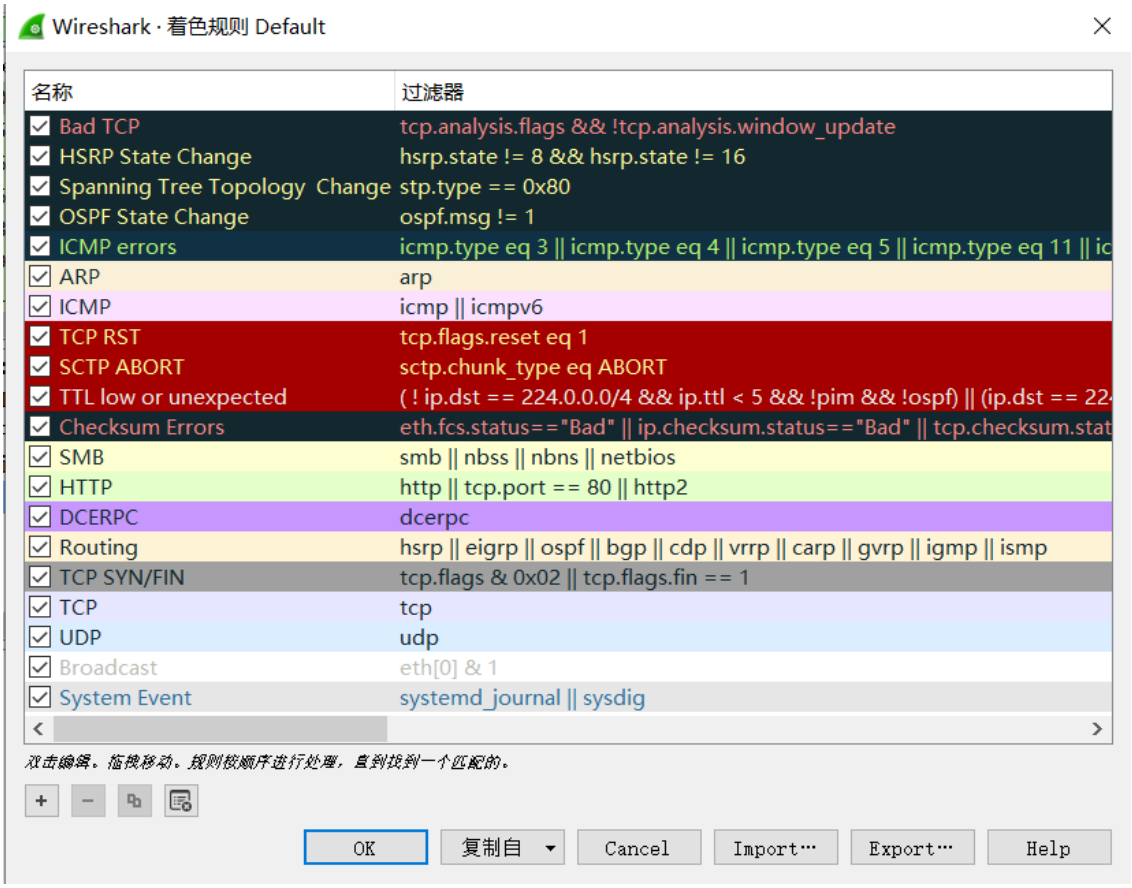
Lab1

SID: 11811407

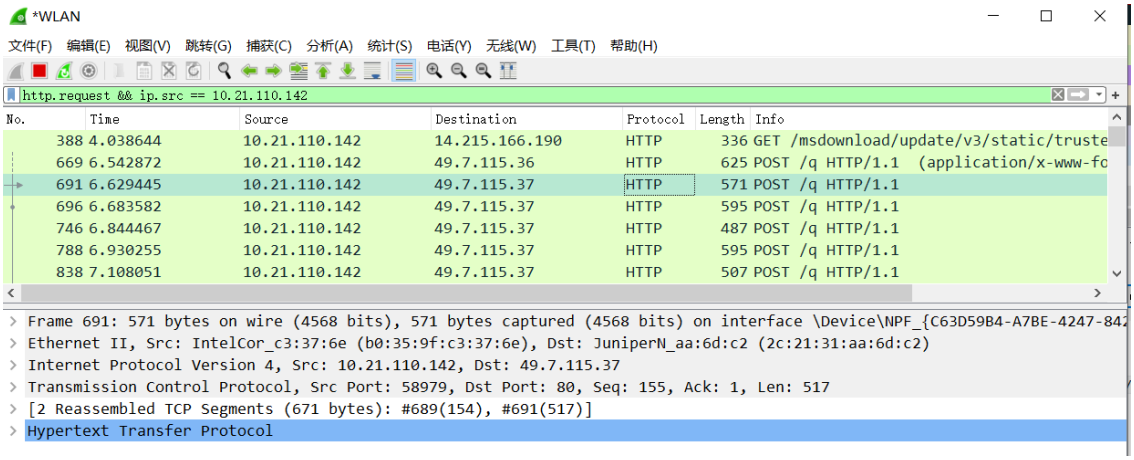
Name: 黎诗龙

2. From the tutorial lab1 we can get "Black identifies TCP packets with problems, e.g., they could have been delivered out-of-order."

   From the official help we get **black** also means `HSRP state change`, `Spanning Tree topology change`, `OSPF state change`, `ICMP errors` and `checksum errors`.



3. http.request && ip.src == `my ip address`, here my ip address is 10.21.110.142.



4.

DNS uses UDP while HTTP uses TCP to transfer.

UDP has smaller response time than TCP.

UDP cannot guarantee the transmission but TCP can.

UDP usually transfers the message that shorter than 512B, but TCP has not such limit.

DNS needs faster queries and most messages can be stored in 512B, so most DNS chooses UDP.

However, HTTP sends large messages that exceeds 512B, and must guarantee that the message is complete. So most HTTP chooses TCP.

5.

I use wireshark to filter the ftp, and we can get the password from "Request: PASS WSU-csc5991.", which is `WSU-csc5991.`