Instituto Tecnológico de San Juan del Río

Tópicos de ciberseguridad

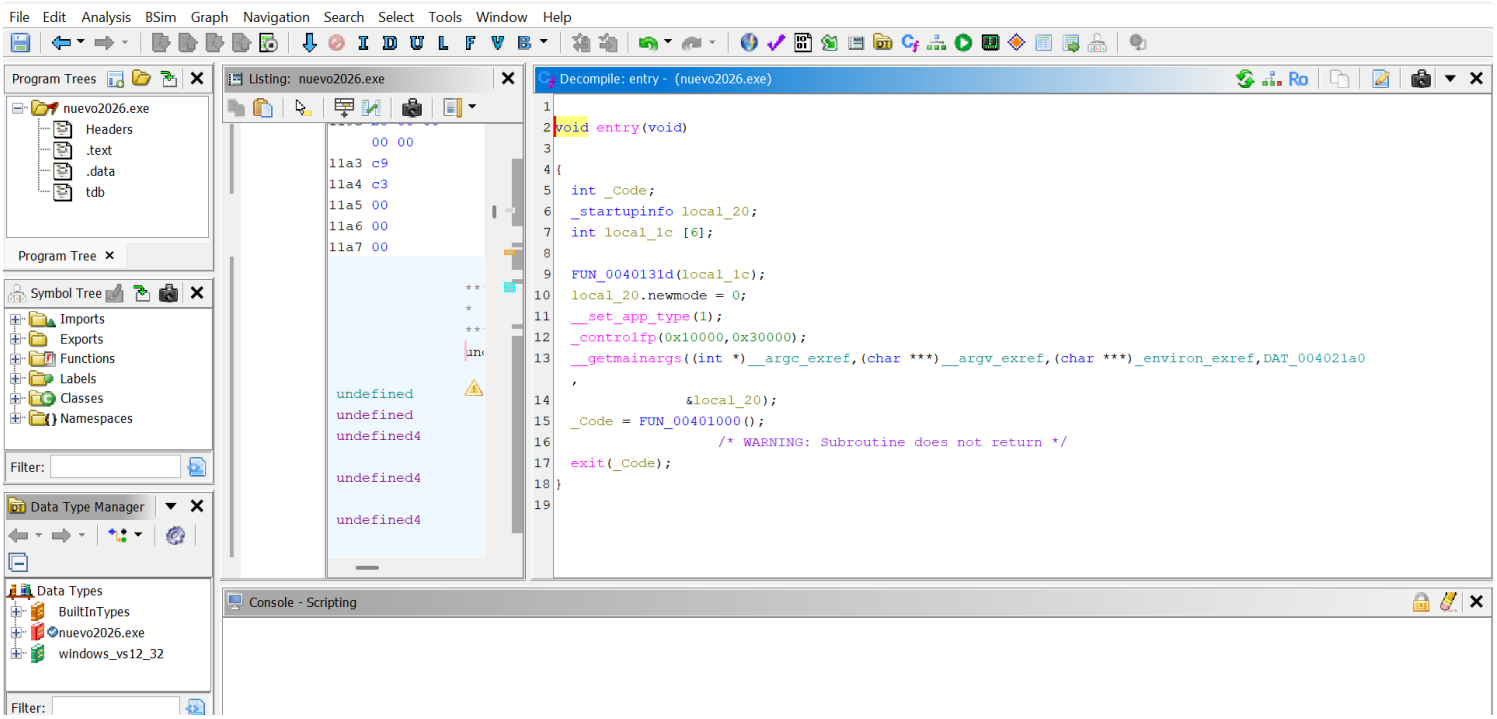
P R E S E N T A:

Abelardo Garduño Fuertes 22590040
Alejandro Pérez Piña 22590068
Brandon Ismael Trejo Hernández 22590049

Ingeniería en Sistemas Computacionales

PERIODO [ENE-JUN 2026]

Lo primero que se obtiene después de abrir el Ghidra, crear el proyecto y cargar el ejecutable, es la siguiente pantalla:



Viendo el código que se nos proporciona, en esta parte es donde se encuentra el main del ejecutable:

```
,
                    &local_20);
_Code = FUN_00401000();
                    /* WARNING: Subroutine does not return */
exit(_Code);
```

Si le damos doble click a “FUN_00401000(), aparecerá el siguiente código, que, al analizarlo, coincide con el main del ejecutable:

```
undefined4 FUN_00401000(void)

{
  int iVar1;
  time_t tVar2;

  tVar2 = time((time_t *)0x0);
  DAT_00402198 = (uint)tVar2;
  srand(DAT_00402198);
  DAT_0040219c = fopen(s_nuevo2026.ppm_0040201e,&DAT_0040202c);
  fwrite(&DAT_00402000,1,0xf,DAT_0040219c);
  for (DAT_00402010 = 0; DAT_00402010 < 0x1e0; DAT_00402010 = DAT_00402010 + 1) {
    for (DAT_00402014 = 0; DAT_00402014 < 0x280; DAT_00402014 = DAT_00402014 + 1) {
      iVar1 = rand();
      DAT_0040200f = (undefined1)(iVar1 % 6);
      fwrite(&DAT_00402018 + (iVar1 % 6 & 0xff),1,1,DAT_0040219c);
      iVar1 = rand();
      DAT_0040200f = (undefined1)(iVar1 % 6);
      fwrite(&DAT_00402018 + (iVar1 % 6 & 0xff),1,1,DAT_0040219c);
      iVar1 = rand();
      DAT_0040200f = (undefined1)(iVar1 % 6);
      fwrite(&DAT_00402018 + (iVar1 % 6 & 0xff),1,1,DAT_0040219c);
    }
  }
  fclose(DAT_0040219c);
  return 0;
}
```

Una vez abierto el código, procedemos a analizarlo. En la primera parte podemos ver que se declaran 2 variables, iVar1 y tVar2, pero lo interesante es que tVar2 es de tipo time_t, lo que significa que esa variable va a almacenar tiempo, específicamente la fecha actual, después con unit se transforma tVar2 a unsigned int almacenándose en DAT_00402198, y con esta, se inicializa el generador pseudoaleatorio con la semilla utilizando el valor de DAT_00402198y con ayuda de srand (DAT_00402198). En Python podemos sustituir esas líneas usando un random.seed con el parámetro time.time() que se transforma a entero con int.

```
int iVar1;
time_t tVar2;

tVar2 = time((time_t *)0x0);
DAT_00402198 = (uint)tVar2;
srand(DAT_00402198);
```

```
import time
import random
#import os

random.seed(int(time.time()))
```

Continuando con el código, vemos que procede a abrirse un archivo con el nombre de "nuevo2026.ppm", almacenándose en DAT_0040219c, y después vemos que se hace una escritura al archivo, lo cual es: fwrite(&DAT_00402000,1,0xf,DAT_0040219c); esto significa que en el archivo se va a escribir desde la dirección &DAT_00402000, 15 bytes (porque es en decimal el valor de 0xf).

```
DAT_0040219c = fopen(s_nuevo2026.ppm_0040201e,&DAT_0040202c);
fwrite(&DAT_00402000,1,0xf,DAT_0040219c);
```

Para saber de que manera va a abrir el archivo, basta con darle doble click al apuntador &DAT_0040202c (línea roja) y en la parte de la izquierda de la pantalla nos va a decir de que manera se va a abrir, en este caso wb.

```
0040202c 77          ??          77h    w
0040202d 62          ??          62h    b
0040202e 00          ??          00h
0040202f 00          ??          00h
```

Y para saber lo que va a escribir en el archivo, de igual manera damos doble click al apuntador &DAT_00402000 (línea azul) y nos va a aparecer del lado izquierdo, el cual podemos pensar que es el encabezado del archivo.

```
00402000 50          ??          50h    P
00402001 36          ??          36h    6
00402002 0a          ??          0Ah
00402003 36          ??          36h    6
00402004 34          ??          34h    4
00402005 30          ??          30h    0
00402006 20          ??          20h
00402007 34          ??          34h    4
00402008 38          ??          38h    8
00402009 30          ??          30h    0
0040200a 0a          ??          0Ah
0040200b 32          ??          32h    2
0040200c 35          ??          35h    5
0040200d 35          ??          35h    5
0040200e 0a          ??          0Ah
```

En Python, esas líneas quedan de la siguiente manera:

```python
with open("nuevo2026.ppm", "wb") as f:
    f.write(b"P6\n640 480\n255\n")
```

Lo siguiente que podemos ver en el ghidra es la ejecución de un for anidado, es fácil reconocer sus componentes, pero lo interesante es ver el límite de los for: 0x1e0 y 0x280, que convertidos a decimal son 480 y 640 respectivamente. Ya con esto, podemos hacer su traducción a Python.

```
for (DAT_00402010 = 0; DAT_00402010 < 0x1e0; DAT_00402010 = DAT_00402010 + 1) {
  for (DAT_00402014 = 0; DAT_00402014 < 0x280; DAT_00402014 = DAT_00402014 + 1) {
```

```python
    for i in range(480):
        for j in range(640):
```

Continuando con el ghidra vemos lo siguiente:

```
iVar1 = rand();
DAT_0040200f = (undefined1)(iVar1 % 6);
fwrite(&DAT_00402018 + (iVar1 % 6 & 0xff),1,1,DAT_0040219c);
iVar1 = rand();
DAT_0040200f = (undefined1)(iVar1 % 6);
fwrite(&DAT_00402018 + (iVar1 % 6 & 0xff),1,1,DAT_0040219c);
iVar1 = rand();
DAT_0040200f = (undefined1)(iVar1 % 6);
fwrite(&DAT_00402018 + (iVar1 % 6 & 0xff),1,1,DAT_0040219c);
```

Analizándolo, podemos ver que el código se repite 3 veces. Lo primero que notamos es que en la variable iVar1 se almacena la generación de un número pseudoaleatorio entero para después sacarle el modulo de 6, esto lo que va a hacer es que el resultado este entre los valores

de 0 y 5, para que después, en esta línea: fwrite(&DAT_00402018 + (iVar1 % 6 & 0xff),1,1,DAT_0040219c) se escriba, en el archivo que abrimos anteriormente, el desplazamiento (que es el valor entre 0 y 5 generado con iVar1 % 6) del apuntador &DAT_00402018, este apuntador lo que contiene es una serie de valores hexadecimales, que podemos verlos si de igual manera hacemos doble click en el apuntador.

```
00402018 00              ??         00h
00402019 32              ??         32h
0040201a 64              ??         64h
0040201b 96              ??         96h
0040201c c8              ??         C8h
0040201d fa              ??         FAh
```

En Python, quedaría de la siguiente manera:

```
for p in range(3):
    index = random.randint(0, 5)
    f.write(bytes([colores[index]]))
```

Cabe destacar que se sustituyo la ejecución de las 3 líneas por un for, se sustituyo la operación del módulo por la generación de un número pseudoaleatorio entero entre 0 y 5 (que va a cumplir exactamente con la misma función que el módulo de 6 anteriormente) y por último se hace la escritura del archivo. A demás, se creo un arreglo para almacenar los valores que se observaron en el apuntador &DAT_00402018.

```
colores = bytes([0x00, 0x32, 0x64, 0x96, 0xC8, 0xFA])
```

Finalmente, el archivo Python queda de la siguiente manera, teniendo la misma función que el código analizado en ghidra:

```python
import time
import random
#import os

random.seed(int(time.time()))

colores = bytes([0x00, 0x32, 0x64, 0x96, 0xC8, 0xFA])

with open("nuevo2026.ppm", "wb") as f:
    f.write(b"P6\n640 480\n255\n")

    for i in range(480):
        for j in range(640):
            for p in range(3):
                index = random.randint(0, 5)
                f.write(bytes([colores[index]]))

print("Imagen generada: nuevo2026.ppm")
```