Línea horizontal

**CIM31\_07**

Ignacio García García

Guillermo Rojo Martín

Pablo Ramiro Foronda Iraizós

Marianela Estévez Bosso

Práctica Criptografía Aplicada

**Seguridad en Sistemas y Redes**

# INTRODUCCIÓN

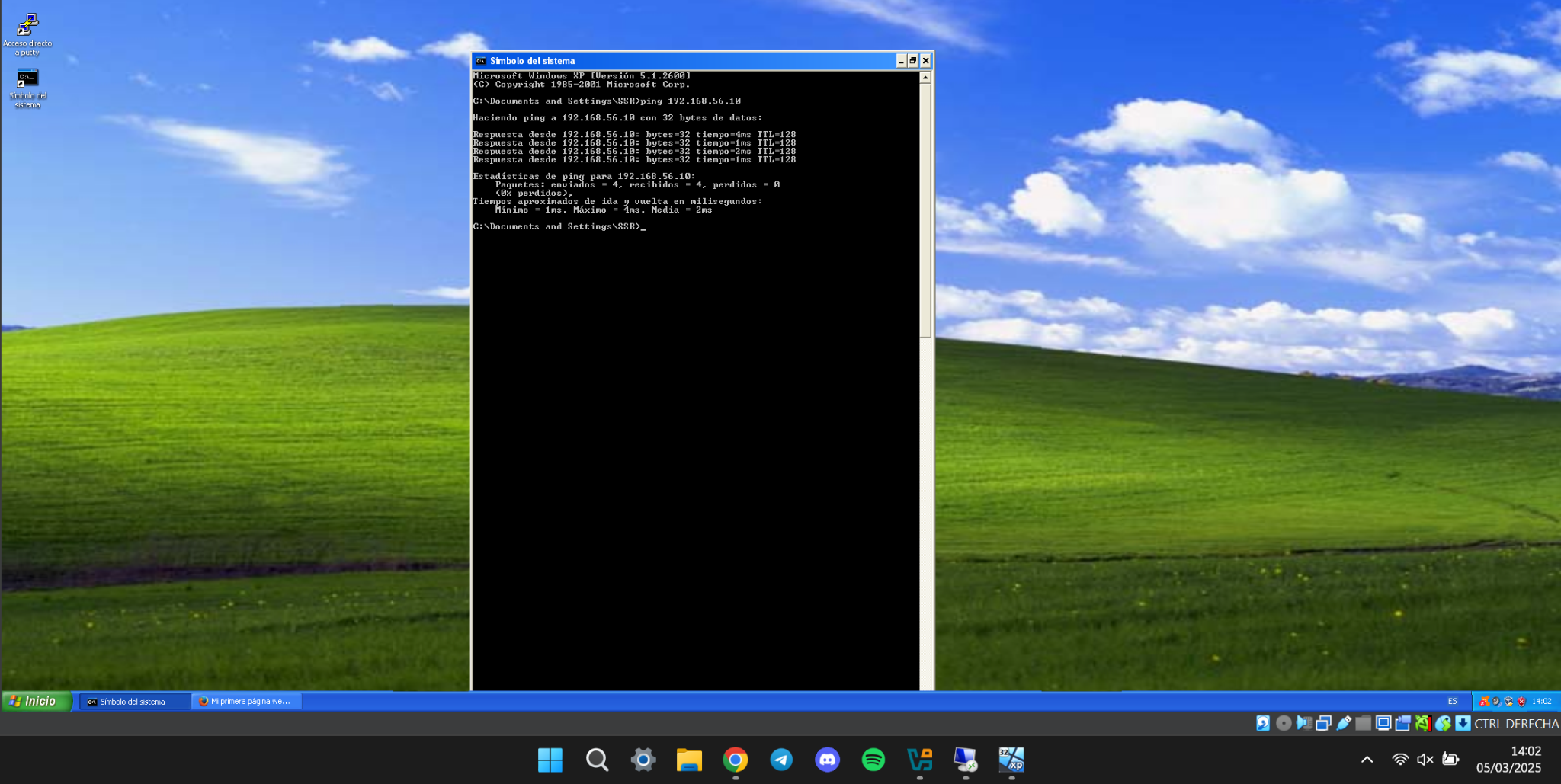
Esta memoria documenta el proceso de implementación de medidas de seguridad avanzadas para proteger la información durante la transmisión y el almacenamiento. A través de la configuración de un servidor web, la generación de certificados digitales y el análisis del tráfico de red Wireshark, demostramos la diferencia entre las comunicaciones seguras e inseguras. Además de explorar el uso de OpenSSL para cifrar datos y firmar digitalmente documentos, garantizando confidencialidad, integridad y autenticidad de la información.

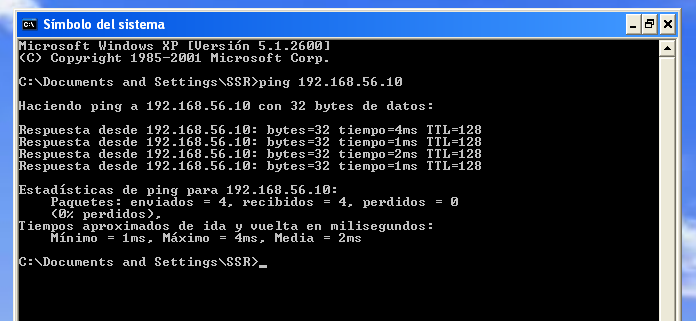
# PRUEBAS REALIZADAS Y RESULTADOS

## Conectividad ICMP (ping) entre cliente y servidor

**Captura ping XP a W10**

Se ejecutó el comando ping desde Windows XP hasta Windows 10, cuya dirección IP es 192.168.56.10.



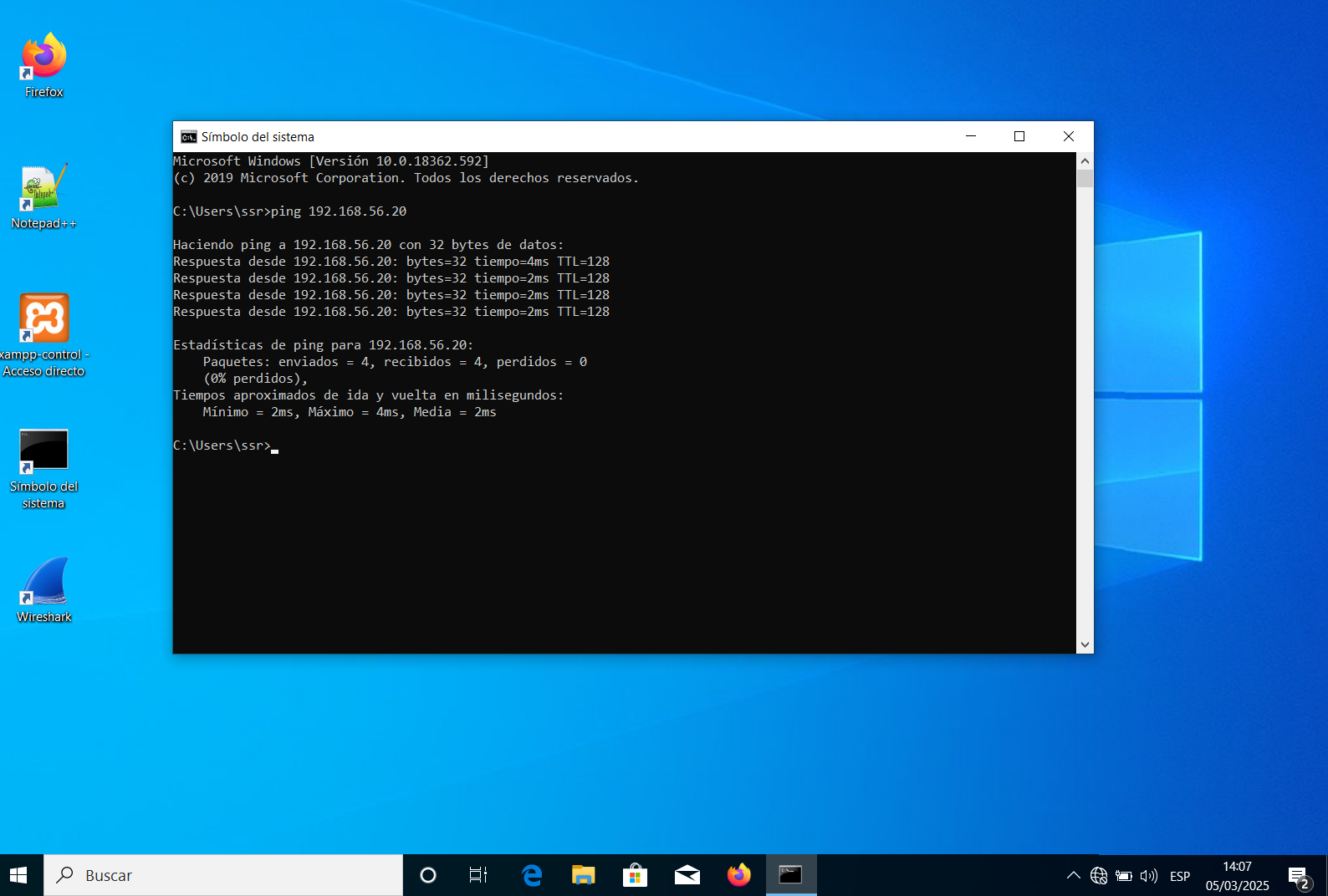


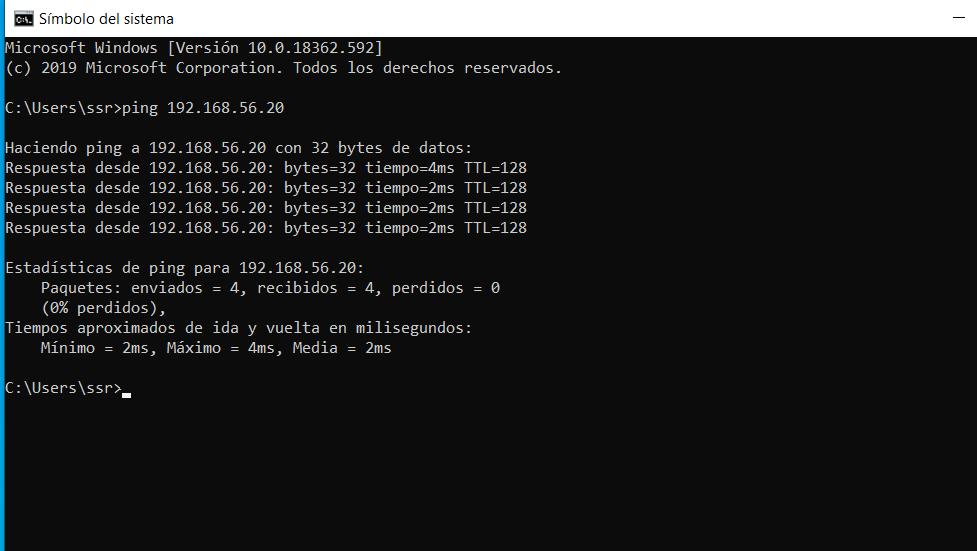
Análisis de la captura:

* Se enviaron 4 paquetes ICMP de 32 bytes desde el host (XP) hacia el destino (W10)
* Todos los paquetes fueron recibidos correctamente, sin pérdidas. Lo que indica una comunicación bidireccional funcional entre ambas máquinas en la red.
* Los tiempos de respuesta oscilaron entre 1 ms y 4 ms, con un tiempo medio de 2 ms. Los tiempos de respuesta indican una baja latencia en la comunicación, lo que sugiere una conexión de red eficiente entre ambos hosts.
* El TTL (Time To Live) es de 128, valor típico en sistemas WIndows.

**Captura ping de W10 a XP:**

Se ejecutó el comando ping desde Windows 10 hasta Windows XP, cuya dirección IP es 192.168.56.20.



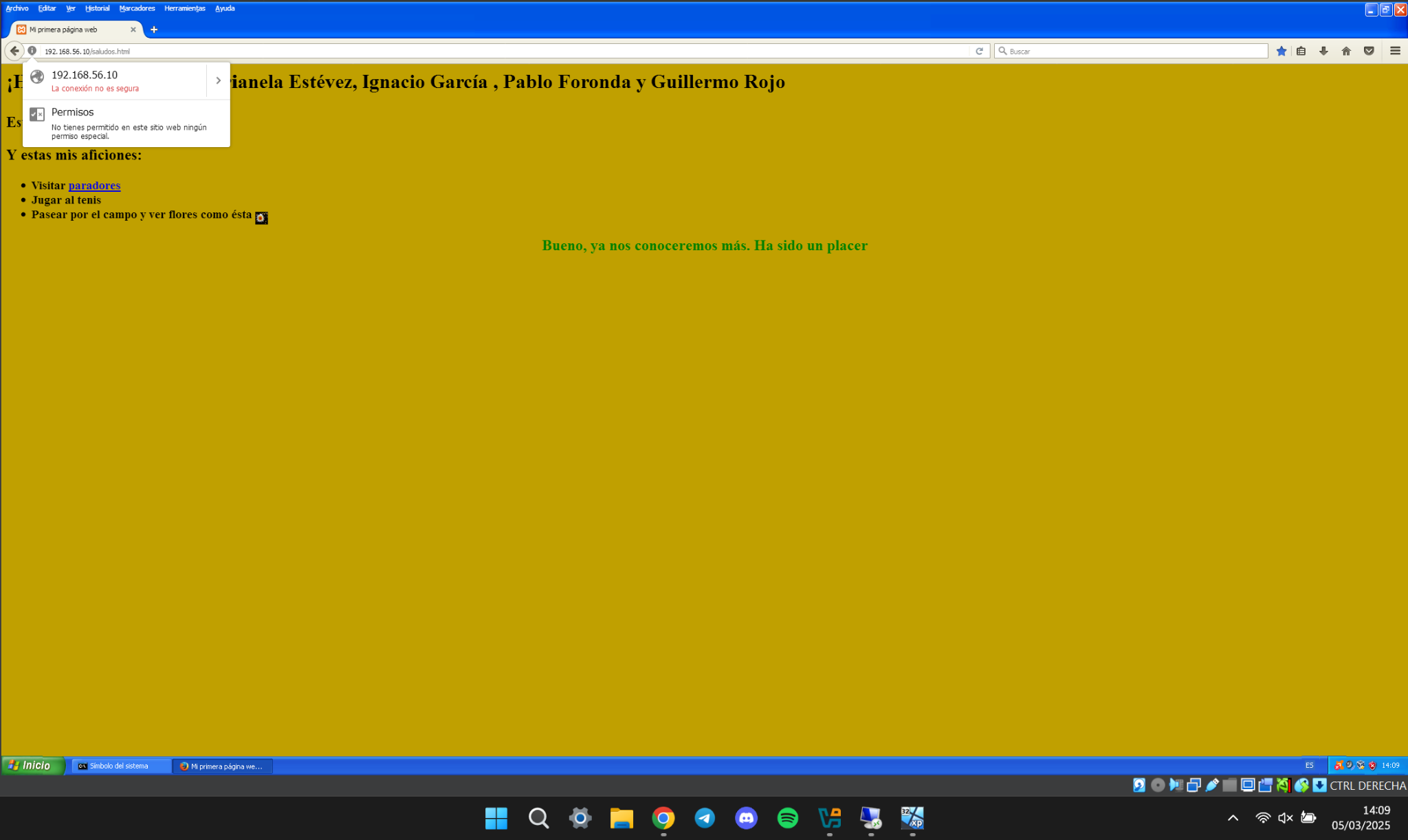


Análisis de la captura:

* Se enviaron 4 paquetes ICMP de 32 bytes a Windows XP
* Todos los paquetes fueron recibidos correctamente, sin pérdidas también. Al igual que en la prueba anterior, esta captura confirma la comunicación bidireccional entre Windows 10 y Windows XP.
* Se puede observar una ligera variación en los tiempos de respuesta, con un mínimo de 2ms y un máximo de 4ms. Esta variación puede deberse a la carga de la red o a otros procesos ejecutándose en las máquinas
* El TTL es de 128, valor predeterminado en sistemas Windows.

## Acceso inseguro HTTP

Para evaluar el acceso inseguro al servidor web se realizó una conexión HTTP utilizando un navegador desde el cliente a la dirección http://192.168.52.10.

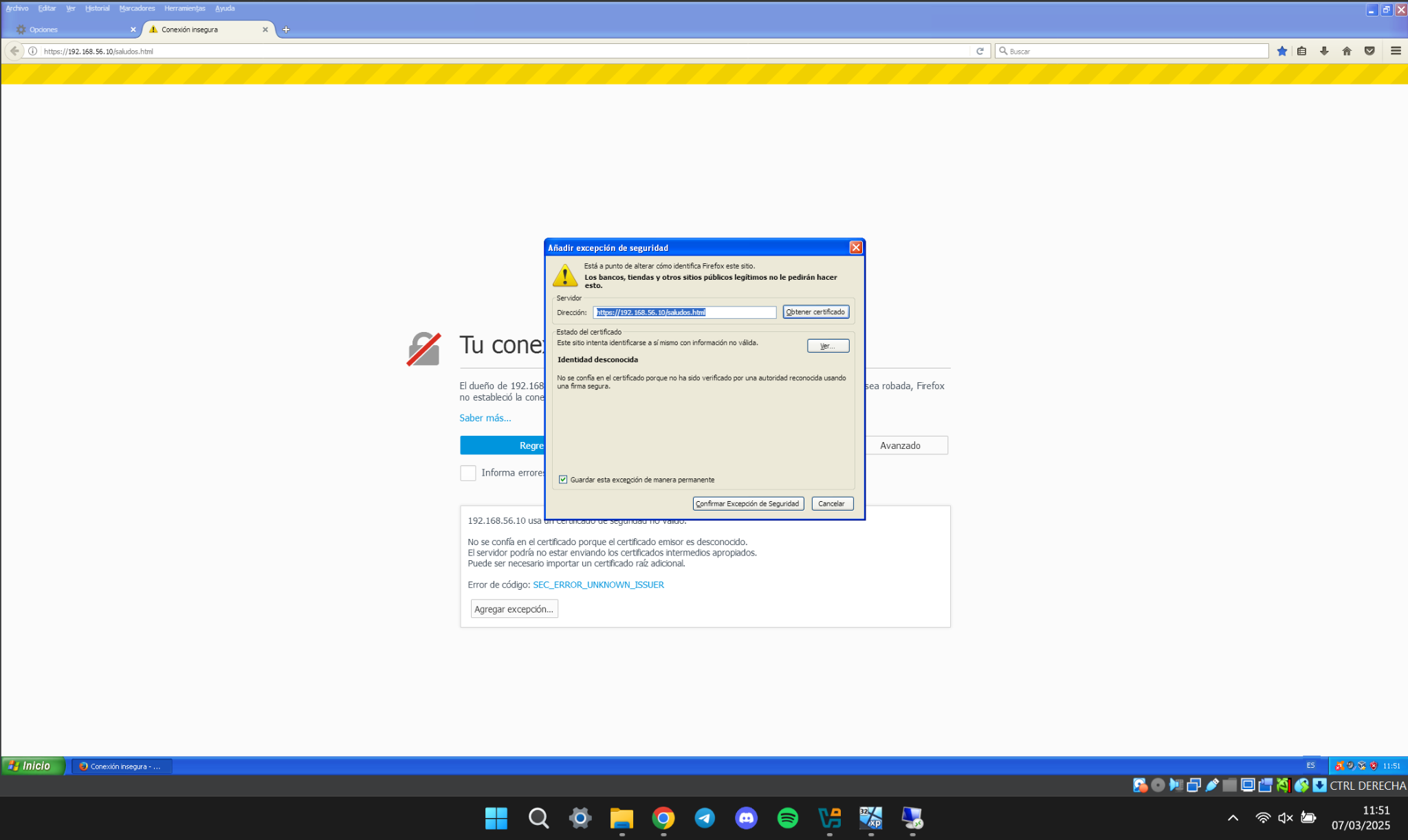


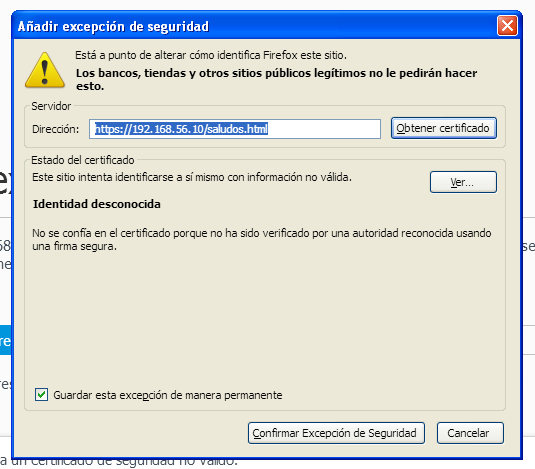
En esta captura de pantalla se muestra el acceso a una página web a través del protocolo HTTP, lo que implica que la comunicación entre el cliente y el servidor no está cifrada.

Análisis de la captura:

* Se observa que la página cargó correctamente, mostrando el contenido alojado en el servidor
* En la barra de direcciones del navegador se puede ver la dirección IP 192.68.56.10, confirmando que el acceso se realizó mediante HTTP y no HTTPS
* Aparece una advertencia indicando que la conexión no es segura, lo que significa que los datos intercambiados no están protegidos.
* Al utilizar HTTP, la información transmitida, puede ser interceptada por terceros malintencionados. Esto subraya la importancia de utilizar HTTPS para proteger la confidencialidad de la información.

## Momento en que se solicita el certificado del usuario en acceso seguro (https)



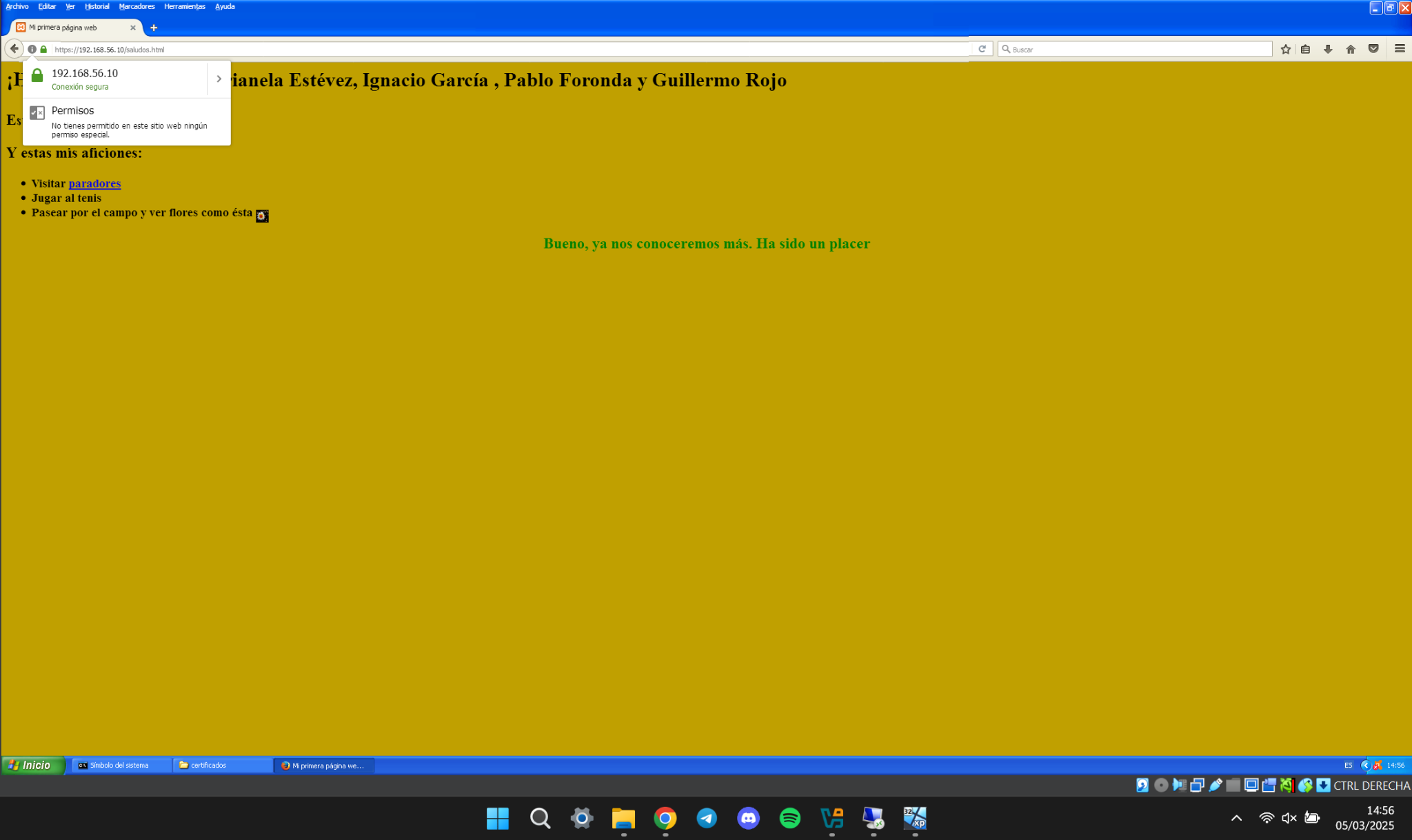


Se muestra una advertencia de seguridad emitida por el navegador, indicando que el sitio web está intentando identificarse a sí mismo con información no válida.

* Certificado no confiable: El navegador advierte que no se confía en el certificado porque no ha sido verificado por una autoridad reconocida utilizando una firma segura.
* Riesgo de agregar excepción: Agregar una excepción de seguridad puede exponer al usuario a riesgos de seguridad.
* Se subraya la importancia de utilizar certificados válidos y emitidos por autoridades de certificación de confianza para garantizar la seguridad de la comunicación HTTPS.

## Acceso seguro HTTPS

Acceso a la misma página web que en el caso de acceso inseguro HTTP, pero esta vez a través del protocolo HTTPS, lo que indica que la comunicación entre el cliente y el servidor está cifrada.



* El navegador muestra un candado verde en la barra de direcciones, lo que confirma que la conexión es segura y que la información transmitida está protegida mediante cifrado SSL/TLS.
* Al hacer clic en el candado se puede verificar que el certificado del servidor es válido y ha sido emitido por una autoridad de certificación de confianza (CA) o, en este caso, por una CA creada.
* En comparación con la captura de pantalla del acceso inseguro HTTP, en este caso se muestra claramente la diferencia en términos de seguridad y confianza.

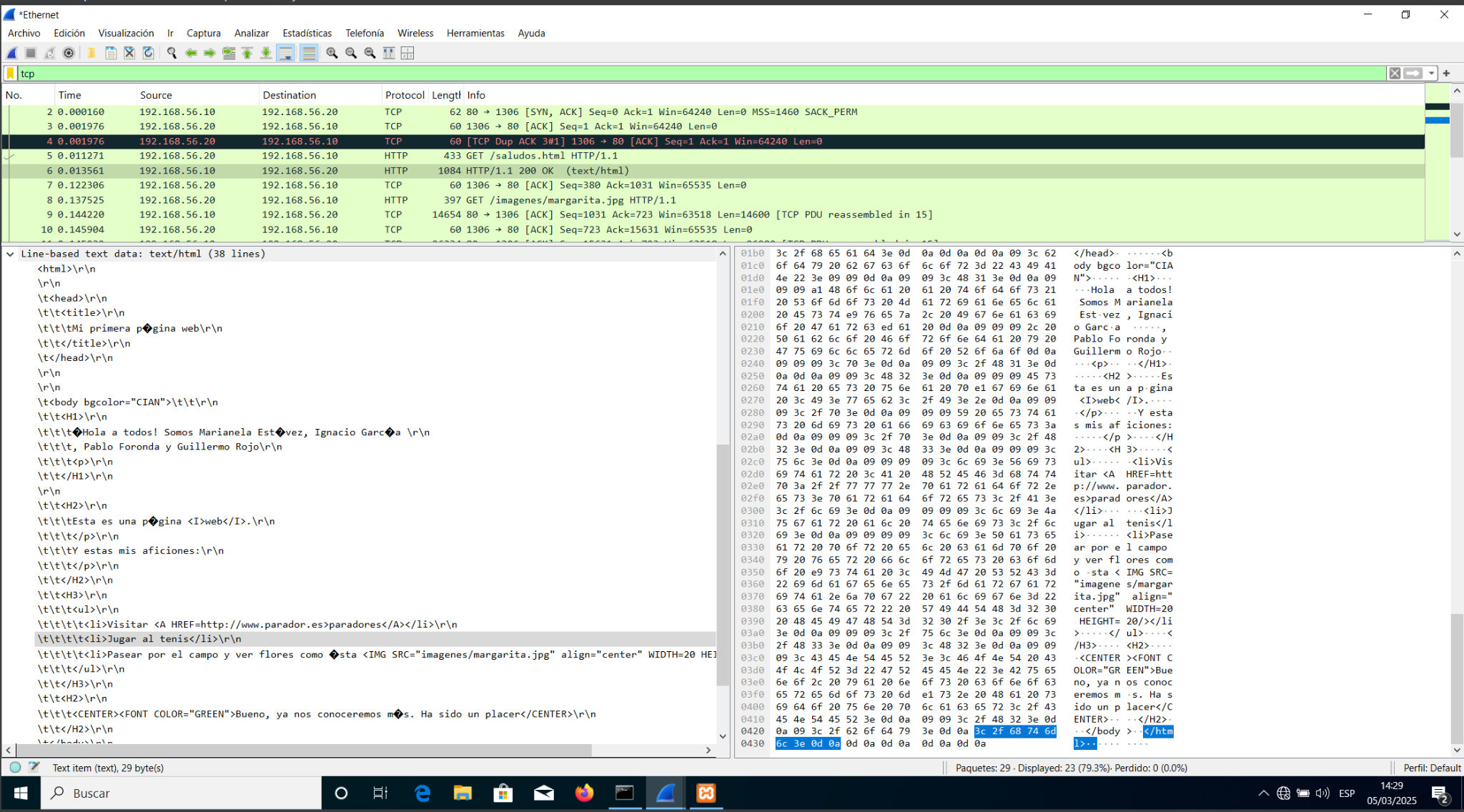
## 

## 

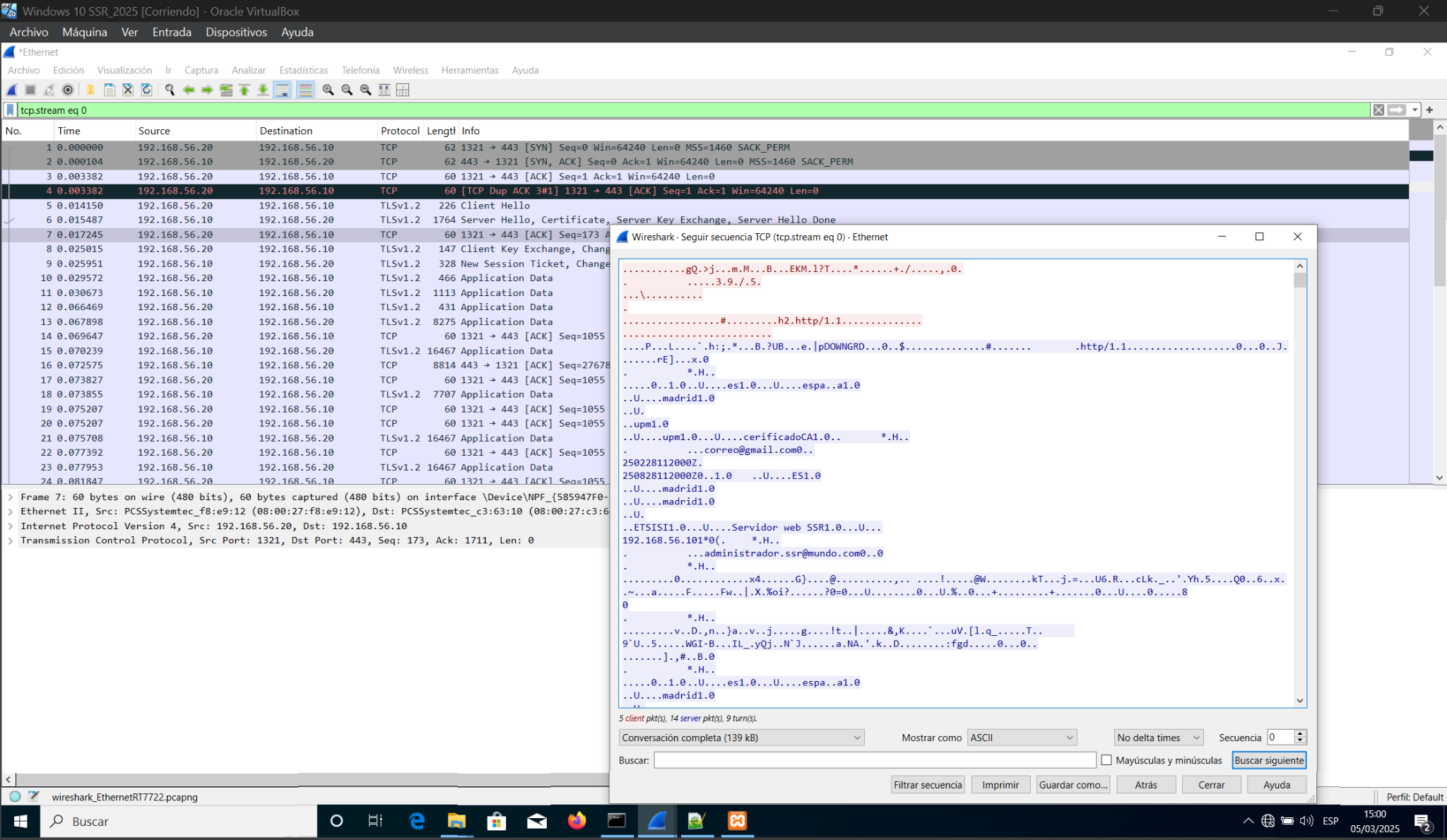
## 

## 

## Análisis de tráfico con Wireshark



Esta imagen nos muestra el acceso inseguro http en los paquetes wireshark, observando que el protocolo usado por los paquetes es http y no https



Aquí podemos observar los paquetes referidos al acceso seguro https, donde vemos que los paquetes usan el protocolo Transport Layer Security referidos al https.