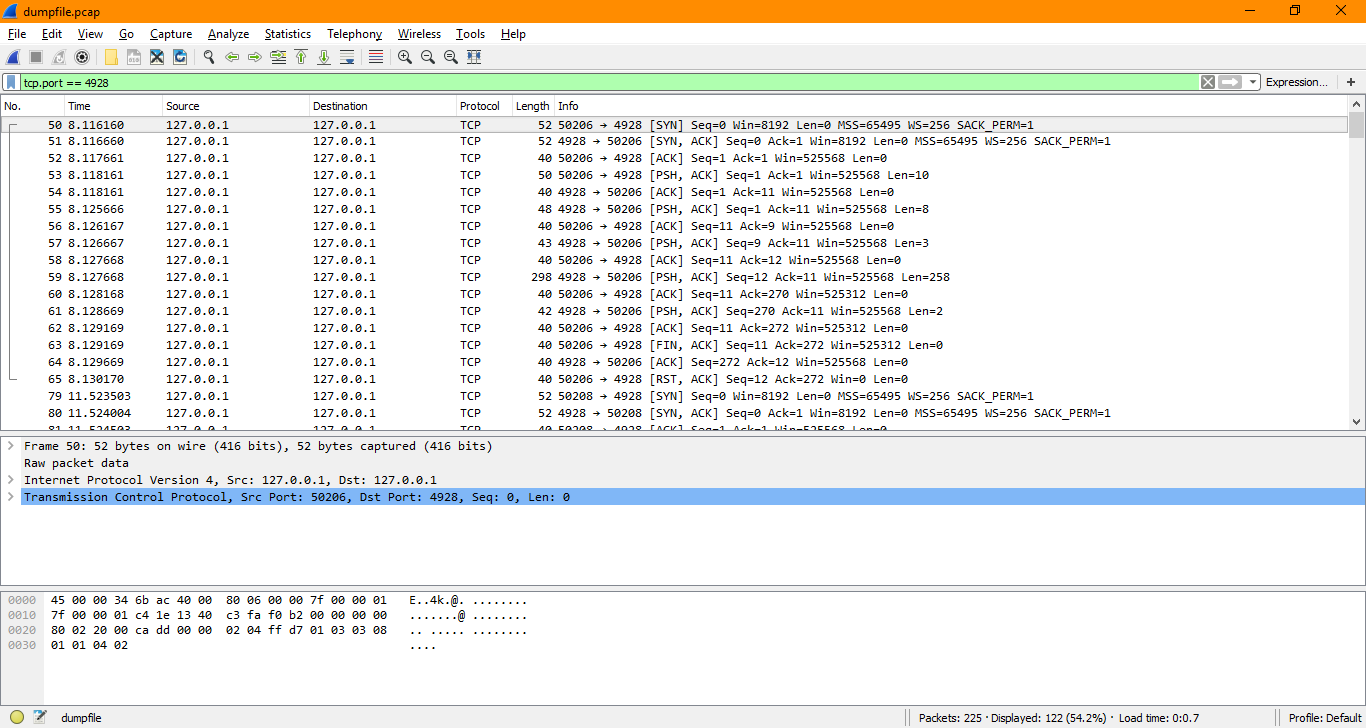
**Wireshark and Book Store Protocol**



**การดักจับข้อมูล โดยใช้Wireshark**

โดยWiresharkไม่สามารถดักจับpacketที่เป็น Localhost ได้ จึงต้องใช้ RawCap ช่วย โดยใช้คำสั่งรันRawCapโดยใช้ Localhost (IP) คือ 127.0.0.1 และบันทึกการดักจับpacketลงไฟล์ แล้วเปิดผ่าน Wireshark

ในโปรเจคนี้จะทดลองการใช้Wiresharkในการดักจับpacket ที่Client ส่ง request message ไปที่ Server และ response message ที่Server ส่งกลับมาให้Client โดยใช้ Protocol แบบ TCP, มี port number คือ 4928, มี request message คือ การค้นหารายการหนังสือ และการเพิ่มหนังสือ, และมี response message เป็น รายการหนังสือที่ค้นหาเจอ และสถานะของการเพิ่มหนังสือ ดังนั้นจะใช้ Filter ค้นหาเป็น tcp.port == 4928 เพื่อหาการดักจับ packet ของ TCP ใน port number ที่ 4928