計算機安全 HW 0x0c Writeup

- Real name: 張瀚文
- Nickname on course website: Hwww
- Student ID: b07505027.

ChristmasGift

用ida看，裡面把輸入跟一個字串做比對，如果相同則輸出一堆資料，而那堆資料如果用file看發現是gzip壓縮檔gift，如果再解壓縮，又可以得到一個gift elf，如此循環下去...聽說禮物要拆1000次才拆得完...（未解）

JustOnLinux

此題將一個輸入的字串編碼並輸出。用ida看source code可以找到編碼的規則：

假設輸入的字串是C，編碼後字串是S。編碼方式為C中每3個字元$c_1c_2c_3$轉換為S中4個字元$s_1s_2s_3s_4$

轉換方法如下：

若字元c_n轉為二進位後為$c_n = c_{n8}c_{n7}c_{n6}c_{n5}c_{n4}c_{n3}c_{n2}c_{n1}$

$$
\begin{aligned}
s_1 &= 00c_{18}c_{17}c_{16}c_{15}c_{14}c_{13} \\
s_2 &= c_{14}c_{13}c_{12}c_{11}c_{28}c_{27}c_{26}c_{25} \\
s_3 &= c_{26}c_{25}c_{24}c_{23}c_{22}c_{21}c_{38}c_{37} \\
s_4 &= c_{38}c_{37}c_{36}c_{35}c_{34}c_{33}c_{32}c_{31}
\end{aligned}
$$

並將s_n以一個對照表做轉換。

而對照表可以得到逆轉換，c也可從s反推：

$$
\begin{aligned}
c_1 &= (s_1 << 2) + ((s_2 >> 4)\&3) \\
c_2 &= ((s_2\&15) << 4) + (s_3 >> 2) \\
c_3 &= ((s_3\&3) << 6) + s_4
\end{aligned}
$$

最後就可以寫出解碼程式，解出flag~

程式碼可參考： `code/JustOnLinux/hack.py`