# La Casa de Papel. Episodio 3.

Con todo el dinero robado, necesitamos escapar dando una distracción a la policía. Para ello, hace falta encontrar la bomba programada en el firmware del sistema informático. Una vez resuelta, podremos acceder al servidor, donde tras buscar bien, conseguiremos la flag final y escaparemos con el premio.

Info: La flag tiene el formato UAM{md5}

Resolución

Disponemos de un fichero, *"**firmware.zip**"*, lo descargamos y descomprimimos, obteniendo un fichero de imagen, ***backup.raw***.

Identificamos el fichero:

**file backup.raw**

> *backup.raw: Linux rev 1.0 ext4 filesystem data,*
> *UUID=046b9ae6-97df-49fd-8785-2c68de053b05 (extents) (large files) (huge files)*

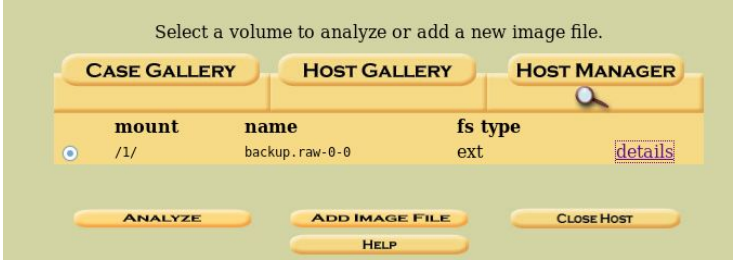
Tenemos una imagen en formato de ficheros ext4.

Montamos la imagen:

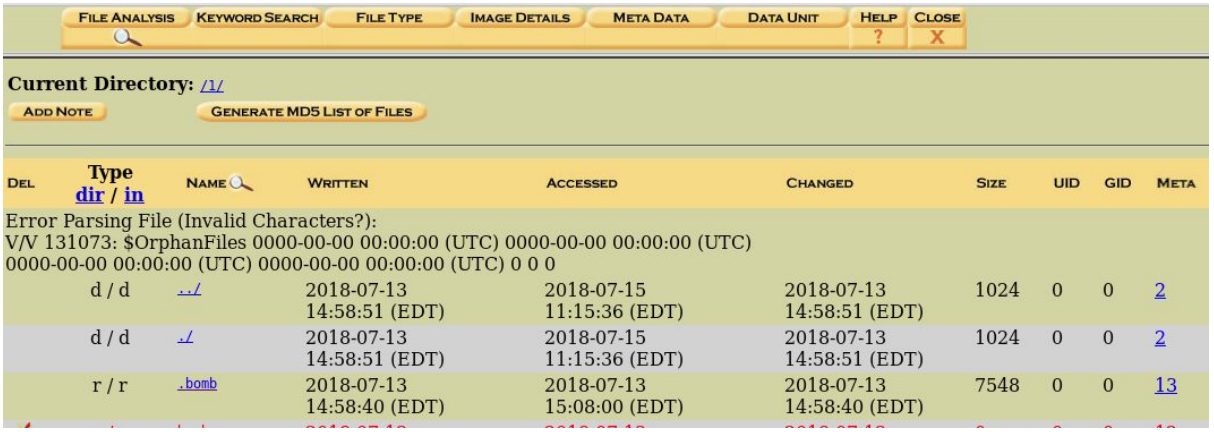
**sudo mount -t ext4 -o loop,rw,offset=0 backup.raw /mnt**

No encontramos nada interesante, algunos ficheros con pistas falsas /lib/, /tmp/.
**bomb.0** *Texto Base64 + asdas (Lorem ipsum…)*
**bomb.key** *Texto -nop- ( Rot13 -abc- )*
**bomb.resolve** *Texto Base64 (Lorem ipsum…)*
**flag.txt** *Texto (alalalallalaa no es nada de nada)*

Abrimos la imagen con un programa de análisis forense, **"autopsy".**




Analizamos ficheros y aparece algo interesante, un ejecutable **bomb**

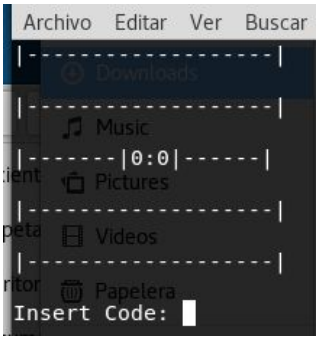



Exportamos el fichero y lo identificamos.

**file bomb**

> *bomb: ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, stripped*

Ejecutamos y nos aparece una cuenta atrás de 1 minuto, al finalizar nos pide un código, si ponemos cualquier cosa -> BOOM.




Toca reversing y encontrar el código ….

**binwalk bomb**

*DECIMAL HEXADECIMAL DESCRIPTION*
*---*
*0 0x0 ELF, 64-bit LSB executable, AMD x86-64, version 1 (GNU/Linux)*
*3676 0xE5C Copyright string: "Copyright (C) 1996-2013 the UPX Team. All Rights Reserved. $"*

Comprimido con UPX, tendremos que extraer:

**upx -d bomb**

Analizamos strings:

**rabin2 -z bomb**

```
000 0x000016c4 0x004016c4  16  17 (.rodata) ascii _dbf7c981d7e_fe8
001 0x000016d5 0x004016d5  12  13 (.rodata) ascii _c462eab3c39
002 0x000016e2 0x004016e2   9  10 (.rodata) ascii _f2b06_fd
003 0x000016ec 0x004016ec  15  16 (.rodata) ascii Tienes 1 minuto
004 0x000016fc 0x004016fc   5   6 (.rodata) ascii clear
005 0x00001702 0x00401702  22  23 (.rodata) ascii |--------------------|\n
006 0x00001719 0x00401719   9  10 (.rodata) ascii |-------|
007 0x00001725 0x00401725   9  10 (.rodata) ascii |------|\n
008 0x00001731 0x00401731  13  14 (.rodata) ascii Insert Code:
009 0x0000173f 0x0040173f   5   6 (.rodata) ascii italy
010 0x00001745 0x00401745   6   7 (.rodata) ascii BOOOM\n
```

Aquí ya tenemos mucha información, tenemos **italy** y algunas cadenas. Probamos con este código en el ejecutable y obtenemos:

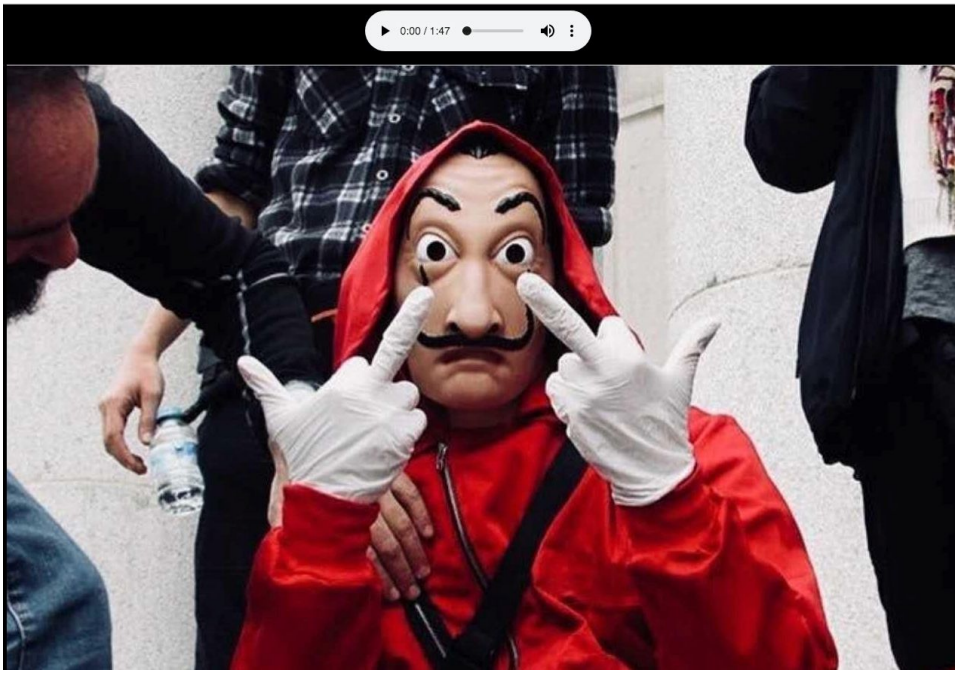
**_dbf7c981d7e_fe8_c462eab3c39_f2b06_fd**

Debe ser la dirección del servidor, no parece una URL, un MD5 (32 caracteres), pero sobran los caracteres '_'.

Probamos con  dbf7c981d7efe8c462eab3c39f2b06fd en https://www.md5online.org/

Found : **http://95.216.138.194/**
(hash = dbf7c981d7efe8c462eab3c39f2b06fd)

Ya tenemos dirección servidor. Accedemos, tras solventar algunos problemas con el certificado del servidor, nos aparece una página simple, un archivo de audio y una imagen de fondo.



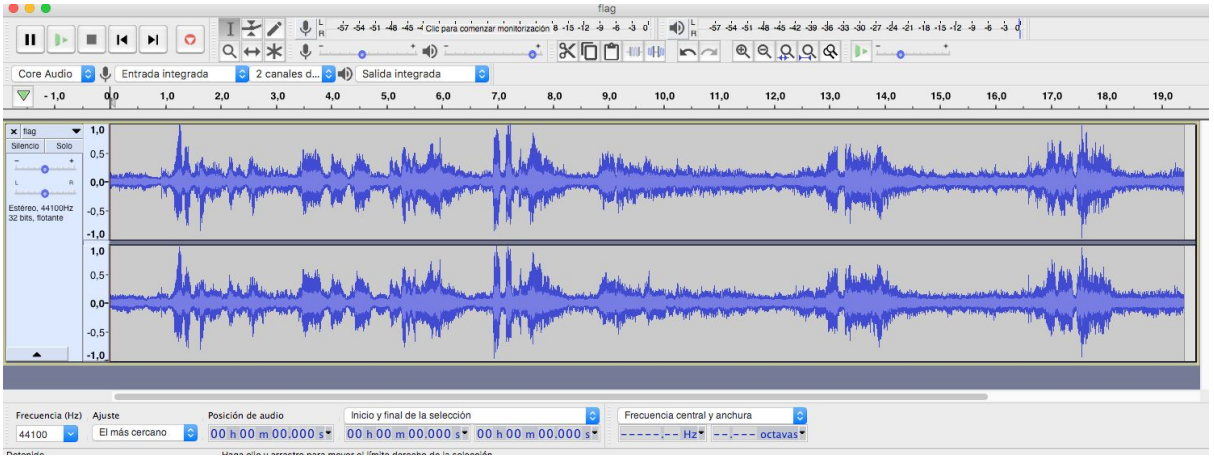
```html
<html>
<head>
    <title>La casa de papel</title>
</head>
<body bgcolor="black">
<!-- <audio src="audio/Bella_Ciao.mp3"></audio> -->
<center>
    <audio controls>
        <source src="audio/Bella_Cia0.wav" type="audio/mp4">
    </audio>
</center>
<br />
<center>
    <img src="images/back.jpg" />
</center>
</body>
</html>
```

En este punto y tras utilizar herramientas de stego, tanto para detectar en el audio como en la imagen, no obtuvimos ningún resultado. Un fichero de datos que nos dió la herramienta MP3Stego sobre el fichero mp3, pero que no tenía ningún sentido, nada en los espectrogramas de audio….

Pero llegó un HINT. *“Pero no ponéis realmente atención a lo que suena”.*

Y tras escuchar detenidamente los dos audios, en el fichero Bella_Cia0.wav, se escuchan unos pequeños tonos de fondo!!!!!!. Tenemos MORSE. desde el 0:46 - 1:03.

Extraemos el fragmento con “**AUDACITY”**

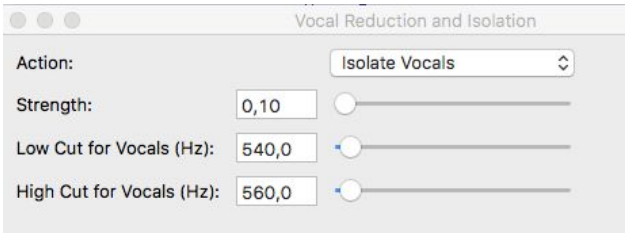



Toca filtrar para extraer sólo el código morse. Lo primero fue buscar con el “Efecto de Ecualización” la frecuencia. Obtenemos que 500-600. Pues aplicamos filtros para eliminar todo lo que no se encuentre entre esas frecuencias.

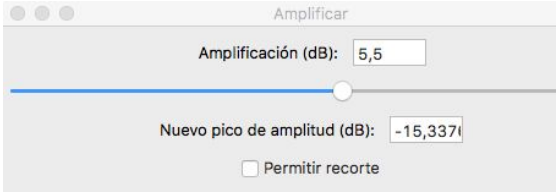
**Filtro Paso Alto (High Pass Filter)  600 Hz Rolloff (6db)**
**Filtro Paso Bajo(Low Pass Filter)  500 Hz Rolloff (6db)**

Ahora tenemos que afinar más, para dejar sólo el morse.

**Efecto Vocal Reduction and Isolation**

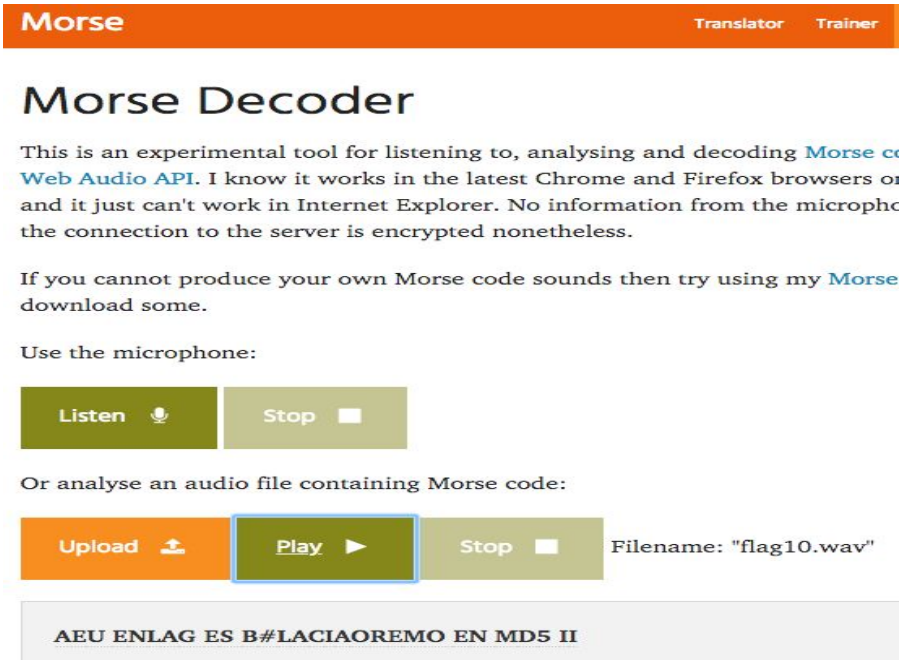



Y con esto ya tenemos el audio del morse. Podemos amplificar un poco con otro filtro.




Buscamos alguna página o software que nos reconozca morse, encontrando:

*https://morsecode.scphillips.com/labs/audio-decoder-adaptive/*




Deducimos que la flag es la canción + remo => md5(bellaciaoremo)

**UAM{f3b2c8d7436ccb3eaebc832c447f9051}**

@bicacaro