

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).

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40955 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&n
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40955 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40955 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr=
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

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?

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface 0
> Ethernet II, Src: GlobalSC_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
  > Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
    > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
    > Queries
      > cdn-0.nflximg.com: type A, class IN
    > Answers
    > Authoritative nameservers
```

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?

Lab 4 – Introduction to Wireshark



- 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