Universiteit Antwerpen
Faculteit Toegepaste Ingenieurswetenschappen

Lab of 3-Network Architecture

Ruben Nietvelt, Nabeel Nisar Bhat

2024-2025

Scheduled labs for PR01

Session	Date	Subject	Evaluation	Deadline (23:59)
1	01/10/2024	Introduction to the Linux Operating System	**N/A**	**N/A**
2	08/10/2024	Using the shell & exploring the filesystem	Report	14/10/2024
3	15/10/2024	Working with text files, managing running processes and writing shell scripts	Report	22/10/2024
4	23/10/2024	Learning system administration, getting & managing software	Report	28/10/2024
5	29/10/2024	Wireshark introduction	Report	05/11/2024
6	06/11/2024	Protocols in action: TCP and UDP	Report	11/11/2024
7	12/11/2024	Ethernet and ARP	Report	19/11/2024
8	20/11/2024	Setting up a DHCP server	Report	25/11/2024
9	26/11/2024	Setting up a DNS server	Report	03/12/2024
10	04/12/2024	Network Address Translation	Report	09/12/2024
11	10/12/2024	Remote Access & Firewalls (1)		**N/A**
12	18/12/2024	Remote Access & Firewalls (2)	Blackboard test	

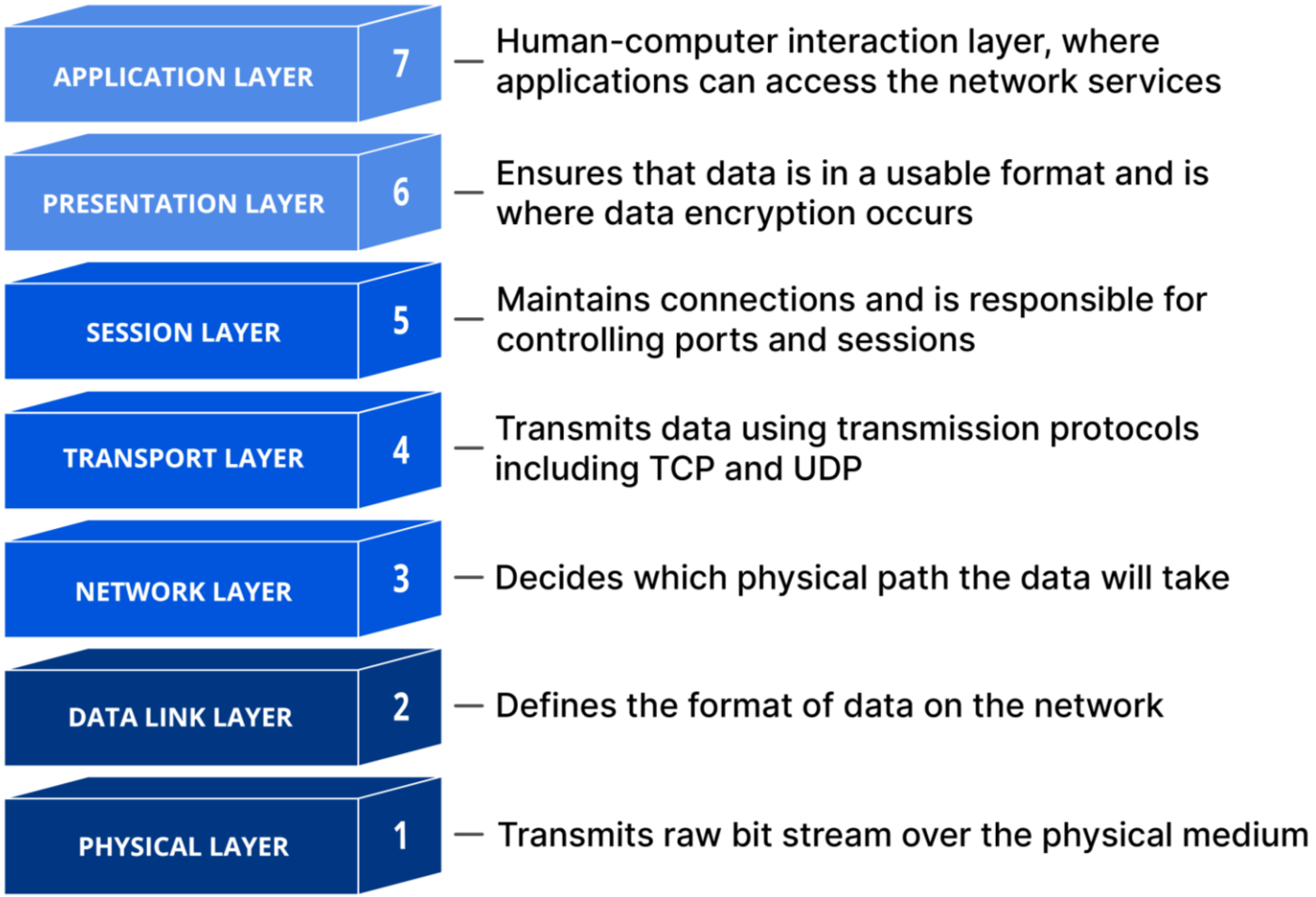
Scheduled labs for PR02

Session	Date	Subject	Evaluation	Deadline (23:59)
1	02/10/2024	Introduction to the Linux Operating System	N/A	N/A
2	09/10/2024	Using the shell & exploring the filesystem	Report	15/10/2024
3	16/10/2024	Working with text files, managing running processes and writing shell scripts	Report	22/10/2024
4	23/10/2024	Learning system administration, getting & managing software	Report	29/10/2024
5	30/10/2024	Wireshark introduction	Report	05/11/2024
6	06/11/2024	Protocols in action: TCP and UDP	Report	12/11/2024
7	13/11/2024	Ethernet and ARP	Report	19/11/2024
8	20/11/2024	Setting up a DHCP server	Report	26/11/2024
9	27/11/2024	Setting up a DNS server	Report	03/12/2024
10	04/12/2024	Network Address Translation	Report	10/12/2024
11	11/12/2024	Remote Access & Firewalls (1)		**N/A**
12	18/12/2024	Remote Access & Firewalls (2)	Blackboard test	

Session 5

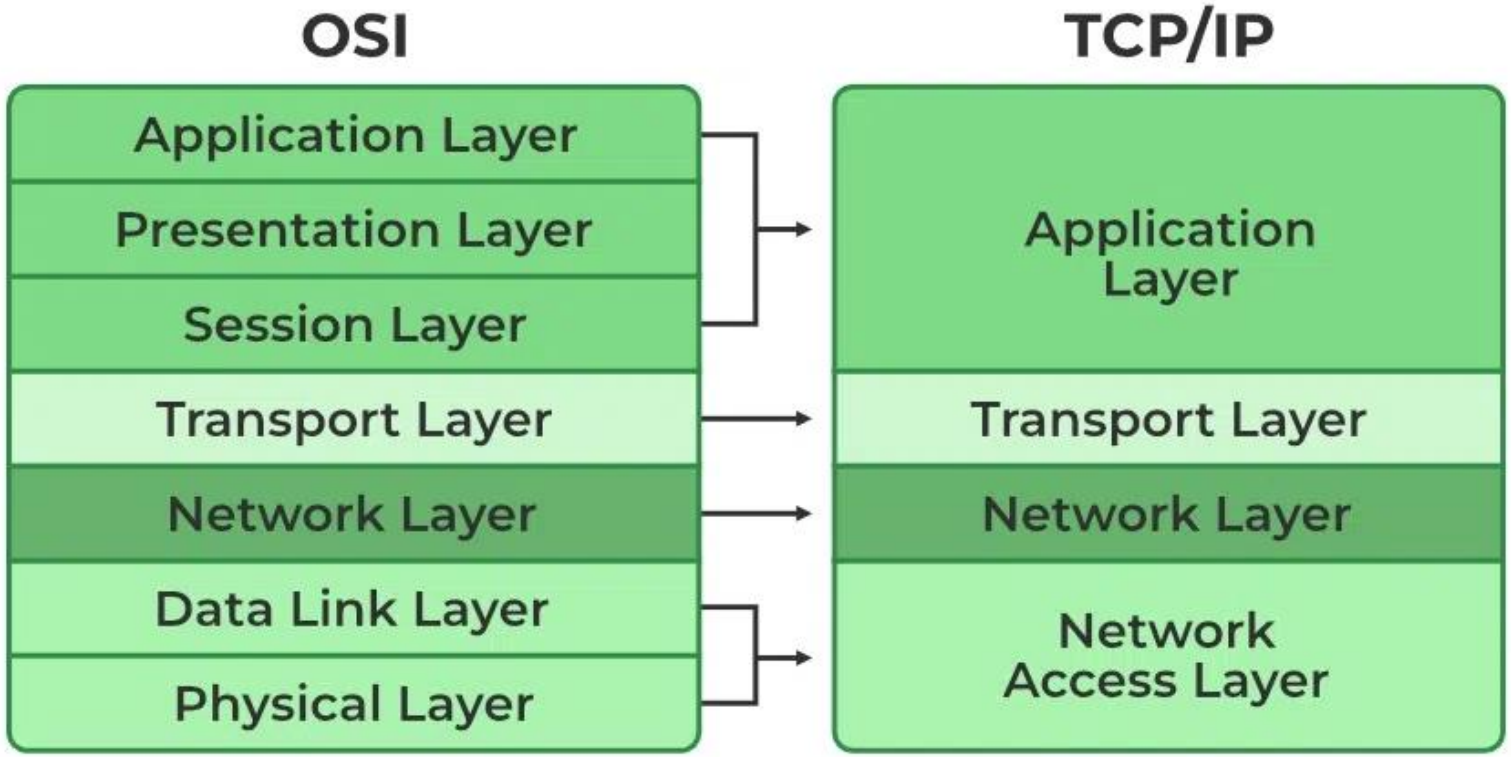
Wireshark introduction

OSI model



Source: https://www.cloudflare.com/it-it/learning/ddos/glossary/open-systems-interconnection-model-osi/

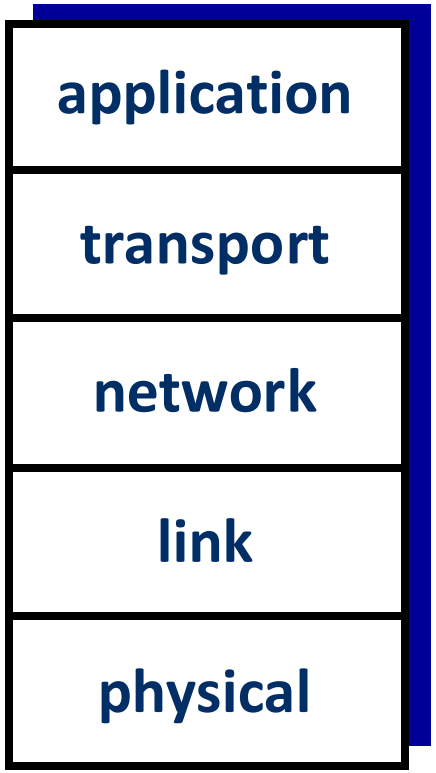
OSI vs TCP/IP



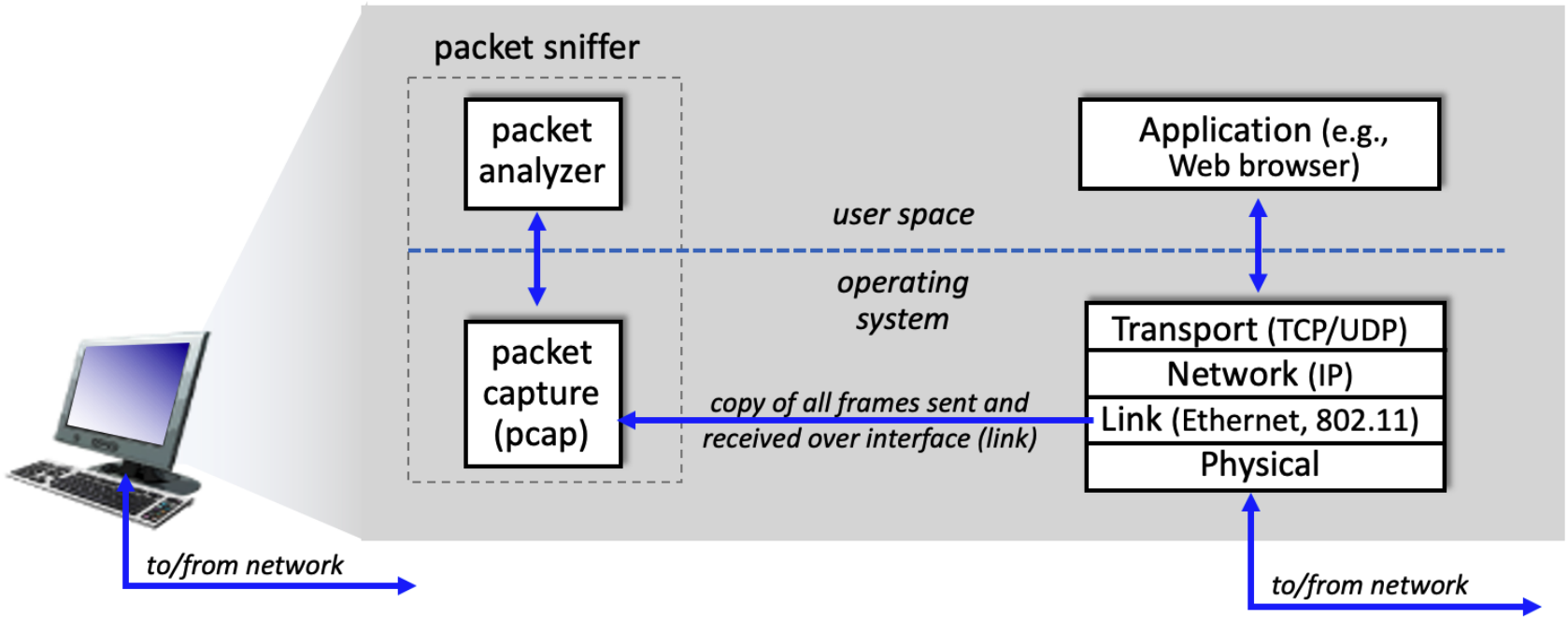
Source: https://www.geeksforgeeks.org/tcp-ip-model/

Internet protocol stack

- *application:* supporting network applications
  - IMAP, SMTP, HTTP
- *transport:* process-process data transfer
  - TCP, UDP
- *network:* routing of datagrams from source to destination
  - IP, routing protocols
- *link:* data transfer between neighboring network elements
  - Ethernet, 802.11 (WiFi), PPP
- *physical:* bits “on the wire”

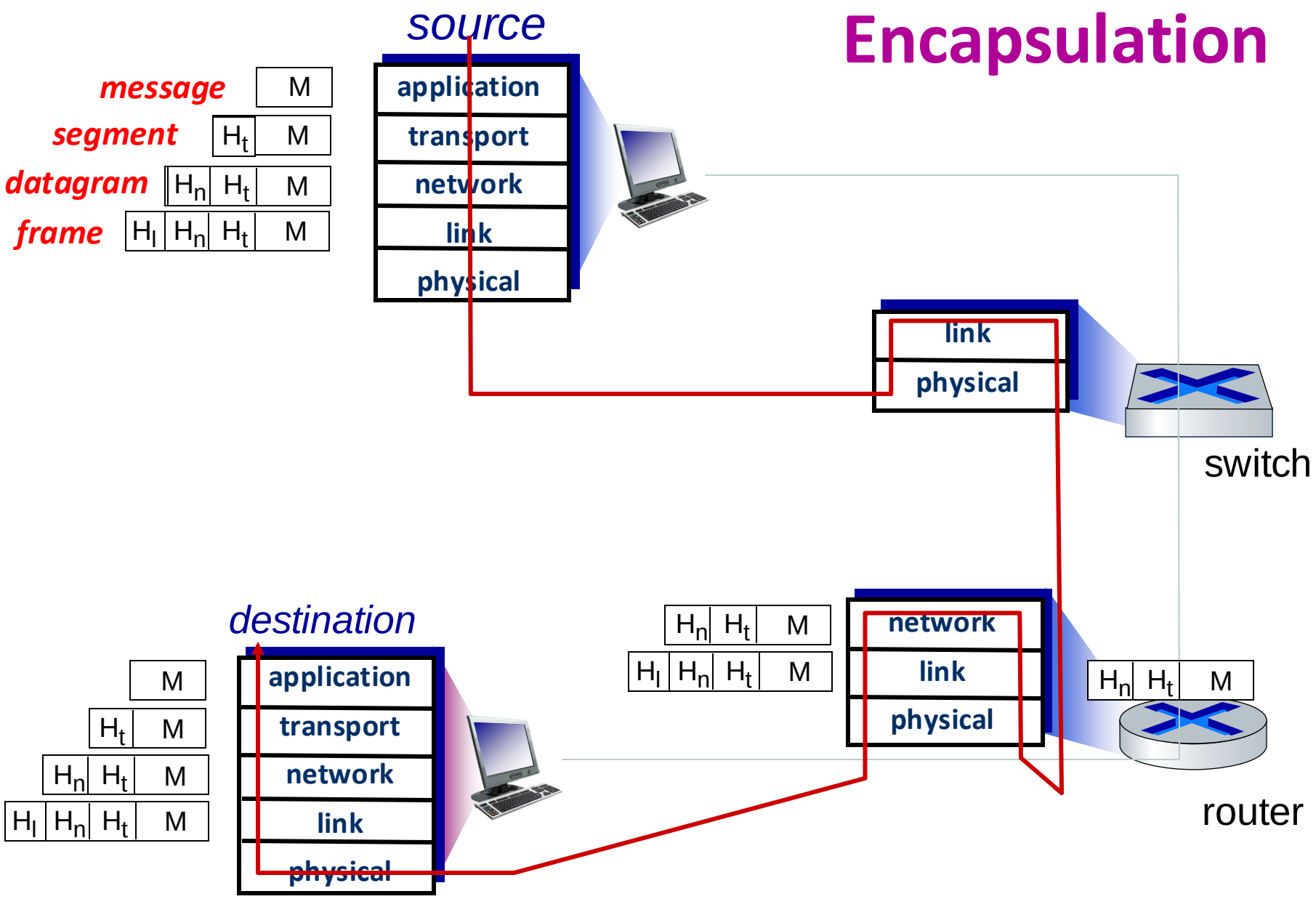


Packet sniffer

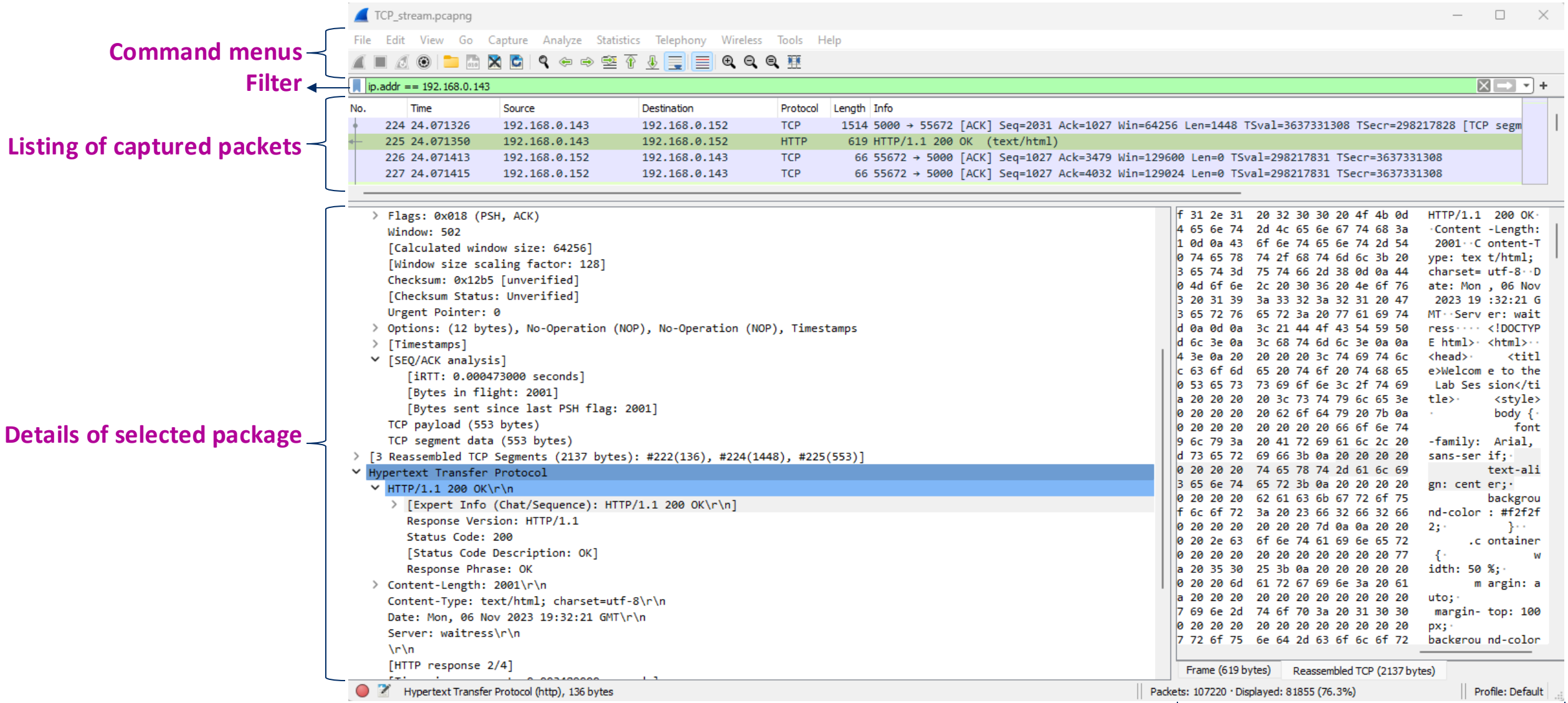


Source: https://gaia.cs.umass.edu/kurose_ross/wireshark.php

Encapsulation

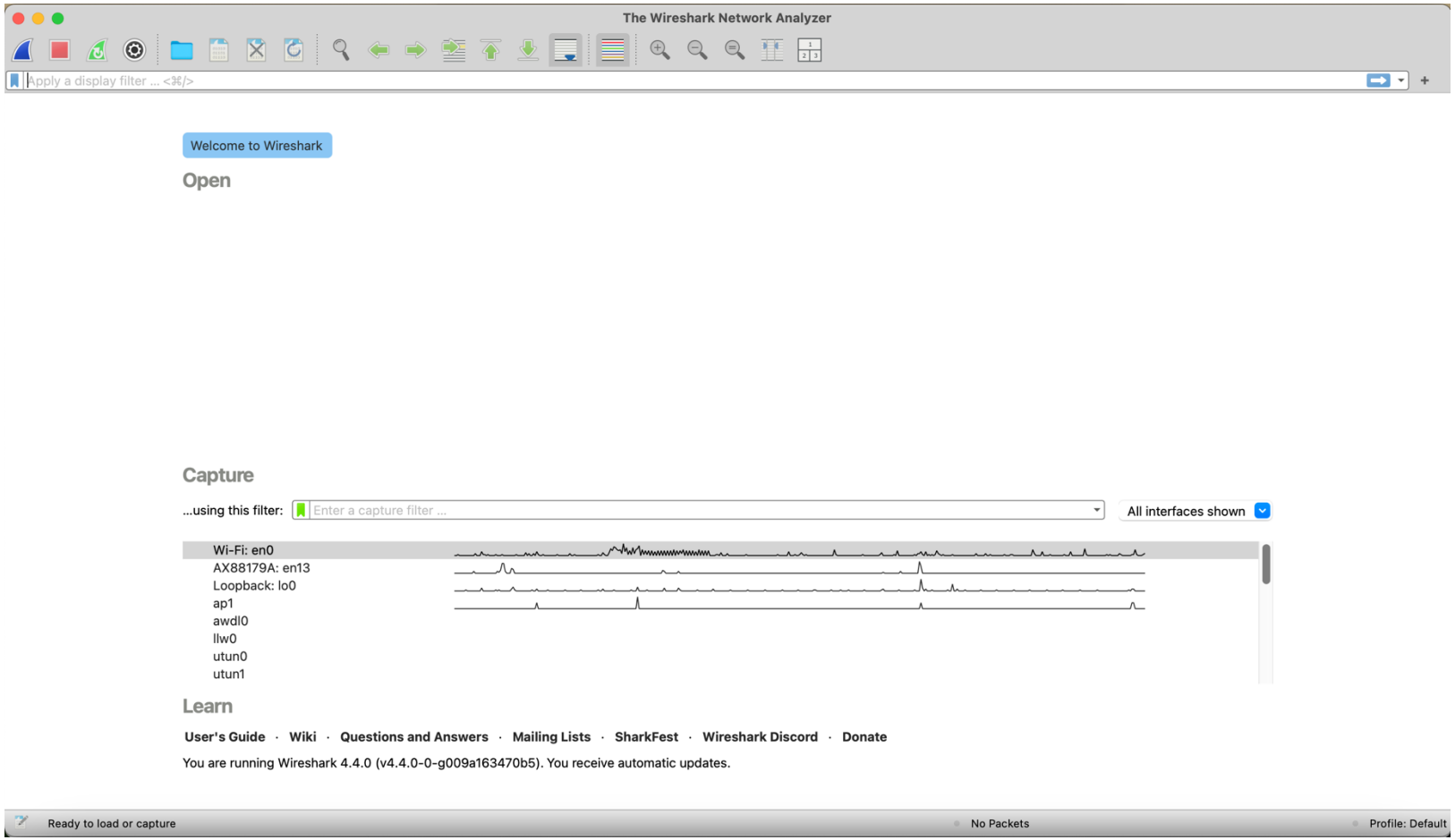


Wireshark


Command menus
Filter
Listing of captured packets
Details of selected package
TCP_stream.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.0.143
No. Time Source Destination Protocol Length Info
224 24.071326 192.168.0.143 192.168.0.152 TCP 1514 5000 → 55672 [ACK] Seq=2031 Ack=1027 Win=64256 Len=1448 TSval=3637331308 TSecr=298217828 [TCP segm
225 24.071350 192.168.0.143 192.168.0.152 HTTP 619 HTTP/1.1 200 OK (text/html)
226 24.071413 192.168.0.152 192.168.0.143 TCP 66 55672 → 5000 [ACK] Seq=1027 Ack=3479 Win=129600 Len=0 TSval=298217831 TSecr=3637331308
227 24.071415 192.168.0.152 192.168.0.143 TCP 66 55672 → 5000 [ACK] Seq=1027 Ack=4032 Win=129024 Len=0 TSval=298217831 TSecr=3637331308
Flags: 0x018 (PSH, ACK)
Window: 502
[Calculated window size: 64256]
[Window size scaling factor: 128]
Checksum: 0x12b5 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]
[iRTT: 0.000473000 seconds]
[Bytes in flight: 2001]
[Bytes sent since last PSH flag: 2001]
TCP payload (553 bytes)
TCP segment data (553 bytes)
[3 Reassembled TCP Segments (2137 bytes): #222(136), #224(1448), #225(553)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Content-Length: 2001\r\n
Content-Type: text/html; charset=utf-8\r\n
Date: Mon, 06 Nov 2023 19:32:21 GMT\r\n
Server: waitress\r\n
\r\n
[HTTP response 2/4]
f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK·
4 65 6e 74 2d 4c 65 6e 67 74 68 3a ·Content -Length:
1 0d 0a 43 6f 6e 74 65 6e 74 2d 54 2001··C ontent-T
0 74 65 78 74 2f 68 74 6d 6c 3b 20 ype: tex t/html;
3 65 74 3d 75 74 66 2d 38 0d 0a 44 charset= utf-8··D
0 4d 6f 6e 2c 20 30 36 20 4e 6f 76 ate: Mon , 06 Nov
3 20 31 39 3a 33 32 3a 32 31 20 47 2023 19 :32:21 G
3 65 72 76 65 72 3a 20 77 61 69 74 MT··Serv er: wait
d 0a 0d 0a 3c 21 44 4f 43 54 59 50 ress···· <!DOCTYP
d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 0a E html>· <html>··
4 3e 0a 20 20 20 20 3c 74 69 74 6c <head>· <titl
c 63 6f 6d 65 20 74 6f 20 74 68 65 e>Welcom e to the
0 53 65 73 73 69 6f 6e 3c 2f 74 69 Lab Ses sion</ti
a 20 20 20 20 3c 73 74 79 6c 65 3e tle>· <style>
0 20 20 20 20 62 6f 64 79 20 7b 0a · body {·
0 20 20 20 20 20 20 20 66 6f 6e 74 font
9 6c 79 3a 20 41 72 69 61 6c 2c 20 -family: Arial,
d 73 65 72 69 66 3b 0a 20 20 20 20 sans-ser if;·
0 20 20 20 74 65 78 74 2d 61 6c 69 text-ali
3 65 6e 74 65 72 3b 0a 20 20 20 20 gn: cent er;·
0 20 20 20 62 61 63 6b 67 72 6f 75 backgrou
f 6c 6f 72 3a 20 23 66 32 66 32 66 nd-color : #f2f2f
0 20 20 20 20 20 20 7d 0a 0a 20 20 2;· }··
0 20 2e 63 6f 6e 74 61 69 6e 65 72 .c ontainer
0 20 20 20 20 20 20 20 20 20 20 77 {· w
a 20 35 30 25 3b 0a 20 20 20 20 20 idth: 50 %;·
0 20 20 6d 61 72 67 69 6e 3a 20 61 m argin: a
a 20 20 20 20 20 20 20 20 20 20 20 uto;·
7 69 6e 2d 74 6f 70 3a 20 31 30 30 margin- top: 100
0 20 20 20 20 20 20 20 20 20 20 20 px;·
7 72 6f 75 6e 64 2d 63 6f 6c 6f 72 backgrou nd-color
Frame (619 bytes)
Reassembled TCP (2137 bytes)
Hypertext Transfer Protocol (http), 136 bytes
Packets: 107220 · Displayed: 81855 (76.3%)
Profile: Default
Packet content
(hexadecimal or ASCII)

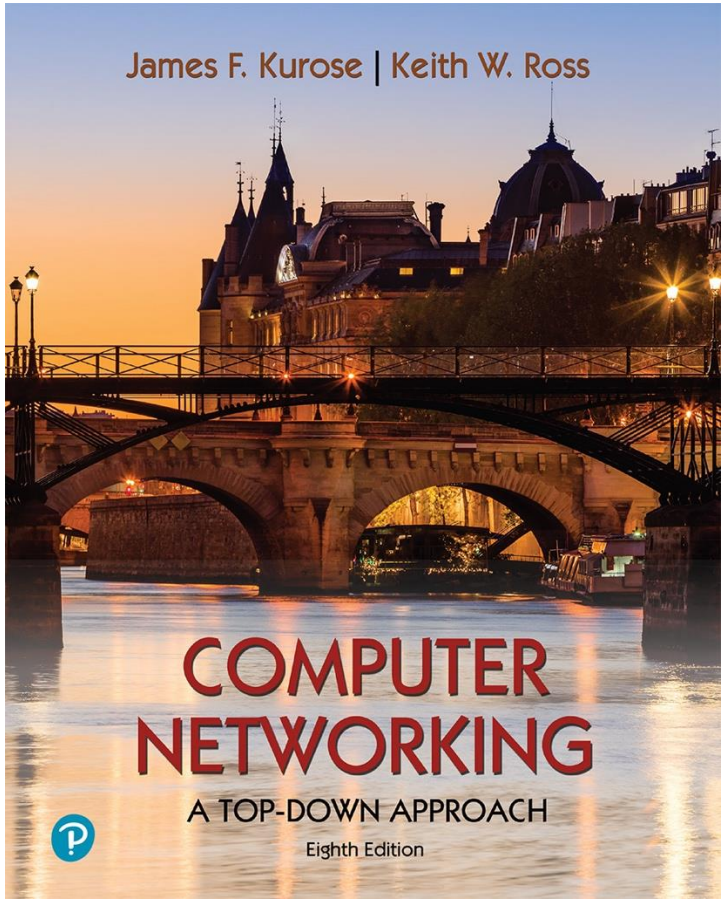
Wireshark

- https://www.wireshark.org/download.html



Resources

- **Computer Networking: A Top-Down Approach**
  8th edition
  Jim Kurose, Keith Ross
  Pearson, 2020

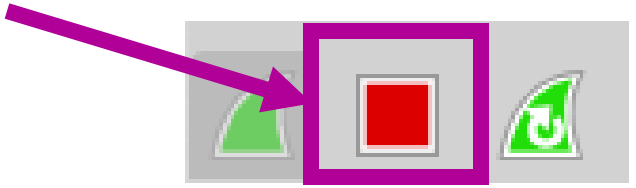


Exercises

Introduction to Wireshark

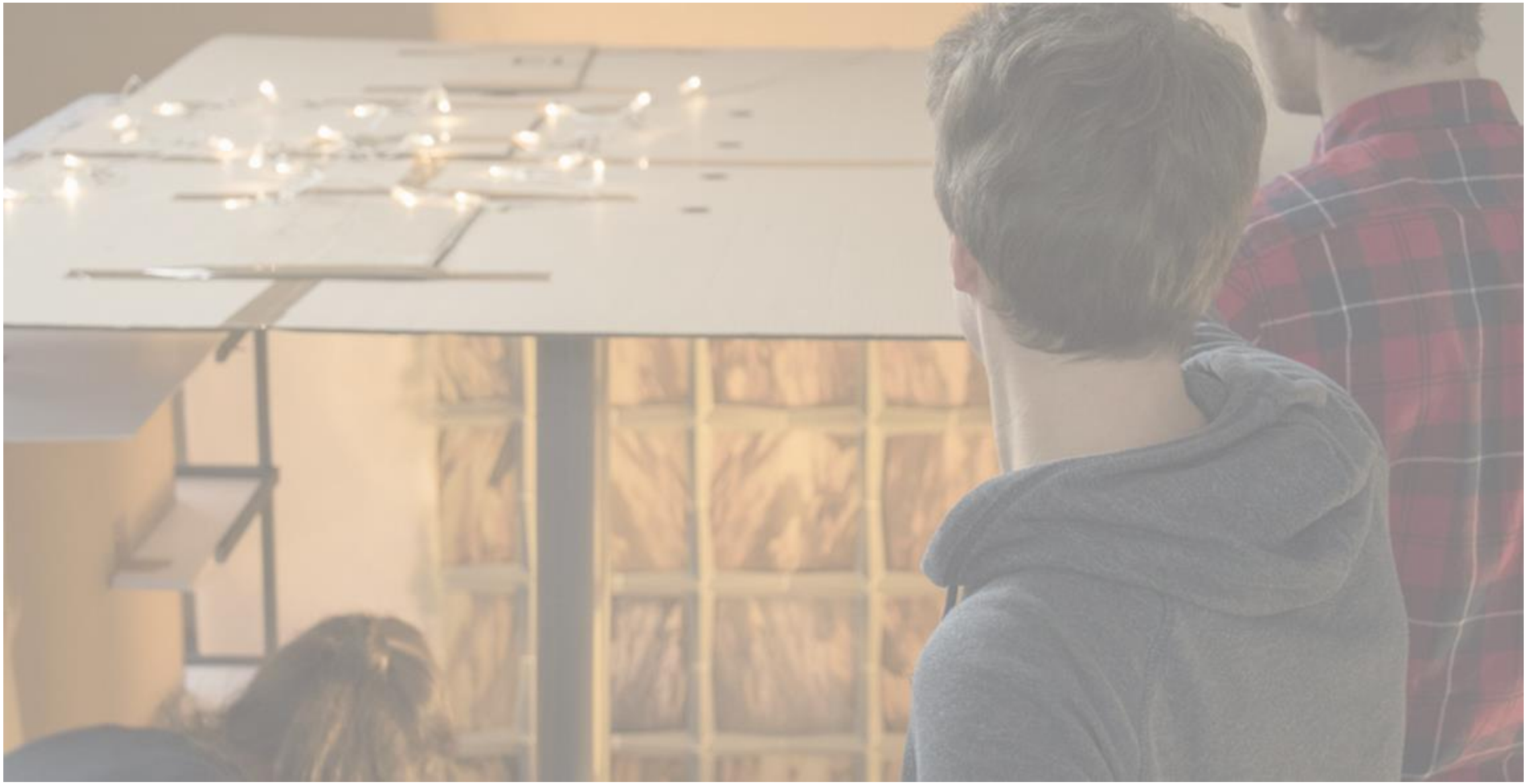
Exercise

1. Open Wireshark on your computer
2. Open your favorite browser
3. Start your Wireshark capture by selecting your ethernet interface.
4. Browse to http://course-3networkarchitecture.ei.fti.uantwerpen.be
5. Stop the Wireshark capture by pressing the red, stop button in the left top corner of Wireshark and save the file.



Questions

- Which protocols are needed, and visible in the Wireshark trace, to be able to access the webpage of session 5? Visualise the protocols by placing them next to the correct layer of the Internet Protocol stack of slide 8.
- What is the role of each protocol identified in the Wireshark trace in the webpage access process?
- What happens when you open the webpage of session 5? How many packets will be exchanged between your PC and the server?
- What is the internet address of course-3networkarchitecture.ei.fti.uantwerpen.be? Search for it in the Wireshark trace and find the Linux command to translate it to an internet address. Try it on your VM.



Universiteit Antwerpen
Faculteit Toegepaste Ingenieurswetenschappen