Due Date:09.06.2023 23:55

CENG 312-Computer Networks

Spring 2023

Assignment 3- IP, ICMP, NAT, DHCP

IP and ICMP Section

1. Answer the following questions by analyzing the packet traffic in “assignment3-ip-1”.
    a. Identify the packets in the capture that trigger the "Fragmentation Needed" ICMP message. What are the characteristics of these packets that necessitate fragmentation?
    b. When endpoints receive a packet with the “Fragmentation Needed” flag, how can these packets be processed and what steps can they take to ensure successful delivery? Are there any such steps in this packet traffic? Please explain.
2. Answer the following questions by analyzing the packet traffic in “assignment3-ip-2”.
    a. Identify any fragmented (just one is enough) IP packets in the captured packet capture. How can you determine if a packet is fragmented?
    b. What is the purpose of IP fragmentation? Why is it necessary?
    c. Determine the number of fragments that make up a reassembled IP packet. How can you identify and reassemble fragmented IP packets in Wireshark?
    ç. Calculate the total size of the original IP packet by analyzing the Fragmentation Offset and Fragment Length fields of the fragments.
    d. Analyze the Time to Live (TTL) field in each fragment. Does the TTL value remain the same for all fragments, or does it change? What could be the reason behind any changes in the TTL value?
3. In the packet traffic analysis of “assignment3-ip-3”, it is observed that there is no direct IPv6 connectivity between the two networks. Describe the action that is taken to send IP datagrams between these networks. How would you identify and understand this action within Wireshark? Describe the steps or indicators you would look for to recognize this action.

4.
    - Start packet capture on Wireshark.
    - Perform a “tracert” command to a destination of your choice. (Traceroute is implemented in different ways in Unix/Linux/MacOS and in Windows. See the author’s ICMP lab for detailed information and example.)
    - Stop packet capture on Wireshark.
    - Examine the ICMP packets in your screenshot.

a. Examine the ICMP types and codes that you encounter on Wireshark, and explain each of them.

b. Compare the "tracer" results with the results obtained from Wireshark analysis. Are the intermediate network devices identified in both cases the same? Why or why not.

c. How many packets are sent to each hop (router)?

NAT Section

Using the given python code, generate 2 pcap files and open them in Wireshark (you can install scapy library with the command "pip install scapy")

According to these packets in these files, answer the following questions:

1. What is NAT protocol?
2. These packets are created using Python. If these packets were collected from a real environment, where might these packets be collected? How may these packets be related to NAT protocol, explain.
3. Provide screenshots from Wireshark related to your explanation.

DHCP Section

- Open the command prompt/terminal and Wireshark.
- Begin Wireshark packet capture and type **dhcp** into the display filter field.
- Run the following commands in the command prompt.

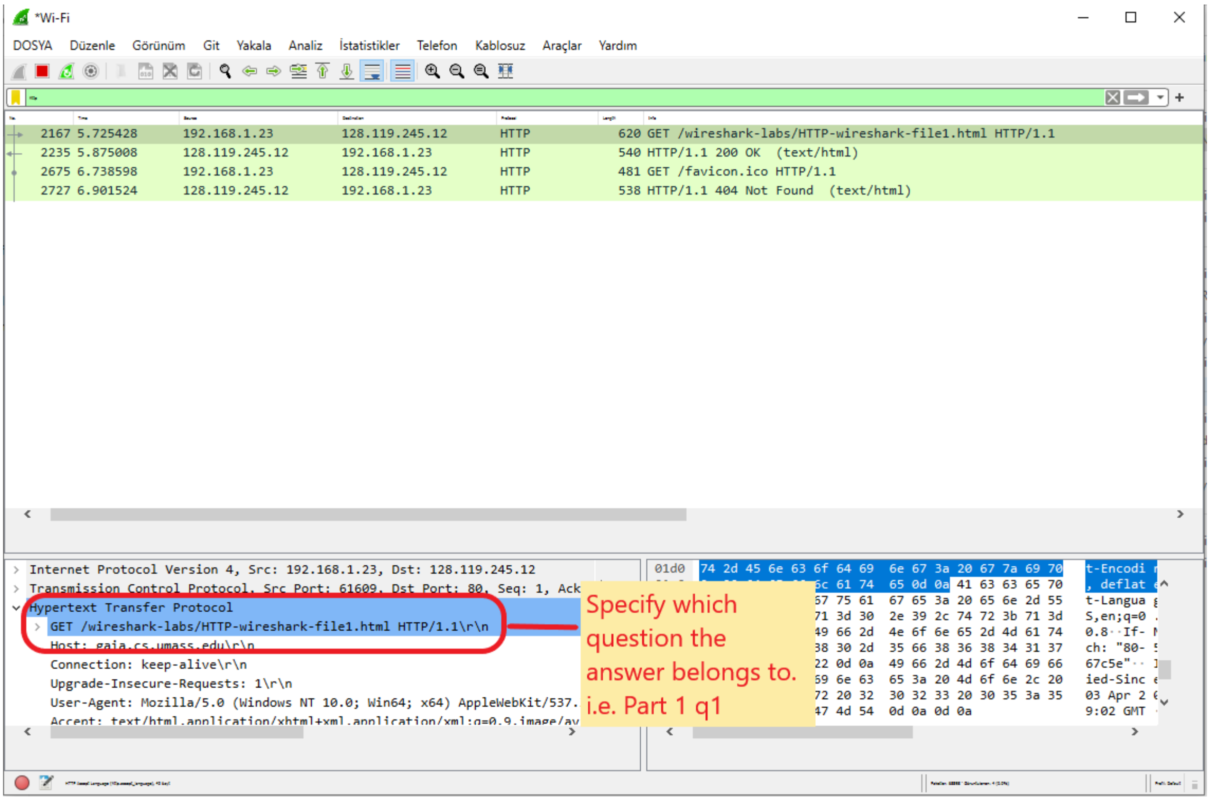
Firstly, enter "**ipconfig /release"** command. Next, enter "**ipconfig /renew**" command. After this command has terminated, enter "**ipconfig /renew"** command again.

Answer the following questions by inspecting the DHCP packets in Wireshark.

1. What is the relation of these "**ipconfig /release"** and "**ipconfig /renew"** commands with DHCP?
2. How many DHCP packets are captured for each command?
3. Are there any differences between captured packets as the result of the first and the second **"ipconfig /renew"** commands? Explain your answer.
4. What types of DHCP packets do you see by inspecting the packets as the result of the first **"ipconfig /renew"** command? Explain these DHCP types.
5. By inspecting the option fields in captured DHCP packets as the result of the first **"ipconfig /renew"** command, do you see common options for all packets? Explain these options.

Submission rules: When answering the questions, you should take the screenshot of wireshark or terminal (if necessary) and indicate where in the message you've found the information that answers the following questions. When you hand in your assignment, annotate the output so that it's clear where in the output you're getting the information for your answer (e.g.,annotate electronic copies with text in a colored font).

Example output:


*Wi-Fi
DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım

```
2167 5.725428   192.168.1.23     128.119.245.12   HTTP   620 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2235 5.875008   128.119.245.12   192.168.1.23     HTTP   540 HTTP/1.1 200 OK  (text/html)
2675 6.738598   192.168.1.23     128.119.245.12   HTTP   481 GET /favicon.ico HTTP/1.1
2727 6.901524   128.119.245.12   192.168.1.23     HTTP   538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Internet Protocol Version 4, Src: 192.168.1.23, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61609, Dst Port: 80, Seq: 1, Ack
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/av
```

```
01d0  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 67 7a 69 70   t-Encodi
                        6c 61 74  65 0d 0a 41 63 63 65 70   , deflat
                        67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua
                        71 3d 30  2e 39 2c 74 72 3b 71 3d   S,en;q=0
                        49 66 2d  4e 6f 6e 65 2d 4d 61 74   0.8··If-
                        38 30 2d  35 66 38 36 38 34 31 37   ch: "80-
                        22 0d 0a  49 66 2d 4d 6f 64 69 66   67c5e"··
                        69 6e 63  65 3a 20 4d 6f 6e 2c 20   ied-Sinc
                        72 20 32  30 32 33 20 30 35 3a 35   03 Apr 2
                        47 4d 54  0d 0a 0d 0a               9:02 GMT
```

Specify which question the answer belongs to. i.e. Part 1 q1

- All submissions must be performed via **Microsoft Teams.**
- You must submit a single pdf file containing the answers to the questions. Do not send separate files, screenshots for each question. All materials related to your answer should be included in a single pdf file. And your filename must follow the following rules:

StudentNo_StudentName_Assignment3.pdf (i.e. 12345_BusraCalmaz_Assignment3.pdf)

- Submissions that do not comply with the rules above are penalized.

.