Wireshark Challenge

For every question, please insert the right answer, AND the EXACT full filter you used in order to get to this answer. Feel free to always explore and try new functions and options in Wireshark, or use google anytime you need.

GOOD LUCK!

Basic filters:

1. How many packets are in the pcap file?
2. How many packets are sent by the IP 131.151.32.129?
3. What time was packet number 400 sent (HH:MM:SS format)?
4. How many DNS packets are there?
5. How many TCP packets are there?
6. How many HTTP packets are in the pcap file?
7. Who is the client that is sending requests to the HTTP server?
8. What are the two HTTP servers' IPs?
9. What were the 4 types of DHCP packets that were sent in the pcap?
10. What is the MAC of the DHCP server? (You can read about how DHCP works as a reminder).
11. What is the TTL of the ping request that was sent from the IP 131.151.6.171?
12. What is the source mac address of the computer, that is sending ARP requests, searching for the IP 31.151.111.254?
13. What is the destination mail the SMTP mail is sent to?

    Hint: read about follow TCP stream
14. What is the IP of the device sending SNMP get requests?
15. What is the IP of the device responding to the SNMP requests?
16. How many packets are with a VLAN?
17. How many ICMP packets are there?

Note: before you continue, read about the difference between RX and TX bytes and packets, when using the statistics in Wireshark

18. How many TCP conversations are there?

19. What is the IP that sent the most bytes in the pcap, not necessarily only to one other address? (Hint: read about the endpoint tab).
20. What is the IP that sent the most TCP packets?
21. How many bytes are in all the SNMP packets sent? (Hint: Read about Wireshark protocol hierarchy)
22. What is the MAC address that most packets were sent to (as the destination)?

Complex Filters:

Hint: Make sure you look and explore the extended information about every packet (at the bottom of the screen), to help yourself build exactly the relevant filters.

23. How many packets have VLAN but their VLAN id is not 32?
24. How many packets are http packets responding with status code 200 (OK)?
25. How many SNMP get request packets are there that request 3 mibs (variable bindings)?
26. How many ICMP packets are not ping replies/requests?
27. How many packets are sent from an IP in the subnet 172.31.0.0/16?
28. How many packets are at least 100 bytes?

    Reminder: telnet send the commands in clear text so you can actually see the command sent in Wireshark.
29. How many packets are sent with the telnet protocol, that contains only the phrase\r\n (new line)?
30. How many packets are UDP packets, but also either SNMP or in the subnet 192.0.0.0/8?
31. How many packets in the pcap are NTP or telnet protocol, and also are smaller than 200 bytes?
32. How many packets are ARP packets that are requesting the IP 24.166.174.167?
33. How many packets are ARP packets that are requesting an IP in the subnet 69.76.223.0/25?
34. How many DNS query are for google.com?
35. How many DNS query responses are for google.com?
36. How many OSPF packets that their message type is a hello packet, were sent by the ip 192.168.170.2?
37. How many packets are with an IP TTL of either bellow 50 or at least 200?

38. Find a filter (in one line) that finds how many packets are:

- Sent to a UDP dst port above 200, and are not SNMP

  or

- TCP packets, and sent with a src port bellow 100

39. How many packets are sent by MAC addresses that start with 00:07:0d?

BONUS – SUPER HARD:

40. How many addresses in the subnet 172.0.31.0.0/16, are sending packets in the pcap?
41. How many DNS servers that respond the DNS queries, are in the capture?
42. What was the IP pinged through the data telnet TCP stream?
43. What is the title of the file being transferred in the data of the TFTP UDP stream?
44. What is the content length of the /download.html file that is requested in an HTTP Get request?