Assignment 1: Reading a PCAP File

Computer Networks (CS-UH 3012) - Spring 2022

1 Code of Conduct

All assignments are graded, meaning we expect you to adhere to the academic integrity standards of NYU Abu Dhabi. To avoid any confusion regarding this, we will briefly state what is and isn't allowed when working on an assignment.

1. Any document and program code that you submit must be fully written by yourself.
2. You can discuss your work with fellow students, as long as these discussions are restricted to general solution techniques. In other words, these discussions should not be about concrete code you are writing, nor about specific results you wish to submit.
3. When discussing an assignment with others, this should never lead to you possessing the complete or partial solution of others, regardless of whether the solution is in paper or digital form, and independent of who made the solution.
4. You are not allowed to possess solutions by someone from a different year or section, by someone from another university, or code from the Internet, etc.
5. There is never a valid reason to share your code with fellow students.
6. There is no valid reason to publish your code online in any form.
7. Every student is responsible for the work they submit. If there is any doubt during the grading about whether a student created the assignment themselves (e.g. if the solution matches that of others), we reserve the option to let the student explain why this is the case. In case doubts remain, or we decide to directly escalate the issue, the suspected violations will be reported to the academic administration according to the policies of NYU Abu Dhabi. More details can be found at: https://students.nyuad.nyu.edu/academics/registration/academic-policies/academic-integrity/

2 Assignment Goal

The goal of this assignment is to implement a program to read, parse and display UDP packets from PCAP files on the command line terminal. This will give you practice in working with PCAP files, understanding their structure and getting familiar with the UDP packet format.

3 PCAP File Structure

Packet Capture (PCAP) files are data files that are created using network analyzers like Wireshark or tcpdump to collect and record packet data from a network communication. These files are mostly used to identify and solve network issues and contain a copy of all captured

packets for a given timespan. Each packet consists of a Record Header (16 bytes, can be ignored for this assignment) and its corresponding data for the respective ISO/OSI layers (layer 2 to 4 in this assignment only).

The format of a PCAP file containing two UDP packets is shown below:

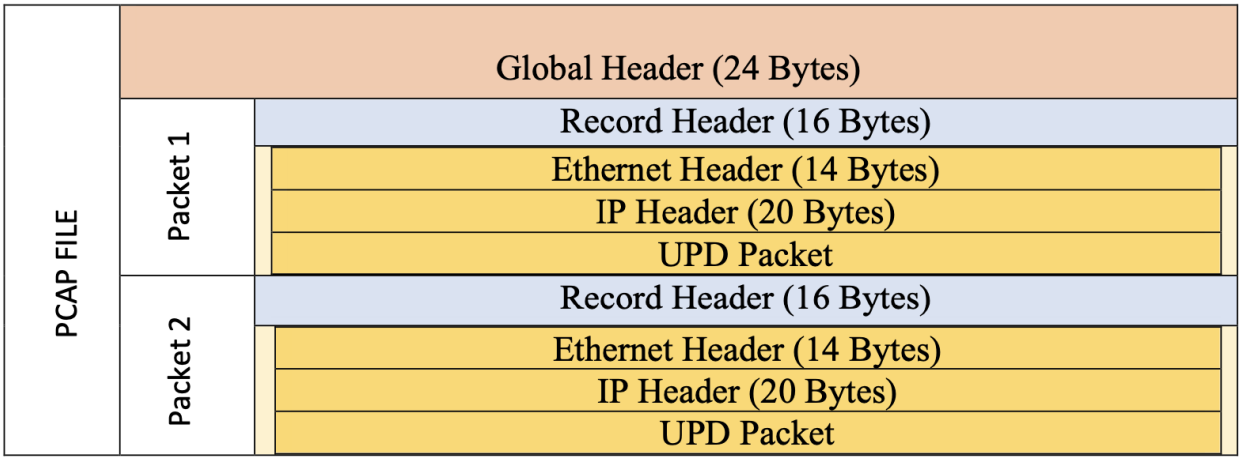

Figure 1: Format of a PCAP file

Refer to www.ietf.org/id/draft-ietf-opsawg-pcap-00.html for more details of the PCAP file format.

4 UDP Packet Format

The User Datagram Protocol (UDP) is a transport layer protocol that uses a simple and connectionless communication model to send messages between two hosts. A UDP packet (datagram) consists of an 8-byte header and a data section of up to 65,535 bytes. The structure of an UDP datagram format is shown below:

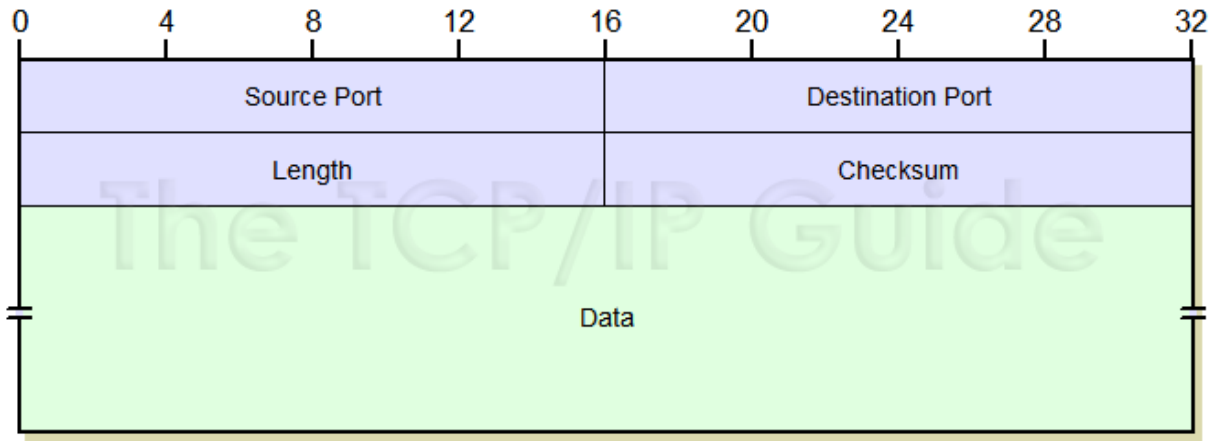

Figure 2: UDP packet format
(Image source: www.tcpipguide.com/free/t_UDPMessageFormat.htm)

Source Port: The 16-bit port number of the process that originated the UDP message on the source host.
Destination Port: The 16-bit port number of the process that is the ultimate intended recipient of the message on the destination host.
Length: The length of the entire UDP datagram, including both header and Data fields.
Checksum: An optional 16-bit checksum computed over the entire UDP datagram plus a special "pseudo header" of fields.
Data: The encapsulated higher-layer message to be sent.

Please note: You need to convert the UDP header fields from network byte order to host byte order before printing. You can use the `ntohs()` function of C to do the conversion.

5 Task Description

The task of this assignment is to write a C program which reads a PCAP file containing multiple UDP packets. The program should accept a PCAP file as a command line argument (if no argument is given, an error message should be displayed) to identify which file to read from:

```
./read_pcap.out <pcap_file>
```

The two files (capture1.pcap and capture2.pcap) provided for this assignment consist of multiple UDP packets. The program should read all UDP packets from the file and store their content in a data structure of your choice. The program should then display the UDP packet headers and their corresponding data (in ASCII representation), as shown in Figure 3.

The output of the program should look like shown below:

```
iMac:lab2 khalid$ gcc read_udp.c
iMac:lab2 khalid$ ./a.out capture2.pcap

-------------------------
Src Port: 50717
Des Port: 8801
UDP Packet Length: 89
Checksum: 0x412f
.......H^......@T....-..!....8B...VN.Y!c.....:.J.s.5.e.......BT.D..3.T.@y....A.E.
-------------------------
Src Port: 8801
Des Port: 50717
UDP Packet Length: 89
Checksum: 0x870c
.......H^......@..^i.J.*V @..x...a.#0...0..?9....#.E9a..WX..*j-.6....Ug...h..~.s.
-------------------------
```

Figure 3: Example program output of capture2.pcap file

You can use the following website to verify your output: apackets.com

6 Grading

Description	Score (/4)
Successful compiling of the program using a Makefile	0.5
Proper use of command line argument and displaying error message if argument is missing	0.5
Printing of the packet content, as depicted in Figure 3	2
Usage of meaningful comments	1

7 Submission Details and Policy

Submission Deadline: The deadline of this assignment is after 5 days of its release via Brightspace. No extensions will be given.

Submission Format and System: You can directly submit your files (C file and Makefile) as a zip file on Brightspace (https://brightspace.nyu.edu/). Due to technical limitations, submissions via email are not accepted.

Late Submissions: Late submissions will be penalized by 10% per 24 hours. In case of a late submission, please upload your zip file to Brightspace and inform the TA and the professor.