Mission 6

Figure out the Dark Side's secret wireless key by using Aircrack-ng.

Solution:

Change directory to where the word lists file is, and run the following command:

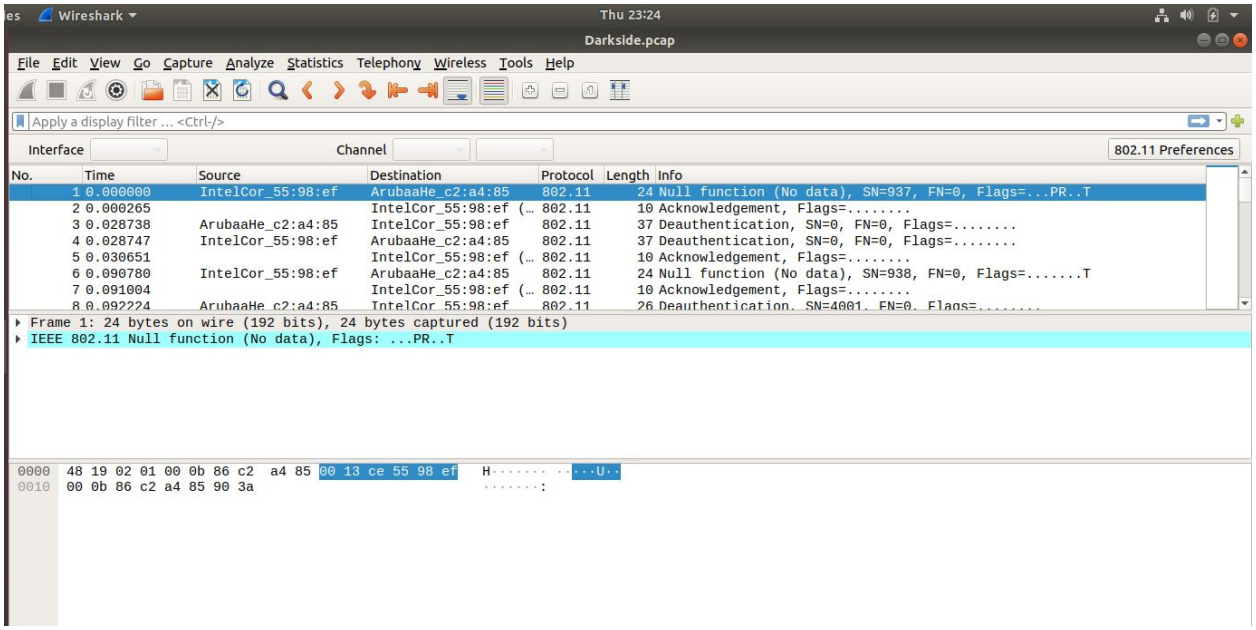
```
sysadmin@UbuntuDesktop:~/darkside$ cd /usr/share/wordlists
sysadmin@UbuntuDesktop:/usr/share/wordlists$ ls
rockyou.txt
sysadmin@UbuntuDesktop:/usr/share/wordlists$ sudo aircrack-ng -w rockyou.txt ~/darkside/Da
rkside.pcap
Opening /home/sysadmin/darkside/Darkside.pcap
Read 586 packets.

   #  BSSID              ESSID                     Encryption

   1  00:0B:86:C2:A4:85  linksys                   WPA (1 handshake)

Choosing first network as target.

Opening /home/sysadmin/darkside/Darkside.pcap
Reading packets, please wait...




                               Aircrack-ng 1.2 rc4

     [00:00:01] 2300/8053877 keys tested (1920.24 k/s)

     Time left: 1 hour, 9 minutes, 53 seconds                  0.03%

                          KEY FOUND! [ dictionary ]


     Master Key     : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2
                      52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2
```

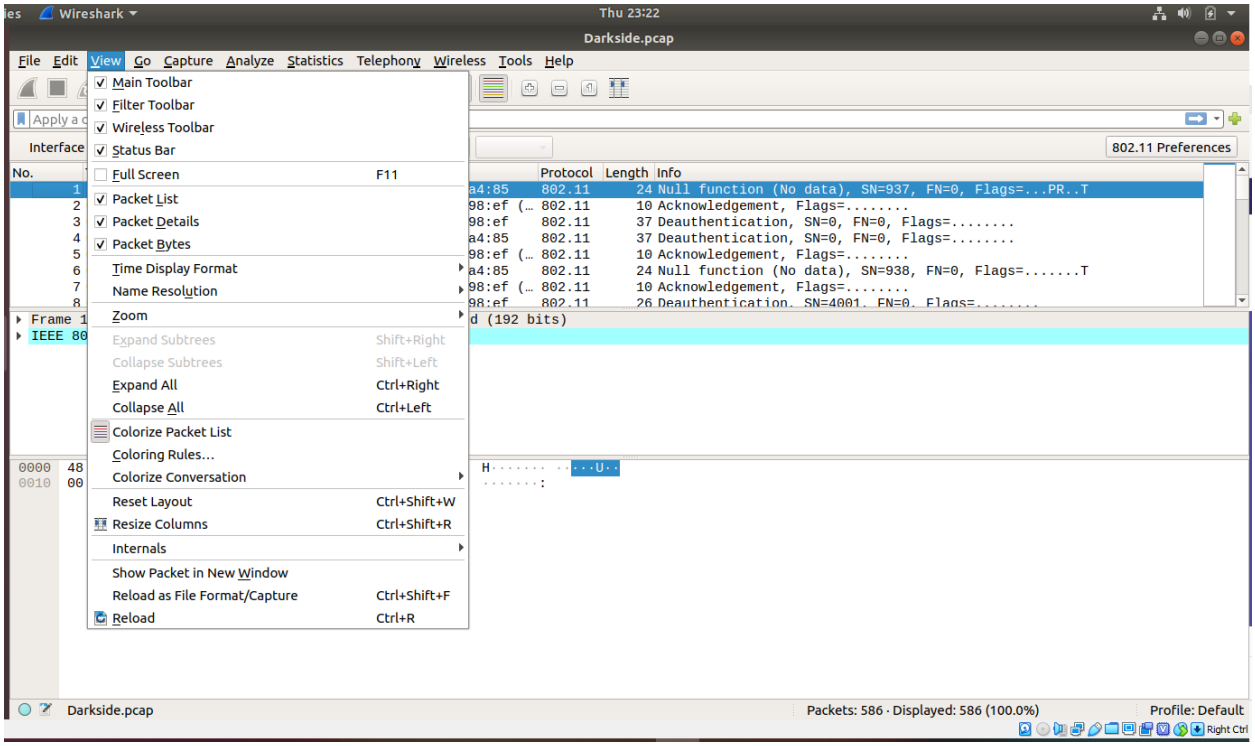
```
   1  00:0B:86:C2:A4:85  linksys                 WPA (1 handshake)

Choosing first network as target.

Opening /home/sysadmin/darkside/Darkside.pcap
Reading packets, please wait...









                              Aircrack-ng 1.2 rc4

      [00:00:01] 2300/8053877 keys tested (1920.24 k/s)

      Time left: 1 hour, 9 minutes, 53 seconds                  0.03%

                           KEY FOUND! [ dictionary ]


      Master Key     : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2
                       52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2

      Transient Key  : 1B 7B 26 96 03 F0 6C 6C D4 03 AA F6 AC E2 81 FC
                       55 15 9A AF BB 3B 5A A8 69 05 13 73 5C 1C EC E0
                       A2 15 4A E0 99 6F A9 5B 21 1D A1 8E 85 FD 96 49
                       5F B4 97 85 67 33 87 B9 DA 97 97 AA C7 82 8F 52

      EAPOL HMAC     : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51
sysadmin@UbuntuDesktop:/usr/share/wordlists$
```

The cracked passphrase is: dictionary.

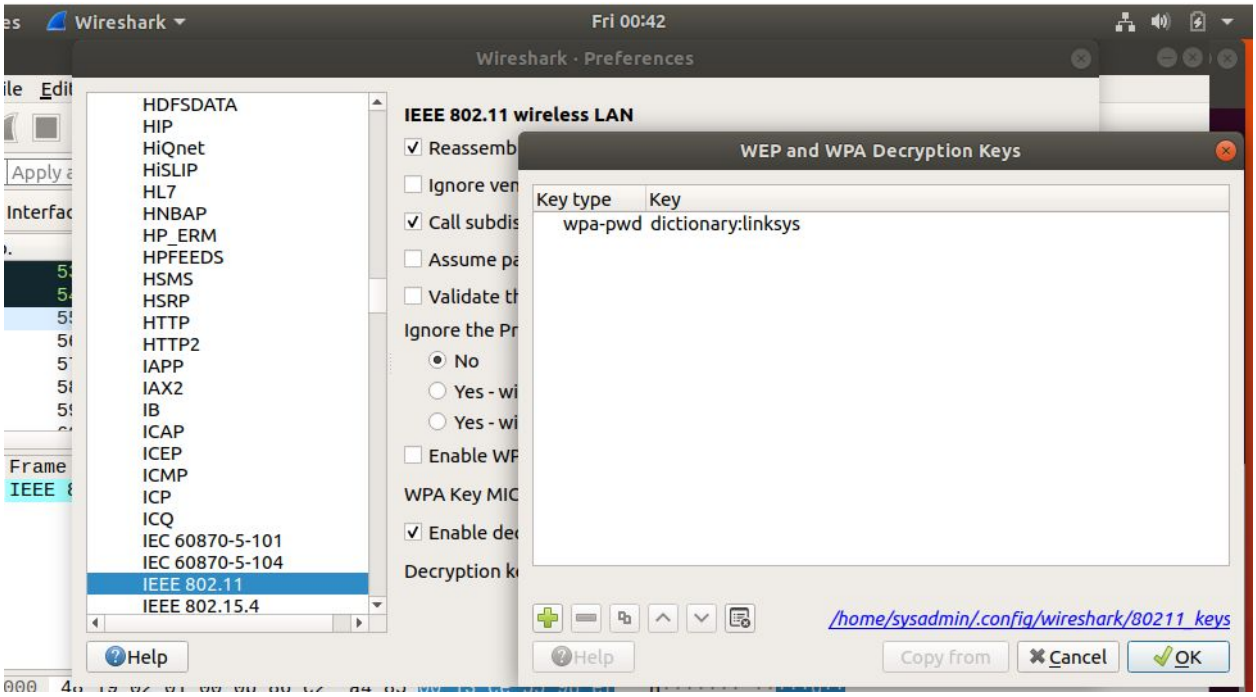
Then run wireshark on Darkside.pcap like:

```
sysadmin@UbuntuDesktop:~/darkside$
sysadmin@UbuntuDesktop:~/darkside$ wireshark Darkside.pcap
```



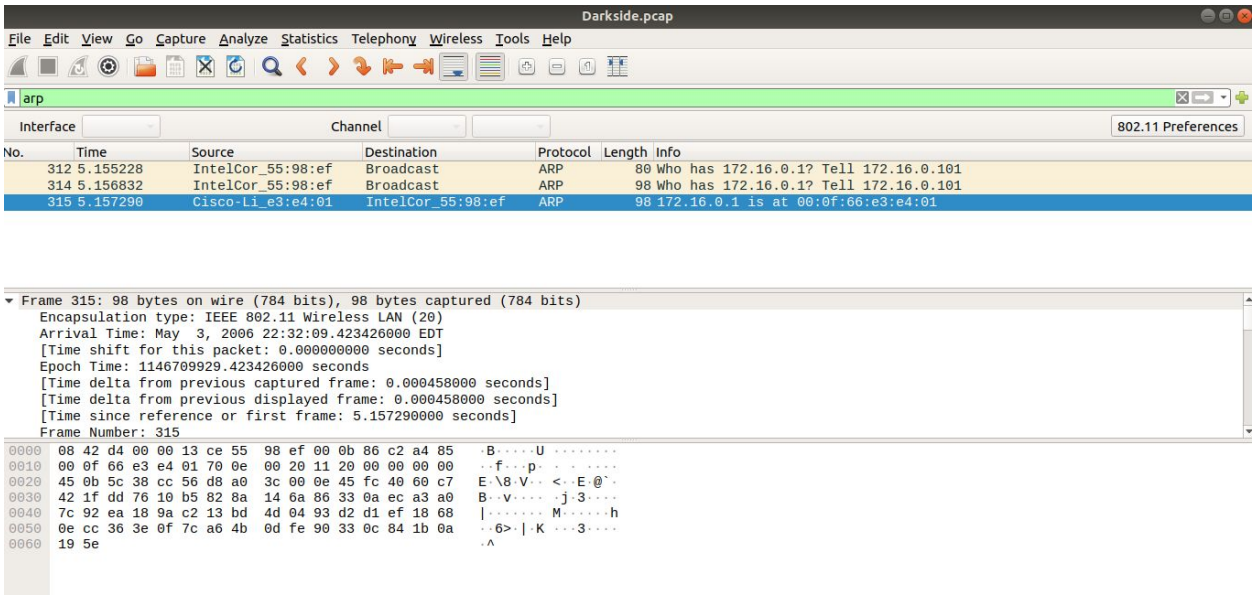


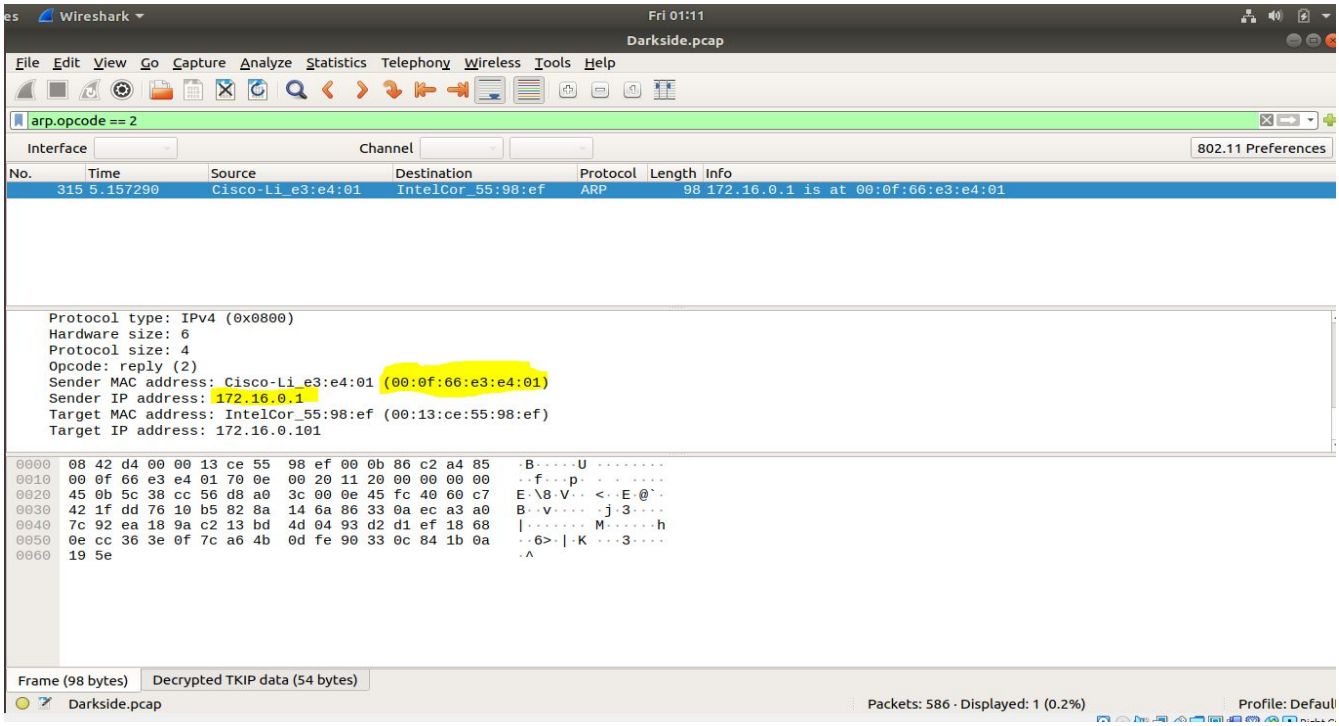
Type in the passphrase with the SSID separated only by colon in the WEP and WPA Decryption keys Window shown below.



Click the OK button.

Looking into the decrypted arp traffic,





The host IP address is 172.16.0.1
The MAC address is 00:0f:66:e3:e4:01