EL AGENTE OCULTO

Para comenzar, analicé la imagen en aperi'Solve.

Lo cual descargue los 7zip que son Steghide, Outguess, Binwalk y Foremost.
Y en dos carpetas encontré:

1)un jpg junto a un audi.txt

2) dos archivos uno 0 y 1E

Volvi a la img(sm01.jpeg) la pase por HxD para ver si encontraba algo..
Intente con exiftool sm01.jpeg donde puedo ver datos que me podrían ayudar como x e y, el titulo = kdrmy6get4 y un hash.

Al hash lo cifré con base64 en CyberChef y dice "HayunadireccionIPaqui" lo cual procedí a juntar el x e y

x=54.157

y=215.99

IP=54.157.215.99

Pruebo escanear la IP con nmap lo cual nos devuelve:
ec2-54-157-215-99.compute-1.amazonaws.com
y al buscarlo en internet veo que es un archivo de Apache2Ubuntu.

Ahora para ver si es la IP es correcta la pruebo en google y obtengo 6 hx

h01-> aHR0cHM6Ly

h02 -> 9wYXN0ZWJpbi5

h03 -> jb20vUWV3e

h04 -> HF1a3Q=

h05 -> muchos hexa

h06 ->
U2kgbGxlZ8OzIGhhc3RhIGFxdcOtIGVzdG95IHNlZ3VybyBxdWUgZXN0ZSBtZW5zYWplIGxsZWdhcsOhIGEgbGFzIGZyb250ZXJhcyBkZSBtZWRpbyBvcmllbnRlIGEgc2Fsdm8uIFNhbnRvcywgZXN0YSBlbmNyaXB0YWRvIGNvbiB1bmEgY2xhdmUgYWxmYW51bWVyaWNhIGRlIDQgZGlnaXRvcywgbm8gcHVlZG8gZGVjaXJsZSBlbCBmb3JtYXRvIHBlcm8gZXN0b3kgc2VndXJvIHF1ZSBsby BwdRyw6EgcmVzb2x2ZXIgbGV5ZW5kbyBsb3MgZGF0b3MgZGVsIGFyY2hpdm8uCgpBdHRlIEZlaGxlcg==

Con esta información lo que hice fue lo siguiente:

Traducí el h01 y era un http entonces probé juntar varios…
Junté del h01 al h04 :
aHR0cHM6Ly9wYXN0ZWJpbi5jb20vUWV3eHF1a3Q= lo pasé from Base64 y aparece https://pastebin.com/Qewxqukt
Lo cual nos pide una clave.

Empecé probando con una clave que da en la imagen con aperi'Solve (que también salia en exiftool) : `KdrmY6get4` y pude ingresar.
El resultado que nos da es un dibujo de la Mona Jimenez que nos dice que no es el camino correcto.
Ahora debemos buscar otro camino…

Sigo analizando los demas hx

Al h05 lo paso a HxD y nos da una foto de un hombre.
la cual si la paso por aperi'Solve nos dice datos como:
feler.jpeg, fehler.jpeg, mariano.jpg ,d'leliasospechoso, donsantos.jpeg , segundosospechoso.jpeg que nos podrían servir para descubrir el agente..

el h6: Si llegÃ³ hasta aquÃ estoy seguro que este mensaje llegarÃ¡ a las fronteras de medio oriente a salvo. Santos, esta encriptado con una clave alfanumérica de 4 digitos, no puedo decirle el formato pero estoy seguro que lo podrÃ¡ resolver leyendo los datos del archivo.

Atte Fehler

En este punto podemos decir que el agente es Santos, ya que el mensaje lo nombra y en la imagen del señor lo dice.
Ahora debemos seguir buscando el mensaje oculto

Analizando por kali los comprimidos formato (7z) de la imagen del hombre observo que tengo un “4100” que pide contraseña para abrirlo
La cual tengo que encontrar.
Ahora paso a hacer lo siguiente:

creo un hash de 4100 , (para el hash : 7z2john 4100 > hash.txt
)

creeo un crunch con numeros y letras (crunch 4 4
0123456789abcdefghijklmnopqrstuvwxyz > password.txt
)
ya que la pista anterior era una clave que estaba compuesta de 4 dígitos alfanuméricos.

y se los pasé a John the ripper para tratar de conseguir la contraseña
(john –wordlist=password.txt hash.txt)

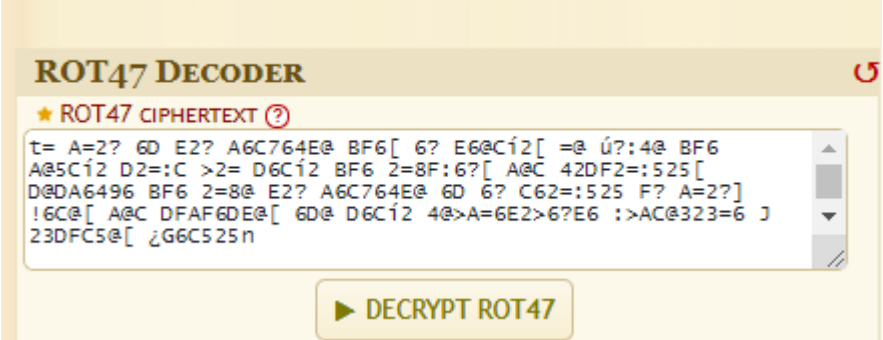
al encontrar la clave (9ofs) me da :

```
1 dD0gQT0yPyA2RCBFMj8gQTZDNzY0RUAgQkY2WyA2PyBFNkBD7TJbID1AIPo/
  OjRAIEJGNiBBQDVD7TIgRDI9OkMgPjI9IEQ2Q+0yIEJGNiAyPThGOjY/
  WyBBQEMgNDJERjI9OjUyNVsgREBEQTY0OTYgQkY2IDI9OEAgRTI/IEE2Qzc2NEVAIDZEIDY/
  IEM2Mj06NTI1IEY/
  IEE9Mj9dICE2Q0BbIEFAQyBERkFGNkRFQFsgNkRAIEQ2Q+0yIDRAPkE9NkUyPjY/
  RTYgOj5BQ0AzMjM9NiBKIDIzREZDNUBbIL9HNkM1MjVu
```

lo cual lo paso por cyberchef from 64 y me devuelve;

t= A=2? 6D E2? A6C764E@ BF6[6? E6@Cí2[=@ ú?:4@ BF6 A@5Cí2 D2=:C >2= D6Cí2 BF6 2=8F:6?[A@C 42DF2=:525[D@DA6496 BF6 2=8@ E2? A6C764E@ 6D 6? C62=:525 F? A=2?] !6C@[A@C DFAF6DE@[6D@ D6Cí2 4@>A=6E2>6?E6 :>AC@323=6 J 23DFC5@[¿G6C525n

vuelvo a cifrar lo anterior por Dcode y obtengo:



El plan es tan perfecto que, en teoría, lo único que podría salir mal sería que alguien, por casualidad, sospeche que algo tan perfecto es en realidad un plan. Pero, por supuesto, eso sería completamente improbable y absurdo, ¿verdad?

Entonces podemos decir que hemos finalizado el trabajo .