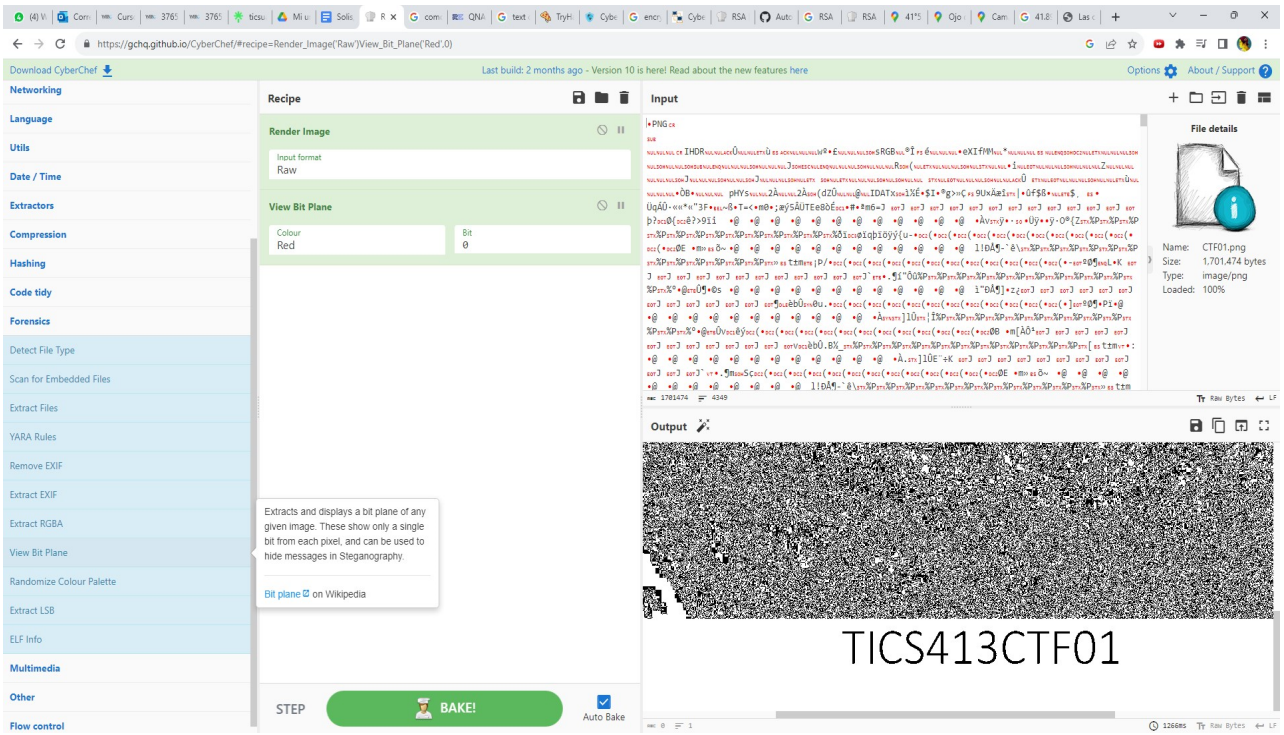
CTF01

Nombre: Fernando Solís Hernández

Para empezar con este “Capture the flag” en primer lugar había que buscar la llave pública y privada, las cuales se encontraban en un archivo bloqueado con contraseña y que sirvieron para modificar la ubicación del premio.

Por ende comencé el desencriptado cargando la imágen entregada por medio de CyberChef, tuve una intensa búsqueda sobre qué operación servía para nuestro propósito, probé con operaciones como ‘From base64’, ‘OCR’, entre otras. Lamentablemente esta búsqueda fue en vano y lo se me ocurrió hacer es ir viendo las operaciones integradas, hasta que en el apartado ‘Forensics’ se llegó a la opción ‘View Bit plane’, la cual muestra un único bit de cada píxel en una imágen y es usada para esconder mensajes. Al usar esta operación se descubrió un mensaje secreto, ‘TICS413CTF01’.



Este mensaje sería la clave del archivo con las llaves que buscamos.

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgGxtOm3j+z442Kgf4f0ZnHsBw43gfyeBTtBS3GStnlBv1Ff+IfzT
pNihPvuXguV/JsecBhP2MvqCR0C2LwinTWZlxBy9Hq7KXKhTRVbheBAc3IQHgJpy
PWcGv6EzPHRwgpGKP1B470ZCx8IvGVrcJUedw1BowRPDCj4mYU7I0ihnAgMBAAEC
gYAQtiEcUNgndfGGsCtPrEPe/Z2bX2+ZsidommzXo57T/Ph4e3XXlvNAZFHlyytk
nd1nRJf3OaoPzEaZJbtIFSkrnGu7ARPbHAy+YGzILSrSM3Hs7FNFLFH83pu5JuFn
8OKvpHp+y7y2jAazLA6oqdvKL3+i2i2a/9E34uuGEijggQJBALtXfgWk9QJOg9Fb
mGbzc6c0bUAcM6jzlBlAEbuS9Pfh+bNpFlVnvSEaz7hVvC1d4QJIqzaHZy1chVbE
JUTotic CQQCUKeDelbninpe+E2T2+4qV1x4/vv5nlUSulFLA0PARO69nrKfsV7RM
jSkjG5iWSPvTXf9meRsS7FrBfKVhKqPBAkEAt+8yCyana8lcwLvWiRXz8jGWJkDK
M9JbEOOHxYuGuq4CtLSzucyts4gYc9qxdDVdCxoAB/yvP6k8PTE9ikeVNwJAPQy0
d4LCQTqP0+Yx6ALlq7Aj6qhMM2oyDq1XG9P71138fH+MAbpxtElF9g1c5i/Uc9d7
cUHdggKZsrglfNARAQJAXijomQyphaLvNLLqPKChxku8nHR/0hSPBE9LLoBlMcY7
em4ovUoGT7t/7zQtD2QSA+D7T/ZeOjnVScB1SgAx9w==
-----END RSA PRIVATE KEY-----
-----BEGIN PUBLIC KEY-----
MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgGxtOm3j+z442Kgf4f0ZnHsBw43g
fyeBTtBS3GStnlBv1Ff+IfzTpNihPvuXguV/JsecBhP2MvqCR0C2LwinTWZlxBy9
Hq7KXKhTRVbheBAc3IQHgJpyPWcGv6EzPHRwgpGKP1B470ZCx8IvGVrcJUedw1Bo
wRPDCj4mYU7I0ihnAgMBAAE=
-----END PUBLIC KEY-----
```

Estas claves nos ayudaron para descifrar las coordenadas del premio, para esto había que encontrar un algoritmo de criptografía donde en cyberchef se encontraba RSA, en este caso usé ‘RSA decrypt’ donde se usó la clave privada y resultó que el premio sería entregado en la universidad (el output arrojado fue: -33.489742, -70.513682).

Luego, en segundo lugar de este CTF, había que cifrar un archivo .dat donde se cambiarían las coordenadas para la entrega de este premio, para esto se usó 'RSA encrypt' y la llave pública entregada anteriormente. Para este caso decidí que el premio cambiaría su ubicación al Coliseo Romano en Italia (se ingresó como input: 41.890210, 12.492231).