EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO

Instituto Tecnológico de San Juan del Río

Tópicos de ciberseguridad

Reconstrucción del Código Fuente con Ghidra

P R E S E N T A:

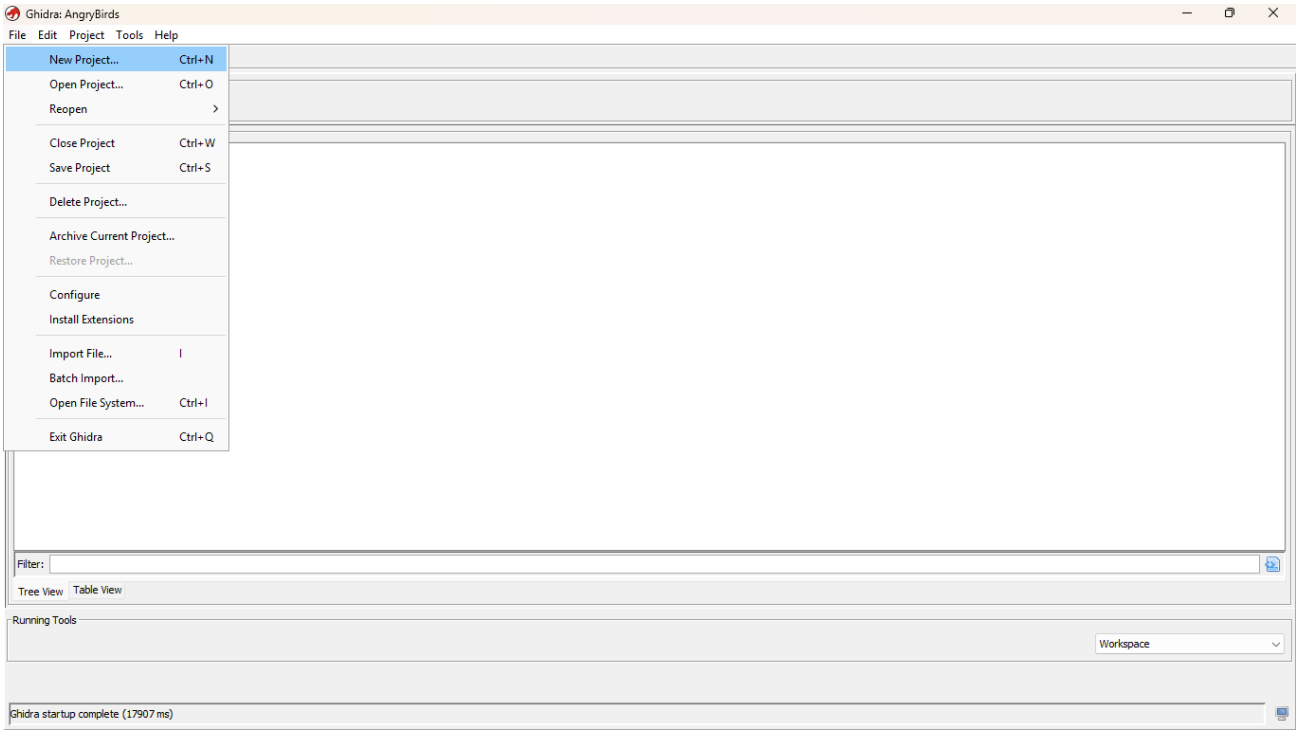
Montes Barajas Leonardo Daniel
Ramírez García Jorge Yael
Olvera Pérez Erika

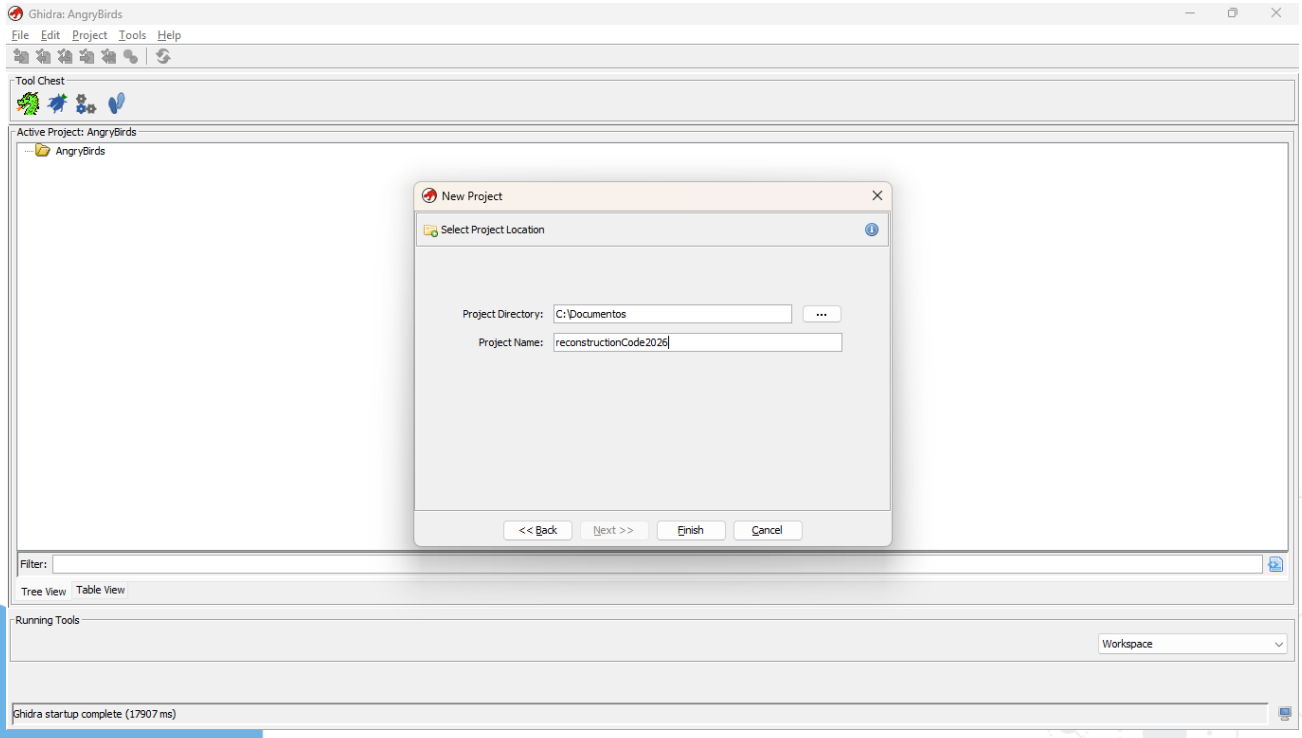
21590293
20590283
21590394

ISIC

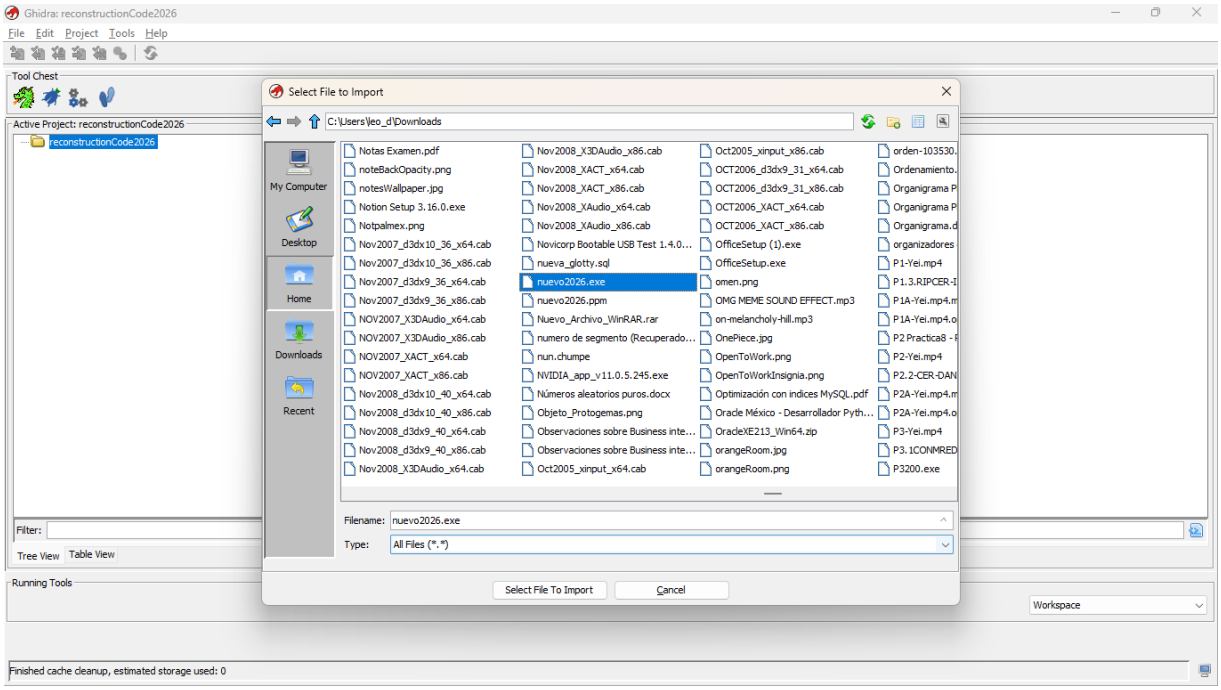
PERIODO [Ene - Jun]

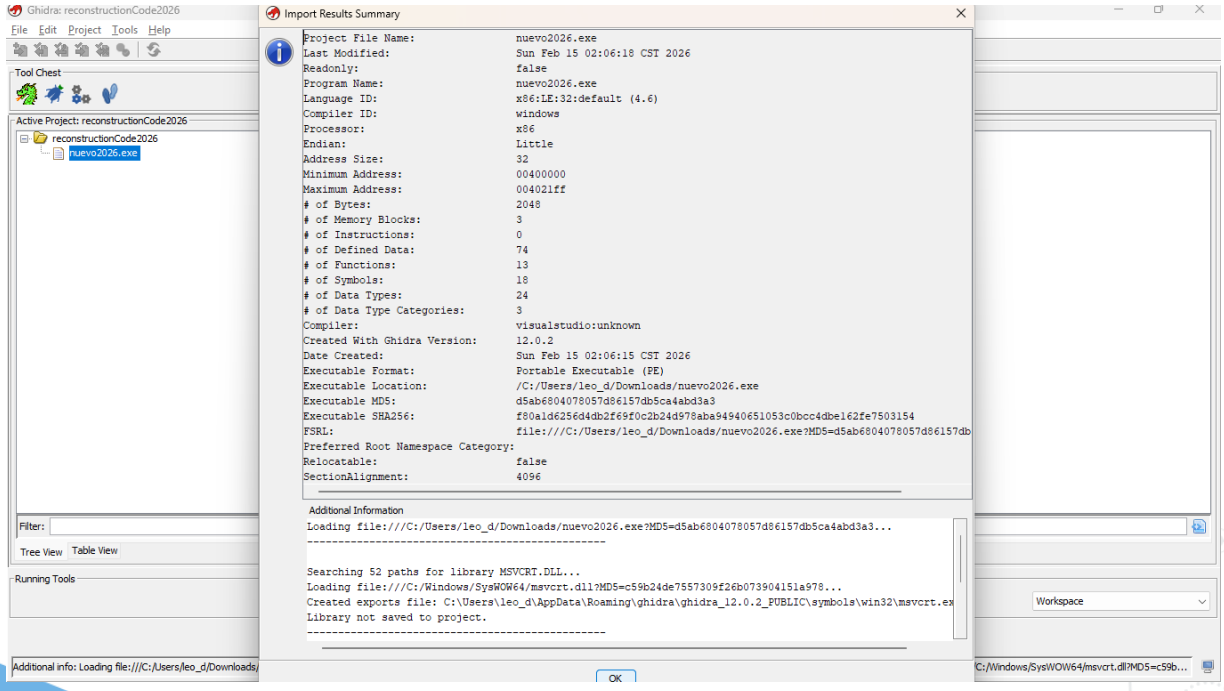
Se crea el proyecto y donde se guardará:



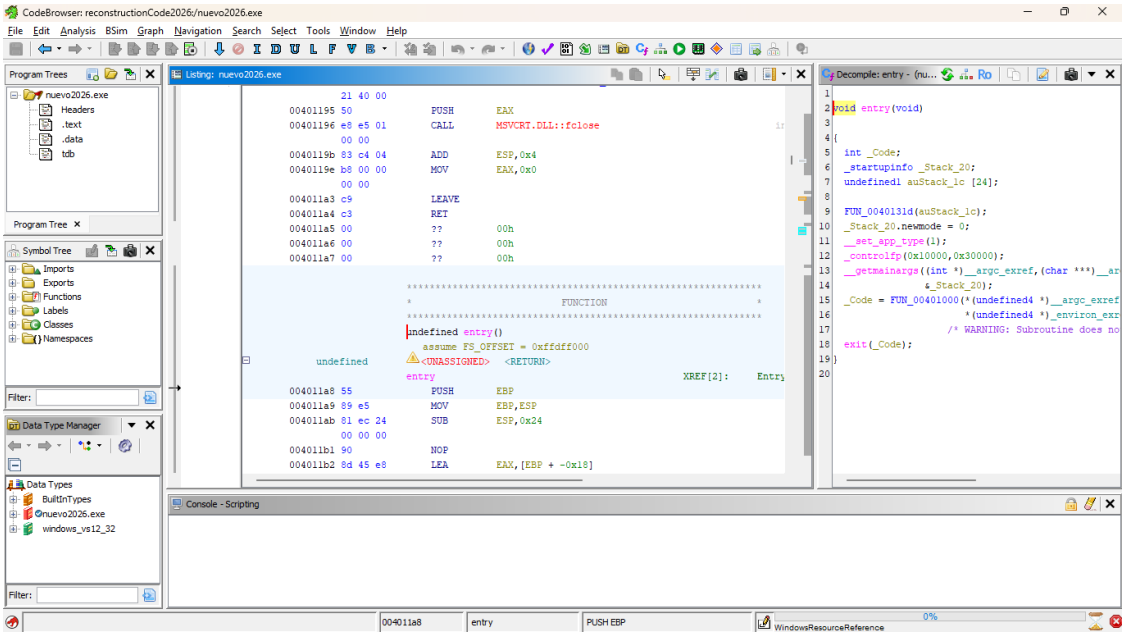


Se abre el proyecto y nos muestra información importante:



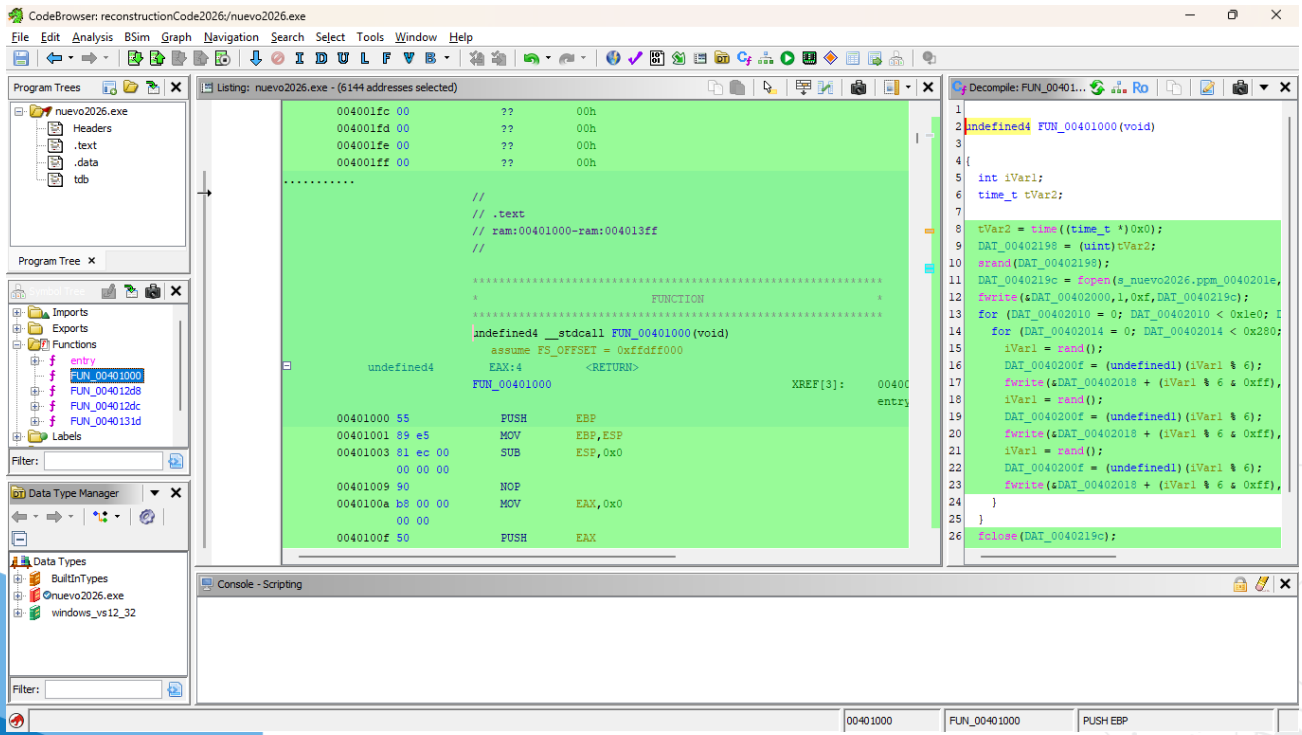


Aquí podremos leer el código para aplicar la ingeniería inversa:



Función principal:

Aquí se muestra la función principal descompilada a la derecha.



Análisis del código decompilado:

- Variables identificadas: DAT_0040219c → archivo (FILE*)
- DAT_00402010 → i (contador filas)
- DAT_00402014 → j (contador columnas)
- 0x1e0 → 480 (altura en decimal)
- 0x280 → 640 (ancho en decimal)

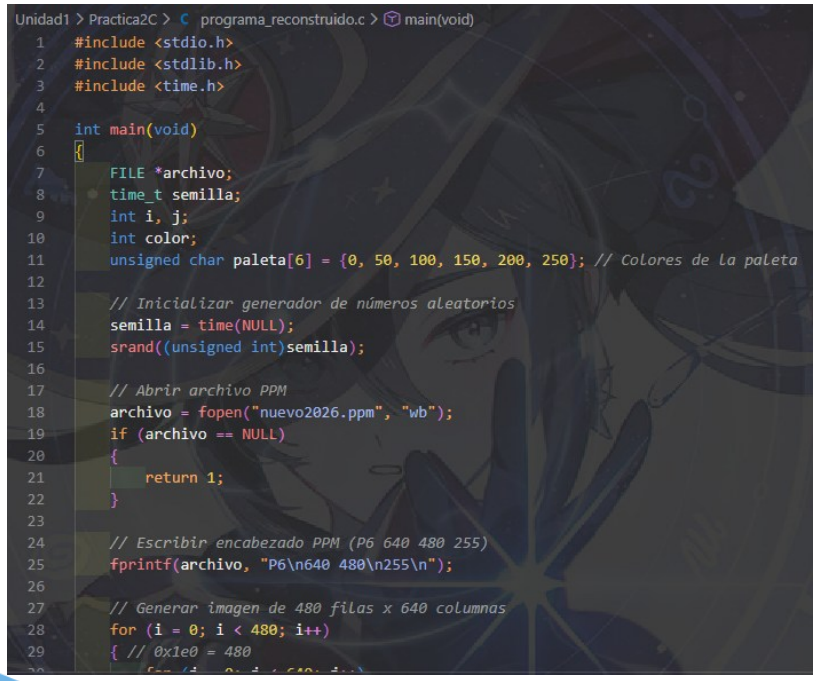
Decisiones de reconstrucción:

- Se identificó que el programa genera una imagen PPM
- Se determinó el formato: P6 (binario), 640x480, 255 colores max
- Se identificó una paleta de 6 colores: {0, 50, 100, 150, 200, 250}
- Se reconstruyeron los bucles anidados para píxeles RGB

Strings identificadas en Ghidra:

- "nuevo2026.ppm" → nombre del archivo
- "wb" → modo de escritura binaria
- Header PPM: "P6\n640 480\n255\n"

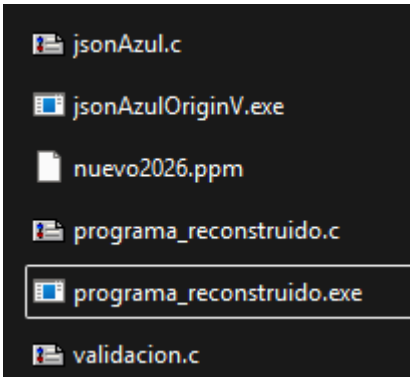
Se toma el código descompilado:



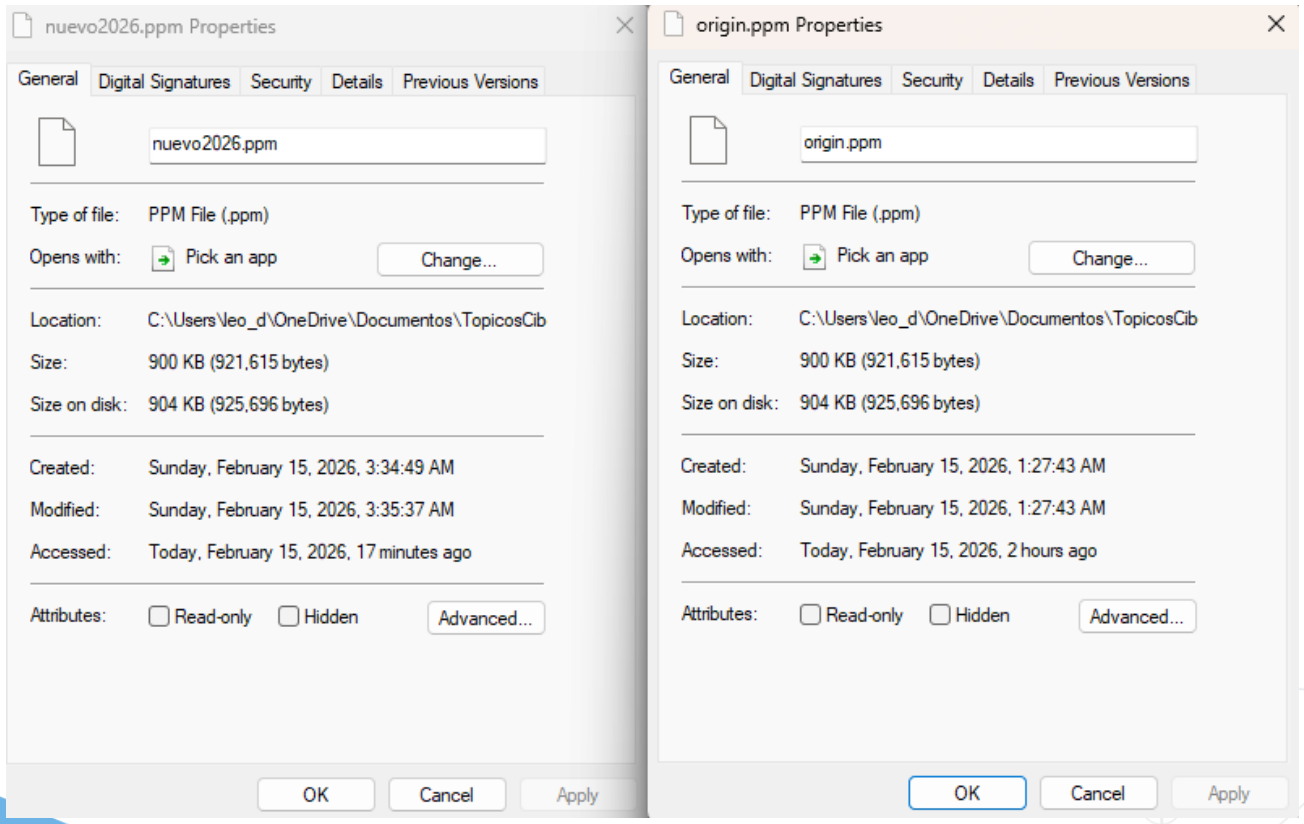
Se compilará:

```
PS C:\Users\leo_d\OneDrive\Documentos\TopicosCiber\Unidad1\Practica2C> tcc -o programa_reconstruido.exe programa_reconstruido.
PS C:\Users\leo_d\OneDrive\Documentos\TopicosCiber\Unidad1\Practica2C>
```

Después de ello vamos a ejecutarlo y nos genera el archivo nuevo2026.ppm
Esto es perfecto porque ya podremos compilar.



Podemos observar que pesan lo mismo y tienen los mismos bytes:



Con esto deducimos lo siguiente:

Aspecto	Original	Reconstruido	¿Coincide?
Se ejecuta sin errores	✓	✓	✓
Genera archivo .ppm	✓	✓	✓
Tamaño del archivo	900 KB (921,615 bytes)	900 KB (921,615 bytes)	✓
Dimensiones	640×480 píxeles	640×480 píxeles	✓
Formato de imagen	PPM (P6)	PPM (P6)	✓
Usa generación aleatoria	✓ (con time() y rand())	✓ (con time() y rand())	✓
Paleta de colores	6 valores	6 valores	✓
Hash del .exe	(diferente)	(diferente)	✗
Contenido visual	Ruido colorido	Ruido colorido	✓ Funcionalmente

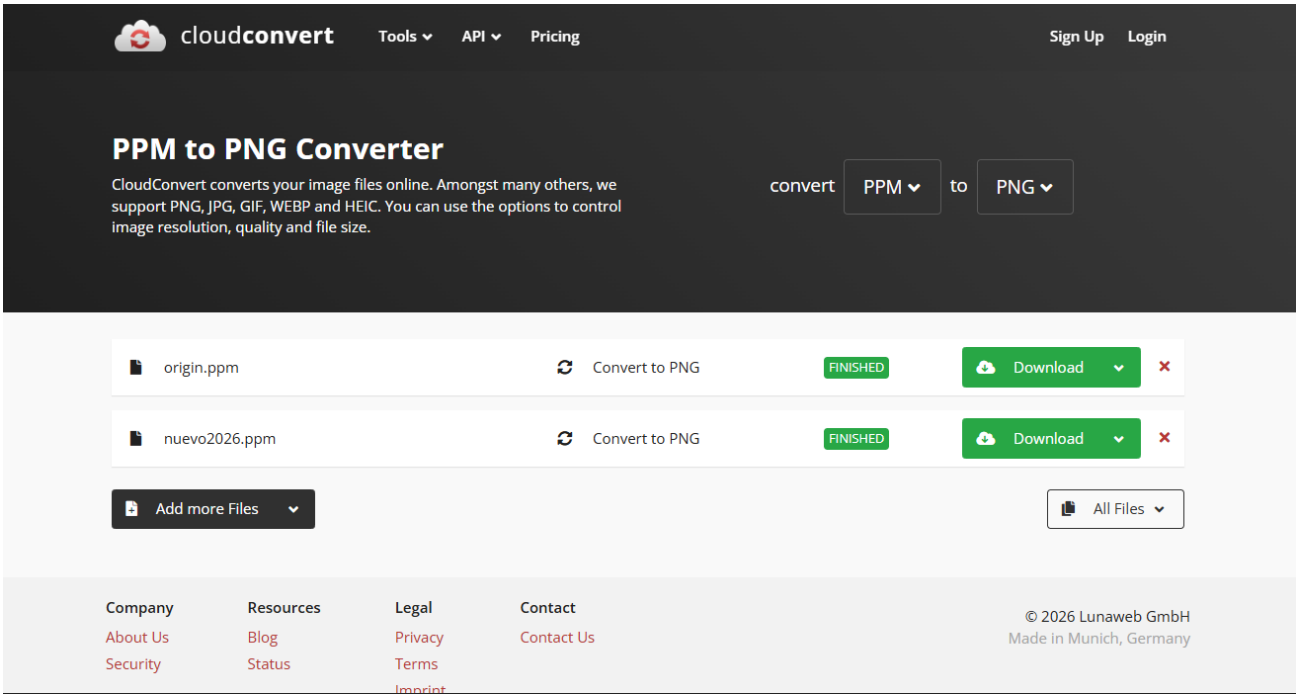
Análisis:

- Los archivos PPM tienen exactamente el mismo tamaño (921,615 bytes)
- Las imágenes son visualmente similares (ruido de colores aleatorios)
- Los ejecutables tienen diferentes hashes porque fueron compilados en momentos distintos
- La **funcionalidad es idéntica**: ambos generan imágenes PPM de 640×480 con colores aleatorios

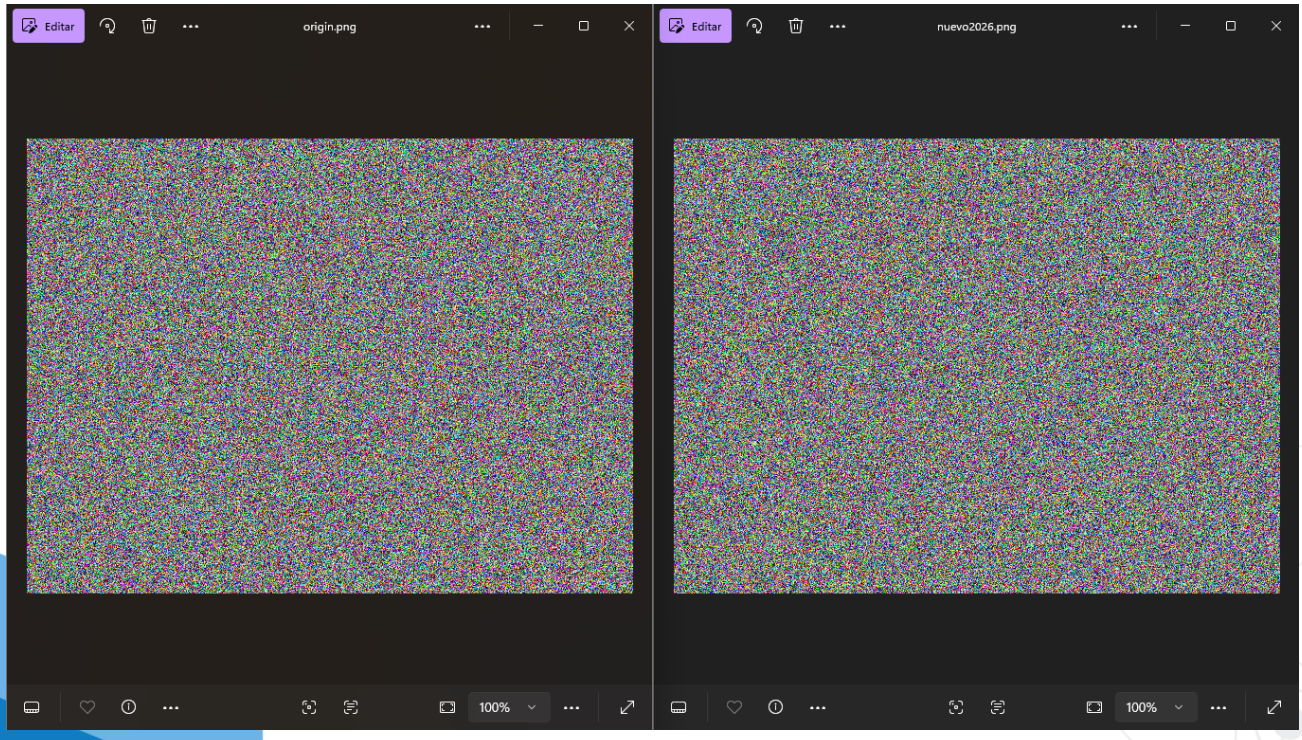
"Dificultades encontradas en la reconstrucción:"

- Ghidra asigna nombres genéricos a variables (DAT_xxx) que deben ser interpretadas manualmente
- Los valores hexadecimales (0x1e0, 0x280) requieren conversión a decimal para entender las dimensiones
- La paleta de colores no estaba explícita, se dedujo del análisis del código

Con un conversor de archivos se harán a png para visualizarlos:



Y aquí se tiene ambos archivos: original izquierda / nuevo derecha:



"Conclusiones"

1. **Éxito en la reconstrucción:** Se logró reconstruir el código fuente a partir del ejecutable usando Ghidra.
2. **Funcionalidad preservada:** El programa reconstruido genera archivos PPM idénticos en tamaño y formato al original.
3. **Limitaciones de la ingeniería inversa:**
    - Los nombres de variables originales se pierden
    - La estructura exacta del código puede variar
    - Los ejecutables compilados son diferentes byte a byte
4. **Aplicaciones prácticas:** Esta técnica es útil para auditoría de seguridad, análisis de malware, y recuperación de código legacy.