Assignment 2: Using Wireshark

Assignment goals:

1.Learn how to use wireshark;

2. Reinforce the understanding of TCP and DNS

Background:

Wireshark is a network protocol analyzer that allows for live capturing and analysis of network traffic in real-time. It can also analyze pre-captured files. With a user-friendly interface and a comprehensive set of features, Wireshark is widely adopted by network administrators, security experts, and developers for troubleshooting, protocol analysis, and network optimization.

Wireshark supports a wide range of protocols, including TCP, IP, HTTP, DNS, FTP, and many others. It provides detailed packet inspection, filtering, and searching capabilities to help users quickly identify network issues, security vulnerabilities, and performance bottlenecks. Additionally, Wireshark offers advanced functionality such as VoIP analysis, decryption of SSL/TLS traffic, and integration with other tools like tcpdump and TShark.

Overall, Wireshark is an indispensable tool for anyone involved in network analysis or troubleshooting. It can help users gain a deep understanding of network behavior, identify potential problems, and optimize network performance.

Task 1 (Observe TCP，45 Points):

1. Download and install Wireshark (https://www.wireshark.org/) on your computer.

2. Open a TCP connection. For example, you can visit a website, which will establish a TCP connection.

3. Capture the data packets of this TCP connection using Wireshark.

4. Analyze the captured TCP data packets using Wireshark and finish following the steps and include them in your report.

- Observe the TCP handshake process. Please provide a screenshot as proof that you have completed this process.

- Observe the SYN and ACK packets. Please provide a screenshot as proof that you have completed this process.

- What are the sequence and acknowledgement numbers of the TCP stream? How do they change during transmission?

- Which fields in the TCP header are used as sequence and acknowledgement numbers?

Tips:

- Use filtering function of Wireshark to capture only the packets related to the TCP connection.
- The TCP statistics can be found under the "Statistics" menu in Wireshark.
- The "Follow TCP Stream" function in Wireshark can help you better understand the TCP flow.

Task 2 (Observe DNS，45 Points):

1. Open Wireshark and start capturing packets.
2. Enter "nslookup www.example.com" in the command line and press enter.
3. Observe the packets captured in Wireshark.
4. Find the DNS protocol packet and expand it to review its content.
5. Observe the source and destination addresses, query type, and query result, and try to explain the meaning of these fields.

You need to write the following contexts in your report:

1. Source and destination addresses: The source address is the IP address of the host that initiates the DNS query, and the destination address is the IP address of the DNS server. You should provide a screenshot as proof that you have completed this process.

2. Query type and query result: The query type refers to the type of DNS request, which includes A records and MX records, etc. The query result is the resolution result that DNS returns to the host, which is usually an IP address. You should provide a screenshot as proof that you have completed this process.

Task 3 (Optional，10 Points):

Please select and analyze any other protocol of your choice, e.g. ICMP. There are no specific requirements; simply provide brief evidence of your observation and analysis.

Submission:

Submit your report/document (pdf/docx) at the Web Learning (网络学堂).

Please answer the question objectively and concisely, avoid length answers.