8. CONCLUSIONES

- Hoy en día es posible encontrar al alcance de cualquiera, un conjunto de herramientas para manipulación de archivos, que integradas de manera correcta y bajo un método formal como el propuesto en la presente tesis, permite a investigadores y otros interesados en el tema de recuperación y visualización de archivos una aproximación acertada que puede llevar de manera exitosa a la identificación precisa de los mismos, partiendo siempre del supuesto que estos son legibles.

- Los métodos y herramientas disponibles para la identificación de archivos incompletos, dañados o corruptos no son ciento por ciento seguros y eficaces, debido a que las características que deben estar disponibles en los archivos para su recuperación e identificación plena, no siempre están presentes. Adicionalmente, requieren de mucha pericia por parte de las personas que los usan.

- Los archivos tienen en su estructura interna un conjunto de datos a partir de los cuales se determina cómo se hará la visualización. Ésta puede hacerse efectiva dependiendo del número de parámetros que la herramienta visualizadora considere como obligatorios, pues en algunas ocasiones es imposible definir acertadamente todos los metadatos que se ubican en los encabezados del archivo.

- Para construir los formateadores de archivo es necesario disponer del documento de especificación del formato, pues en él se consigna la forma cómo funciona el formato. En algunas ocasiones, acceder a este

documento puede ser difícil, porque si es un formato abierto, los desarrolladores pueden no haberse tomado el tiempo para definir la especificación, o si es un formato propietario, pagar por el documento podría ser algo costoso.

- El método de medición de la entropía, usando los parámetros especificados en este proyecto, aunque es usado para identificar los formatos en archivos, se descarta como una medida confiable y acertada, excepto para formatos comprimidos, como son: mp3, zip y jpg, en los cuales se evidenció una entropía alta, lo cual permite que sean más fácilmente diferenciables usando el programa generado en el proyecto.

- Es importante que las personas que cuenten con la extensión del archivo sobre el cual están trabajando y que siguen el método propuesto en este documento, se apoyen en los recursos expuestos, que han demostrado contar con la experiencia e investigación necesaria – incluso con base de datos que pueden ser consultadas-, para determinar el formato al que corresponde y el software con el cual puede ser visualizado.

- Los visores hexadecimales son herramientas de funcionalidades muy similares, sólo muy pocos, como el de las plantillas, resultan apropiados para el método expuesto, ya que preparan de manera ágil y fácil, la manipulación de los archivos para proceder a su identificación y recuperación con los pasos aquí presentados.

9. RECOMENDACIONES

- En nuestro proyecto de grado exponemos ilustrativamente los formateadores para archivos de audio WAV y archivos de imagen BMP. Queda abierta la posibilidad de desarrollar otras herramientas que formateen archivos de otro tipo y que complementen el método propuesto.

- Explorar la posibilidad de complementar los visores hexadecimales existentes con el uso de plantillas que estructuren un archivo

- Se debe desarrollar un trabajo futuro para determinar el uso real de la entropía. Los resultados obtenidos no son concluyentes, hecho que llama la atención porque en el artículo *Sliding Window Measurement for FileType Identification* plantean la entropía como una buena alternativa. Como se mencionó anteriormente, una exploración más a fondo está fuera del alcance de este trabajo, pero es importante diseñar una validación experimental más sofisticada de esta hipótesis.