Key

I. Nmap Scan

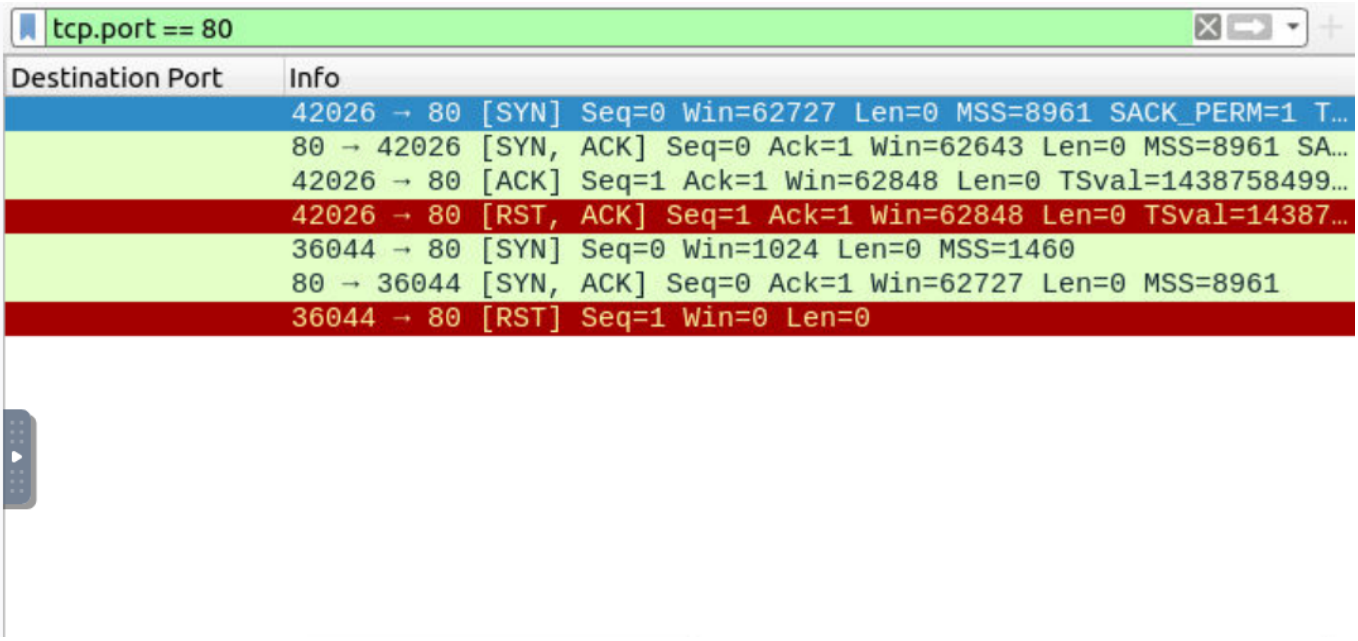
1. What is the total number of the "TCP Connect" scans?

```
tcp.flags.syn==1 and tcp.flags.ack==0 and tcp.window_size > 1024
```

Key: 1000

2. Which scan type is used to scan the TCP port 80?

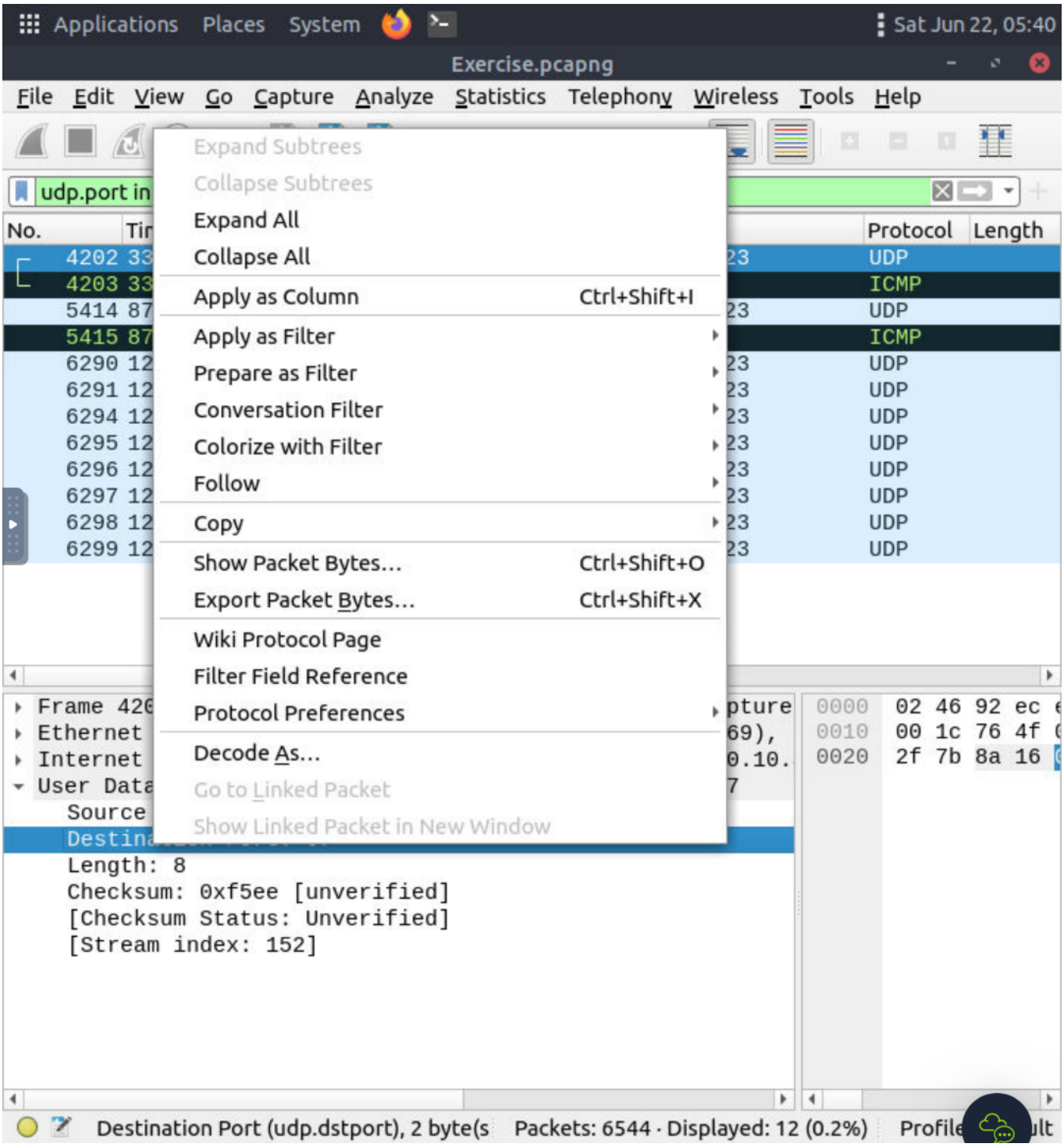
```
tcp.port == 80
```



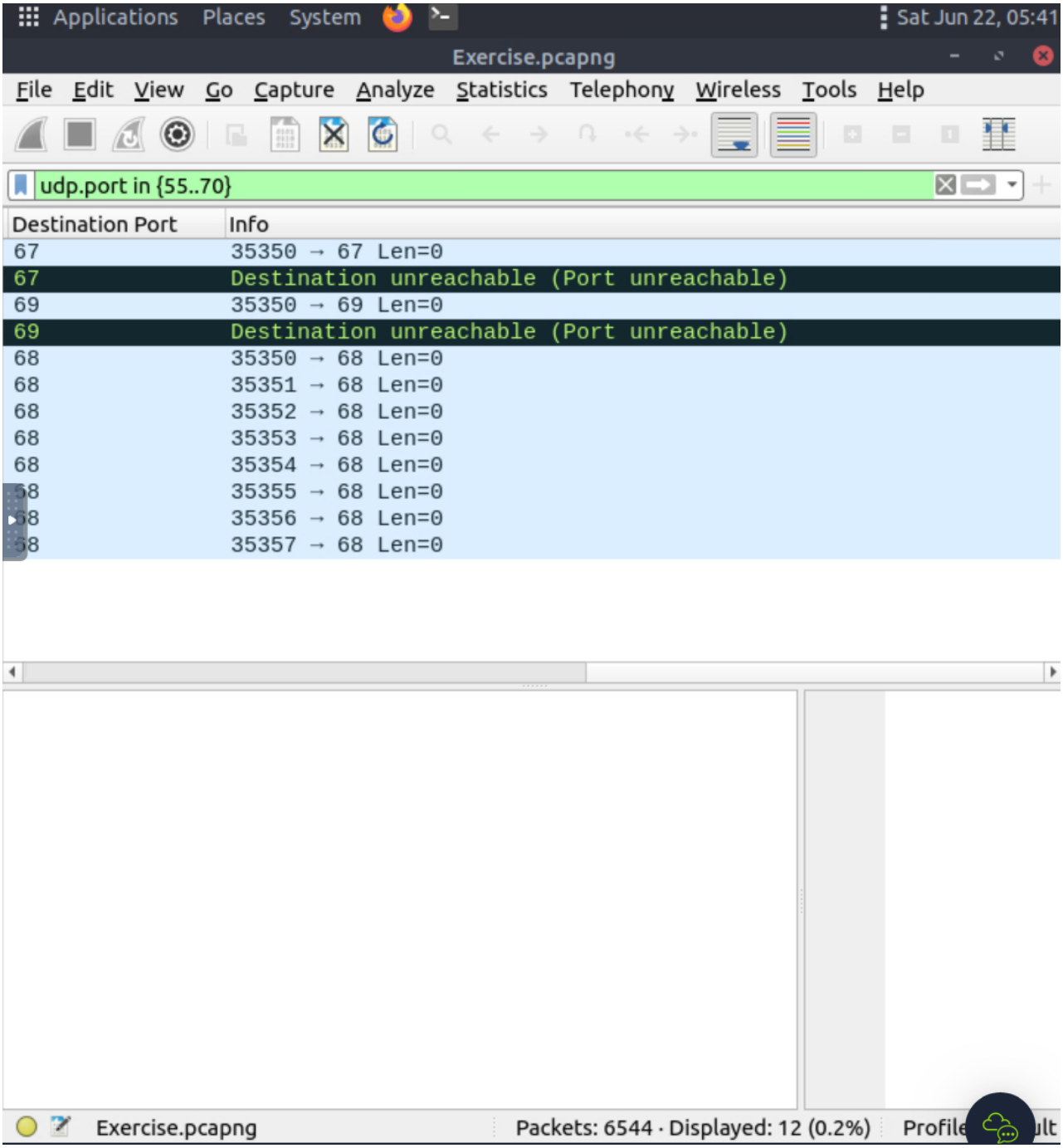
- You can see result. It is TCP connect.
  Key: TCP connect

5. Which UDP port in the 55-70 port range is open?

```
udp.port in {55-70}
```


Applications
Places
System
Sat Jun 22, 05:40
Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.port in
No.
Protocol
Length
4202 33
UDP
4203 33
ICMP
5414 87
UDP
5415 87
ICMP
6290 12
UDP
6291 12
UDP
6294 12
UDP
6295 12
UDP
6296 12
UDP
6297 12
UDP
6298 12
UDP
6299 12
UDP
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Frame 420
Ethernet
Internet
User Data
Source
Length: 8
Checksum: 0xf5ee [unverified]
[Checksum Status: Unverified]
[Stream index: 152]
0000 02 46 92 ec
0010 00 1c 76 4f
0020 2f 7b 8a 16
Destination Port (udp.dstport), 2 byte(s
Packets: 6544 · Displayed: 12 (0.2%)
Profile

- Then choose *Apply as Column* for Destination port.



- As you can see, port 67 and 69 close. Port 68 open.

  Key: 68

II. ARP Poisoning & Man In The Middle!

1. What is the number of ARP requests crafted by the attacker?

- First find spoofing MAC address

```
arp.duplicate-address-detected or arp.duplicate-address-frame
```

- We find `00:0c:29:e2:18:b4` is duppicated more time.
- Find arp resquest crafted by the attacker:

```
((arp) && (arp.opcode == 1)) && (arp.src.hw_mac ==
00:0c:29:e2:18:b4)
```

Key 284

2. What is the number of HTTP packets received by the attacker?

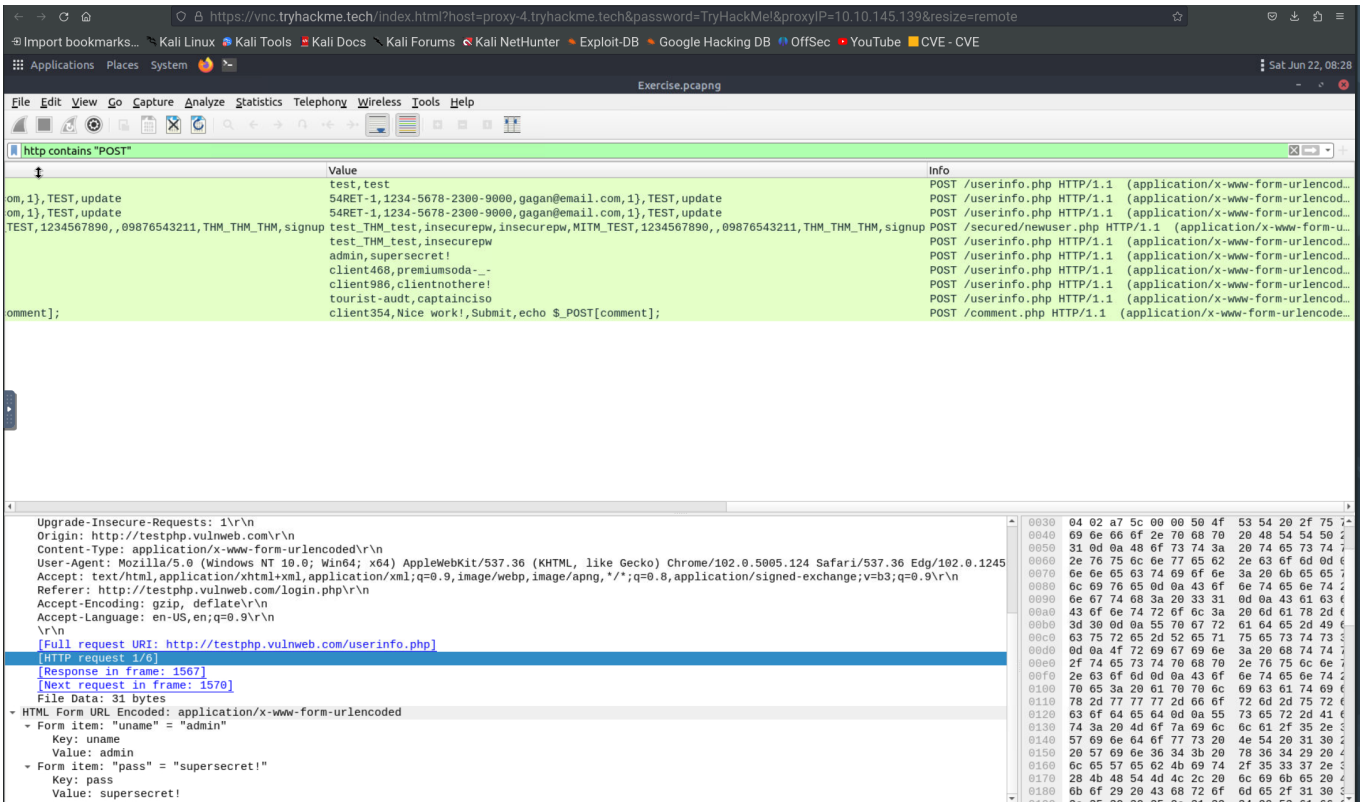
- Find anonimous ip of attacker and website.

```
http and ip.addr == 44.228.249.3 and ip.addr == 192.168.1.12
```

Key: 90

3. What is the number of sniffed username&password entries?

```
(http contain "POST") && (ip.addr == 192.168.1.12)
```



- Note *userinfo.php* and value. We can see username and pass but note 54RET.., it is not username and password. It logins using cookie so it is not user name and pass.

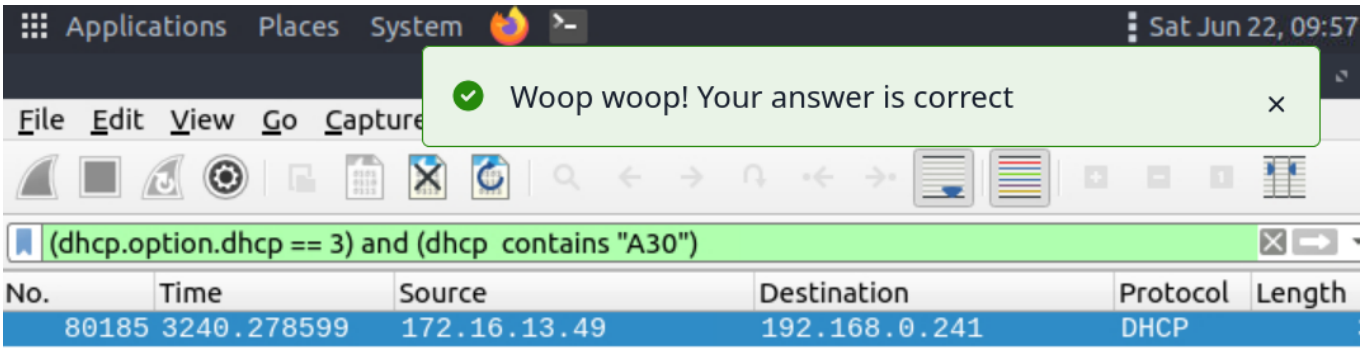
- After countering we find 6 username and password.
  Key 6
- See picture bellow to complete a rest of question.

III. Identifying Host: DHCP, NetBIOS, and Kerberos

1. What is the MAC address of the host "Galaxy A30"?

- **"DHCP Request"** packets contain the hostname information
- Filtering

```
(dhcp.option.dhcp == 3) and (dhcp contains "A30")
```



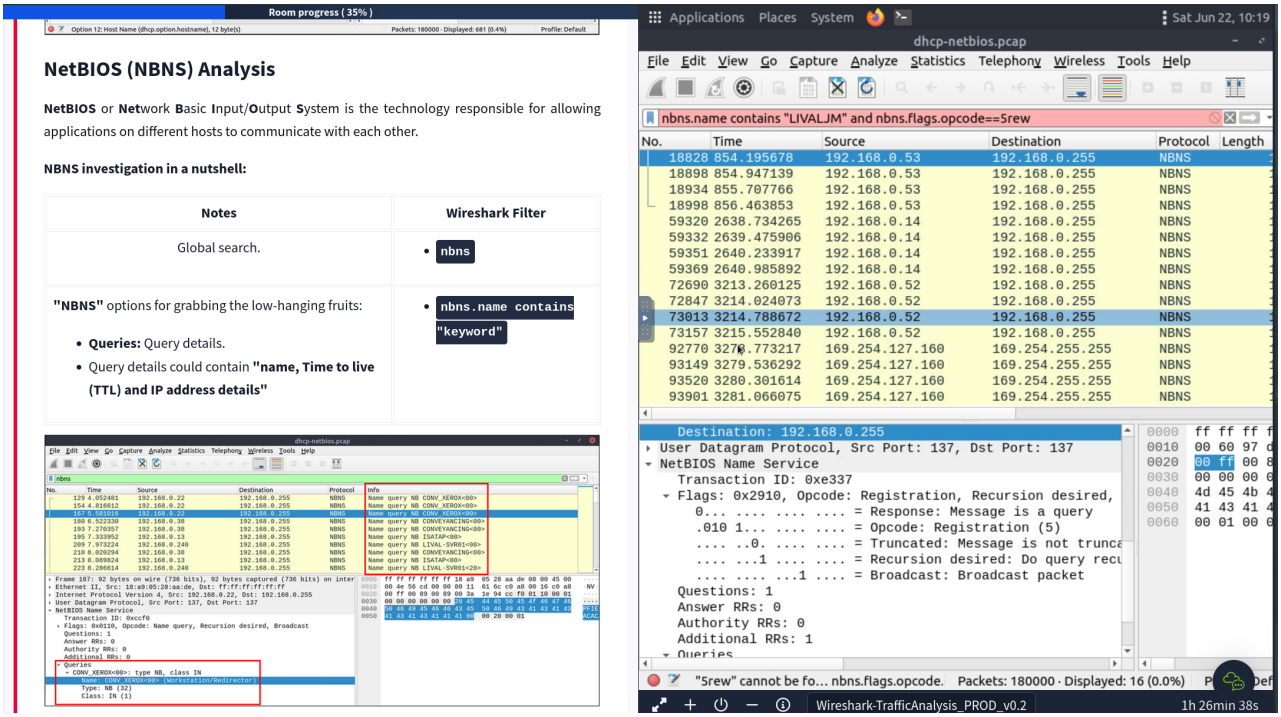
2. How many NetBIOS registration requests does the "LIVALJM" workstation have?

- First, we can see queries name "LIVALJM". We start filter with "LIVALMJ"

```
nbns.name contains "LIVAJM"
```

- After filtering, we will see info column. It is not only containing opcode "Registration".

- Starting analysis. Go to a packet has opcode "Registration". We will see:

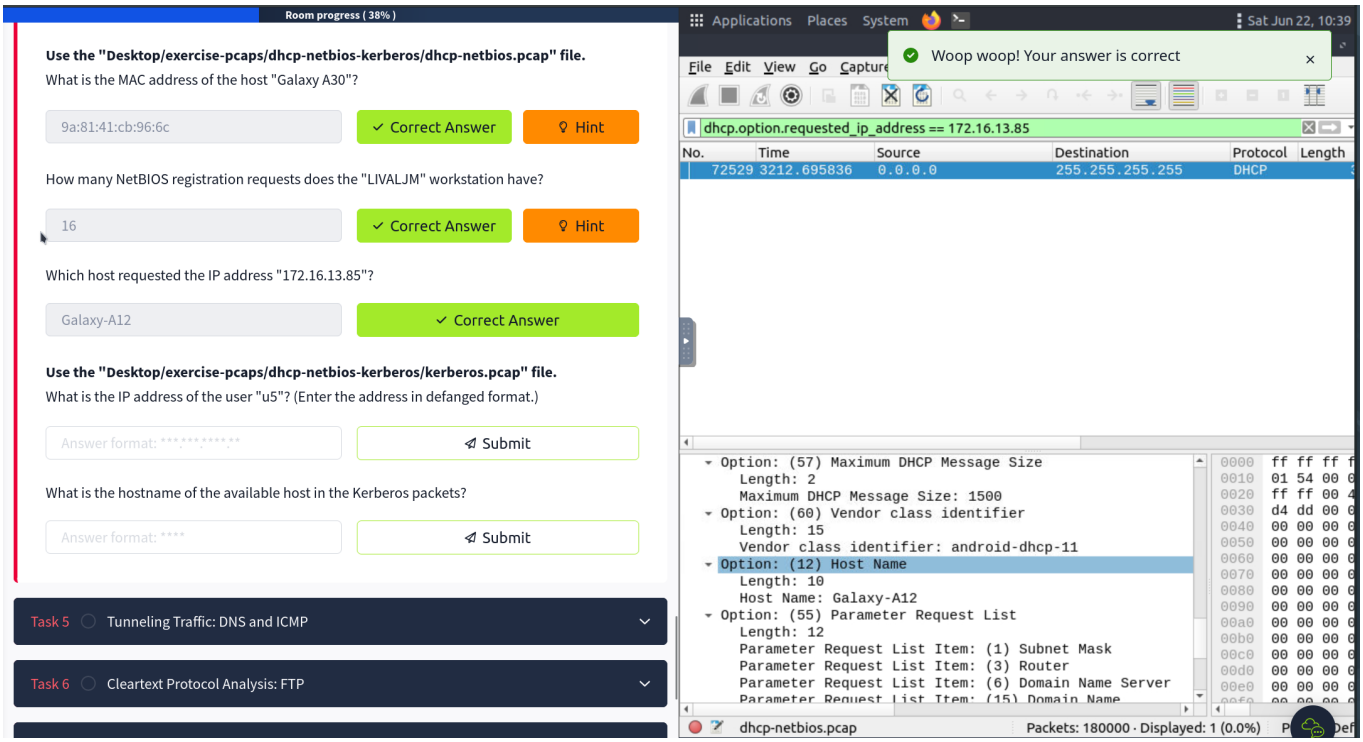


- Notice in Flags, we can see Opcode: Registration (5). Continuing filtering with command:

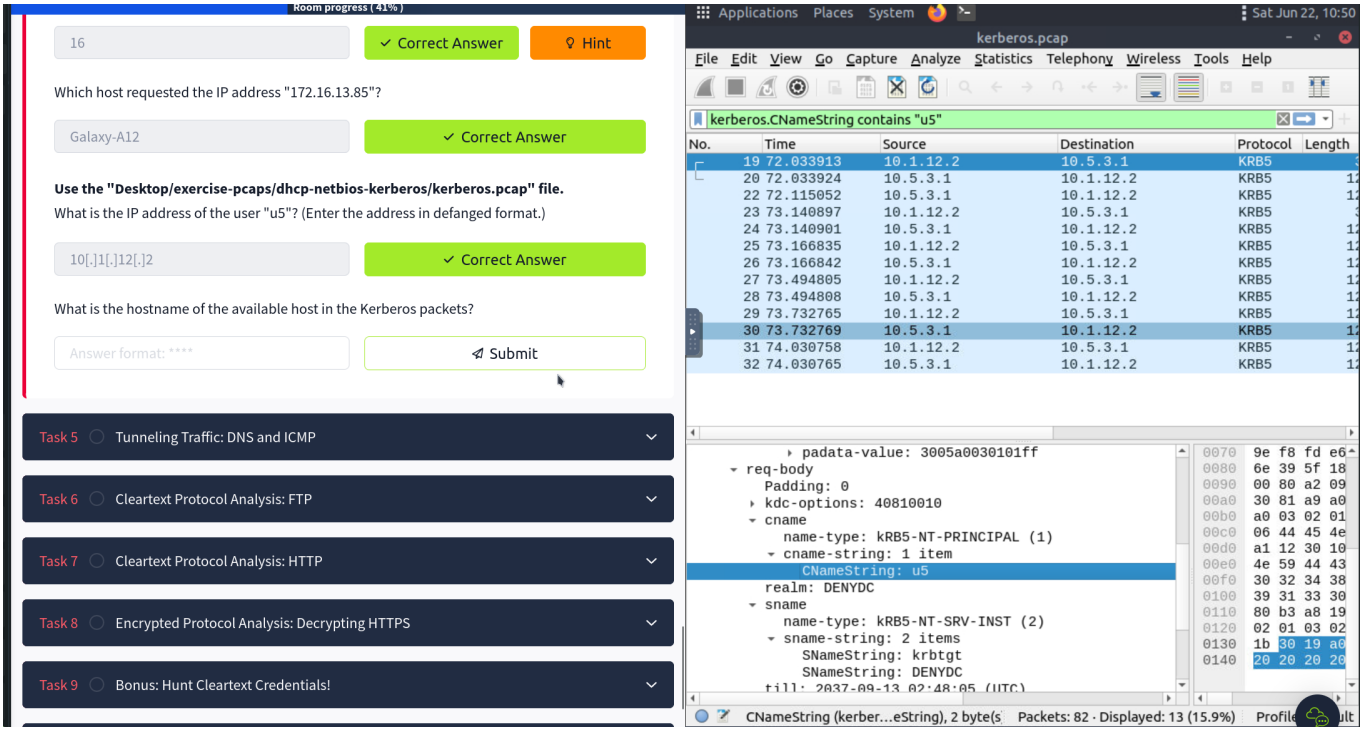
```
nbns.name contains "LIVALJM" and nbns.flags.opcode == 5
```

Key: 16

3. Which host requested the IP address "172.16.13.85"?



4. What is the IP address of the user "u5"? (Enter the address in defanged format.)



Key: 10[.]1[.]12[.]2

5. What is the hostname of the available host in the Kerberos packets?