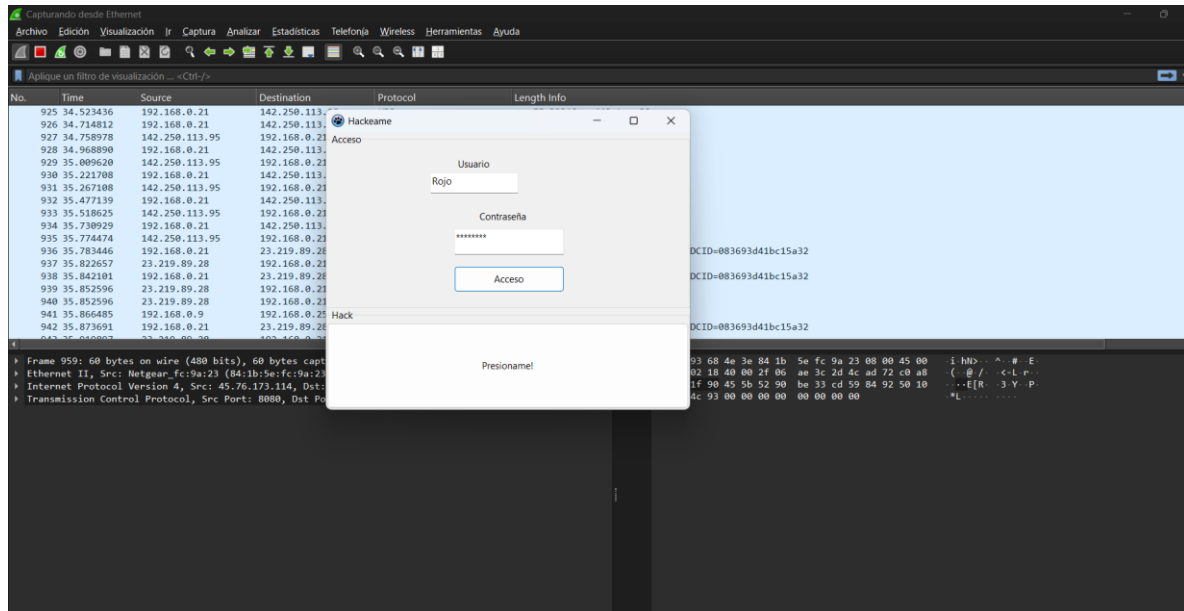
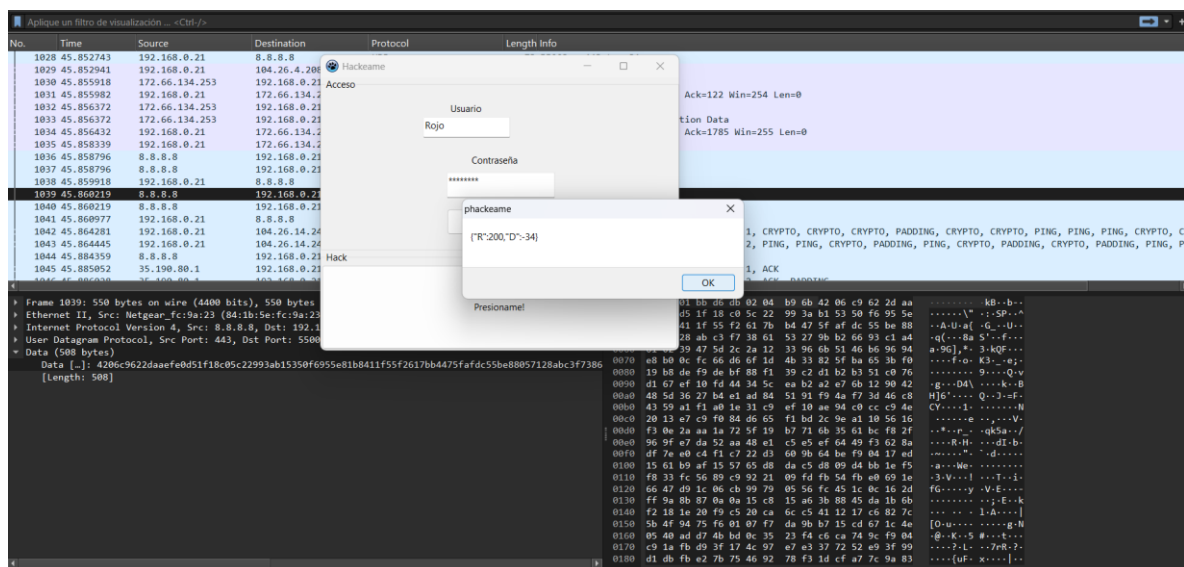


Primero realizaremos una prueba para poder a que IP es a la que se están mandando los paquetes para interceptarlos, para esto ejecutaremos el programa, ingresaremos la contraseña y el usuario.



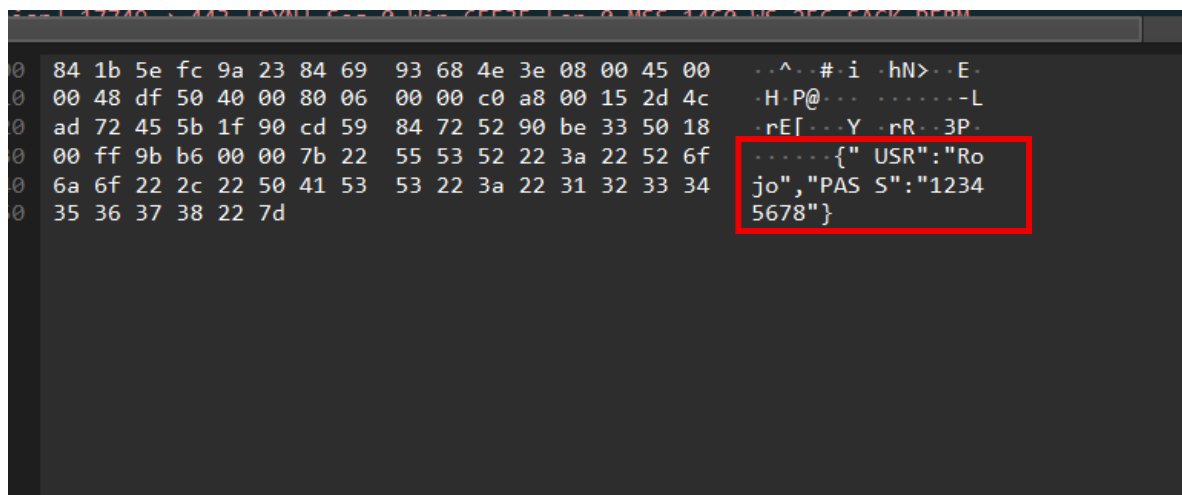
Una vez ya ejecutado el programa y de haber ingresado una contraseña y usuario buscamos con ayuda de WIRESHARK a que IP es con la que se está haciendo la conexión.



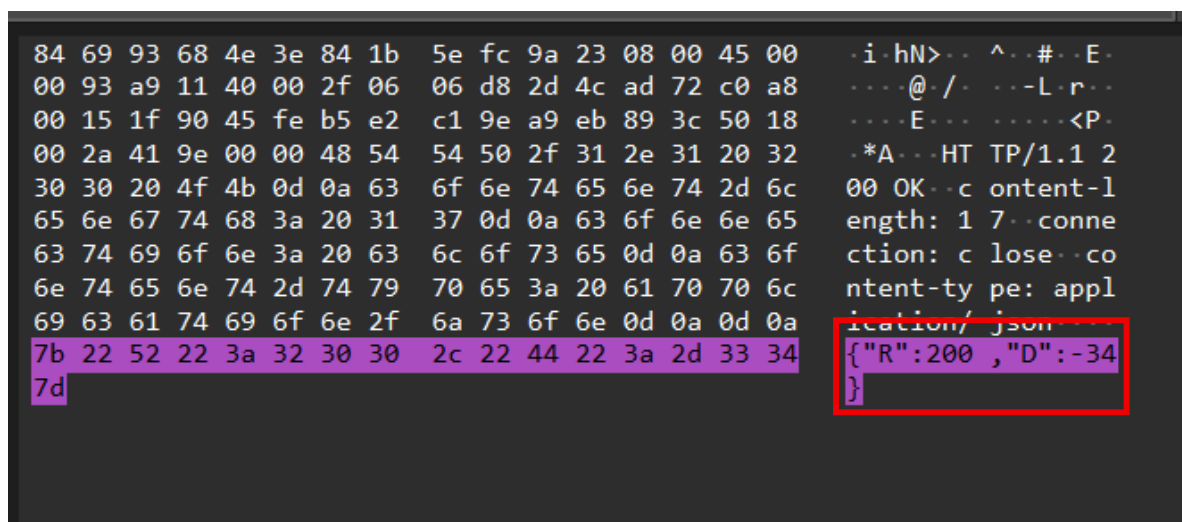
En Wireshark una vez detectados los paquetes de la conexión verificamos a que IP se mandan que en este caso es la IP 45.76.173.114.

952	39.237069	192.168.0.21	45.76.173.114	TCP	66	17755 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
953	39.322935	45.76.173.114	192.168.0.21	TCP	66	8080 → 17755 [SYN, ACK] Seq=0 Ack=1 Min=42340 Len=0 MSS=1460 SACK_PERM WS=1024
954	39.323070	192.168.0.21	45.76.173.114	TCP	54	17755 → 8080 [ACK] Seq=1 Ack=1 Min=65280 Len=0
955	39.341368	192.168.0.21	45.76.173.114	TCP	311	17755 → 8080 [PSH, ACK] Seq=1 Ack=1 Min=65280 Len=257 [TCP PDU reassembled in 957]
956	39.420000	45.76.173.114	192.168.0.21	TCP	60	8080 → 17755 [ACK] Seq=1 Ack=258 Min=43008 Len=0
957	39.420644	192.168.0.21	45.76.173.114	HTTP/JSON	86	POST /login HTTP/1.1, 2506 (application/json)
958	39.450874	45.76.173.114	192.168.0.21	TCP	66	[TCP Retransmission] 17748 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
959	39.505537	45.76.173.114	192.168.0.21	TCP	60	8080 → 17755 [ACK] Seq=1 Ack=290 Min=43008 Len=0
960	39.505537	45.76.173.114	192.168.0.21	HTTP/JSON	161	HTTP/1.1 200 OK, JSON (application/json)
961	39.505537	45.76.173.114	192.168.0.21	TCP	60	8080 → 17755 [FIN, ACK] Seq=100 Ack=290 Min=43008 Len=0
962	39.505661	192.168.0.21	45.76.173.114	TCP	54	17755 → 8080 [ACK] Seq=290 Ack=109 Min=65280 Len=0
963	39.505782	192.168.0.21	45.76.173.114	TCP	54	17755 → 8080 [FIN, ACK] Seq=290 Ack=109 Min=65280 Len=0
964	39.591093	45.76.173.114	192.168.0.21	TCP	60	8080 → 17755 [ACK] Seq=109 Ack=291 Min=43008 Len=0

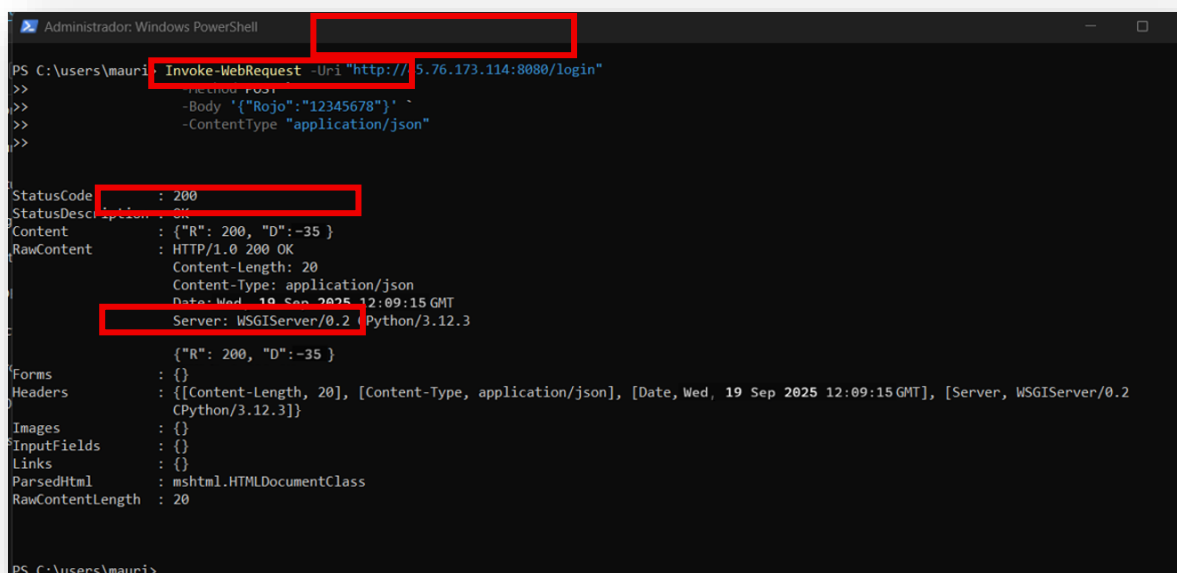
Aquí podemos observar también los datos que mandamos que seria el usuario con el que ingresamos y la contraseña.



Y también podemos ver el paquete de la respuesta del programa que nos devolvió cuando intentamos ingresar.



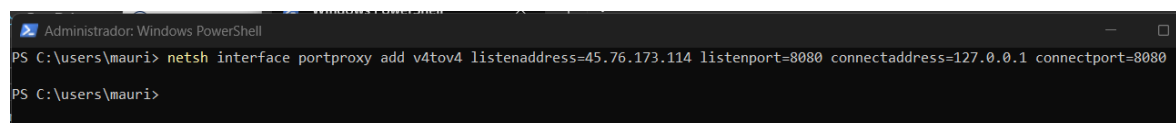
Realizamos la misma ejecución, pero ahora en consola ya con la IP que obtuvimos del proceso anterior, con la misma contraseña y usuario. Y podemos ver que nos devuelve inmediatamente lo que es la respuesta que es la misma que nos mostró con la ejecución anterior



```
Administrador: Windows PowerShell
PS C:\users\mauri> Invoke-WebRequest -Uri "http://45.76.173.114:8080/login"
>> -Method POST
>> -Body '{"Rojo":"12345678"}'
>> -ContentType "application/json"
>>

StatusCode      : 200
StatusDescription: OK
Content         : {"R": 200, "D": -35 }
RawContent      : HTTP/1.0 200 OK
                  Content-Length: 20
                  Content-Type: application/json
                  Date: Wed, 19 Sep 2025 12:09:15 GMT
                  Server: WSGIServer/0.2 (Python/3.12.3)
                  {"R": 200, "D": -35 }
Forms           : {}
Headers         : {[Content-Length, 20], [Content-Type, application/json], [Date, Wed, 19 Sep 2025 12:09:15 GMT], [Server, WSGIServer/0.2
                  CPython/3.12.3]}
Images          : {}
InputFields     : {}
Links           : {}
ParsedHtml      : mshtml.HTMLDocumentClass
RawContentLength: 20
PS C:\users\mauri>
```

Para interceptar los paquetes durante la conexión vamos a redirigir los paquetes a IP local que en este caso redirigimos los paquetes de 45.76.173.114 a 127.0.0.1



```
Administrador: Windows PowerShell
PS C:\users\mauri> netsh interface portproxy add v4tov4 listenaddress=45.76.173.114 listenport=8080 connectaddress=127.0.0.1 connectport=8080
PS C:\users\mauri>
```

Ejecutamos el comando para observar las interfaces y verificar que este correcto.

```
Administrador: Windows PowerShell
PS C:\users\mauri> netsh interface portproxy add v4tov4 list
PS C:\users\mauri> netsh interface portproxy show all

Escuchar en ipv4:      Conectar a ipv4:

Dirección      Puerto      Dirección      Puerto
-----
45.76.173.114   8080        127.0.0.1      8080

PS C:\users\mauri>
```

Y realizamos la ejecución del programa y como podemos observar redirige los paquetes y nos muestra ya otra respuesta diferente.

```
PS C:\users\mauri> Invoke-WebRequest -Uri "http://45.76.173.114:8080/login"
>>
>> -Body '{"Rojo":"12345678"}'
>> -ContentType "application/json"
>>

StatusCode      : 200
StatusDescription : OK
Content         : {"R": 200, "D": 199}
RawContent      : HTTP/1.0 200 OK
                  Content-Length: 20
                  Content-Type: application/json
                  Date: Wed, 19 Sep 2025 12:11:17 GMT
                  Server: WSGIServer/0.2 CPython/3.12.3

                  {"R": 200, "D": 199}

Forms           : {}
Headers         : {[Content-Length, 20], [Content-Type, application/json], [Date, Wed, 19 Sep 2025 12:11:17 GMT], [Server, WSGIServer/0.2
                  CPython/3.12.3]}
Images          : {}
InputFields     : {}
Links           : {}
ParsedHtml      : mshtml.HTMLDocumentClass
RawContentLength : 20
```