Informática Forense y Auditoría

Ejercicios prácticos entregables

Convocatoria diciembre 2024

Los ejercicios prácticos entregables para evaluar las prácticas de laboratorio serán los siguientes:

- **Práctica 2** (1 punto)
  - **Ejercicio 21** (0,25 puntos). Adquisición de evidencia en red incluyendo integridad hash con Bash.
  - **Ejercicio 35** (0,25 puntos). Análisis de evidencia textual con Bash.
  - **Ejercicio 36** (0,25 puntos). Análisis de evidencia textual con Bash.
  - **Ejercicio 37** (0,25 puntos). Análisis de evidencia textual con Bash.

- **Práctica 3** (1,5 puntos)
  - **Ejercicio 1** (0,5 puntos). Carving de imagen JPG con Bash.
  - **Ejercicio 10** (0,5 puntos). Carving de archivos de audio con Autopsy.
  - **Ejercicio 14** (0,5 puntos). Recuperación de evidencias borradas mediante metadatos con Autopsy.

- **Práctica 4** (2,5 puntos)
  - **Ejercicio 8** (apartados: (bb, vv, xx, ccc, fff, iii, mmm, nnn, ppp, rrr, sss) (1,25 puntos). Análisis de imagen física de smartphone con Autopsy.
  - **Ejercicio 9** (apartados: aa, bb, cc, dd, ee, ff, gg, hh, ii, jj) (1,25 puntos). Análisis de imagen lógica de smartphone con Aleapp.

- **Práctica 5a** (4 puntos)
  - **Ejercicio 28** (apartados: i, j, k, l, m, n, o, p, q) (1 punto). Análisis de volcado de memoria principal con Volatility.
  - **Ejercicio 34** (imágenes: 2, 4 y 15) (0,5 puntos). Análisis de metadatos EXIF.
  - **Ejercicio 35** (ficheros: 3, 6 y 9) (0,5 puntos). Análisis de metadatos de ficheros.
  - **Ejercicio 42** (apartados: a, b, c, d, e, f, g, h, i) (1 punto). Análisis de cabeceras de correo electrónico incluyendo recursos OSINT.
  - **Ejercicio 45** (apartados: a, b, c, d, e, f, g) (1 punto). Análisis de registros de servicio móvil.

- **Práctica 5b** (1 punto)
  - **Ejercicio 3** (todos los apartados) (1 punto). Análisis de resolución DNS mediante sondeo de interfaz de red en cliente web con Wireshark.

Normas de presentación y entrega de los ejercicios

- Los ejercicios deberán ser entregados en un documento **Word** (**formato docx**).
- El nombre del documento será el nombre y apellidos del alumno (**sin blancos separatorios**) seguido de un guion alto y **el número de PL asignado oficialmente al alumno**. Por ejemplo, si el alumno se llamase Juan Asturias

y estuviese asignado al grupo PL1, el nombre del fichero debería ser **JuanAsturias-PL1.docx**.

- El documento deberá tener **OBLIGATORIAMENTE** los siguientes apartados:

Portada

- Identificación del autor (Nombre, apellidos, uo y dirección de correo electrónico).
- Fecha de finalización del documento.

Índice

El documento deberá tener un índice que permita localizar rápidamente cada uno de los ejercicios.

Objeto del peritaje

En este apartado deben figurar las preguntas/apartados/ejercicios a los que se deben dar respuesta, como si se tratase de una pericial judicial. Puede figurar simplemente la relación indicada en la página anterior.

Resolución

Por cada pregunta/apartado/ejercicio al que se deba responder, se deberá tener un subapartado (**Práctica X-Ejercicio-Y**-**Apartado-Z**) dentro del apartado de Resolución. Cada subapartado deberá incluir el enunciado del ejercicio correspondiente. Por cada subapartado se deberá seguir una secuencia lógica que guíe al corrector en su resolución:

- **Análisis de la documentación**: en su caso, si fue necesario examinar documentación vinculada a la pregunta/apartado/ejercicio para proceder a su resolución. Indicar qué documentación se examinó/consultó.
- **Toma de pruebas**: en su caso, cómo se realizó la toma de pruebas justificada con capturas de pantalla, (ej.: imagen forense de una partición de un disco).
- **Análisis de las pruebas**: a qué procedimientos de análisis se sometieron las pruebas, ej.: búsqueda de ficheros borrados utilizando técnicas de carving, etc.
- **Resultados obtenidos**: justificados mediante capturas de pantalla y **explicaciones aclaratorias** que el alumno@ crea conveniente. Las **capturas de pantalla** deberán ser **claras**, **visibles (sin necesidad de aumentar el documento al 150%), sin ambigüedades** y **explicativas** de las acciones realizadas, donde **quede claro que se realizan bajo la autoría del alumno (por ejemplo, haciendo visible el nombre de la cuenta que utilizó para realizar el ejercicio)**. **Aquellos ejercicios que se realicen mediante línea de comandos, deberán mostrar el prompt donde deberá aparecer OBLIGATORIAMENTE la cuenta con el nombre del alumno.**
- **Conclusiones preliminares**: si las hubiere, que se deduzcan de los análisis practicados (ej.: se encontraron 12 imágenes borradas de tales tipos y tal tamaño).
- **Conclusiones:** resumen de los resultados obtenidos para cada ejercicio/pregunta/apartado a resolver.

- El tamaño del dicho archivo no podrá exceder de 40MB. En caso de superar este tamaño, deberá comprimir el archivo en formato 7z antes de subirlo a la tarea de entrega en el campus virtual.
- El fichero deberá ser comprobado antes de ser subido por el/la alumn@ utilizando un antivirus. Si al ser descargado por el profesor, dicho archivo está contaminado de alguna manera, se considerará la práctica como no entregada.
- **Al subir el fichero a la tarea se deberá pulsar un botón de aceptación para que la entrega se considere definitiva y no quede como borrador**.
- **Cada alumn@ será responsable del contenido del fichero que suba a la tarea, debiendo comprobar que sea la versión definitiva del mismo antes de la subida.**
- **La tarea de subida de los ejercicios estará disponible desde las 16:00h del 20 de diciembre de 2024 hasta las 16:00h del 22 de diciembre de 2024 inclusive.**
- **NO SE ADMITEN TAREAS RETRASADAS NI ENVÍOS POR OTRO MEDIO DIFERENTE. ABSTENERSE DE ENVIAR LAS TAREA POR CORREO ELECTRÓNICO.**