

CONTENIDO

1. INTRODUCCIÓN.....	1
2. FORMULACIÓN DEL PROBLEMA	3
3. OBJETIVOS.....	5
3.1 OBJETIVO GENERAL.....	5
3.2 OBJETIVOS ESPECÍFICOS	5
4. MARCO REFERENCIAL	6
4.1 COMPUTACIÓN FORENSE.....	6
4.2 EVIDENCIA DIGITAL	8
4.3 FORMATO DE ARCHIVO	10
4.4 PROCEDIMIENTO PARA EL MANEJO DE INVESTIGACIONES FORENSES	11
4.4.1 Planeación	11
4.4.2 Recolección.....	11
4.4.3 Aseguramiento	12
4.4.4 Análisis.....	12
4.4.5 Presentación de la evidencia digital	12
4.5 TEORÍA DE LA INFORMACIÓN.....	13
4.5.1 Entropía.....	16
4.6 SOFTWARE LIBRE	20

4.7	RECONOCIMIENTO DE PATRONES.....	20
4.7.1	Búsquedas de proximidad.....	22
4.7.2	Reconocimiento de patrones y aproximación de funciones	22
4.7.3	Espacios Métricos	23
4.7.4	Consultas de proximidad.....	24
5.	ESTADO DEL ARTE.....	25
5.1	IDENTIFICACIÓN DEL FORMATO DEL ARCHIVO.....	25
5.1.1	Extensión del nombre del archivo	25
5.1.2	Número mágico.....	26
5.1.3	Comando <i>File</i>	28
6.	MÉTODO PROPUESTO.....	32
6.1	ETAPA 1: Identificación del archivo.....	32
6.1.1	Identificar la extensión del archivo	33
6.1.2	Determinar si el archivo es texto	34
6.1.3	Ejecutar el comando <i>file</i>	34
6.1.4	Identificar el número mágico	35
6.1.5	Utilizar herramientas y librerías públicas de identificación	36
6.1.6	Medición de la Entropía en los archivos.....	37
6.2	ETAPA 2: Formateado o reconstrucción del archivo	45

6.2.1	Formateador BMP	46
6.2.2	Formateador WAV.....	50
6.3	ETAPA 3: Visualización	53
7.	EJEMPLO DE APLICACIÓN DEL MÉTODO.....	54
8.	CONCLUSIONES	68
9.	RECOMENDACIONES.....	70
	BIBLIOGRAFÍA	71

TABLAS

Tabla 1: Ejemplos de números mágicos para formatos de archivo comunes	27
Tabla 2: Muestra de archivos para la medición de la entropía.....	40
Tabla 3: Encabezado del archivo BMP	47
Tabla 4: Información del Bitmap	48
Tabla 5: Encabezado RIFF del archivo WAV	50
Tabla 6: Encabezado format del archivo WAV	51
Tabla 7: Encabezado de datos del archivo WAV	51

ILUSTRACIONES

Ilustración 1: Página de búsqueda de tipos de archivo por extensión	33
Ilustración 2: Identificación del número mágico en un archivo PDF	35
Ilustración 3: Valores de entropía para un archivo .doc	41
Ilustración 4: Valores de entropía para un archivo .doc. Tomada de artículo: "Sliding Window Measurement for File Type Identification"	41
Ilustración 5: Gráfica de valores consolidados promediados para 1229 archivos .doc	42
Ilustración 6: Gráfica de valores promediados para formato .doc. Tomada de artículo: "Sliding Window Measurement for File Type Identification"	42
Ilustración 7: Valores de entropía para un archivo .mp3.....	43
Ilustración 8: Gráfica de valores consolidados promediados para 2812 archivos .mp3.....	43
Ilustración 9: Gráfica de valores promediados para formato .mp3. Tomada de artículo: "Sliding Window Measurement for File Type Identification"	44
Ilustración 10: Visualización del archivo en un editor hexadecimal.....	54
Ilustración 11: Uso del comando strings en archivoPrueba	55
Ilustración 12: Uso del comando file sobre el archivo de prueba	56
Ilustración 13: Visualización de los primeros bytes del archivo.....	57
Ilustración 14: Modificación del número mágico en el archivo de prueba	58

Ilustración 15: Salida del comando file para el archivo con el número mágico alterado.....	58
Ilustración 16: Valores entropía para archivoPrueba	59
Ilustración 17: Gráfica valores entropía para el archivo de prueba	60
Ilustración 18: Imagen bmp0.bmp.....	62
Ilustración 19: Imagen bmp1.bmp.....	63
Ilustración 20: Imagen bmp2.bmp.....	64
Ilustración 21: Imagen bmp3.bmp.....	65
Ilustración 22: Imagen bmp4.bmp.....	66
Ilustración 23: Imagen bmp5.bmp.....	67