TCP, FTP packet analysis Wireshark practical exam Questions and answers

1. What is the ip address of the client machine?
2. What is the ip address of the host machine?
3. How many ip address are involved in communication in this capture file?
4. Which is the display filter used to display all the packets having source ip as 192.168.1.231?
5. What are the packet numbers in this capture file which shows the TCP 3-way handshake process?
6. What is the display filter used to display all the packets with ftp protocol only?
7. What is the display filter used to display packets with ftp server response code as 200?
8. List any two types of ftp server response codes with their meanings from this capture file.

9. What is the client port number and the server port no.?

10. Why is Server port no is 21?

11. List 5 commands that User tried on the ftp server CMD Line after a successful login attempt.

12. How many times does that user has tried to login to the ftp server?

13. Which is the display filter used to display all the tcp ERROR packets i.e. Black labeled one?

14. What is the original window size value and multiplication factor for the new window size during the transmission of 97th packet?

15. What is the display filter used to display all the packets with no protocol used as ftp?

16. Why all the packets get displayed even after trying to filter out tcp packets?

.

17. What is the RTT for given capture file?

18. Which flags are set in the 111th and 58th packet?

19. In which directory did the User found README file on the ftp server?

20. How many packets are there where user deals with resume.doc with different commands in the ftp server command line?

21. Demonstrate TCP 3 way handshake for given pcap file. Also show how flow diagram can be viewed.

22. Draw header format of Ethernet? And explain data in each field of header for given pcap

23. . Draw header format of TCP and explain data in each field of header for given pcap

24. . Draw header format of IP. And explain data in each field of header for given pcap