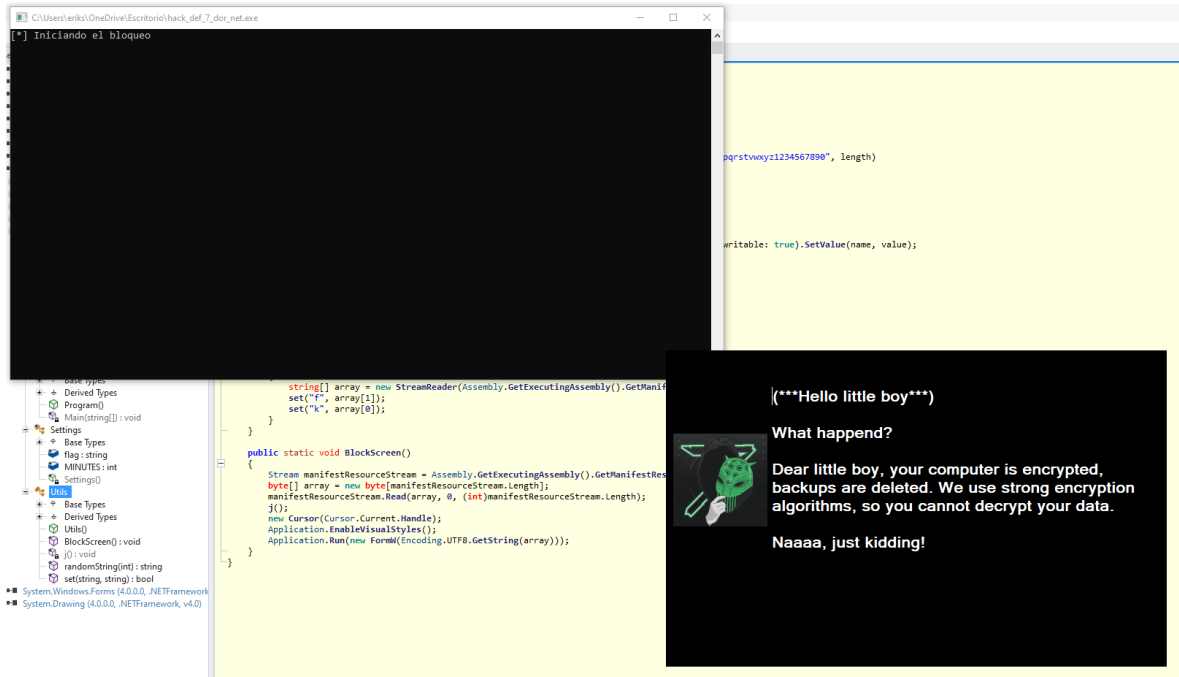


Resolver el problema de HackDef Dot Net (Ransomware)

Al descargar y ejecutar el programa tenemos esta vista:



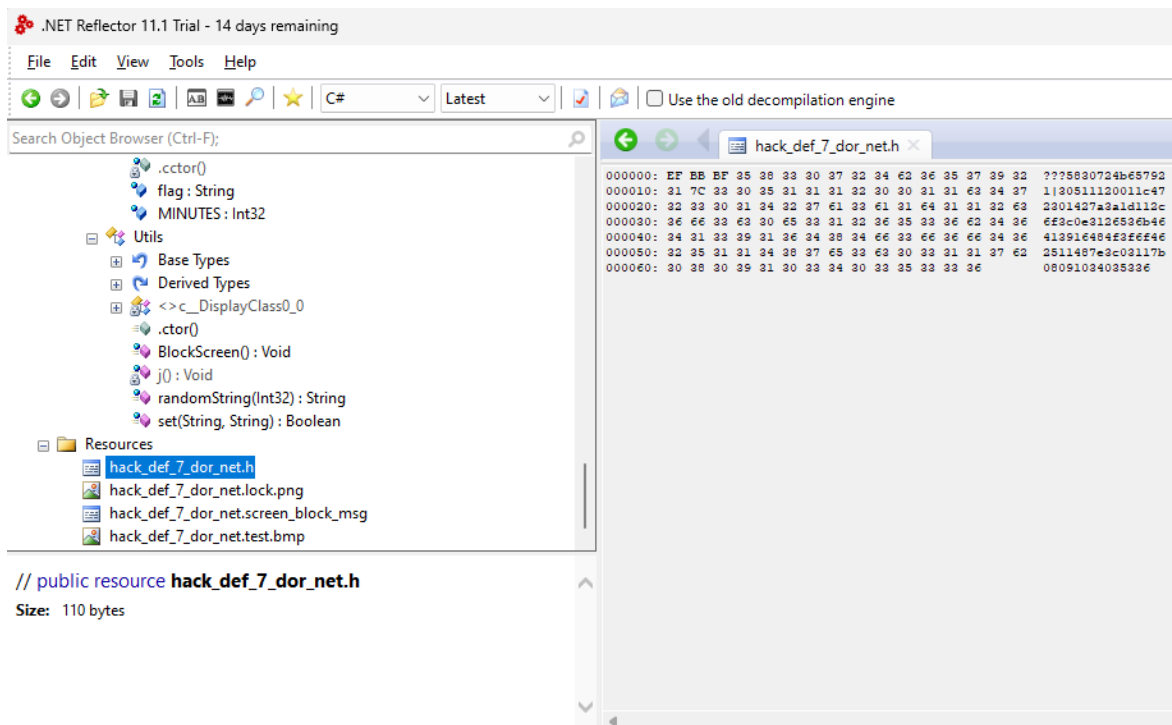
Usando una aplicación que permita descompilar el programa, en este caso usaremos ILSpy, para ver el código fuente. En este podemos ver varias cosas de interés:

#1:

Que triste
jeje

```
// hackdef.Settings
public static class Settings
{
    public static string flag = "flag{this_is_A_dummy_flag!}";
    public static int MINUTES = 120;
}
```

#2: Encontramos una “biblioteca” llamada hackdef7.h que contiene varios números raros:



Podemos traducir estos números a algo mas o menos legible:

Hex to String

♥ Add to Fav

New

Save & Share

Enter the hexadecimal text to decode

Sample



```
5830724b657921|30511120011c472301427a3a1d112c6f3c0e3126536b46413916484f3f6f462511487
e3c03117b08091034035336
```

Size : **107** B, 107 Characters

☒ Auto

Hex to String

File..

Load URL






The Converted string:



```
X0rKey!Är0'£iNÆóÄäe6'dóóôbQäÄ1@53
```

Size : **54** B, 54 Characters

Estos números también los podemos obtener sin usar el decompilador, pero esta bastante oculto, que nos da mas pistas. El programa crea 2 registros en tu computadora:

Nombre	Tipo	Datos
 (Predeterminado)	REG_SZ	(valor no establecido)
 f	REG_SZ	30511120011c472301427a3a1d112c6f3c0e3126536b...
 k	REG_SZ	5830724b657921
 MicrosoftEdgeA...	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Applicati...
 OneDrive	REG_SZ	"C:\Users\eriks\AppData\Local\Microsoft\OneDriv...

En este caso podemos ver que los registros se llaman f y k, ósea Flag y Key, sabiendo que k es XORKey!, igualmente usando f traducido de hex a string podemos hacer XOR con la key y obtenemos:

```
hackdef{101_d0t_NkT_r3v3rs1ng_4nt1_d3c}
```