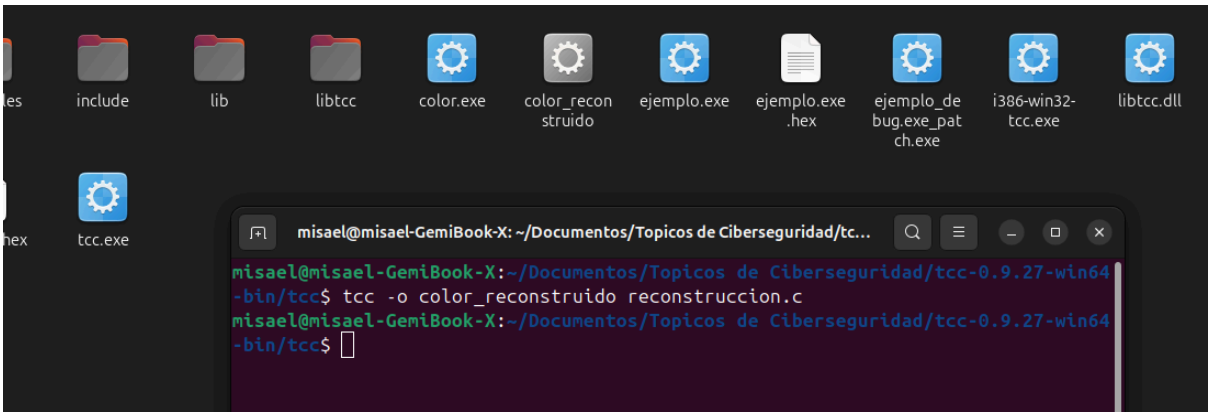
Instituto Tecnológico de San Juan del Río

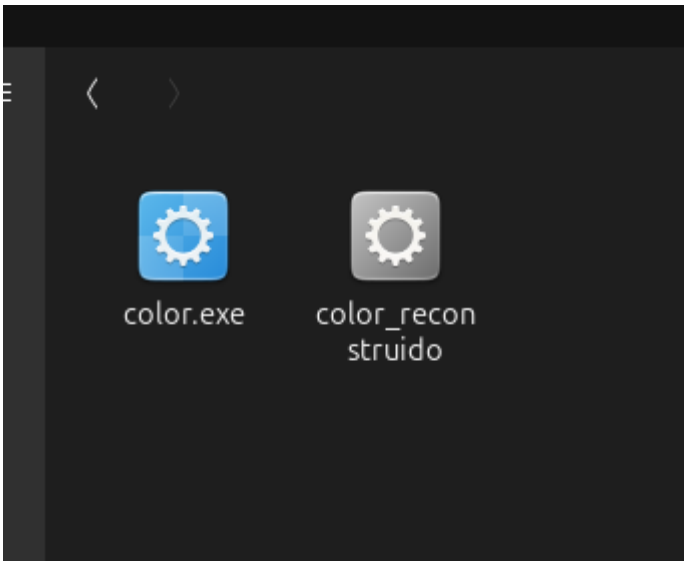
Topicos de Ciber Seguridad

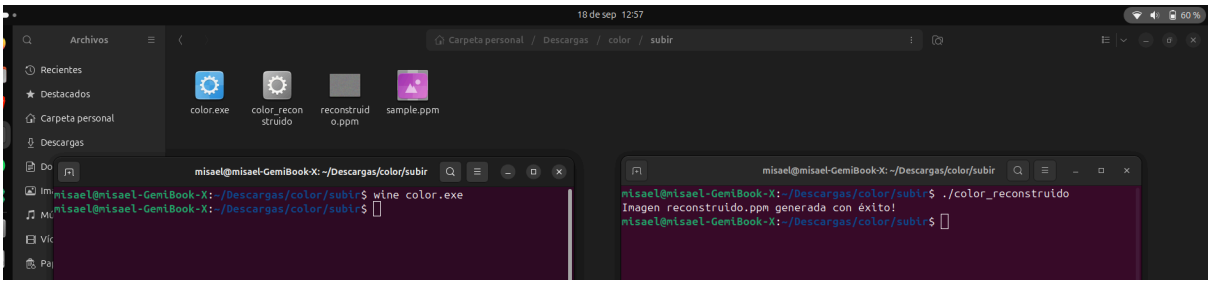
Ghidra comparacion

PERIODO

AGOSTO- DICIEMBRE 2025







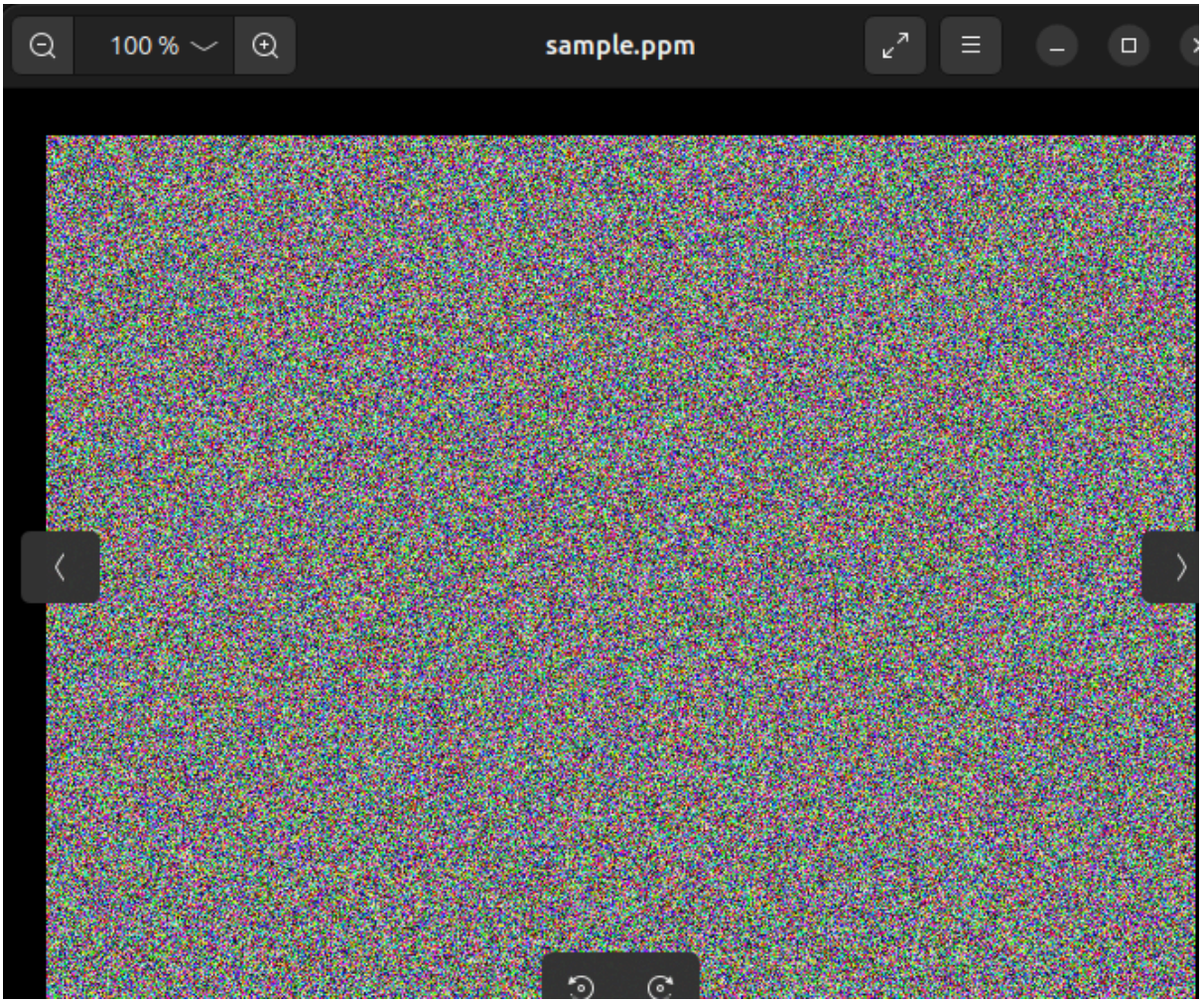
Proceso de compilación usando TCC (Tiny C Compiler):

- **Comando:** `tcc -o color_reconstruido reconstruccion.c`
- **Compilación exitosa sin errores**
- **Generación del ejecutable** `color_reconstruido`
- **Comparación visual entre el original (**`color.exe`**) y el reconstruido**

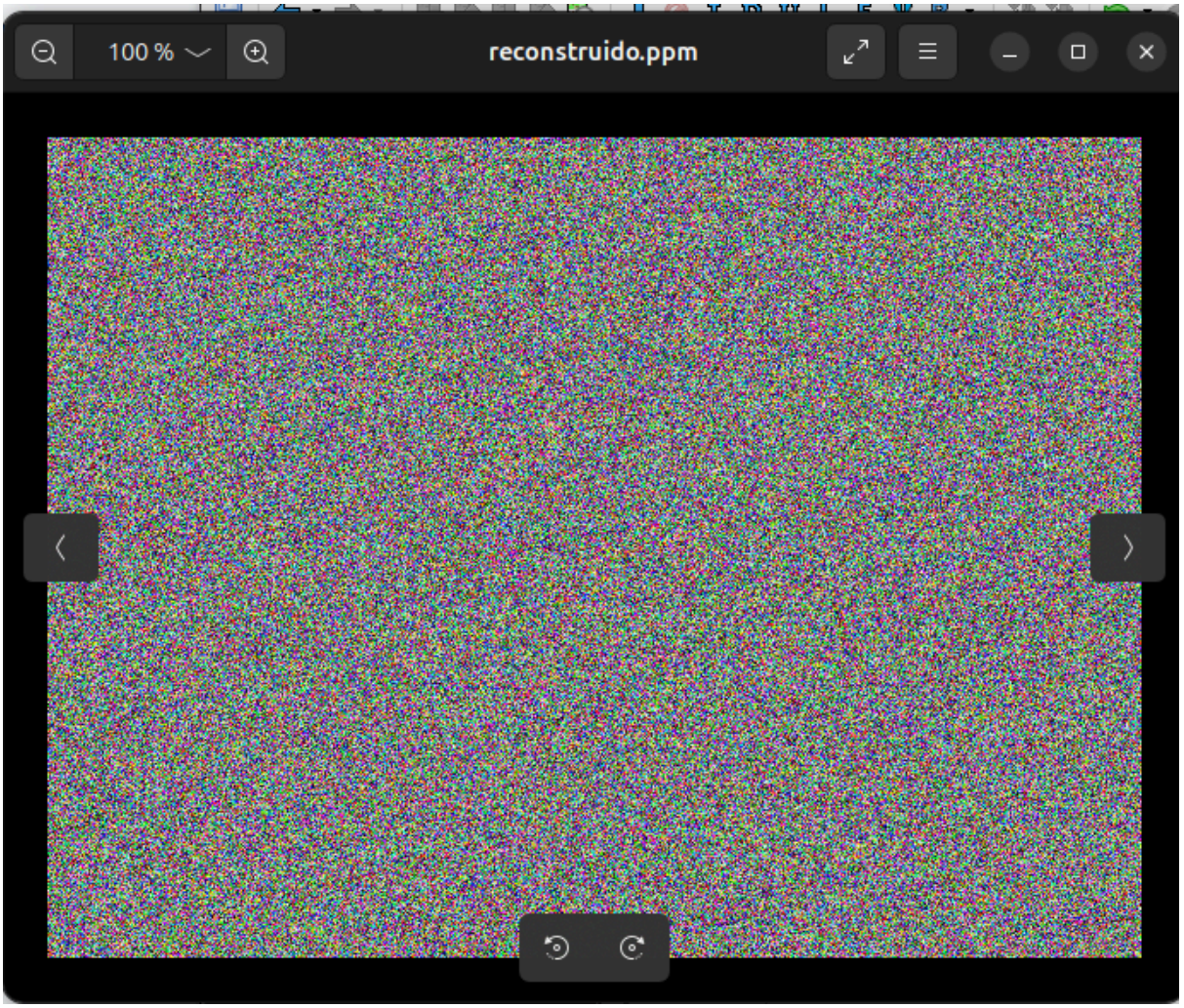
Comparaciones
ódigo C reconstruido basado en el análisis de Ghidra:

- **Implementación fiel de la lógica descompilada**
- **Uso de `time()` y `srand()` para aleatoriedad**
- **Generación de imágenes PPM 640x480**
- **Estructura idéntica a la función `FUN_00401000`**

original (color.exe):

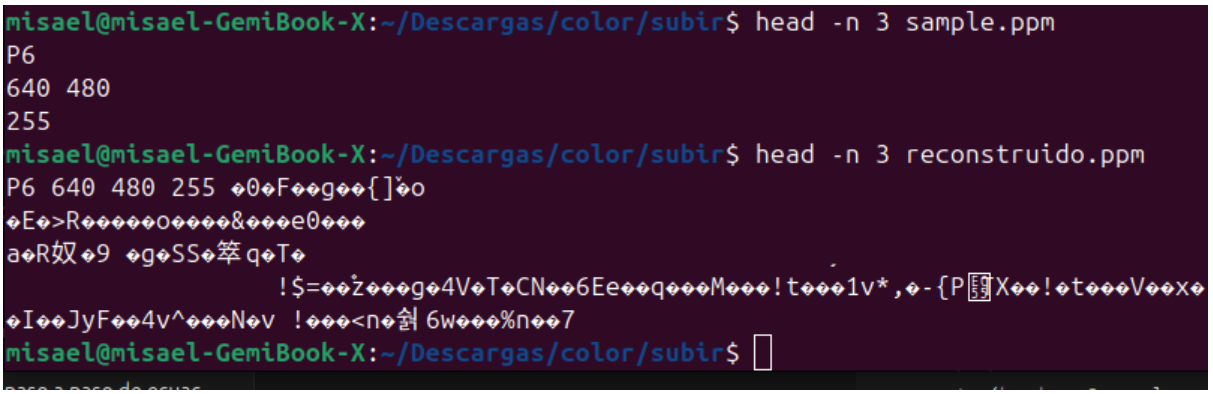


reconstruido codigo fuente(ghidra):




```
misael@misael-GemiBook-X: ~/Descargas/color/subir
misael@misael-GemiBook-X:~/Descargas/color/subir$ ls -la sample.ppm reconstruido
.ppm
-rw-rw-r-- 1 misael misael 921615 sep 18 12:57 reconstruido.ppm
-rw-rw-r-- 1 misael misael 921615 sep 18 12:57 sample.ppm
misael@misael-GemiBook-X:~/Descargas/color/subir$
```

```
misael@misael-GemiBook-X:~/Descargas/color/subir$ file sample.ppm reconstruido.p
pm
sample.ppm:       Netpbm image data, size = 640 x 480, rawbits, pixmap
reconstruido.ppm: Netpbm image data, size = 640 x 480, rawbits, pixmap
misael@misael-GemiBook-X:~/Descargas/color/subir$
```



Evidencia técnica de la comparación:

- **Comando:** `ls -la sample.ppm reconstructdo.ppm`
- **Mismo tamaño: 921,615 bytes para ambos archivos**
- **Comando:** `file sample.ppm reconstructdo.ppm`
- **Mismo formato: PPM 640x480 para ambas imágenes**

Diferencia clave en los headers:

- `sample.ppm`**: Header correcto con saltos de línea (**`P6\n640 480\n255`**)**
- `reconstructdo.ppm`**: Header con formato incorrecto (sin saltos de línea)**
- **Esto explica por qué los hashes MD5 eran diferentes**
- **La funcionalidad es la misma, solo difiere el formato de escritura**