

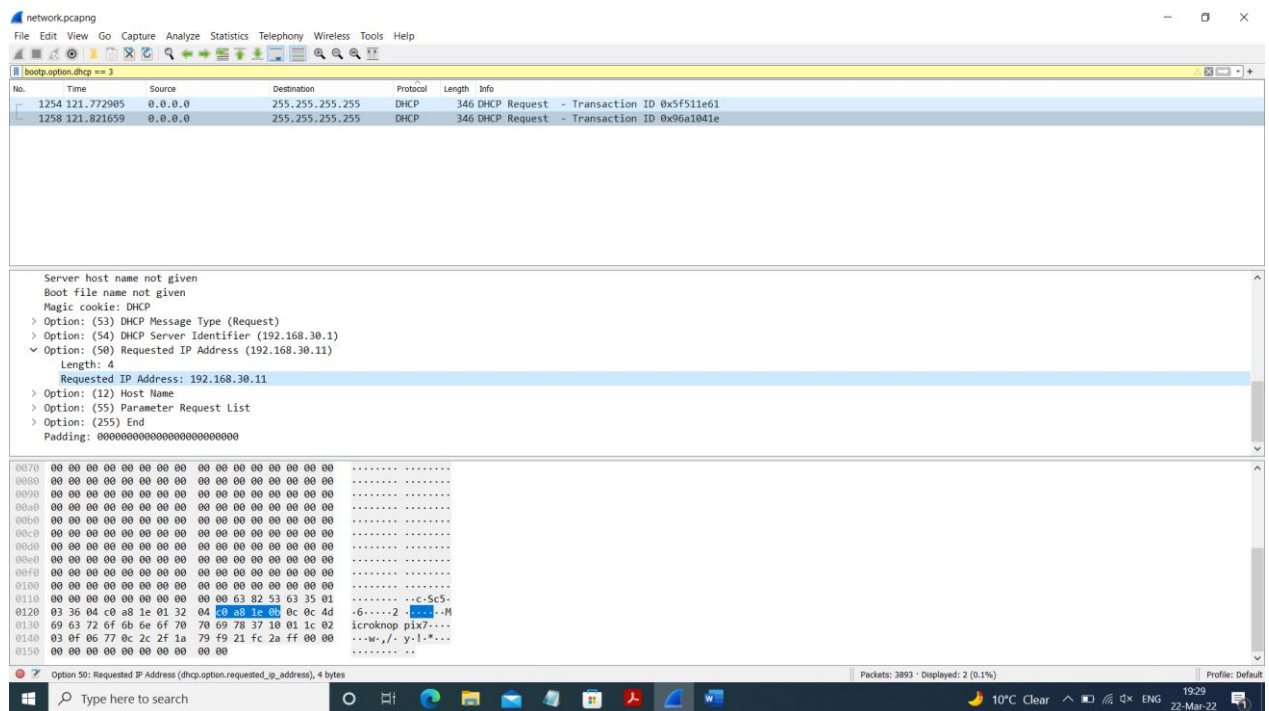
# Tema 1

## 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`.

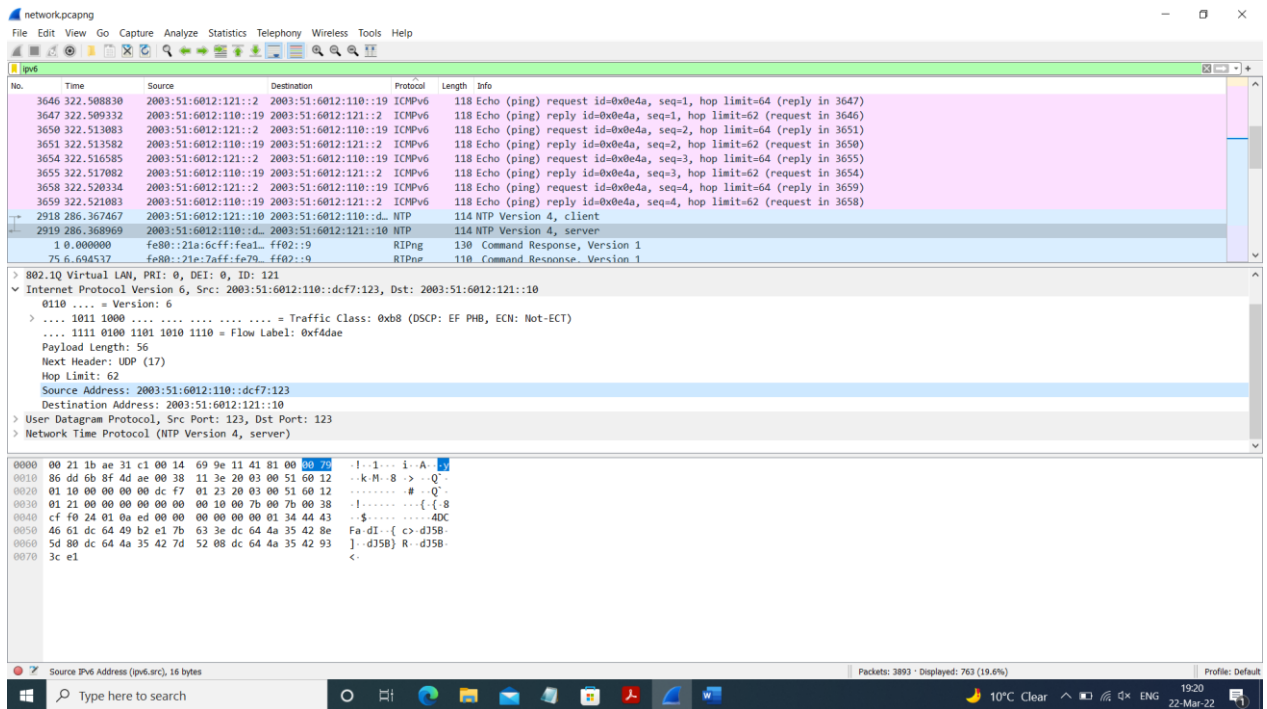
O sa returneze 2 rezultate, dar alegem numarul 1258, deoarece cautand primul pachet (cu IP-ul 192.168.20.11) observam ca are statusul NAK (not acknowledged), deci este invalid.



## 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.



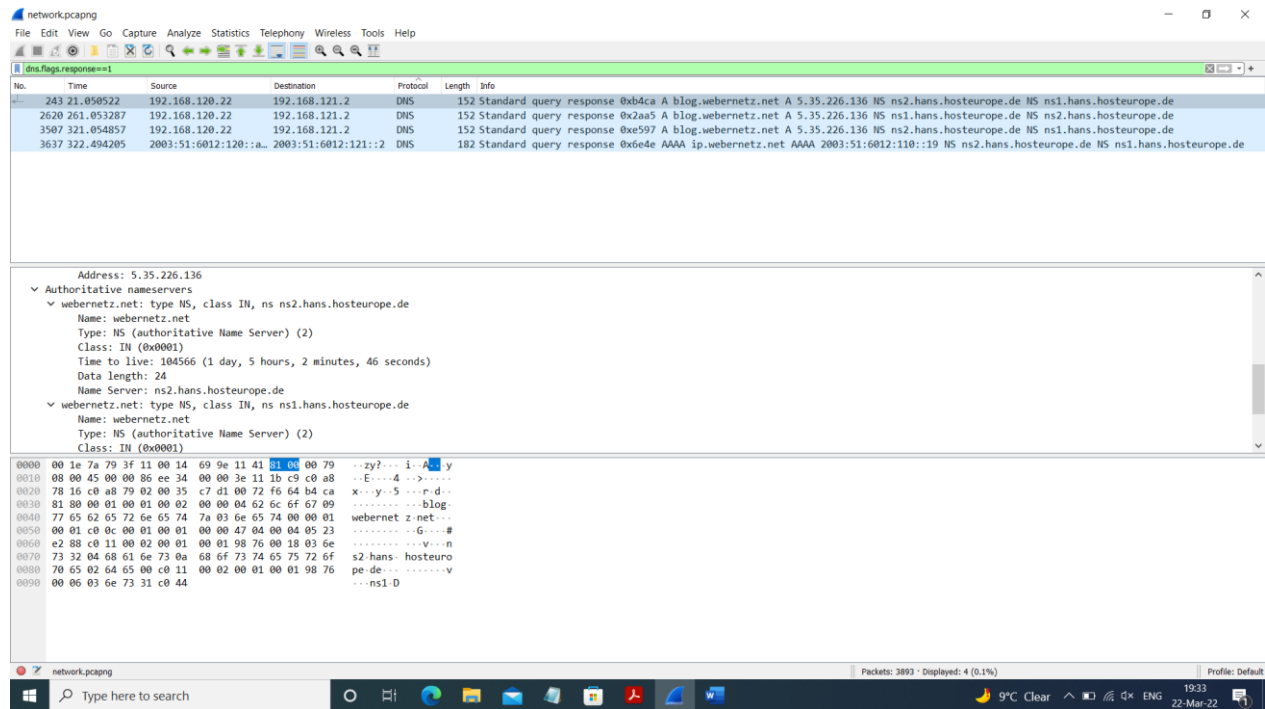
3. Care este numele serverului autoritar (authoritative name server) pentru domeniul care este căutat?

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

SAU

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

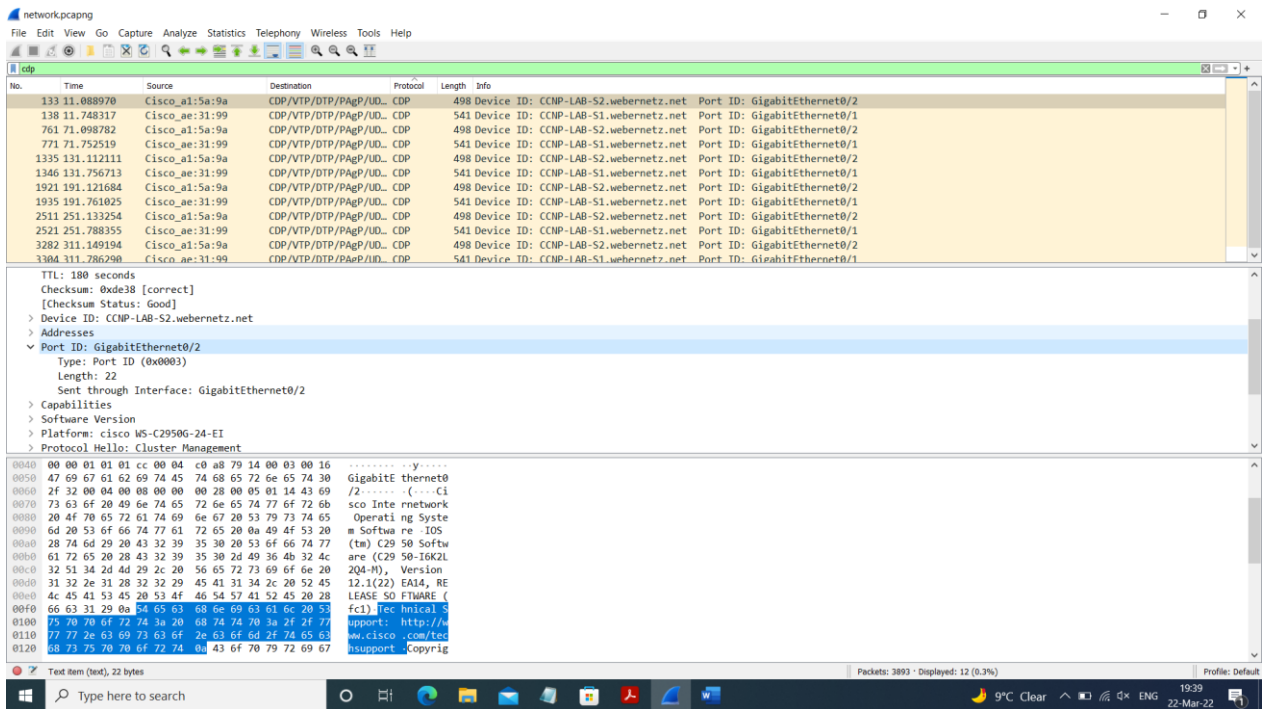
Numele serverului autoritar se gaseste in pachetele DNS Response, ce pot fi filtrate cu filtrul dns.flags.response==1.



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

R: Port ID: GigabitEthernet0/2

Filtram protocolele 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 Bytes pentru a cauta in interiorul pachetelor si pe string si cautam NVRAM. Cautarea returneaza pachetul 3770 cu datele cautate despre NVRAM.

The screenshot shows the Wireshark interface with packet 3770 selected. The packet list pane shows the following details:

No.	Time	Source	Destination	Protocol	Length	Info
3766	327.855911	192.168.121.2	192.168.110.10	TFTP	88	Write Request, File: CCNP-LAB-R2-Mar--3-20-02-38.701-7, Transfer type: octet
3767	327.874841	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 0
3770	327.877414	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 1
3771	327.877915	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 1
3772	327.879916	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 2
3773	327.880417	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 2
3774	327.881915	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 3
3775	327.882172	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 3
3776	327.883918	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 4
3777	327.884176	192.168.110.10	192.168.121.2	TFTP	64	Acknowledgement, Block: 4
3778	327.885666	192.168.121.2	192.168.110.10	TFTP	562	Data Packet, Block: 5

The packet details pane for packet 3770 shows the following structure:

- Frame 3770: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface unknown, id 0
- Ethernet II, Src: Cisco\_79:3f:11 (00:1e:7a:79:3f:11), Dst: Cisco\_9e:11:41 (00:14:69:9e:11:41)
- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 121
- Internet Protocol Version 4, Src: 192.168.121.2, Dst: 192.168.110.10
- User Datagram Protocol, Src Port: 54445, Dst Port: 1556
- Trivial File Transfer Protocol
- Data (512 bytes)

The packet bytes pane shows the raw data of the selected packet, which is a hexadecimal string representing the NVRAM data.

```
0070 62 79 20 77 65 62 65 72 6a 6f 68 0a 21 20 75 52 by weber joh l
0080 75 70 64 61 74 65 64 20 61 74 20 32 31 3a 30 32 updated at 21:02
0090 3a 33 36 20 55 54 43 20 46 72 69 20 4d 61 72 20 :36 UTC Fri Mar
00a0 33 20 32 30 31 37 20 62 79 20 77 65 62 65 72 6a 3 2017 b y weberj
00b0 6f 68 0a 21 20 4e 56 52 41 4d 20 63 6f 6e 66 69 oh l NVR AM confi
00c0 67 20 6c 61 73 74 20 75 70 64 61 74 65 64 20 61 g last u pdated e
00d0 74 20 32 31 3a 30 32 3a 33 36 20 55 54 43 20 46 t 21:02: 36 UTC F
00e0 72 69 20 4d 61 72 20 33 20 32 30 31 37 20 62 79 ri Mar 3 2017 by
00f0 20 77 65 62 65 72 6a 6f 68 0a 76 65 72 73 69 6f weberjo h-versio
0100 6e 20 31 35 2e 31 0a 73 65 72 76 69 63 65 20 74 n 15.1.s ervice t
0110 69 6d 65 73 74 61 6d 70 73 20 64 65 62 75 67 20 imestamp s debug
0120 64 61 74 65 74 69 6d 65 20 6d 73 65 63 0a 73 65 datetime msec-se
0130 72 76 69 63 65 20 74 69 6d 65 73 74 61 6d 70 73 rvicetimestamps
0140 20 6c 6f 67 20 64 61 74 65 74 69 6d 65 20 6d 73 log dat etime ms
```