[Curso de Informática Forense](https://platzi.com/clases/forense/)

**ArtículoElaborar un informe a partir de los resultados obtenidos en cada una de las etapas de análisis**

[**Juan Pablo Caro**](https://platzi.com/@juanpcaro)

23 de Mayo de 2019

Hace un par de módulos elaboraste tu informe preliminar. Ahora vamos a ampliar un poco cada una de las secciones para incluir la información que encontraste en tu etapa de análisis. Vamos a ir paso por paso:

1. **Introducción al caso**: ¿Qué ha cambiado? ¿Has incluido nueva información? ¿Ha cambiado en algo el contexto del caso? Si no, probablemente el contenido sea muy similar al de tu informe.
2. **Resumen general**: Deberías incluir ahora todas las actividades realizadas, pero especialmente enfocándote en las que te dieron resultados más importantes.
3. **Inventario de evidencia identificada**: Este inventario probablemente siga siendo el mismo.
4. **Reportes de adquisición de evidencia**: En este punto, tal vez tengas algo más de información técnica. Además de los reportes de adquisición, puedes tener informes técnicos de herramientas que hayas usado para el análisis.
5. **Información general de los sistemas preservados**: Si no has incluido evidencia nueva, tal vez la información en esta sección no haya cambiado.
6. **Información encontrada en las imágenes forenses**: Esta es una de las secciones que probablemente más cambios tuvieron. Prepara la información técnica de los resultados de todos tus análisis.
7. **Hallazgos preliminares, si existen**: Aquí ya no vamos a hablar de hallazgos preliminares, sino de todos los hallazgos que encontraste. ¿Qué fue lo más importante o significativo?, ¿Cuál es el dato o la respuesta más relevante?, ¿Vale la pena incluir un análisis de línea de tiempo?
8. **Siguientes pasos**: Puede ser que no haya siguientes pasos en la investigación, pero tal vez sí tienes recomendaciones para tu cliente o para quien reciba tus resultados. Tal vez mejorar su sistema de seguridad, instalar algún parche en particular. Este tipo de sugerencias dan mucho valor agregado a tu trabajo. Debes incluirlas cada vez que puedas.

Recuerda que este proceso debes poder hacerlo independientemente de las herramientas que uses o el contexto de la investigación en la que estés. Como reto para este módulo, deberás elaborar un primer borrador de tu informe, actualizando la información que obtuviste como parte del análisis. Más adelante estaremos ordenando esta información en dos informes separados.