

# DECT Sniffing Dedected

## Desde BackTrack Linux

[Whitepaper Gratis](#)

[www.sourcefire.com/agile](http://www.sourcefire.com/agile)

12 Principios Básicos para la Seguridad Para el Mundo Real.



Este artículo fue contribuido por 5M7X.

- URL: <http://www.back-track.de/index.php?page=team> # SMTX
- Twitter: ! <http://twitter.com/> # / 5M7X
- Email: 5M7X@mail.ru

**BIG FAT HAIRY ADVERTENCIA:** . ES ILEGAL grabar conversaciones telefónicas EN MUCHOS PAÍSES  
Para obtener una lista de las leyes de privacidad estatales en los EE.UU.,

## Contenido

- 1 ¿Qué es DECT?
  - 1.1 El problema?
  - 1.2 Probado en
- 2 Instalación dedected
  - 2.1 Instalación del repositorio
  - 2.2 Instalación desde el código fuente
- 3 Instale algunas herramientas adicionales
- 4 Cargue los controladores
- 5 Analizar en busca de fijo fp partes aka (estaciones base DECT)
- 6 No haga caso de los teléfonos que no quieren oler (por ejemplo, sus vecinos!)
- 7 Grabe la llamada telefónica
- 8 Decodificar la llamada de la corriente de datos
- 9 Importe los arroyos en audacia y escuchar las llamadas
- 10 Limpiar / Recargar
- 11 DECT protocolo
- 12 Vídeo: Sniffing teléfonos DECT con BackTrack 5

## ¿Qué es DECT?

[http://en.wikipedia.org/wiki/Digital\\_Enhanced\\_Cordless\\_Telecommunications](http://en.wikipedia.org/wiki/Digital_Enhanced_Cordless_Telecommunications)

## El problema?

La mayoría de los vendedores no implementar el cifrado en sus dispositivos, de forma que uno puede olerlo con det

hardware y software.

Para un post anterior sobre el tema, consulte: <http://www.offensive-security.com/backtrack/sniffing-dect-phones>

## Probado en

- BackTrack 5 KDE último kernel 2.6.38 con x86
- Original Dosch y Amand Tipo II PCMCIA Card
- SIEMENS C1 Teléfonos DECT configurado en modo repetidor

**NOTA:** Este es un programa experimental que no está muy apoyado activamente más!

## Instalación dedected

Con el fin de obtener dedected instalado en BackTrack, usted tiene las siguientes opciones:

1. Utilice dedected de los BackTrack 5 repositorios.
2. Compilar por su cuenta si usted quiere experimentar.

## Instalar desde repositorio

```
root @ bt: ~ # apt-get update
root @ bt: ~ # apt-get install dedected
```

## Instalación desde el código fuente

Esta etapa es opcional para aquellos que quieran construir las herramientas de código fuente.

```
root @ bt: ~ # preparan-kernel-sources
root @ bt: ~ # cd / usr / src / linux
root @ bt: ~ # cp-rf include / genera / * include / linux /
root @ bt: ~ # cd / pentest / telefonía
root @ bt: ~ # svn co https://dedected.org/svn/trunk dedected_svn
root @ bt: ~ # cd dedected_svn / com-on-linux-air_cs /
root @ bt: ~ # make && make - C herramientas
```

## Instale algunas herramientas adicionales

```
root @ bt: ~ # apt-get-y install audacia
```

## Cargue los controladores

```
root @ bt: ~ # cd / pentest / telefonía / dedected / com-on-air_cs-linux
root @ bt: ~ # hacer nodo
```

Si no ha introducido su Dosch y tipo Amand 2 o Tipo 3 o Voo: doo # PCMCIA tarjeta hágalo ahora! A continuación controlador:

```
root @ bt: ~ # make load
```

## Analizar en busca de partes fijas aka fp (estaciones base DECT)

```
root @ bt: ~ # cd / pentest / telefonía / dedected / com-on-air_cs-linux / tools
root @ bt: ~ # . / dect_cli
```

Si necesita información sobre el tipo de uso "ayuda". Si usted vive en la cerradura de EE.UU. a los EE.UU. / DECT de la "banda" de comandos. Vamos a permitir someverbosity:

```
verbo
```

Y empezará a buscar las estaciones base:

```
fpscan
```

Después de escanear 2-3 veces a través de todos los canales de desactivar la verbosidad, y detener la exploración:

```
verbo
stop
```

```
tools : dect_cli
File Edit View Bookmarks Settings Help
root@root:/pentest/telephony/dedected/com-on-air_cs-linux/tools# ./dect_cli
DECT command line interface
type "help" if you're lost
dump
### nothing found so far
verb
### verbosity turned ON
fpscan
### starting fpscan
### mode: stopped, switching to channel 9
### mode: fpscan, switching to channel 8
### found new station 01 03 b8 ea f8 on channel 8 RSSI 24
### mode: fpscan, switching to channel 7
### mode: fpscan, switching to channel 6
### mode: fpscan, switching to channel 5
### found new station 00 ba f9 95 14 on channel 5 RSSI 11
### mode: fpscan, switching to channel 4
### found new station 00 34 03 72 e8 on channel 4 RSSI 10
### mode: fpscan, switching to channel 3
### found new station 00 82 ab b0 29 on channel 3 RSSI 30 name "stallowned"
### mode: fpscan, switching to channel 2
### mode: fpscan, switching to channel 1
### found new station 01 30 95 be c0 on channel 1 RSSI 5
### mode: fpscan, switching to channel 0
verb
### verbosity turned OFF
stop
### stopping DIP
dump
### stations
01 03 b8 ea f8 ch 8 RSSI 20.60 count 10 first 1307845571 last 1307845572
00 ba f9 95 14 ch 5 RSSI 11.11 count 9 first 1307845577 last 1307845578
00 34 03 72 e8 ch 4 RSSI 10.86 count 7 first 1307845579 last 1307845580
00 82 ab b0 29 ch 3 RSSI 29.46 count 13 first 1307845581 last 1307845582 name "stallowned"
01 30 95 be c0 ch 1 RSSI 5.50 count 2 first 1307845586 last 1307845586
### calls
name 00 82 ab b0 29 stallowned
### named 00 82 ab b0 29 as stallowned
### renaming station stallowned
```

**No haga caso de los teléfonos que no quieren oler (por ejemplo, sus vecino**

Iniciar un callscan

```
callscan
```

Ahora toma el teléfono DECT y hacer una llamada de prueba y espere hasta que aparezca la llamada telefónica. Así suficiente si usted acaba de obtener un tono de marcación. Debería ver algo como

```
Llamada # # # encontrado nuevo 00 82 31 33 73 en el canal 7 RSSI 34
```

```
detener
```

El nombre de su estación base si desea:

```
Nombre 00 82 31 33 73 stallowned
```

Volcar todos los teléfonos se encuentran:

```
arrojar
```

No haga caso de todos los teléfonos excepto el suyo a través del siguiente comando! **IMPORTANTE!**

```
ignorar 01 30 95 13 37
```

## Grabe la llamada telefónica

Comience automáticamente registro de cada llamada telefónica que detecta:

```
AUTOREC
```

Ahora toma el teléfono telefonía DECT y hacer una Llamada prueba. Recomendando llamar un "servicio tiempo diciendo llegar a través de un número de teléfono normal. Usted debe obtener algo como esto:

```
# # # A partir AUTOREC
# # # Parando DIP
# # # A partir callscan
# # # Intentando sincronizar en ab b0 00 82 29
# # # Tiene sincronización
# # # Dumping dump_2011-06-11_21_37_37_RFPI_00_82_ab_b0_29.pcap
# # # Parando DIP
```

Después de colgar tu llamada telefónica al vertimiento debería detenerse:

```
tools : dect_cli
File Edit View Bookmarks Settings Help
### verbosity turned ON
fpSCAN
### starting fpSCAN
### mode: stopped, switching to channel 9
### mode: fpSCAN, switching to channel 8
### found new station 01 03 b8 ea f8 on channel 8 RSSI 24
### mode: fpSCAN, switching to channel 7
### mode: fpSCAN, switching to channel 6
### mode: fpSCAN, switching to channel 5
### found new station 00 ba f9 95 14 on channel 5 RSSI 11
### mode: fpSCAN, switching to channel 4
### found new station 00 34 03 72 e8 on channel 4 RSSI 10
### mode: fpSCAN, switching to channel 3
### found new station 00 82 ab b0 29 on channel 3 RSSI 30 name "stallowned"
### mode: fpSCAN, switching to channel 2
### mode: fpSCAN, switching to channel 1
### found new station 01 30 95 be c0 on channel 1 RSSI 5
### mode: fpSCAN, switching to channel 0
verb
### verbosity turned OFF
stop
### stopping DIP
dump
### stations
01 03 b8 ea f8 ch 8 RSSI 20.60 count 10 first 1307845571 last 1307845572
00 ba f9 95 14 ch 5 RSSI 11.11 count 9 first 1307845577 last 1307845578
00 34 03 72 e8 ch 4 RSSI 10.86 count 7 first 1307845579 last 1307845580
00 82 ab b0 29 ch 3 RSSI 29.46 count 13 first 1307845581 last 1307845582 name "stallowned"
01 30 95 be c0 ch 1 RSSI 5.50 count 2 first 1307845586 last 1307845586
### calls
name 00 82 ab b0 29 stallowned
### named 00 82 ab b0 29 as stallowned
### renaming station stallowned
autorec
### starting autorec
### stopping DIP
### starting callscan
### found new call on 00 82 ab b0 29 on channel 1 RSSI 31
### trying to sync on 00 82 ab b0 29
### got sync
### dumping to dump_2011-06-11_22_28_44_RFPI_00_82_ab_b0_29.pcap
### stopping DIP
### starting callscan
```

## Decodificar la llamada de la corriente de datos

Detenga el AUTOREC:

```
detener
```

Decodificar el audiostream de la basura cruda

```
root @ bt: ~ # . / decode.sh
```

```

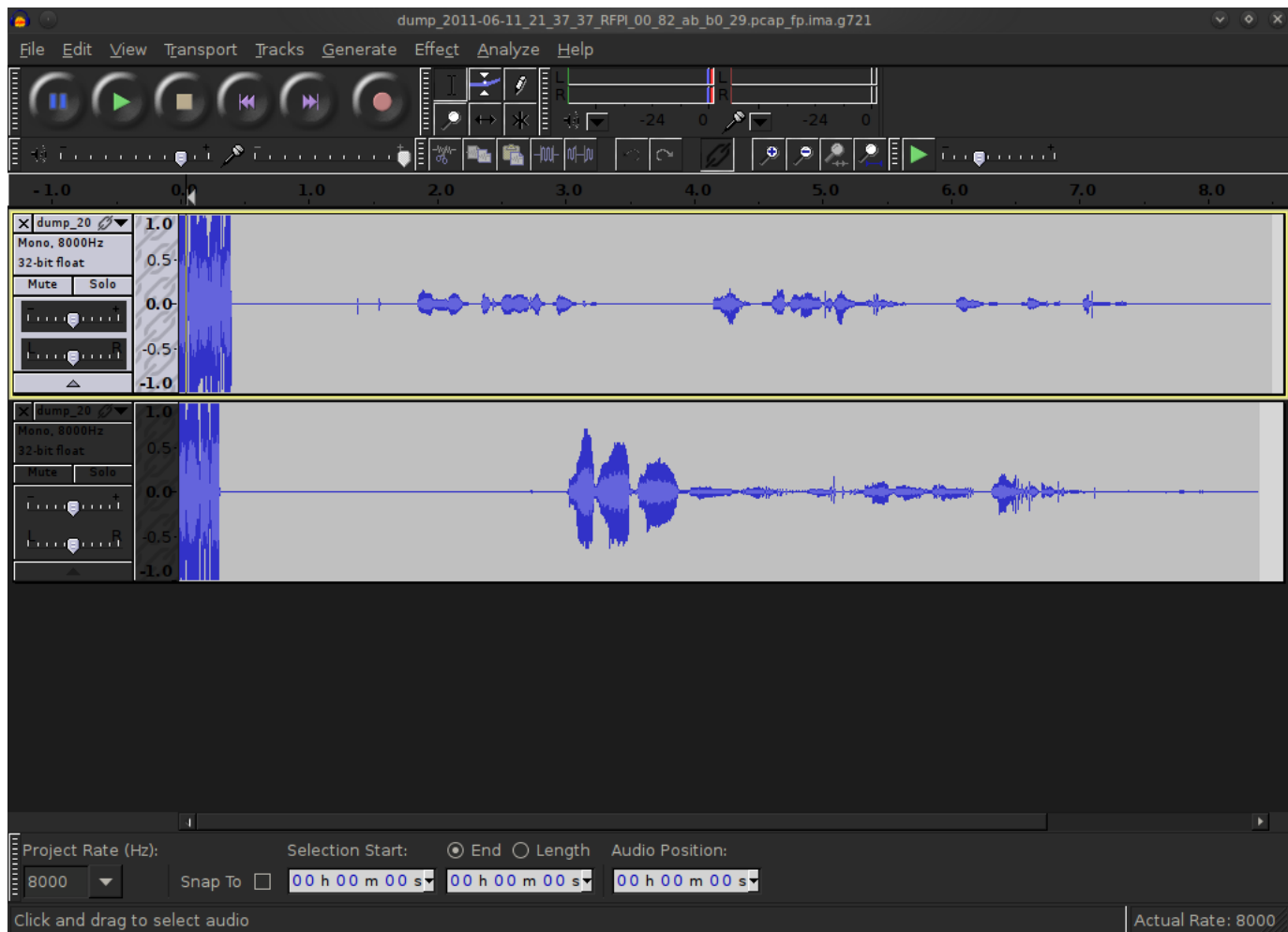
tools : bash
File Edit View Bookmarks Settings Help
### stations
01 03 b8 ea f8 ch 8 RSSI 20.60 count 10 first 1307845571 last 1307845572
00 ba f9 95 14 ch 5 RSSI 11.11 count 9 first 1307845577 last 1307845578
00 34 03 72 e8 ch 4 RSSI 10.86 count 7 first 1307845579 last 1307845580
00 82 ab b0 29 ch 3 RSSI 29.46 count 13 first 1307845581 last 1307845582 name "stallowned"
01 30 95 be c0 ch 1 RSSI 5.50 count 2 first 1307845586 last 1307845586
### calls
name 00 82 ab b0 29 stallowned
### named 00 82 ab b0 29 as stallowned
### renaming station stallowned
autorec
### starting autorec
### stopping DIP
### starting callscan
### found new call on 00 82 ab b0 29 on channel 1 RSSI 31
### trying to sync on 00 82 ab b0 29
### got sync
### dumping to dump_2011-06-11_22_28_44_RFPI_00_82_ab_b0_29.pcap
### stopping DIP
### starting callscan
stop
### stopping DIP
quit
### stations
01 03 b8 ea f8 ch 8 RSSI 20.60 count 10 first 1307845571 last 1307845572
00 ba f9 95 14 ch 5 RSSI 11.11 count 9 first 1307845577 last 1307845578
00 34 03 72 e8 ch 4 RSSI 10.86 count 7 first 1307845579 last 1307845580
00 82 ab b0 29 ch 3 RSSI 29.46 count 13 first 1307845581 last 1307845582 name "stallowned"
01 30 95 be c0 ch 1 RSSI 5.50 count 2 first 1307845586 last 1307845586
### calls
00 82 ab b0 29 ch 1 RSSI 31.43 count 3806 first 1307845723 last 1307845745
root@root:/pentest/telephony/dedected/com-on-air_cs-linux/tools# ./decode.sh
mkdir: cannot create directory `.`: File exists
libpcap version 1.0.0
pcap file version 2.4
pcap_loop() = 0
root@root:/pentest/telephony/dedected/com-on-air_cs-linux/tools# ls -lah *.wav
-rw-r--r-- 1 root root 81K 2011-06-11 22:31 dump_2011-06-11_22_28_44_RFPI_00_82_ab_b0_29.pcap_fp.ima.g721.wav
-rw-r--r-- 1 root root 162K 2011-06-11 22:31 dump_2011-06-11_22_28_44_RFPI_00_82_ab_b0_29.pcap_fp.ima.g726.L.wav
-rw-r--r-- 1 root root 162K 2011-06-11 22:31 dump_2011-06-11_22_28_44_RFPI_00_82_ab_b0_29.pcap_fp.ima.g726.R.wav
-rw-r--r-- 1 root root 80K 2011-06-11 22:31 dump_2011-06-11_22_28_44_RFPI_00_82_ab_b0_29.pcap_pp.ima.g721.wav
-rw-r--r-- 1 root root 159K 2011-06-11 22:31 dump_2011-06-11_22_28_44_RFPI_00_82_ab_b0_29.pcap_pp.ima.g726.L.wav
-rw-r--r-- 1 root root 159K 2011-06-11 22:31 dump_2011-06-11_22_28_44_RFPI_00_82_ab_b0_29.pcap_pp.ima.g726.R.wav
root@root:/pentest/telephony/dedected/com-on-air_cs-linux/tools#

```

## Importe los arroyos en audacia y escuchar las llamadas

Comience audacia a través de "alt + f2" y escriba "audacia" y pulse Enter. Importe las partes fijas y portátiles hte-p-wav / pentest / telefonía / dedected / com-on-air\_cs-linux / tools través de Archivo -> Importar -> Audio o simplern + I". Importar los archivos que terminan en. Pcap\_fp.ima.g721.wav y pcap\_pp.ima.g721.wav..

Juega tu llamada telefónica con el botón de reproducción:



Sugerencia: si sólo se puede oír el ruido del teléfono parece utilizar algunos de codificación / cifrado. Puede activar repetidor en su teléfono por lo que deshabilita el cifrado y se puede probar si su configuración está funcionando correctamente.

## Limpiar / Recargar

Si tiene que volver a cargar los controladores

```
root @ bt: ~ # cd / pentest / telefonía / dedected / com-on-air_cs-linux
root @ bt: ~ # hacer reload
```

Si ha terminado y desea limpiar:

```
root @ bt: ~ # cd / pentest / telefonía / dedected / com-on-air_cs-linux
root @ bt: ~ # hacer descargar
root @ bt: ~ # rm / dev / coa
```

## Protocolo DECT

Si usted está interesado en más detalles del protocolo, puede abrir el archivo pcap en Wireshark.:



The image shows a Wireshark capture of DECT traffic. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, and Info. The bottom pane shows the details of the selected packet (No. 29), including Slot, Frame#, RSSI, Preamble, Packet-Type, and a hex dump of the data.

No.	Time	Source	Destination	Protocol	Info
23	0.000085	00:00:00_00:00:00	00:00:00_00:00:00	DECT PP	Use Custom Columns for Infos
24	0.000088	00:00:00_00:00:00	00:00:00_00:00:00	DECT RFP	Use Custom Columns for Infos
25	0.000092	00:00:00_00:00:00	00:00:00_00:00:00	DECT PP	Use Custom Columns for Infos
26	0.000096	00:00:00_00:00:00	00:00:00_00:00:00	DECT RFP	Use Custom Columns for Infos
27	0.000100	00:00:00_00:00:00	00:00:00_00:00:00	DECT PP	Use Custom Columns for Infos
28	0.000103	00:00:00_00:00:00	00:00:00_00:00:00	DECT RFP	Use Custom Columns for Infos
29	0.000107	00:00:00_00:00:00	00:00:00_00:00:00	DECT PP	Use Custom Columns for Infos
30	0.000111	00:00:00_00:00:00	00:00:00_00:00:00	DECT RFP	Use Custom Columns for Infos
31	0.000114	00:00:00_00:00:00	00:00:00_00:00:00	DECT PP	Use Custom Columns for Infos
32	0.000118	00:00:00_00:00:00	00:00:00_00:00:00	DECT RFP	Use Custom Columns for Infos
33	0.000122	00:00:00_00:00:00	00:00:00_00:00:00	DECT PP	Use Custom Columns for Infos
34	0.000125	00:00:00_00:00:00	00:00:00_00:00:00	DECT RFP	Use Custom Columns for Infos

Details of packet 29:

- Slot: 12
- Frame#: 2
- RSSI: 33
- Preamble: 555555
- Packet-Type: 1675 Phone Packet
- Columns
- A-Field: 610082abb0290000
- B-Field: 95932226598e366fbed6eddc191876bb90d1367963e88e4...
- Full Slot (320 bit data, 4 bit xcrc)
- Descrambled Data
- No X-CRC logged (Calc:40)

Hex dump:

```

0020 00 95 93 22 26 59 8e 36 6f be d6 ed dc b1 91 87  ..."&Y.6 o.....
0030 6b b9 0d 13 67 96 3e 88 e4 3c 6c 2c f5 da f8 7b  k...g.>. .<l,...{
0040 a5 bd d1 e6 77 61 06 6f 4e  ...wa.o N

```

## Video: Sniffing teléfonos DECT con BackTrack 5

Oler los teléfonos DECT con BackTrack desde SMTX .

Obtenido de " [http://www.backtrack-linux.org/wiki/index.php/DECT\\_Sniffing\\_Dedected](http://www.backtrack-linux.org/wiki/index.php/DECT_Sniffing_Dedected) "

**Network Monitoring**

[www.gigamon.com](http://www.gigamon.com)

See More of Your Network with Existing Network Security Tools



AdChoices

Esta página fue modificada por última vez el 15 de junio de 2011, a las 20:18.