***CS 421 Wireshark Assignment  
Görkem Kadir Solun 22003214***

Taking Wireshark for a Test Run

# What to hand in

## 1. List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

ieee1905, UDP, TLSv1.3, TLSv1.2, TCP, STP, SKYPE, HTTP, DNS, BFCP, ARP

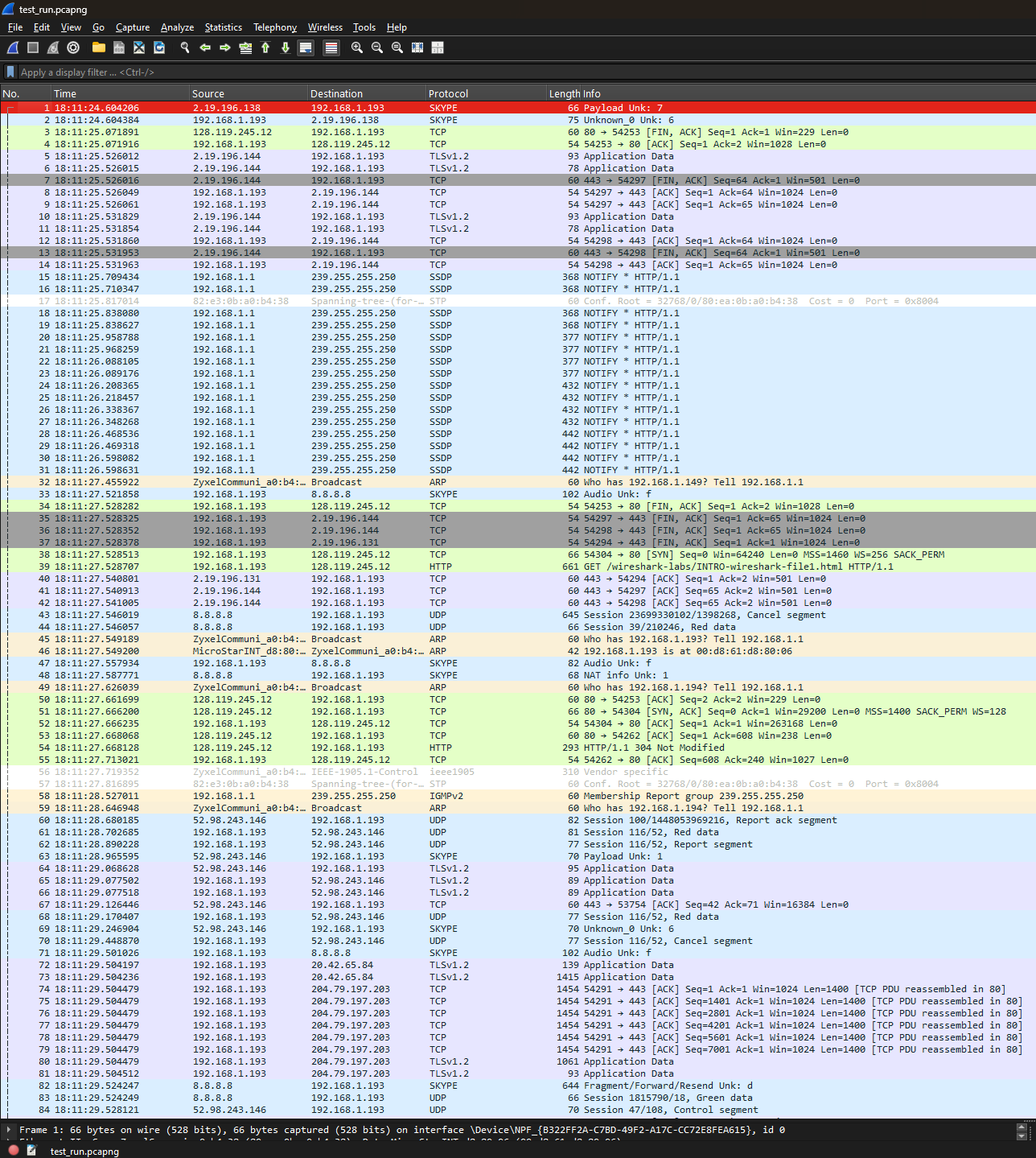


Figure 1: Some of the protocols from the first task

## 2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)



~0.12 seconds

## 3. What is the Internet address of gaia.cs.umass.edu (also known as www.net.cs.umass.edu)? What is the Internet address of your computer?

My computer: 192.169.1.193

gaia.cs.umass.edu: 128.119.245.12

## 4. Print the two HTTP messages displayed in step 9 above. To do so, select Print from the Wireshark File command menu, and select “Selected Packet Only” and “Print as displayed” and then click OK.

A screenshot of a computer

Description automatically generated

Figure 2: Print of HTTP OK

A screenshot of a computer

Description automatically generated

Figure 3: Print of HTTP OK

Wireshark Lab: HTTP

# 1. The Basic HTTP GET/response interaction

A screenshot of a computer

Description automatically generated

Figure 4: Downloaded the first HTML file

## A screenshot of a computer Description automatically generated

Figure 5: HTML file download GET

## A screenshot of a computer Description automatically generated

Figure 6: HTML file download OK

## 1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

We can see it uses HTTP 1.1 by checking the response and request versions in the header.

## 2. What languages (if any) does your browser indicate that it can accept to the server?

“Accept-Language: en-US,en;q=0.9,tr;q=0.8\r\n” at GET request implies US English and TR Turkish.

## 3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

In the GET request, it says my IP is 192.168.1.193, and gaia.cs.umass.edu’s IP is 128.119.245.12.

## A close-up of a number Description automatically generated4. What is the status code returned from the server to your browser?

It is “200” as written in the OK response.

## A close up of a text Description automatically generated5. When was the HTML file that you are retrieving last modified at the server?

It is “Sun, 13 Oct 2024 05:59:02” as written in the OK response.

## A black text on a white background Description automatically generated6. How many bytes of content are being returned to your browser?

This value is located in the "Content-Length: 128" line of the HTTP OK response header.

## 7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

No additional headers are visible within the raw data that are not already displayed in the packet-listing window. All the key HTTP headers, such as Date, Server, Last-Modified, ETag, Content-Length, Keep-Alive, Connection, and Content-Type, appear fully displayed in the packet-listing window. Please check Figure 6 above.

# 2. The HTTP CONDITIONAL GET/response interaction