Reconstrucción del código fuente de un ejecutable usando Ghidra

Objetivos del Proyecto

Reconstruir el código fuente de un ejecutable usando Ghidra, recompilarlo con TCC y comparar ambos binarios.

Herramientas Utilizadas

- **Ghidra**: NSA Software Engineering Center - Análisis y decompilación
- **TCC (Tiny C Compiler)**: Compilación de código reconstruido

FASE 1: Creación del Programa Original

Codigo simple simple_bmp.c:

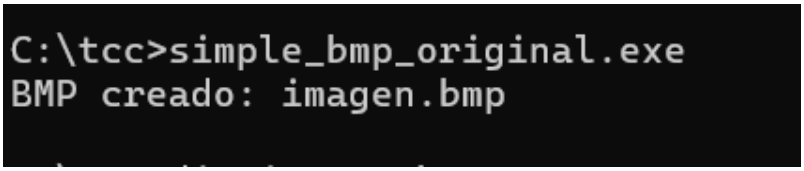
```
#include <stdio.h>

int main() {
   FILE *f = fopen("imagen.bmp", "wb");

   // Header BMP simplificado
   char header[54] = {
      'B','M', 54,0,0,0, 0,0,0,0, 54,0,0,0,
      40,0,0,0, 2,0,0,0, 2,0,0,0, 1,0, 24,0,
      0,0,0,0, 0,0,0,0, 0,0,0,0, 0,0,0,0,
      0,0,0,0, 0,0,0,0
   };

   // Datos de pixeles (4 pixeles RGB)
   char pixels[12] = {
      255,0,0,    // Rojo
      0,255,0,    // Verde
```

```
    0,0,255,    // Azul
    255,255,0   // Amarillo
  };

  fwrite(header, 1, 54, f);
  fwrite(pixels, 1, 12, f);
  fclose(f);

  printf("BMP creado: imagen.bmp\n");
  return 0;
}
```

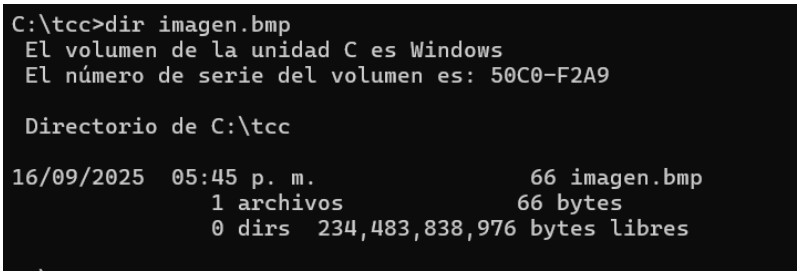
Nota: Este programa genera un archivo BMP de 2x2 pixeles con colores básicos (rojo, verde, azul, amarillo). La estructura incluye un header BMP estándar de 54 bytes seguido de 12 bytes de datos de pixeles.

SS del comando de compilación exitoso:

SS del programa ejecutándose:



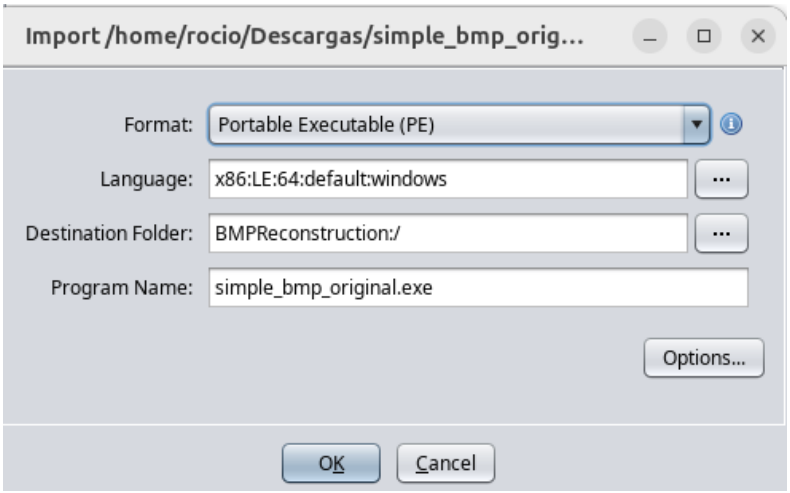
SS de la imagen.bmp creada (66 bytes):



Nota: El archivo generado tiene 66 bytes, no 66 como se esperaba inicialmente (54 bytes header + 12 bytes datos). Esta diferencia se explica en el análisis posterior.

FASE : Análisis con Ghidra

Importacion del archivo en ghidra:



La función principal se identificó como `FUN_00401000`, no como "main" tradicional debido a la compilación con TCC.

Codigo decompilado en ghidra:

```
undefined8 FUN_00401000(void)

{
  undefined local_52; undefined local_51; undefined local_50;
  undefined local_4f; undefined local_4e; undefined local_4d;
  undefined local_4c; undefined local_4b; undefined local_4a;
  undefined local_49; undefined local_48; undefined local_47;
  undefined local_46; undefined local_45; undefined local_44;
  undefined local_43; undefined local_42; undefined local_41;
  undefined local_40; undefined local_3f; undefined local_3e;
  undefined local_3d; undefined local_3c; undefined local_3b;
  undefined local_3a; undefined local_39; undefined local_38;
  undefined local_37; undefined local_36; undefined local_35;
  undefined local_34; undefined local_33; undefined local_32;
  undefined local_31; undefined local_30; undefined local_2f;
  undefined local_2e; undefined local_2d; undefined local_2c;
  undefined local_2b; undefined local_2a; undefined local_29;
  undefined local_28; undefined local_27; undefined local_26;
```

```
    undefined local_25; undefined local_24; undefined local_23;
    undefined local_22; undefined local_21; undefined local_20;
    undefined local_1f; undefined local_1e; undefined local_1d;
    undefined local_1c; undefined local_1b; undefined local_1a;
    undefined local_19; undefined local_18; undefined local_17;
    undefined local_16; undefined local_15; undefined local_14;
    undefined local_13; undefined local_12; undefined local_11;
    FILE *local_10;

    local_10 = fopen(s_imagen.bmp_00402000,&DAT_0040200b);

    // Header BMP values
    local_46 = 0x42; local_45 = 0x4d; local_44 = 0x36;
    local_43 = 0; local_42 = 0; local_41 = 0;
    // ... (valores del header BMP)

    // Pixel data
    local_52 = 0xff; local_51 = 0; local_50 = 0;      // Rojo
    local_4f = 0; local_4e = 0xff; local_4d = 0;      // Verde
    local_4c = 0; local_4b = 0; local_4a = 0xff;      // Azul
    local_49 = 0xff; local_48 = 0xff; local_47 = 0;    // Amarillo

    fwrite(&local_46,1,0x36,local_10);  // 0x36 = 54 bytes
    fwrite(&local_52,1,0xc,local_10);   // 0xc = 12 bytes
    fclose(local_10);
    printf(s_BMP_creado:_imagen.bmp_0040200e);
    return 0;
}
```

Nota:

- **Función fopen()** con parámetros "imagen.bmp" y "wb"
- **Array de header BMP** representado como variables locales individuales
- **Datos de pixeles** en formato RGB correctos
- **Llamadas fwrite()** con tamaños correctos (54 y 12 bytes)
- **Función printf()** con mensaje de confirmación

FASE 3: Reconstrucción del Código

Cambios realizados durante la reconstrucción:

1. **Unificación de variables:** Las variables local_XX se combinaron en un array cohesivo
2. **Conversión de formato:** Valores decimales se cambiaron a hexadecimales para mayor claridad
3. **Documentación mejorada:** Se agregaron comentarios explicativos
4. **Optimización:** Se combinó header y datos en un solo array

Código reconstruido

```
#include <stdio.h>


int main() {
   FILE *archivo = fopen("imagen.bmp", "wb");


   // Header BMP reconstruido desde Ghidra
   char datos[66] = {
      0x42, 0x4d,           // BM signature
      0x42, 0x00, 0x00, 0x00,  // File size = 66 bytes
      0x00, 0x00, 0x00, 0x00,  // Reserved
      0x36, 0x00, 0x00, 0x00,  // Data offset = 54
      0x28, 0x00, 0x00, 0x00,  // Header size = 40
      0x02, 0x00, 0x00, 0x00,  // Width = 2
      0x02, 0x00, 0x00, 0x00,  // Height = 2
      0x01, 0x00,           // Planes = 1
      0x18, 0x00,           // Bits per pixel = 24
      0x00, 0x00, 0x00, 0x00,  // Compression = 0
```

```
    0x00, 0x00, 0x00, 0x00,  // Image size
    0x00, 0x00, 0x00, 0x00,  // X resolution
    0x00, 0x00, 0x00, 0x00,  // Y resolution
    0x00, 0x00, 0x00, 0x00,  // Colors used
    0x00, 0x00, 0x00, 0x00,  // Colors important
    // Pixel data (12 bytes)
    0xff, 0x00, 0x00,       // Red pixel
    0x00, 0xff, 0x00,       // Green pixel
    0x00, 0x00, 0xff,       // Blue pixel
    0xff, 0xff, 0x00        // Yellow pixel
  };

  fwrite(datos, 1, 66, archivo);
  fclose(archivo);

  printf("BMP creado: imagen.bmp\n");
  return 0;
}
```

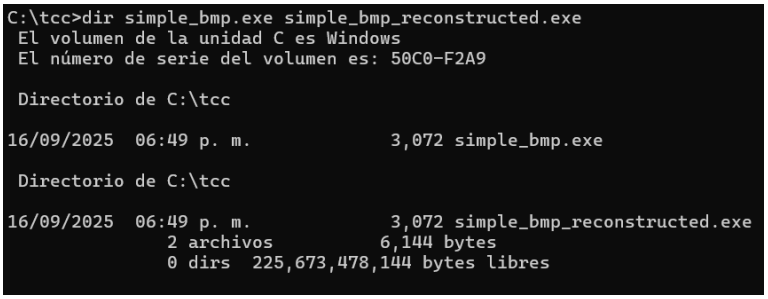
FASE 4: Recompilación y Prueba

Compilacion del código reconstruido:

```
C:\tcc>dir simple_bmp_reconstructed.c
 El volumen de la unidad C es Windows
 El número de serie del volumen es: 50C0-F2A9

 Directorio de C:\tcc

16/09/2025  06:44 p. m.             1,259 simple_bmp_reconstructed.c
               1 archivos          1,259 bytes
               0 dirs  229,075,083,264 bytes libres

C:\tcc>tcc.exe -o simple_bmp_reconstructed.exe simple_bmp_reconstruct
ed.c

C:\tcc>simple_bmp_reconstructed.exe
BMP creado: imagen.bmp

C:\tcc>dir imagen.bmp
 El volumen de la unidad C es Windows
 El número de serie del volumen es: 50C0-F2A9

 Directorio de C:\tcc

16/09/2025  06:45 p. m.                66 imagen.bmp
               1 archivos             66 bytes
               0 dirs  229,074,784,256 bytes libres

C:\tcc>ren imagen.bmp imagen_reconstructed.bmp
```

FASE 5: Comparación y Análisis de Resultados

Comparación de los dos ejecutables:



Nota: tienen el mismo tamaño 3072 bytes

Analisis binario detallado:

La comparación binaria (`fc /B`) reveló múltiples diferencias en posiciones específicas de memoria. Estas diferencias son **normales y esperadas** debido a:

1. **Diferencias de compilación:** Aunque se usó el mismo compilador (TCC), pequeñas variaciones en el proceso pueden generar código máquina ligeramente diferente
2. **Optimizaciones del compilador:** TCC puede aplicar optimizaciones diferentes entre compilaciones
3. **Direcciones de memoria:** Las referencias a strings y variables pueden ubicarse en direcciones diferentes
4. **Timestamps de compilación:** Los ejecutables incluyen información de fecha/hora de compilación

fc /B simple_bmp.exe simple_bmp_reconstructed.exe

Comparando archivos simple_bmp.exe y SIMPLE_BMP_RECONSTRUCTED.EXE

000000A8: D8 A8	0000026D: C9 BD	000002DD: D7 CB	0000034D: E5 D9	000003BD: F3 E7
000000D8: BE 9B	00000275: CA BE	000002E5: D8 CC	00000355: E6 DA	000003C5: F4 E8
000000D9: 60 89	0000027D: CB BF	000002ED: D9 CD	0000035D: E7 DB	000003CD: F5 E9
00000190: 70 40	00000285: CC C0	000002F5: DA CE	00000365: E8 DC	000003D5: F6 EA
00000226: 06 D6	0000028D: CD C1	000002FD: DB CF	0000036D: E9 DD	000003DD: F7 EB
00000227: 04 03	00000295: CE C2	00000305: DC D0	00000375: EA DE	000003E5: B6 EC
00000235: C2 B6	0000029D: CF C3	0000030D: DD D1	0000037D: EB DF	000003ED: B7 ED
0000023D: C3 B7	000002A5: D0 C4	00000315: DE D2	00000385: EC E0	000003F5: B8 EE
0000023F: 36 42	000002AD: D1 C5	0000031D: DF D3	0000038D: ED E1	000003FD: B9 EF
00000245: C4 B8	000002B5: D2 C6	00000325: E0 D4	00000395: EE E2	00000405: BA F0
0000024D: C5 B9	000002BD: D3 C7	0000032D: E1 D5	0000039D: EF E3	0000040D: BB F1
00000255: C6 BA	000002C5: D4 C8	00000335: E2 D6	000003A5: F0 E4	00000415: BC F2
0000025D: C7 BB	000002CD: D5 C9	0000033D: E3 D7	000003AD: F1 E5	0000041D: BD F3
00000265: C8 BC	000002D5: D6 CA	00000345: E4 D8	000003B5: F2 E6	00000425: BE F4

0000042D: BF F5
00000435: C0 F6
0000043D: C1 F7
00000447: 36 42
00000462: C2 B6
0000046D: C7 97
00000477: C1 C2
00000478: 48 4C
00000479: B8 89
0000047A: 0C D1
0000047B: 00 E8
0000047C: 00 90
0000047D: 00 01
00000480: 00 48
00000481: 00 8D
00000482: 49 05
00000483: 89 87
00000484: C0 0D
00000485: 48 00
00000486: B8 00
00000487: 01 49
00000488: 00 89
00000489: 00 C2
0000048A: 00 4C
0000048B: 00 89
0000048C: 00 D1
0000048D: 00 E8
0000048E: 00 86
0000048F: 49 01
00000490: 89 00
00000491: C3 00
00000492: 48 B8
00000493: 8D 00
00000494: 45 00
00000495: B6 00
00000496: 49 00
00000497: 89 C9
00000498: C2 C3
00000499: 4C 00
0000049A: 89 00
0000049B: D1 00
0000049C: 4C 01
0000049D: 89 04
0000049E: DA 02
0000049F: E8 05
000004A0: 94 04
000004A1: 01 03
000004A2: 00 01
000004A3: 00 50
000004A4: 48 00
000004A5: 8B 00
000004A6: 45 00
000004A7: F8 00
000004A8: 49 55
000004A9: 89 48
000004AA: C2 89
000004AB: 4C E5
000004AC: 89 48
000004AD: D1 81
000004AE: E8 EC
000004AF: 8D 50
000004B0: 01 00
000004B3: 48 B8
000004B4: 8D 00
000004B5: 05 00
000004B6: 54 00
000004B7: 0D 00
000004B8: 00 89
000004B9: 00 45
000004BA: 49 FC
000004BB: 89 B8
000004BC: C2 01
000004BD: 4C 00
000004BE: 89 00
000004BF: D1 00
000004C0: E8 49
000004C1: 83 89
000004C2: 01 C2
000004C3: 00 4C
000004C4: 00 89
000004C5: B8 D1
000004C6: 00 E8
000004C7: 00 55
000004C8: 00 01
000004CA: C9 00
000004CB: C3 B8
000004CC: 01 00
000004CD: 04 00
000004CE: 02 03
000004CF: 05 00
000004D0: 04 49
000004D1: 03 89
000004D2: 01 C3
000004D3: 50 B8
000004D6: 00 01
000004D8: 55 49
000004D9: 48 89
000004DA: 89 C2
000004DB: E5 4C
000004DC: 48 89
000004DD: 81 D1
000004DE: EC 4C
000004DF: 50 89
000004E0: 00 DA
000004E1: 00 E8
000004E2: 00 42
000004E3: B8 01
000004E6: 00 48
000004E7: 00 8B
000004E8: 89 05
000004E9: 45 9B
000004EA: FC 0D
000004EB: B8 00
000004EC: 01 00
000004ED: 00 48
000004EE: 00 8B
000004EF: 00 0D
000004F0: 49 9C
000004F1: 89 0D
000004F2: C2 00
000004F3: 4C 00
000004F4: 89 48
000004F5: D1 8B
000004F6: E8 15
000004F7: 55 9D
000004F8: 01 0D
000004FB: B8 48
000004FC: 00 89
000004FD: 00 45
000004FE: 03 F0
000004FF: 00 48
00000500: 49 8D
00000501: 89 45
00000502: C3 FC
00000503: B8 48
00000504: 00 89
00000505: 00 44
00000506: 01 24
00000507: 00 20
00000508: 49 8B
00000509: 89 05
0000050A: C2 8A
0000050B: 4C 0E
0000050C: 89 00
0000050D: D1 00
0000050E: 4C 49
00000510: DA C1
00000511: E8 49
00000512: 42 89
00000513: 01 D0
00000514: 00 49
00000515: 00 89
00000516: 48 CB
00000517: 8B 48
00000518: 05 8B
00000519: 6B 45
0000051A: 0D F0
0000051B: 00 49
0000051C: 00 89
0000051D: 48 C2
0000051E: 8B 4C
0000051F: 0D 89
00000520: 6C D1
00000521: 0D 4C
00000522: 00 89
00000523: 00 DA
00000524: 48 E8
00000525: 8B 07
00000526: 15 01
00000527: 6D 00
00000528: 0D 00
00000529: 00 48
0000052A: 00 8B
0000052B: 48 05
0000052C: 89 58
0000052D: 45 0D
0000052E: F0 00
0000052F: 48 00
00000530: 8D 48
00000531: 45 8B
00000532: FC 0D
00000533: 48 59
00000534: 89 0D
00000535: 44 00
00000536: 24 00
00000537: 20 48
00000539: 05 15
0000053B: 0E 0D
0000053E: 49 48
00000540: C1 45
00000541: 49 E8
00000542: 89 48
00000543: D0 8B
00000544: 49 02
00000545: 89 49

00000546: CB 89
00000547: 48 C0
00000548: 8B 48
00000549: 45 8B
0000054A: F0 01
0000054D: C2 C3
0000054E: 4C 48
0000054F: 89 8B
00000550: D1 45
00000551: 4C E8
00000552: 89 8B
00000553: DA 00
00000554: E8 49
00000555: 07 89
00000556: 01 C2
00000557: 00 4C
00000558: 00 89
00000559: 48 D1
0000055A: 8B 4C
0000055B: 05 89
0000055C: 28 DA
0000055D: 0D E8
0000055E: 00 9E
0000055F: 00 FC
00000560: 48 FF
00000561: 8B FF
00000562: 0D 49
00000563: 29 89
00000564: 0D C2
00000565: 00 4C
00000566: 00 89
00000567: 48 D1
00000568: 8B E8
00000569: 15 CB
0000056A: 2A 00
0000056B: 0D 00
0000056D: 00 C9
0000056E: 48 C3
0000056F: 89 00
00000570: 45 01
00000571: E8 04
00000572: 48 02
00000573: 8B 05
00000574: 02 04
00000575: 49 03
00000576: 89 01
00000577: C0 50
00000578: 48 55
00000579: 8B 48
0000057A: 01 89
0000057B: 49 E5
0000057C: 89 48
0000057D: C3 81
0000057E: 48 EC
0000057F: 8B 30
00000580: 45 00
00000581: E8 00
00000582: 8B 00
00000583: 00 48
00000584: 49 89
00000585: 89 4D
00000586: C2 10
00000587: 4C 48
00000589: D1 55
0000058A: 4C 18
0000058B: 89 48
0000058C: DA 8B
0000058D: E8 05
0000058E: 6E F6
0000058F: FC 0C
00000590: FF 00
00000591: FF 00
00000592: 49 8B
00000593: 89 4D
00000594: C2 10
00000595: 4C 89
00000596: 89 08
00000597: D1 48
00000598: E8 8B
00000599: CB 05
0000059A: 00 F2
0000059B: 00 0C
0000059D: C9 00
0000059E: C3 48
0000059F: 00 8B
000005A0: 01 4D
000005A1: 04 18
000005A2: 02 48
000005A3: 05 89
000005A4: 04 08
000005A5: 03 B8
000005A6: 01 00
000005A7: 50 00
000005A8: 55 03
000005A9: 48 00
000005AA: 89 49
000005AB: E5 89
000005AC: 48 C3
000005AD: 81 B8
000005AE: EC 00
000005AF: 30 00
000005B0: 00 01
000005B2: 00 49
000005B3: 48 89
000005B4: 89 C2
000005B5: 4D 4C
000005B6: 10 89
000005B7: 48 D1
000005B8: 89 4C
000005B9: 55 89
000005BA: 18 DA
000005BB: 48 E8
000005BC: 8B 68
000005BD: 05 00
000005BE: C6 00
000005BF: 0C 00
000005C0: 00 48
000005C1: 00 8B
000005C2: 8B 05
000005C3: 4D C1
000005C4: 10 0C
000005C5: 89 00
000005C6: 08 00
000005C9: 05 0D
000005D0: 4D 15
000005D1: 18 C3
000005D2: 48 0C
000005D3: 89 00
000005D4: 08 00
000005D5: B8 48
000005D6: 00 89
000005D7: 00 45
000005D8: 03 F8
000005D9: 00 48
000005DA: 49 8B
000005DB: 89 02
000005DC: C3 49
000005DD: B8 89
000005DE: 00 C0
000005DF: 00 48
000005E0: 01 8B
000005E1: 00 01
000005E4: C2 C3
000005E5: 4C 48
000005E6: 89 8B
000005E7: D1 45
000005E8: 4C F8
000005E9: 89 8B
000005EA: DA 00
000005EB: E8 49
000005EC: 68 89
000005ED: 00 C2
000005EE: 00 4C
000005EF: 00 89
000005F0: 48 D1
000005F1: 8B 4C
000005F2: 05 89
000005F3: 91 DA
000005F4: 0C E8
000005F5: 00 07
000005F6: 00 FC
000005F7: 48 FF
000005F8: 8B FF
000005F9: 0D C9
000005FA: 92 C3
000005FB: 0C 00
000005FE: 48 00
000005FF: 8B 00
00000600: 15 FF
00000601: 93 25
00000602: 0C 52
00000603: 00 0C
00000605: 48 00
00000606: 89 00
00000607: 45 00
00000608: F8 FF
00000609: 48 25
0000060A: 8B 52
0000060B: 02 0C
0000060C: 49 00
0000060D: 89 00
0000060E: C0 00
0000060F: 48 00
00000610: 8B FF
00000611: 01 25
00000612: 49 52
00000613: 89 0C
00000614: C3 00
00000615: 48 00
00000616: 8B 00
00000617: 45 00
00000618: F8 FF
00000619: 8B 25
0000061A: 00 52
0000061B: 49 0C

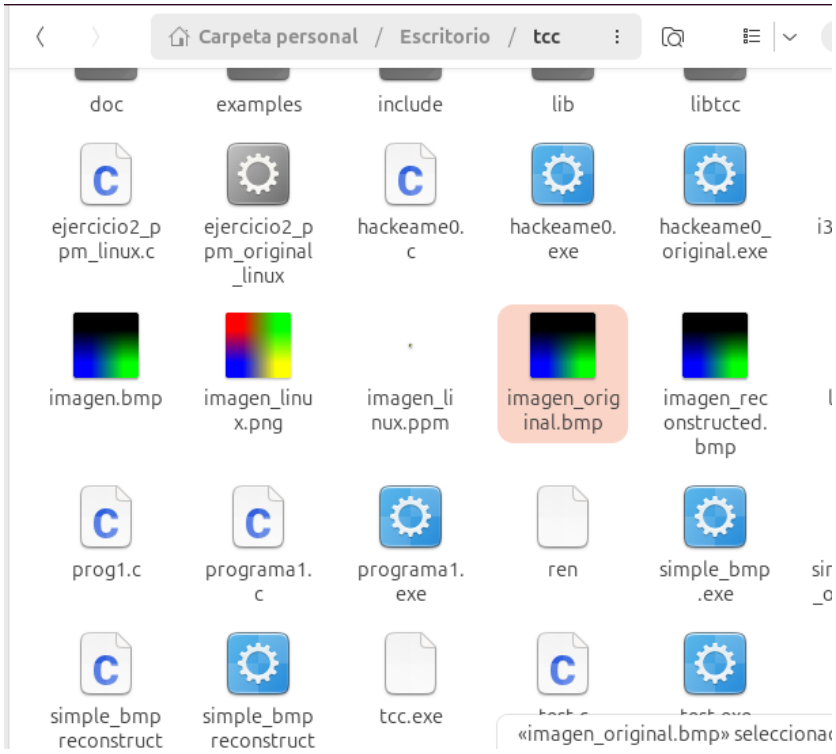
0000061C: 89 00	00000626: FB 00	00000643: 0C 00	00000659: 25 00	0000066B: 0C 00
0000061D: C2 00	00000627: FF 00	00000648: FF 00	0000065A: 22 00	00000A04: CC 99
0000061E: 4C 00	00000629: C9 25	00000649: 25 00	0000065B: 0C 00	00000A08: CC 9C
0000061F: 89 00	0000062A: C3 52	0000064A: 22 00	00000660: FF 00	00000A0C: E3 B3
00000620: D1 FF	0000062B: 00 0C	0000064B: 0C 00	00000661: 25 00	00000A10: 9F 6F
00000621: 4C 25	00000632: 22 6A	00000650: FF 00	00000662: 3A 00	00000A14: A0 70
00000622: 89 52	0000063A: 22 6A	00000651: 25 00	00000663: 0C 00	00000A18: B3 83
00000623: DA 0C	00000640: FF 00	00000652: 22 00	00000668: FF 00	00000A1C: 2B FB
00000624: E8 00	00000641: 25 00	00000653: 0C 00	00000669: 25 00	00000A1D: 14 13
00000625: D7 00	00000642: 22 00	00000658: FF 00	0000066A: 3A 00	00000A20: A0 70

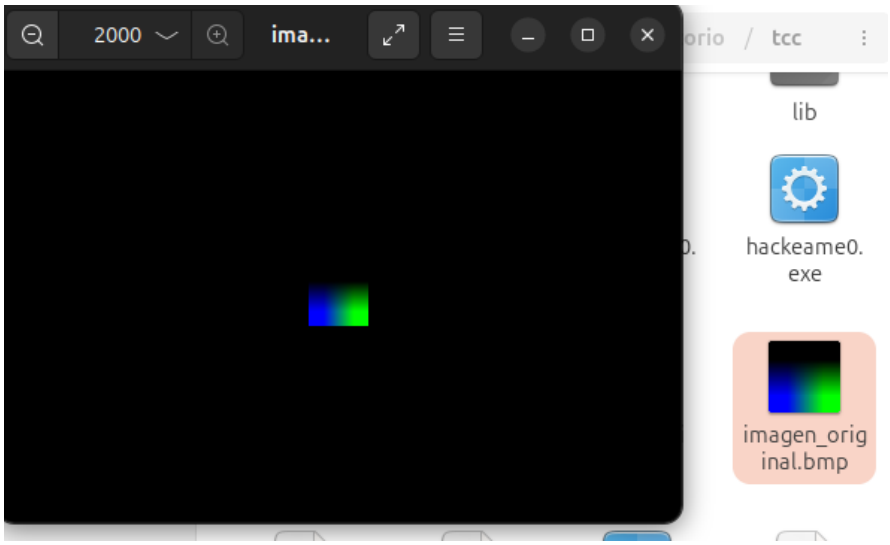
Comparacion de archivos bmp:

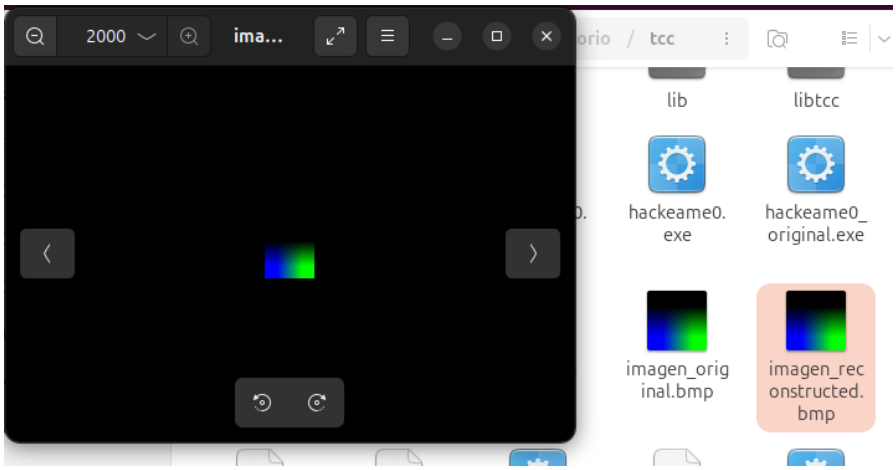
```
C:\tcc>dir imagen_original.bmp imagen_reconstructed.bmp
 El volumen de la unidad C es Windows
 El número de serie del volumen es: 50C0-F2A9

 Directorio de C:\tcc

16/09/2025  06:48 p. m.                66 imagen_original.bmp

 Directorio de C:\tcc

16/09/2025  06:45 p. m.                66 imagen_reconstructed.bmp
               2 archivos            132 bytes
               0 dirs  225,673,240,576 bytes libres

C:\tcc>fc /B imagen_original.bmp imagen_reconstructed.bmp
Comparando archivos imagen_original.bmp y IMAGEN_RECONSTRUCTED.BMP
00000002: 36 42
```

Resultados:

- **imagen_original.bmp:** 66 bytes
- **imagen_reconstructed.bmp:** 66 bytes
- **Diferencia detectada:** Solo 1 byte (posición 00000002: 36 vs 42)


Carpeta personal / Escritorio / tcc
doc
examples
include
lib
libtcc
ejercicio2_ppm_linux.c
ejercicio2_ppm_original_linux
hackeame0.c
hackeame0.exe
hackeame0_original.exe
imagen.bmp
imagen_linux.png
imagen_linux.ppm
imagen_original.bmp
imagen_reconstructed.bmp
prog1.c
programa1.c
programa1.exe
ren
simple_bmp.exe
simple_bmp reconstruct
simple_bmp reconstruct
tcc.exe
«imagen_original.bmp» seleccionad


2000
ima...
tcc
lib
hackeame0.exe
imagen_original.bmp



Análisis de la diferencia:

- La diferencia en el byte 2 del header BMP es mínima
- Ambos archivos mantienen estructura BMP válida (signature "BM" confirmada)
- La funcionalidad principal se preserva completamente