HW3 - Network Packet Analysis

▾ Class	CS 408
▾ Type	Homework

Name: Berna Yildiran

ID: 26431

1. What is the IP address of http://www.columbia.edu/~fdc/sample.html website?

   128.59.105.24

2. What are the source port and destination port of the HTTP request to http://www.columbia.edu/~fdc/sample.html ?

   Src Port: 50374

   Dst Port: 80

3. What is the IP address of example.com domain?

   93.184.216.34

4. What is the IP address of your default gateway?

   10.50.0.1

5. What are the type numbers of your ICMP Echo request and ICMP Echo reply?

   request: 8

   reply: 0

6. What is the length of the Data field of ICMP Echo reply packet from “example.com”?

   32

7. Write a Wireshark filter for showing packets with destination IP address 192.168.19.15 and destination port 5656?

   ip.dst == 192.168.19.15 && tcp.port == 5656

8. What is the Target IP Address of your ARP Request packet?

   10.50.160.100

9. What is the value of the User-Agent header field of HTTP requests sent by your browser?

   Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36

10. What is the Content-Length header field of HTTP response for "http://www.columbia.edu/~fdc/sample.html"?

    12038

11. What is the HTTP Status Code of HTTP response for "http://www.columbia.edu" ?

    302

12. Locate the DNS query and response messages for "www.sabanciuniv.edu". Are they sent over UDP or TCP?

    UDP

13. Examine the DNS query message for "www.sabanciuniv.edu". What "Type" of DNS query is it? Does the query message contain any "answers"?

    - Two queries of Type: A (IPv4 Address). It doesn't contain any answers (0).
    - Two queries of Type: AAAA (IPv6 Address).

14. Examine the DNS response message. How many "answers" are provided for IPv4? If you obtain more than one answer, what do each of these answers contain, what is the data length of the answers?

    - 2 Answers
        - www.sabanciuniv.edu: type CNAME, class IN, cname virtual2.sabanciuniv.edu
            - Name: www.sabanciuniv.edu
            - Type: CNAME (Canonical NAME for an alias) (5)
            - Class: IN (0x0001)

    - Time to live: 7200 (2 hours)
    - Data length: 11
    - CNAME: virtual2.sabanciuniv.edu
  - virtual2.sabanciuniv.edu: type A, class IN, addr 10.4.10.101
    - Name: virtual2.sabanciuniv.edu
    - Type: A (Host Address) (1)
    - Class: IN (0x0001)
    - Time to live: 7200 (2 hours)
    - Data length: 4
    - Address: 10.4.10.101