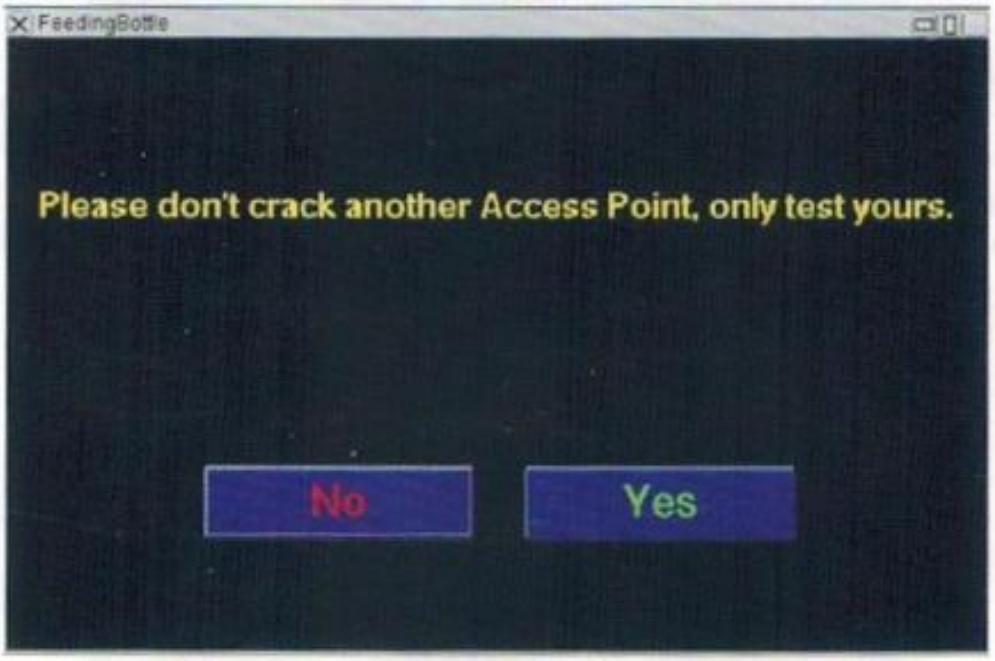
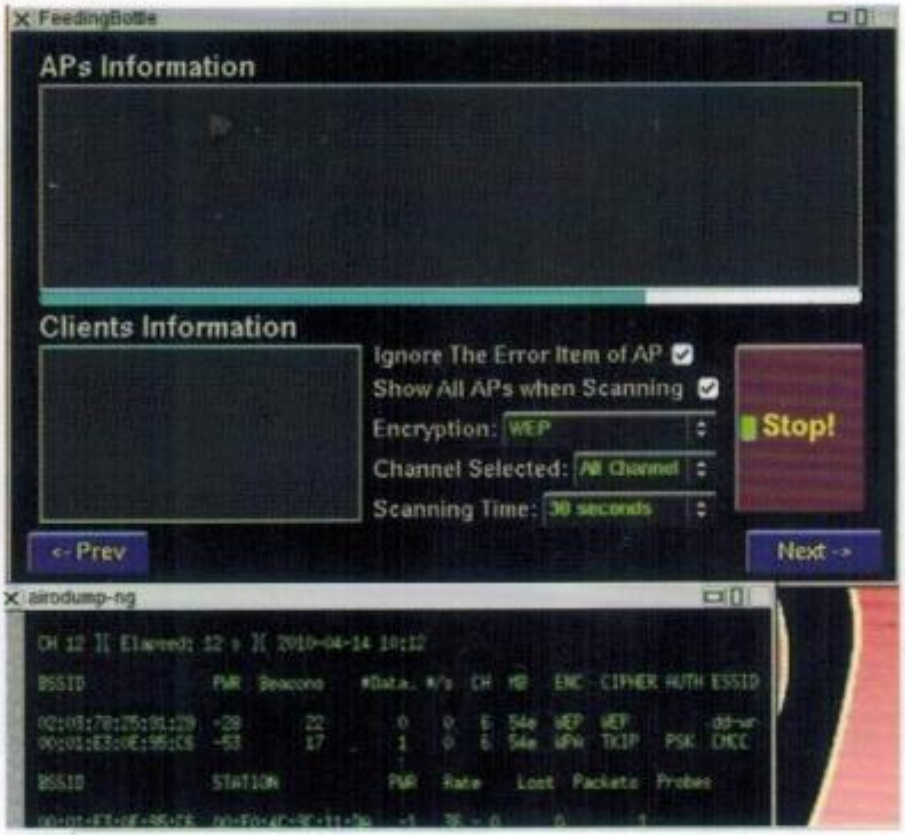
Manual para auditorías con Beini

1. Arrancar la distribución de Beini desde el cd, recuerda que para esta opción debes tener las bios del pc preparadas para que arranque desde la unidad de cd/dvd. Espera 10 segundos, cuando aparezca el escritorio del Beini tienes que hacer click encima dei icono delprograma FeedingBottle 3.0 Final (es el icono con forma de biberón).

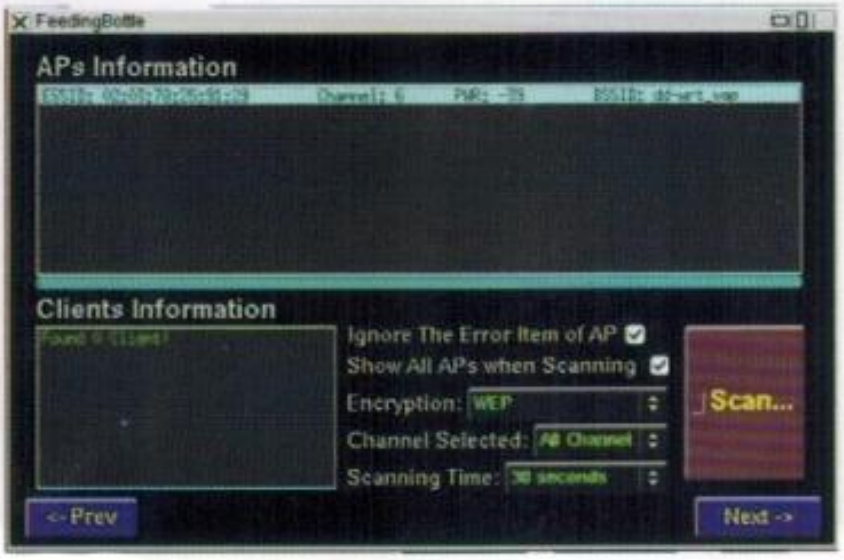
2. Una vez iniciado te indicara que uses solo el programa para realizar auditorias de tus propias redes, elegimos "YES" para continuar.



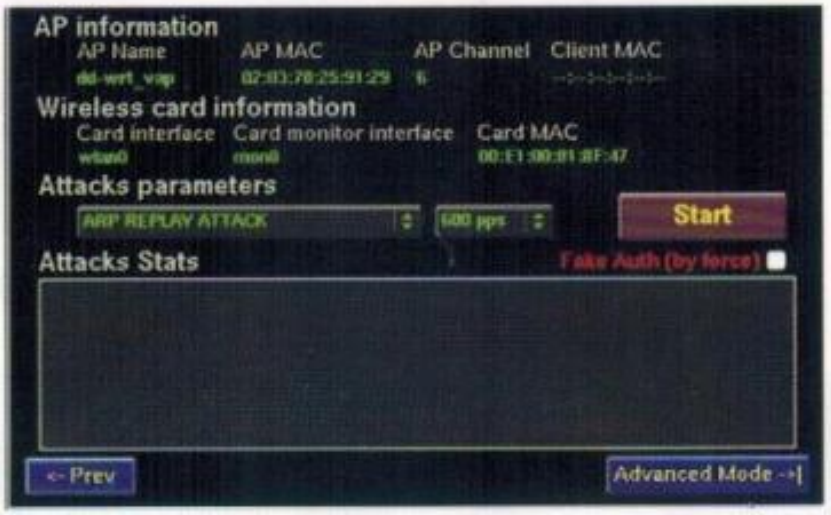
3. Elegir tu tarjeta de red inalómbrica, espera a que te salga el mensaje



5. Después de los 30 segundos, en la parte superior te aparecern todas las redes que se han detectado, selecciona la red a la cual quieres realizar la auditoría (aquella que tenga un valor de power más alto será la que esta más cerca y por tanto las mas óptima para averiguar la clave). Pulsa "Next" para continuar.

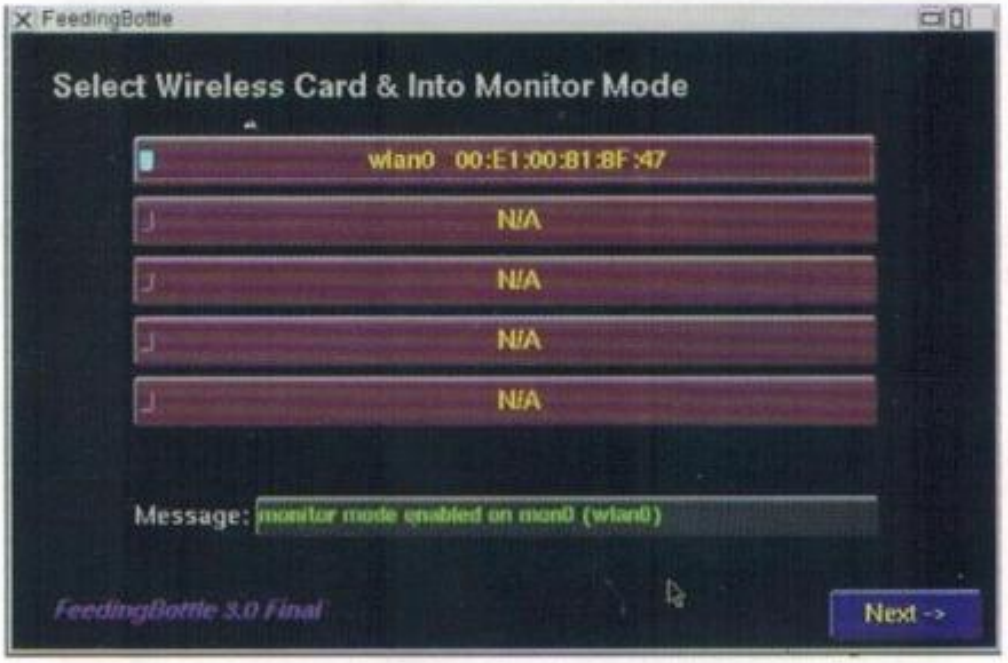
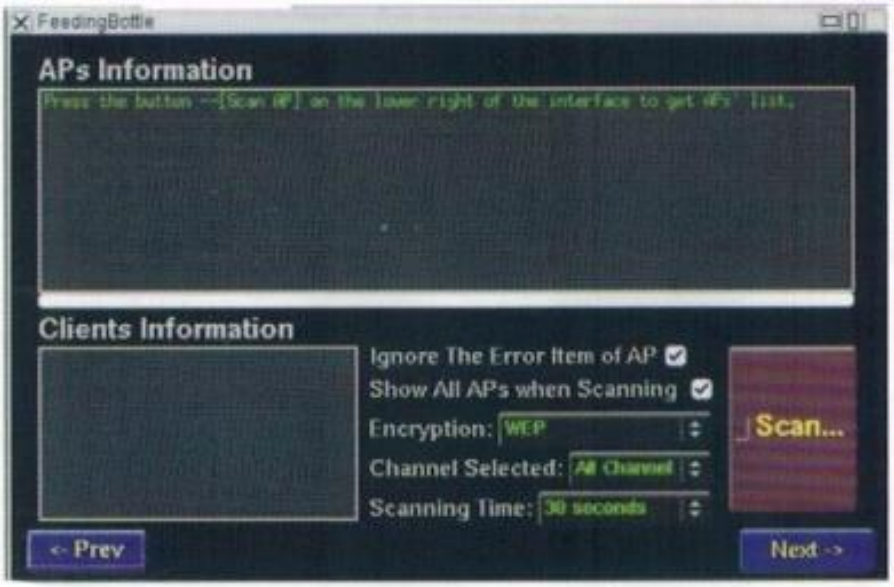


6. Elige en "Attack parameters" la opción "ARP REPLAY ATTACK" (puedes elegir otro método de ataque para averiguar la clave, no obstante es la que viene por defecto y es bastante efecticaz). Haz click en "Start" para empezar la auditoría. De acuerdo con los usurios el Beini, las auditorias se realizan más rápidas si existen varios clientes que esten usando la red, por eso siempre se recomienda que se realice la auditoría de la red que se este usando por otros clientes.
Además puedes usar la opción de "Advanced Mode" si tienes conocimientos de auditorías, el cual te permite ampliar las opciones de la misma, así como crear clientes falsos para una mayor rapidez a la hora de realizar la misma.



7. Una vez el programa haya capturado un numero de paquetes necesarios desencriptara la red y te dará la clave en la parte inferior: "Key Found"

de "monitor mode enable on mon0 (wlan0)" y pulsar en "NEXT" para continuar.



4. En esta pantalla deberás colocar las siguientes opciones:
Encryption: WEP (el programa solo puede comprobar las clave wep)
Channel Selected: All Channel (para que te busque todos los canales que se encuentre dentro de tu posición)
Scannig Time: 30 seconds (es el tiempo que estará buscando redes)
Una vez introducidas pulsar "Scan..." para empezar a buscar.