# Lab 4 – Introduction to Wireshark

## Lab Learning Goals

This lab explores the basics of capturing and analyzing traffic using Wireshark, and analyzing protocols in layer 2, 3, and 4, and 7.

## Required Resources

- **Wireshark 3.2.x** (on your laptop)

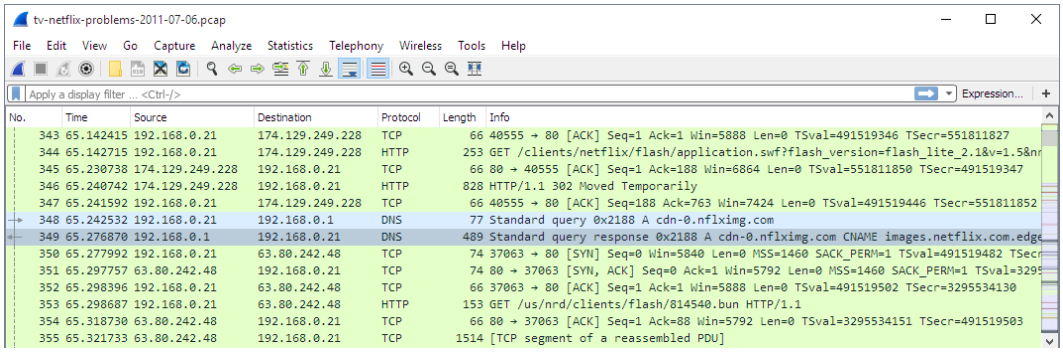
## Submission Instructions

- Complete the lab quiz: **Lab 4 – Introduction to Wireshark**

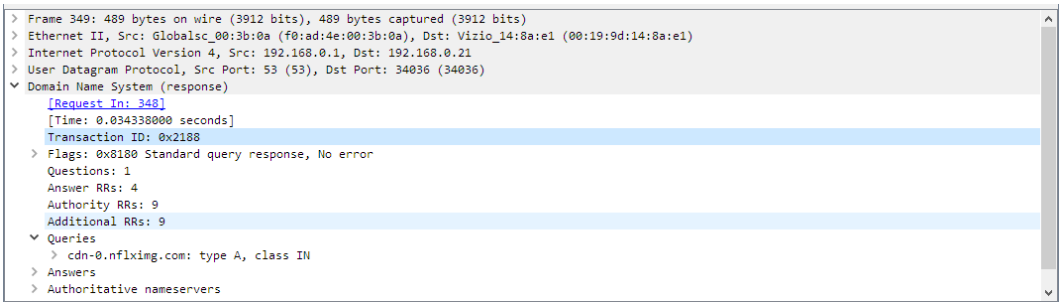
# Lab 4 – Introduction to Wireshark

## Exploring the Wireshark Interface

1. Open Wireshark and capture about 10 seconds of packets from an active network interface (Ethernet only on campus). Generate some traffic by opening Firefox and navigating to a website that uses HTTP (not HTTPS).




2. Explore the packet list pane and the information found in this view
   a. How can you tell a packet is the first in the conversation?
   b. What about the last?
   c. Is the packet part of a TCP 3-way handshake?




3. Select an IPv4 packet in the packet list window and take a closer look at the packet detail pane paying attention to the information contained in the Frame, Ethernet, IP and TCP sections.
   a. Frame:
      i. How long after the preceding packet (delta) did this packet arrive?
      ii. What is the Wireshark frame number?
      iii. How long is the frame?
   b. Ethernet II
      i. What is the source and destination MAC address?
      ii. Was this frame a unicast or broadcast message?
      iii. What protocol is described in the layer 2 type field?
   c. Internet Protocol Version 4
      i. What is the size of the layer 3 header length?
      ii. Was the frame fragmented? If so, what part of the message does this frame represent?
      iii. What is the value of the TTL? Was this packet routed?

iv. What layer 4 protocol is described in the IP section?
v. What value is the header checksum? Is it valid? (This may be disabled)

d. Transmission Control Protocol
i. What source and destination ports are being used?
ii. What is the TCP Segment length?
iii. What sequence and acknowledgement numbers (relative) are used?
iv. What is the current TCP window size?


4. Select a value in the packet detail pane and notice that selection in the packet byte pane.
   a. Can the pane also display the information as bits?

## Exploring Filters

1. Start a new capture and while capturing ping www.google.ca. When the ping completes, end the capture.
2. Find the ICMP packet in the packet list pane.
   a. From the arrow to the left of the numbering column, can you tell if this packet is an echo request or an echo response?
3. In the filter toolbar, type the filter: **ip.src == x.x.x.x && icmp** (substitute x.x.x.x for your IP address)
   a. Notice how the hundreds or perhaps thousands of packets have been greatly reduced.
   b. How would you modify the filter to see the echo responses?
   c. Try using **ip.addr** to see both the requests and responses at once.
4. Open the Display Filter Expression window (Analyze > Display Filter Expression) and look at some of the many thousands of filter options available.
5. With the Expressions window open, do a search for **tcp.analysis** and apply the SEQ/ACK analysis filter.
   a. Can you find a SYN, SYN/ACK, ACK sequence in the packet list?

# Lab 4 – Introduction to Wireshark

## Analyze Capture Files

1. From the website http://packetlife.net/captures/ download and open the capture file **ipv4-smtp.cap**.
2. By looking at the first packet in the capture, can you determine:
    a. What operating system sent the SYN request?
    b. What was the source port number?
    c. What was the destination port number?
3. Return to packetlife.net and select the **Encryption** category from the right side of the page. Download and open the capture file **SSHv2.cap**.
4. From analyzing the capture file, can you determine:
    a. The application layer protocol that is running?
    b. What version of the protocol is being used?
    c. Can you determine the encryption method used in the key exchange?
5. Return to packetlife.net and select the **Tunneling** category from the right side of the page. Download and open the capture file **ICMP_across_dot1q.cap**.
6. Notice that packets in this capture have an 802.1Q Virtual LAN section in the packet details. This section contains details about the VLAN trunking information inside the Ethernet framing.
    a. Can you determine the VLAN ID?

## Lab Challenge

CloudShark provides a cloud-based packet analysis platform very similar to Wireshark. Explore the CloudShark interface as you did for Wireshark. Access the challenge located at: https://www.cloudshark.org/captures/289c2fe55c9d

Use the Wireshark documentation (https://www.wireshark.org/docs/wsug_html_chunked/) and online search resources to build the following filters:

- Display only packets that have both the TCP flags SYN + ACK enabled
- Display only packets that are sourced from or destined to the IP address 66.228.57.241
- Display only packets that are sourced from the host 173.230.134.104
- Display only packets that are sourced from or destined to the TCP port 52177
- Display only packets that contain HTTP resource requests