

# Informe Laboratorio 3

## Sección x

Alumno Jorge Toro Macías  
e-mail: jorge.toro1@mail.udp.cl

Mayo de 2024

## Índice

<b>1. Descripción de actividades</b>	<b>2</b>
<b>2. Desarrollo (PASO 1)</b>	<b>3</b>
2.1. En qué se destaca la red del informante del resto . . . . .	3
2.2. Explica matemáticamente porqué se requieren más de 5000 paquetes para obtener la pass . . . . .	3
2.3. Obtiene la password con ataque por defecto de aircrack-ng . . . . .	3
2.4. Indica el tiempo que demoró en obtener la password . . . . .	4
2.5. Descifra el contenido capturado . . . . .	4
2.6. Describe como obtiene la url de donde descargar el archivo . . . . .	6
<b>3. Desarrollo (PASO 2)</b>	<b>6</b>
3.1. Script para modificar diccionario original . . . . .	6
3.2. Cantidad de passwords finales que contiene rockyou_mod.dic . . . . .	7
<b>4. Desarrollo (Paso 3)</b>	<b>8</b>
4.1. Obtiene contraseña con hashcat con potfile . . . . .	8
4.2. Nomenclatura del output . . . . .	8
4.3. Obtiene contraseña con hashcat sin potfile . . . . .	8
4.4. Nomenclatura del output . . . . .	8
4.5. Obtiene contraseña con aircrack-ng . . . . .	8
4.6. Identifica y modifica parámetros solicitados por pycrack . . . . .	9
4.7. Obtiene contraseña con pycrack . . . . .	10

## 1. Descripción de actividades

Su informante quiere entregarle la contraseña de acceso a una red, pero desconfía de todo medio para entregársela (aún no llega al capítulo del curso en donde aprende a comunicar una password sin que nadie más la pueda interceptar). Por lo tanto, le entregará un archivo que contiene un desafío de autenticación, que al analizarlo, usted podrá obtener la contraseña que lo permite resolver. Como nadie puede ver a su informante (es informante y debe mantener el anonimato), él se comunicará con usted a través de la redes inalámbricas y de una forma que solo usted, como experto en informática y telecomunicaciones, logrará esclarecer.

1. Identifique cual es la red inalámbrica que está utilizando su informante para enviarle información. Obtenga la contraseña de esa red utilizando el ataque por defecto de aircrack-ng, indicando el tiempo requerido para esto. Descifre el contenido transmitido sobre ella y descargue de Internet el archivo que su informante le ha comunicado a través de los paquetes que usted ha descifrado.
2. Descargue el diccionario de Rockyou (utilizado ampliamente en el mundo del pentesting). Haga un script que para cada string contenido en el diccionario, reemplace la primera letra por su letra en capital y agregue un cero al final de la password.

Todos los strings que comiencen con número toca eliminarlos del diccionario. Indique la cantidad de contraseñas que contiene el diccionario modificado debe llamarse rockyou\_mod.dic A continuación un ejemplo de cómo se modifican las 10 primeras líneas del diccionario original.

3. A partir del archivo que descargó de Internet, obtenga la password asociada a la generación de dicho archivo. Obtenga la llave mediante un ataque por fuerza bruta. Para esto deberá utilizar tres herramientas distintas para lograr obtener la password del archivo: hashcat, aircrack-ng, pycrack. Esta última, permite entender paso a paso de qué forma se calcula la contraseña a partir de los valores contenidos en el handshake, por lo que deberá agregar dichos valores al código para obtener la password a partir de ellos y de rockyou\_mod.dic. Antes de ejecutar esta herramienta deberá deshabilitar la función RunTest().

Al calcular la password con hashcat utilice dos técnicas: una donde el resultado se guarda en el potfile y otra donde se deshabilita el potfile. Indique qué información retorna cada una de las 2 técnicas, identificando claramente cada campo.

Recuerde indicar los 4 mayores problemas que se le presentaron y cómo los solucionó.

## 2. Desarrollo (PASO 1)

### 2.1. En qué se destaca la red del informante del resto

```

CH 12 [ ] Elapsed: 1 min [ ] 2024-05-14 09:05
BSSID PWR Beacons #Data, #S CH MD ENC CIPHER AUTH ESSID
E6:AB:89:1C:85:38 -1 0 0 0 6 -1 WPA <length: 0>
B0:48:7A:D2:DD:74 -55 242 5005 0 8 54e WEP WEP WEP
9B:FC:11:8B:0B:09 -57 22 1768 0 11 130 WPA2 CCMP PSK Telefonica
B0:1F:8C:E2:14:A1 -64 78 0 0 1 130 DPM Invitados-UDP
B0:1F:8C:E2:14:A7 -65 67 1 0 1 130 WPA2 CCMP MGT Administrativos-UDP
B0:1F:8C:E2:14:A6 -65 74 0 0 1 130 DPM VIP-UDP
B0:1F:8C:E2:14:A6 -66 79 0 0 1 130 WPA3 CCMP OWE <length: 0>
B0:1F:8C:E2:14:A3 -69 82 0 0 1 130 DPM Alumnos-UDP
B0:1F:8C:E2:14:A0 -69 72 0 0 1 130 WPA3 CCMP SAE Sala Híbrida-UDP
AC:FA:BC:10:00:00 -74 14 0 0 1 130 WPA2 CCMP PSK VTR-402479
B0:1F:8C:E2:14:A2 -78 76 0 0 1 130 WPA3 CCMP OWE <length: 0>
B4:1C:8B:83:DA:07 -74 5 0 0 1 130 WPA2 CCMP PSK ZTE-352497
F4:AB:89:87:57:38 -75 37 0 0 1 130 WPA2 CCMP PSK SoftS22_2,4G
7C:00:AD:97:8A:74 -75 58 0 0 1 480 WPA2 CCMP PSK DPTD-187
58:EF:08:47:59:CB -74 85 0 0 1 130 WPA2 CCMP PSK cabledatafemotica
58:EF:08:47:59:CB -75 114 0 0 1 130 DPM
44:AB:89:AA:3C:F8 -77 4 0 0 1 130 WPA2 CCMP PSK Saveria
BA:0B:18:C6:83:E9 -78 46 0 0 2 195 WPA2 CCMP PSK <length: 0>
B0:1F:8C:E2:14:A4 -79 65 11 0 1 130 WPA3 CCMP OWE _owetr_Alumnos-UDP1993294148
BA:0B:18:C6:83:E9 -82 43 0 0 2 195 WPA2 CCMP PSK FamiliaCA_EXT
7C:00:AD:97:8A:74 -82 7 0 0 1 130 WPA2 CCMP PSK Expedientes
18:35:D1:48:EB:39 -84 0 0 0 1 130 WPA2 CCMP PSK VTR-537275
AC:FA:BC:10:00:00 -86 19 0 0 1 130 WPA2 CCMP PSK VTR-551041
18:EB:29:90:89:63 -82 13 0 0 1 130 WPA2 CCMP PSK New-Lapine
3E:EB:29:90:89:63 -93 0 0 0 3 130 WPA2 CCMP PSK HK Supervisores
B0:1F:8C:E2:14:A3 -83 1 0 0 1 130 DPM VIP-UDP
18:35:D1:48:EB:39 -93 3 0 0 1 130 WPA2 CCMP PSK VTR-295921
B0:1F:8C:E2:14:A3 -1 0 0 0 1 130 WPA2 CCMP <length: 0>
18:35:D1:48:EB:39 -87 4 0 0 1 130 WPA2 CCMP PSK VTR-673269
B0:1F:8C:E2:14:A1 -89 1 0 0 1 130 DPM Invitados-UDP
14:51:28:57:6C:ED -83 2 0 0 0 270 WPA2 CCMP PSK <length: 0>
B0:1F:8C:E2:14:A7 -84 2 0 0 1 130 WPA2 CCMP MGT Administrativos-UDP
B0:1F:8C:E2:14:A6 -78 3 0 0 11 130 WPA3 CCMP OWE <length: 0>
4B:03:13:31:89:09 -86 2 0 0 0 130 WPA2 CCMP PSK VTR-207881
14:51:28:57:6C:ED -84 3 1 0 0 270 WPA2 CCMP PSK SoftS22
BA:0B:18:C6:83:E9 -79 7 0 0 10 130 WPA2 CCMP PSK ZTE-23081F
7C:00:AD:97:8A:74 -85 18 1 0 1 360 WPA2 CCMP PSK <length: 0>
B0:1F:8C:E2:14:A4 -73 3 0 0 1 130 WPA3 CCMP OWE <length: 0>

BSSID STATION PWR Rate Lost Frames Notes Probes
(not associated) FB:85:4D:F2:D4:70 -38 0 - 1 0 3 Alumnos-UDP,_owetr_Alumnos-UDP1993294148
(not associated) 3E:FB:D2:96:78:EE -48 0 - 1 0 0 WFL_F30
(not associated) A2:9D:A6:89:97:0A -58 0 - 1 0 3
(not associated) 92:EE:DC:8F:48:89 -61 0 - 1 0 1
(not associated) BA:0F:7B:38:1B:1C2 -64 0 - 5 0 3 _owetr_Alumnos-UDP1993294148

```

Figura 1: Lista de redes escuchadas.

```

B0:48:7A:D2:DD:74 -55 242 5005 0 8 54e WEP WEP WEP

```

Figura 2: Identificación de red del informante.

En la figura 2 se observa que se ha logrado identificar la red del informante, la cual destaca del resto por ser la única red wi-fi de cifrado tipo WEP. Esto quiere decir que cifra el tráfico con claves hexadecimales de 64 o 128 bits.

### 2.2. Explica matemáticamente porqué se requieren más de 5000 paquetes para obtener la pass

### 2.3. Obtiene la password con ataque por defecto de aircrack-ng

```

Attack will be restarted every 5000 captured Ivs.

Aircrack-ng 1.6

[00:02:22] Tested 10523 keys (got 15027 Ivs)
Got 15027 out of 15000 Invistarting PTW attack with 15027 Ivs.

KB depth byte(vote)
0 0/ 3 32(28642) 16(23048) C9(21248) 66(19968) E1(19968) 08(19456) 83(19200) 38(18944) ED(18944) 20(18688) 14(18432) 30(18432) 61(18432) 25(18176) 26(18176) 03(18176)
1 1/ 1 12(18048) 46(16888) 02(16888) 01(16888) 04(16888) 7B(16432) 7F(16432) A1(16432) D1(16432) 23(16432) 06(16176) 9A(16176) F5(16176) 07(15920) C1(15720)
2 2/ 29 56(19456) 24(19456) 91(19200) 97(19200) 66(19200) 21(19200) AB(18944) 66(18944) A6(18688) D3(18688) DE(18688) BE(18432) 39(18432) 68(18176) 2E(18176) 45(18176)
4 4/ 10 38(18096) 72(16488) AB(15712) 21(15720) AB(15720) 31(15720) 04(15944) AC(15944) 2B(15432) 3F(15432) 0E(15432) 9A(15176) 0E(15176) 87(15176)
4 4/ 1 06(14576) 97(11768) 47(20488) 98(20488) C2(20224) 91(19968) 37(19712) 6C(19456) 12(19200) A6(19200) A7(19200) C0(19200) F8(19200) 86(18944) 86(18688) BA(18688)

KEY FOUND! [ 12:34:56:78:90 ]
Decrypted correctly: 100%

```

Figura 3: Ataque de aircrack en funcionamiento.

En la figura 3 se puede observar que aircrack-ng está realizando el ataque a la vez que se escuchan los canales y se captura tráfico con airodump-ng. Se indica que cada 5000 IVs capturados se reinicia el ataque.



Figura 4: Llave encontrada.

En la figura 4 la llave fue encontrada, después de los 15000 IVs. Esta corresponde a **12:34:56:78:90**.

## 2.4. Indica el tiempo que demoró en obtener la password

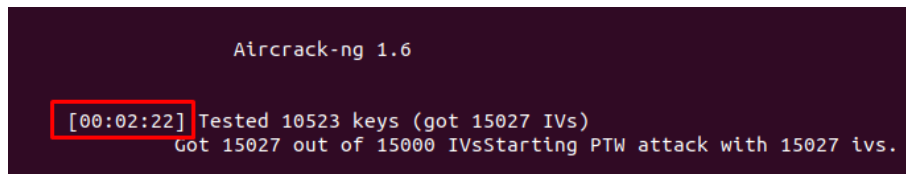


Figura 5: Tiempo que demoró el ataque realizado.

De la figura 3 se puede analizar cierta información, como el tiempo que tomó el ataque para encontrar la password y los IVs obtenidos. En la figura 5 se destaca el tiempo en una casilla roja, donde se indica que el ataque demoró **2 minutos y 22 segundos**.

## 2.5. Descifra el contenido capturado

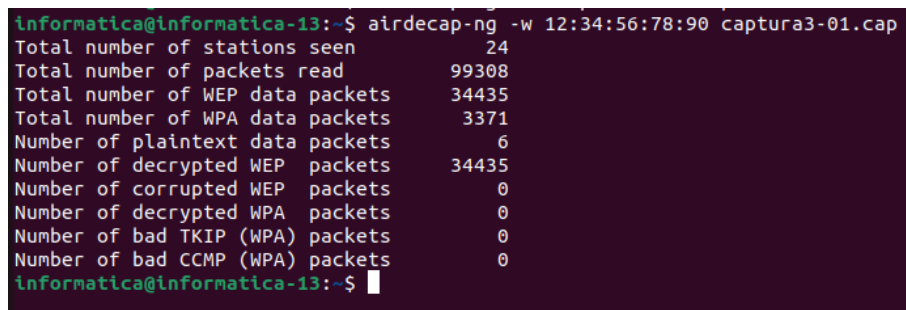


Figura 6: Comando utilizado para descifrar el contenido de la captura.

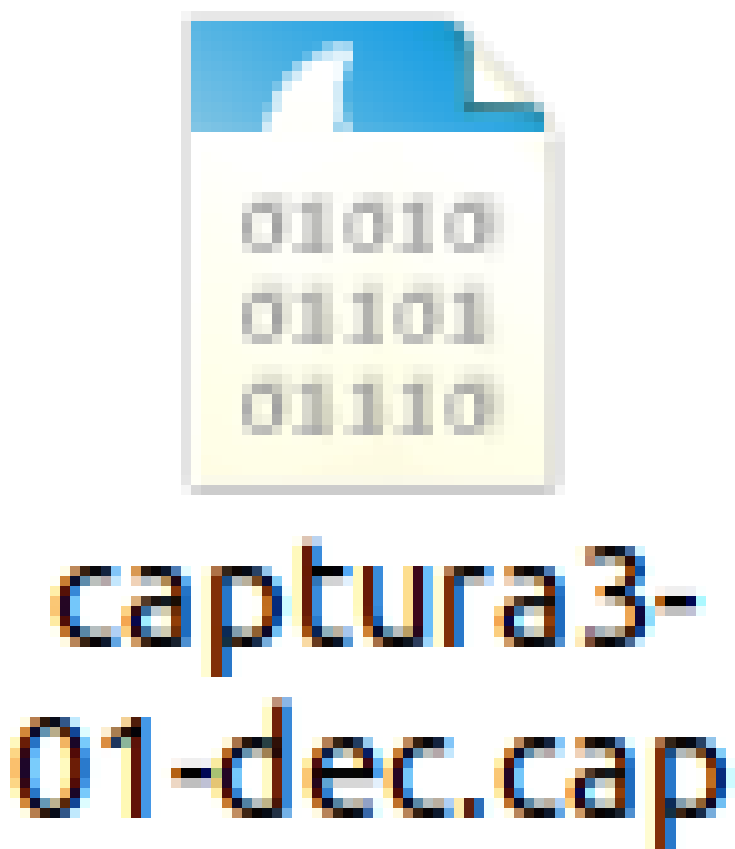


Figura 7: Archivo creado al descifrar la captura con airdecap-ng.

Haciendo uso de la llave obtenida mediante el ataque se descifra la captura realizada, para encontrar el contenido transmitido por el informante. El procedimiento se puede observar en la figura 6. En la figura 7 se muestra la creación de un archivo que representa la captura descifrada.

## 2.6 Describe como obtiene la url de donde descargar el archivo DESARROLLO (PASO 2)

### 2.6. Describe como obtiene la url de donde descargar el archivo

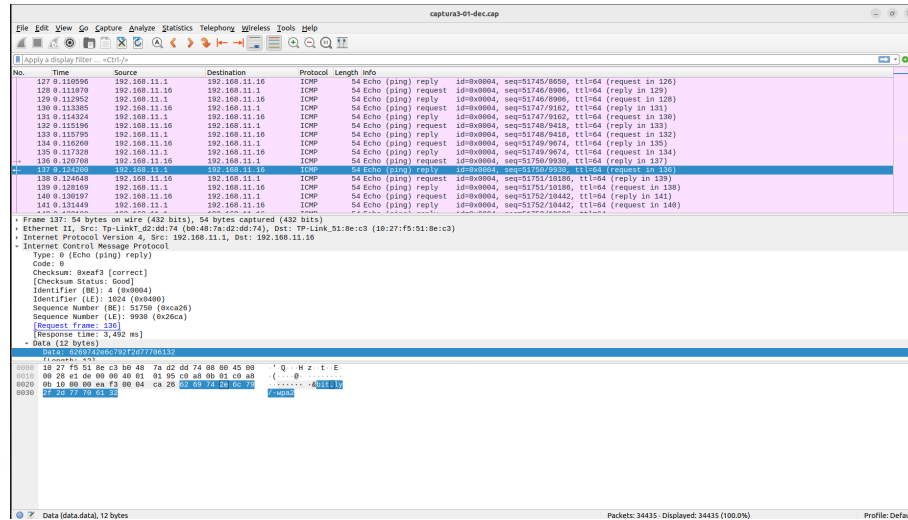


Figura 8: Captura descifrada analizado en Wireshark.

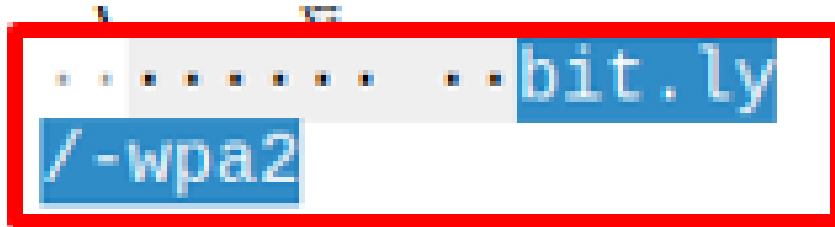


Figura 9: Link del informante.

El archivo de la captura descifrada es abierto en Wireshark para su análisis tal como en la figura 8. Si se analizan los campos y la data de los paquetes transmitidos por la red WEP del informante se logra identificar el contenido que quería transmitirnos, el cual corresponde a un link. El link se puede observar en la figura 9.

## 3. Desarrollo (PASO 2)

### 3.1. Script para modificar diccionario original

```
prime@ubuntu:~/Documents/lab3cripto$ sed 's/^(.\\)/\\U\\1/' rockyou.txt > rockyou_mod.dic
prime@ubuntu:~/Documents/lab3cripto$ vim rockyou_mod.dic
prime@ubuntu:~/Documents/lab3cripto$
```

Figura 10: Script utilizado para agregar letra capital.

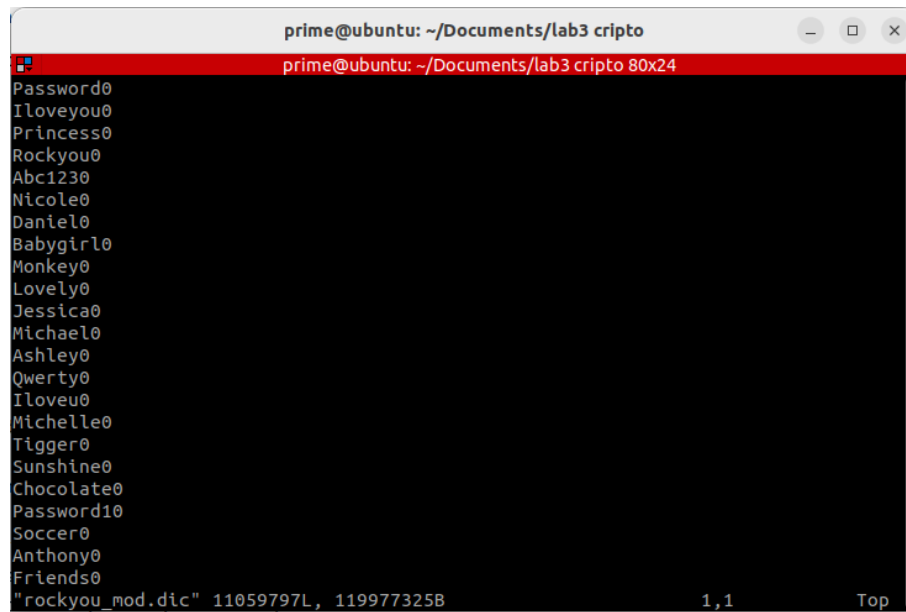
### 3.2 Cantidad de passwords finales que contiene rockyou\_mod.dic (PASO 2)

```
prime@ubuntu:~/Documents/lab3 cripto$ sed -i 's/$/0/' rockyou_mod.d
```

Figura 11: Script utilizado para agregar un 0 al final.

```
prime@ubuntu:~/Documents/lab3 cripto$ sed -i '/^[0-9]/d' rockyou_mod.dic
```

Figura 12: Script utilizado para eliminar las líneas con números al comienzo.



```
prime@ubuntu: ~/Documents/lab3 cripto
prime@ubuntu: ~/Documents/lab3 cripto 80x24
Password0
Iloveyou0
Princess0
Rockyou0
Abc1230
Nicole0
Daniel0
Babygirl0
Monkey0
Lovely0
Jessica0
Michael0
Ashley0
Qwerty0
Iloveu0
Michelle0
Tigger0
Sunshine0
Chocolate0
Password10
Soccer0
Anthony0
Friends0
"rockyou_mod.dic" 11059797L, 119977325B 1,1 Top
```

Figura 13: Nuevo diccionario modificado.

En las figuras 10-12 se pueden observar los scripts para agregar letra capital al comienzo de cada línea, para agregar un 0 al final, y para eliminar las líneas que comenzaran con números, respectivamente. En la figura 13 se logra observar el resultado, el cual es guardado en un nuevo diccionario llamado **rockyou-mod.dic**

### 3.2. Cantidad de passwords finales que contiene rockyou\_mod.dic

```
prime@ubuntu:~/Documents/lab3 cripto$ wc -l rockyou_mod.dic
11059797 rockyou_mod.dic
```

Figura 14: Nuevo diccionario modificado.

En la figura 14 se muestra el comando wordcount utilizado para enumerar la cantidad de contraseñas que existen en el diccionario a utilizar, las cuales son 11059797.

## 4. Desarrollo (Paso 3)

- 4.1. Obtiene contraseña con hashcat con potfile
- 4.2. Nomenclatura del output
- 4.3. Obtiene contraseña con hashcat sin potfile
- 4.4. Nomenclatura del output
- 4.5. Obtiene contraseña con aircrack-ng

```
prime@ubuntu:~/Documents/lab3 cripto$ aircrack-ng -w rockyou_mod.dic handshake.pcap
Reading packets, please wait...
Opening handshake.pcap
Read 13 packets.

# BSSID          ESSID          Encryption
1 B0:48:7A:D2:DC:18 VTR-1645213    WPA (1 handshake)

Choosing first network as target.
Reading packets, please wait...
Opening handshake.pcap
Read 13 packets.

1 potential targets
```

Figura 15: Descifrado con aircrack-ng.

```
Aircrack-ng 1.6

[00:00:05] 2917/11059797 keys tested (612.49 k/s)

Time left: 5 hours, 52 seconds                                0.03%

KEY FOUND! [ Security0 ]

Master Key      : 55 E1 E0 F0 8E D7 53 80 F6 27 C6 DC 48 20 74 54
                  B7 54 98 37 71 FF C8 03 1D 89 C5 19 8D 6F AC 76

Transient Key   : 3C 1B 89 A6 31 30 BA 04 B6 59 D9 7E 65 BD D2 07
                  9E C6 8D 2A D6 EF 7F 9E A1 95 1C BC CC 62 A6 5D
                  CC 07 B2 E3 9D 12 99 A7 66 D4 12 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 18 13 AC B9 76 74 1B 44 6D 43 36 9F B9 6D BF 90
```

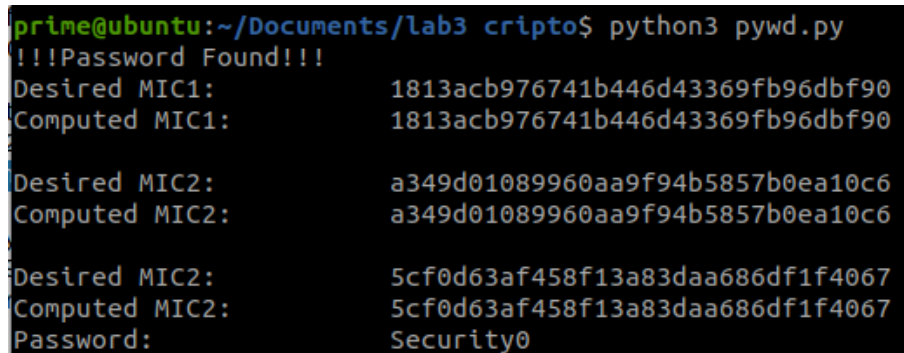
Figura 16: Descifrado con aircrack-ng.

En las figura 14 y 15 se evidencia el uso de aircrack-ng para descifrar la contraseña de la captura descargada utilizando aircrack-ng y el diccionario. El resultado es **Security0**





## 4.7. Obtiene contraseña con pycrack



```
prime@ubuntu:~/Documents/lab3 cripto$ python3 pywd.py
!!!Password Found!!!
Desired MIC1:      1813acb976741b446d43369fb96dbf90
Computed MIC1:     1813acb976741b446d43369fb96dbf90

Desired MIC2:      a349d01089960aa9f94b5857b0ea10c6
Computed MIC2:     a349d01089960aa9f94b5857b0ea10c6

Desired MIC2:      5cf0d63af458f13a83daa686df1f4067
Computed MIC2:     5cf0d63af458f13a83daa686df1f4067
Password:          Security0
```

Figura 21: Contraseña obtenida con pycrack.

En la figura 18 se puede observar que el ataque pycrack fue exitoso, dando como resultado la contraseña **Security0**

## Conclusiones y comentarios

### Issues