TAREA 05

DOCUMENTACIÓN Y ELABORACIÓN DE INFORMES DE ANÁLISIS FORENSES

ANÁLISIS FORENSE INFORMÁTICO

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

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.

Apartado 1: Análisis de Informe Forense.
En esta tarea analizaremos un informe forense real, para entender cómo se refleja nuestro trabajo y conclusiones. Veremos qué puntos deberemos incluir y cuáles podrían haber mejorado nuestro informe.
Puedes encontrar el informe en: DOC.CUATRO.1_2_Censurado-1.pdf
https://drive.google.com/file/d/1xB1QosHqXz5NO3TlPAoSL5UY_X1Q3KaX/view?pli=1

PREGUNTA 1: ¿Qué puntos echas de menos dentro del informe?
El informe está bastante técnico y detallado, pero hay algunos aspectos clave que faltan:

- Falta dar un contexto más claro, no se explica en profundidad para qué se analiza el video, ni por qué es importante. Se podría especificar si es una prueba para un juicio o si están poniendo en duda su validez, estos detalles ayudarían a entender mejor la relevancia del análisis.
- Herramienta utilizada, se menciona el análisis del video pero no se especifica que software o técnica se empleó para la verificación. Saber la herramienta que se utilizaron ayudaría a validar el análisis. Por ejemplo si se usaron programas forenses como Amped Authenticate o herramientas para el análisis de metadatos, esto daría más credibilidad al informe.
- Explicaciones visuales, aunque el documento incluya imágenes y capturas, sería útil tener explicaciones más detalladas de cada una y cómo se relacionan con el análisis realizado. Para tener una mejor comprensión del informe, sobre todo para quienes no tengan conocimientos técnicos, se podrían añadir gráficos o diagramas que ilustren los resultados.
- Limitaciones del análisis, se mencionan que hay restricciones, pero no se entra en detalle de cuales son (si es la calidad del video, la falta de datos, ediciones previas...) detallar estas limitaciones ayudaría a entender mejor los posibles errores o incertidumbre del resultado..

PREGUNTA 2: ¿Qué puedes decir del marcado de TLP del informe? ¿Qué grado le darías?
El TLP (Traffic Light Protocol) es un sistema que indica el nivel de confidencialidad de un documento. En este caso, el informe no parece tener marcado explícitamente el TLP, lo cual ya indica un problema, porque este sistema indica la sensibilidad de la información.
Si tuviese que asignar un grado, le daría TLP:AMBER porque parece ser un documento con información sensible relevante en un caso legal, no debería circular libremente, solo debe compartirse con aquellas personas relacionadas con el caso. Esto significa que la información es sensible y debe ser manejada con cuidado, compartida solo con aquellos que necesiten saber para cumplir con sus responsabilidades.
En caso de que el informe debiera ser completamente privado y solo pudiese acceder a él un número muy reducido de personas, podría ser TLP:RED, esto indicaría que la información es extremadamente sensible y su distribución debe limitarse al máximo. Pero si estuviese destinado a un ser público, debería tener una versión con TLP:WHITE, lo que significa que la información puede ser compartida libremente.

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

Las conclusiones sacadas del informe ejecutivo:

- El video no presenta signos de haber sido manipulado.
- La transcripción del audio es precisa y fiable.
- Se garantiza la autenticidad del contenido del video

Se podría añadir:

- Se podría añadir una parte con una explicación del análisis incluyendo términos simples en la que se detalle lo realizado y las conclusiones, sin necesidad de ser experto en informática. Esto ayudaría a que cualquier persona independientemente de su nivel de conocimiento técnico pueda entender el análisis.
- Pruebas visuales que muestren cómo se analizaron las imágenes o el audio. Esto proporciona una representación visual de los hallazgos, haciendo que el informe sea más fiable y entendible.
- Indicar consecuencias según el resultado del análisis, en caso de que el video fuese falso indicar las consecuencias que hubiese podido haber y en caso de ser verdadero cómo afecta al proceso legal. Además de indicar el margen de error existente y que pruebas respaldan esa resolución. Esto ayudaría a entender las implicaciones legales de los resultados obtenidos.

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

La identificación de evidencias está bien estructurada y es bastante precisa, pero algunos aspectos podrían mejorarse. La parte positiva sería que se documentan momentos clave del video con las marcas de tiempo y se menciona el uso de técnicas forenses para garantizar que el video no ha sido editado. Como partes a mejorar se podrían destacar:

- Informar acerca de la cadena de custodia, no se explica cómo se obtuvo el video, quién lo entregó y cómo se asegura que no fue alterado antes del análisis. Detallar la cadena de custodia ayudaría a demostrar la integridad de esa información.
- No se menciona si analizaron los metadatos, como la fecha de creación, posibles modificaciones, dispositivos usados… Revisar los metadatos proporciona información adicional sobre su autenticidad.
- Realizar una doble verificación, no se detalla qué técnicas usaron para descartar manipulaciones, ni indican una contrastación con varias herramientas.Utilizar múltiples herramientas y técnicas para realizar las verificaciones, demuestra la autenticidad del video y por tanto la fiabilidad del análisis.

PREGUNTA 5: ¿Qué opinas del lenguaje usado?

El lenguaje usado en el informe es técnico y formal, lo cual es adecuado para un documento pericial. Mantiene una estructura ordenada y clara para expertos en la materia. Sin embargo, para alguien sin mucho conocimiento en informática forense podría resultar complicado, por tanto sería útil incluir explicaciones más sencillas y ejemplos para hacer el contenido más entendible a personas con menos nivel en la materia.

- Se deduce que es un informe técnico por no aclarar términos que podrían ser desconocidos para una persona sin formación técnica, falta claridad en las explicaciones y faltarían ejemplos para apoyar los hallazgos.
- Está bien para un informe legal, pero se agradecería un poco más de claridad en las explicaciones. Utilizar un lenguaje más accesible y menos técnico ayudaría a que el informe sea comprensible para un público más amplio.

PREGUNTA 6: ¿Qué más te llama la atención?

- El análisis del comportamiento de las personas dentro del video proporciona información adicional relevante para el caso, no se limita solo a verificar la autenticidad de la grabación, esto sugiere que puede ser parte de una investigación judicial.
- Se hace un estudio exhaustivo de la transcripción del video, no solo se analiza la imagen, lo que refuerza su autenticidad. La transcripción es crucial para garantizar que el contenido es auténtico y no ha sido manipulado.
- No queda clara la conclusión definitiva sobre su autenticidad, se hacen observaciones sobre el video pero no se afirma su veracidad. Sería útil tener una conclusión clara y definitiva.
- La estructura del informe está bien estructurada pero se repiten aspectos sin aportar nueva información. Se debería mejorar la estructura del informe para evitar repeticiones y dar la máxima información relevante a la vez.

En conclusión el informe es sólido y bien estructurado, pero podría mejorar en claridad y profundidad, desarrollando y explicando con lenguaje menos técnico algunos conceptos. Faltan detalles técnicos sobre el software y los métodos utilizados, una mejor identificación de la evidencia, como su origen o finalidad y una explicación más accesible del análisis. Además, no tiene un marcado TLP, lo que podría generar dudas sobre la confidencialidad del documento.