Scenario 1 - Latency issue Wireshark

Q - Download the ZIP file, extract the PCAP file and list the observations.
Ans - Here we will refer host as 10.10.10.10 and server as 10.10.10.30
Now, We will Analyse packets:-

- Packet 1,2 ⇒ ARP resolution.
- Packet 3,4 ⇒ host→ server (on port 135) = SYN; server (from port 135)→ host = RST,ACK ; it means server port 135 is closed.
- Packet 5,6, ⇒ host → server (on port 22) = SYN; server (from port 22)→ host = SYN,ACK ; but host ACK was delayed.
- Packet 7,8 ⇒ host→ server (on port 21) =SYN; server (from port 21)→ host = RST,ACK; it means server port 21 is closed
- Packet 9,16⇒ Packet 3,4 & 7,8 condition is being repeated till Packet 16.
- Packet 17,18 ⇒ host → server (on port 80) = SYN; server (from port 80)→ host = SYN,ACK ; but host ACK was delayed.
- Packet 19,26 ⇒ Packet 3,4 & 7,8 condition is being repeated till Packet 26
- Packet 27,28 ⇒ host→ server = ACK (on port 22,80); These are delayed ACK packets (in relation with Packet 5,6 and Packet 17,18) that are being retransmitted by the host to the server in order to complete the 3 way handshake.
- Packet 29,30 ⇒ server (from port 22,80)→ host = RST, ACK; it means in relation with Packet 5,6 and Packet 17,18 and Packet 27,28, in context with 3 way hand shake, that was established with delay ACK, now the server has closed the connection by sending RST, ACK.
- Packet 31,32,35,36 ⇒ host → server = SYN; server→ host = SYN,ACK, but host didn’t sent ACK so 3 way handshake was incomplete but host got to know that the server port (port 443, 3306) which it was trying to reach is open.

Conclusion:-

This process is being repeated throughout this whole pcapng file which indicates that our host is scanning for open ports on the server machine due to which there is large volume of traffic generation which can congest the network as well as it can also slow down the server. Our host is flooding the network with packets to check for open ports that is ultimately causing DOS like situation due to which i think latency issue happening.