Facultad de Informática	Módulo 1 (Curso 2020/21): Análisis forense de sistemas. Auditoría Informática II	

Nombre y Apellidos: ……..

Tarea 2

1. Prácticas de Metadatos
   - **a.** Objetivo
     - i. Analizar los metadatos de documentos DOC, PDF e imágenes.
     - ii. Evitar fuga de información.
   - **b.** Documentación principal
     - i. FOCA Final Version
     - ii. Metashieldanalyzer
     - iii. Extractmetadata
     - iv. Inspección documentos en Word, Adobe Reader y otros.
   - **c.** Documentación auxiliar
     - i. www.elevenpaths.com
     - ii. https://metashieldanalyzer.elevenpaths.com
     - iii. www.elladodelmal.com
     - iv. www.extractmetadata.com
     - v. Presentación módulo AI2_01
     - vi. Otras herramientas que se estimen necesarias

Desarrollo

1. Logística

Los alumnos podrán realizar la Tarea por equipos de 2-5 personas. Si se desea la práctica se puede realizar de forma individual. Descargarán las aplicaciones, programas y utilidades necesarias de las direcciones indicadas o de donde se estime. Para esta práctica de metadatos se descargarán la carpeta del CV que contiene diversos ficheros a analizar.

2. Desarrollo

   a. Se analizarán los ficheros contenidos en la carpeta FOCA publicado en el CV (el profesor podrá sugerir nuevos ficheros) y se constatarán para cada uno qué metadatos sensibles contienen. Para ello se utilizarán al menos 2-3 herramientas o métodos.
   b. Se analizarán otros ficheros PDF (al menos cinco) de otras webs públicas que estime el alumno.
   c. Se generará un informe con los resultados explicando los métodos y acciones seguidos en el análisis forense realizado.
   d. Uno de los miembros del equipo subirá un ZIP con el informe de resultados. Es deseable que se ponga gran interés tanto en el contenido como en el continente. En el informe se incluirá, además de lo indicado en el punto anterior, la siguiente información:

i. Identificación de los alumnos.
ii. Explicación y análisis detallado del laboratorio o escenario de análisis forense.
iii. Explicación detallada de las acciones realizadas en las fases:
    1. Evaluar
    2. Adquirir
    3. Analizar
    4. Informar
iv. Evidencias digitales (los PDF del 2.b), hash de todas las evidencias y método para obtener estos hash. Los ficheros de cada una de las evidencias (sólo 2.b) se incluirán en el ZIP.

e. Entregable. ZIP con al menos:
    i. Informe
    ii. Evidencias digitales (2.b)