# Computer Networks

|  |  |  |
| --- | --- | --- |
|  | At-home Lab1 |  |

For this assignment, you have to use **Wireshark**, a packet analyzer available for free download and use. .

**College Policy**. Please be aware that The College at Brockport’s Internet Use Policy prohibits capture of network traffic on campus network. Violations may lead to serious consequences. In this and other laboratory exercises, you will only analyze captured traffic.

**Wireshark**. Wireshark relies on a packet capture library such as libpcap or WinPCap that is sometimes installed within an operating system. To run the packet capture component, you need to access to your network interfaces, and hence you need administrative rights on your machine. Thus, capturing network traffic using the PCs in Drake classrooms is not possible. On the other hand, a packet analyzer merely displays the contents of all fields in a message. In order to do so, the analyzer must know the structure of messages transmitted with various protocols. Indeed, Wireshark is a very versatile and popular tool that there is a certification examination – Wireshark Certified Network Analyst.

1. **Download and install WirsharkPortable on your P: Drive**.
2. Use Chrome browser to download **Windows PortableApps (32-bit)**. Note that it was originally downloaded from <https://www.wireshark.org/#download> and the latest version is fine for the assignment.
3. Create a folder named Wireshark on your P: drive. Create a subfolder named Download under P:\Wireshark. Copy the downloaded the latest WiresharkPortable file to the folder P:\Wireshark\Download. (Right click the tab for the downloaded file, and select show in a folder. The executable file will be shown in the download folder. Copy the file and paste it on P:\Wireshark\Download.)
4. Now that we have downloaded an executable file, we want to be sure that it does not have any virus content and has not been tampered with.

To verify that the file has not been tampered with check its SHA-256 hash. Open a command window and type the following command (x should be replaced by the corresponding version). You will see the SHA256 hash value for data integrity test.

**certutil –hashfile P:\Wireshark\Download\WiresharkPortable\_x.x.x.paf.exe SHA256**

**SHA256 hash of C:\Wireshark\Download\Wireshark-win64-4.0.5.exe:**

**3164b91cc3f08268a795090c8478fcf80e741d3e620f06e8441e0f9d4418ac4f**

**CertUtil: -hashfile command completed successfully.**

1. Double-click the WiresharkPortable executable file in the folder P:\Wireshark\Download. It will begin the installation of Wireshark. Indicate the **Destination Folder** as: **P:\Wireshark\WiresharkPortable**
2. Finish the installation. Under P:\Wireshark\WiresharkPortable you will see and executable named **WiresharkPortable.exe** for the packet analyzer.

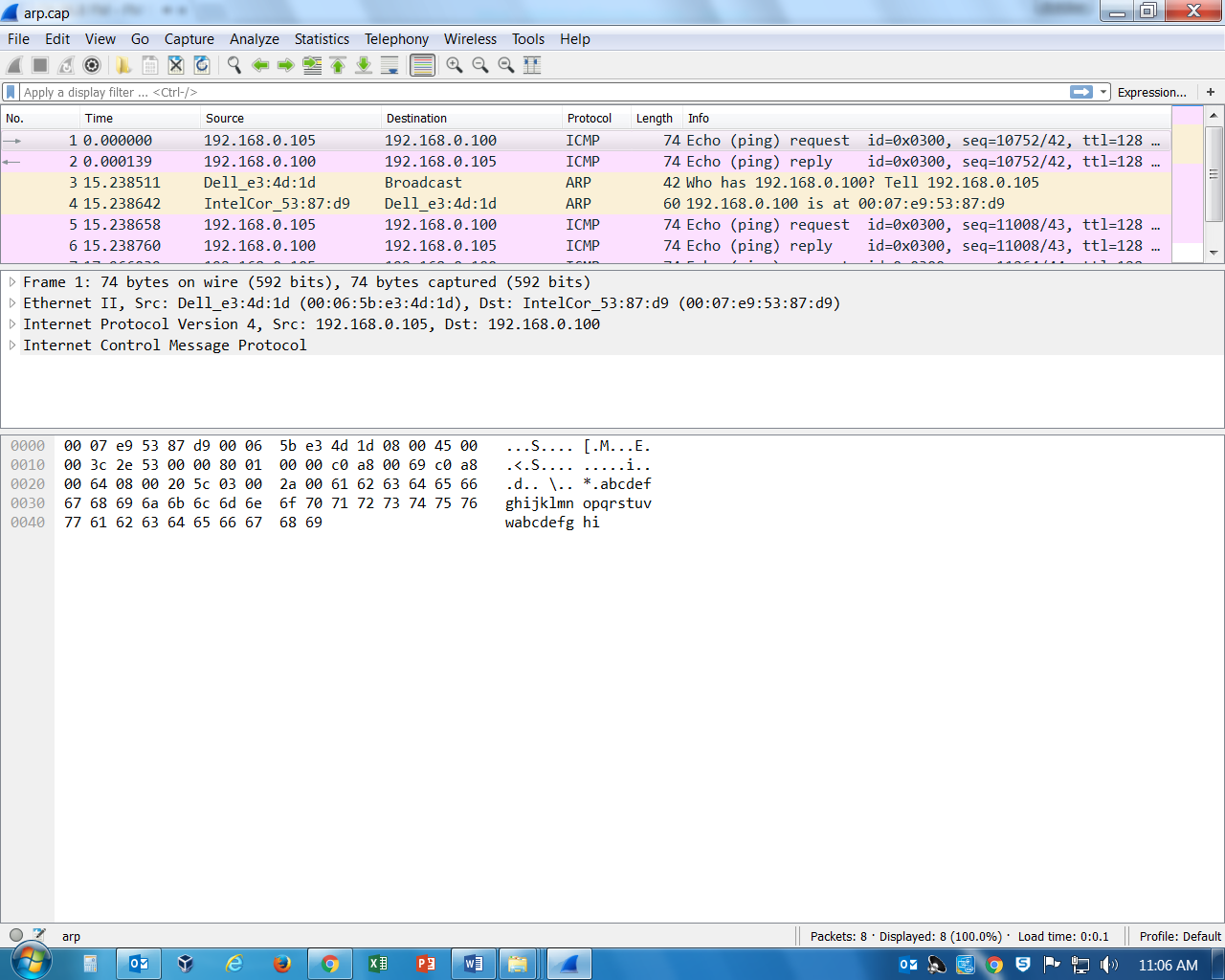
Did you successfully install WiresharkPortable?

Yes

If you have difficulties, please see me in person during office hours.

1. **Download network traffic file from Blackboard**.
2. Create a subfolder named CaptureFile under P:\Wireshark.
3. Access Blackboard. See Assignments Folder. Download the captured file arp.cap and copy it into the folder named P:\Wireshark\CaptureFile
4. **Launch Wireshark**.
5. Open the folder P:\Wireshark\WiresharkPortable and launch WoresharkPortable.exe by double clicking it.
6. A window with a message “**Welcome to Wireshark**” will appear. It may ask you for some information regarding data capture. Remember that we do not have administrative rights on Drake classroom PCs and do not plan to capture network traffic.
7. Open the data file P:\Wireshark\CaptureFile\arp.cap. You will see a window as shown below, showing exactly **eight** date frames.

Unfortunately, Wireshark, Ethernet, and many more data link layer technology will use the term “**packet**” even though they should technically use the term “**frame**”. In other words, terms such as “Wireshark packet”, “Ethernet packet”, etc., are quite common in the literature. So, we will also use that terminology, even though that is not desirable.



**Wireshark Interface**. Wireshark interface has five major parts.

1. **Command menus**. On the top of the window are the command menus, similar to many Windows programs. I strongly recommend that you explore the options carefully so you are aware of them.
2. **Filter**. Immediately below is a small box labeled **filter**. It is used to specify packet display filter option.
3. **Packet listing**. This part displays one-line summary of each packet, including a number and time of capture, source, destination, protocol type, etc. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highest-level protocol that sent or received this packet.
4. **Packet detail**. This part provides all the information about the selected packet. The amount of information displayed is controlled (i.e., expanded or minimized) by clicking the “►” and “▼” as appropriate.
5. **Packet content**. This part displays the packet content in hexadecimal and ASCII. (Non displayable characters are shown with a dot.)

You may adjust the size of the last three parts as needed, by dragging the boundary lines.

**Data Capture Setup**. For this exercise we connected two machines – a desktop and a laptop to an Ethernet switch. They were both assigned static IP addresses and ensured that they can communicate with each other. The network traffic was captured on the desktop, and the following commands were issued on the desktop, one by one, before the capture was closed.

**ping –n 1 192.168.0.100 // ping the laptop just once**

**arp -d 192.168.0.100 // delete the arp entry relating**

**// to laptop from cache**

**ping –n 1 192.168.0.100 // ping the laptop just once**

**ping –n 1 192.168.0.100 // ping the laptop just once**

The first command causes flow of two packets, the **ping** from the desktop and the reply from the laptop. The second command causes the cache entry relating to the laptop to be deleted from the **arp** cache of the desktop and does not cause any network traffic. The next ping requires the desktop to determine the physical (MAC) address of the laptop before the **ping** can be sent on the local area network. This causes an **arp** request and an **arp** reply. Once the physical address (MAC) address of the laptop has been determined, the **ping** is sent and the replied is received. Thus, the third command causes four packets to flow. The fourth command adds two more packets to the capture because the physical (MAC) address of the laptop is known. Thus, the capture includes exactly eight Wireshark packets.

The physical (MAC) address is used to identify a device interface in a local area network and deliver a frame. The IP address is used to identify a device interface in an internet – a network of networks – and deliver a packet.

The purpose of the **address resolution protocol** (ARP) is to help find an interface’s MAC address from its IP address. The purpose of the **reverse address resolution protocol** (RARP) is to help find an interface’s IP address from its MAC address.

A local area network Ethernet frame in which the destination physical (MAC) address is set to ff:ff:ff:ff:ff:ff (i.e., all 48 bits of one) is called a **broadcast address** as it is intended for all device interfaces on the local area network.

1. **Analyze the capture file**.
2. Use Wireshark Statistics-Capture File Properties to report

Date and time of capture of first packet:

Jan 25, 2035 15:30:00.240835000 Eastern Standard Time

Date and time of capture of last packet:

Jan 25, 2035 15:30:18.207010000 Eastern Standard Time

Number of packets captured and displayed: 8 packets

Average size of the packets (in bytes): 74 bytes

1. Select the **third** packet in the packet listing. (It is the ARP request packet). In the packet detail, expand at various levels as appropriate and determine the following.

Frame length: Frame Length: 42 bytes (336 bits)

Protocols in frame: [Protocols in frame: eth:ethertype:arp]

Ethernet destination MAC address: Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Ethernet source MAC address: Source: Dell\_e3:4d:1d (00:06:5b:e3:4d:1d)

Is this ARP request a broadcast on the LAN? Yes

Ethernet packet type and what it stands for: Type: ARP (0x0806)

ARP type: ARP (0x0806)

ARP sender MAC address: Dell\_e3:4d:1d (00:06:5b:e3:4d:1d)

ARP sender IP address: IP address: 192.168.0.105

ARP target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)

ARP target IP address: 192.168.0.100

Why is target MAC address all zero? It cannot map to the Target IP address. This is intentional, because the reason for sending the ARP Probe is to prevent an IP conflict.

1. Select the **fourth** packet in the packet listing. (It is the ARP reply packet). In the packet detail, expand at various levels as appropriate and determine the following.

Frame length: Frame Length: 60 bytes (480 bits)

Protocols in frame: [Protocols in frame: eth:ethertype:arp]

Ethernet destination MAC address: Destination: Dell\_e3:4d:1d (00:06:5b:e3:4d:1d)

Ethernet source MAC address: Source: Intel\_53:87:d9 (00:07:e9:53:87:d9)

Is this ARP frame a broadcast on the LAN? No

Ethernet packet type and what it stands for: ARP (0x0806)

Address Resolution Protocol

ARP type: Type: ARP (0x0806)

Address Resolution Protocol

ARP sender MAC address: Intel\_53:87:d9 (00:07:e9:53:87:d9)

ARP sender IP address:192.168.0.100

ARP target MAC address: Dell\_e3:4d:1d (00:06:5b:e3:4d:1d)

ARP target IP address: 192.168.0.105

1. Knowing that the desktop initiated the ARP resolution, summarize your findings:

Desktop MAC address: 00:06:5b:e3:4d:1d

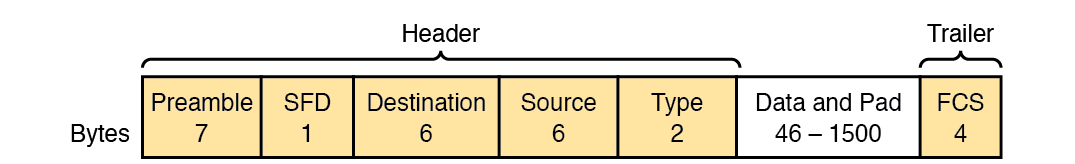
Desktop IP address: 192.168.0.105

Laptop MAC address: Destination: 00:07:e9:53:87:d9

Laptop IP address: 192.168.0.100

1. **Ethernet Frame Format**

An Ethernet frame has the following structure:



When Wireshark records the data frame in its capture file, the preamble, SFD, pad, and FCS are stripped out. So, if we look at an Ethernet header in Wireshark, you should see Destination MAC address, Source MAC address, and frame type only. The data given to the data link layer by the network layer will follow.

1. Select the **first** packet in the packet listing. Minimize at all levels in the packet detail window.

Click on the line marked Ethernet II. The header part of the Ethernet packet will be highlighted in the packet content window. (Remember that the content of interest is displayed in hexadecimal on the left and interpreted in ASCII, if possible, on the right. Ignore the ASCII interpretation.)

How many bytes were highlighted? 14 bytes

What did the highlighted portion show? The Header

With the Ethernet packet format shown above, separate the highlighted portion to determine the three fields.

Ethernet destination MAC address: Intel\_53:87:d9 (00:07:e9:53:87:d9)

Ethernet source MAC address: Dell\_e3:4d:1d (00:06:5b:e3:4d:1d)

Ethernet packet type and what it stands for: IPv4 (0x0800)

Internet Protocol Version 4

1. The Ethernet packet type indicates the type of data from layer above this Ethernet packet encapsulates.

Inspect all eight Wireshark packets and look for Ethernet type. You will notice only two types in this capture. What are they and what do they stand for?

Type: IPv4 (0x0800)

Address Resolution Protocol

Type: ARP (0x0806)

Internet Protocol Version 4

1. **Ping, ICMP, and Data Encapsulation**

Ping is used to check the connectivity between two networked devices. Ping uses **Echo Request** and **Echo Reply** ICMP messages to get the job done. Ping hands this **ICMP** message to the network layer for routing to the pinged device. Thus, the ICMP message is encapsulated in an IP packet. The network layer passes this IP packet to the layer below, where the data link layer adds its own headers and trailers to make an Ethernet packet, and so on.

1. Select the **fifth** packet in the packet listing. Minimize at all levels in the packet detail window.
2. Select Internet Control Message Protocol. How long is this message? That is, how many bytes are highlighted in the packet content window?

How long is the ICMP message (in bytes)? 40 bytes

1. Select Internet Protocol Version 4. The header added by the network layer will be highlighted in the packet content window.

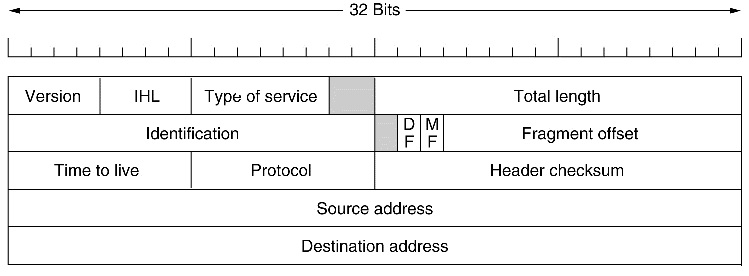
How many bytes does the IP header constitute? (only 1 byte is getting highlighted but it says the length of the header is 20 bytes

1. Select Ethernet II. The header added by the data link layer will be highlighted in the packet content window.

How many bytes does the Ethernet header constitute? 14 bytes

(Recall that Preamble, SFD, Pad, and FCS needed for transport of Ethernet packet have already been stripped out by Wireshark).

1. Again, select Internet Protocol Version 4. The header added by the network layer will be highlighted in the packet content window. Knowing the IP header format as given below, determine the following from the highlighted information.



Destination IP address (in hex): c0 a8 00 64

(in dotted decimal): 192.168.0.100

Source IP address (in hex): c0 a8 00 69

(in dotted decimal): 192.168.0.105

TTL value: (in hex) 80 (in decimal) 128

Protocol version: ICMP (in hex) 01 (in decimal) 1