CS 315: Computer Networks Lab
Spring 2023-24, IIT Dharwad

End-semester Exam

April 13, 2024
11:30 AM to 1 PM

Total Marks: 64

Instructions

- Login to the Ubuntu OS on your machine using the following credentials:
  - Username: `cs101`
  - Password: `cprg@123`
- Use the correct `.pcapng` file to answer each question.
- Save all your answers in a single text file (named after your roll number), convert it to a PDF, and place it in the `/home/cs101/end_sem_24/` folder.
- At the end of your exam, ensure that the `/home/cs101/end_sem_24/` folder contains only one file, which is your final submission created as per the above instructions.

Part-1: `1_HTTP_Packet_Capture.pcapng`**:** This packet trace was captured while fetching the following URL:
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

1. [4 marks] What are the source and destination IP addresses and port numbers?
2. [1 mark] What is the hostname in the HTTP GET request?
3. [1 mark] Does the HTTP client request a persistent or non-persistent connection?
4. [1 mark] What is the total amount of data being returned by the web server to your browser?
5. [1 mark] State the number of data-carrying TCP segments, with their payload values.
6. [1 mark] How many packets are part of the corresponding TCP stream for the above URL request?
7. [1 mark] How many *Conversation Completeness flags*[1] are set to non-zero values in the HTTP GET and OK packets? List them out. Do you see any difference between the values of these flags between the HTTP GET and HTTP OK packets?
8. [1 mark] Is the HTTP GET request a *Conditional* GET request?
9. [1 mark] From where does the client fetch the IPv4 address of `gaia.cs.umass.edu`?

Part-2: Use the `2_DHCP_Packet_Capture.pcapng` trace file to answer the following questions. This packet trace was captured by executing the following command in the terminal.

```
sudo dhclient en0
```

10. [1 mark] What is the link-layer address of the client interface on which the above packet trace was captured?
11. [1 mark] Which transport layer protocol is used to send the DHCP discover message?
12. [2 marks] A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! 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.
13. [1 mark] What is the IP address of the DHCP server?
14. [4 marks] Match the following DHCP messages with their traffic type.

[1] The TCP Conversation Completeness flags in HTTP GET and OK packets are used to identify elements contained in captured TCP conversations. It assigns a value to each of the following packet types: 32 for RST, 16 for FIN, 8 for DATA, 4 for ACK, 2 for SYN-ACK, and 1 for SYN.

a. Discover
b. Offer
c. Request
d. ACK

i. Unicast-only
ii. Broadcast-only
iii. Either Unicast or Broadcast

15. [1 mark] What is/are the IP Address(es) requested by the client to the DHCP server?
16. [1 mark] In the client's LAN, are the DNS server, DHCP server and first-hop Router hosted on the same IP Address?
17. [1 mark] Is the local DNS server within the client's subnet?

Part-3: Use the `3_ICMP_traceroute_Packet_Capture.pcapng` trace file to answer the following questions. This packet trace was captured by executing the following command in the terminal. The source IP address is 10.250.61.113.

```
traceroute -I www.google.com
```

18. [1 mark] In the given trace, is the traceroute executed using UDP or ICMP messages?
19. [1 mark] In the given trace, how does the client determine when to stop incrementing the TTL values for the ICMP Echo (ping) request packets?
20. [1 mark] What type(s) of ICMP message(s) is/are sent by the client PC?
21. [1 mark] What type(s) of ICMP message(s) is/are received by the client PC?
22. [2 marks] State the sequence of IP Addresses of the nodes along the path from the client to the destination.
23. [1 mark] How does the client map each received ICMP message with the corresponding ICMP Echo Request message?

Part-4: Use the `4_TLS.pcapng` trace file to answer the following questions. This packet trace was captured while fetching the webpage `https://www.cics.umass.edu`.

24. [1 mark] How many versions of TLS are observed in the packet trace? Which TLS version is used for fetching the above webpage?
25. [1 mark] What is the packet number of the first Client Hello message (as part of the TLS handshake) from the client to the web server?
26. [2 marks] In the TLS handshake between the client and the server, how many cipher suites are advertised by the client to the server? Which cipher suite does the server select?
27. [1 mark] How many packets are exchanged between the client and the web server as part of the TLS handshake?

Part-5: Use the `5_Ethernet_and_ARP_Packet_Capture.pcapng` trace file to answer the following questions. This packet trace was captured while fetching "http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html" on the web browser.

28. [1 mark] What is the MAC address of the client interface from which the above webpage was requested?
29. [1 mark] What is the MAC address of the web server interface from which the web page was sent?
30. [1 mark] What is the total length of ARP reply packet?
31. [5 marks] List out the different fields (and their corresponding length), that you observe in this ARP reply packet?
32. [1 mark] How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin for the client's ARP request?

Part-6: Use the `6_Wifi_trace.pcap` trace file to answer the following questions. This trace was captured at the WiFi interface of Apple_98:f0:6f.

33. [2 marks] What are the IP and MAC addresses of the client interface?
34. [2 marks] What are the IP and MAC addresses of the WiFi Access Point?
35. Inspect the first data frame which carries packets across the 802.11 network to answer the following questions.
    a. [1 mark] What are three MAC address fields in this 802.11 frame? Which of these are the MAC addresses corresponding to the source, destination, and BSS?
    b. [1 mark] What is the total length of the frame payload data?
36. [1 mark] What is the channel frequency across the 802.11 network?
37. [1 mark] What are the supported data rates in a Beacon frame?
38. [3 marks] List out the three types of these 802.11 frames[2] and their filter expression. Also, mention the total number of packets belonging to each of these types observed in the trace.
39. [2 marks] Use a filter corresponding to the data frames to find the count of the original data frames[3] and the retransmission data frames.

NS-3 Questions

40. [5 marks] What are the key abstraction objects/components in NS3?
41. [1 mark] Which NS3 tool helps to visualize the traffic between nodes?

[2] The filter "wlan.fc.type" helps to distinguish different types of 802.11 frames
[3] "wlan.fc.retry==0" provides the number of retransmissions