Practical task on traffic analysis

1. Install Wireshark packet analyzer and see how it works
2. Run the program and enable packet capture
3. Go to any web site, such as epam.com
4. Click on any of the tabs on this site
5. Close the web browser window
6. From the command prompt, run the command: ping 8.8.8.8
7. Stop packet capture
8. Determine the size of the smallest and largest packet
9. Determine which packet length is the most
10. To which public IP address was the most IP traffic transmitted?
11. From which public IP address was the most IP traffic received?
12. Determine the percentage of TCP, UDP, and ICMP packets
13. Filter ICMP packets
14. Find in the header of one of them the MAC addresses of the source and destination, the IP addresses of the source and destination.
15. Find a pair of Echo Request and Echo Reply packets, find the value of the TTL field in them, and explain why it has a different value.
16. Change filter, new filtering condition – TCP segments with SYN flag.
17. In one of the segments, find the source and destination ports, the size of the window, the sequence number, and the acknowledgment number. Explain the purpose of these fields.