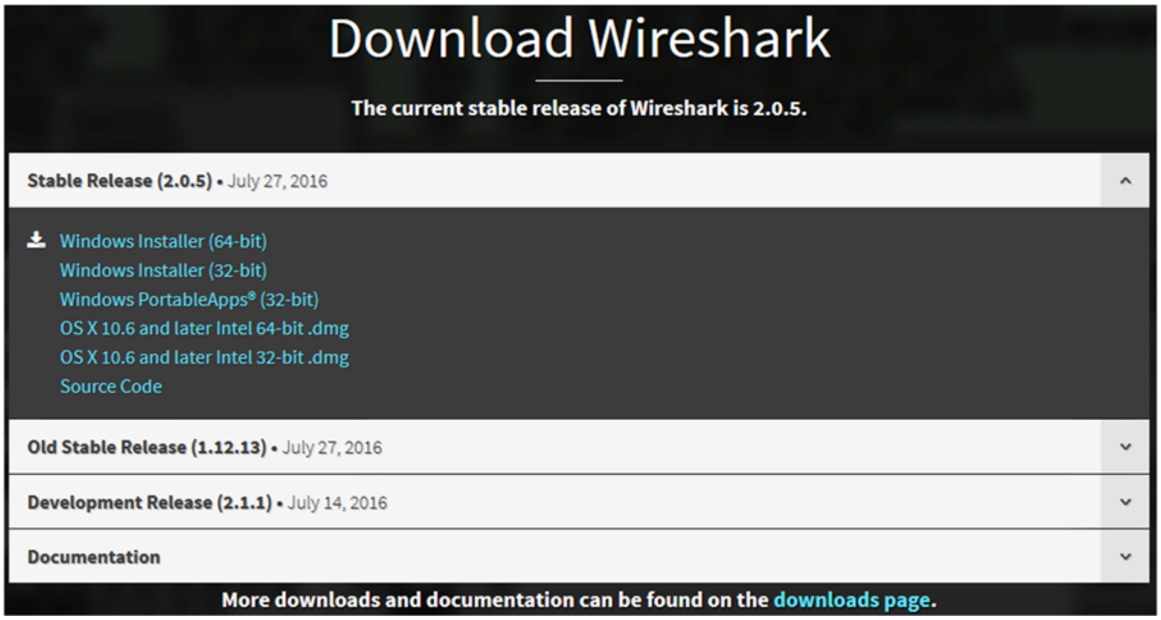
Step 1:   Download Wireshark.

a. Wireshark can be downloaded from www.wireshark.org.

b. Click **Download**.



c. Choose the software version you need based on your PC's architecture and operating system. For instance, if you have a 64-bit PC running Windows, choose **Windows Installer (64-bit)**.



Download Wireshark

The current stable release of Wireshark is 2.0.5.

Stable Release (2.0.5) • July 27, 2016

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- OS X 10.6 and later Intel 64-bit .dmg
- OS X 10.6 and later Intel 32-bit .dmg
- Source Code

Old Stable Release (1.12.13) • July 27, 2016

Development Release (2.1.1) • July 14, 2016

Documentation

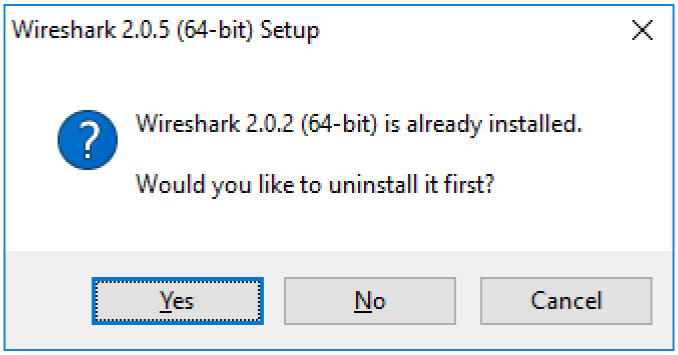
More downloads and documentation can be found on the downloads page.

d. After making a selection, the download should start. Click **Save File** if prompted. The location of the downloaded file depends on the browser and operating system that you use. For Windows users, the default location is the **Downloads** folder.

Step 2: Install Wireshark.

a. The downloaded file is named **Wireshark-win64-x.x.x.exe**, where **x** represents the version number. Double-click the file to start the installation process. It is version 2.0.5 in this example.

b. Respond to any security messages that may display on your screen. If you already have a copy of Wireshark on your PC, you will be prompted to uninstall the old version before installing the new version. It is recommended that you remove the old version of Wireshark prior to installing another version. Click **Yes** to uninstall the previous version of Wireshark.

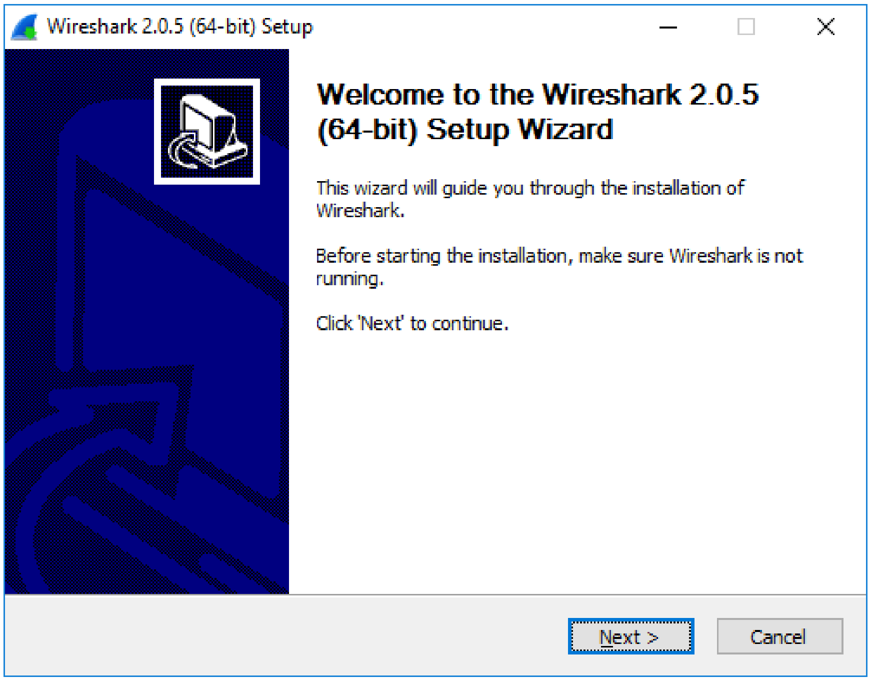


Wireshark 2.0.5 (64-bit) Setup

Wireshark 2.0.2 (64-bit) is already installed.

Would you like to uninstall it first?

c. If this is the first time to install Wireshark, or after you have completed the uninstall process, you will navigate to the Wireshark Setup wizard. Click **Next**.



Wireshark 2.0.5 (64-bit) Setup

Welcome to the Wireshark 2.0.5 (64-bit) Setup Wizard

This wizard will guide you through the installation of Wireshark.

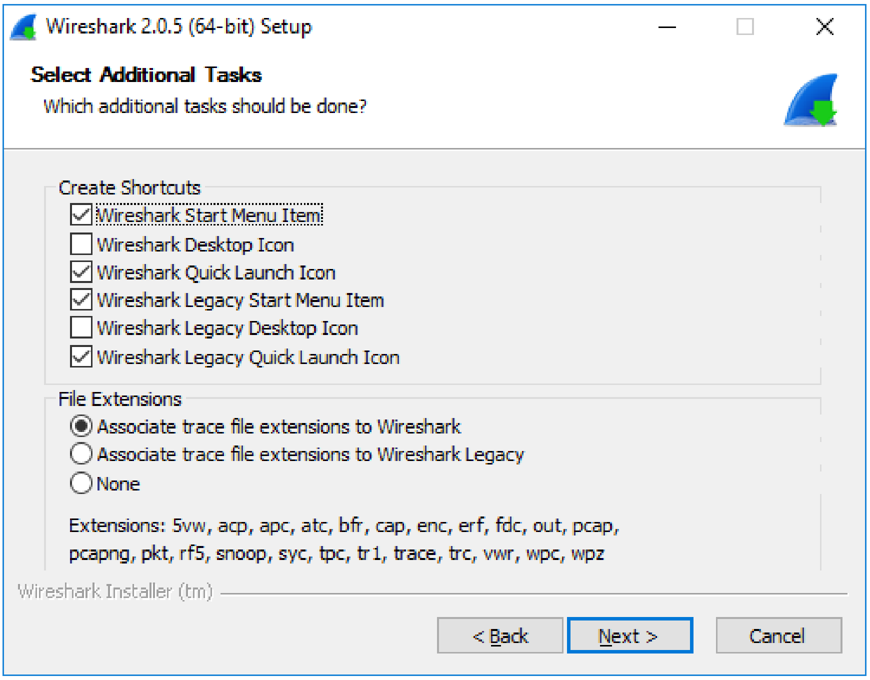
Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

d. Continue advancing through the installation process. Click **I Agree** when the License Agreement window displays.

e. Keep the default settings on the Choose Components window and click **Next**.

f. Choose your desired shortcut options and click **Next**.



Wireshark 2.0.5 (64-bit) Setup

Select Additional Tasks

Which additional tasks should be done?

Create Shortcuts

☑ Wireshark Start Menu Item
□ Wireshark Desktop Icon
☑ Wireshark Quick Launch Icon
☑ Wireshark Legacy Start Menu Item
□ Wireshark Legacy Desktop Icon
☑ Wireshark Legacy Quick Launch Icon

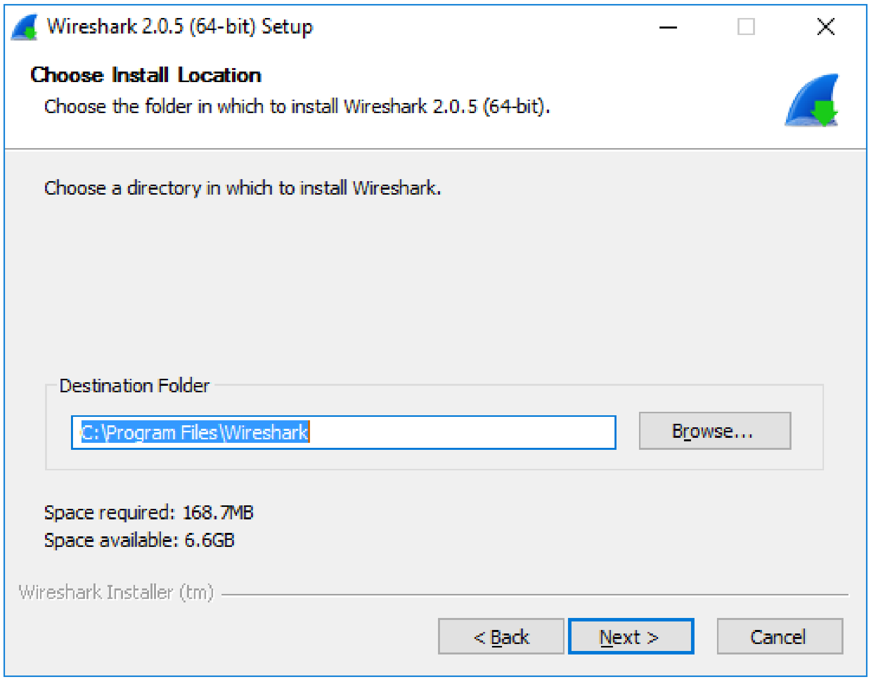
File Extensions

● Associate trace file extensions to Wireshark
○ Associate trace file extensions to Wireshark Legacy
○ None

Extensions: 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, out, pcap, pcapng, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, wpz

Wireshark Installer (tm)

g. You can change the installation location of Wireshark, but unless you have limited disk space, it is recommended that you keep the default location.



Wireshark 2.0.5 (64-bit) Setup

Choose Install Location

Choose the folder in which to install Wireshark 2.0.5 (64-bit).

Choose a directory in which to install Wireshark.

Destination Folder

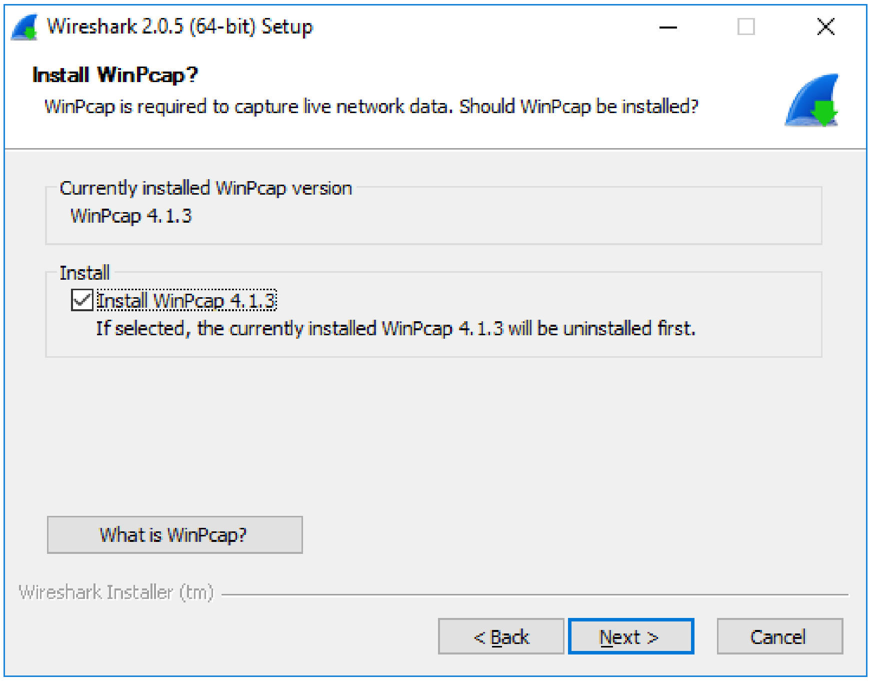
C:\Program Files\Wireshark

Space required: 168.7MB

Space available: 6.6GB

h. To capture live network data, WinPcap must be installed on your PC. If WinPcap is already installed on your PC, the Install check box will be unchecked. If your installed version of WinPcap is older than the version that comes with Wireshark, it is recommend that you allow the newer version to be installed by clicking the **Install WinPcap x.x.x** (version number) check box.

Finish the WinPcap Setup Wizard if installing WinPcap.



Wireshark 2.0.5 (64-bit) Setup

Install WinPcap?

WinPcap is required to capture live network data. Should WinPcap be installed?

Currently installed WinPcap version

WinPcap 4.1.3

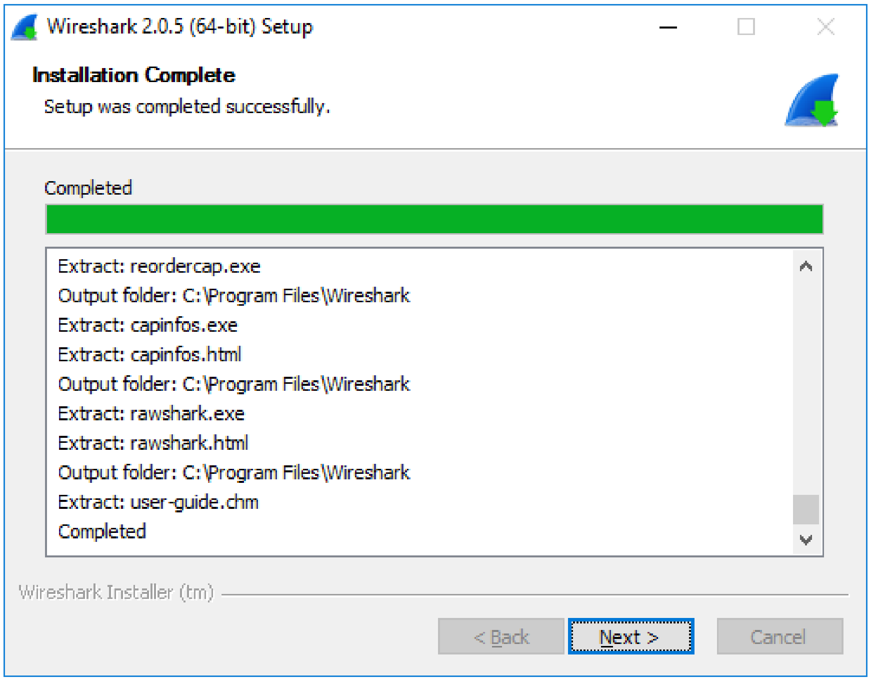
Install

☑ Install WinPcap 4.1.3

If selected, the currently installed WinPcap 4.1.3 will be uninstalled first.

Note: You maybe prompted to install USBPcap. The installation of USBPcap is optional.

i. Wireshark starts installing its files and a separate window displays with the status of the installation. Click **Next** when the installation is complete.



Wireshark 2.0.5 (64-bit) Setup

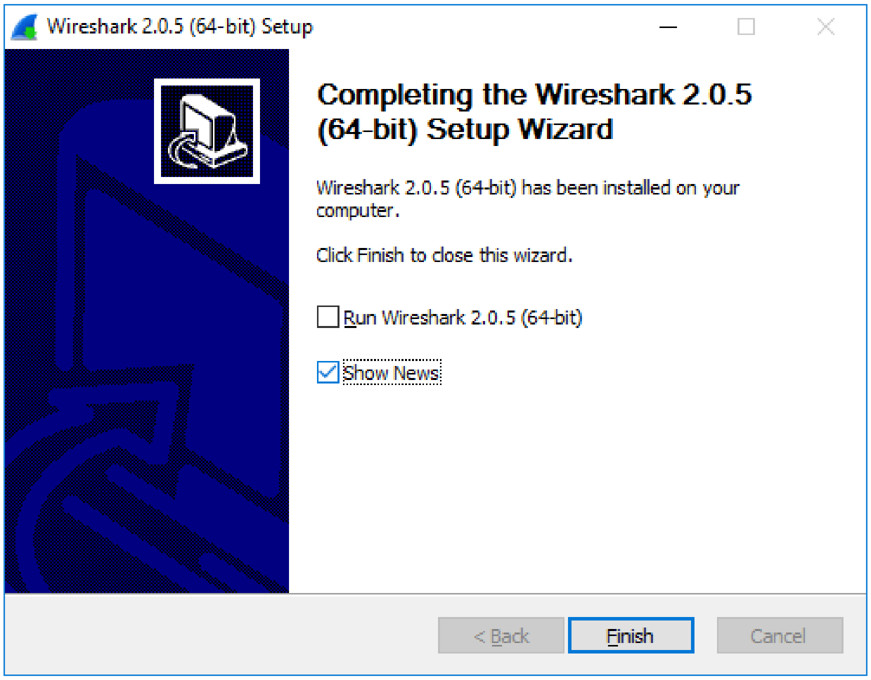
Installation Complete

Setup was completed successfully.

Completed

```
Extract: reordercap.exe
Output folder: C:\Program Files\Wireshark
Extract: capinfos.exe
Extract: capinfos.html
Output folder: C:\Program Files\Wireshark
Extract: rawshark.exe
Extract: rawshark.html
Output folder: C:\Program Files\Wireshark
Extract: user-guide.chm
Completed
```

j. Click **Finish** to complete the Wireshark install process.



Wireshark 2.0.5 (64-bit) Setup

Completing the Wireshark 2.0.5 (64-bit) Setup Wizard

Wireshark 2.0.5 (64-bit) has been installed on your computer.

Click Finish to close this wizard.

☐ Run Wireshark 2.0.5 (64-bit)

☑ Show News

Part 2: Capture and Analyze Local ARP Data in Wireshark

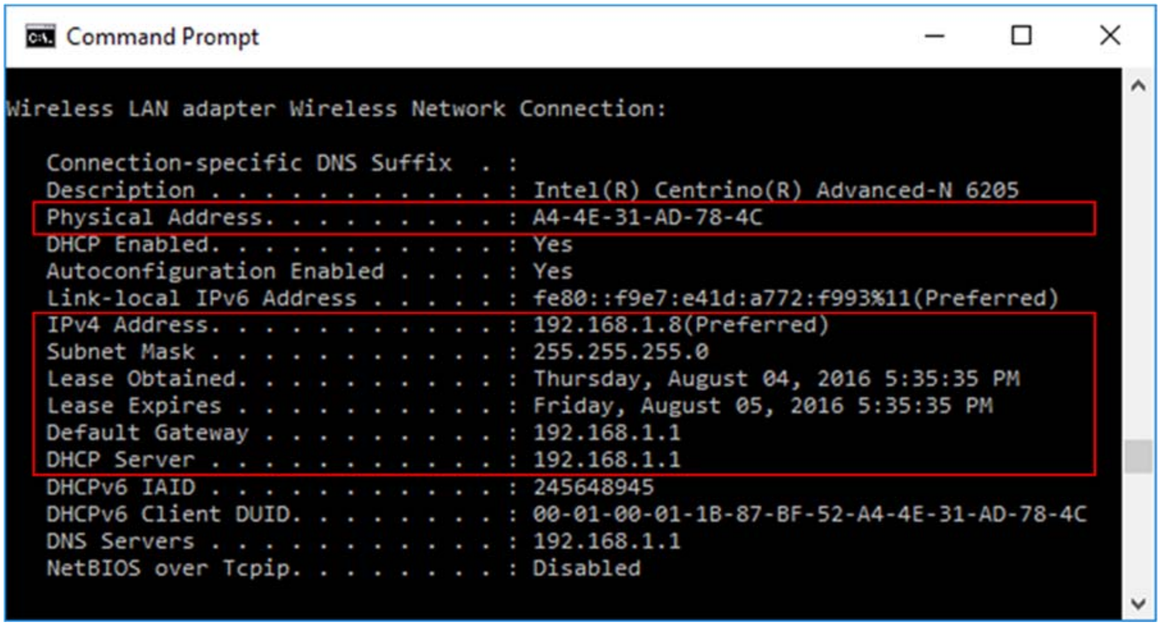
In Part 2 of this lab, you will ping another PC on the LAN and capture ARP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

Step 1: Retrieve your PC's interface addresses.

For this lab, you will need to retrieve your PC's IPv4 address and the MAC address.

a. Open a command window, type **ipconfig /all**, and then press Enter.

b. Note which network adapter that the PC is using to access the network. Record your PC interface's IPv4 address and MAC address (Physical Address).



```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6205
   Physical Address. . . . . . . . . : A4-4E-31-AD-78-4C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f9e7:e41d:a772:f993%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, August 04, 2016 5:35:35 PM
   Lease Expires . . . . . . . . . . : Friday, August 05, 2016 5:35:35 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 245648945
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-87-BF-52-A4-4E-31-AD-78-4C
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Disabled
```

c. Ask a team member for their PC's IPv4 address and give your PC's IPv4 address to them. Do not provide them with your MAC address at this time.

Record the IPv4 addresses of the default gateway and the other PCs on the LAN.

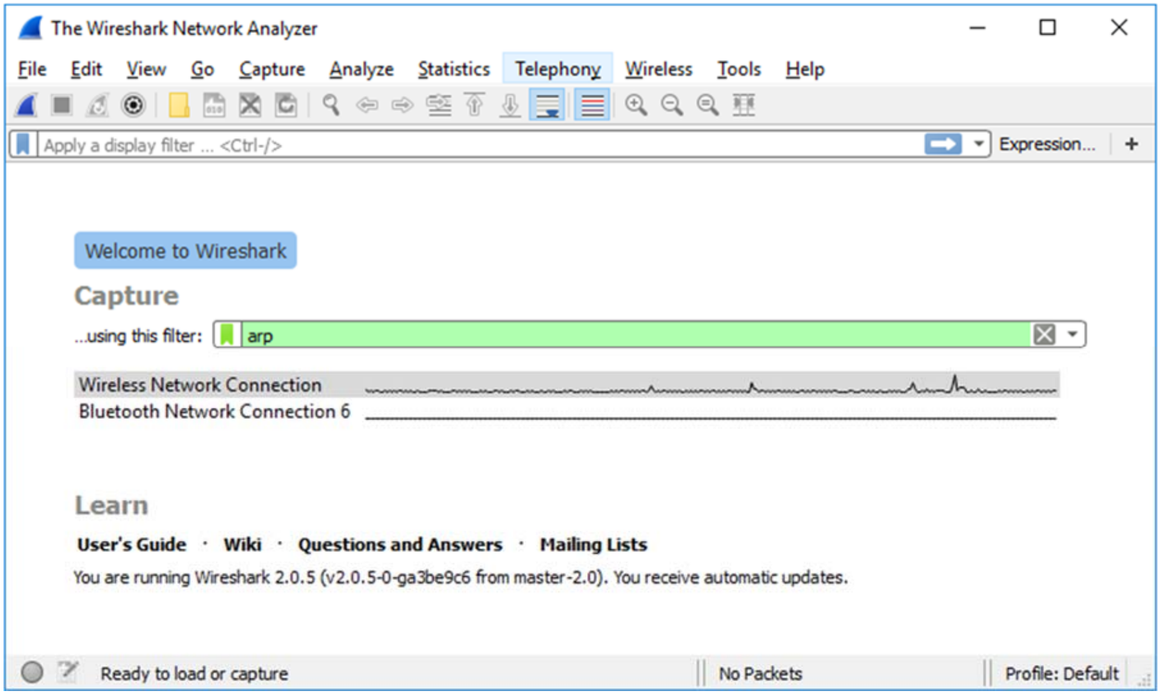
____

Step 2: Start Wireshark and begin capturing data.

a. On your PC, click **Start** and type **Wireshark**. Click **Wireshark Desktop App** when it appears in the search results window.

Note: Alternatively, your installation of Wireshark may also provide a Wireshark Legacy option. This displays Wireshark in the older but widely recognized GUI. The remainder of this lab was completed using the newer Desktop App GUI.

b. After Wireshark starts, select the network interface that you identified with the **ipconfig** command. Enter **arp** in the filter box. This selection configures Wireshark to only display packets that are part of the ARP exchanges between the devices on the local network.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Welcome to Wireshark
Capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

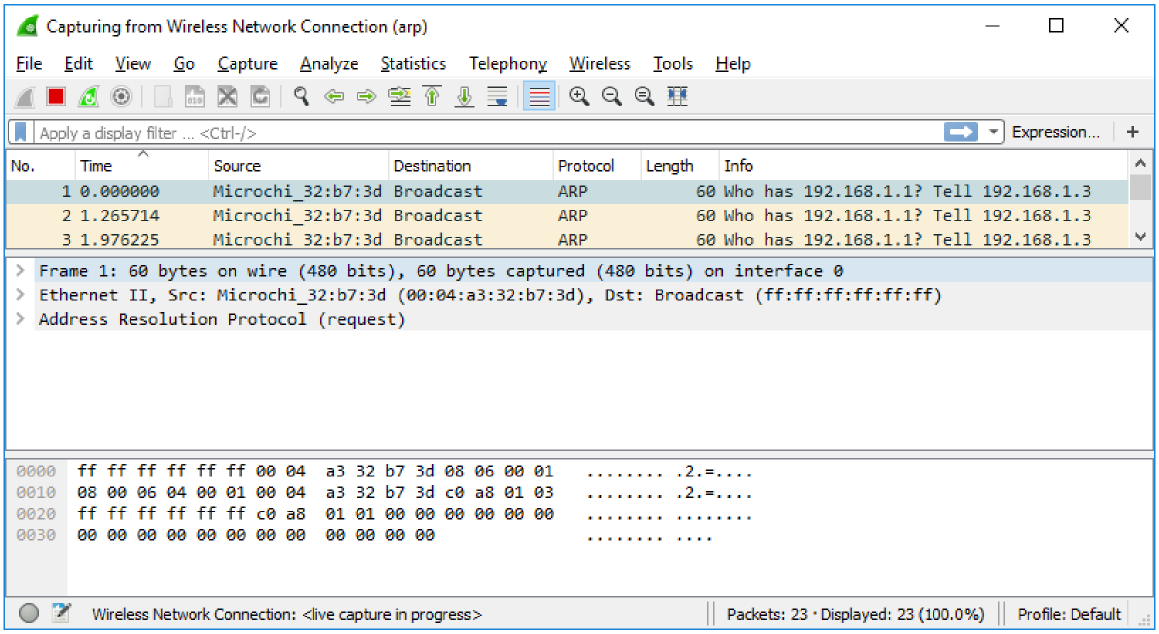
...using this filter: arp

Wireless Network Connection
Bluetooth Network Connection 6

You are running Wireshark 2.0.5 (v2.0.5-0-ga3be9c6 from master-2.0). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

c. After you have selected the correct interface and entered the filter information, click **Start** ( ) to begin the data capture. Information will start scrolling down the top section in Wireshark. Each line represents a message being sent between a source and destination device on the network.


Capturing from Wireless Network Connection (arp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

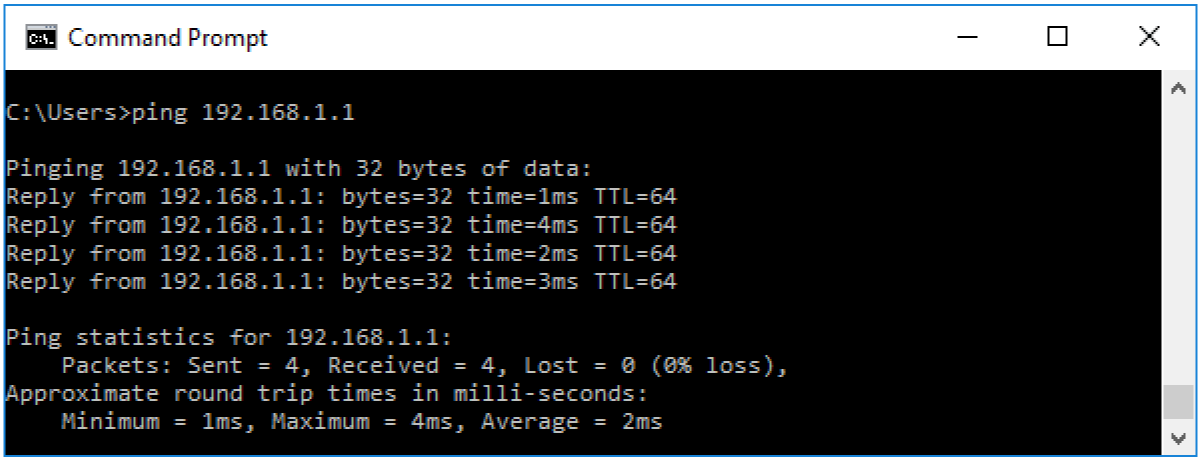
```
No.  Time      Source             Destination  Protocol  Length  Info
   1 0.000000  Microchi_32:b7:3d  Broadcast    ARP           60  Who has 192.168.1.1? Tell 192.168.1.3
   2 1.265714  Microchi_32:b7:3d  Broadcast    ARP           60  Who has 192.168.1.1? Tell 192.168.1.3
   3 1.976225  Microchi_32:b7:3d  Broadcast    ARP           60  Who has 192.168.1.1? Tell 192.168.1.3
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Microchi_32:b7:3d (00:04:a3:32:b7:3d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 04  a3 32 b7 3d 08 06 00 01   ........ .2.=....
0010  08 00 06 04 00 01 00 04  a3 32 b7 3d c0 a8 01 03   ........ .2.=....
0020  ff ff ff ff ff ff c0 a8  01 01 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Wireless Network Connection: <live capture in progress> | Packets: 23 · Displayed: 23 (100.0%) | Profile: Default

d. Open a command prompt window. Use the **ping** command to test connectivity to the default gateway address that you identified in Part 2, step 1c.



```
C:\Users>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 2ms
```

e. Ping the IPv4 addresses of other PCs on the LAN that were provided to you by your team members.

Note: If your team member's PC does not reply to your pings, this may be because their PC firewall is blocking these requests. Ask your instructor for assistance if necessary to disable the PC firewall.

f. Stop capturing data by clicking **Stop Capture (**■**)** on the toolbar.

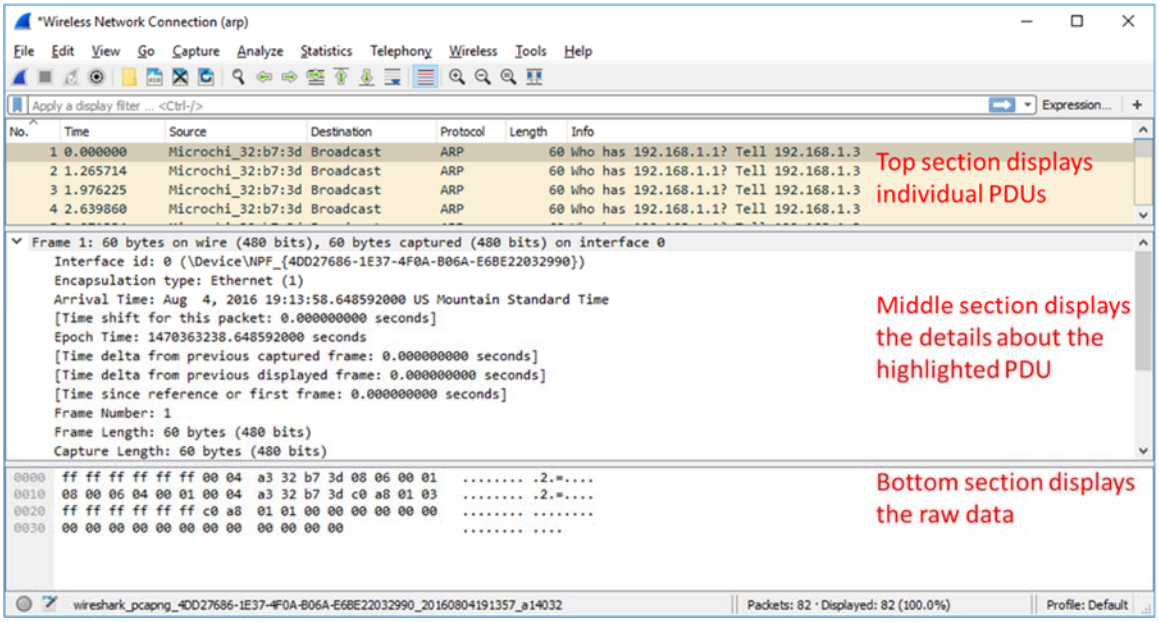
Step 3: Examine the captured data.

In Step 3, examine the data that was generated by the **ping** requests of your team member's PC. Wireshark data is displayed in three sections:

1) The top section displays the list of PDU frames captured with a summary of the IPv4 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. The raw data is displayed in both hexadecimal and decimal form.


*Wireless Network Connection (arp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time       Source             Destination  Protocol  Length  Info
   1 0.000000   Microchi_32:b7:3d  Broadcast    ARP           60  Who has 192.168.1.1? Tell 192.168.1.3
   2 1.265714   Microchi_32:b7:3d  Broadcast    ARP           60  Who has 192.168.1.1? Tell 192.168.1.3
   3 1.976225   Microchi_32:b7:3d  Broadcast    ARP           60  Who has 192.168.1.1? Tell 192.168.1.3
   4 2.639860   Microchi_32:b7:3d  Broadcast    ARP           60  Who has 192.168.1.1? Tell 192.168.1.3
```

Top section displays individual PDUs

```
v Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
     Interface id: 0 (\Device\NPF_{4DD27686-1E37-4F0A-B06A-E6BE22032990})
     Encapsulation type: Ethernet (1)
     Arrival Time: Aug  4, 2016 19:13:58.648592000 US Mountain Standard Time
     [Time shift for this packet: 0.000000000 seconds]
     Epoch Time: 1470363238.648592000 seconds
     [Time delta from previous captured frame: 0.000000000 seconds]
     [Time delta from previous displayed frame: 0.000000000 seconds]
     [Time since reference or first frame: 0.000000000 seconds]
     Frame Number: 1
     Frame Length: 60 bytes (480 bits)
     Capture Length: 60 bytes (480 bits)
```

Middle section displays the details about the highlighted PDU

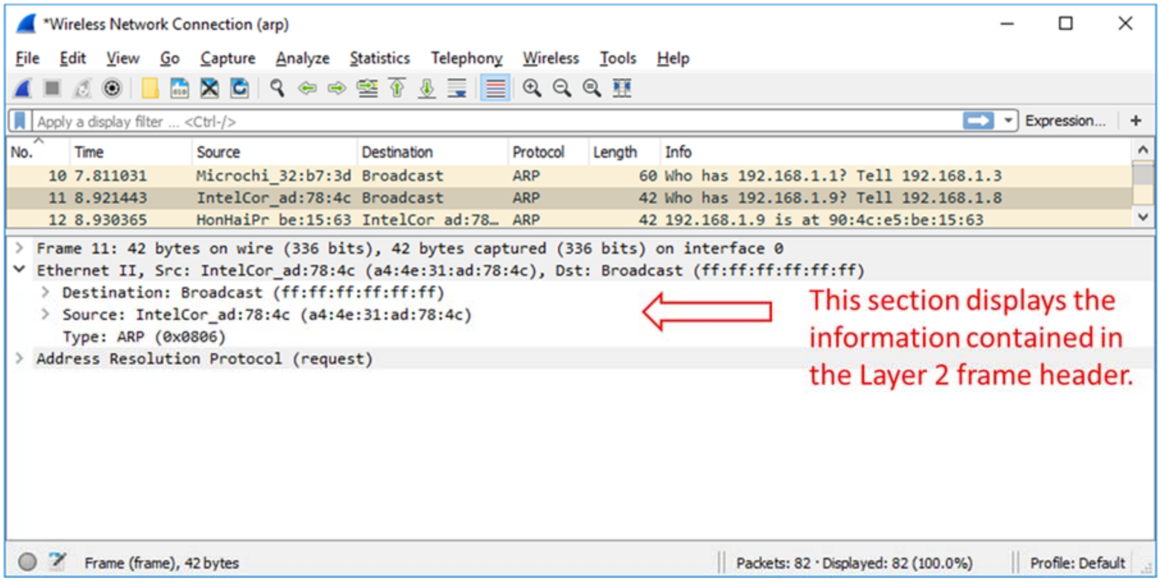
```
0000  ff ff ff ff ff ff 00 04  a3 32 b7 3d 08 06 00 01   ........ .2.=....
0010  08 00 06 04 00 01 00 04  a3 32 b7 3d c0 a8 01 03   ........ .2.=....
0020  ff ff ff ff ff ff c0 a8  01 01 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Bottom section displays the raw data

```
wireshark_pcapng_4DD27686-1E37-4F0A-B06A-E6BE22032990_20160804191357_a14032 | Packets: 82 · Displayed: 82 (100.0%) | Profile: Default
```

a. Click one of the ARP frames in the top section that has your PC MAC address as the source address in the frame and "broadcast" as the destination of the frame.

b. With this PDU frame still selected in the top section, navigate to the middle section. Click the arrow to the left of the Ethernet II row to view the Destination and Source MAC addresses.


*Wireless Network Connection (arp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time       Source             Destination       Protocol  Length  Info
  10 7.811031   Microchi_32:b7:3d  Broadcast         ARP           60  Who has 192.168.1.1? Tell 192.168.1.3
  11 8.921443   IntelCor_ad:78:4c  Broadcast         ARP           42  Who has 192.168.1.9? Tell 192.168.1.8
  12 8.930365   HonHaiPr_be:15:63  IntelCor_ad:78…   ARP           42  192.168.1.9 is at 90:4c:e5:be:15:63
```

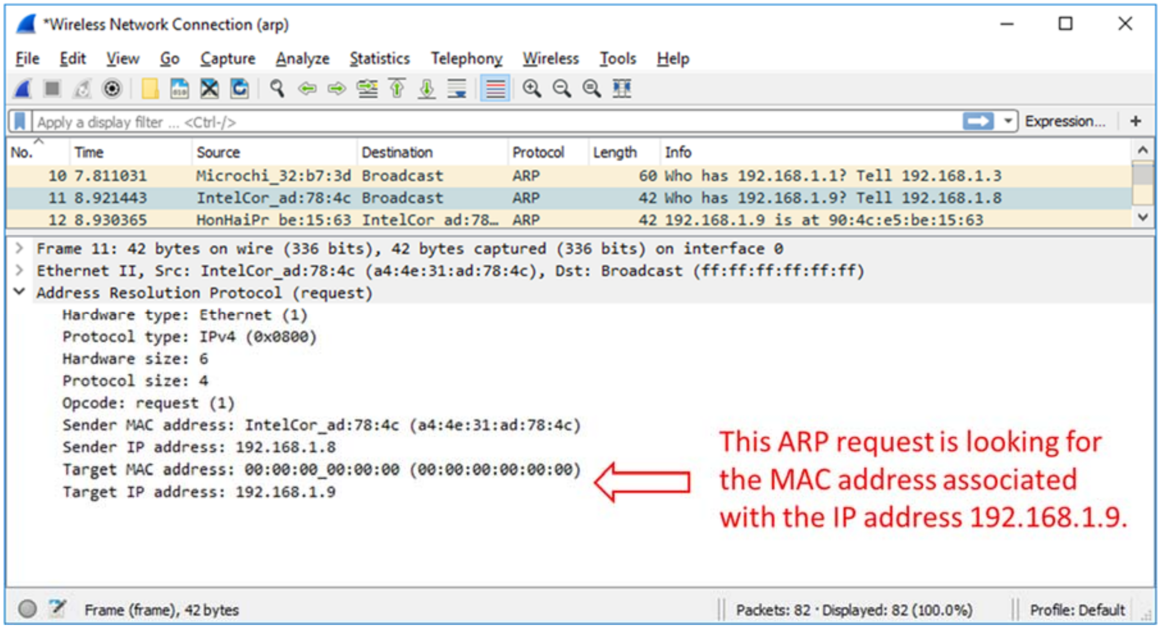
```
> Frame 11: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
v Ethernet II, Src: IntelCor_ad:78:4c (a4:4e:31:ad:78:4c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
   > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   > Source: IntelCor_ad:78:4c (a4:4e:31:ad:78:4c)
     Type: ARP (0x0806)
> Address Resolution Protocol (request)
```

This section displays the information contained in the Layer 2 frame header.

```
Frame (frame), 42 bytes | Packets: 82 · Displayed: 82 (100.0%) | Profile: Default
```

Does the Source MAC address match your PC's interface? ______________________________

c. Click the arrow to the left of the Address Resolution Protocol (request) row to view the content of the ARP request.


*Wireless Network Connection (arp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time       Source            Destination      Protocol  Length  Info
  10 7.811031   Microchi_32:b7:3d Broadcast        ARP           60  Who has 192.168.1.1? Tell 192.168.1.3
  11 8.921443   IntelCor_ad:78:4c Broadcast        ARP           42  Who has 192.168.1.9? Tell 192.168.1.8
  12 8.930365   HonHaiPr_be:15:63 IntelCor_ad:78…  ARP           42  192.168.1.9 is at 90:4c:e5:be:15:63

> Frame 11: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: IntelCor_ad:78:4c (a4:4e:31:ad:78:4c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_ad:78:4c (a4:4e:31:ad:78:4c)
    Sender IP address: 192.168.1.8
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.9
```

This ARP request is looking for the MAC address associated with the IP address 192.168.1.9.

Frame (frame), 42 bytes | Packets: 82 · Displayed: 82 (100.0%) | Profile: Default

Step 4: Locate the ARP response frame that corresponds to the ARP request that you highlighted.

a. Using the Target IPv4 address in the ARP request, locate the ARP response frame in the upper section of the Wireshark capture screen.

What is the IPv4 address of the Target device in your ARP request? ____________________

b. Highlight the response frame in the upper section of the Wireshark output. You may have to scroll the window to find the response frame that matches the Target IPv4 address identified in the previous step. Expand the Ethernet II and Address Resolution Protocol (response) rows in the middle section of the screen.

Is the ARP response frame a broadcast frame? ____________________

What is the destination MAC address of the frame? ____________________

Is this the MAC address of your PC? ____________________

What MAC address is the source of the frame? ____________________

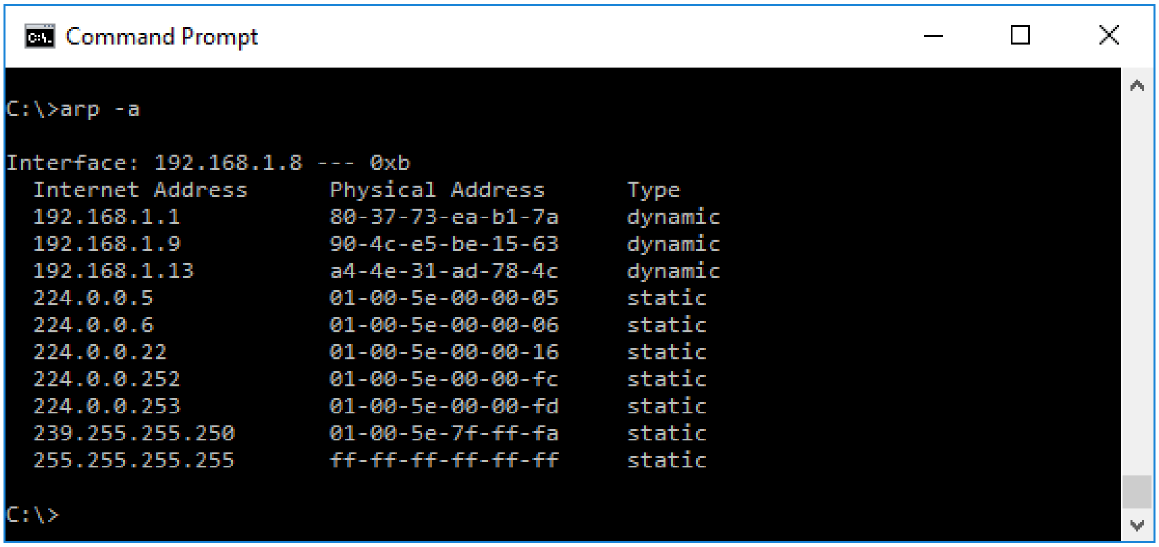
c. Verify with your team member that the MAC address matches the MAC address of their PC.

Part 3: Examine the ARP cache entries on the PC.

After the ARP reply is received by the PC, the MAC Address to IPv4 address association is stored in cache memory on the PC. These entries will stay in memory for a short period of time (from 15 to 45 seconds), then, if they are not used within that time, they will be removed from cache.

Step 1: View ARP cache entries on a Windows PC.

a. Open a command prompt window on the PC. At the prompt, enter **arp –a** and press enter.



```
C:\>arp -a

Interface: 192.168.1.8 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           80-37-73-ea-b1-7a     dynamic
  192.168.1.9           90-4c-e5-be-15-63     dynamic
  192.168.1.13          a4-4e-31-ad-78-4c     dynamic
  224.0.0.5             01-00-5e-00-00-05     static
  224.0.0.6             01-00-5e-00-00-06     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\>
```

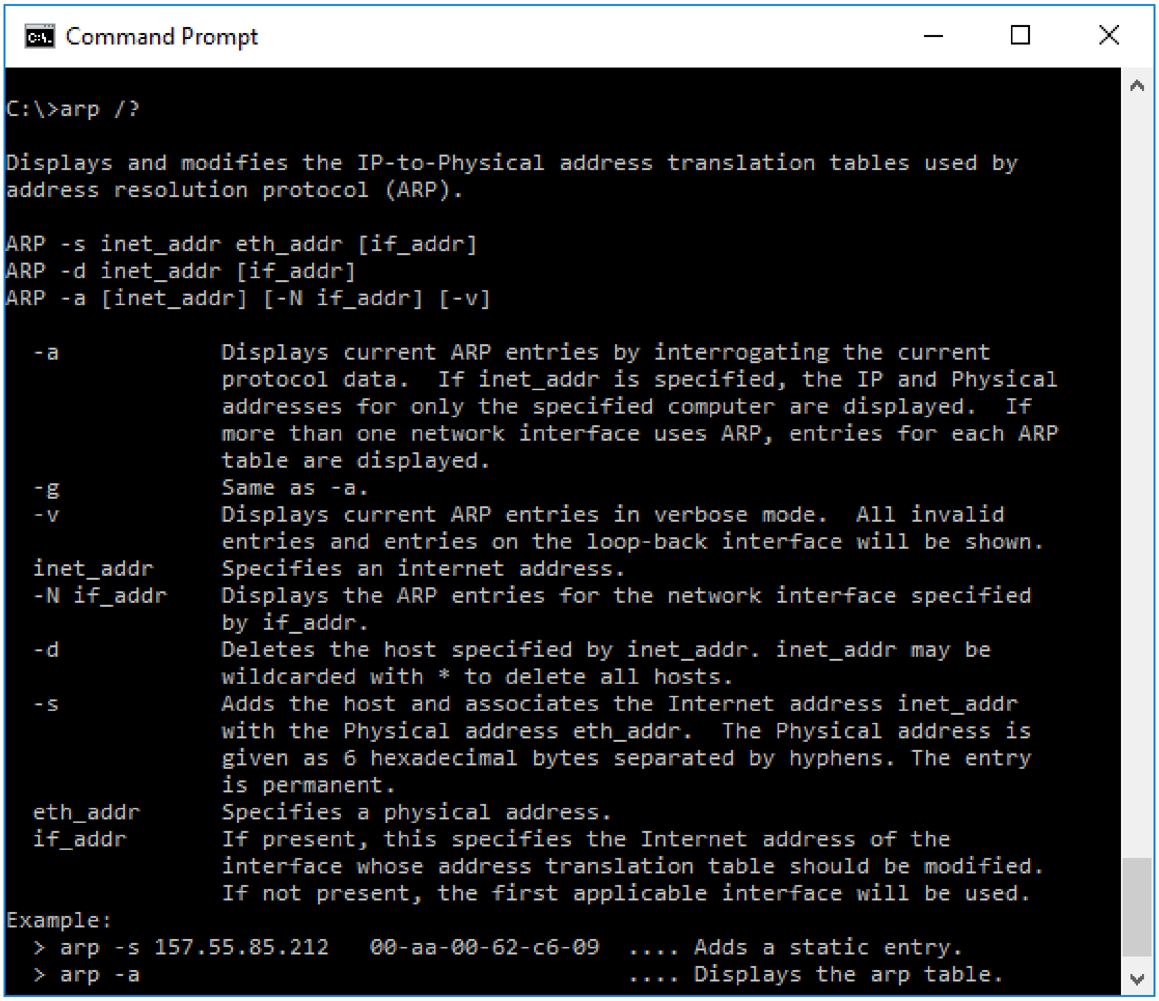
The output of the **arp –a** command displays the entries that are in the cache on the PC. In the example, the PC has entries for the default gateway (192.168.1.1) and for two PCs that are located on the same LAN (192.168.1.9 and 192.168.1.13).

What is the result of executing the **arp –a** command on your PC?

____

____

b. The **arp** command on the Windows PC has another functionality. Enter **arp /?** at the command prompt and press enter. The **arp** command options enable you to view, add and remove ARP table entries if necessary.



```
C:\>arp /?

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

Which option deletes an entry from the ARP cache? ______________________________________

What would be the result of issuing the **arp –d *** command? ________________________________

Reflection

1. What is a benefit of keeping ARP cache entries in memory on the source computer?

____

____

2. If the destination IPv4 address is not located on the same network as the source host, what MAC address will be used as the destination target MAC address in the frame?

____

____