Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Análisis Forense Informático

UD05. Análisis Forense Informático.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

Caso práctico

María se enfrenta a la parte final de su trabajo: el informe forense.

Sabe que este informe debe recoger el trabajo de duras semanas de análisis de evidencias y extracción de información.

Cualquier actuación realizada relevante debe de estar recogida en el informe, así como las principales conclusiones y análisis técnico realizado. María sabe que si no lo reporta en el informe es como si no se hubiera hecho.

Por otra parte, sabe que, aunque explique técnicamente como se ha llegado a las conclusiones debe también hacer un resumen ejecutivo donde se explique sin tecnicismos las principales conclusiones de la investigación.

¿Qué te pedimos que hagas?

- ✓ **Apartado 1: Análisis de Informe Forense.**

  Esta tarea nos analizaremos un informe forense real, para entender cómo se refleja nuestro trabajo y conclusiones. Veremos qué puntos deberemos de incluir y cuáles podrían haber mejorado nuestro informe.

  - ➢ Puedes encontrar el informe disponible públicamente en: https://buscandojusticia.es/wp-content/uploads/2019/03/DOC.CUATRO.1_2_Censurado-1.pdf

    - PREGUNTA 1: ¿Qué puntos echas de menos dentro del informe?

      Es difícil pronunciarse en este aspecto, tanto por ser el primer informe al que tenemos acceso, como por la información sobre ellos que he podido reunir.

      El hecho, además, de no haber un modelo predeterminado, también deja cierto margen para el trabajo del perito que acaba siendo en este caso una barrera para detectar el correcto desarrollo e implementación del informe.

      Dicho esto, podría remarcar algunos aspectos que o se omiten o no se reflejan de manera correcta:

      - Hay poco detalle respecto a las herramientas utilizadas a lo largo del análisis. Es cierto que nombra WinHex, Izotope Rx o FOCA, pero creo que no queda correctamente reflejado y más cuando va a pasar por personas que posiblemente no reconozcan las mismas.
      - No veo marcado TLP en todo el desarrollo del documento.
      - Tampoco el Alcance, aunque se detalla parcialmente en el resumen ejecutivo, por ejemplo.
      - El resumen ejecutivo, debería mostrar las conclusiones a alto nivel. Entiendo que debe ser escueto, pero parece quedarse excesivamente corto en ese aspecto y estar más centrado en ser un resumen per se.

- PREGUNTA 2: ¿Qué puedes decir del marcado de TLP del informe? ¿Qué grado le darías?

  Como apuntaba anteriormente, no tiene marcado TLP. Al ser un informe referente a un video de un procedimiento judicial y entendiendo que se enmarca en periciales asociadas al mismo, la información requerirá una distribución limitada entre las personas relacionadas con dicho proceso, por lo que utilizaría **TLP:AMBER**

- PREGUNTA 3: ¿Cuáles son las conclusiones del resumen ejecutivo? ¿En qué añadirías y en qué lo basarías?

  Este es otro aspecto ya comentado en el primer apartado. No incluye conclusiones como tal.

  Esperaba ver reflejado a modo general lo aportado en el último apartado.

  Yo lo basaría en el listado de conclusiones que aporta en ese punto y que considera, tras el profundo análisis forense realizado, que no ha habido manipulación del contenido aportado.

- PREGUNTA 4: ¿Qué opinas de la identificación de evidencias?

  En este punto, entiendo que el apartado de evidencias parte del video facilitado, dividido en audio y video sobre los que realiza el análisis y las pruebas periciales.

  Las imágenes gráficas que acompañan el análisis parecen una base sólida para la elaboración del informe, aunque las respuestas, en buena medida vienen dadas por su opinión profesional tras el análisis.

- PREGUNTA 5: ¿Qué opinas del lenguaje usado?

  Hay que pensar que el objetivo es explicar lo sucedido de forma correcta y reproducible. Mantiene un lenguaje apropiado, siendo más general o técnico, según el apartado en el que se encuentre. Es finalmente legible en toda su extensión y bastante concreto.

- PREGUNTA 6: ¿Qué más te llama la atención?

  La ausencia de marcado TLP que identifique visualmente el nivel de intercambio posible de esta información.

  La anonimización de los datos tampoco es correcta. No ha sido nada complejo saber que el perito es Carlos Aldama Sáinz, de Aldama Informática Legal (no me extiendo en el resto de los datos como direcciones, teléfonos, nº de colegiado, todo accesible). Hay también demasiados nombres expuestos que podrían servir como identificadores en un momento dado.

Webgrafía.

https://www.mecd.es/cidead/aulavirtual/course/view.php?id=2367#section-5

https://www.incibe.es/incibe-cert/sobre-incibe-cert/tlp