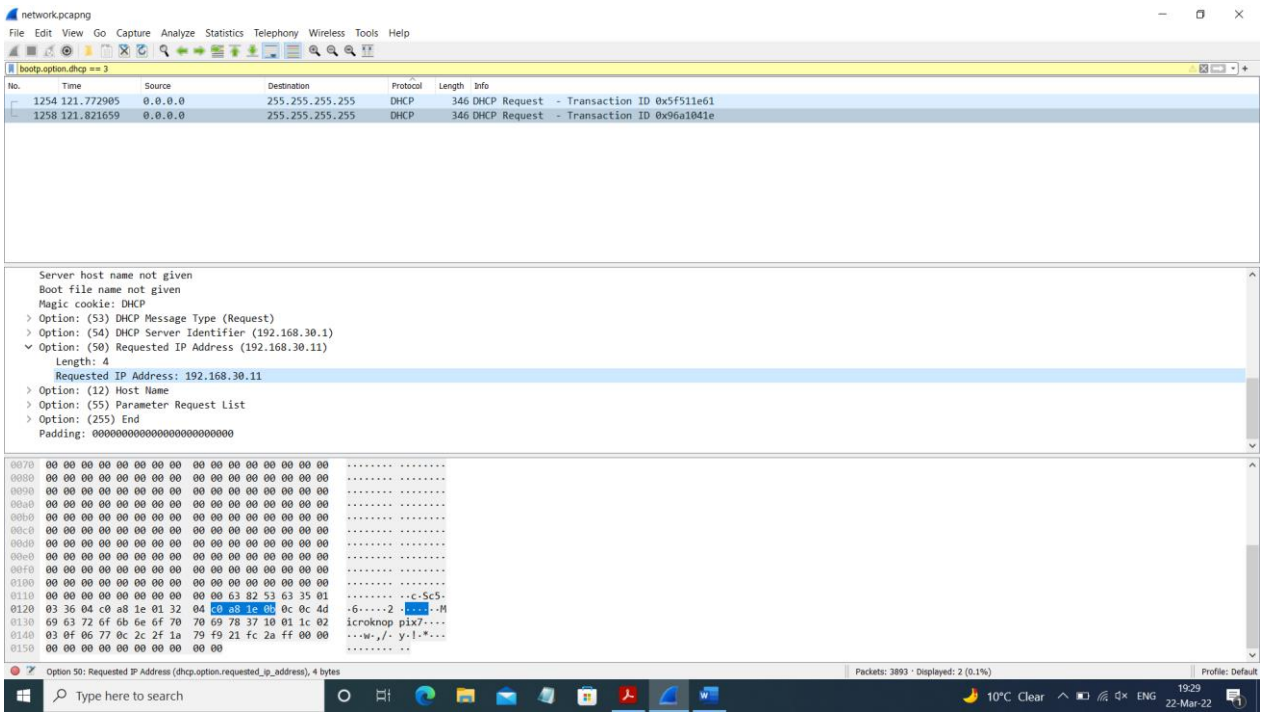
Tema 1

1. Care este adresa de IP cerută de clientul DHCP?

   R: Requested IP Address: 192.168.30.11

   Izolam request-urile de tip DHCP cu comanda bootp.option.dhcp==3.

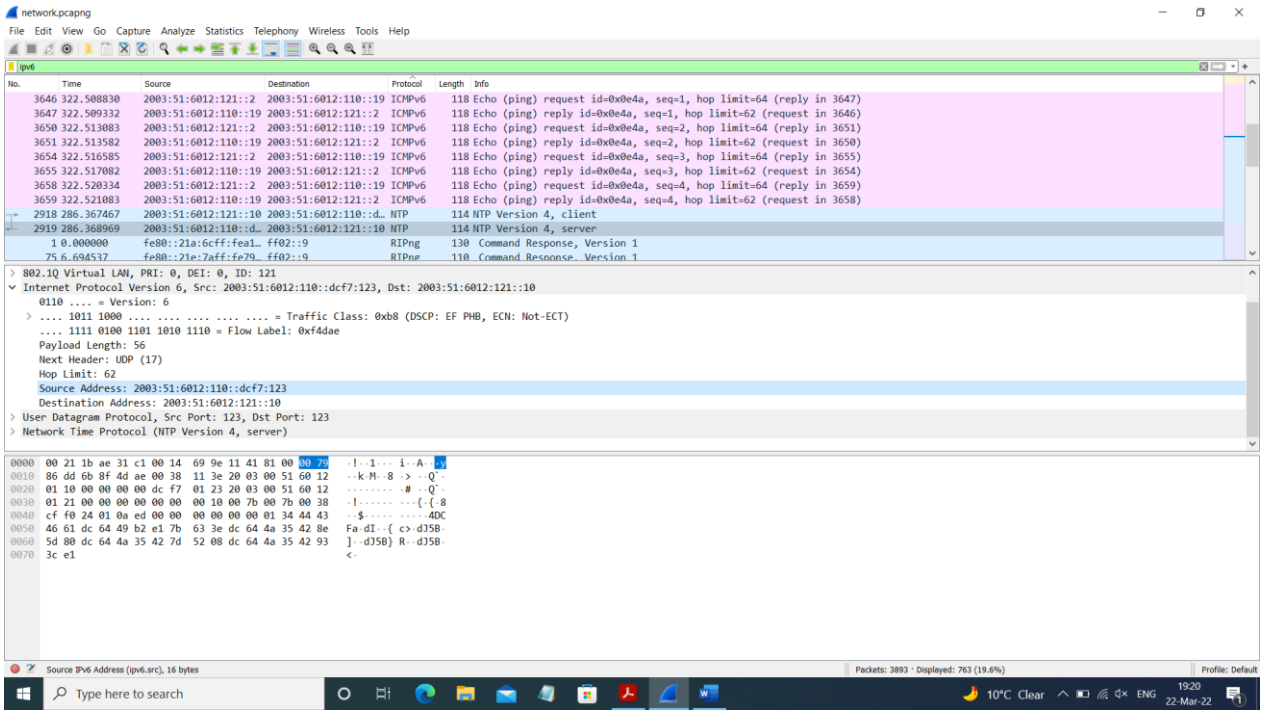
   O sa returneze 2 rezultate, dar alegem numarul 1258, deoarece cautand primul pachet (cu IP-ul 192.168.20.11) observam ca are statusul NAK (not acknowledged), deci este invalid.



2. Care este adresa de IPv6 a serverului de NTP?

   R: Source Address: 2003:51:6012:110::dcf7:123

   Am filtrat toate conexiunile IPV6 si cautam in lista serverul NTP, cautam in server conexiunea sursa sau in client conexiunea destinatie.



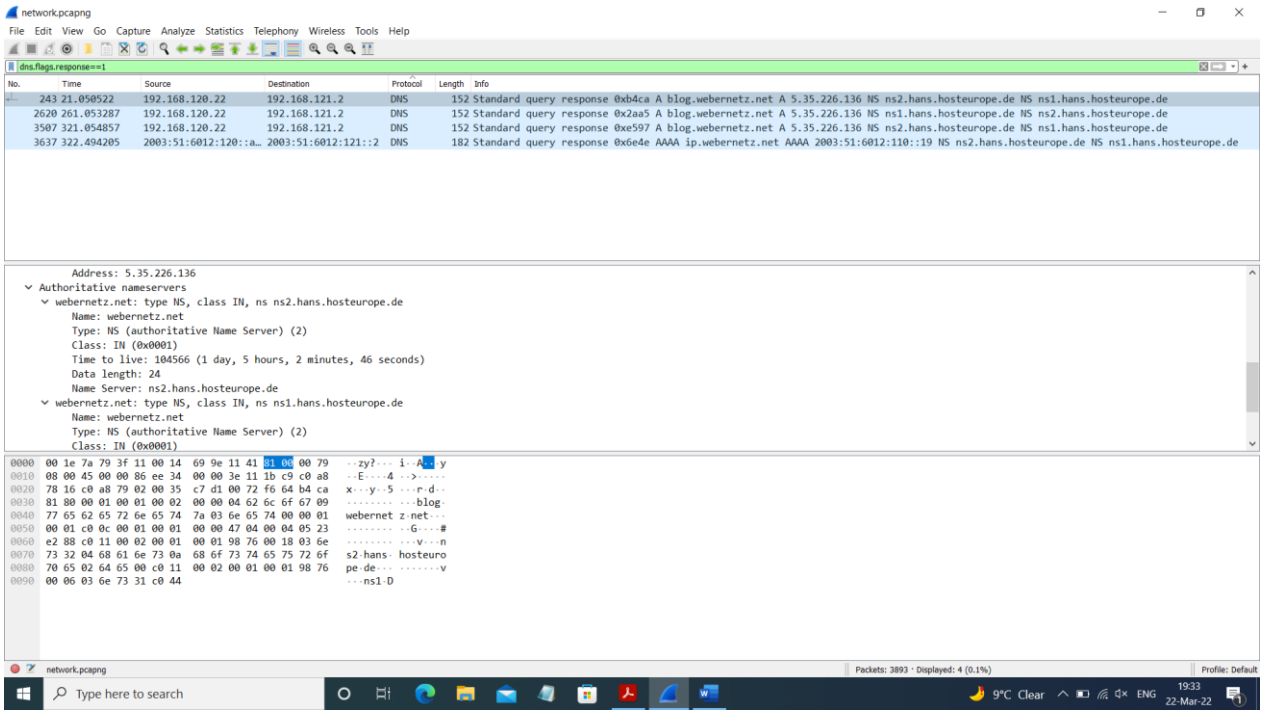
3. Care este numele serverului autoritar (authoritative name server) pentru domeniul care este căutat?

R: webernetz.net: type NS, class IN, ns ns2.hans.hosteurope.de

SAU

webernetz.net: type NS, class IN, ns ns1.hans.hosteurope.de

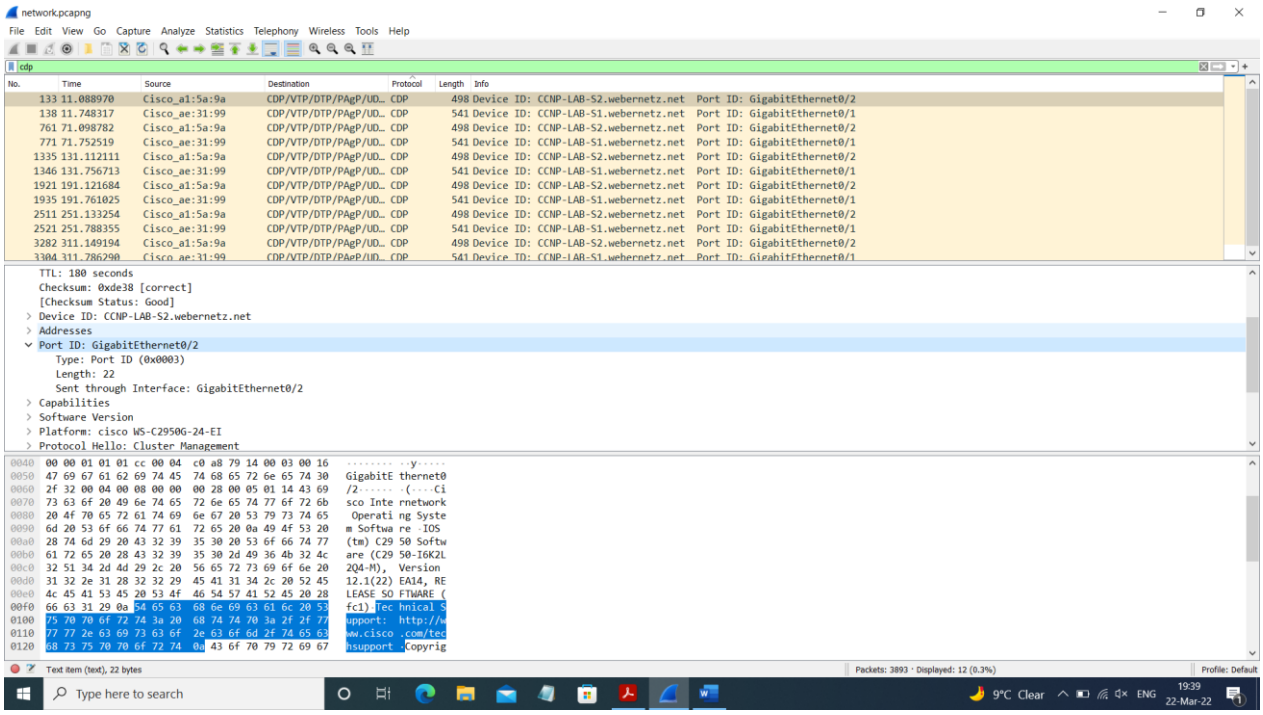
Numele serverului autoritar se gaseste in pachetele DNS Response, ce pot fi filtrate cu filtrul dns.flags.response==1.



4. Care este portul pentru protocolul CDP al host-ului CCNP-LAB-S2?

   R: Port ID: GigabitEthernet0/2

   Filtram protocoalele CDP cu filtrul cdp. Se observa ca primul care apare (133) are ca host CCNP-LAB-S2 si observam in informatiile pachetului Port ID-ul.



Nota: Se poate utiliza si filtrul cdp.devideid contains S2.

5. Ce versiune de IOS rulează pe host-ul CCNP-LAB-S2?

   R: Software version: IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA14, RELEASE SOFTWARE (fc1)

   Folosind unul dintre cele 2 filtre de la exercitiul anterior, gasim in cadrul pachetului 133 in Cisco Discovery Protocol, in Software Version, versiunea actuala de IOS.

6. Cand a fost config-ul de NVRAM actualizat ultima dată?

R: 21:02:36 UTC Fri Mar 3 2017

Folosim search-ul (Ctrl+F), setam pe Packet Byes pentru a cauta in interiorul pachetelor si pe string si cautam NVRAM. Cautarea returneaza pachetul 3770 cu datele cautate despre NVRAM.