RETO UAM - SILICON VALLEY – EPISODIO 3

Richard mandó a Gilfoyle montar un servicio oculto que mantuviera a flote "El Flautista" pero este ya no recuerda donde se encuentra. Gracias a dios, como buen sysadmin, siempre hace backup de todo su trabajo, pero se trata de backups un tanto peculiares... Gilfoyle guarda el trabajo que hace en archivos encriptados relacionados con temáticas que le gustan.

Tenemos el fichero que contiene información sobre el servicio. Necesitamos que extraigas la información, accedas al servicio y consigas la flag de UAM. ¡Mucha suerte!

Enlace de descarga: https://drive.google.com/open?id=1qTuI9VndJ24krrO8U1WF3JpS77M4M2hV

Info: La flag tiene el formato UAM{md5}

Descargamos el fichero, y al descomprimirlo vemos que tiene dentro un fichero .WAV de música. Si lo reproducimos, es correcto.

Analizamos el inicio del fichero, y se confirma el formato WAV:

```
          0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: 52 49 46 46 E6 77 FC 01 57 41 56 45 66 6D 74 20 ; RIFFæwü.WAVEfmt
00000010h: 12 00 00 00 01 00 02 00 44 AC 00 00 10 B1 02 00 ; ........D¬...±..
00000020h: 04 00 10 00 00 00 64 61 74 61 C0 77 FC 01 04 00 ; ......dataÀwü...
00000030h: 04 00 05 00 03 00 04 00 03 00 04 00 06 00 00 00 ; ................
```

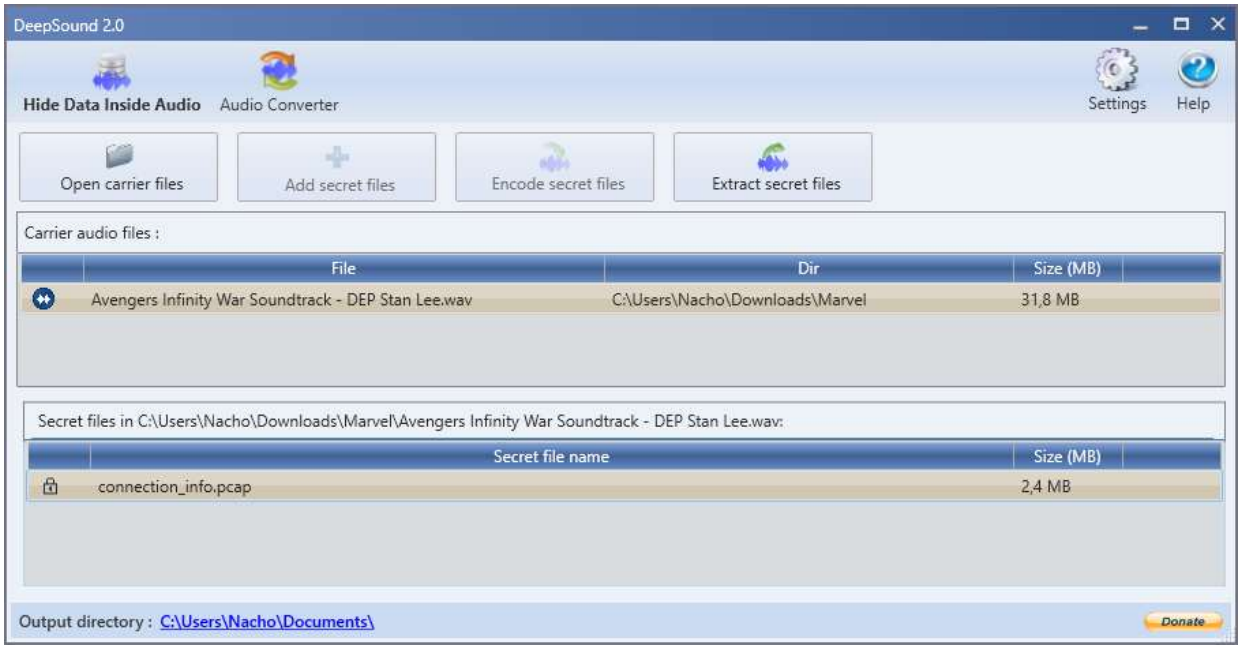
Vemos que al final del fichero lleva un texto oculto:

```
01fc77d0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
01fc77e0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 32 ; ..............U2
01fc77f0h: 39 75 61 57 52 76 55 48 4A 76 5A 6E 56 75 5A 47 ; 9uaWRvUHJvZnVuZG
01fc7800h: 38 37 4B 51 6F 3D 0A                           ; 87KQo=.
```

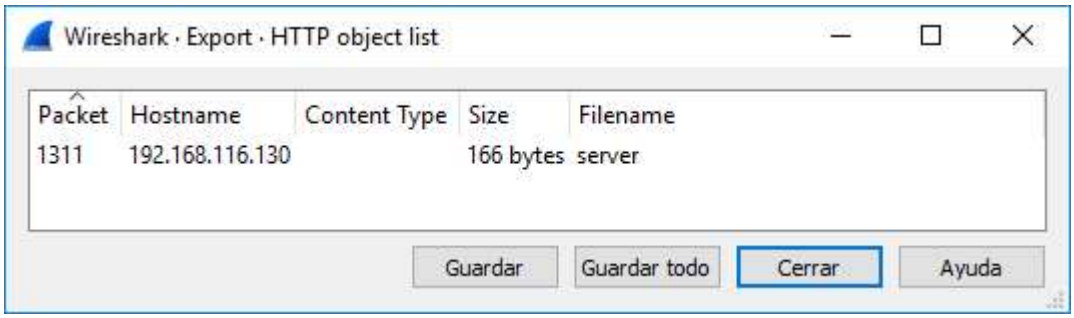
Aparentemente es Base64, si lo desciframos para una pista falsa. Encima cachondeíto.. 😉

```
SonidoProfundo;)
```

Utilizamos una herramienta para detectar información oculta en un fichero WAV, como Deep Sound (v2.0). Cargamos el fichero, y al darle al Extract Secret Files, nos aparece un fichero oculto:



Es un archivo de tráfico de red. Si lo cargamos con WireShark, buscamos los objetos HTTP y nos indica que dentro lleva un fichero:

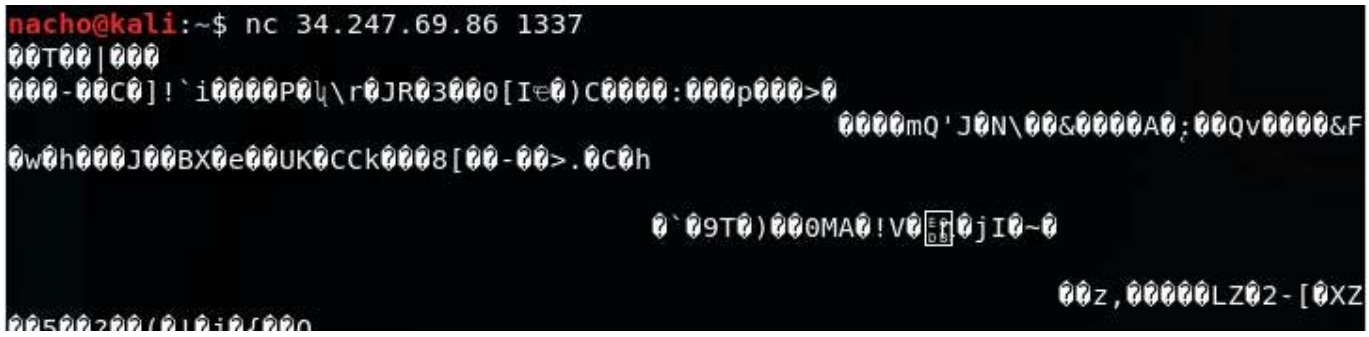


Al abrir el fichero, esto parece morse!

```
...-- ....- .--. ..- -. - --- ..--- ....- --... .--. ..- -. - --- -.... ----. .--. ..- -. - --- ---
```

Lo analizamos con un conversor de morse online y nos devuelve una cadena, que parece una IP:Puerto.

Si lo cargamos vía navegador, se queda descargando pero no termina, así que no parece un servicio HTTP. Nos vamos a Kali y lo invocamos vía netcat:



Devuelve texto binario, y de manera continua. Así que repetimos el comando, pero lo sacamos a fichero, y lo dejamos un rato:

Ahora abrimos el fichero en modo HEX, y buscamos algo de información que nos pueda servir. Busco algunos caracteres por si se van repitiendo y es un mismo fichero muchas veces, pero la información va variando, no se repiten las cadenas. Entonces busco “UAM” y aparece en el fichero, y ésta si sale varias veces:

```
002770b0h: 9B A4 4D 44 B4 20 55 41 4D 3A 4F 57 59 35 4D 54 ; ›¤MD´ UAM:OWY5MT
002770c0h: 42 68 4E 6A 4E 69 4D 47 52 6C 4E 57 4D 7A 4E 6A ; BhNjNiMGRlNWMzNj
002770d0h: 4D 34 59 54 41 33 4D 54 67 34 4D 7A 46 69 4E 32 ; M4YTA3MTg4MzFiN2
002770e0h: 4A 6B 4F 44 6B 30 4D 47 59 78 4E 32 45 79 5A 6A ; JkODk0MGYxN2EyZj
002770f0h: 5A 6A 59 54 51 34 4D 54 45 32 4D 44 56 6C 59 6D ; ZjYTQ4MTE2MDVlYm
00277100h: 55 30 4E 47 4D 77 5A 6A 4E 6B 59 6A 4A 69 4E 6D ; U0NGMwZjNkYjJiNm
00277110h: 49 32 59 7A 51 7A 5A 6A 55 31 4E 6D 5A 68 59 6A ; I2YzQzZjU1NmZhYj
00277120h: 59 77 4D 57 5A 38 61 32 56 35 4F 6A 46 5A 52 55 ; YwMWZ8a2V5OjFZRU
00277130h: 46 53 20 03 74 69 0F C8 36 B3 E1 6A 21 F8 33 C9 ; FS .ti.È6³áj!ø3É
00277140h: 78 F9 87 82 E1 BD BB E8 0A B3 9D 50 FE 98 BB 90 ; xù‡,á½»è.³ Pþ˜»
```

Veo que se repite varias veces en el fichero, pero siempre con el mismo texto después, así que debe ser el bueno. Claramente es un Base64:

UAM:OWY5MTBhNjNiMGRlNWMzNjM4YTA3MTg4MzFiN2JkODk0MGYxN2EyZjZjYTQ4MTE2MDVlYmU0NGMwZjNkYjJiNmI2YzQzZjU1NmZhYjYwMWZ8a2V5OjFZRUFS

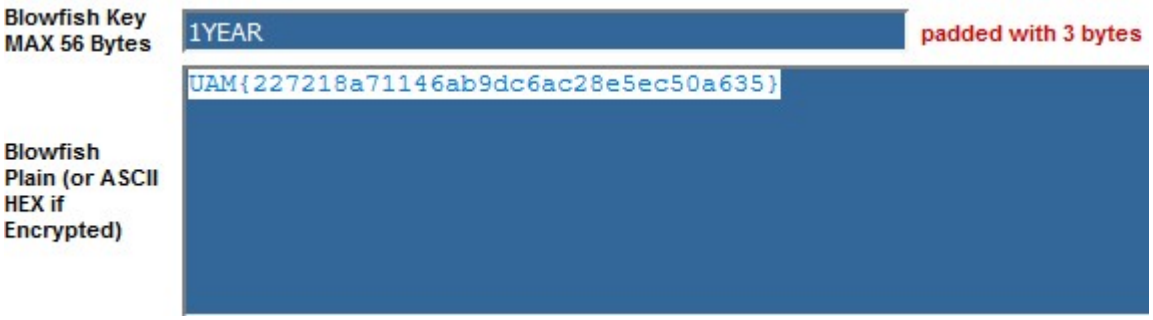
Así que lo descifro y me da esta otra cadena:

```
9f910a63b0de5c3638a0718831b7bd8940f17a2f6ca4811605ebe44c0f3db2b6b6c43f556fab601f|key:1YEAR
```

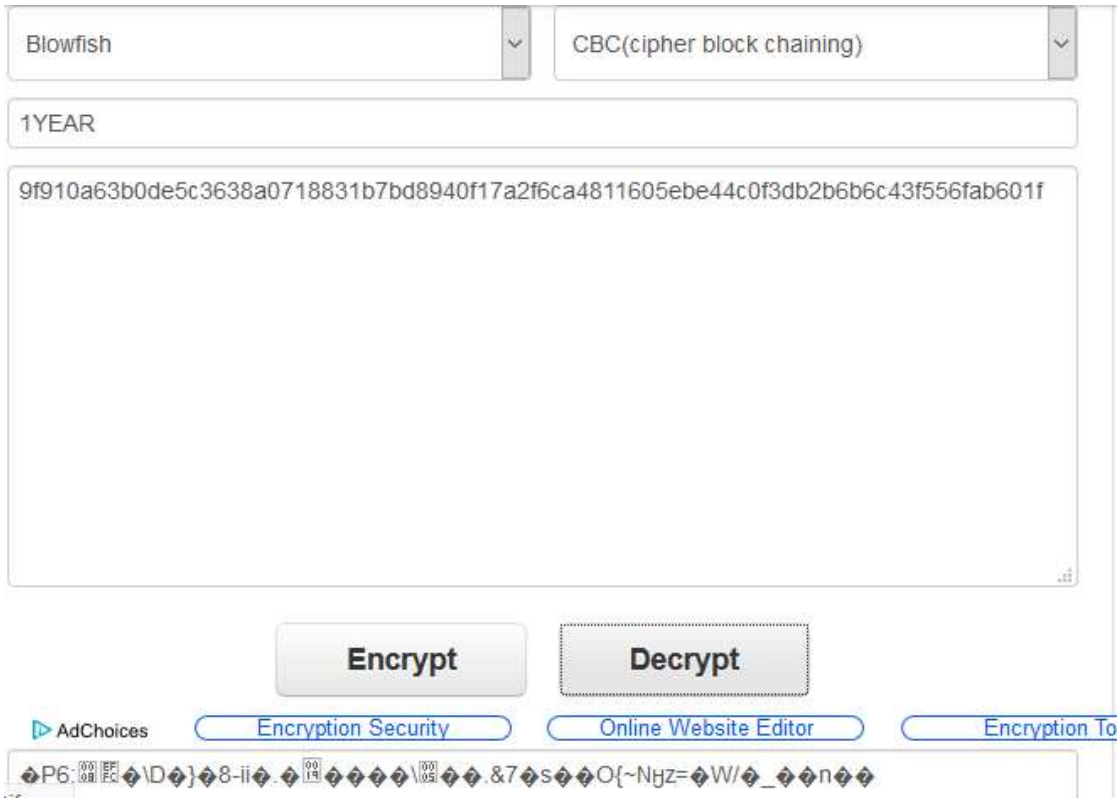
Esto ahora es un Hexadecimal, y además lleva “key:1YEAR”, por lo que parece que ya no es un HASH, sino un texto encriptado con dicha clave “1YEAR”.

Voy probando distintas herramientas, y distintos algoritmos de encriptación con clave simétrica, muchos de ellos tienen distintos modos que también voy probando, pero no logro encontrar la solución.

Finalmente, pruebo una Web de cifrado BlowFish específica, y esta vez sí, damos con la solución:



Lo curioso es como, pese a haber probado dicho algoritmo Blowfish en varias Webs anteriormente, no lo descifraba de manera correcta hasta que probé en esa web:



User: nachinho3

Telegram: @jignaciodemiguel