LAB 2

What is an ephemeral port number?

Basically a range of port numbers that is used by client. Apart from the well known port numbers like 80, 21 etc. 49152 to 65535.

DNS
Linux DNS: no OS level DNS but there can be other caching services
https://linuxize.com/post/how-to-clear-the-dns-cache/#clearflush-dns-cache-on-linux
clear browser DNS using this:
https://linuxize.com/post/how-to-clear-the-dns-cache/#clearflush-browser-dns-cache
because browser dns can still be persistent

PORT commands is sent when we need to establish data connection

Nevermind sir, I checked the timing of the packets. PORT was executed a few milliseconds before the RETR command so they are both associated with the same get command.

112 18.131255 172.18.19.179 172.22.1.29 FTP 68 Request: OPTS UTF8 ON

OPTS request sent between Windows machines. As the server is Windows server and the client is Linux, no OPTS.

In the filter typing in opts alone won't work. try pgm.otps

OPTS allows ftp client to define a parameter that will be used by a subsequent command.

Q: How the server is able to send PORT command successful, even when the three-way handshake required to complete the TCP connection that got initiated due to PORT command has not been completed.

A: You can see the port command successful packet between the SYN and SYN,ACK packet. the question is why is it so even though the fin,ack has not been received

Authoritative name server where DNS entry url vs IP is stored. If all the intermediate DNS server have not cached that DNS entry, then it looks up the entry from the name server.

It checks if the DNS cache at the router is holding any entry first. then moves on to the next DNS caching server if not available.
You can also see that, the nslookup may give multiple IP Addresses

It happens when the site is hosted on multiple servers. Multiple servers with different IPs for balancing the load on the servers

query is the link that is being queried for the IP address. transaction ID keeps track of the query and response message is the response from the DNS server

type=(Name Server)NS