Instituto Tecnológico de San Juan del Río

TOPICOS DE CIBERSEGURIDAD

VALDES ARTEAGA LEONARDO

PRACTICA 4 EJECUTABLE SIN IMPORTAR EL USUARIO O CONTRASEÑA

P R E S E N T A:

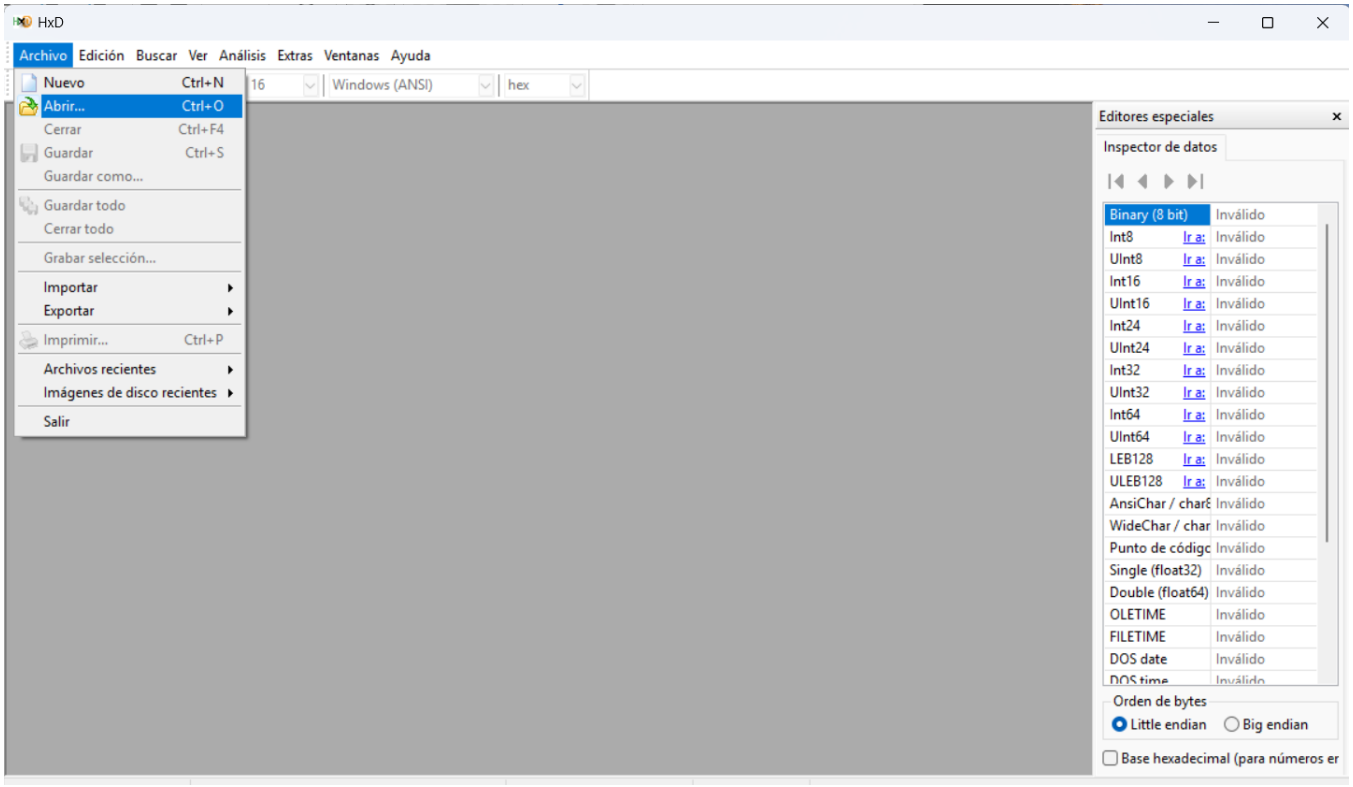
María del Carmen Pérez Cruz, Emma Belen Marquez García, Karla Daniela Pérez González

Ingeniería en Sistemas Computacionales

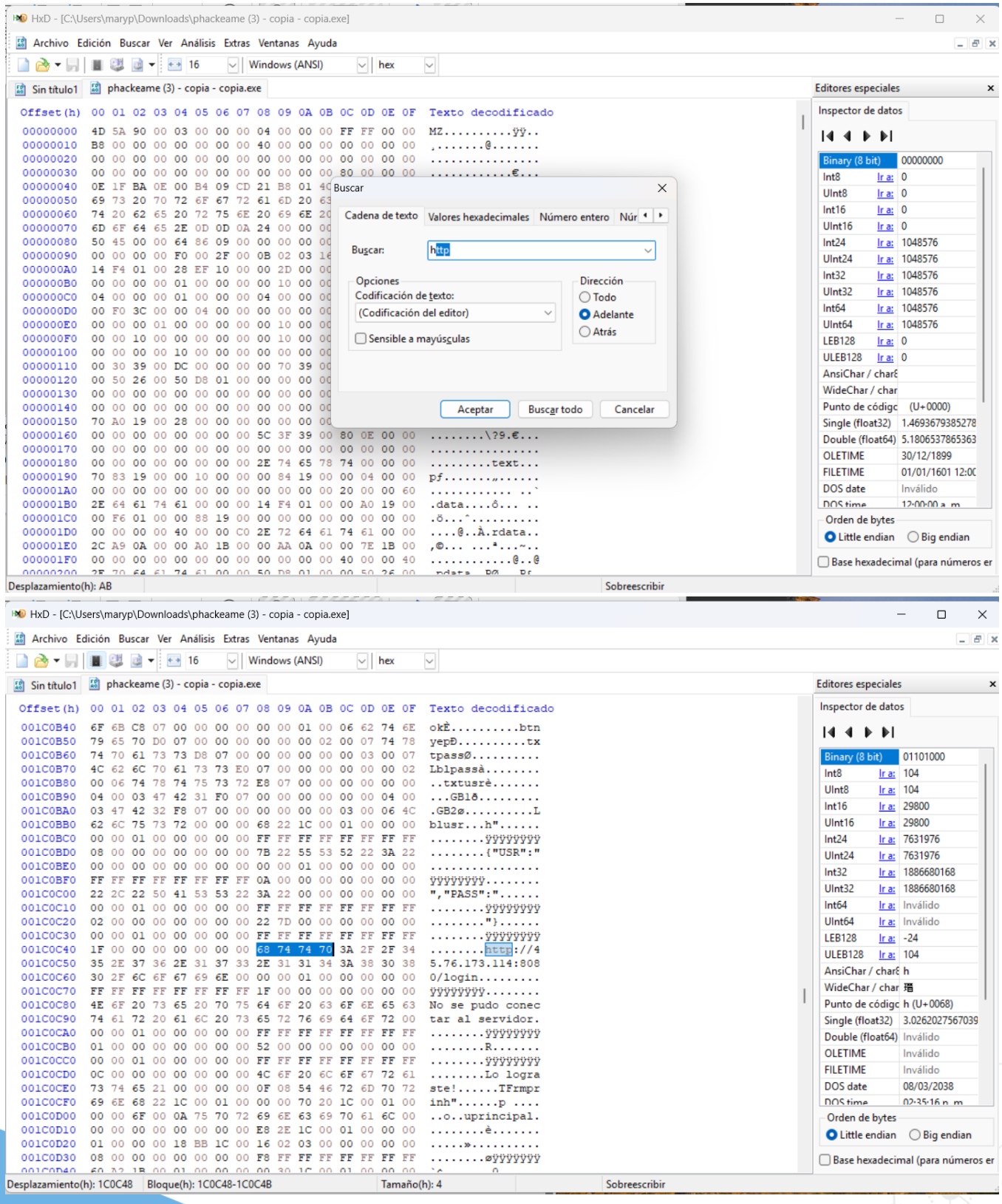
NO. DE CONTROL: 21590485, 21590481, 21590486

PERIODO Enero-Junio

Primero abrimos un archivo nuevo en la aplicación de HxD para que podamos abrir nuestro ejecutable y analizar los hexadecimales

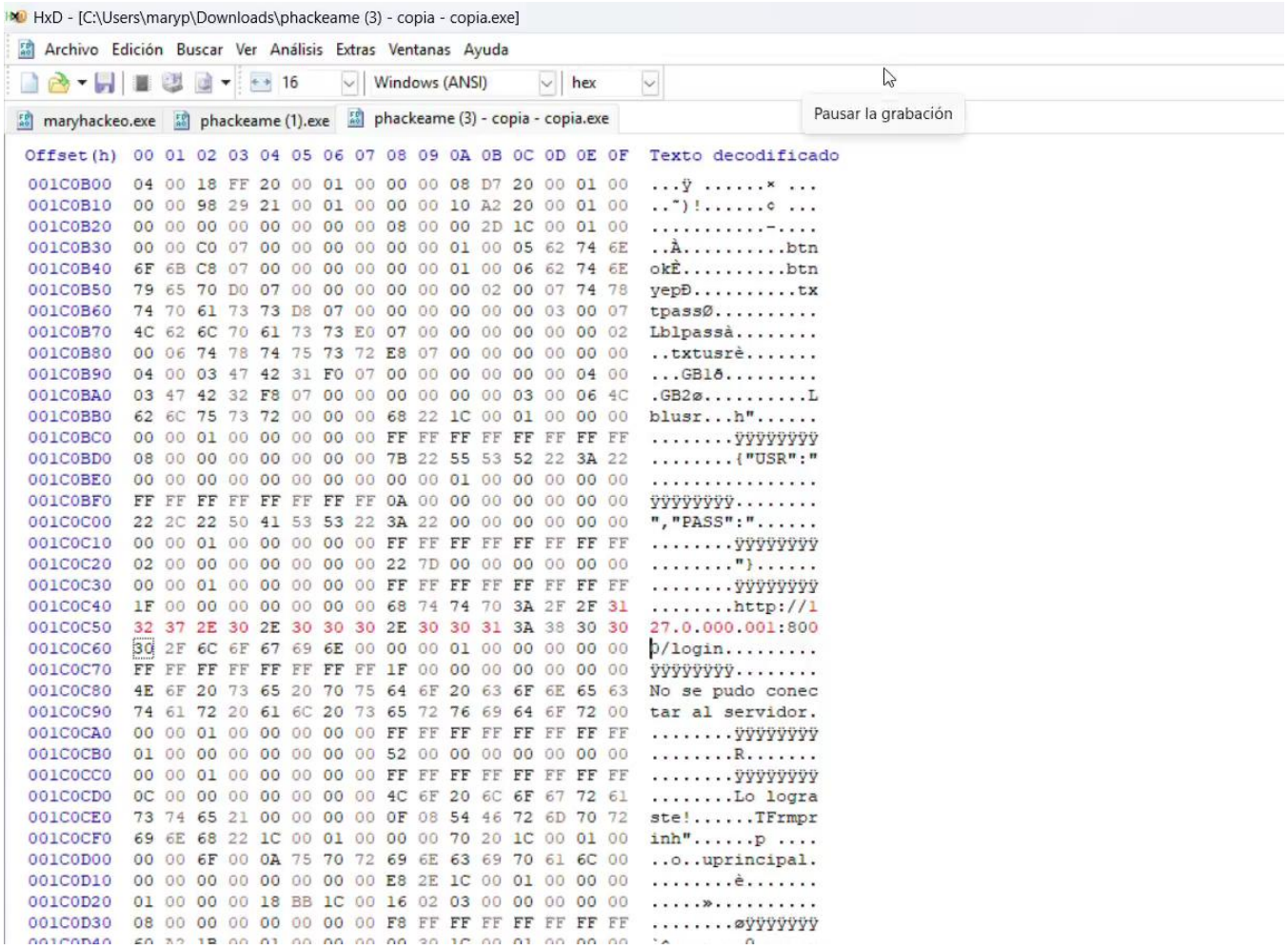


Despues presionamos ctrl+f parta buscar el http o sea la ip que esta usando nuestro archivo

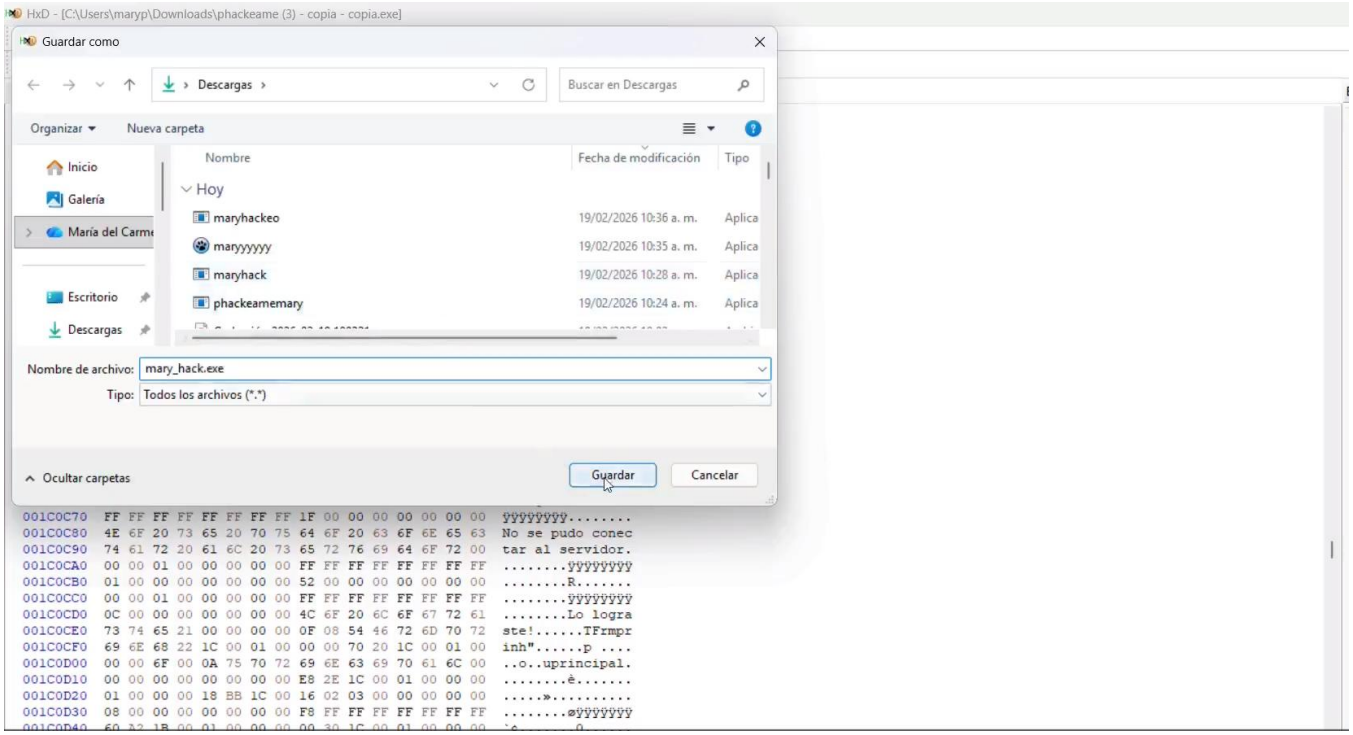

HxD - [C:\Users\maryp\Downloads\phackeame (3) - copia - copia.exe]
Archivo Edición Buscar Ver Análisis Extras Ventanas Ayuda
Windows (ANSI)
hex
Sin título1
phackeame (3) - copia - copia.exe
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Texto decodificado
Buscar
Cadena de texto
Valores hexadecimales
Número entero
Buscar:
http
Opciones
Codificación de texto:
(Codificación del editor)
Sensible a mayúsculas
Dirección
Todo
Adelante
Atrás
Aceptar
Buscar todo
Cancelar
Editores especiales
Inspector de datos
Binary (8 bit) 00000000
Int8 0
UInt8 0
Int16 0
UInt16 0
Int24 1048576
UInt24 1048576
Int32 1048576
UInt32 1048576
Int64 1048576
UInt64 1048576
LEB128 0
ULEB128 0
Punto de código (U+0000)
Single (float32) 1.4693679385278
Double (float64) 5.1806537865363
OLETIME 30/12/1899
FILETIME 01/01/1601 12:00
DOS date Inválido
Orden de bytes
Little endian
Big endian
Base hexadecimal (para números er
Desplazamiento(h): AB
Sobreescribir

HxD - [C:\Users\maryp\Downloads\phackeame (3) - copia - copia.exe]
Archivo Edición Buscar Ver Análisis Extras Ventanas Ayuda
Windows (ANSI)
hex
Sin título1
phackeame (3) - copia - copia.exe
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Texto decodificado
001C0B40 6F 6B C8 07 00 00 00 00 00 00 01 00 06 62 74 6E okÈ.....btn
001C0B50 79 65 70 D0 07 00 00 00 00 00 00 02 00 07 74 78 yepÐ.....tx
001C0B60 74 70 61 73 73 D8 07 00 00 00 00 00 03 00 07 tpassØ.....
001C0B70 4C 62 6C 70 61 73 73 E0 07 00 00 00 00 00 00 02 Lblpassà.....
001C0B80 00 06 74 78 74 75 73 72 E8 07 00 00 00 00 00 00 ..txtusrè.....
001C0B90 04 00 03 47 42 31 F0 07 00 00 00 00 00 04 00 ...GB1ð.....
001C0BA0 03 47 42 32 F8 07 00 00 00 00 00 03 00 06 4C .GB2ø.....L
001C0BB0 62 6C 75 73 72 00 00 00 68 22 1C 00 01 00 00 00 blusr...h".....
001C0BC0 00 00 01 00 00 00 00 00 FF FF FF FF FF FF FF FF ....ÿÿÿÿÿÿÿÿ
001C0BD0 08 00 00 00 00 00 00 00 7B 22 55 53 52 22 3A 22 ....{"USR":"
001C0BE0 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 .....
001C0BF0 FF FF FF FF FF FF FF FF 0A 00 00 00 00 00 00 00 ÿÿÿÿÿÿÿÿ.....
001C0C00 22 2C 22 50 41 53 53 22 3A 22 00 00 00 00 00 00 ","PASS":".....
001C0C10 00 00 01 00 00 00 00 00 FF FF FF FF FF FF FF FF ....ÿÿÿÿÿÿÿÿ
001C0C20 02 00 00 00 00 00 00 00 22 7D 00 00 00 00 00 00 ...."}.....
001C0C30 00 00 01 00 00 00 00 00 FF FF FF FF FF FF FF FF ....ÿÿÿÿÿÿÿÿ
001C0C40 1F 00 00 00 00 00 00 00 68 74 74 70 3A 2F 2F 34 ....http://4
001C0C50 35 2E 37 36 2E 31 37 33 2E 31 31 34 3A 38 30 38 5.76.173.114:808
001C0C60 30 2F 6C 6F 67 69 6E 00 00 00 01 00 00 00 00 00 0/login.....
001C0C70 FF FF FF FF FF FF FF FF 1F 00 00 00 00 00 00 00 ÿÿÿÿÿÿÿÿ.....
001C0C80 4E 6F 20 73 65 20 70 75 64 6F 20 63 6F 6E 65 63 No se pudo conec
001C0C90 74 61 72 20 61 6C 20 73 65 72 76 69 64 6F 72 00 tar al servidor.
001C0CA0 00 00 01 00 00 00 00 00 FF FF FF FF FF FF FF FF ....ÿÿÿÿÿÿÿÿ
001C0CB0 01 00 00 00 00 00 00 00 52 00 00 00 00 00 00 00 ....R.....
001C0CC0 00 00 01 00 00 00 00 00 FF FF FF FF FF FF FF FF ....ÿÿÿÿÿÿÿÿ
001C0CD0 0C 00 00 00 00 00 00 00 4C 6F 20 6C 6F 67 72 61 ....Lo logra
001C0CE0 73 74 65 21 00 00 00 00 0F 08 54 46 72 6D 70 72 ste!.....TFrmpr
001C0CF0 69 6E 68 22 1C 00 01 00 00 00 70 20 1C 00 01 00 inh".....p ....
001C0D00 00 00 6F 00 0A 75 70 72 69 6E 63 69 70 61 6C 00 ..o..uprincipal.
001C0D10 00 00 00 00 00 00 00 00 E8 2E 1C 00 01 00 00 00 ....è.....
001C0D20 01 00 00 00 18 BB 1C 00 16 02 03 00 00 00 00 00 .....».....
001C0D30 08 00 00 00 00 00 00 00 F8 FF FF FF FF FF FF FF ....øÿÿÿÿÿÿÿ
Editores especiales
Inspector de datos
Binary (8 bit) 01101000
Int8 104
UInt8 104
Int16 29800
UInt16 29800
Int24 7631976
UInt24 7631976
Int32 1886680168
UInt32 1886680168
Int64 Inválido
UInt64 Inválido
LEB128 -24
ULEB128 104
AnsiChar / char8 h
WideChar / char 瑨
Punto de código h (U+0068)
Single (float32) 3.0262027567039
Double (float64) Inválido
OLETIME Inválido
FILETIME Inválido
DOS date 08/03/2038
Orden de bytes
Little endian
Big endian
Base hexadecimal (para números er
Desplazamiento(h): 1C0C48
Bloque(h): 1C0C48-1C0C4B
Tamaño(h): 4
Sobreescribir

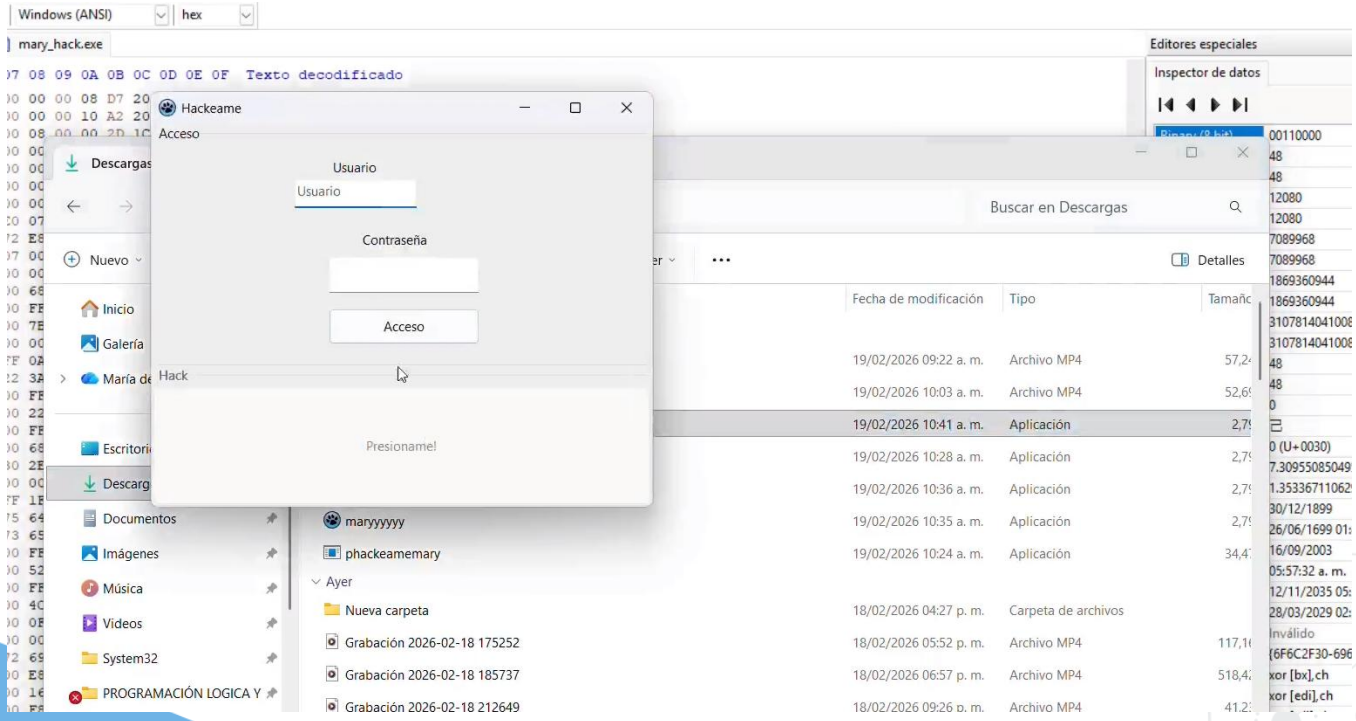
Despues vamos a cambiar los dígitos uno a uno en el hexadecimal hasta lograr la ip que deseamos en este caso es 127.0.0.1, pero para que no se pierdan los bit vamos a hacer que sea de manera que sea 127.0.000.001

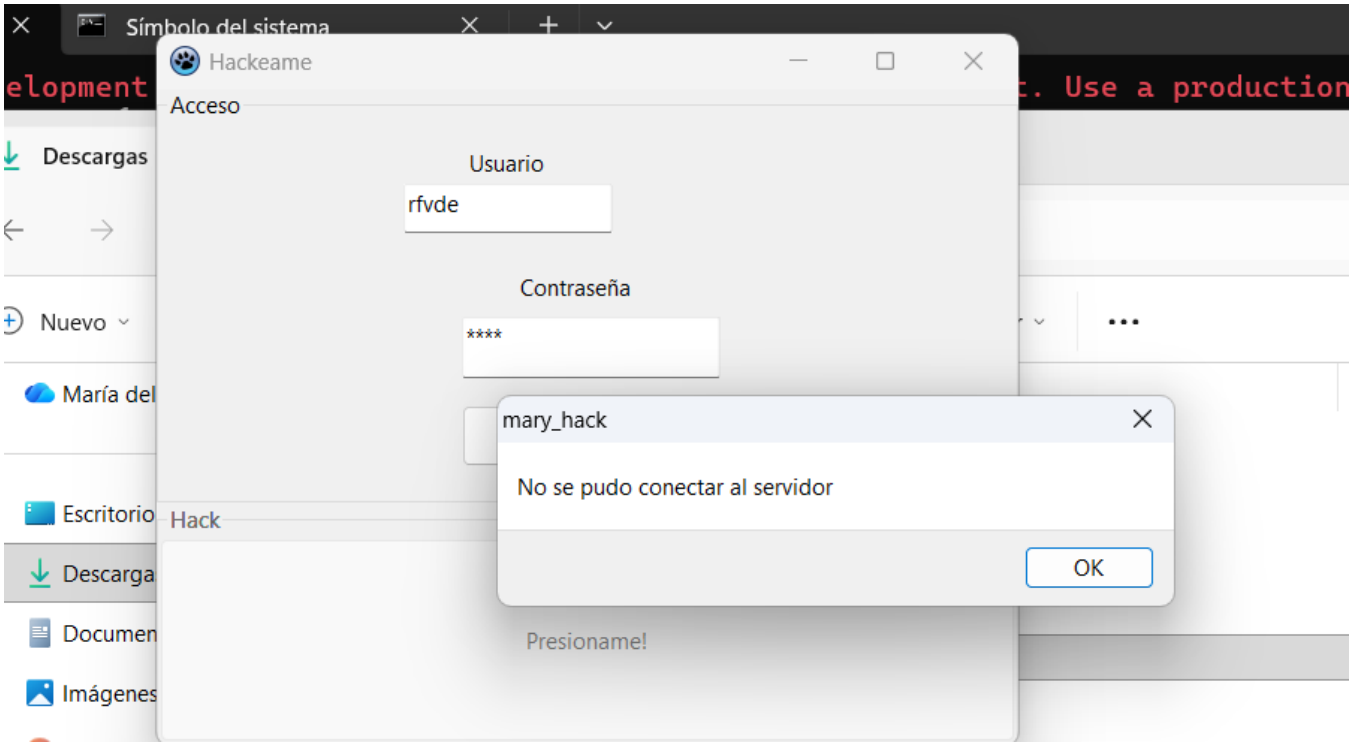


Guardamos muestro ejecutable con .exe al final para que no haya problemas con el ejecutable después



Abrimos nuestro ejecutable creado para comprobar que aun sigue sin funcionar con cualquier usuario y contraseña





Abrimos nuestro geany con nuestro código previamente realizado ya solo para ejecutar

yp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE - Geany

Ver Documento Proyecto Construir Herramientas Ayuda

soloPares.py parche.py

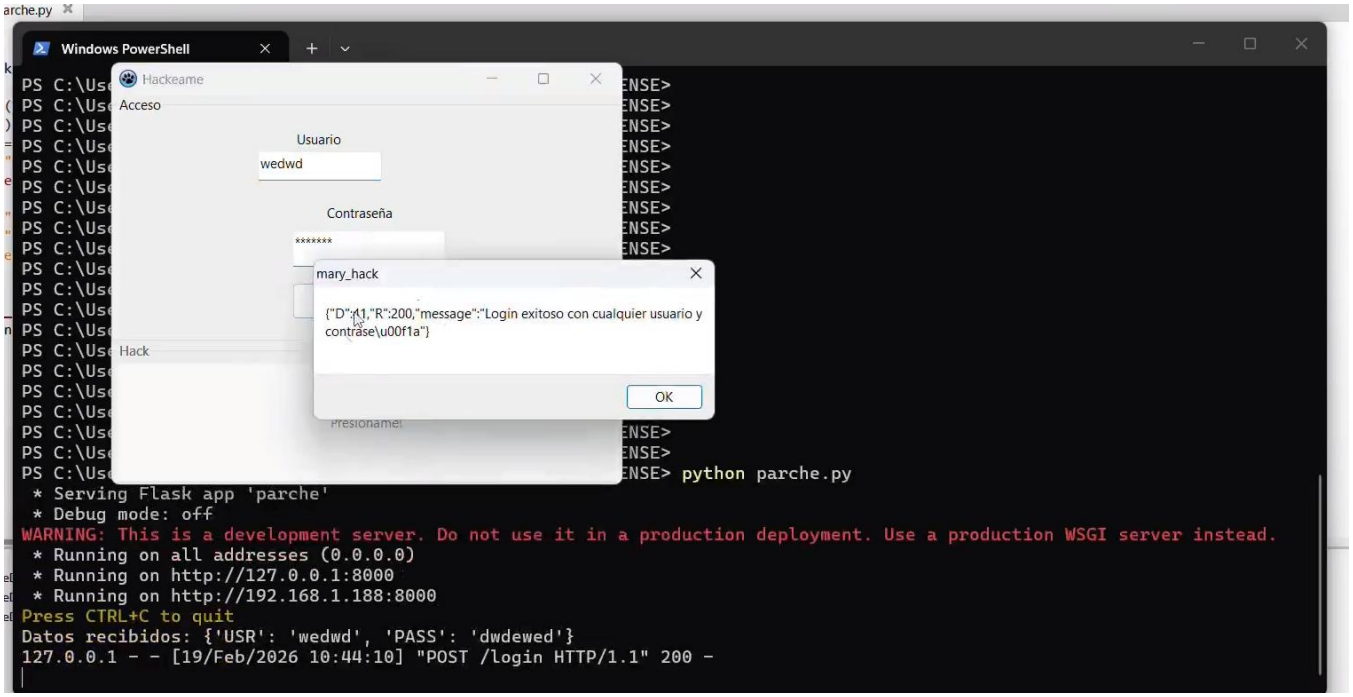
```python
from flask import Flask, request, jsonify

app = Flask(__name__)

@app.route('/login', methods=['POST'])
def login():
    datos = request.json
    print("Datos recibidos:", datos)  # sigue mostrando lo que envían
    # Puedes personalizar la respuesta si quieres
    return jsonify({
        "R": 200,    # código de éxito
        "D": 41,     # valor que quieras mantener
        "message": "Login exitoso con cualquier usuario y contraseña"
    })

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=8000)
```

Ejecutamos nuestro script de Python

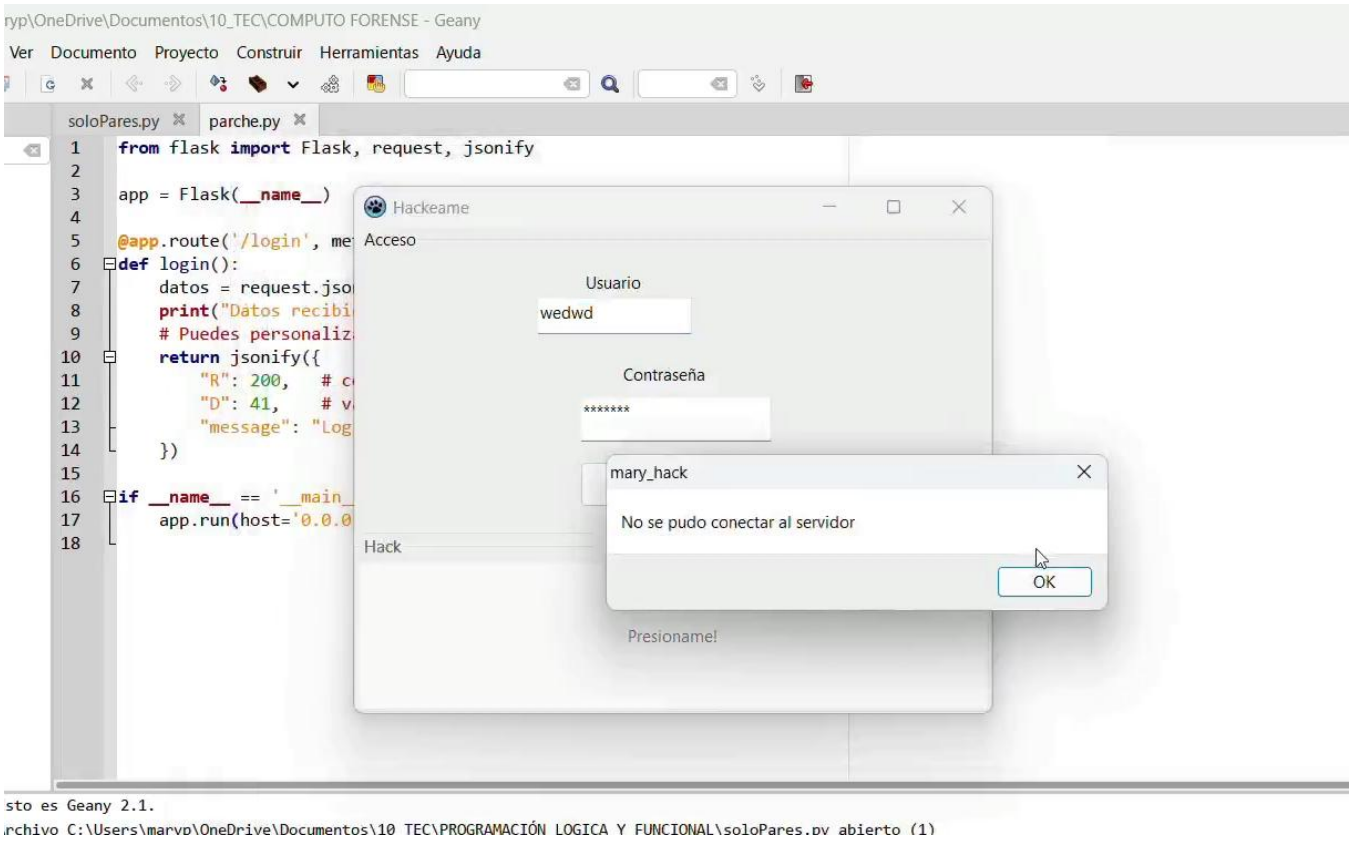
Windows PowerShell | Símbolo del sistema

```
127.0.0.1 - - [19/Feb/2026 17:37:47] "POST /login HTTP/1.1" 200 -
PS C:\Users\maryp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE> python parche.py
 * Serving Flask app 'parche'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:8000
 * Running on http://192.168.224.125:8000
Press CTRL+C to quit
Datos recibidos: {'USR': 'naranja', 'PASS': 'Cyber123456'}
127.0.0.1 - - [19/Feb/2026 17:40:50] "POST /login HTTP/1.1" 200 -
Datos recibidos: {'USR': 'naranja', 'PASS': 'Cyber123456651651+'}
127.0.0.1 - - [19/Feb/2026 17:40:58] "POST /login HTTP/1.1" 200 -
Datos recibidos: {'USR': 'naranja', 'PASS': 'Cyber123456651651+'}
127.0.0.1 - - [19/Feb/2026 17:41:30] "POST /login HTTP/1.1" 200 -
Datos recibidos: {'USR': 'bggb', 'PASS': 'btbg'}
127.0.0.1 - - [19/Feb/2026 18:00:58] "POST /login HTTP/1.1" 200 -
PS C:\Users\maryp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE>
PS C:\Users\maryp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE>
PS C:\Users\maryp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE>
PS C:\Users\maryp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE>
PS C:\Users\maryp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE> python parche.py
 * Serving Flask app 'parche'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:8000
 * Running on http://192.168.224.125:8000
Press CTRL+C to quit
```

Comoprobamos en el ejecutable si esta correcto y podemos acceder con cualquier usuario y contraseña que deseemos



Y para corroborar que si es verdad que solo es con el código de Python nos salimos y comprobamos que el ejecutable ya no funciona con cualquier usuario y contraseña


ryp\OneDrive\Documentos\10_TEC\COMPUTO FORENSE - Geany
Ver Documento Proyecto Construir Herramientas Ayuda
soloPares.py
parche.py
from flask import Flask, request, jsonify
app = Flask(__name__)
@app.route('/login', me
def login():
datos = request.jso
print("Datos recibi
# Puedes personaliz
return jsonify({
"R": 200, # c
"D": 41, # v
"message": "Log
})
if __name__ == '__main_
app.run(host='0.0.0
Hackeame
Acceso
Usuario
wedwd
Contraseña
****
Hack
Presioname!
mary_hack
No se pudo conectar al servidor
OK
sto es Geany 2.1.
rchivo C:\Users\marvp\OneDrive\Documentos\10 TEC\PROGRAMACIÓN LOGICA Y FUNCIONAL\soloPares.py abierto (1)