DECT Sniffing Dedected

Desde BackTrack Linux

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

¿Qué es DECT?

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 / telefonia / 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:

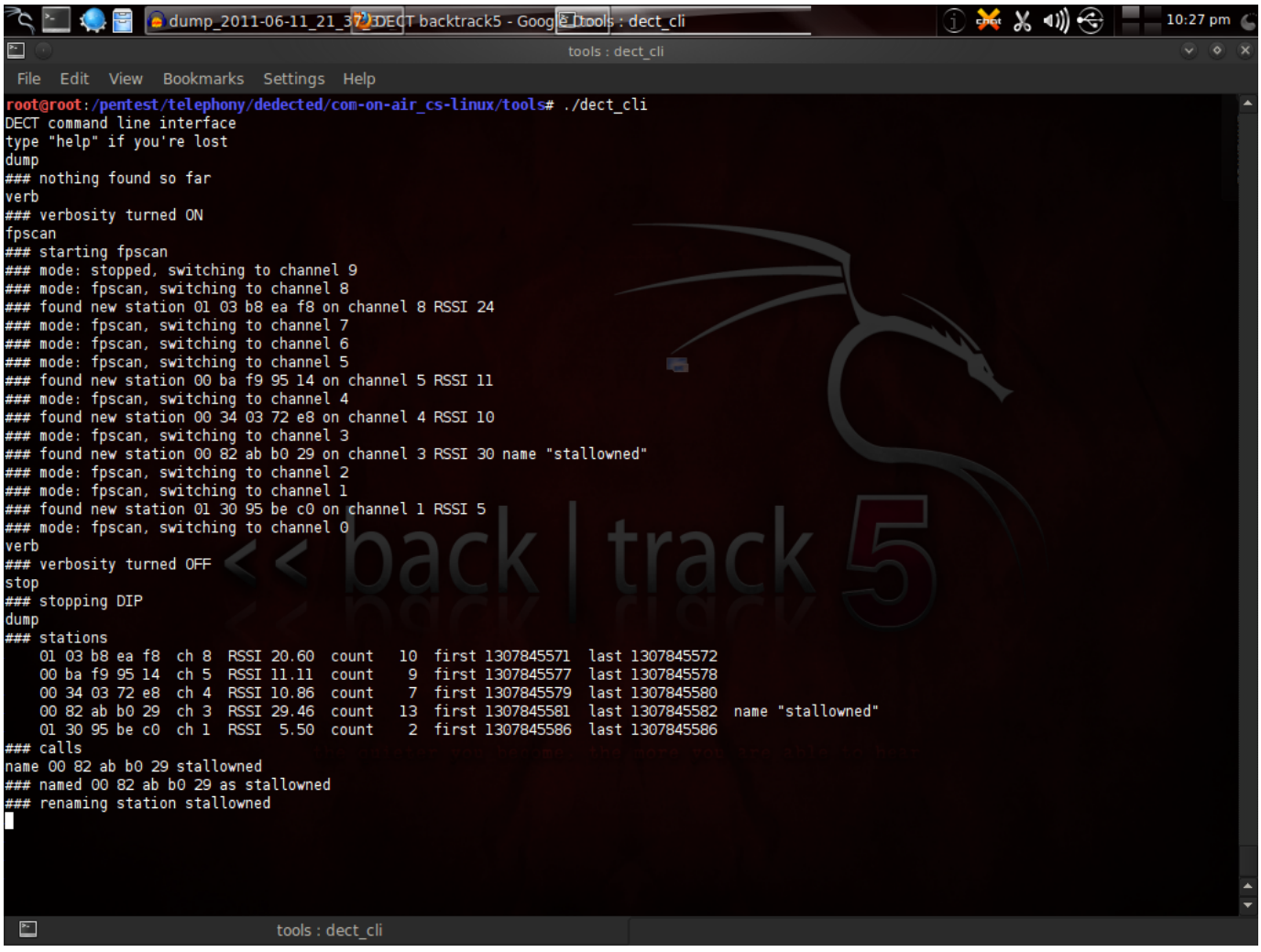
```
verbo
```

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
```



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. As 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

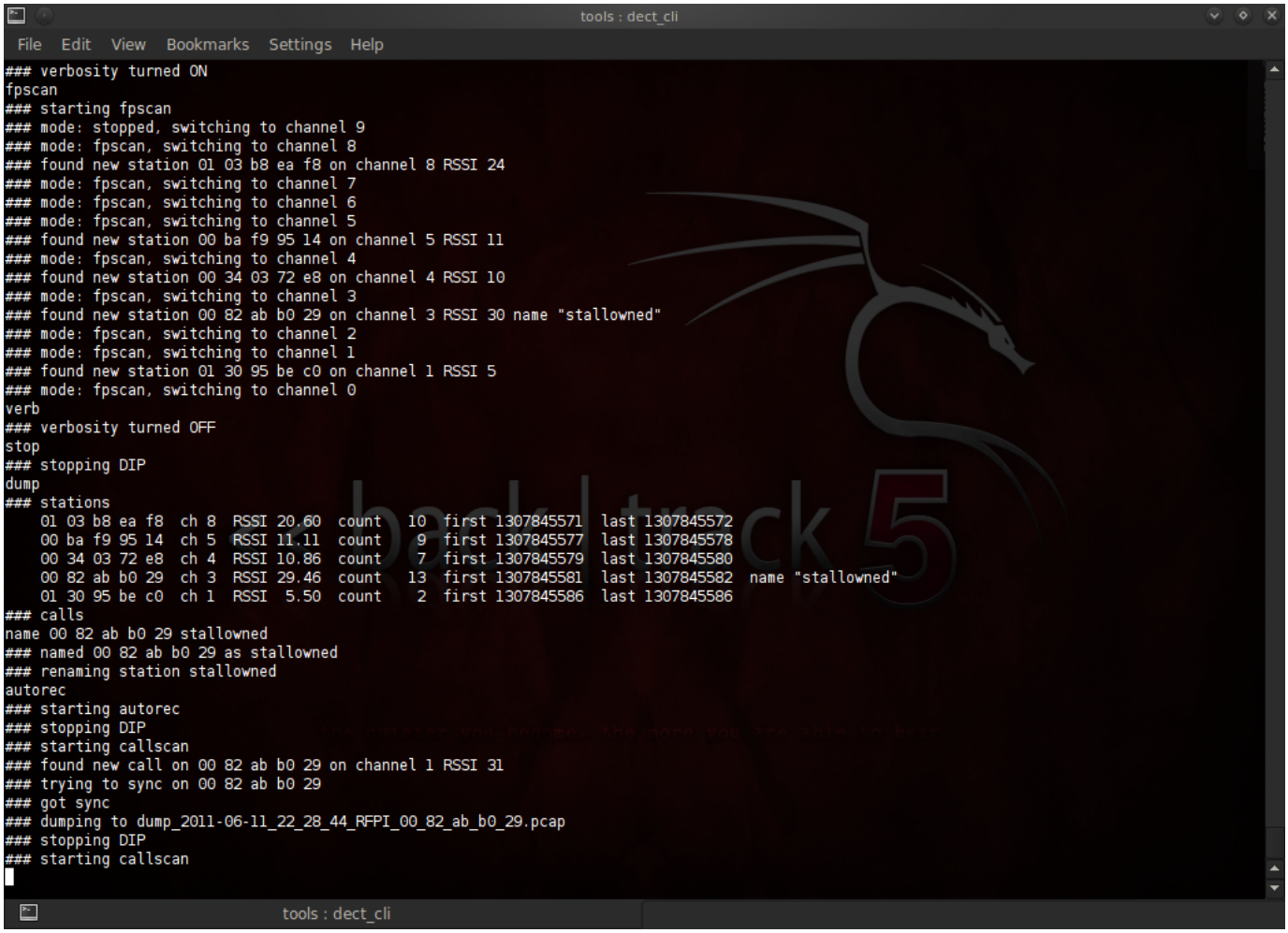
Comience automaticially registro de cada llamada telefónica que detecta:

```
AUTOREC
```

Ahora toma el teléfono telefonía DECT y hacer una Llamada prueba. Recomiendo llamar un "serivce tiempo dicien 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:



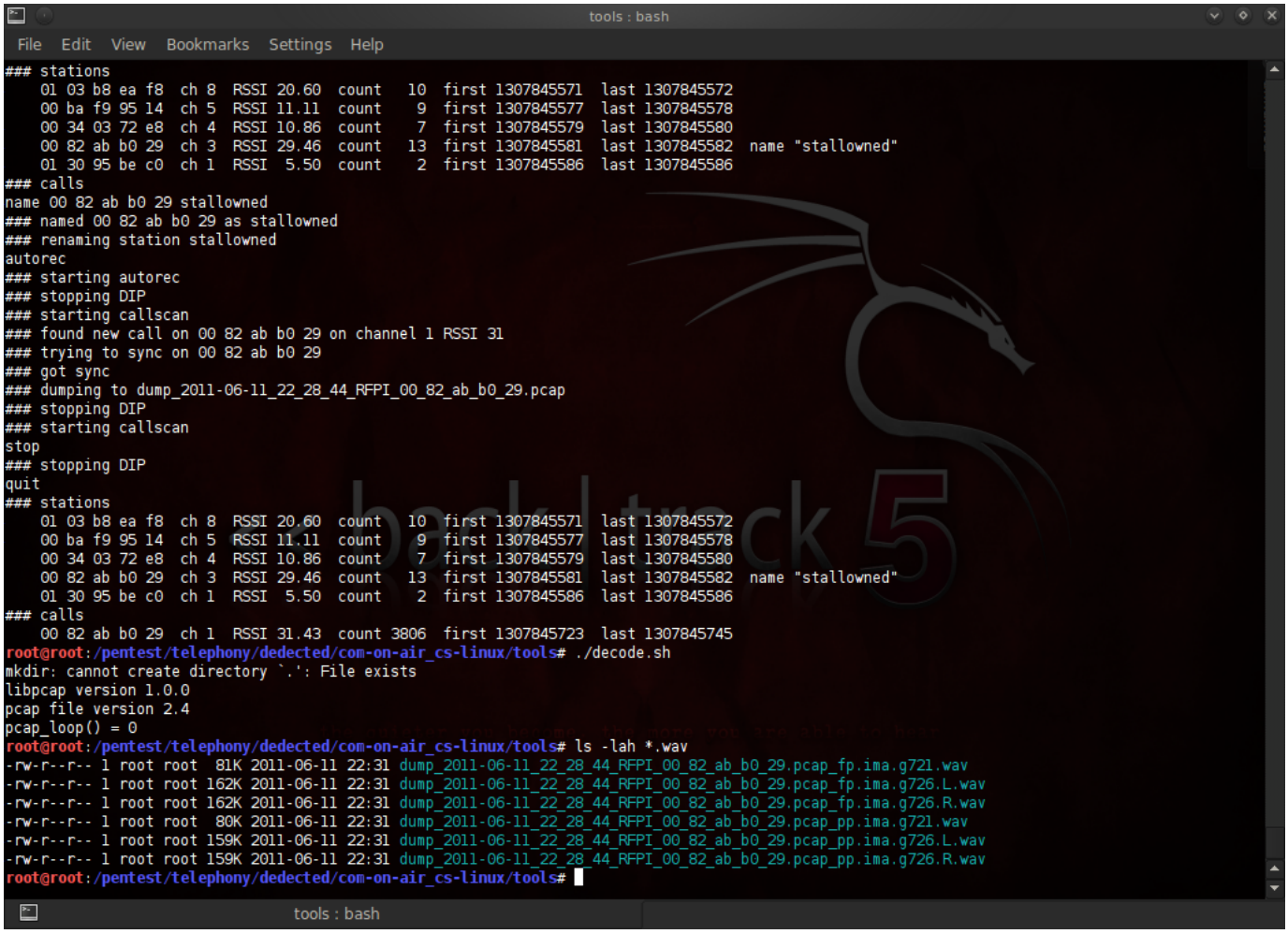
Decodificar la llamada de la corriente de datos

Detenga el AUTOREC:

```
detener
```

Decodificar el audiostream de la basura cruda

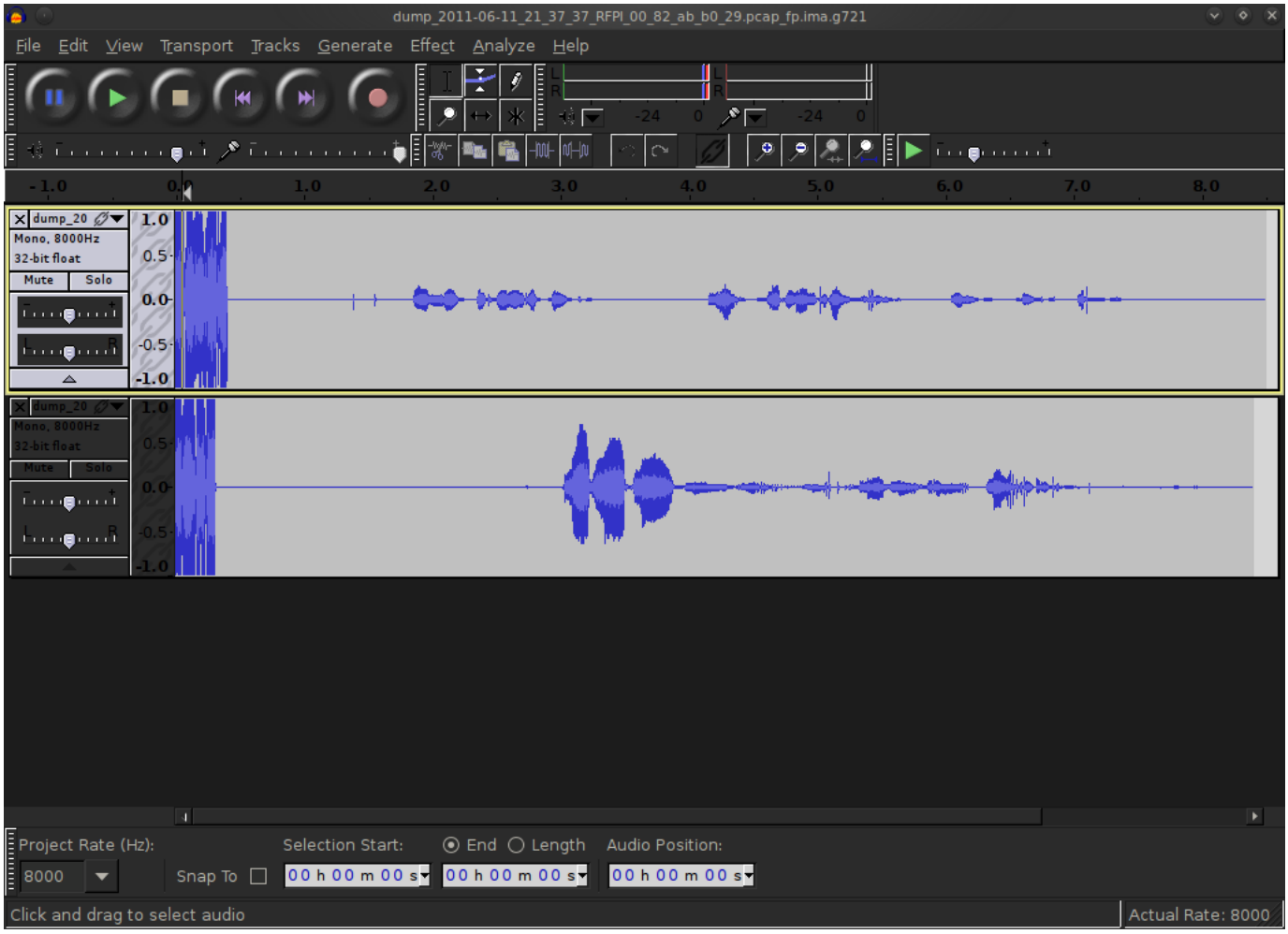
```
root @ bt: ~ # . / decode.sh
```



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 simplem + 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 cor

Limpiar / Recargar

Si tiene que volver a cargar los controladores

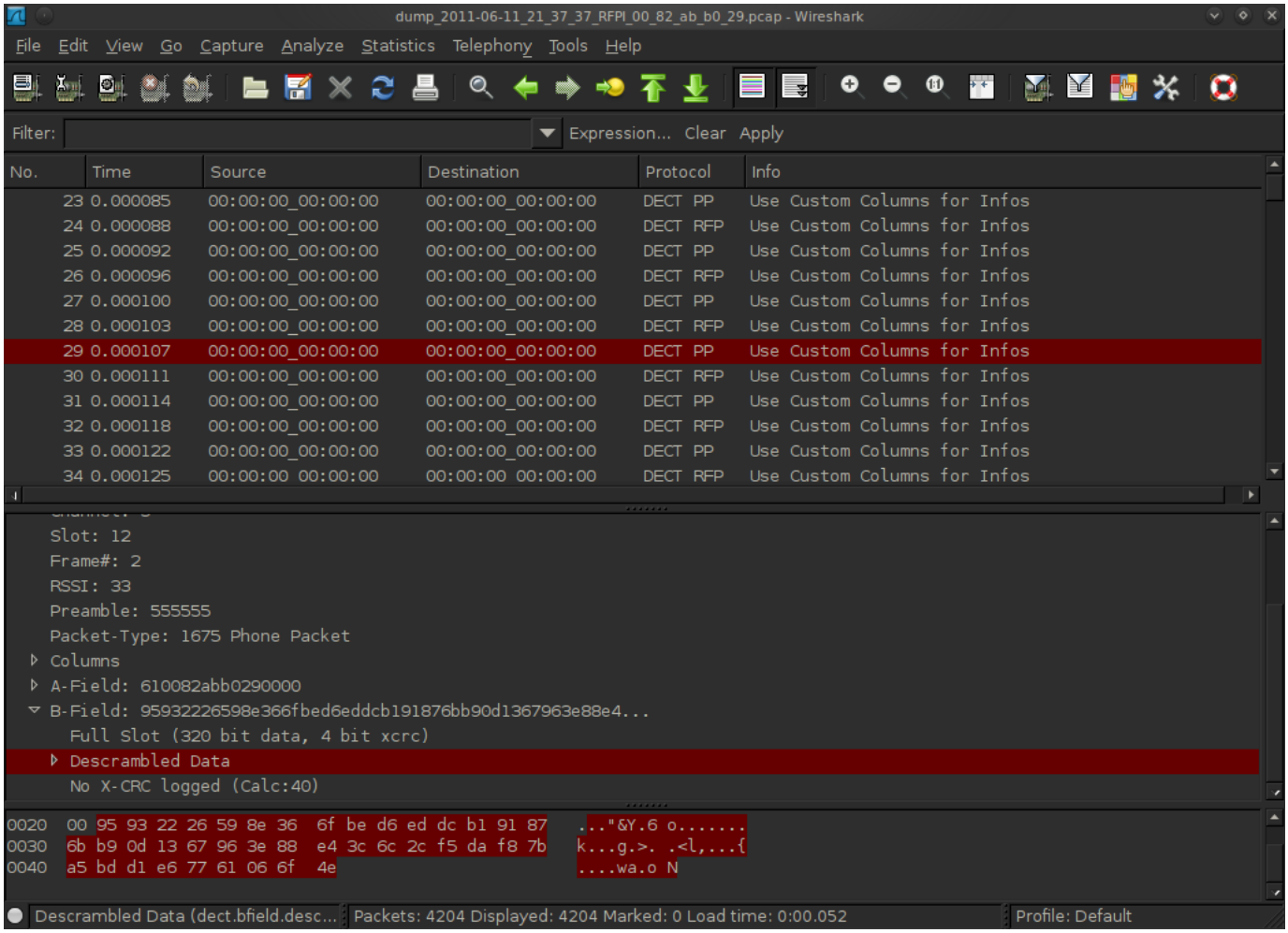
```
root @ bt: ~ # cd / pentest / telefonia / dedected / com-on-air_cs-linux
root @ bt: ~ # hacer reload
```

Si ha terminado y desea limpiar:

```
root @ bt: ~ # cd / pentest / telefonia / 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.:



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** "

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