***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

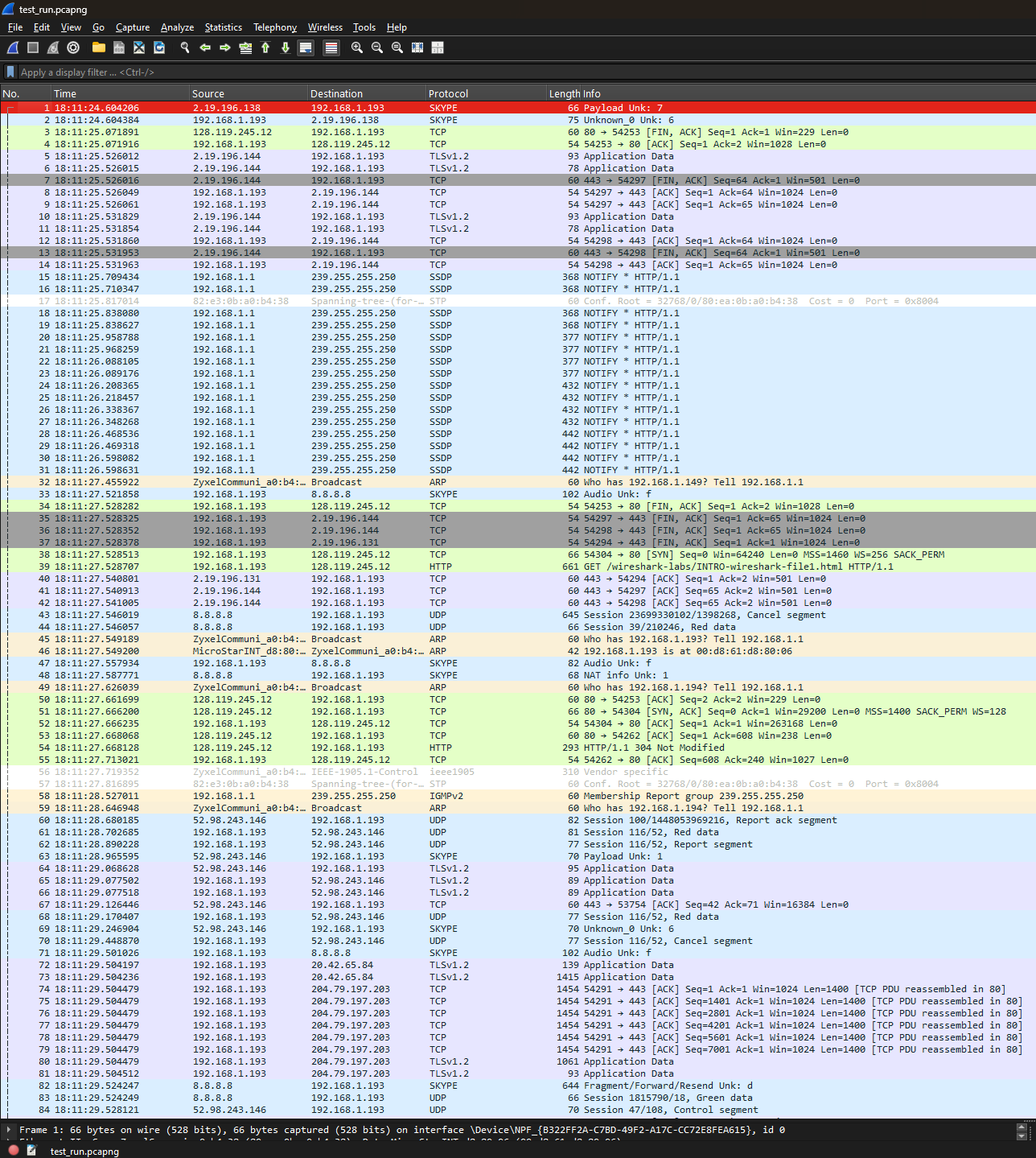


Figure 1: Some of the protocols from the first task

## 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?

Both use HTTP 1.1 as we can see 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 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 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

A screenshot of a computer

Description automatically generated

Figure 7: Not modified

A screenshot of a computer

Description automatically generated

Figure 8: The third GET request of the cached file.

A screenshot of a computer

Description automatically generated

Figure 9: Successful file retrieval with an OK response.

A screenshot of a computer

Description automatically generated

Figure 10: The first GET request of the file.

## A screen shot of a computer Description automatically generated8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

No.

## 9. Inspect the contents of the server response. Did the server explicitly return the contents of the *file? How can you tell?*

A screen shot of a computer

Description automatically generatedBy comparing Figure 9 with 7, we can see that the OK response has the file data. With this, we can tell that the file was retrieved in the OK response and not in the Not modified response.

## A screenshot of a computer Description automatically generated10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Yes. When we first got our file.

## A screen shot of a computer program Description automatically generated11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

No. The server did not return the file's contents requested as the file was not modified.

# 3. Retrieving Long Documents

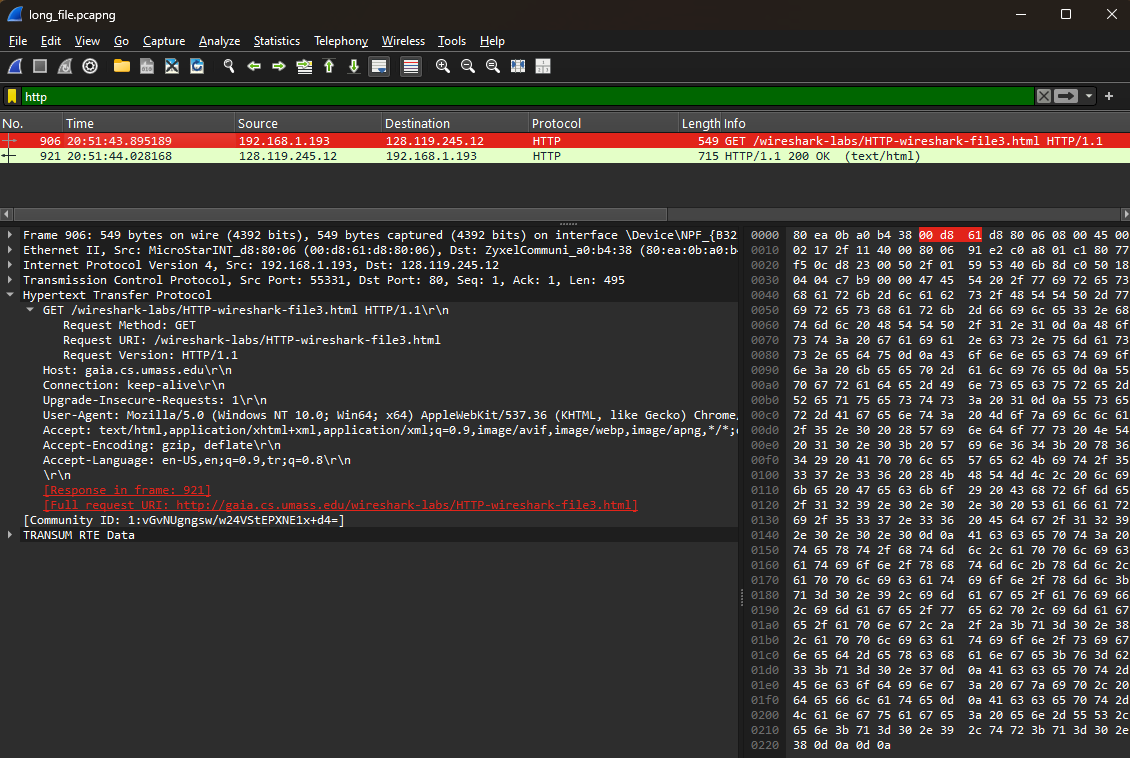


Figure 11: GET request for the long file.

A screenshot of a computer

Description automatically generated

Figure 12: Retrieved long file

## 12. How many HTTP GET request messages were sent by your browser?

One.

## A screenshot of a computer program Description automatically generated13. How many data-containing TCP segments were needed to carry the single HTTP response?

Four.

## A screen shot of a computer Description automatically generated14. What is the status code and phrase associated with the response to the HTTP GET request?

200 OK.

## 15. Are there any HTTP status lines in the transmitted data associated with a TCP induced “Continuation”?

There is no additional HTTP status line in these continuation packets—just the payload's continuation.

# 4. HTML Documents with Embedded Objects

A screenshot of a computer

Description automatically generated

Figure 13: HTTP image get

## A screen shot of a computer Description automatically generatedA screen shot of a computer Description automatically generated16. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?

3. One base HTML file and two objects. Addresses are the following: <http://kurose.cslash.net/8E_cover_small.jpg>, <http://gaia.cs.umass.edu/pearson.png>.  
178.79.137.164, 128.119.245.12

## 17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

Parallel. You can see that two GET requests are sent consecutively immediately after the HTML file is downloaded.

# 5. HTTP Authentication

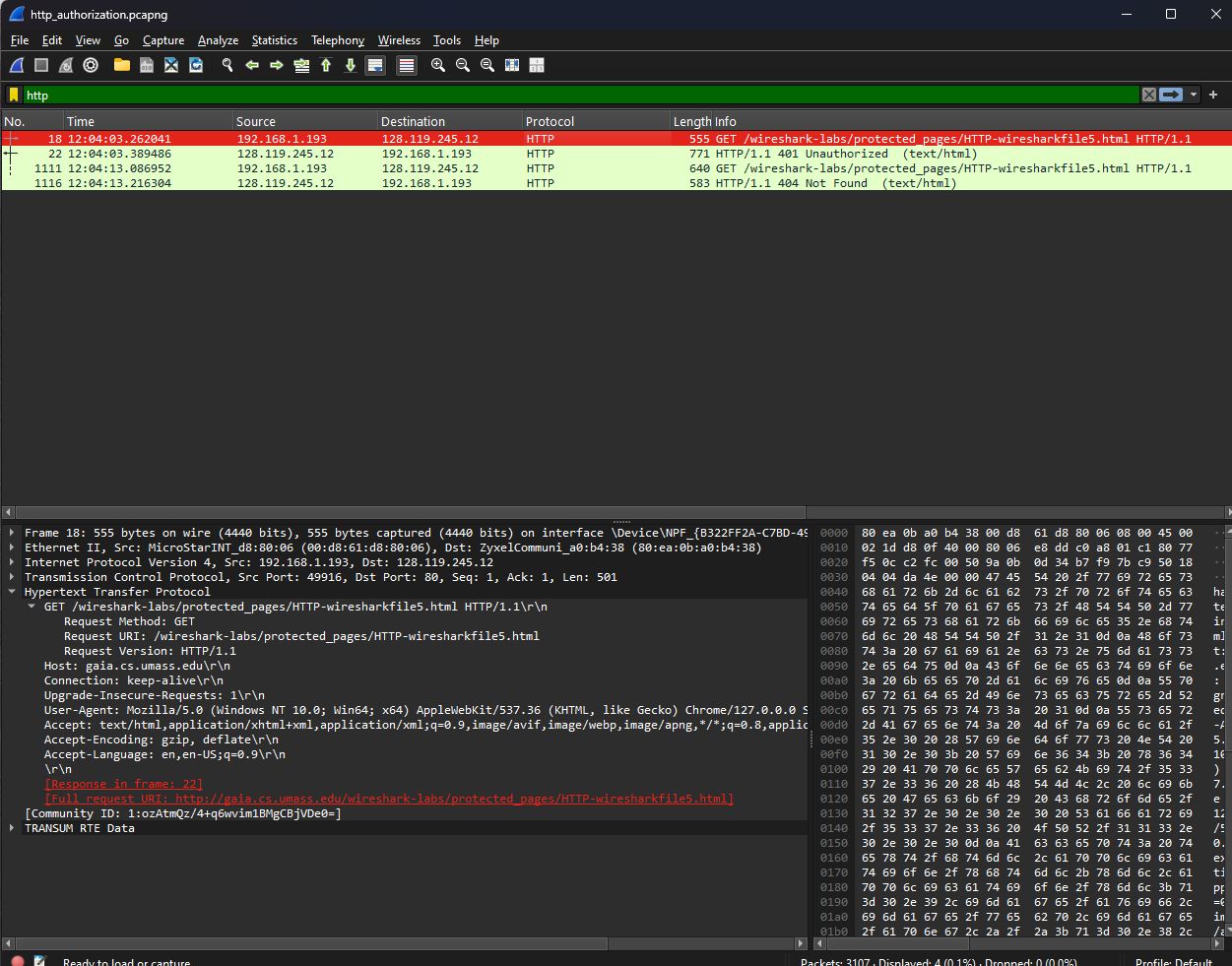


Figure 14: HTTP authorization

## A screen shot of a computer Description automatically generated18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?

401 Unauthorized.

## 19. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Authorization

DNS

# nslookup

A computer screen with white text

Description automatically generatedA screenshot of a computer program

Description automatically generated

A computer screen with white text

Description automatically generatedA screen shot of a computer

Description automatically generated

A screen shot of a computer code

Description automatically generatedGeneral syntax: nslookup –option1 –option2 host-to-find dns-server

## 1. Run nslookup to obtain the IP address of a Web server in Asia.

[百度一下，你就知道 (baidu.com)](https://www.baidu.com/)

Addresses: 45.113.192.102, 45.113.192.101

## 2. Run nslookup to determine the authoritative DNS servers for a university in Europe.

## [The Entrepreneurial University - TUM](https://www.tum.de/)

## A computer screen shot of a black screen Description automatically generated3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail.

They couldn’t find the answer.

# 2. ipconfig

A screenshot of a computer program

Description automatically generated

Figure 15: ipconfig /all

A black screen with white text

Description automatically generated

Figure 16: ipconfig /displaydns

A black screen with white text

Description automatically generated

Figure 17: ipconfig /flushdns

# 3. Tracing DNS with Wireshark

I switched to my laptop.

## A screenshot of a computer Description automatically generated

Figure 18: DNS query for ietf

## A screenshot of a computer Description automatically generated

A screenshot of a computer program

Description automatically generatedFigure 19: DNS response for ietf

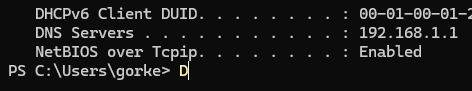
## 4. Locate the DNS query and response messages. Are they sent over UDP or TCP?

UDP

## A screenshot of a computer program Description automatically generated5. What is the destination port for the DNS query message? What is the source port of DNS response message?

Both 53

## 6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

They are the same 192.168.1.1

## A screen shot of a computer Description automatically generated7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

A type A query. However, it does not contain any answers.

## A screenshot of a computer Description automatically generated8. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

2. These include name, type, class, TTL, data length, and address information.

## 9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

A screenshot of a computer

Description automatically generatedYes, the TCP SYN packets are sent to 104.16.45.99, which is one of the provided answers from the DNS response message. You can check the image below.

## 10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

## There is no need for extra DNS requests since all the images are loaded from www.ietf.org, and the host uses a cached address.

A computer screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

Figure 20: nslookup mit query

A screenshot of a computer

Description automatically generated

Figure 21: nslookup mit response

## 11. What is the destination port for the DNS query message? What is the source port of DNS response message?

As seen in figures 20 and 21, both are 53.

## 12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The query is sent to the IP address 192.168.1.1, which corresponds to my default local DNS server.

## A screen shot of a computer Description automatically generatedTop of Form

## Bottom of Form

## 13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

A screenshot of a computer program

Description automatically generatedThe query is classified as an A type. It does not contain any answers.

## 14. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

## There are 3 answers. These include name, type, class, TTL, data length and cname or address information.

## 15. Provide a screenshot.

A screenshot of a computer

Description automatically generated

## A screen shot of a computer Description automatically generated16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The query is sent to the IP address 192.168.1.1, which is my default local DNS server.

## A screenshot of a computer Description automatically generated

## 17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The query is an NS type query. The query does not contain any answer.

## A screenshot of a computer Description automatically generated18. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?

It does not include any name servers, but it does contain the IP address of mit.edu's A record (104.66.66.27).

## 19. Provide a screenshot.

## A screen shot of a computer Description automatically generated

## 20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

The request is made to bitsy.mit.edu, which is located at 18.72.0.3.

A screenshot of a computer

Description automatically generated

## A screenshot of a computer Description automatically generated21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

It is a Standard Query of type. It does not contain any answers.

## 22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

The DNS response message provides a single solution, which includes the following details: the domain name is bitsy.mit.edu, with a type A record, class IN, and an address of 18.0.72.3. The record is classified as a host address (type A) with a class of IN (0x0001). The time to live (TTL) is set to 1315 seconds, and the data length is 4 bytes, representing the IP address 18.0.72.3.A screenshot of a computer

Description automatically generated

## 23. Provide a screenshot.

A screenshot of a computer

Description automatically generated