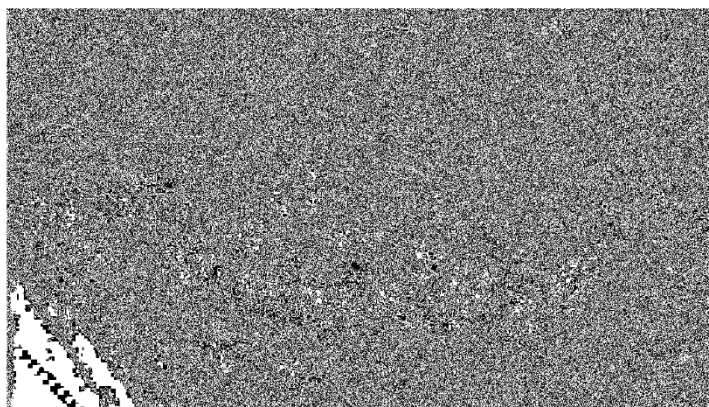


Catalina Loyola

Paso 1: Abrir la imagen llamada CTF01 encontrada por los especialistas y descargarla, la cual se descarga para subirla a CyberChef.



Paso 2: Al subir la imagen al CyberChef, se ocupa la herramienta View bit plane, la cual extrae y muestra un plano de bits de cualquier imagen determinada y se puede usar para ocultar mensajes en esteganografía. Gracias a esto obtenemos la contraseña que estaba oculta en la imagen que es TICS413CTF01.



TICS413CTF01

Paso 3: Al obtener la contraseña la utilizamos para abrir el archivo que esta “protegido” que cuenta con la llave pública y privada.

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgGxtOm3j+z442Kgf4f0ZnHsBw43gfyeBTtBS3GStnlBv1Ff+IfzT
pNihPvuXguV/JsecBhP2MvqCR0C2LwinTWZlxBy9Hq7KXKhTRVbheBAc3IQHgJpy
PWcGv6EzPHRwgpGKP1B470ZCx8IvGVrcJUedw1BowRPDCj4mYU7I0ihnAgMBAAEC
gYAQtiEcUNgndfGGsCtPrEpe/Z2bX2+ZsidommxXo57T/Ph4e3XXlvNAZFhlytk
nd1nRJf30aoPzEaZJbtIFSkrrnGu7ARpbHAy+YGzILSrSM3Hs7FNFLFH83pu5JuFn
80KvpHp+y7y2jAazLA6oqdvKL3+i2i2a/9E34uuGEijggQJBALtXfgWk9QJ0g9Fb
mGbzc6c0bUAcM6jzLB1AEbuS9Pfh+bNpFLVnvSEaz7hVvC1d4QJIqzaHZy1chVbE
JUToticCQQUKeDeLbninpe+E2T2+4qV1x4/vv5nlUSulFLA0PAR069nrKfsV7RM
jSkjG5iWSPvTXf9meRsS7FrBfKVhKqPBAKEAt+8yCyana8lcwLvWiRXz8jGWJkDK
M9JbE00HxYuGuq4CtLSzucyts4gYc9qxdDVdCxoAB/yvP6k8PTE9ikeVNwJAPQy0
d4LCQTqP0+Yx6ALlq7Aj6qhMM2oyDq1XG9P71138fH+MAbpxtElF9g1c5i/Uc9d7
cUHDggKZsrglfNARAQJAXijomQyphaLvNLLqPKChxku8nHR/0hSPBE9LLOBLMcY7
em4ovUoGT7t/7zQtD2QSA+D7T/Ze0jnVScB1SgAx9w==
-----END RSA PRIVATE KEY-----
-----BEGIN PUBLIC KEY-----
MIGeMA0GCSqGSIb3DQEBQUAA4GMADCBiAKBgGxtOm3j+z442Kgf4f0ZnHsBw43g
fyeBTtBS3GStnlBv1Ff+IfzTpNihPvuXguV/JsecBhP2MvqCR0C2LwinTWZlxBy9
Hq7KXKhTRVbheBAc3IQHgJpyPWcGv6EzPHRwgpGKP1B470ZCx8IvGVrcJUedw1Bo
wRPDCj4mYU7I0ihnAgMBAAE=
-----END PUBLIC KEY-----
```

Paso 4: Ahora debemos subir el archivo que tiene las coordenadas iniciales a CyberChef, este archivo esta cifrado, por lo tanto, con la herramienta RSA Decrypt nos permite descifrarlo con ayuda de la llave privada y obtenemos las coordenadas iniciales: -33.489742, -70.513682

RSA Decrypt

RSA Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgGxtOm3j+z442Kgf4f0ZnHsBw43gfyeB
TtBS3GStnlBv1Ff+IfzT
```

Key Password

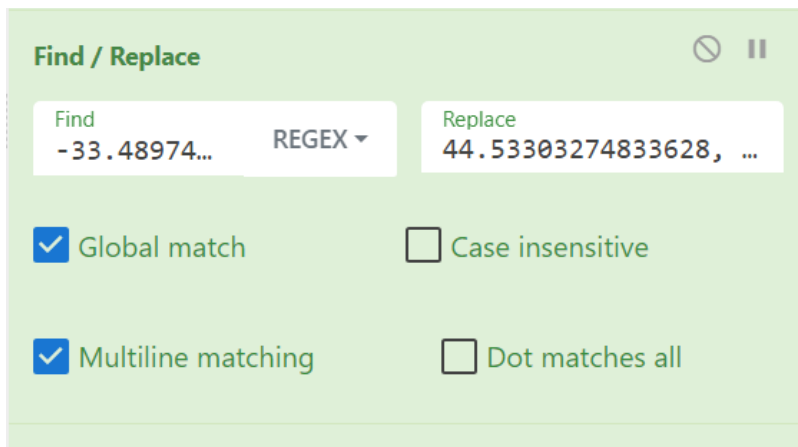
Encryption Scheme: RSA-OAEP

Message Digest Algorithm: SHA-1

Output

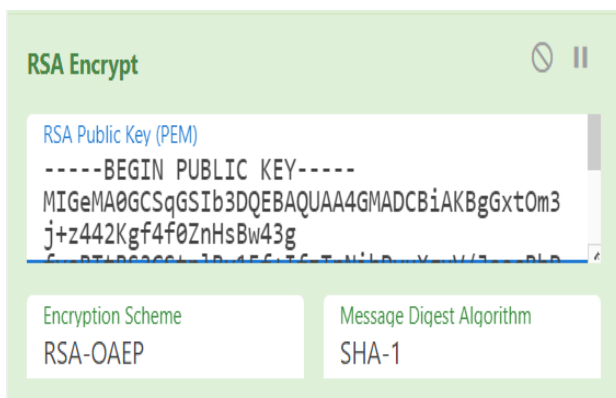
-33.489742, -70.513682

Paso 5: Con la herramienta Find/Replace reemplazamos las coordenadas originales por 44.53303274833628, 10.864521068979164 (las cuales son las coordenadas de la fábrica de automóviles de Ferrari en Italia).



The screenshot shows the 'Find / Replace' window with a light green header. The 'Find' field contains '-33.48974...' and the 'Replace' field contains '44.53303274833628, ...'. A dropdown menu is set to 'REGEX'. Below the fields, there are four checkboxes: 'Global match' (checked), 'Case insensitive' (unchecked), 'Multiline matching' (checked), and 'Dot matches all' (unchecked). The window has a close button and a pause button in the top right corner.

Paso 6: Ahora que reemplazamos las coordenadas originales, debemos volver a cifrar el archivo otra vez, para eso utilizamos RSA Encrypt, el cual nos pide una llave publica, para eso utilizaremos la llave publica que se encuentra en el archivo con las llaves.



The screenshot shows the 'RSA Encrypt' window with a light green header. The 'RSA Public Key (PEM)' field contains the text: '-----BEGIN PUBLIC KEY-----', 'MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgGxtOm3', 'j+z442Kg4f0ZnHsBw43g', and a partially visible line '6-RTLR006L-1D-456-T6-T-N'LD-X-V/3-PLD'. Below this field, there are two dropdown menus: 'Encryption Scheme' set to 'RSA-OAEP' and 'Message Digest Algorithm' set to 'SHA-1'. The window has a close button and a pause button in the top right corner.

Paso7: Una vez cambiamos las coordenadas y volvemos a cifrar el archivo, se debe descargar el dat y estamos listos, logramos sustituir las coordenadas para la entrega del premio.