Analyze Network Traffic

Scenario

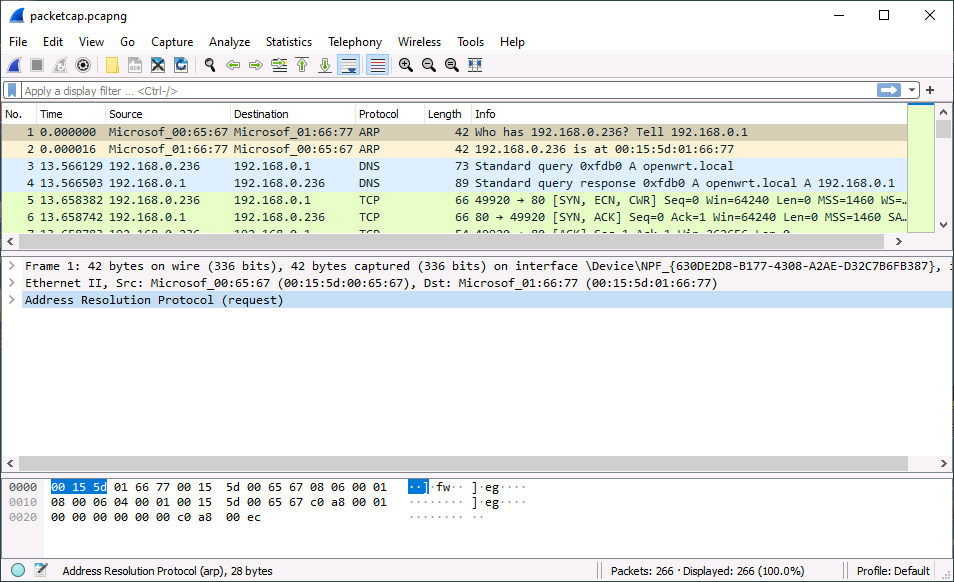
You are deploying an employee's laptop on their home network so that they can work remotely. To assist with support and to ensure security, the company asks that each home network be set up in the same way. You have recorded a sample of network traffic. Verify this to ensure that the network is operating normally and in compliance with the company's policies.

Objectives

* Identify features of network traffic and protocols.

Open packet capture

1. Sign in to the [LAPTOP](https://labclient.labondemand.com/Instructions/8ae20a5b-a1e2-477b-9ae8-11568f3c13ee) VM as **Bobby** with the password Pa$$w0rd.
2. From the desktop, open the **Wireshark** shortcut icon Wireshark desktop icon.
3. In Wireshark, select **File > Open**. From the Downloads folder, select **packetcap** and click **Open**.
4. Maximize the Wireshark window.



The file you opened contains the frames exchanged over the network in a previous session. Each frame is listed in the top pane. The middle pane contains a decoded analysis of the various protocol headers and data carried by the frame. The bottom pane shows the computer's view of the frame content as a series of bits, expressed in hex notation.

1. 

Looking at the top pane, the fields show the source and destination addresses of each frame, plus the protocol it is transporting. Which protocol is being transported in the first frame?

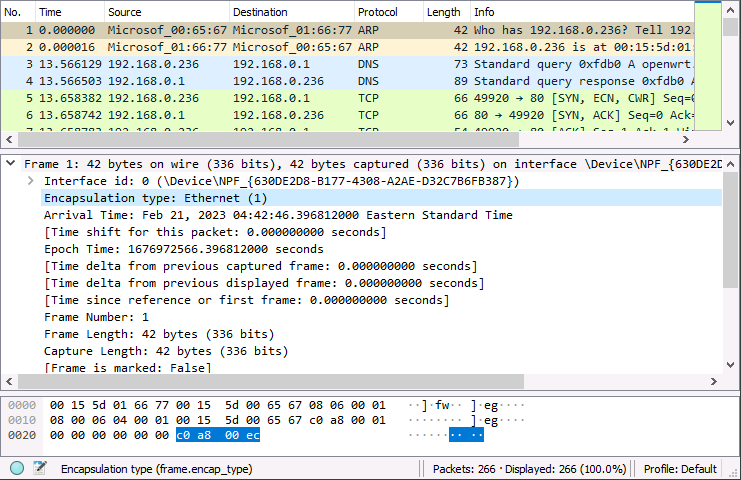


Keep the Wireshark window open for the whole of this lab.

Analyze frames

Network devices and protocols are often analyzed using a layer structure. The lowest layer is the physical one, where electrical or light signals are sent over cables or radio signals are transmitted wirelessly. The packet capture records the first "software" layer that runs on top of the physical layer, where transmissions are organized into frames of data. This is referred to as the link layer.

1. With frame #1 selected, in the middle pane, observe the first protocol summary line. Click the arrow to expand it.



The format of a frame controls the way it can carry other protocols within it. This is referred to as encapsulation.

1. 

What method of encapsulation is used for the frame?



1. Click the arrow to collapse the *Frame 1* summary line. Select the **Ethernet II** summary line.

At the link layer, interfaces are identified by Media Access Control (MAC) addresses. These are recorded in hex notation.

1. 

What is the source address of the first frame?



1. Observe the *Address Resolution Protocol* line. Note that this is identified as a request.
2. Select frame #2 and observe the following details:
   * The source and destination addresses are reversed compared to frame #1.
   * This frame is a reply to the Address Resolution Protocol request in frame #1.

Network traffic often follows this request/reply pattern.

Analyze network addresses

MAC addresses are typically tied to a specific hardware network interface. If the network card in the computer were replaced, it would have a new MAC address. This type of change would be difficult to manage in terms of administering network devices. Also, the MAC address contains no information about which logical network the computer is connected to.

These issues are mitigated by the next layer up: the network or internet layer. This layer imposes a more flexible system of logical addressing, using Internet Protocol (IP) addresses. An IP address contains information about the network ID and the host ID.

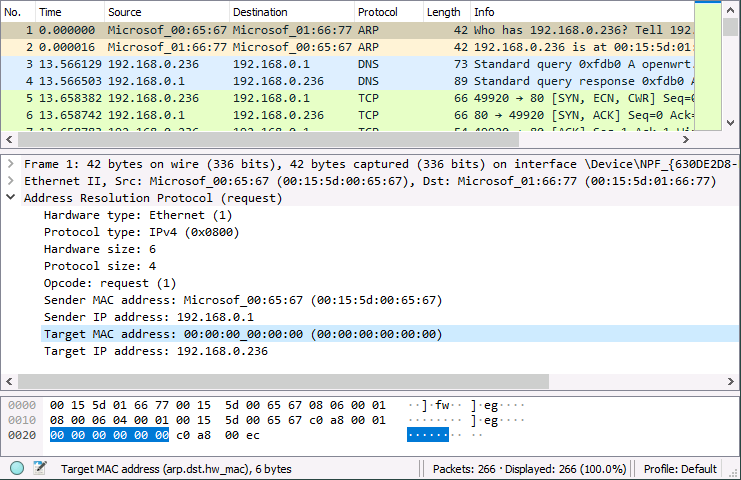
This means that there must be some way of mapping between an interface's MAC address used at the link layer and the IP address used at the network/internet layer. This mapping is performed by the Address Resolution Protocol (ARP) frames that you are examining.

1. Select frame #1 again. Observe the text in the *Info* field. The Info field summarizes the packet contents.

This is an ARP request from the host with IP 192.168.0.1 attempting to find the MAC address of the host with IP address 192.168.0.236.

1. Expand the *Address Resolution Protocol (request)* summary line.

You can now read the headers in the ARP packet.



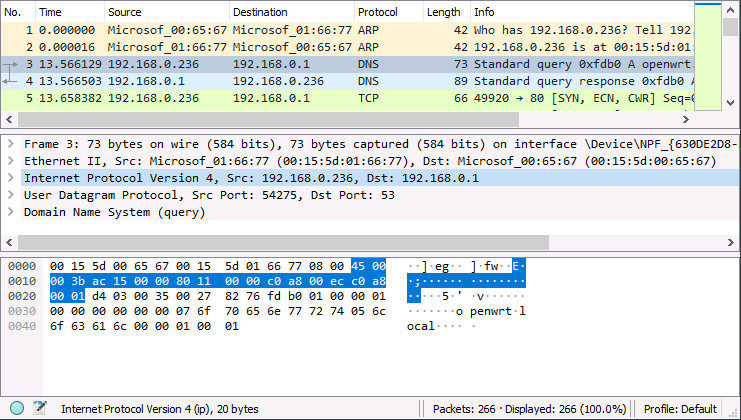
1. Observe the target MAC address.

This comprises all zeroes, meaning that the request is broadcast to all hosts on the local network.

1. Select frame #2 and expand the *Address Resolution Protocol (reply)* line.

This represents the host 192.168.0.236 replying with its MAC address (00:15:5d:00:66:77).

1. Select frame #3 and observe the following details from the middle pane:
   * The frame is still transported using Ethernet and MAC addresses at the link layer (2nd line).
   * At the network/internet layer (3rd summary line), the frame encapsulates Internet Protocol version 4. The source and destination addresses are IP addresses.



In this lab, you are exploring the properties of IP version 4 addressing. IP version 6 (IPv6) is also in widespread use. IPv4 and IPv6 traffic is often exchanged over the same network. IPv6 uses longer addresses and a different mechanism to map logical IP addresses with MAC interface identifiers.

Analyze network ports

The link and network/internet layers are primarily concerned with addressing. They only exist to carry (encapsulate) higher level protocols that carry interesting data, such as web pages or email messages.

Each of these higher level protocols must be identified. This is accomplished by assigning a port to each application protocol. This port identification takes place at the transport layer.

1. If necessary, select frame #3.
2. 

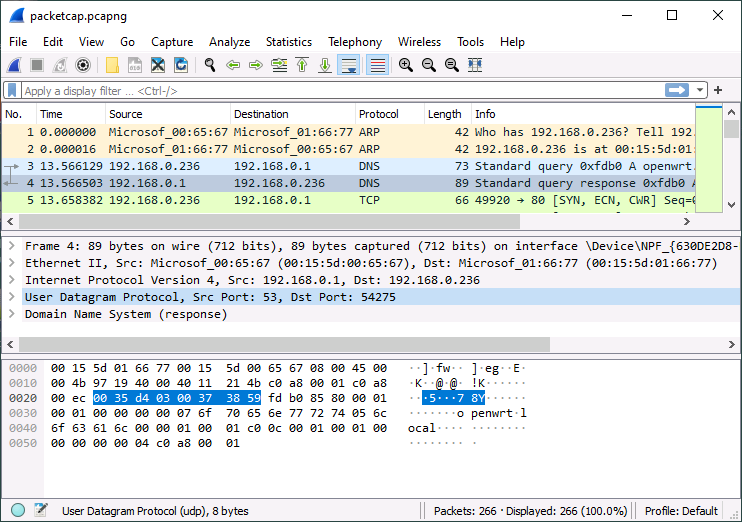
What is the destination port number?



1. Make a note of the source port number:  
     
   
2. Select frame #4.

This application protocol (DNS) also uses a request/response pattern. Frame #4 is the response to the request made in frame #3. Observe that the destination port is frame #3's source port value (<client\_port>).

In this exchange, port \* is the server port and <client\_port> is the client port. Clients assign a random port value to keep track of multiple requests to the same or different servers. The server uses the client port to direct its responses to the matching request.



1. 

In the middle pane, observe the fourth summary line: what type of protocol is used to identify the port number?



1. Select frame #5.
2. 

What type of protocol is used to identify the port number in frame #5?



The transport layer uses two kinds of protocols to identify ports:

* User Datagram Protocol (UDP) provides connectionless transfers with no reliability features. This means that the application must correct for any missing or out-of-sequence packets.
* Transmission Control Protocol (TCP) provides connection-oriented transfers with reliability features that identify missing or out-of-order packets. This makes each packet header larger, however.

You can see that the DNS application protocol typically only needs one packet per request or reply. It can use User Datagram Protocol (UDP) because it doesn't need to manage a sequence of request or response packets. Conversely, the application protocol session starting in frame #5 (HTTP) uses lots of request and response packets. It needs the reliability features of the Transmission Control Protocol (TCP) to keep track of these.

Analyze network names

Frames #3 and #4 carry Domain Name System (DNS) application protocol traffic. DNS maps IP addresses to network names. Names are human language labels applied to systems to make it easier for people to identify hosts and services on networks.

1. 

Analyze the DNS headers in frames #3 and #4 and the summary in the "Info" field. What is the name of the host with IP address 192.168.0.1?



SUCCESS: You selected and analyzed packets to identify a host name

1. 

Can you identify the name of the host with IP address 192.168.0.236 from frames #3 and #4?

Yes

No

SUCCESS: You identified information that could not be obtained from analyzing the frame

Analyze application protocol data

1. If necessary, select frame #5.
2. 

What is the source port for frame #5?



SUCCESS: You selected and analyzed a frame to identify a source port value

In the top pane, observe the sequence of frames that establish a TCP connection:

* In frame #5, the client sends a SYN packet to the server on port 80. SYN(chronize) is a request to start a TCP session. It assigns the source port 49920 to track this session.
* In frame #6, the server responds with a SYN,ACK segment to acknowledge and accept the client's request.
* In frame #7, the client acknowledges the server's response.
* In frame #9, the client sends an application request, using the HyperText Transfer Protocol (HTTP).
* In frames #12-14, the client and server exchange more ACKs.
* In frame #15, the server responds to the request with some HTTP data.

As you can see, TCP incurs quite a lot of overhead in terms of extra data to ensure reliable transfer of packets.

In frame #8, you can see another TCP handshake starting. Note that this is assigned a different client source port (49921). Web applications often use multiple sessions to speed up transfers.

Notice that the HTTP requests and responses are readable. This indicates that there is no connection security. A secure protocol would encrypt the traffic, making it unreadable in a packet capture.

Analyze remote network traffic

The traffic you have observed so far has been sent between two hosts on the same local network:

* Host 192.168.0.1 has MAC address 00:15:5d:01:65:67. This host is the network's router. It is also running an HTTP web management application.
* Host 192.168.0.236 has MAC address 00:15:5D:01:66:77. This is the laptop client machine.

These hosts are on the IP network 192.168.0.0/24. The /24 indicates the number of values in the address that constitute the network ID. This works out as 192.168.0. The last part is the host ID (.1 and .236).

1. Scroll through the packet capture to select frame #216.

There is a block of DNS requests and responses as the client tries to connect to a host on the Internet named neverssl.com.

1. 

What is the IP address of neverssl.com?



1. Select frame #222.
2. 

What host owns the destination MAC address for this frame?

neverssl.com host

client host (192.168.0.236)

router host (192.168.0.1)

neverssl.com uses the IP address 34.223.124.45, which is a different IP network to 192.168.0.0/24. To access it, packets must be routed across the Internet:

* Because the client recognizes that the packet must be routed, it addresses the packet to its default gateway (the router) and sends it across the local network to the router's MAC address.
* The router also recognizes that the packet must be routed and so forwards it out of its wide area network (WAN) interface to an Internet router.
* The packet will be processed by a number of other routers as it traverses the Internet to be delivered to 34.223.124.45.
* Responses from the Internet host are routed back to the local network router and then forwarded over the local area network (LAN) to the client.

Additionally, the router has to translate between the private IP address used by the client and a public IP address that can be used across the Internet.