A close up of a logo

Description automatically generated

|  |  |  |  |
| --- | --- | --- | --- |
| أولاً: البيانات الخاصة بالمادة و فريق العمل | | | |
| **الفرقة الدراسية** | **الرابعة** | | | |
| **اسم القسم** | **تكنولوجيا المعلومات** | | |
| **اسم المقرر** | **شبكات الحاسب 1** | | |
| ثانياً: البيانات الخاصة بالطلبة | | | |
| **اسماء الطلاب المشاركين فى العملى**  **(يكتب الاسم رباعيا)** | **م** | **الاسم رباعى** | **رقم الجلوس** |
| **1** | **ميادة غنيم محمود محمد غنيم** | **4175** |
| **2** | **عبدالرحمن مسعد رمضان حسن** | **3922** |
| **3** | **محمد تامر محمد السيد** | **3980** |
| **4** | **إيمان المتولى فهيم المتولى** | **4842** |
| **5** | **محمد توفيق محمد** | **4734** |
|  | **6** |  |  |

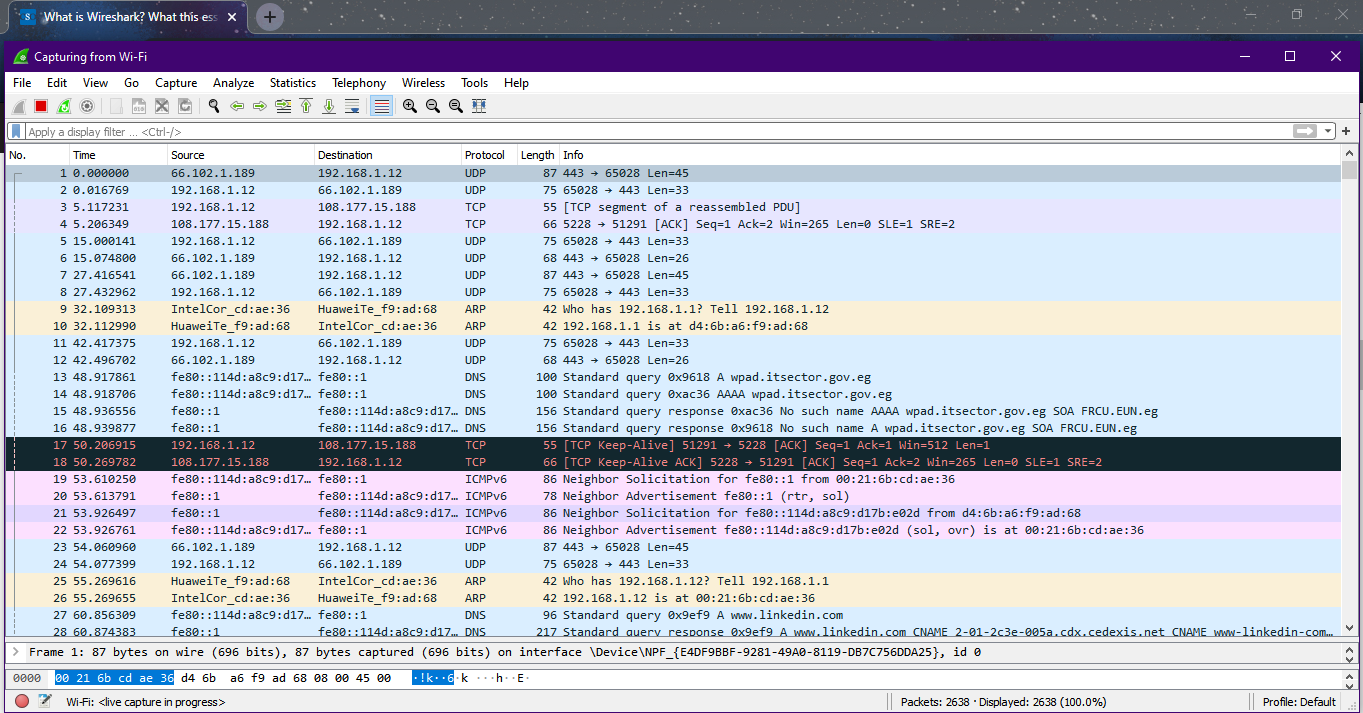
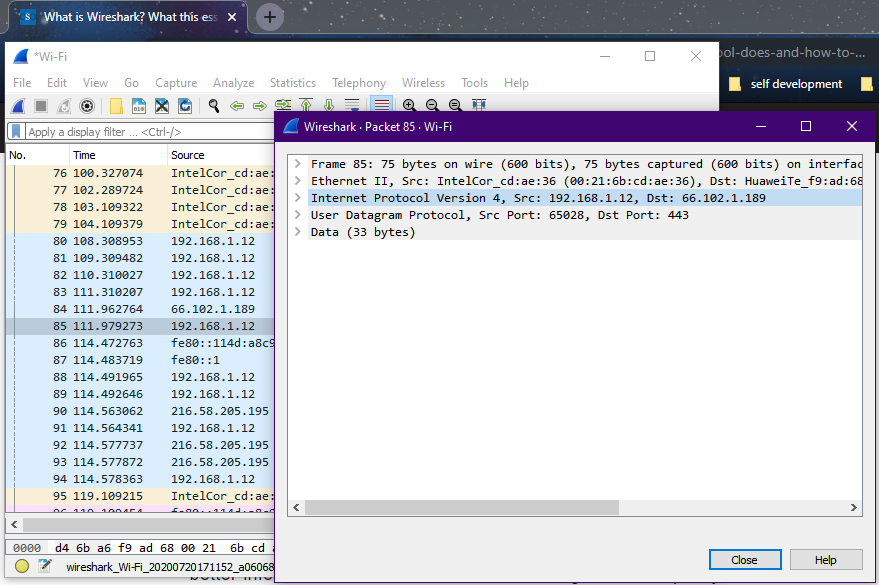
**Wireshark labs**

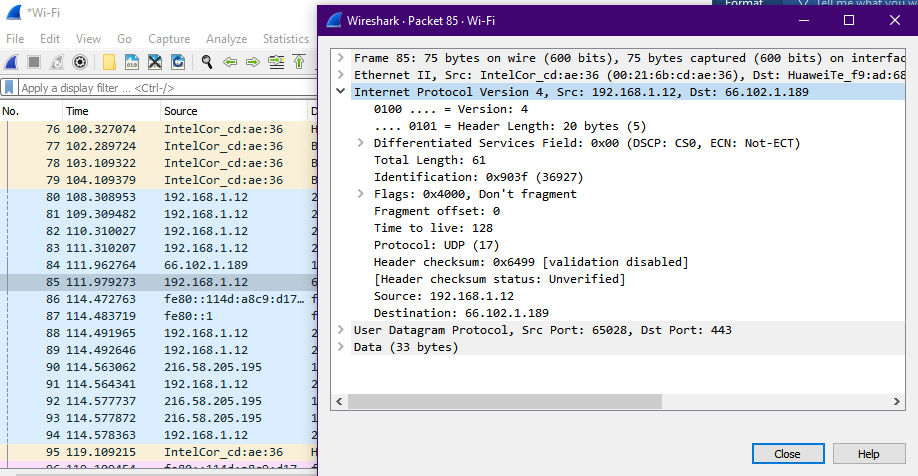
# **INTRODUCTION**

Wireshark is the world's leading network traffic analyzer, and an essential tool for any security professional or systems administrator. This free software lets you analyze network traffic in real time, and is often the best tool for troubleshooting issues on your network.

# **Lab 1**

* Steps:

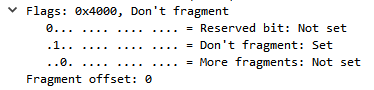
1. Open Wireshark and start capture from the right network interface.
2. Enable the internet connection in your PC.
3. Open your web browser and browsing any websites for a few seconds.
4. Stop the Wireshark.
5. Secondly, double click on any packet and open the “Internet Protocol version 4” field
6. Finally, try to answer any question such as the following:



* What is the IP address of your computer?
* 192.168.1.12, my computer is the (Source) of this packet.



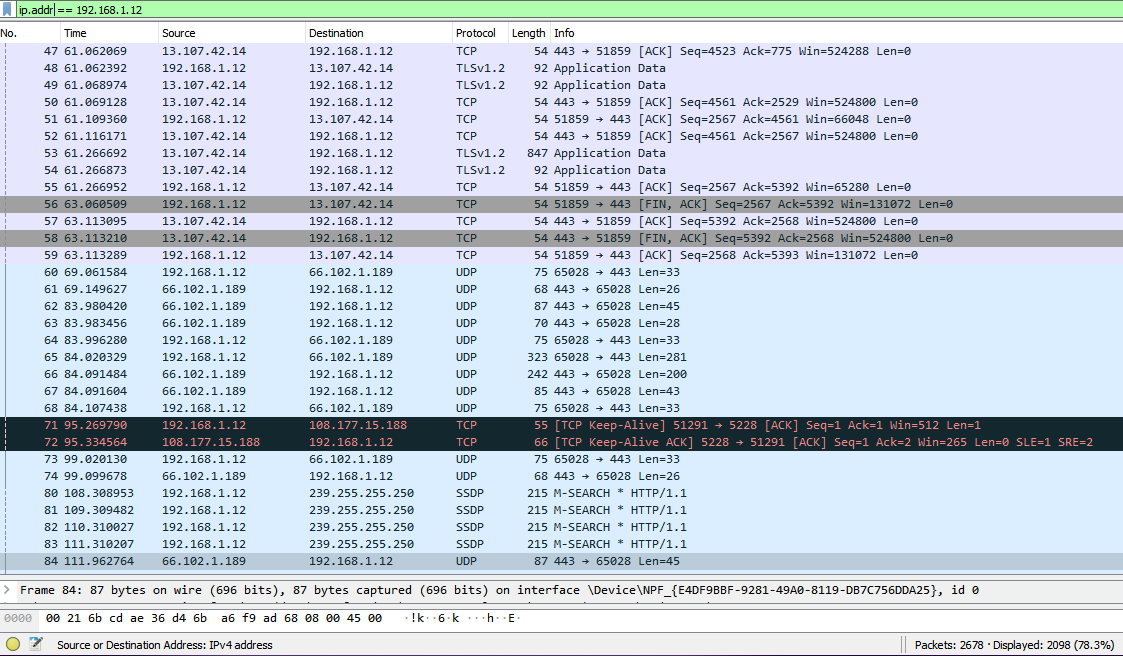
* Within the IP packet header, what is the value in the upper layer protocol field?
* UDP (17)
* How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
* Header length = 20 bytes
* Payload length = 41 bytes
* Payload length = Total length - Header length = 61 – 20 = 41 bytes.
* Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

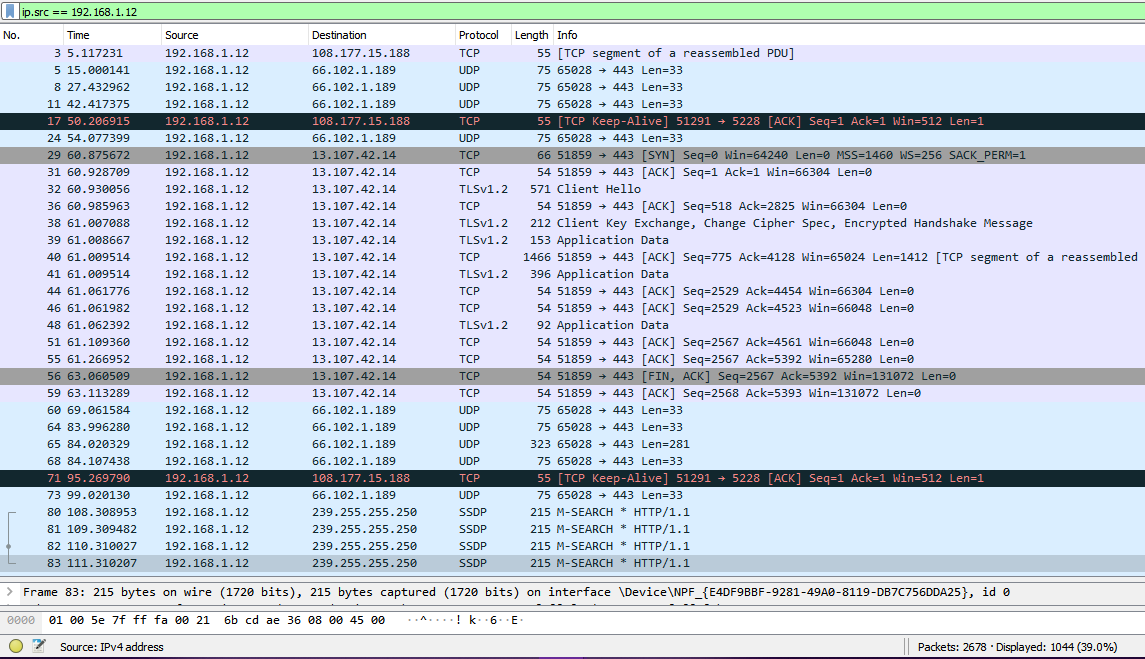
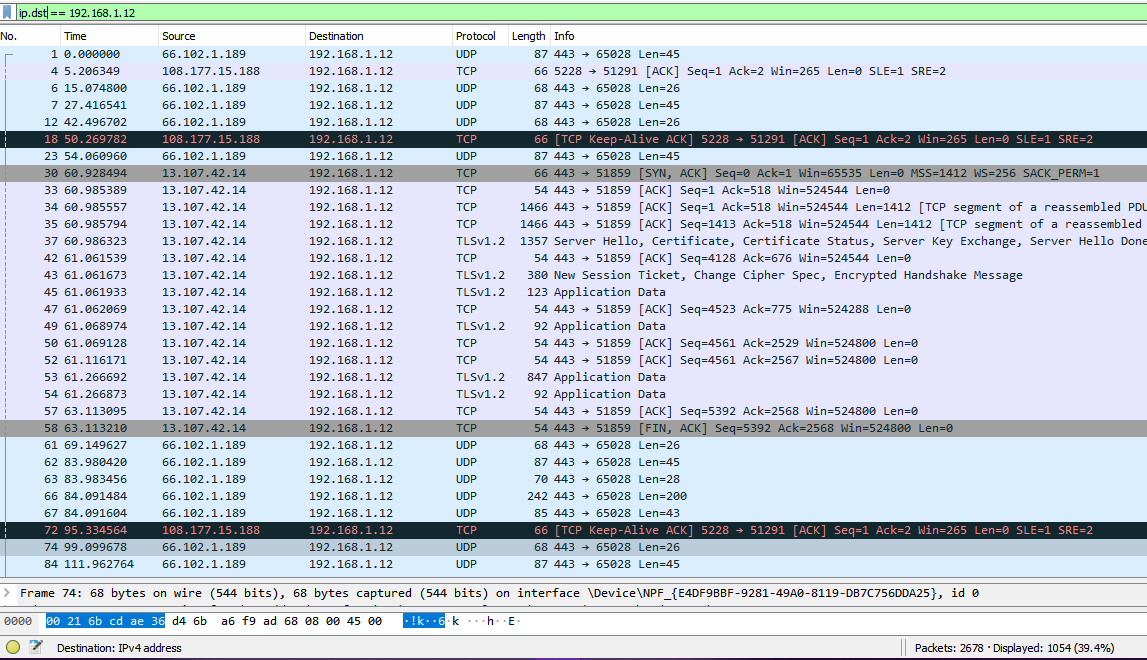


* No, there is no fragmentation (1. Don’t fragment)
* As the fragment offset = 0 it carry the whole packet,

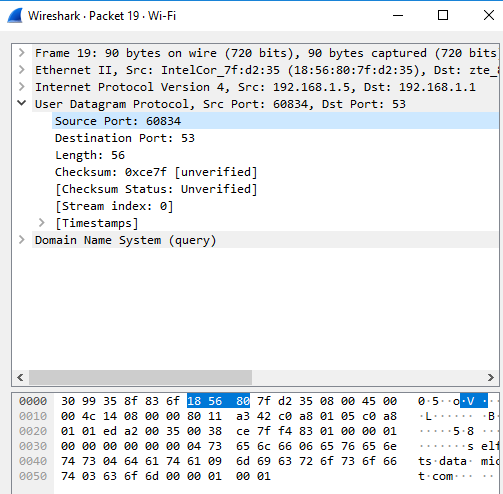
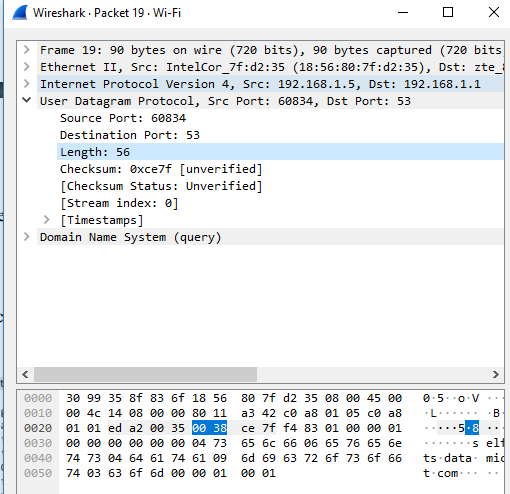
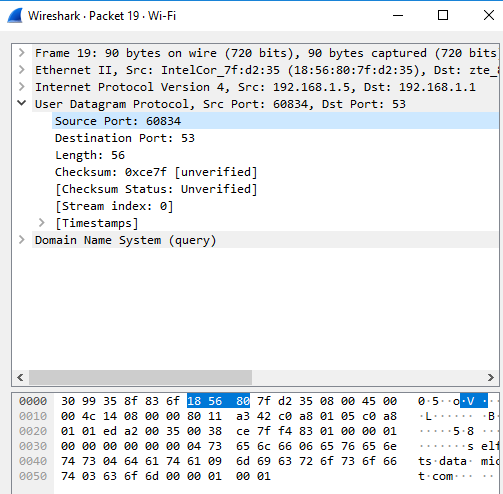
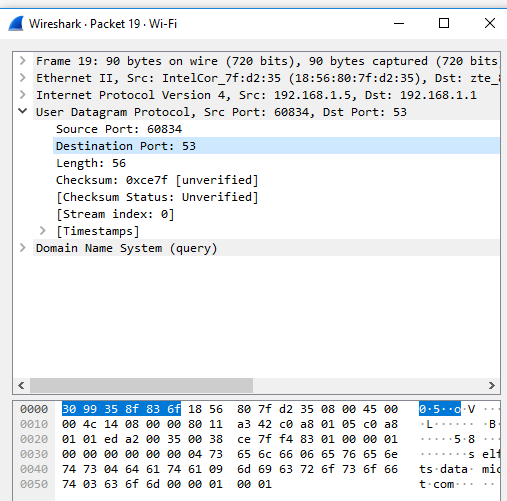
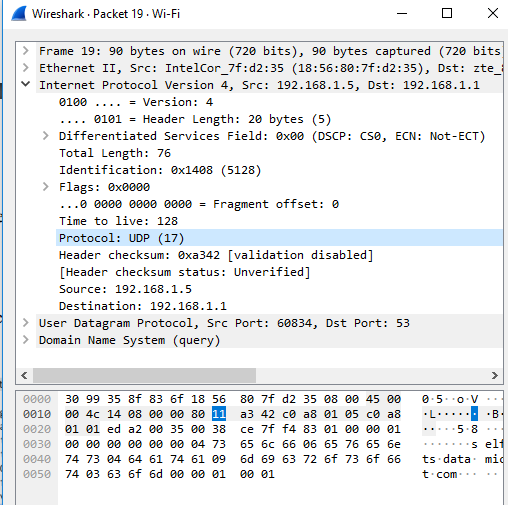
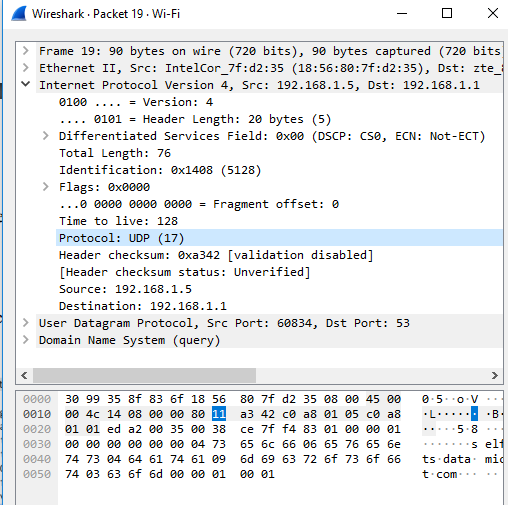
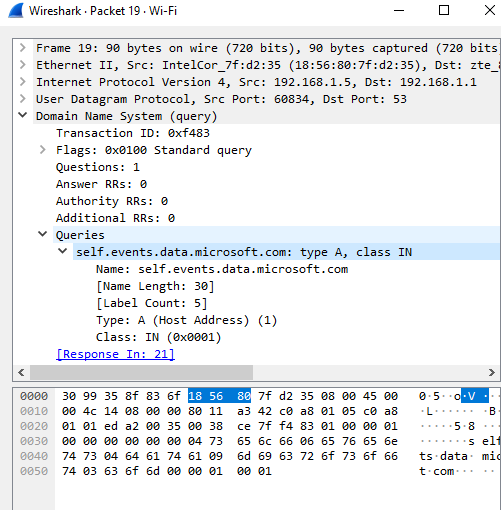
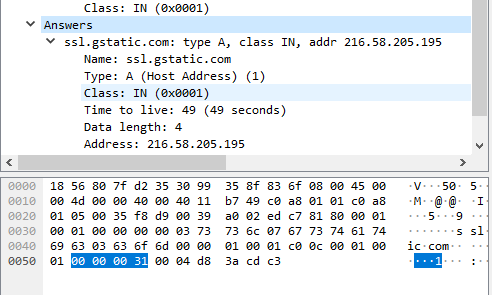
Also the flags = 0 there is no other fragments.

* What is the value in the Identification field and the TTL field?
* Identification = 0x903f (36927)
* Time to live = 128
* There are many filters that can be used the IP packets such as the following:
  + - Display all packets that contain that ip.addr == 192.168.1.12 (all addresses) :



* + - Display all packets with ip.src == 192.168.1.12 (all source addresses):
    - Display all packets with ip.dst == 192.168.1.12 (all destination addresses):

# **Lab 2**

* 1. how many fields there are in the UDP header? Ans: 4 fields (8 bytes): source port, destination port, length, and checksum. 
  2. From the packet content field, determine the length (in bytes) of each of the UDP header fields. Ans: Each of the UDP 4 header fields is 2 bytes long.
  3.  The value in the Length field is the length of what? The value in the length field is the sum of the 8 header bytes, plus the 48 encapsulated data byte
  4. What is the maximum number of bytes that can be included in a UDP payload? Ans: The maximum number of bytes that can be included in a UDP payload is (2^16 – 1) bytes plus the header bytes. This gives 65535 bytes – 8 bytes = 65527 bytes.
  5. What is the source port number? Ans: 60834
  6. What is the destination port number? Ans: 53
  7. What is the largest possible source port number? Ans: The largest possible source port number is (2^16 – 1) = 65535.
  8. What is the protocol number for UDP? Ans: The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value.
  9. The DNS query and response messages. Are then sent over UDP or TCP? Ans: They are sent over UDP
  10. What is the source port for the DNS query message? What is the destination port of DNS response message? Ans: Source port:60834 , destination port: 53
  11.  From and To what IP addresses are the DNS query message sent? Ans: from source 192.168.1.5 and to destination 192.168.1.1
  12.  Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? Ans: The query is of type A and it doesn’t contain any answers
  13. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? Ans: The response DNS message contains one answer containing the name of the host, the type of address, the class, and the IP address
  14. What is the IP address of the DNS server? Ans: 192.168.1.1

# **Lab 3**

# **Lab 4**

Laboratory #4 (TCP and HTTP):

HTTP AND TCP PROTOCOLS

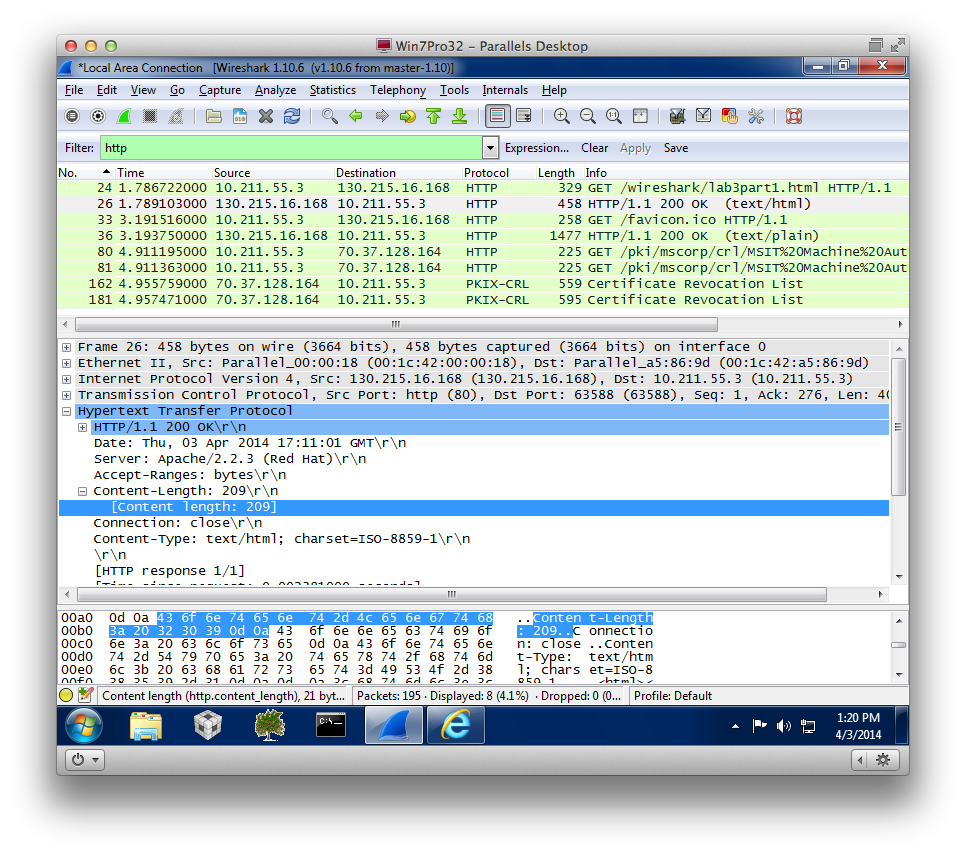
\* We will talk in this lab about the http and the tcp protocol, the http is an abbreviation of his word(Transmission Control Protocol) It is an abbreviation for Tcp, .(Transmission Control Protocol)

\* Open a browser and log in to any website, then open Wireshark and start this process

The capture of its blue shark tag above will start to have protocols The filter for http will show all the packets of the protocol by default http open Any one of them

\* It will be opened by a hypertexy trandfer protocol

1- The word "post" or "get" means "my" parameters The needs that I do request request remain clear, which means that they are present in the URL What I sold, unlike the post post, is the one I ordered to be located at The message itself is aired, and after that, it will open a menu again



1. What is the request Method?

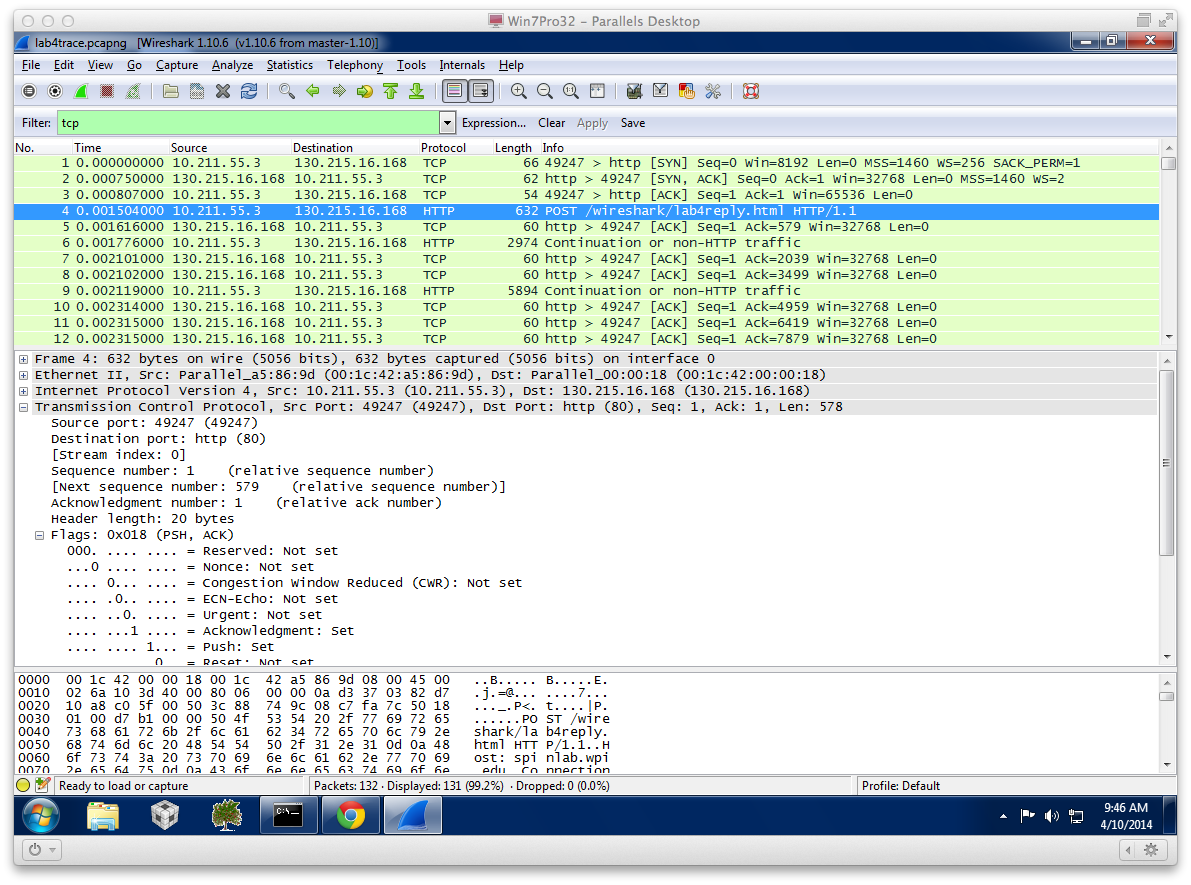
I will see it provided by post, i.e. my type of recoat

1. What is the request URI?

This is the URI that I am applying for

1. What is the request Version?

For example, HTTP / 1.1. This means that I am saying it Show the version, the http value is 1.1, the http is more than the version (1.2,1.1, 1.0)

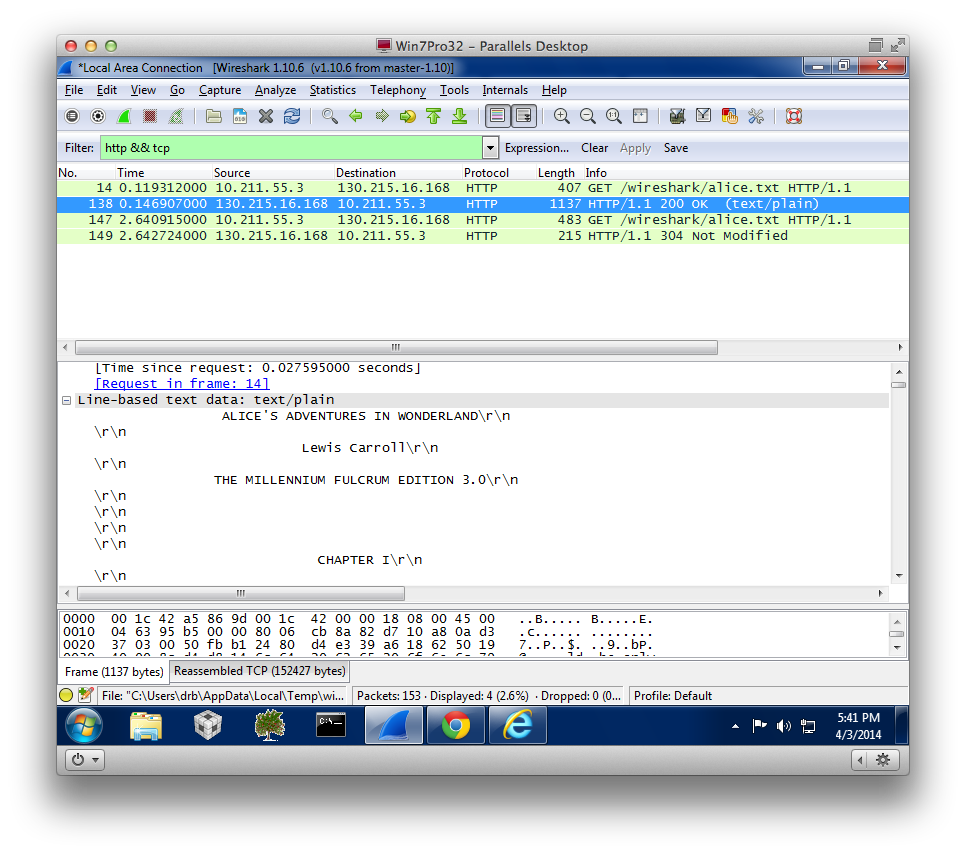


4-What is content of the host field?

Who ever I am going, I will see numbers in front of it,forexample.)192.168.1.8 : 5357.(

5-What is content of the connection field?

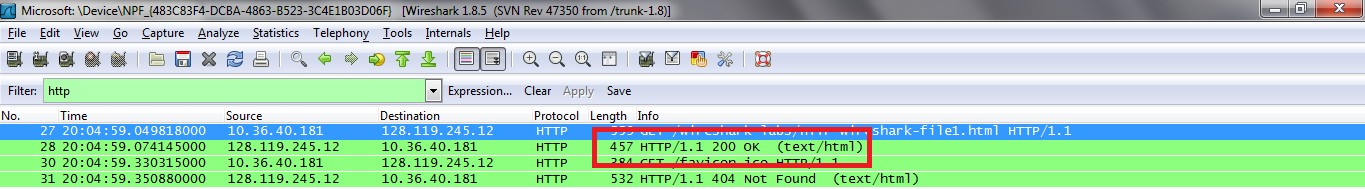
This is the connection type, for example. Keep Alive



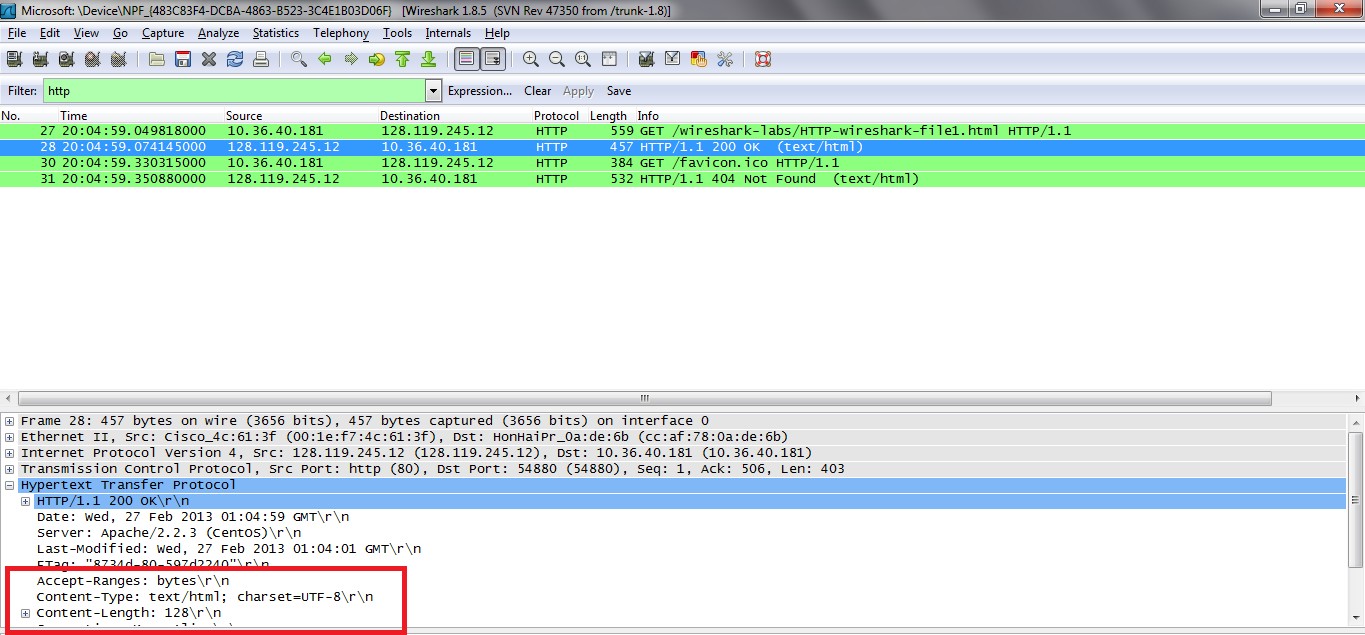
6-What languages does your browser indicate that it can accept to the server?

en-US (US English) as shown

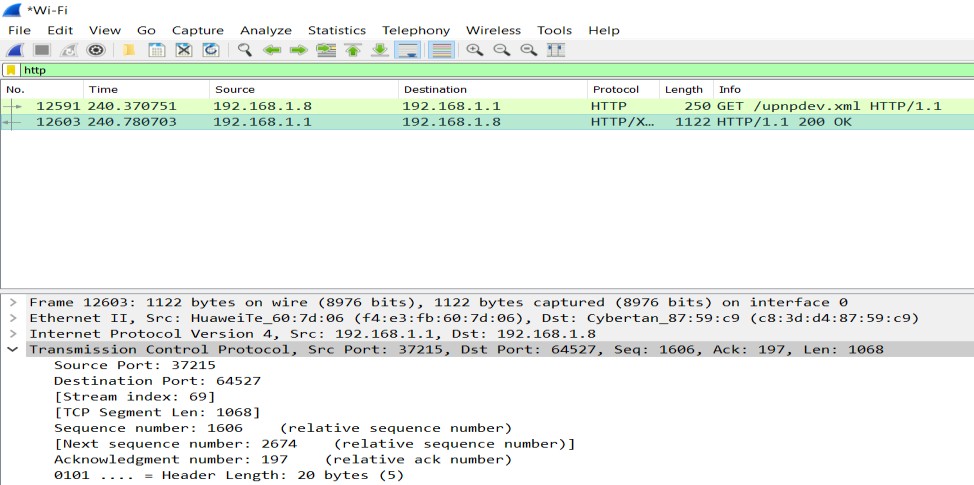
7-What is the status code returned from the server to your browser?



8-How many bytes of content are being returned to your browser?



Opens up hypertext transfer protocol filed And after that content-length We will see its value as it is here 128\r\n . 128 bytes of content are being returned

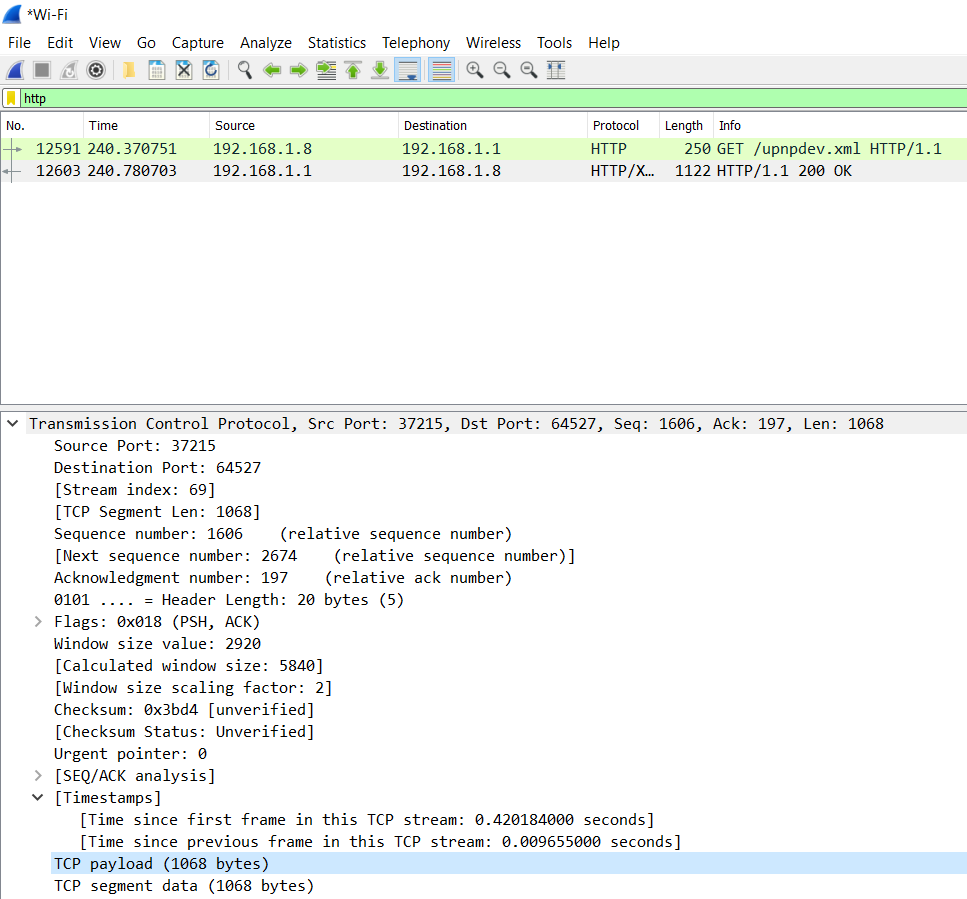


9-What are the source and destination port numbers?

64527 = ـdestination port and 37125 =source port

10-What are the sequence and acknowledgement numbers?

2674 =acknowledgment number



11-What is the TCP header length?

20-bytes =ـheader length

12-How many bytes are in the TCP payload?

TCP payload=1068

13-How many TCP segments are sent?

TCP segments = 1068

# **Lab 5**

# **Lab 6**