Computer Networks
Wireshark Assignment
Due: 24 Farvardin 1399

Take the following steps before answering the questions:

- Download and Install the wireshark software in your system. You can use the link below:

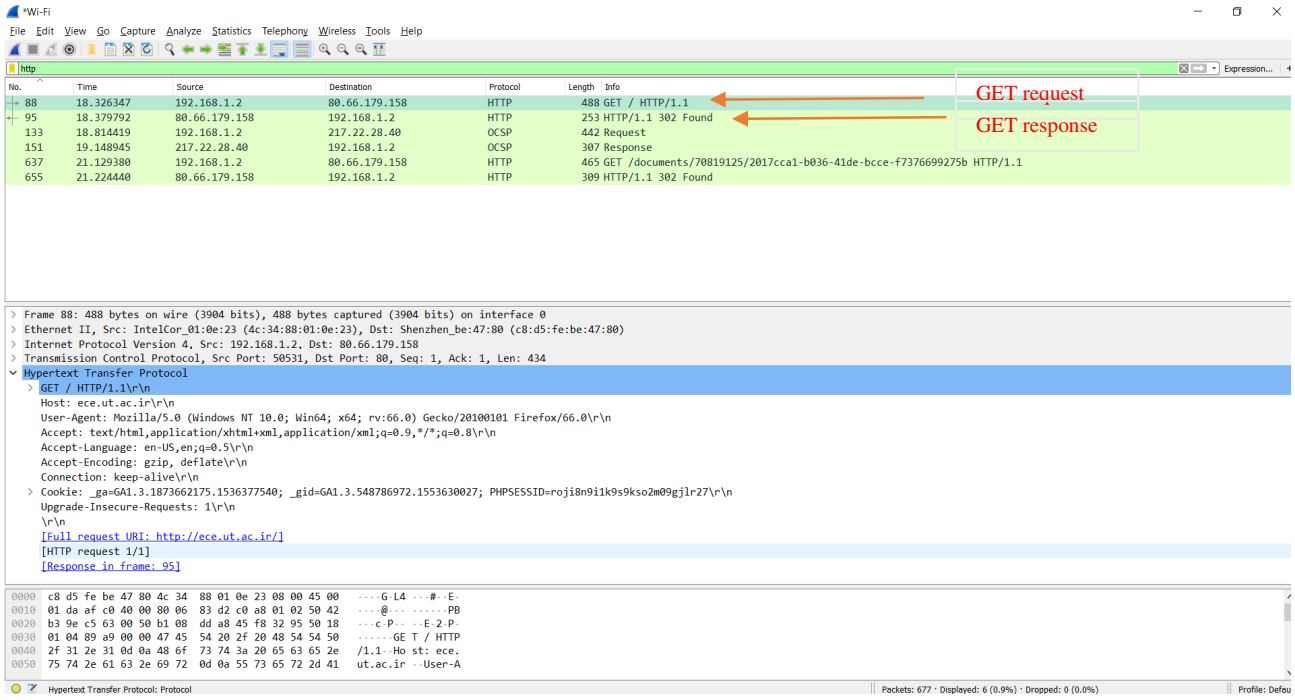
  http://www.wireshark.org/download.html
- Close all VPNs, tunnels, proxies, ….
- Close all the programs in your computer which use Internet.
- Open wireshark and then choose the interface you want to capture form the menu capture, Options.

The goal of this assignment is to get familiar with Ethernet and address resolution protocol (ARP).
Please prepare a report to answer the following 10 questions. You do not need to submit your capture files but include the screen shot of the packets when necessary in the document.

Part 1. Capturing and analyzing Ethernet and IP headers

Follow these steps to prepare:

- Run and start up the Wireshark packet sniffer.
- Enter the following URL into your browser
  www.ece.ut.ac.ir
- When the page is loaded, stop the Wireshark.
- Filter http packets in your captured data. You should be able to see GET request and GET response packets as below. Find the first GET request and Get response packets and write down their packet numbers (88 and 95 in this case). You need these numbers later in this lab.



Select the Ethernet frame containing the HTTP GET message. Recall that the HTTP GET message is carried inside of a TCP segment, which is carried inside of an IP datagram, which is carried inside of an Ethernet frame. Expand the Ethernet II information in the packet details window. Note that the contents of the Ethernet frame (header as well as payload) are displayed in the packet contents window.

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message. Whenever possible, when answering a question you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. You can annotate the printout to explain your answer.

1. What is IP address of the source and destination?
2. What is Time to Live?
3. What is the 48-bit Ethernet address of your computer?
4. What is the 48-bit destination address in the Ethernet frame? What device has this as its Ethernet address?
5. What is the header size?
6. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

Part 2. The Address Resolution Protocol

In this section, we'll observe the ARP protocol in action. Recall that the ARP protocol typically maintains a cache of IP-to-Ethernet address translation pairs on your computer. The *arp* command (in both MSDOS and Linux/Unix) is used to view and manipulate the contents of this cache.
If you are using windows, open a command prompt and type arp –a. You should be able to see the arp table.

1. Write down the contents of your computer's ARP cache. What is the meaning of column value?

In order to observe your computer sending and receiving ARP messages, we'll need to clear the ARP cache, since otherwise your computer is likely to find a needed IP-Ethernet address translation pair in its cache and consequently not need to send out an ARP message.

- Start up the Wireshark packet sniffer
- In the windows command prompt (or Linux shell), type arp – d * to clear the arp table. You many need elevated permission. In this case, run command prompt as administrator.
- Open www.ece.ut.ac.ir website.
- Stop Wireshark packet capture. Again, we're not interested in IP or higher-layer protocols, so change Wireshark's "listing of captured packets" window so that it shows information only about protocols below IP. To have Wireshark do this, select *Analyze->Enabled Protocols.* Then uncheck the IP box and select *OK*.
- Filter the arp messages in the captured file.
- Answer the following questions:

2. Find the arp request and answer the following questions
    a) What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
    b) Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
    c) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?
    d) Does the ARP message contain the IP address of the sender?
    e) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?
3. Now find the ARP reply that was sent in response to the ARP request.
    a) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?
    b) Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?
    c) What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

Goal: the purpose of this lab is become familiar with two protocols of IP suite.

Part 3. DHCP

You need to carry out this lab somewhere that your IP address is assigned dynamically. In order to observe DHCP in action, you will perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands. Do the following:

- Begin by opening the Windows Command Prompt application and type "*ipconfig /release*". This command releases your current IP address, so that your host's IP address becomes 0.0.0.0.
- Start up the Wireshark packet sniffer.
- Now, go back to the Windows Command Prompt and enter "*ipconfig /renew*". This instructs your host to obtain a network configuration, including a new IP address.
- Wait until the "*ipconfig /renew*" has terminated.
- Run "*release*" and "*renew*" one more time.
- Stop Wireshark packet capture.

To see only the DHCP packets, enter into the filter field "bootp". (DHCP derives from an older protocol called BOOTP. Both BOOTP and DHCP use the same port numbers, 67 and 68. To see DHCP packets in the current version of Wireshark, you need to enter "bootp" and not "dhcp" in the filter.)

Answer the following questions:

1. Draw a timing datagram illustrating the sequence of the DHCP packets.
2. What values in the DHCP discover message differentiate this message from the DHCP request message?
3. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?
4. For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.
5. What is the IP address of your DHCP server?
6. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.
7. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?
8. Explain the purpose of the lease time. How long is the lease time in your experiment?