How To Read Wireshark TCP/HTTP Logs

Wireshark logs records in hours, minutes, seconds, and milliseconds; they also go by sections: the number, the time, source, destination, protocol, and information

Log Number

No.	Time
1	3.37546
2	3.38954
3	3.91232

The “No.” section indicate the number of the log

Log Time

The “Time” section represents the time, in this case are seconds and milliseconds

Source and Destination

Source	Destination
198.876.43.21	193.0.256.23
193.0.256.23	198.876.43.21
198.876.43.21	193.0.256.23

The “source” is the machine that sent the packet. The “destination” is the machine receiving the packet, both the source and the destination are represented with their IP addresses.

Protocol and information

Protocol	Info
TCP	34225–>443 [SYN]

TCP	443–>34225 [SYN, ACK]
TCP	34225–>443 [ACK]

The Protocol column represents the protocol being used.
The Info column provides information about the packet. Usually there is more information in this section, such as seq, win, and len; but I will not include that information to keep the information simple.

How this data is represented on Wireshark

No.	Time	Source	Destination	Protocol	Info
1	3.37546	193.0.256.23	198.876.43.21	TCP	34225->443 [SYN]
2	3.38954	198.876.43.21	193.0.256.23	TCP	443->34225 [SYN, ACK]
3	3.91232	193.0.256.23	198.876.43.21	TCP	34225–>443 [ACK]