Nama : Rachma Prayogo Widoyanto

NIM : 1310652054

Menggunakan Wireshark, Paket EAPOL 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)]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         \underline{\text{File}} \quad \underline{\text{Edit}} \quad \underline{\text{V}} \text{iew} \quad \underline{\text{G}} \text{o} \quad \underline{\text{C}} \text{apture} \quad \underline{\text{A}} \text{nalyze} \quad \underline{\text{S}} \text{tatistics} \quad \text{Telephon} \underline{y} \quad \underline{\text{I}} \text{ools} \quad \underline{\text{Internals}} \quad \underline{\text{H}} \text{elp}
Filter:
                                                                                                                                                                                                                                       Expression... Clear Apply Save
                                                                                                                                                                                                                                                                    | Protocol | Length | Info | 802.11 | 125 Beacon frame, SN-258[4, FN-0, Flags=......, SSID=Broadcast | SN-208[4, FN-0], Flags=....., SSID=Broadcast | SN-208[4, FN-0], Flags=....., BI=100, SSID=MDRA | S02.11 | 148 Beacon frame, SN-1051, FN-0, Flags=....., BI=100, SSID=00 | S02.11 | 148 Beacon frame, SN-1051, FN-0, Flags=...., BI=100, SSID=00 | S02.11 | 311 Beacon frame, SN-256, FN-0, Flags=...., BI=100, SSID=00 | S02.11 | 314 Beacon frame, SN-208[4, FN-0], Flags=...., BI=100, SSID=00 | S02.11 | 49 Acknowledgement, Flags=....., BI=100, SSID=00 | S02.11 | 40 Acknowledgement, Flags=....., BI=100, SSID=00 | S02.11 | 50 Authentication, SN-0, FN-0, Flags=...., BI=100, SSID=00 | S02.11 | 372 Beacon frame, SN-393, FN-0, Flags=...., BI=100, SSID=virtue00 | S02.11 | 372 Beacon frame, SN-393, FN-0, Flags=...., C, BI=100, SSID=virtue00 | S02.11 | 40 Acknowledgement, Flags=...., C | S02.11 | 43 Authentication, SN-0, FN-0, Flags=...., C, BI=100, SSID=virtue00 | S02.11 | 40 Acknowledgement, Flags=...., C | S02.11 | 43 Authentication, SN-2183, FN-0, Flags=...., C | S02.11 | 43 Authentication, SN-2183, FN-0, Flags=...., C | S02.11 | 45 Authentication, SN-2183, FN-0, Flags=...., C | S02.11 | 57 Beassociation Request, SN-2184, FN-0, Flags=...., SSID=virtue00 | S02.11 | 40 Acknowledgement, Flags=...., C | S02.11 | 40 Acknowledgement, Flags=...., C | S02.11 | 40 Acknowledgement, Flags=..., C | S02.11 | S02.
               Broadcast
Broadcast
                                                                                                                                                                                          Broadcast
                                                                                                                                                                                         Broadcast
Broadcast
Alfa_61:ec:87 (RA)
Tp-LinkT_96:12:ab
Alfa_61:ec:87
Broadcast
Broadcast
                                                                                                                                                                                       Broadcast
Alfa_61:ec:87 (RA)
Alfa_61:ec:87
Tp-LinkT_96:12:ab
Alfa_61:ec:87 (RA)
Alfa_61:ec:87 (RA)
Alfa_61:ec:87
Alfa_61:ec:87
Alfa_61:ec:87
Alfa_61:ec:87 (RA)
Alfa_61:ec:87 (RA)
Alfa_61:ec:87 (RA)
Tp-LinkT_96:12:ab
                      576 69.984685000
                      577 69.98573800(Tp-LinkT_96:12:ab
                      578 69.988891000
                                                                                                                                                                                                                                                                                                                                       14A key (MasSage 4 of 4)
372 Beacon frame, SN=394, FN=0, Flags=.....C, BI=100, SSID=virtue00
40 Acknowledgement, Flags=.....C
106 Data, SN=395, FN=0, Flags=.....C
40 Acknowledgement, Flags=.....C
40 Acknowledgement, Flags=.....C
372 Beacon frame, SN=396, FN=0, Flags=.....C, BI=100, SSID=virtue00
                                                                                                                                                                                          Tp-LinkT_96:12:au
Broadcast
Apple_00:b1:b1 (RA)
Broadcast
                      579 69.98902900(Alfa_61:ec:87
580 69.99180700(Tp-LinkT_96:12:ab
581 70.02348100(
582 70.02349100(Apple_00:b1:b1
583 70.02468100(
                                                                                                                                                                                         Broadcast
Apple_00:b1:b1 (RA)
Apple_00:b1:b1 (RA)
Broadcast
                      585 70.09403400(Tp-LinkT_96:12:ab
                                                                                                                                                                                                                                                                                           802.11
  ⊕ 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 :

```
Compaq-pc-2000 ~ $ 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