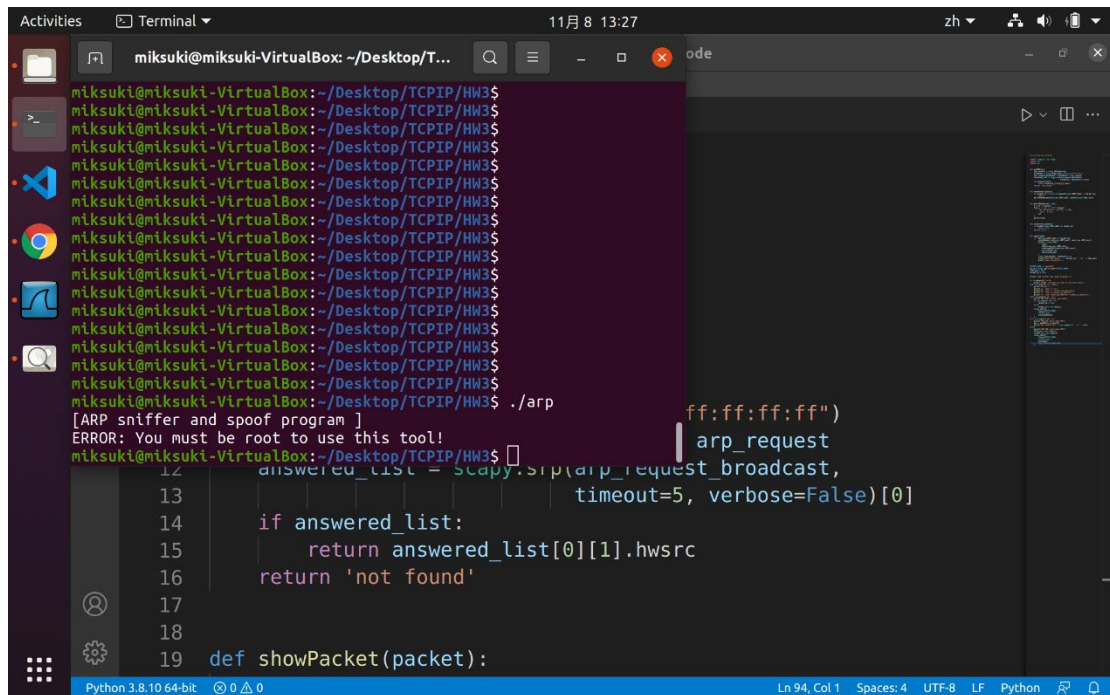


[illegible]

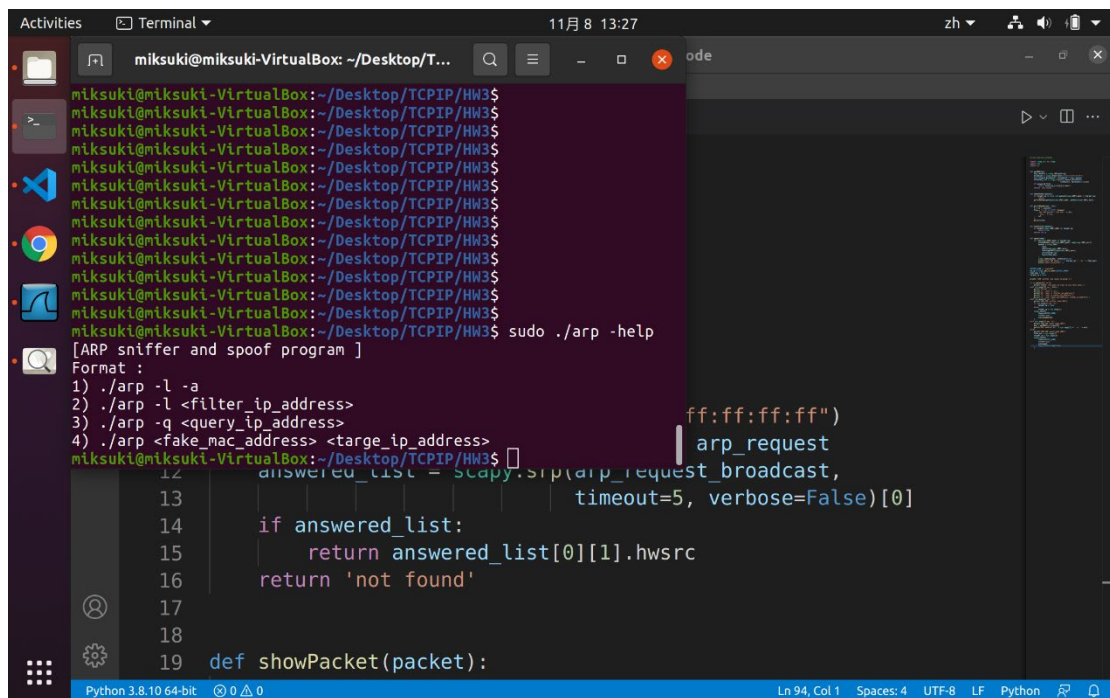
./arp



```
miksuki@miksuki-VirtualBox: ~/Desktop/TCPIP/HW3$ ./arp
[ARP sniffer and spoof program ]
ERROR: You must be root to use this tool!
miksuki@miksuki-VirtualBox: ~/Desktop/TCPIP/HW3$
```

```
12     answered_list = scapy.Sip(arp_request_broadcast,
13                               timeout=5, verbose=False)[0]
14     if answered_list:
15         return answered_list[0][1].hwsrc
16     return 'not found'
17
18
19 def showPacket(packet):
```

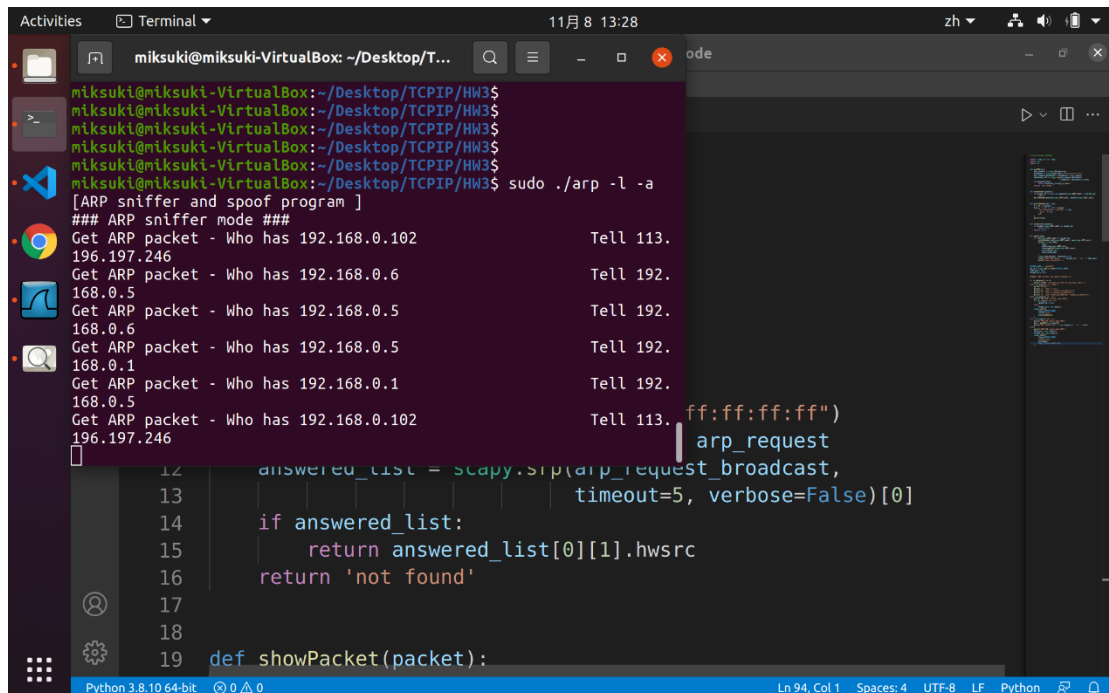
sudo ./arp -help



```
miksuki@miksuki-VirtualBox: ~/Desktop/TCPIP/HW3$ sudo ./arp -help
[ARP sniffer and spoof program ]
Format :
1) ./arp -l -a
2) ./arp -l <filter_ip_address>
3) ./arp -q <query_ip_address>
4) ./arp <fake_mac_address> <target_ip_address>
miksuki@miksuki-VirtualBox: ~/Desktop/TCPIP/HW3$
```

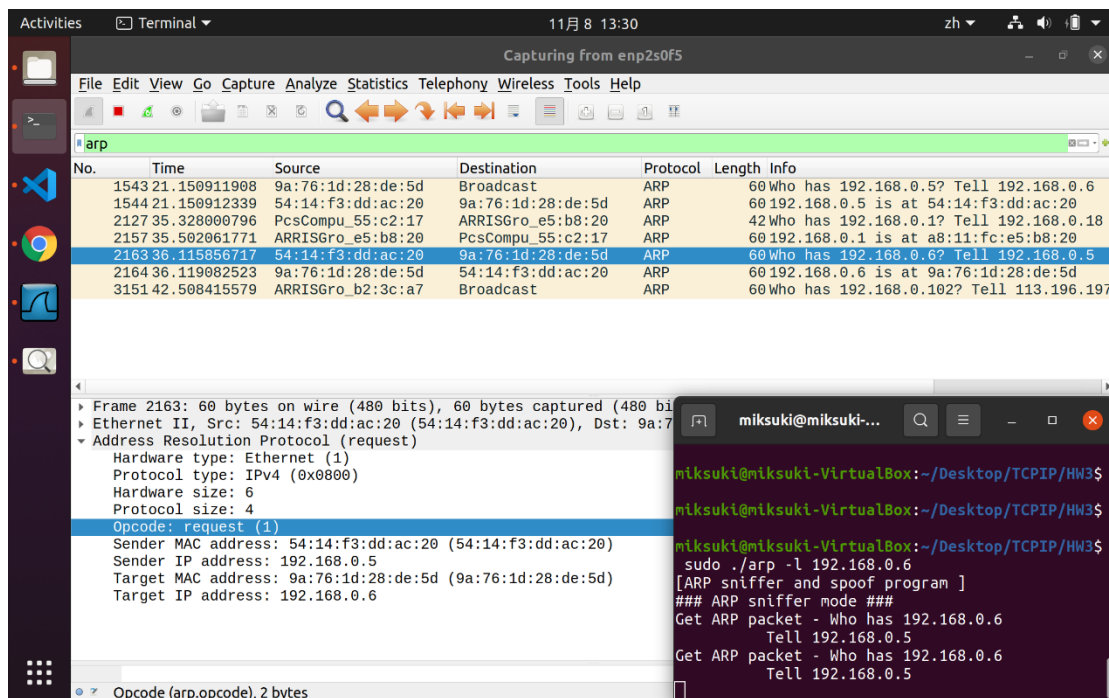
```
12     answered_list = scapy.Sip(arp_request_broadcast,
13                               timeout=5, verbose=False)[0]
14     if answered_list:
15         return answered_list[0][1].hwsrc
16     return 'not found'
17
18
19 def showPacket(packet):
```

`sudo ./arp -l -a`



```
miksuki@miksuki-VirtualBox: ~/Desktop/TCPIP/HW3$ sudo ./arp -l -a
[ARP sniffer and spoof program ]
### ARP sniffer mode ###
Get ARP packet - Who has 192.168.0.102          Tell 113.
196.197.246
Get ARP packet - Who has 192.168.0.6            Tell 192.
168.0.5
Get ARP packet - Who has 192.168.0.5            Tell 192.
168.0.6
Get ARP packet - Who has 192.168.0.5            Tell 192.
168.0.1
Get ARP packet - Who has 192.168.0.1            Tell 192.
168.0.5
Get ARP packet - Who has 192.168.0.102          Tell 113.
196.197.246
    arp_request = scapy.Sip(arp_request_broadcast,
                             timeout=5, verbose=False)[0]
    answered_list = scapy.Sip(arp_request_broadcast,
                             timeout=5, verbose=False)[0]
    if answered_list:
        return answered_list[0][1].hwsrc
    return 'not found'
def showPacket(packet):
```

`sudo ./arp -l 192.168.0.6`



No.	Time	Source	Destination	Protocol	Length	Info
1543	21.150911908	9a:76:1d:28:de:5d	Broadcast	ARP	60	Who has 192.168.0.5? Tell 192.168.0.6
1544	21.150912339	54:14:f3:dd:ac:20	9a:76:1d:28:de:5d	ARP	60	192.168.0.5 is at 54:14:f3:dd:ac:20
2127	35.328000796	PcsCompu_55:c2:17	ARRISGro_e5:b8:20	ARP	42	Who has 192.168.0.1? Tell 192.168.0.18
2157	35.502061771	ARRISGro_e5:b8:20	PcsCompu_55:c2:17	ARP	60	192.168.0.1 is at a8:11:fc:e5:b8:20
2163	36.115856717	54:14:f3:dd:ac:20	9a:76:1d:28:de:5d	ARP	60	Who has 192.168.0.6? Tell 192.168.0.5
2164	36.119082523	9a:76:1d:28:de:5d	54:14:f3:dd:ac:20	ARP	60	192.168.0.6 is at 9a:76:1d:28:de:5d
3151	42.508415579	ARRISGro_b2:3c:a7	Broadcast	ARP	60	Who has 192.168.0.102? Tell 113.196.197.246

Frame 2163: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on enp2s0f5
Ethernet II, Src: 54:14:f3:dd:ac:20 (54:14:f3:dd:ac:20), Dst: 9a:76:1d:28:de:5d (9a:76:1d:28:de:5d)
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: 54:14:f3:dd:ac:20 (54:14:f3:dd:ac:20)
Sender IP address: 192.168.0.5
Target MAC address: 9a:76:1d:28:de:5d (9a:76:1d:28:de:5d)
Target IP address: 192.168.0.6
Opcode (arp.opcode), 2 bytes

```
miksuki@miksuki-VirtualBox: ~/Desktop/TCPIP/HW3$ sudo ./arp -l 192.168.0.6
[ARP sniffer and spoof program ]
### ARP sniffer mode ###
Get ARP packet - Who has 192.168.0.6          Tell 192.168.0.5
Get ARP packet - Who has 192.168.0.6          Tell 192.168.0.5
```

`sudo ./arp -q 192.168.0.6`

The top screenshot shows a Wireshark capture of ARP traffic. The table below represents the data visible in the packet list:

No.	Time	Source	Destination	Protocol	Length	Info
541	2.935339741	PcsCompu_55:c2:17	Broadcast	ARP	42	Who has 192.168.0.6? Tell 192.168.0.18
542	2.970866166	9a:76:1d:28:de:5d	PcsCompu_55:c2:17	ARP	60	192.168.0.6 is at 9a:76:1d:28:de:5d
557	5.654753598	PcsCompu_55:c2:17	Broadcast	ARP	42	Who has 35.224.170.84? (ARP Probe)
564	5.932157149	ARRISGro_e5:b8:20	Broadcast	ARP	60	Who has 192.168.0.19? Tell 192.168.0.1
959	6.682920065	PcsCompu_55:c2:17	Broadcast	ARP	42	Who has 35.224.170.84? (ARP Probe)
1494	7.709466931	PcsCompu_55:c2:17	Broadcast	ARP	42	Who has 35.224.170.84? (ARP Probe)
1496	8.371495841	ARRISGro_e5:b8:20	Broadcast	ARP	60	Who has 192.168.0.19? Tell 192.168.0.1
1514	9.272132873	PcsCompu_55:c2:17	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.19
1515	9.274220711	ARRISGro_e5:b8:20	PcsCompu_55:c2:17	ARP	60	192.168.0.1 is at a8:11:fc:e5:b8:20

The bottom screenshot shows a terminal window with the following output:

```
miksuki@miksuki-VirtualBox:~/Desktop/TCPIP/HW3$  
miksuki@miksuki-VirtualBox:~/Desktop/TCPIP/HW3$  
miksuki@miksuki-VirtualBox:~/Desktop/TCPIP/HW3$  
miksuki@miksuki-VirtualBox:~/Desktop/TCPIP/HW3$  
sudo ./arp -q 192.168.0.6  
[ARP sniffer and spoof program ]  
### ARP query mode ###  
MAC address of 192.168.0.6 is 9a:76:1d:28:de:5d  
miksuki@miksuki-VirtualBox:~/Desktop/TCPIP/HW3$
```

`sudo ./arp 00:11:22:33:44:55 192.168.0.6`

The top screenshot shows a Wireshark capture of ARP traffic. The table below represents the data visible in the packet list:

No.	Time	Source	Destination	Protocol	Length	Info
849	8.818634314	54:14:f3:dd:ac:20	9a:76:1d:28:de:5d	ARP	60	Who has 192.168.0.6? Tell 192.168.0.5
850	8.821667109	PcsCompu_55:c2:17	Broadcast	ARP	42	Who has 192.168.0.5? Tell 192.168.0.19
851	8.821908711	54:14:f3:dd:ac:20	PcsCompu_55:c2:17	ARP	60	192.168.0.5 is at 54:14:f3:dd:ac:20
852	8.826338156	PcsCompu_55:c2:17	Broadcast	ARP	42	Who has 192.168.0.5? Tell 192.168.0.19
853	8.82665849	54:14:f3:dd:ac:20	PcsCompu_55:c2:17	ARP	60	192.168.0.5 is at 54:14:f3:dd:ac:20
854	8.828627104	PcsCompu_55:c2:17	54:14:f3:dd:ac:20	ARP	42	192.168.0.6 is at 00:11:22:33:44:55
855	9.055438182	9a:76:1d:28:de:5d	54:14:f3:dd:ac:20	ARP	60	192.168.0.6 is at 9a:76:1d:28:de:5d

The bottom screenshot shows a terminal window with the following output:

```
miksuki@miksuki-VirtualBox:~/Desktop/TCPIP/HW3$  
miksuki@miksuki-VirtualBox:~/Desktop/TCPIP/HW3$  
sudo ./arp 00:11:22:33:44:55 192.168.0.6  
[ARP sniffer and spoof program ]  
### ARP spoof mode ###  
Get ARP packet - Who has 192.168.0.6  
Tell 192.168.0.5  
Sent ARP Reply : 192.168.0.6 is 00:11:22:33:44:55  
Send successful.  
miksuki@miksuki-VirtualBox:~/Desktop/TCPIP/HW3$
```