

Instituto Tecnológico de San Juan del Río



Tópicos de Ciberseguridad

Actividad 3: Reconstrucción del código fuente (Ghidra)

P R E S E N T A:

Ingeniería Sistemas Computacionales
Hernández Lucio Isaac
21590386

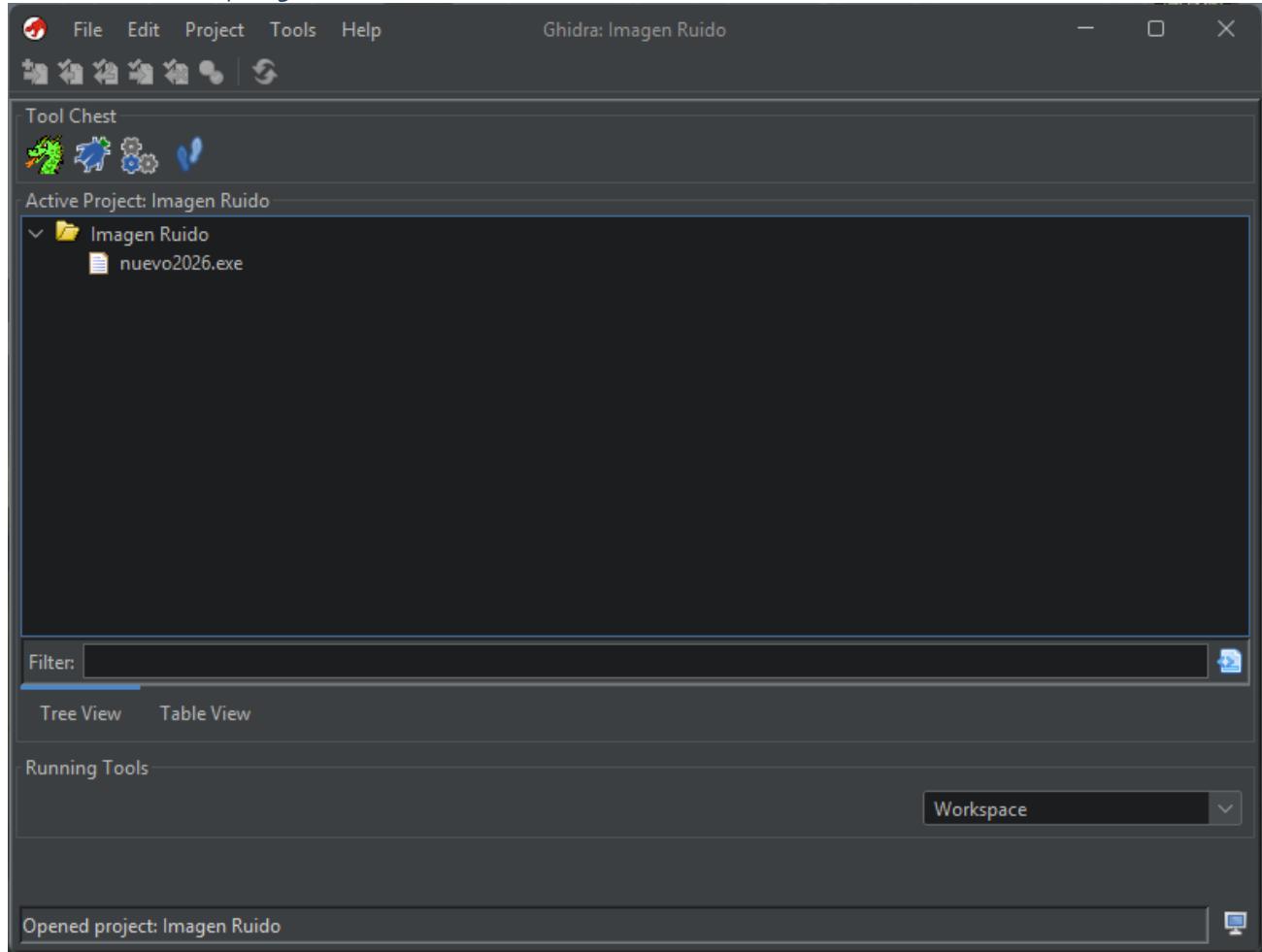
Martínez Yáñez Alexis Jonathan
21590291

Uribe Callejas José Uriel
21021001

ENE-JUL 2026



Creación del proyecto en Ghidra



Función y código descompilado.

```

1 undefined4 FUN_00401000(void)
2 {
3     int iVar1;
4     time_t tVar2;
5
6     tVar2 = time((time_t *)0x0);
7     DAT_00401000 = (uint)tVar2;
8     srand(DAT_00401000);
9     FILE *iVar3 = fopen("nuevo2026.ppm", "w");
10    if(iVar3 != 0)
11        fprintf(iVar3, "#define width 640\n#define height 480\n#define maxColor 255\n");
12    for(iVar1 = 0; iVar1 < height; iVar1 = iVar1 + 1)
13        for(iVar1 = 0; iVar1 < width; iVar1 = iVar1 + 1)
14            iVar1 = rand();
15            iVar3 = (undefined4)(iVar1 % 6);
16            fwrite(iVar3, 0x1, 1, iVar3);
17            iVar1 = rand();
18            iVar3 = (undefined4)(iVar1 % 6);
19            fwrite(iVar3, 0x1, 1, iVar3);
20            iVar1 = rand();
21            iVar3 = (undefined4)(iVar1 % 6);
22            fwrite(iVar3, 0x1, 1, iVar3);
23        }
24    fclose(iVar3);
25    return 0;
26 }
27
28
29

```

Una vez que el ejecutable esté cargado se muestra la interfaz, la pantalla principal es una ventana con el código desensamblado mientras que la pantalla de la izquierda muestra una de las funciones descompilado que en este caso es la función principal.

Análisis del código descompilado (Función: FUN_00401000).

Esta función genera un archivo PPM (Portable Pixmap) llamado “nuevo2026.ppm” con datos aleatorios.

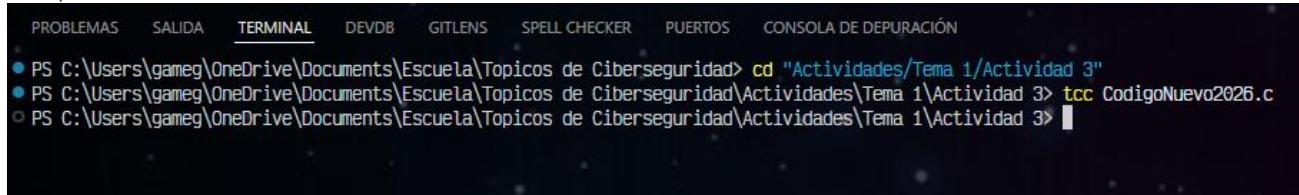
Datos del archivo generado:

- Ancho: 0x280 = 640 píxeles
- Alto: 0x1E0 = 480 píxeles
- Formato: PPM binario P6

Reinterpretación de código.

```
● ● ●  
1 #include <stdio.h>  
2 #include <stdlib.h>  
3 #include <time.h>  
4  
5 int main(void)  
6 {  
7     FILE *archivo;  
8     time_t semilla;  
9     int i, j;  
10    int color;  
11    unsigned char paleta[6] = {0, 50, 100, 150, 200, 250}; // Colores de la paleta  
12  
13    // Inicializar generador de números aleatorios  
14    semilla = time(NULL);  
15    srand((unsigned int)semilla);  
16  
17    // Abrir archivo PPM  
18    archivo = fopen("nuevo2026.ppm", "+wb");  
19    if (archivo == NULL)  
20        return 1;  
21  
22    // Escribir encabezado PPM (P6 640 480 255)  
23    fprintf(archivo, "P6\n640 480\n255\n");  
24  
25    // Generar imagen de 480 filas x 640 columnas  
26    for (i = 0; i < 480; i++)  
27    { // 0x1e0 = 480  
28        for (j = 0; j < 640; j++)  
29        { // 0x280 = 640  
30            // Escribir 3 componentes RGB aleatorios  
31            color = rand() % 6;  
32            fwrite(&paleta[color], 1, 1, archivo); // R  
33  
34            color = rand() % 6;  
35            fwrite(&paleta[color], 1, 1, archivo); // G  
36  
37            color = rand() % 6;  
38            fwrite(&paleta[color], 1, 1, archivo); // B  
39        }  
40    }  
41  
42    fclose(archivo);  
43    return 0;  
44 }
```

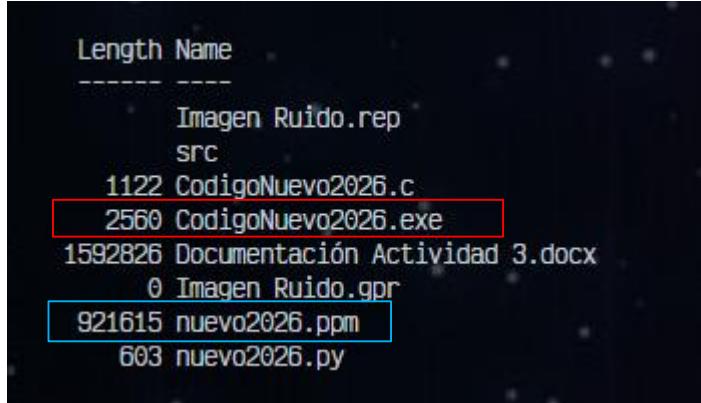
Compilación



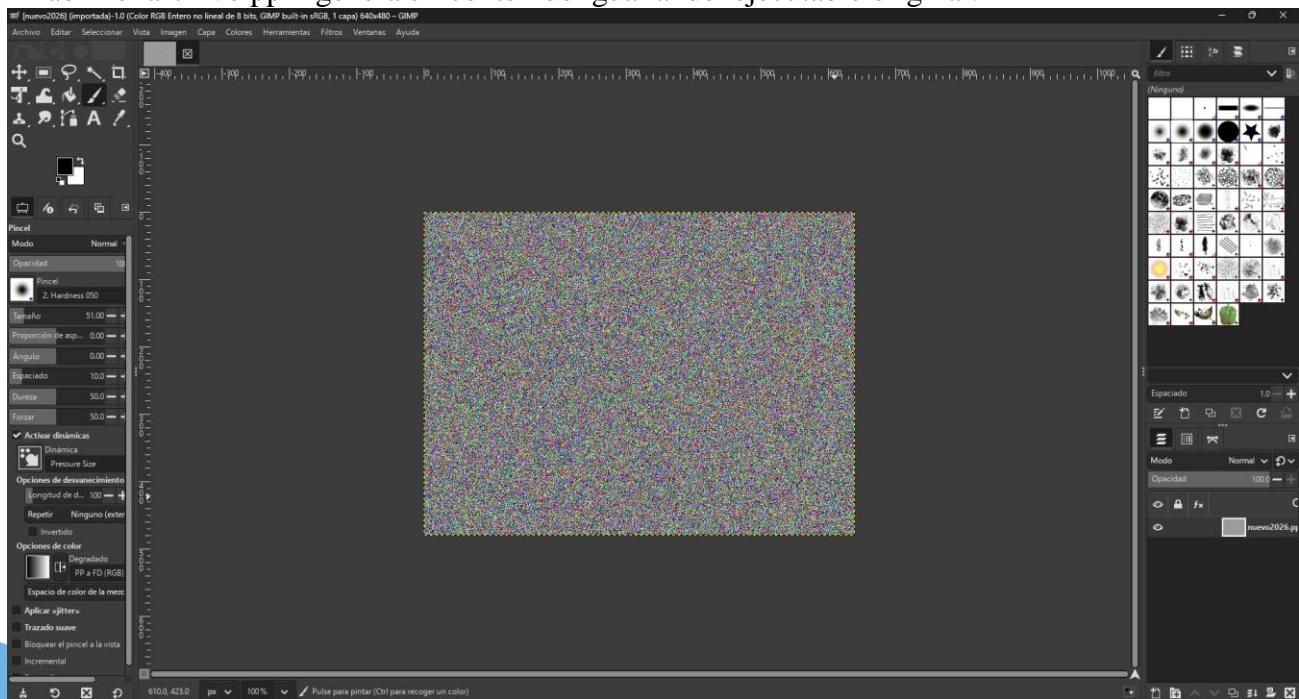
```
PROBLEMAS SALIDA TERMINAL DEVDB GITLENS SPELL CHECKER PUERTOS CONSOLA DE DEPURACIÓN

● PS C:\Users\gameg\OneDrive\Documents\Escuela\Topicos de Ciberseguridad> cd "Actividades/Tema 1/Actividad 3"
● PS C:\Users\gameg\OneDrive\Documents\Escuela\Topicos de Ciberseguridad\Actividades\Tema 1\Actividad 3> tcc CódigoNuevo2026.c
○ PS C:\Users\gameg\OneDrive\Documents\Escuela\Topicos de Ciberseguridad\Actividades\Tema 1\Actividad 3>
```

Una vez compilado el código, genera este ejecutable y al ejecutarlo crea el archivo ppm:



Al abrir el archivo ppm genera un contenido igual al del ejecutable original:



Comparaciones

The image shows two side-by-side Windows file property dialogs. The left dialog is titled 'Propiedades de nuevo2026.exe' and the right one is titled 'Propiedades de CodigoNuevo2026.exe'. Both dialogs have tabs for 'Seguridad', 'Detalles', and 'Versiones anteriores'. Under the 'Seguridad' tab, they both show the file name and a blue folder icon. Under the 'Detalles' tab, they both show the file type as 'Aplicación (.exe)', descriptions ('nuevo2026.exe' and 'CodigoNuevo2026.exe'), and paths ('C:\Users\gameg\OneDrive\Documents\Escue'). Under the 'Versiones anteriores' tab, they both show sizes of 2.00 KB (2,048 bytes) and 4.00 KB (4,096 bytes). A large blue speech bubble labeled 'Ejecutable Original' points to the left window, and another blue speech bubble labeled 'Ejecutable Reconstruido' points to the right window.

Propiedades de nuevo2026.exe		Propiedades de CodigoNuevo2026.exe	
Seguridad	Detalles	Seguridad	Detalles
General	Compatibilidad	General	Compatibilidad
	nuevo2026.exe		CodigoNuevo2026.exe
Tipo de archivo:	Aplicación (.exe)	Tipo de archivo:	Aplicación (.exe)
Descripción:	nuevo2026.exe	Descripción:	CodigoNuevo2026.exe
Ubicación:	C:\Users\gameg\OneDrive\Documents\Escue	Ubicación:	C:\Users\gameg\OneDrive\Documents\Escue
Tamaño:	2.00 KB (2,048 bytes)	Tamaño:	2.50 KB (2,560 bytes)
Tamaño en disco:	4.00 KB (4,096 bytes)	Tamaño en disco:	4.00 KB (4,096 bytes)

Como se puede apreciar los ejecutables tienen un tamaño similar, aunque tengan esa ligera diferencia, el código nuevo hace exactamente el mismo proceso.

Conclusiones

La reconstrucción del código fuente a partir del ejecutable mediante el uso de Ghidra, permitió recuperar la funcionalidad del programa original. El código obtenido fue capaz de generar archivos PPM idénticos, lo que quiere decir que la lógica se mantuvo.

Pero este proceso de ingeniería inversa tiene algunas limitaciones. Durante la compilación se pierde información relevante como los nombres originales de variables y detalles del código. Aunque la funcionalidad sea la misma, los ejecutables recompilados no coinciden byte a byte con el binario original.

A pesar de esto, la ingeniería inversa es una herramienta muy importante, como la auditoría de seguridad, el análisis de malware y la recuperación o mantenimiento de software legado.