

SEHH2238 Computer Networking

Assignment 2 (Group)

Due Date: 22-Apr-2022 (Week 12, Friday) 18:00

Expected Learning Outcomes:

- Grasp the practical skills in analyzing data communication signal strengths in different physical locations.
- Analyze communication systems from the perspectives of communication architectures, system specifications and implementation techniques.
- Explore the considerations of technical and practical issues in choosing the computer network to use.

Instructions

1. It is a **group assignment [5-6 members]**.
2. Plagiarism will be penalized severely. Marks will be deducted for assignments that are plagiarized in whole or in part, regardless of the sources.
3. Submit soft copy of your assignment on or before the due date.
4. Late submission is NOT accepted.
5. Answer ***ALL*** questions.
6. Please state clearly your source of references. You can also attach your reference materials.

Submission

Submit the files below via **Moodle (class page) by the deadline**. Late submission is not accepted.

- **Report: Each group** submits one copy of report in PDF file. Use the file name *GroupLeaderName_StudentID.pdf* and submit it via Moodle.
- **Peer-to-peer evaluation: Each student** needs to fill in a peer-to-peer evaluation form (to be downloaded from Moodle) on self-evaluation and evaluating the performance of other team members in the same group.

Part A (30%)

Question 1 (10%)

A small organization is given a block of IPv4 addresses with one of the addresses being 10.100.111.216/ n (in slash notation), where n is the ("sum of last digits of your student numbers" mod 10) + 17.

- a) Write n and the mask in dotted decimal notation.
- b) What is the range of the block?
- c) What is the network address?
- d) What is the broadcast address?

Show how you arrive at your answers by using binary operations.

Question 2 (20%)

An ISP is granted a block of IPv4 addresses starting with 172.31.0.0/16. The ISP needs to distribute these addresses to three groups of companies as follows:

- a) Group A has 4 companies; each needs at most 1000 addresses. [host](#)
- b) Group B has 32 companies; each needs at most 100 addresses.
- c) Group C has 128 companies; each needs at most 30 addresses.

Using the smallest sub-blocks, design the sub-blocks and give the slash notation for each sub-block. The three groups must be allocated consecutive sub-blocks starting with 172.31.0.0.

For Group A, you should fill out the first and last addresses for ALL companies. For Groups B and C, you should fill out the first and last addresses for the first FOUR and last FOUR companies. You may use the sample tables as given below. The addresses should be in slash notation.

	First address ($x.x.x.x/n$)	Last address ($x.x.x.x/n$)
1 st company		
2 nd company		
3 rd company		
4 th company		
...		
...		
...		
...		

Part B Protocol Analysis Project (70%)

In this project, we are going to perform protocol analysis using the tool Wireshark. You will be asked to submit the packet dump to support your answers in this assignment. All information submitted will only be used for marking this assignment and will be destroyed within 1 month after the assignment has been marked.

Introduction



Wireshark is open source software which is a network packet analyzer. It captures network packets on the specified interface and presents captured packet data in details.[1] In this project, we will use it to learn network protocol internals.

Installation

Installation is simple. Simply download the Wireshark installer from <https://www.wireshark.org/download.html> and execute it. Use the default options will do. For MacBook users, you may need to use MacBook Terminal to work on this assignment.

Using Wireshark

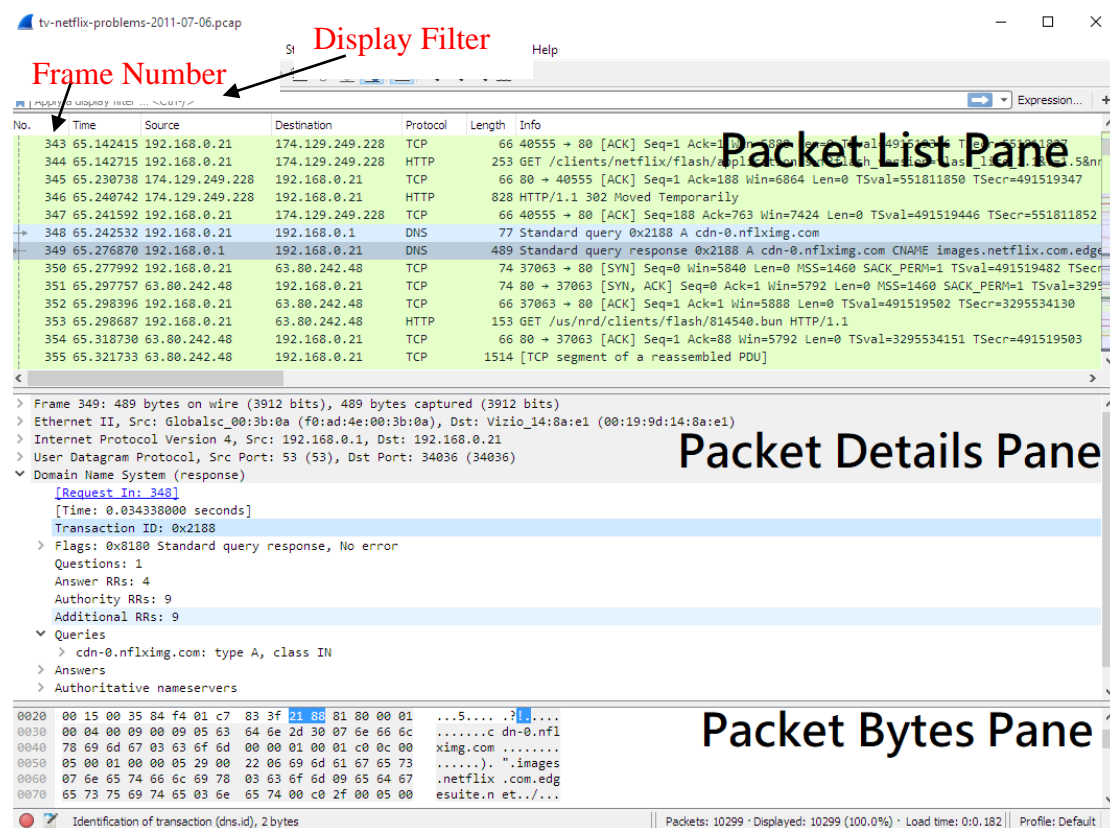
The first time you start Wireshark, you will be asked which interface you want to capture the traffic. Choose either the Ethernet or Wifi.

To start packet capture, choose Capture → Start or press the Start button on the menu  to capture live packets. You will see packet details as in the Main Window. To stop the capture, from the menu, choose Capture → Stop or press the “Stop” button  on the menu.

Note that Wireshark by default captures ALL packets seen on the interface and it may consume a lot of resources and render your system unstable. You should stop the capture when you’ve got enough data to study.

Below is a sample main window taken from wireshark.org. Note where the **Packet List Pane**, **Packet Details Pane** and **Packet Bytes Pane** are. Also note the **Frame Number** and **Display Filter**.

- The **packet list pane** displays a summary of each packet captured. By clicking on packets in this pane you control what is displayed in the other two panes.
- The **packet details pane** displays the packet selected in the packet list pane in more detail.
- The **packet bytes pane** displays the data from the packet selected in the packet list pane, and highlights the field selected in the packet details pane.



Filtering the dump to get meaningful results

Once you have captured some packets or you have opened a previously saved capture file, you can view the packets that are displayed in the packet list pane by simply clicking on a packet in the packet list pane, which will bring up the selected packet in the packet details pane and byte view panes. [2]

Note that as you navigate through the different fields in the packet details pane, the relevant bytes will be highlighted in the packet bytes pane.

You may find there are too many packets to view. How can you filter out the useful information? You will need to build your own **Display Filter Expressions** and put them into the **Display Filter** in the main Window. Try the below sample expressions and see what result do you get.

Purpose	Display Filter Expression
Show packets with ip address 192.168.0.1	ip.addr == 192.168.0.1
Show only tcp traffic	tcp
Show TCP traffic with source IP address 192.168.0.1	ip.src_host == 192.168.0.1 and tcp

Saving your capture

In the below exercises, you will be asked to save your capture to submit together with your report. You can also save your capture for later analysis.

To save your capture, simply go to File→Save As, choose the correct location and save the file as type .pcapng.

Reference Web Sites

- | | | |
|-----|---------------------------|--|
| [1] | Introduction to Wireshark | to https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs |
| [2] | User Interface | https://www.wireshark.org/docs/wsug_html_chunked/ChUseMainWindowSection.html |
| [3] | Display Filter | https://wiki.wireshark.org/DisplayFilters |

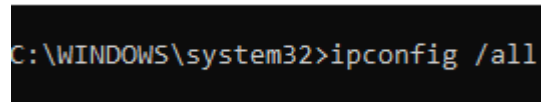
Question 1 Basic information about your device (4%)

Your own Network Interface Card will be the source of all the traces. Thus you will need to collect information about its MAC (Physical) address and IP address.

You may consider masking part of your MAC addresses below to maintain privacy. Your IP address may change from time to time. You should collect your IP address information just before you perform the Wireshark captures.

Steps:

1. Open a command prompt. Issue the command “ipconfig /all”. You will see all network interface cards listed.



```
C:\WINDOWS\system32>ipconfig /all
```

2. Choose the one you are using (Ethernet or Wi-Fi).
3. *Copy and paste a screen capture below AND fill out the below table.*

Physical Address	
IPv4 Address	
Default Gateway	
DNS Server (s)	

Question 2 Ethernet Header (8%)

Steps:

1. Start a Wireshark capture.
2. Use a display filter to display only traffic from your ip address with TCP protocol.
In your report, write down the display filter expression you will use.
3. From the frame you captured, study the **Ethernet header**. Fill out the below table.
Copy and paste a screen capture of the Packet Bytes Pane below AND fill out the below table.

	Information (in hex)
Destination Ethernet Address	
Source Ethernet Address	
Type	

4. To find out which host the Destination Ethernet address belongs to, in Command Prompt, issue the command “arp -a” to display the ARP table. *Copy and paste a screen capture below.*
5. According to the information in the ARP table, answer the following questions:
 - i. Which IP address is mapped to the Destination Ethernet address in 3)?
 - ii. Is it the same as the Destination IP address for the same frame in the Wireshark capture?
 - iii. To which device does this Ethernet address belong?

Question 3 IP Header (12%)

Steps:

For the same frame captured as in Q2, look at the **IP header**. *Copy and paste a screen capture of the Packet Bytes Pane below AND fill out the below table.*

Header Field	Value (hex)	Meaning
Version		
Header Length		
Service type		-
Total Length		
Identification		-
Flags		
Fragment Offset		
Time to Live		
Protocol	06	TCP
Header checksum		-
Source IP address		
Destination address		

Question 4 Loading a Web page (25%)

Steps

1. Start a Wireshark capture.
2. Open a browser. Open the web page <https://www.cpce-polyu.edu.hk>.
3. Click some links on the CPCE homepage.
4. Close the browser tab.
5. Stop the Wireshark capture.
6. *Save the capture as class_group_no_webpage.pcapng. Submit as a separate file.*
7. *Analyze the captured packets and answer the following questions.*

**** hint:** apply the filter *ip.addr == (ip address) and tcp.port == (port number)* to your capture.

- a) *What is the ip address of the CPCE Web server?*
- b) *Identify the server and client port numbers.*

- c) Identify the first 3 packets exchanged by *filling out the following table*.

No.	Source address	IP	Destination IP address	Source port no.	Destination port no.	Flags (0x)	What happened?

- d) Identify the first TLSv1.2 Server Hello packet *and fill out the following table*.

	Length in bytes
Total length	
Ethernet header length	
IP header length	
TCP header length	
TCP Segment length	

- e) Identify the 3 packets for connection tear-down. *Fill in the following table*:

No.	Source address	IP	Destination IP address	Source port no.	Destination port no.	Flags (0x)	What happened?

- f) After the server issues a FIN request, the client still sends TCP Keep-Alive packets. *Explain briefly the connection tear down process observed.*

- g) Identify a TLSv1.2 packet from the web server which is a “TCP segment of a reassembled PDU”. *How many TCP segments are reassembled? How many bytes are there? Fill in the following table with ALL the reassembled TCP segments.*

Frame No.	payload	Payload size (bytes)	Sequence no.	Acknowledge number

- f) Identify the original frame which these frames acknowledge. *What is its frame number? What is the TCP segment length? Put a screen capture of the TCP header of this frame (showing the sequence number) in the space below.*

Question 5 Dynamic Name Service (DNS) (6%)

Steps:

From the same capture, filter out the DNS traffic. Identify THREE pairs of DNS request/response frames and *fill out the below table*.

Frame no.	Source address	IP address	Destination IP address	Transport layer protocol	Source port number	Destination port number	Domain name/IP address

Question 6 ICMP (15%)

“ping” is a command to check connectivity to a remote host. We are going to study how it works by using Wireshark.

Steps:

1. Start your capture on Wireshark.
2. On your command prompt, issue a ping command to a certain remote host by its domain name (e.g. `ping www.microsoft.com`). Note that some hosts may be firewall protected and the pings may be timed out.
3. There should be 4 “Reply from ip_address”, telling you the time it takes for a round trip to that server and the TTL.
4. Stop the capture on Wireshark.
5. *Save the capture as class_group_no_ping.pcapng. Submit as a separate file.*
6. *Answer the following questions.*

****** You may need to use “`ipconfig /displaydns`” and “`ipconfig /flushdns`” to clear your DNS cache before you perform the ping. Elevated rights are required. Open your Command Prompt as “administrator”.

- a) Perform a screen capture of the resulting ping command. *Paste it in the space below.*
- b) The ping command pings the specified host by IP address. Thus, the host

name is resolved into ip address by DNS before the ping request is sent to the host.

Can you see this in action in the Wireshark capture? Write down ONE filter expression you used to obtain the packets for both the DNS request/response and also the ping request/replies.

c) *Perform a screen capture of the filtered header summary in the Packet List Pane, showing the sequence of events, and put in the space below.*

d) *Fill out the below table with the filtered traffic.*

Frame no.	Source address	IP	Destination address	IP	Protocol	Source port number	Destination port number	Domain name/IP address
					DNS			
					DNS			

Frame no.	Time	Source address	IP	Destination IP address	Protocol	Time to Live	Type	Response Time	Sequence Number (BE)	Sequence Number (LE)
					ICMP					
					ICMP					
					ICMP					
					ICMP					
					ICMP					
					ICMP					
					ICMP					
					ICMP					

e) *Can you find any timestamp in the packet headers? How does Wireshark get the response time? Show your evidence.*

f) *Referring to your screen capture in a), how many bytes of data are sent with this ping request?*

Identify the “data” carried by the packet from your Wireshark capture. Copy and paste the data as ASCII AND a screen capture of the Packet Bytes Pane data below.

~ End of Assignment 2~