Reto Forense

Ha habido una filtración empresarial, y en la investigación se ha incautado una tarjeta SD a uno de los empleados sospechoso de la filtración.

Tras el análisis con Autopsy de la imagen de la tarjeta SD, se ha obtenido el fichero Planos.raw. Tu objetivo es averiguar que secreto(s) esconde este fichero, para ver si apoya la hipótesis de culpabilidad del empleado o si bien proporciona evidencias que la refuten. Sabrás que has obtenido la prueba necesaria cuando veas la palabra FLAG.

Las respuestas a las siguientes preguntas te ayudarán a conseguir tu objetivo.

1. ¿Cuál es la extensión real del fichero Planos.raw?

   Utiliza la orden file para averiguarlo

2. ¿Cuál es la contraseña para este fichero?

   Utiliza fcrackzip junto al diccionario de contraseñas rockyou.txt para averiguarla

3. ¿Qué tipo de ficheros hemos obtenido? ¿Qué información proporcionan?

   Utiliza outguess para ver si tiene información oculta.

   La contraseña aparece en todos los documentos de la asignatura aunque no lo se ve mucho!!