CP1

```
sudo ./user
Name:                eth0  Desc :                                          (null)  Flags : 0x16.[up][running][connected]
Addr:   00:15:5d:6e:34:c0
Addr:      172.21.190.242
Addr:fe80::215:5dff:fe6e:34c0
Name:                  lo  Desc :                                          (null)  Flags : 0x37.[up][running][not_applicable]
Addr:   00:00:00:00:00:00
Addr:          127.0.0.1
Addr:                ::1
Name:                 any  Desc :      Pseudo-device that captures on all interfaces  Flags : 0x36.[up][running][not_applicable]
Name:    bluetooth-monitor  Desc :                             Bluetooth Linux Monitor  Flags : 0x38.[wireless][not_applicable]
Name:               nflog  Desc :             Linux netfilter log (NFLOG) interface  Flags : 0x30.[not_applicable]
Name:            nfqueue  Desc :         Linux netfilter queue (NFQUEUE) interface  Flags : 0x30.[not_applicable]
Name:              dummy0  Desc :                                          (null)  Flags : 0x30.[not_applicable]
Addr:   92:79:ed:df:6a:1a
Name:                sit0  Desc :                                          (null)  Flags : 0x30.[not_applicable]
Addr:   00:00:00:00:00:00
Name:               bond0  Desc :                                          (null)  Flags : 0x20.[disconnected]
Addr:   52:ba:59:c5:a2:35
```

This is the output of my implementation running displayAllDevs()。

CP2

```
Link layer header type = 1
Header info : cap_len : 1514, len : 1514
Link layer header type = 1
Header info : cap_len : 54, len : 54
Content:0155d6e34c00155de5cc780450028c2c340080670edac15b01ac15bef2198faf6172fe3511bdc6485501042b16700
Destination MAC : 0:15:5d:6e:34:c0
Source MAC : 0:15:5d:e5:c:c7
Type : 0x8
Link layer header type = 1
Header info : cap_len : 424, len : 424
Link layer header type = 1
Header info : cap_len : 193, len : 193
```

To implement the callback function, I created a new API called start Listen. This API will create a new thread listening on the packets and calls the user defined function when it detected a packet.

```
Frame 11767: 26 bytes on wire (208 bits), 26 bytes captured (208 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_6e:34:c0 (00:15:5d:6e:34:c0), Dst: 12:13:13:22:44:03 (12:13:13:22:44:03)
  Destination: 12:13:13:22:44:03 (12:13:13:22:44:03)
  Source: Microsof_6e:34:c0 (00:15:5d:6e:34:c0)
  Type: Unknown (0x8000)
Data (12 bytes)
  Data: 48656c6c6f20776f726c6421
  [Length: 12]
```

```
000  12 13 13 22 44 03 00 15  5d 6e 34 c0 80 00 48 65   ···"D··· ]n4···He
010  6c 6c 6f 20 77 6f 72 6c  64 21                     llo worl d!
```

This is the packet I injected into the network and captured it using wireshark.