World Scientific Research Journal (WSRJ) ISSN: 2472-3703
www.wsr-j.org

Research on Computer Network Teaching Method Based on Wireshark

Juanjuan Xu, Yongsheng Hu

College of Information Engineering, Binzhou University, Binzhou, Shandong, China.

Abstract: In view of the abstract theory of Computer Networking and the problem of students understanding difficulty, Wireshark is applied to Computer Networking teaching. This paper designs overall teaching program, and it analyzes the three-way handshake process of TCP protocol by a special example. The theoretical study and practice were combined to reduce the difficulty of the course and stimulate students' active exploration spirit.
Keywords: computer network; Wireshark; TCP protocol.

---

1. INTRODUCTION TO WIRESHARK

With the development of information technology, Computer Networking, as a basic course of communication technology, is increasingly concerned by the experts in related fields in colleges and universities. This course takes different layers of protocols as the main line to introduce the process of data communication. It is a theoretical and practical course. If only by learning the theoretical knowledge of textbooks, it is difficult to combine concepts such as network models and protocols with the communication process, so that the relevant knowledge is always abstract and shallow for students. According to several years of teaching experience, the teaching effect is not satisfactory. For the problems in computer network teaching, Wireshark software is introduced to present theoretical knowledge through graphical methods to improve teaching effectiveness and enhance students' practical ability.

2. THE BASIC SITUATION OF WIRESHARK

Wireshark (formerly Ethereal) is the most widely used open source grabbing software in the world, written by Gerald Combs and released with the GPL open source license in 1998[1]. Which has the ability to analyze the underlying network protocols, solve network failures, and find network security issues. it can run on Windows, MacOS, Linux/Unix and other platforms. Wireshark can directly capture the incoming and outgoing traffic of the local network card, the hub environment of the same conflict domain and the switch environment. There are generally three situations in the switch environment: port mirroring, ARP spoofing and MAC flooding. Wireshark's interface is shown in Figure 1. The captured data packets are displayed in the list area and each data packet has corresponding detailed data in the detailed area including frames, Ethernet data packets, IP data packets and TCP data formats etc.

In the Computer Network teaching process, various structured data packets are captured and analyzed in real-time through Wireshark software tool. The structure and content of data units such as TCP messages, IP datagrams, and MAC frames are visually displayed by Wireshark interface, and it also can analyze ARP address resolution[1], three-way handshake, four wave and ICMP tracking process, etc. In this way, students can combine the knowledge model of theoretical learning with the actual work process of the network, so that students can learn more easily, and teachers can explain more easily to achieve a multiplier effect.

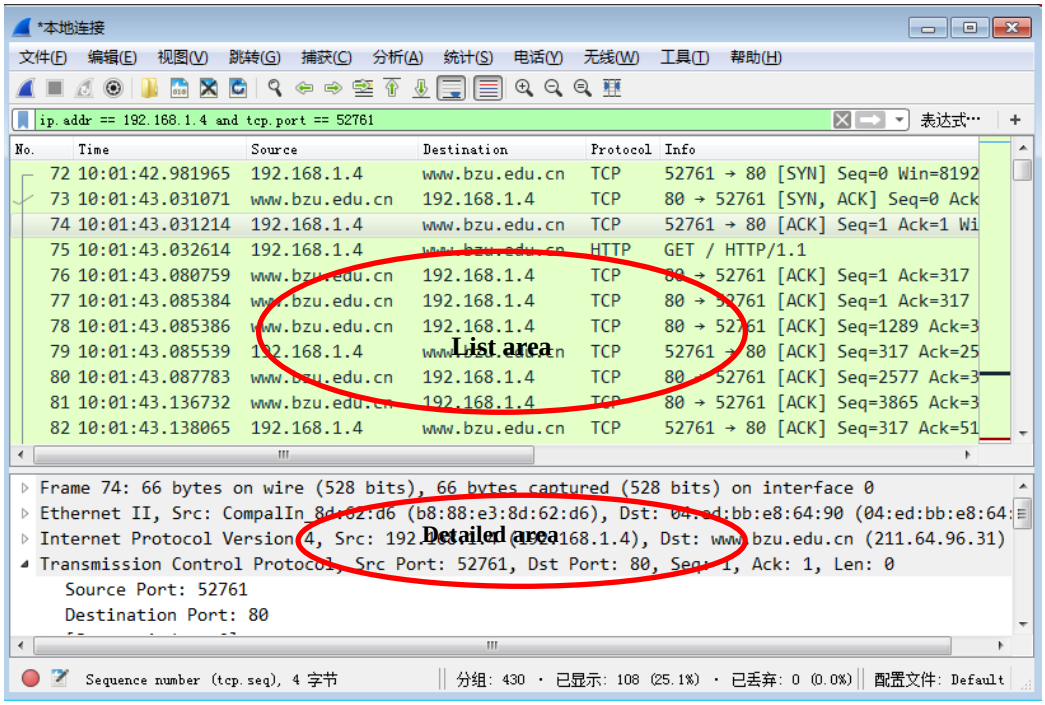


Fig.1 Wireshark Interface

3. WIRESHARK-BASED INSTRUCTIONAL DESIGN

From the perspective of protocol, the network architecture includes the application layer, transport layer, network layer, and network interface layer from top to bottom , and different layers correspond to different data units and protocols. This article studies the four layers showed in Table 1 as the main line. While explaining the theory, each layer is peeled off with Wireshark, and explain in detail the basic data units and corresponding protocols for each layer with the actual case throughout the entire teaching process. The teaching process is compact, and knowledge is clear. Theory study and practice are combined to enable students to understand the process of network communication better[2]. The design of teaching content is shown in Table 1.

Theoretical Analysis of Three-way Handshaking

Tab.1 Design of Teaching Content

Network Hierarchy	Packet	Protocol	Instructional Design
Network interface layer	Frame	Ethernet Frame	1.Analyze the Ethernet frame format and understand the MAC address. 2.Analyze the ARP protocol format and master its working mechanism.
Network layer	IP packet	IP, ICMP, ARP	1.Analyze the IP protocol header format. 2.Understand the concept of IP packet fragmentation. 3.Understand the ICMP Protocol with the ping and traceroute commands.
Transport layer	Message	TCP, UDP	1.Study the meaning and use of the UDP datagram header field to understand the UDP sending and receiving process; 2.Analyze the three-way handshake and four wave of the TCP connection, the processes of sending and receiving segments.
Application layer	Message	HTTP, FTP	1.Capture and analyze HTTP packets, and grasp the working principle of HTTP protocol and HTTP request operation and response. 2.Analyze the working process of FTP.

4. TCP PROTOCOL ANALYSIS

Instructional design is the key when analyzing protocols. Take the three-way handshake of the TCP protocol as an example to illustrate the important role of Wireshark in the teaching process.

4.1 Theoretical Analysis of Three-way Handshaking

TCP is a connection-oriented protocol. The establishment and release of a TCP connection is an indispensable process of communication, which is established with a Client to Server mode. An application process that actively initiates connection establishment is called a client, and an application process that passively waits for connection establishment is called a server. As shown in Figure 2, the client runs the TCP client program and the server runs the TCP server program. The process of establishing a connection is called the three-way handshake. That is, the client sends a connection request, then the receiver confirms the connection request. Finally, the client further confirms the server's confirmation message. After the connection is established, data transfer is performed.

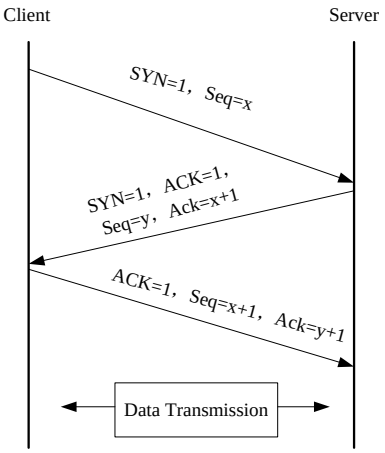
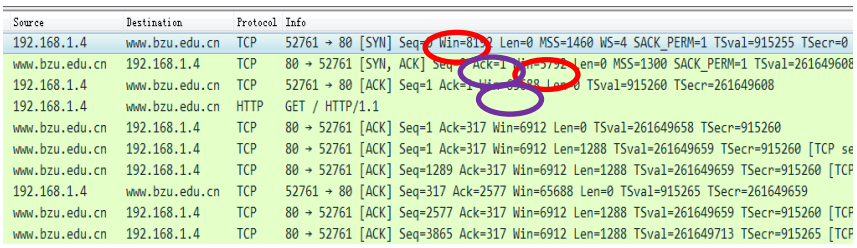


Fig.2 Three-way Handshake to Establish a TCP Connection

4.2 Three-way Handshake Resolution in Wireshark

The three-way handshake is parsed in the Wireshark software environment. The local host is used as the client. its IP address is 192.168.1.4 and the port number is 52761. It sents an application to Binzhou University server. Binzhou University website is www.bzu.edu.cn, IP address is 211.64.96.31 and the port number is 80. Let's use Wireshark Software to Capture TCP Data Streams. Enter ip.addr == 192.168.1.4 and tcp.port == 52761 in the display filter to filter out the client-server data flow. The capture of TCP flow is shown in Figure 3.



Source	Destination	Protocol	Info
192.168.1.4	www.bzu.edu.cn	TCP	52761 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 TSval=915255 TSecr=0
www.bzu.edu.cn	192.168.1.4	TCP	80 → 52761 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1300 SACK_PERM=1 TSval=261649608
192.168.1.4	www.bzu.edu.cn	TCP	52761 → 80 [ACK] Seq=1 Ack=1 Win=65688 Len=0 TSval=915260 TSecr=261649608
192.168.1.4	www.bzu.edu.cn	HTTP	GET / HTTP/1.1
www.bzu.edu.cn	192.168.1.4	TCP	80 → 52761 [ACK] Seq=1 Ack=317 Win=6912 Len=0 TSval=261649658 TSecr=915260
www.bzu.edu.cn	192.168.1.4	TCP	80 → 52761 [ACK] Seq=1 Ack=317 Win=6912 Len=1288 TSval=261649659 TSecr=915260 [TCP se
www.bzu.edu.cn	192.168.1.4	TCP	80 → 52761 [ACK] Seq=1289 Ack=317 Win=6912 Len=1288 TSval=261649659 TSecr=915260 [TCP
192.168.1.4	www.bzu.edu.cn	TCP	52761 → 80 [ACK] Seq=317 Ack=2577 Win=65688 Len=0 TSval=915265 TSecr=261649659
www.bzu.edu.cn	192.168.1.4	TCP	80 → 52761 [ACK] Seq=2577 Ack=317 Win=6912 Len=1288 TSval=261649659 TSecr=915260 [TCP
www.bzu.edu.cn	192.168.1.4	TCP	80 → 52761 [ACK] Seq=3865 Ack=317 Win=6912 Len=1288 TSval=261649713 TSecr=915265 [TCP

Fig.3 The Capture of TCP Flow in Wireshark

As shown in figure 3, the client process sends a request message segment to the server. The synchronous bit SYN=1 in the header, and the initial sequence number Seq=0. At this time, the TCP client process enters the synchronized transmission state. After receiving the request message, the server agrees to establish a connection and sends an acknowledgement message to the client. The SYN and ACK bits are all set to 1, and the acknowledgement number Ack=1. At the same time, an server initial sequence number Seq=0 is selected, and then TCP server process enters Synchronous reception state. After the TCP client receiving the acknowledgment from the server, it also sends a confirmation to the server that the segment ACK is set to 1. The acknowledgment number Ack is the sequence number of previous datagram Seq plus 1. that is, Ack=1. which is the second data packet the client sent, so Seq=1, and the TCP connection is established[3]. Seq indicates the number of packets sent by one end. The value of Ack field is Seq plus 1 of the confirmation data packet.

In Wireshark software, the traffic graph can also be counted. As is shown in Figure 4, the red circle part is a complete three-way handshake process, including the connection establishment time, requests and responses information of the client and the server, etc [4].

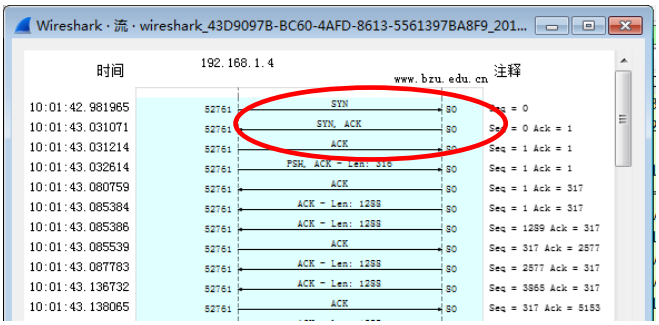


Figure 4 Three-Way Handshake Traffic Graph

5. CONCLUSION

Through theoretical learning and experimental demonstrations, the working principle of the three-way handshake will be understood simple and easy. In addition, the underlying data can be further parsed by Wireshark software. The above is just an example of teaching design. Each part can be presented in this way and the classroom effect will be significantly improved.

ACKNOWLEDGMENTS

This work was supported by Binzhou University Experimental Technology Research Project (BZXYSYXM201715); Binzhou University School-Enterprise Co-construction Course Project (BYXQGJ201704).

REFERENCES

[1] https://www.wireshark.org/.
[2] Li Cheng, Haojun Zhang, Yong Wu. Research on Visual Analysis Teaching Method of Network Protocol. Education and Teaching Forum. 2013, pp.242-243.
[3] Xiren Xie. Computer Networking [M], 5th edition, Beijing: Electronic Industry, 2008.
[4] Shaoqiang Wang, Dongsheng Xu, Shiliang Yan. Analysis and Application of Wireshark in TCP/IP Protocol Teaching. International Conference, 2010, pp.269-272.