1.
    a. mystery_1.pcap
        i. The malicious actor is inserting their malicious packet right after the legitimate user sends their GET request which is packet 5 in the .pcap file. The packet they are sending redirects the user from the website they were trying to go to (slashdot.org) and makes them go to fox-it.com instead
    b. Mystery_2.pcap
        i. The shooter is inserting their packet right after the user sends their GET request which is packet 5 in the .pcap file. This packet they are sending is a regular 200 OK response but they added the text “Bang!” at the end signifying an altered packet. The website the user was trying to access was jsonip.com. And the original non-hijacked packet sent by the user was retransmitted in packet number 9.

2. For my python script I decided a packet was inserted if it met these criteria. One, it had duplicate sequence numbers in the .pcap file. This shows that the same packet could have been sent twice. Then two, if the two packets with the same sequence numbers were both http requests but not with the same content. If both these criteria are met I can safely assume that the packet was injected so I print the injected packet number to the screen followed by the injected packet information.