Nama: Muhammad Risqi Firmansyah

NIM : 1310652020

Disisni saya menggunakan Wireshark, Paket EAPOL itu yang berusaha ngecrack soalnya di manual penggunaan/ help software Whireshark untuk mengecrack sebuah keamanan WPA memerlukan 4 jalan di wiresharknya yang tertulis 4 adalah paket EAPOL

```
paketdata_2.pcapng [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
                                                                                                                                                                                                                                                                                                                                                                                                                                   _ 0 X
Eile Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
                                                                                                             Expression

Destination
Broadcast
Alfa_61:ec:87 (RA)
         Time Source 557 bit 51/4640/14/Ta.blect.8/
558 68.62311800(Tp-1-inkT_a7:a3:39
559 68.63511300(00:4f:62:2d:18:72
560 69.04453700(10:4f:62:2d:18:72
560 69.04535200(Tp-1-inkT_a8:29:64
562 69.147/00300(00:4f:62:2d:18:72
563 69.76059200
564 69.76193300(14/Fa.61:ec:87
565 69.76192900(Tp-1-inkT_96:12:ab
566 69.78692700(Tp-1-inkT_96:12:ab
568 69.96271800(
569 69.96393000(Tp-1-inkT_96:12:ab
568 69.96271800(
569 69.96393000(Tp-1-inkT_96:12:ab
570 69.96405400(A1fa.61:ec:87
571 69.97174900(A1fa.61:ec:87
                                                                                                                                                                                                   802.11
802.11
802.11
802.11
802.11
802.11
802.11
802.11
802.11
            x/2 69, 97204900

$73 69, 9733680017p-LinkT_96:12:ab

$74 69, 9740510017p-LinkT_96:12:ab

$75 69, 983350041Fa_61:ec:87

$76 69, 98468500

$77 69, 9837380017p-LinkT_96:12:ab

$78 69, 98889100

$78 69, 98889100
             572 69.972049000
                                                                                                                                                                          802.11
                                                                                                                                                                         802.11
             579 69.98902900(ATTa_61:ec:67
580 69.99180700(Tp-LinkT_96:12:ab
                                                                                                              Broadcast 802.11
Apple_00:b1:b1 (RA) 802.11
Broadcast 802.11
Apple_00:b1:b1 (RA) 802.11
Apple_00:b1:b1 (RA) 802.11
Broadcast 802.11
                                                                                                                                                                                                      372 Beacon frame, SN=394, FN=0, Flags=......C, BI=100, SSID=virtue00
                                                                                                                                                                                                   581 70.02348100(
582 70.02349100(Apple_00:b1:b1
## Frame 579: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0 

### Radiotap Header v0, Length 13 

■ IEEE 802.11 Data, Flags: ......T
```

Setelah itu di cari yang nama wifi yang menggunakan WPA, dari 5 ssid yang menggunakan WPA adalah virtue00

Habis itu di crack dengan backtrack versi r3 dan dictionarynya menggunakan wordlist dengan aircrack ng terbaru sehingga di dapatkan kunci yaitu

```
risqiRPL@ cyber ~ $ aircrack-ng -w pass.txt neteasy.pcap
Opening neteasy.pcap
Read 785 packets.

# BSSID ESSID Encryption

1 00:4F:62:2D:18:72 00 No data - WEP or WPA
2 A0:F3:C1:96:12:AB virtue00 WPA (1 handshake)
```

## idsecconf2013