



EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



TECNOLÓGICO
NACIONAL DE MÉXICO®



Instituto Tecnológico de San Juan del Río

Ingeniería en Sistemas Computacionales

Tópicos de Ciberseguridad

Reconstrucción de un Código Fuente usando Ghidra

P R E S E N T A:

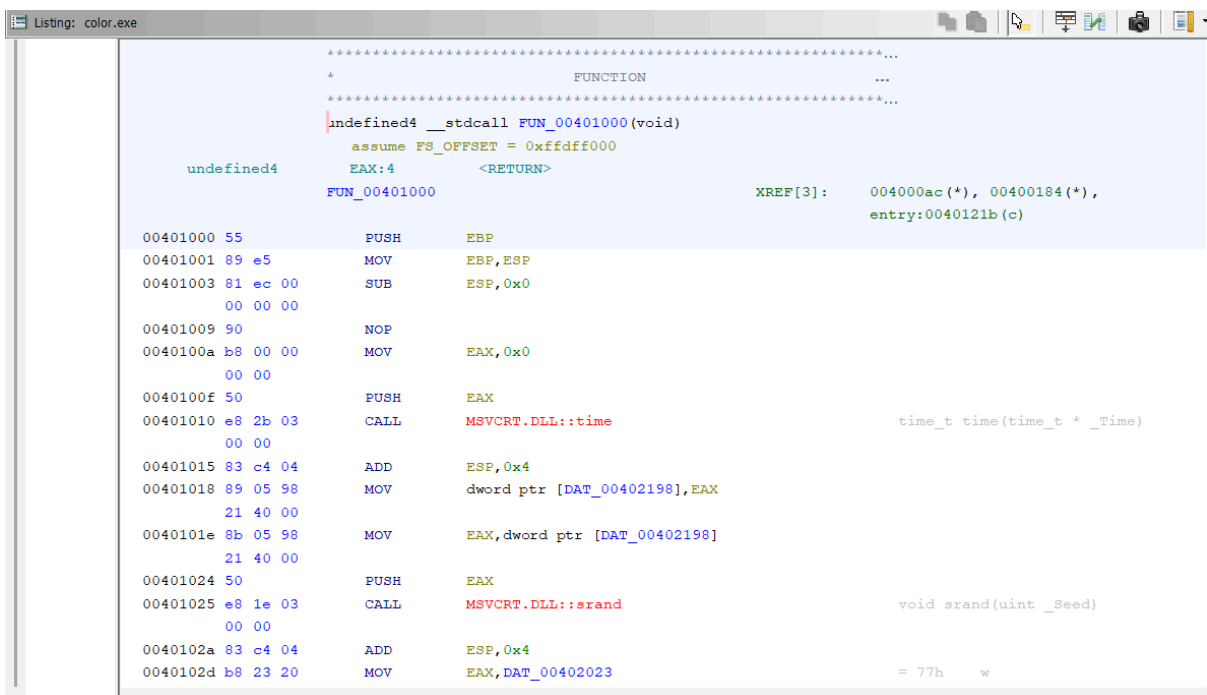
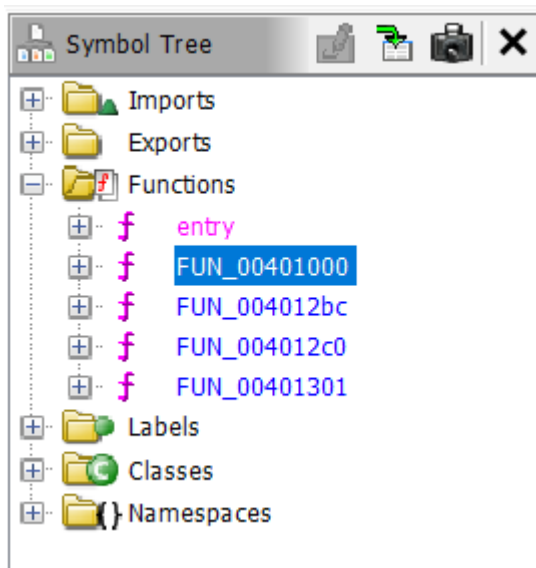
Edgar Alfredo Torres Trujillo - 21590398

Jose Luis Velazquez Trejo - 21590299

López Arteaga Giovanni - 21590287

San Juan del Río, Querétaro a 11 de Septiembre 2025

Desensamblado del ejecutable:




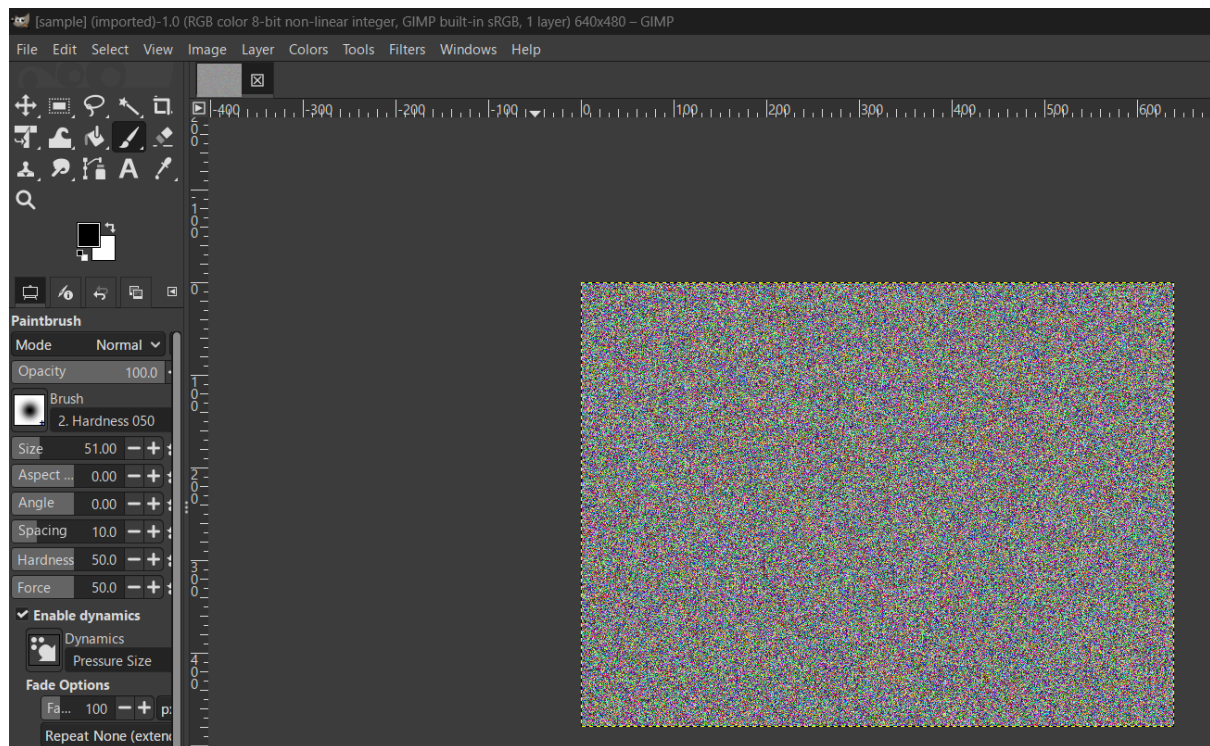
Decompilado de la función principal

```
Decompile: FUN_00401000 - (color.exe)
1
2 undefined4 FUN_00401000(void)
3
4 {
5     int iVar1;
6     time_t tVar2;
7
8     tVar2 = time((time_t *)0x0);
9     DAT_00402198 = (uint)tVar2;
10    srand(DAT_00402198);
11    DAT_0040219c = fopen(s_sample.ppm_00402018,&DAT_00402023);
12    fwrite(&DAT_00402000,1,0xf,DAT_0040219c);
13    for (DAT_00402010 = 0; DAT_00402010 < 0x1e0; DAT_00402010 = DAT_00402010 + 1) {
14        for (DAT_00402014 = 0; DAT_00402014 < 0x280; DAT_00402014 = DAT_00402014 + 1) {
15            iVar1 = rand();
16            DAT_0040200f = (undefined1)(iVar1 % 0x100);
17            fwrite(&DAT_0040200f,1,1,DAT_0040219c);
18            iVar1 = rand();
19            DAT_0040200f = (undefined1)(iVar1 % 0x100);
20            fwrite(&DAT_0040200f,1,1,DAT_0040219c);
21            iVar1 = rand();
22            DAT_0040200f = (undefined1)(iVar1 % 0x100);
23            fwrite(&DAT_0040200f,1,1,DAT_0040219c);
24        }
25    }
26    fclose(DAT_0040219c);
27    return 0;
28 }
```

Invocación del ejecutable:

```
C:\Windows\System32\cmd.e  x  +  v
C:\Users\edgar\OneDrive\Nueva carpeta\Documentos\Noveno semestre\Topicos de ciberseguridad\tcc-0.9.27-win32-bin\tcc>color.exe
C:\Users\edgar\OneDrive\Nueva carpeta\Documentos\Noveno semestre\Topicos de ciberseguridad\tcc-0.9.27-win32-bin\tcc>
```

Name	Date modified	Type	Size
 sample	9/15/2025 10:21 PM	PPM File	901 KB



Conversión a código C:

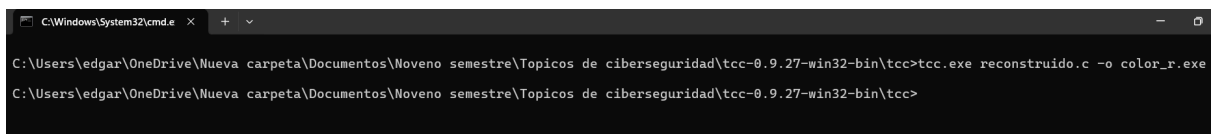
```
reconstruido.c x
1  #include <stdio.h>
2  #include <stdlib.h>
3  #include <time.h>
4
5  int main(void)
6  {
7      FILE *file;
8      int i, j;
9      int random_value;
10     unsigned char pixel_component;
11
12     // Cabecera PPM (P6 indica formato binario, 640x480, máximo valor 255)
13     const char *ppm_header = "P6\n640 480\n255\n";
14
15     // Inicializar generador de números aleatorios
16     srand((unsigned int)time(NULL));
17
18     // Abrir archivo para escritura binaria
19     file = fopen("sample_reconstructed.ppm", "wb");
20     if (file == NULL) {
21         printf("Error: No se pudo crear el archivo\n");
22         return 1;
23     }
24 }
```

```

25 // Escribir cabecera PPM (15 bytes)
26 fwrite(ppm_header, 1, 15, file);
27
28 // Generar imagen de 480x640 píxeles (alto x ancho)
29 for (i = 0; i < 480; i++) { // 0x1e0 = 480 decimal
30     for (j = 0; j < 640; j++) { // 0x280 = 640 decimal
31         // Componente Rojo (0-255)
32         random_value = rand();
33         pixel_component = (unsigned char)(random_value % 256);
34         fwrite(&pixel_component, 1, 1, file);
35
36         // Componente Verde (0-255)
37         random_value = rand();
38         pixel_component = (unsigned char)(random_value % 256);
39         fwrite(&pixel_component, 1, 1, file);
40
41         // Componente Azul (0-255)
42         random_value = rand();
43         pixel_component = (unsigned char)(random_value % 256);
44         fwrite(&pixel_component, 1, 1, file);
45     }
46 }
47
48 fclose(file);
49 printf("Archivo sample_reconstructed.ppm generado exitosamente\n");
50 printf("Dimensiones: 640x480 pixels (formato PPM P6)\n");
51
52 return 0;
53 }

```

Compilación del código reconstruido:



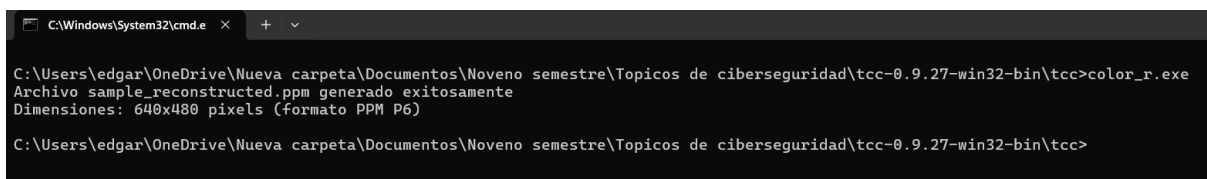
```

C:\Windows\System32\cmd.exe
C:\Users\edgar\OneDrive\Nueva carpeta\Documentos\Noveno semestre\Topicos de ciberseguridad\tcc-0.9.27-win32-bin\tcc>tcc.exe reconstruido.c -o color_r.exe
C:\Users\edgar\OneDrive\Nueva carpeta\Documentos\Noveno semestre\Topicos de ciberseguridad\tcc-0.9.27-win32-bin\tcc>

```

Name	Date modified	Type	Size
color_r	9/15/2025 10:25 PM	Application	3 KB

Invocación al nuevo ejecutable que realiza la misma función:



```

C:\Windows\System32\cmd.exe
C:\Users\edgar\OneDrive\Nueva carpeta\Documentos\Noveno semestre\Topicos de ciberseguridad\tcc-0.9.27-win32-bin\tcc>color_r.exe
Archivo sample_reconstructed.ppm generado exitosamente
Dimensiones: 640x480 pixels (formato PPM P6)
C:\Users\edgar\OneDrive\Nueva carpeta\Documentos\Noveno semestre\Topicos de ciberseguridad\tcc-0.9.27-win32-bin\tcc>

```

Resultado final:

