Introduction

The goal of the project was to create the Ethernet packet sniffer. Sniffer should be able to analyse input and output traffic on a given interface, and to filter certain types of packets. The program supports packet detection of these protocols:

- IPv4:
  - ICP
  - UDP
  - ICMPv4
- IPv6:
  - ICP
  - UDP
  - ICMPv6
- ARP

Implementation details

General

The program utilises `pcap` and `netinet` libraries, the former for packet capturing and the latter for convenient type-casting of packet's header structures on octet sequences.
Entire program is made in OOP manner (except for the packet capture function – it can't be passed as an argument to the `pcap_loop` function). The `sniffer class` interface is stored in `sniffer.hpp` file, methods' implementation is stored in `sniffer.cpp` file.
The `Sniffer class` encapsulates all the required parameters such as strings for filter expression and interface, error buffer for `pcap` functions, integers for packet enumeration and packet's count limitation.

Command line argument parsing

The program uses `getopt_long` function with predefined arrays for both short and long options for command line arguments parsing. The string of filter expression is "constructed" during the arguments parsing: each new filter option (either packet types or port number) is added to result filter expression with `'or'` (in case of packet type) or `'and'` (in case of port number) between them.

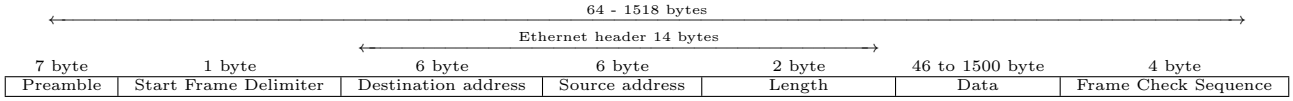
Setting up the filter

Upon finishing of parsing, the program initialises `pcap` library, opens specified device, then it compiles and sets filter according to filter expression. If there is no interface specified program finds first device available via `pcap_findalldevs` function. If neither packet filters nor port are specified, then sniffer will listen on all ports to packets of all protocols.

Packet capturing

Headers

Ethernet header



IPv4 IPv4 packets' size is not fixed.

0	4	8	16	31
Version	IHL	TOS	Total length	
Identification			Flags	Fragment offset
TTL		Protocol	Header checksum	
Source address				
Destination address				
Options				
Data				

IPv6 IPv6 packets have fixed size.

0	4	12	31
Version	Traffic class	Flow label	
Payload length		Next header	Hop limit
Source address			
Destination address			

ARP ARP packets have fixed size.

0	2
Hardware type (HTYPE)	
Protocol type (PTYPE)	
Hardware address length (HLEN)	Protocol address length (PLEN)
Operation (OPER)	
Sender hardware address (SHA) (first 2 bytes)	
(next 2 bytes)	
(last 2 bytes)	
Sender protocol address (SPA) (first 2 bytes)	
(last 2 bytes)	
Target hardware address (THA) (first 2 bytes)	
(next 2 bytes)	
(last 2 bytes)	
Target protocol address (TPA) (first 2 bytes)	
(last 2 bytes)	

Processing pipeline

After everything is set, program starts sniffing packets inside `pcap_loop` via `packetHandler` function. Firstly, it defines variables for packet parsing, such as integers for length of packet, length of packet's part present, length of header offset for proper header type-casting; initialises variables for source and destination ports and defines Ethernet header by casting `ether_header*` structure on byte sequence in `packet` function argument.

Then the program defines timestamp by creating two string buffers (first for day-time, second for timezone) and integer for milliseconds. The strings are created by passing product of `localtime` function with corresponding options to `strftime` function, the milliseconds variable is a product of `lrint` function. All source data (seconds and milliseconds since the *Epoch*) is obtained from `header` of `pcap_pkthdr` type argument at the first place.

MAC source and destination addresses are also given by `header` argument's attributes. They are formatted (`\d\d:\d\d:\d\d:\d\d:\d\d:\d\d`) and passed to according variables by `sprintf` function.

Then function prints acquired information and proceeds in packet processing.
Afterwards, depending on ether type, function branches into three cases (IPv4, IPv6, ARP ether types), obtains source and destination IPs from corresponding ether type header and passes them to `ntohs` function, increments length of header offset and prints ports.

After that (except for ARP case) it branches again on 3 different cases (TCP, UDP, ICMPv4/6), gets source and destination ports and prints them.

At the end function prints out octet representation of entire packet via nested loop with the step of 16.
It prints 16 octet per line in such format:
<hexadecimal offset>: <hexadecimal octets' representation> <ascii octets' representation>

Output format

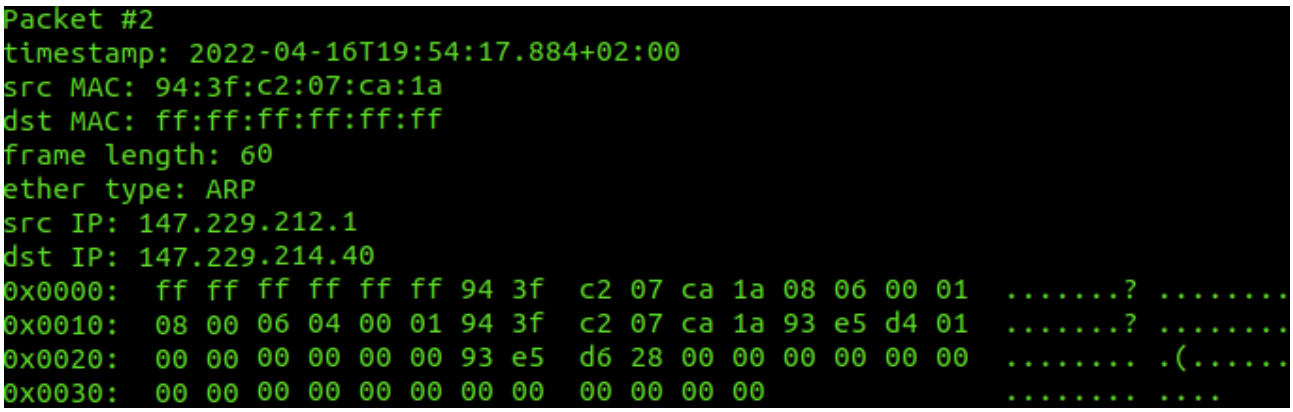


Figure 1: ARP packet

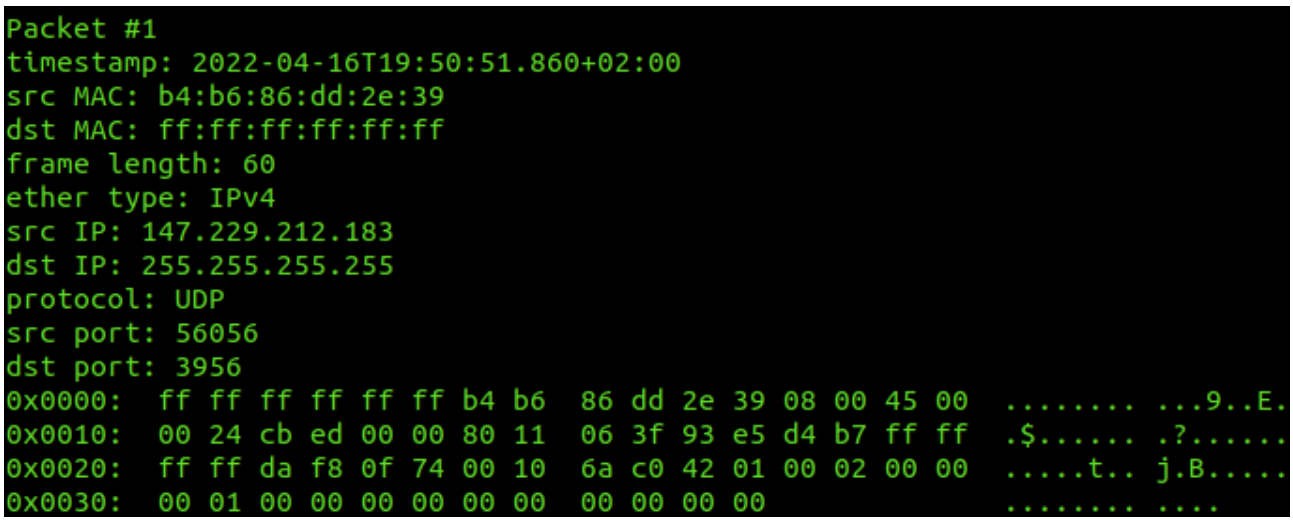


Figure 2: UDP packet

Testing

Testing part consisted of comparing the results of the program and the results of wireshark software.

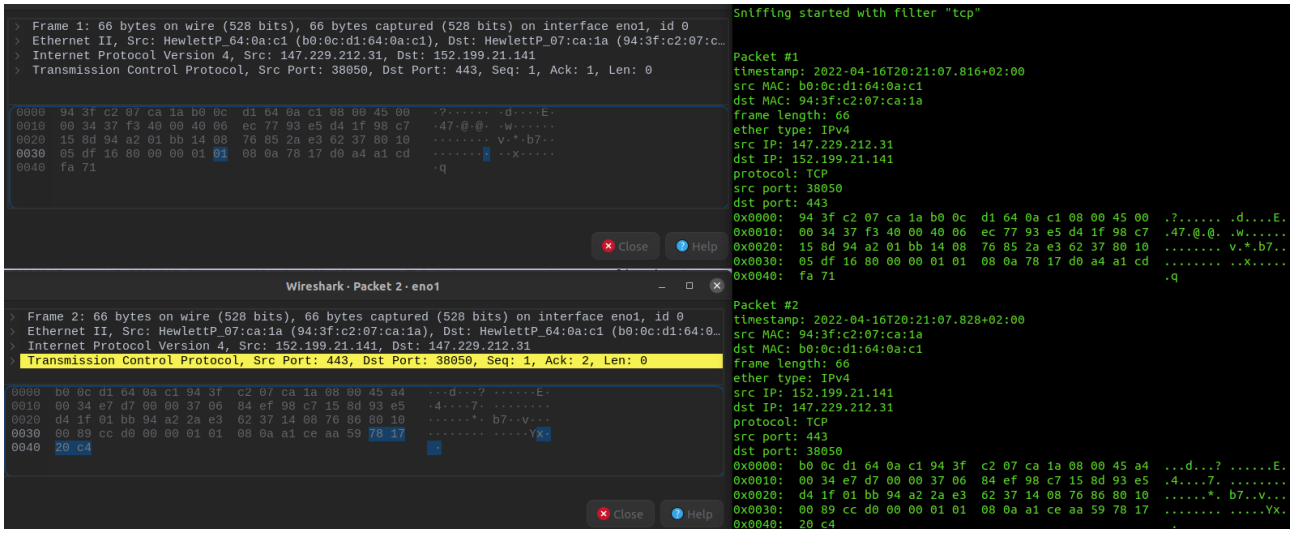


Figure 3: TCP packets comparison

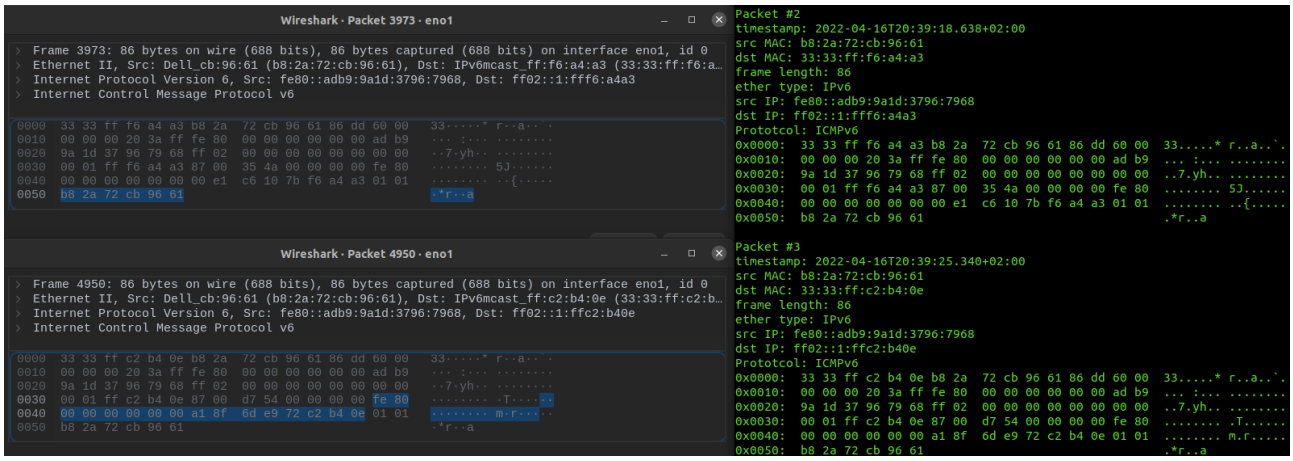


Figure 4: ICMPv6 packets comparison

References

[1] *Size of packets, type-casting.*
https://www.cs.dartmouth.edu/~sergey/cs60/lab4/tcp-listen.c

[2] *Printing octet representation of packets.*
https://www.binarytides.com/packet-sniffer-code-c-libpcap-linux-sockets/

[3] *Timestamp formatting.*
https://stackoverflow.com/questions/3673226/how-to-print-time-in-format-2009-08-1

[4] *Libpcap functions*
https://stackoverflow.com/questions/3673226/how-to-print-time-in-format-2009-08-1

[5] *Pcap functions usage code example.*
https://www.tcpdump.org/pcap.html

[6] *Ethernet frame info.*
https://en.wikipedia.org/wiki/Ethernet_frame