# Actividad | 1 |

## Pérdida de Autenticación y Gestión de Sesiones

### Auditoría Informática

Ingeniería en Desarrollo de Software


**TUTOR: Jessica Hernández Romero**

**ALUMNO: Yanira Lizbeth Lopez Navarro**

**FECHA: 23/06/2024**

# Índice

# Introducción

El ataque de pérdida de autenticación de datos es una amenaza cibernética que afecta gravemente a los usuarios de internet, comprometiendo su seguridad y privacidad. Este tipo de ataque ocurre cuando los sistemas que verifican la identidad de los usuarios fallan, permitiendo que los atacantes accedan a información sensible sin las credenciales adecuadas.

Los usuarios de internet pueden ser víctimas de robo de identidad, donde sus datos personales, como nombres, direcciones y números de tarjetas de crédito, son utilizados fraudulentamente. Además, estos ataques pueden resultar en la pérdida de acceso a cuentas importantes, como correos electrónicos, redes sociales y servicios financieros, causando graves inconvenientes y posibles pérdidas económicas.

La exposición de datos confidenciales puede llevar a problemas de reputación y confianza, tanto para los usuarios afectados como para las empresas involucradas. En el ámbito empresarial, la pérdida de autenticación puede permitir que atacantes internos o externos manipulen datos críticos, afectando la integridad de los sistemas y la continuidad del negocio. Este tipo de ataque subraya la importancia de implementar y mantener sistemas robustos de autenticación y seguridad para proteger a los usuarios de internet.

# Descripción

En esta actividad espero aprender de manera práctica cómo identificar y explotar vulnerabilidades relacionadas con la pérdida de autenticación y la gestión de sesiones en páginas web que carecen de candados de seguridad (SSL). Utilizando WireShark, un potente programa de análisis de tráfico de red, espero adquirir habilidades para interceptar y analizar los datos que se transmiten entre un usuario y el servidor web.

El proceso comenzará con la selección de un proyecto web previo que incluya funciones de inicio de sesión y registro de usuarios, así como una conexión a una base de datos. Subir este proyecto a un servidor web y configurarlo adecuadamente será crucial para simular un entorno realista.

Luego, mediante la instalación y uso de WireShark, espero aprender cómo capturar el tráfico de red para identificar y extraer credenciales que se transmiten sin cifrado. Este ejercicio me permitirá entender mejor las implicaciones de la falta de seguridad en las comunicaciones web y la importancia de implementar medidas como SSL para proteger la información sensible de los usuarios. Además, espero desarrollar una mayor capacidad para realizar auditorías de seguridad y aplicar estas habilidades en la mejora de la protección de aplicaciones web.

# Justificación

Vivimos en una era digital donde gran parte de nuestra vida y actividades cotidianas dependen de la confianza en la seguridad de las plataformas en línea. Sin embargo, muchas páginas web, especialmente aquellas sin SSL, dejan a los usuarios vulnerables a ataques que pueden exponer sus credenciales y datos personales.

Probar la vulnerabilidad de la pérdida de autenticación utilizando WireShark nos permite identificar fallos críticos en la seguridad de estas plataformas. Esta prueba no solo nos enseña a reconocer los riesgos, sino que también nos equipa con el conocimiento necesario para implementar soluciones efectivas. Al interceptar y analizar el tráfico de red, podemos demostrar de manera tangible cómo los datos pueden ser capturados por actores malintencionados, resaltando la importancia de utilizar protocolos de seguridad robustos.

En última instancia, esta actividad nos prepara para proteger mejor a los usuarios finales, asegurando que sus datos permanezcan seguros y confidenciales. A través de estas pruebas, podemos contribuir a crear un entorno digital más seguro y confiable para todos.

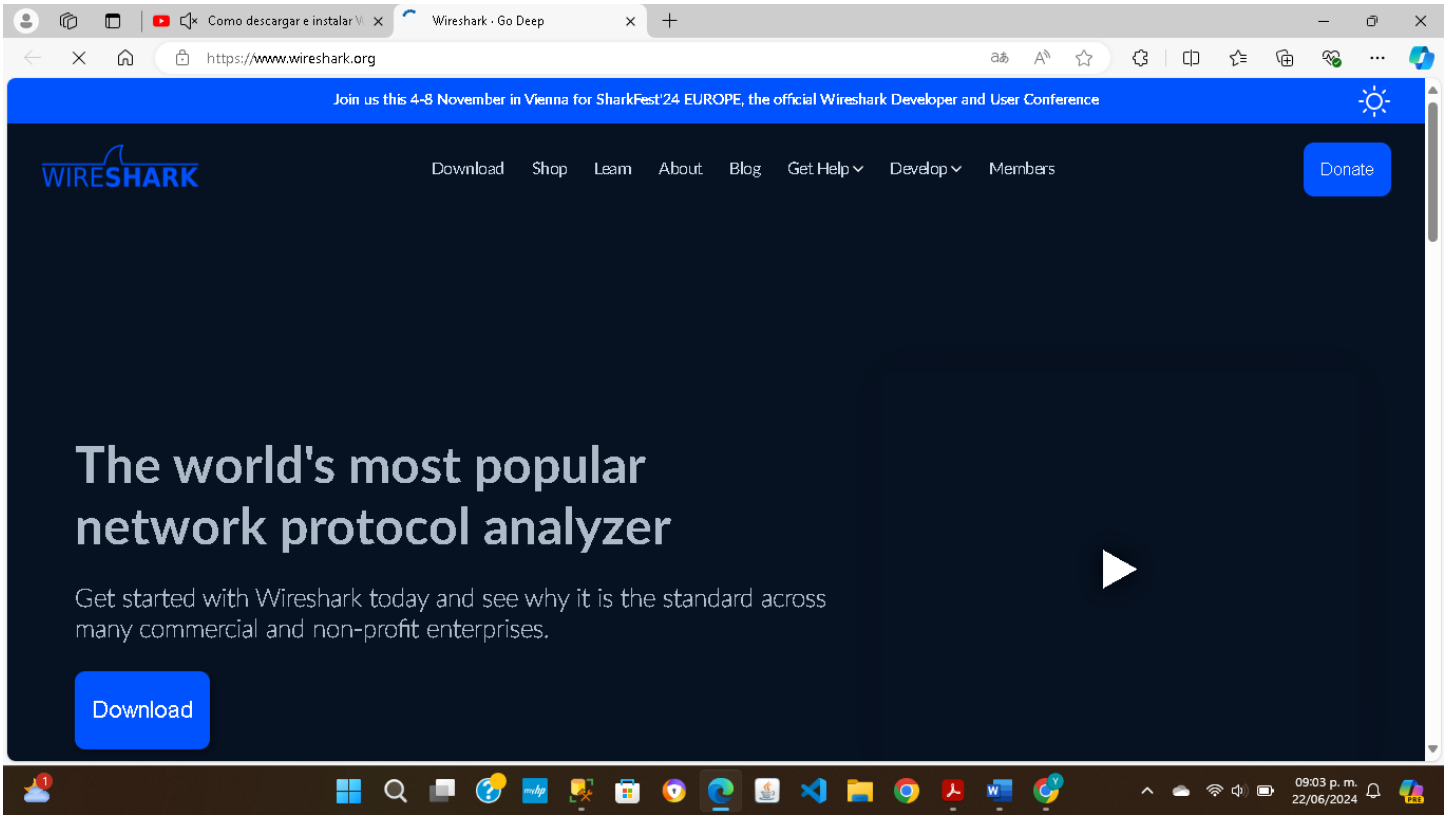
# Descripción del sitio web

De acuerdo a lo solicitado en la actividad se llevó a cabo la Selección de un proyecto web realizado anteriormente, aunque no fue de mi autoría cumple con las características solicitadas en la actividad.

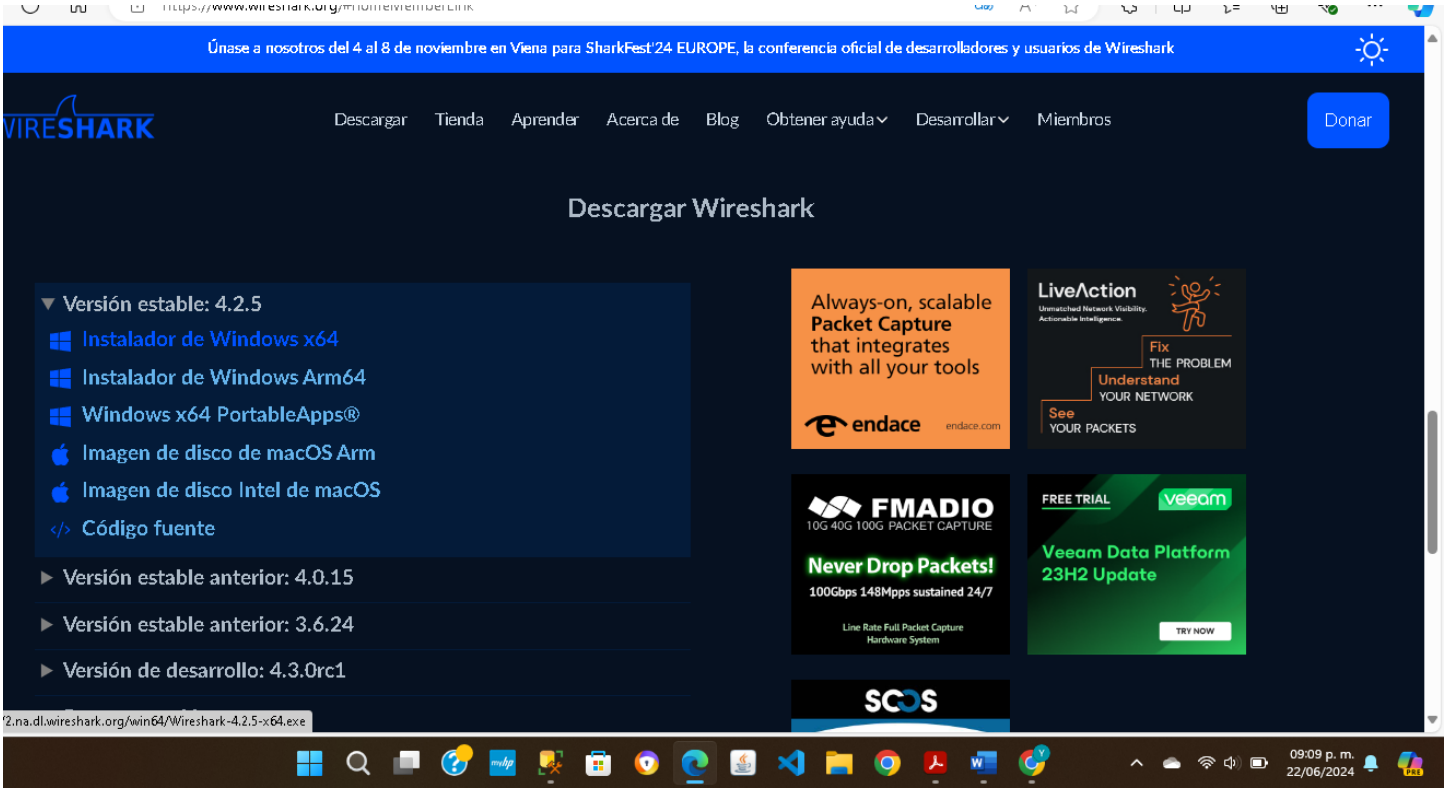
- Función de iniciar sesión y de registro de usuarios
- Conexión con una base de datos

http://www.pruebadeuso.com/index.php?r=site/login

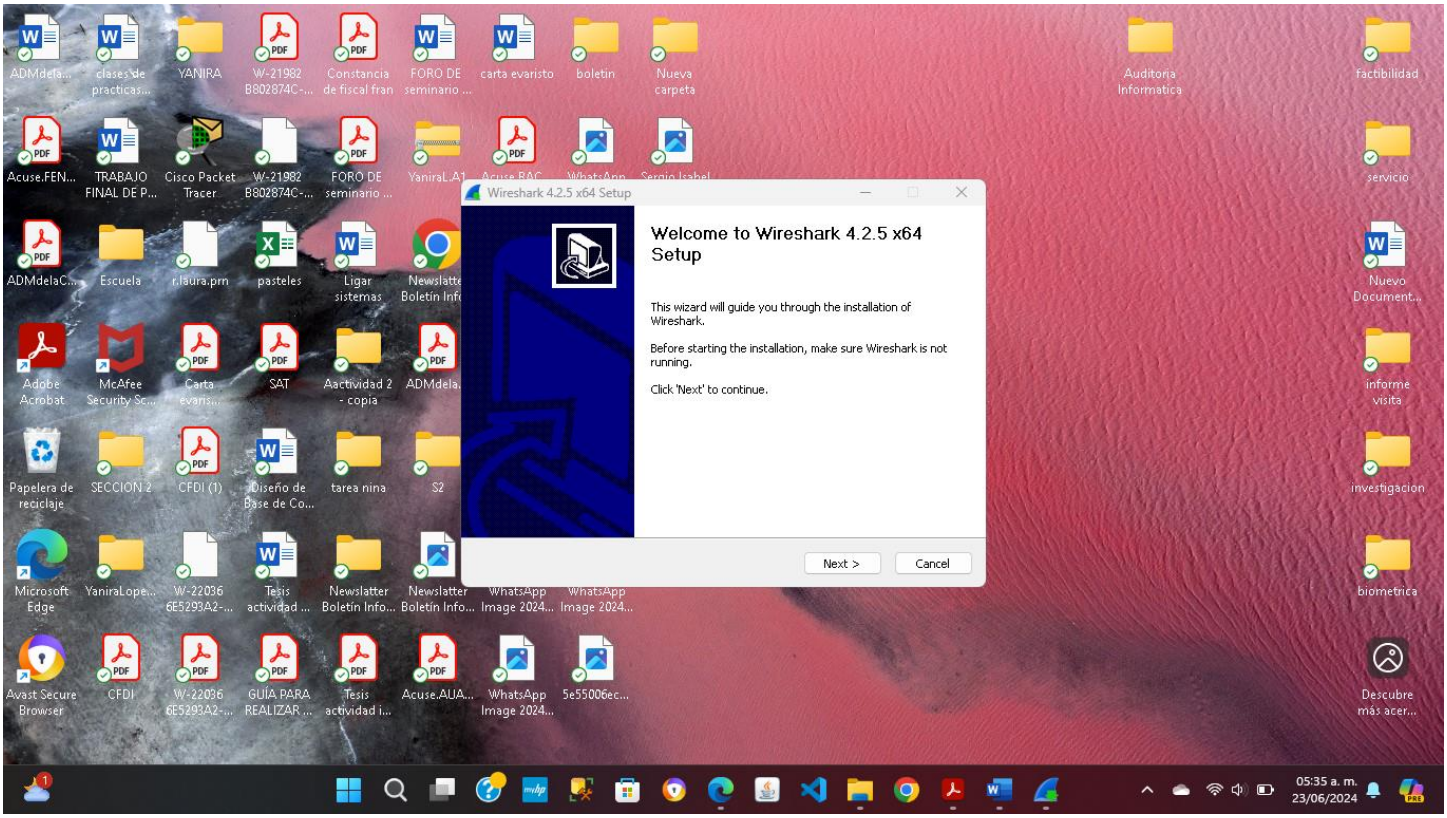
A continuación en la siguiente imagen podemos observar la pagina que nos permite descargar la herramienta recomienda para el desarrollo de la actividad .



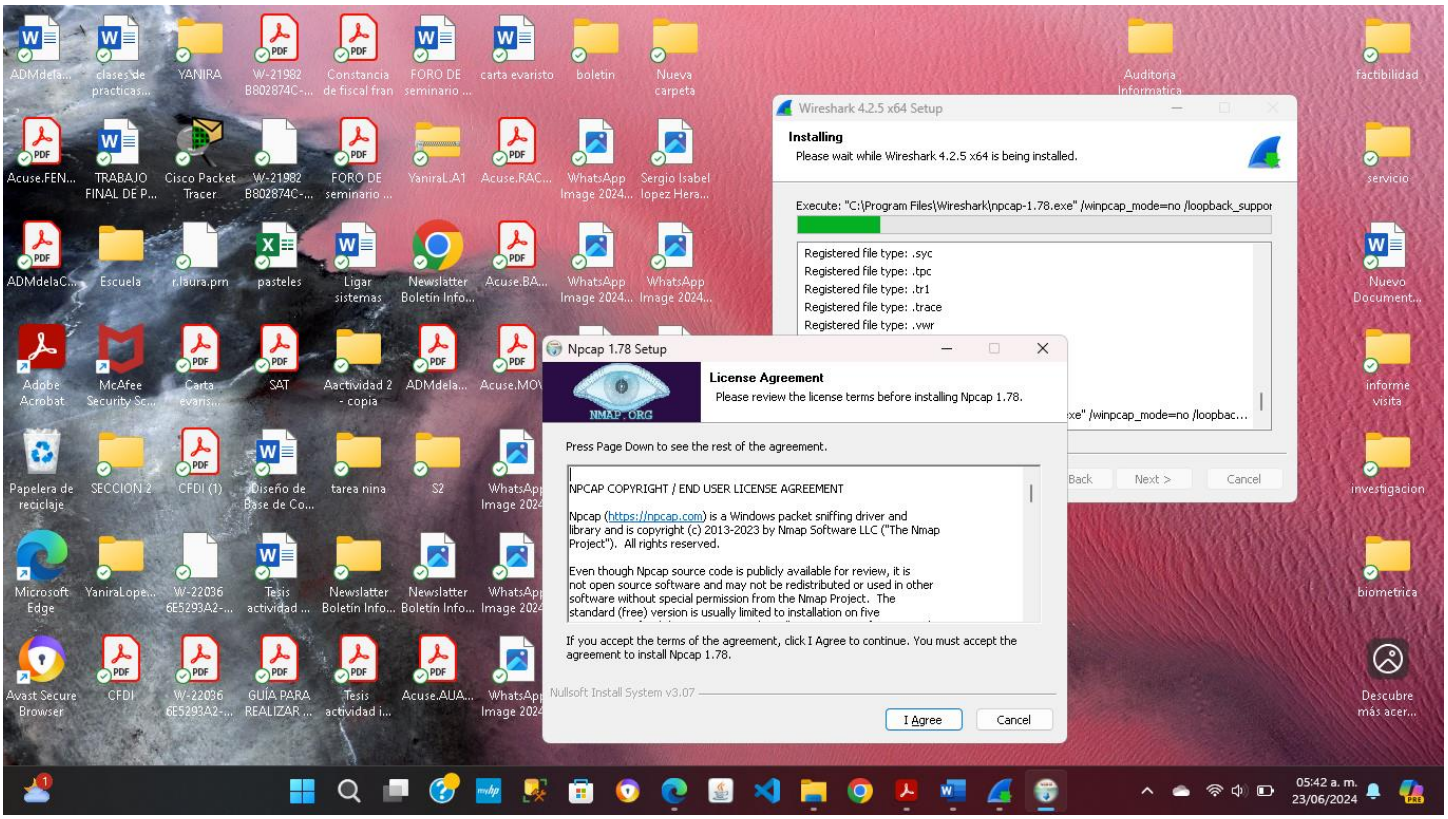
A continuación, seleccionamos es instalador para Windows x64 ya que es el compatible con mi equipo



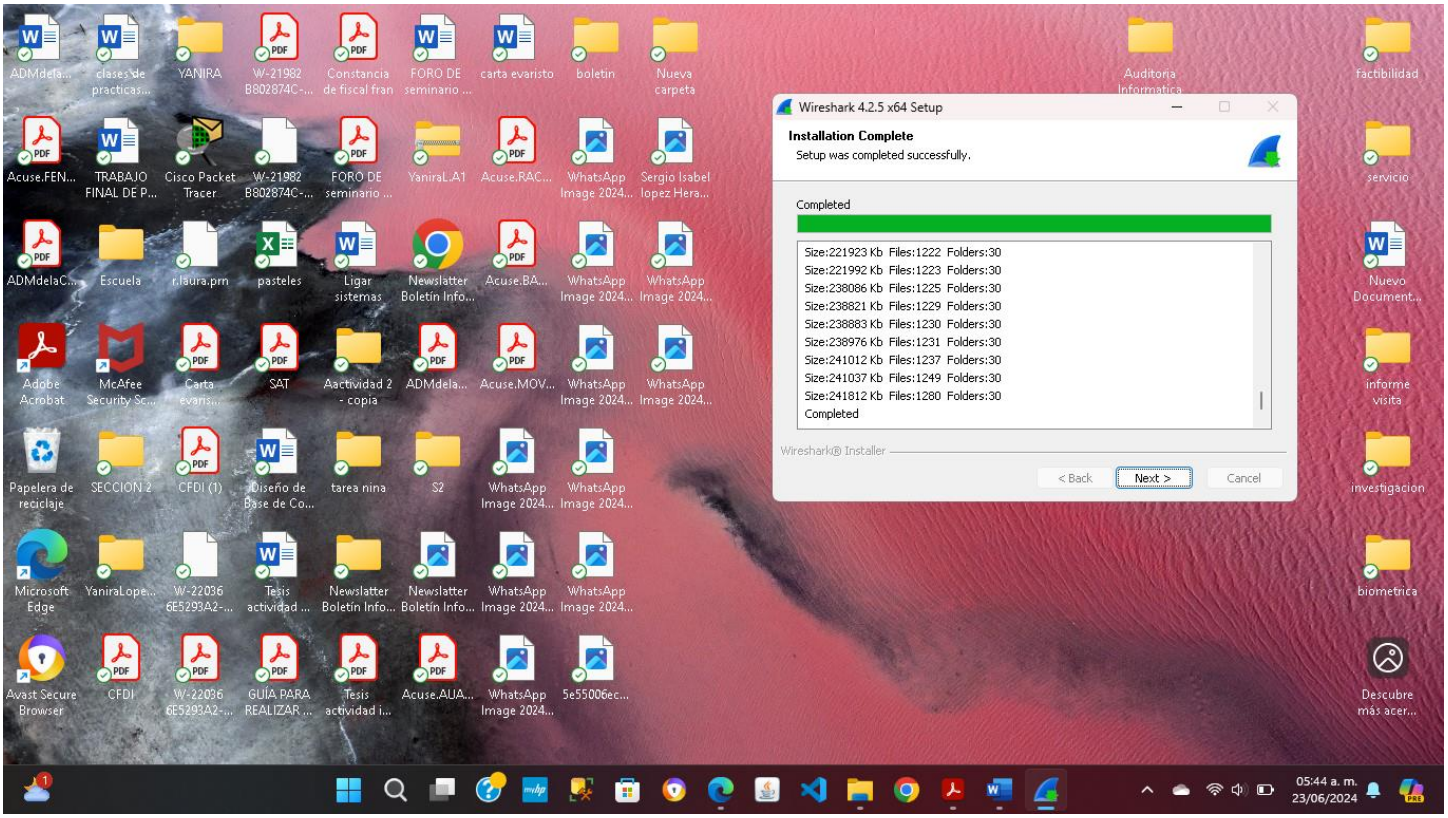

Una vez que WireShark fue descargado procedemos su la instalación.



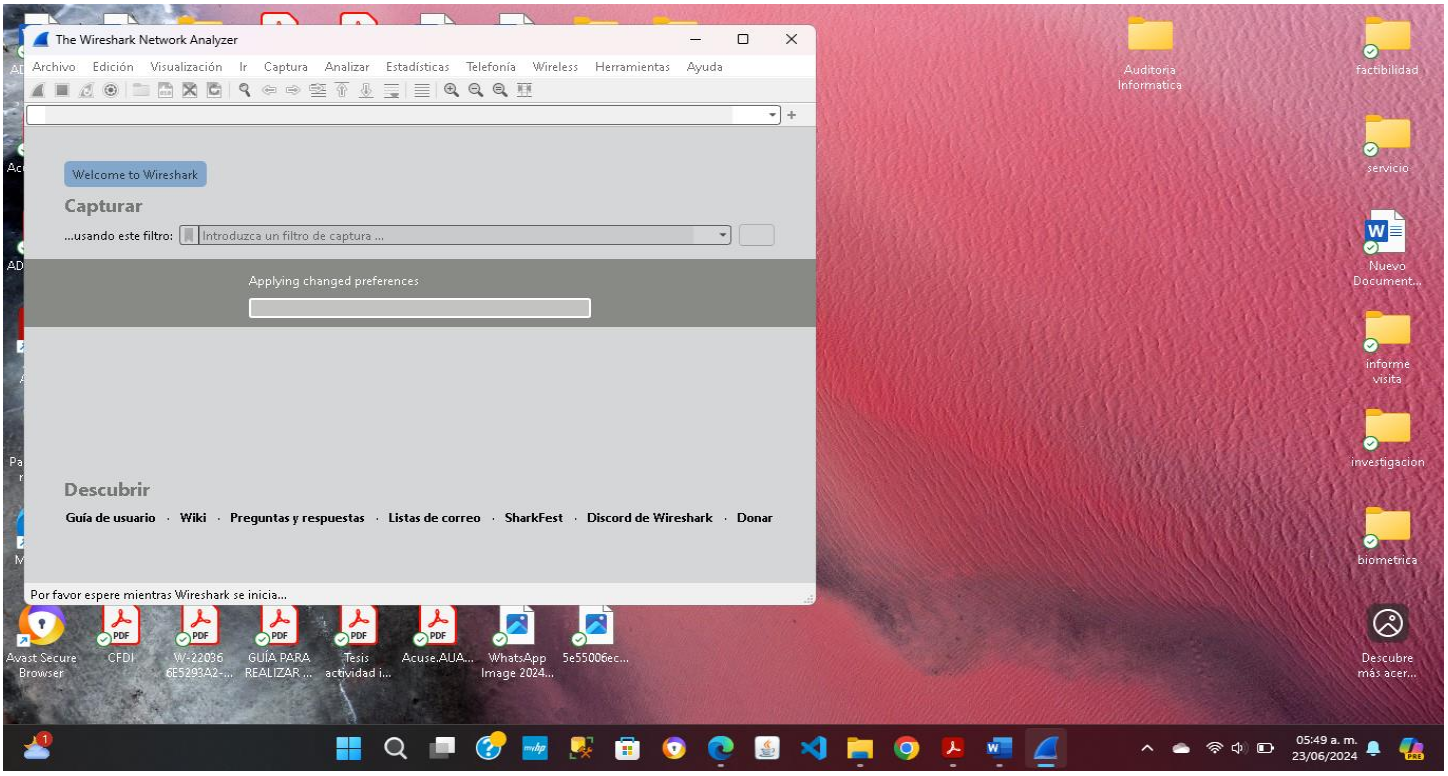
En la siguiente imagen se observa el avance de la instalación de WireShark.



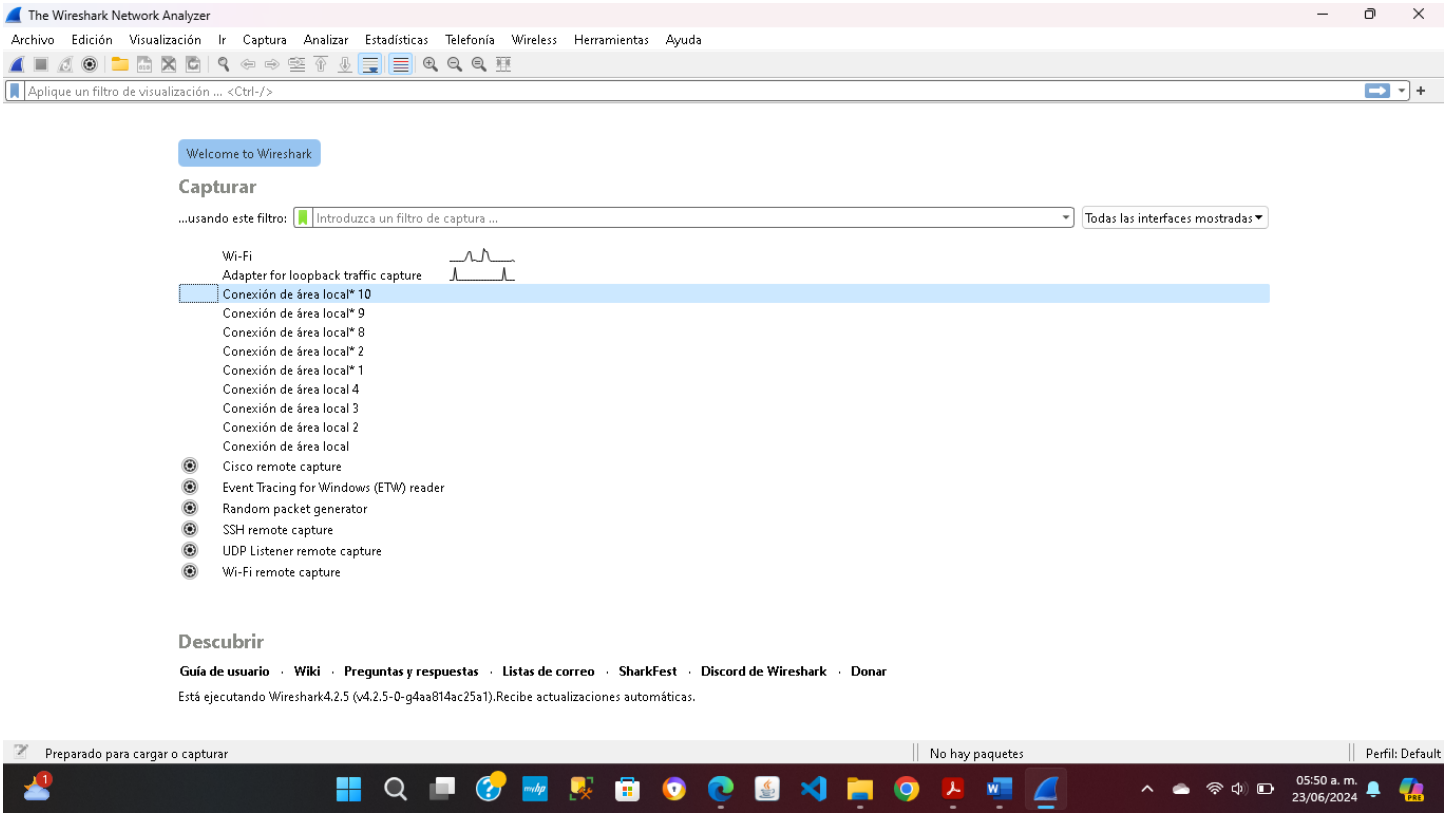

A continuación, podemos observar que esta por finalizar la instalación WireShark.



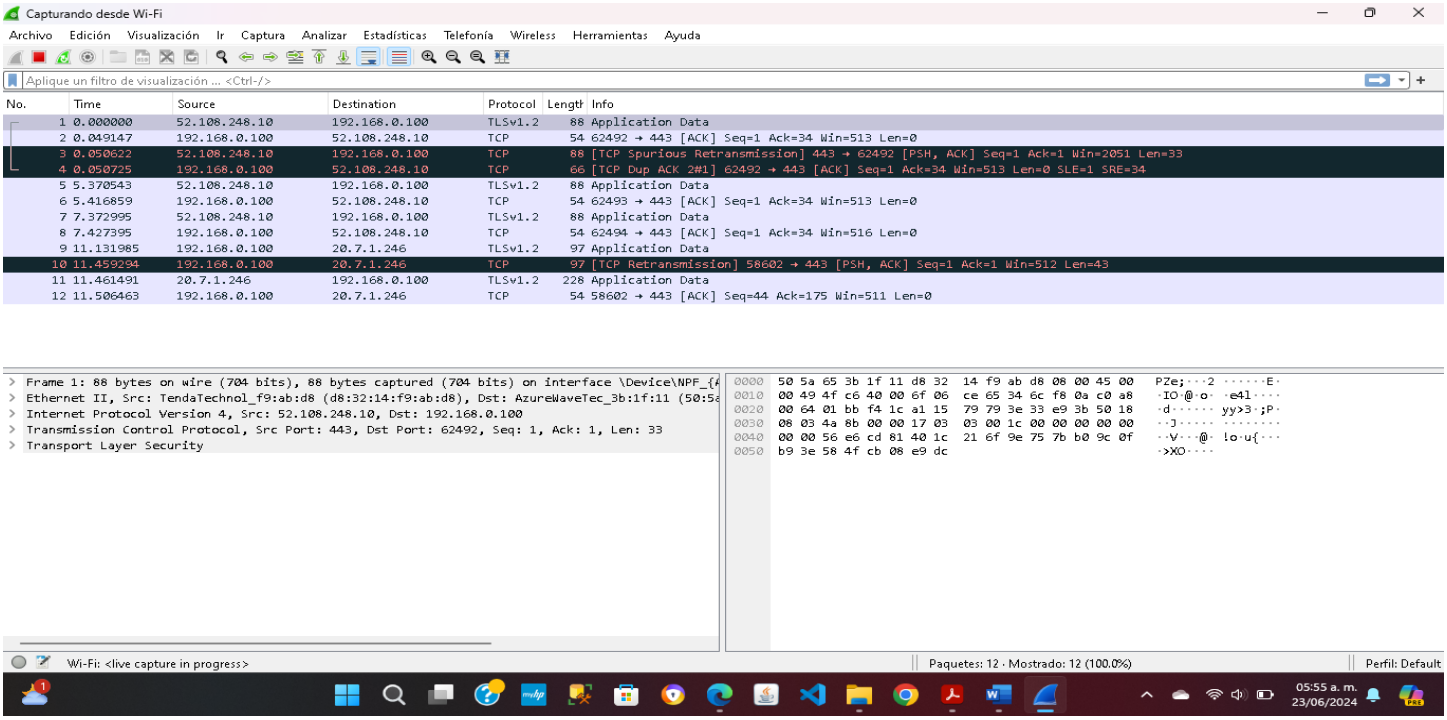
En la siguiente imagen se me muestra la pantalla de inicio de WireShark una vez que esta la fue instalada y le damos iniciar como lo indica la actividad.




En la siguiente imagen se podemos observar que se abrir el programa *WireShark.*

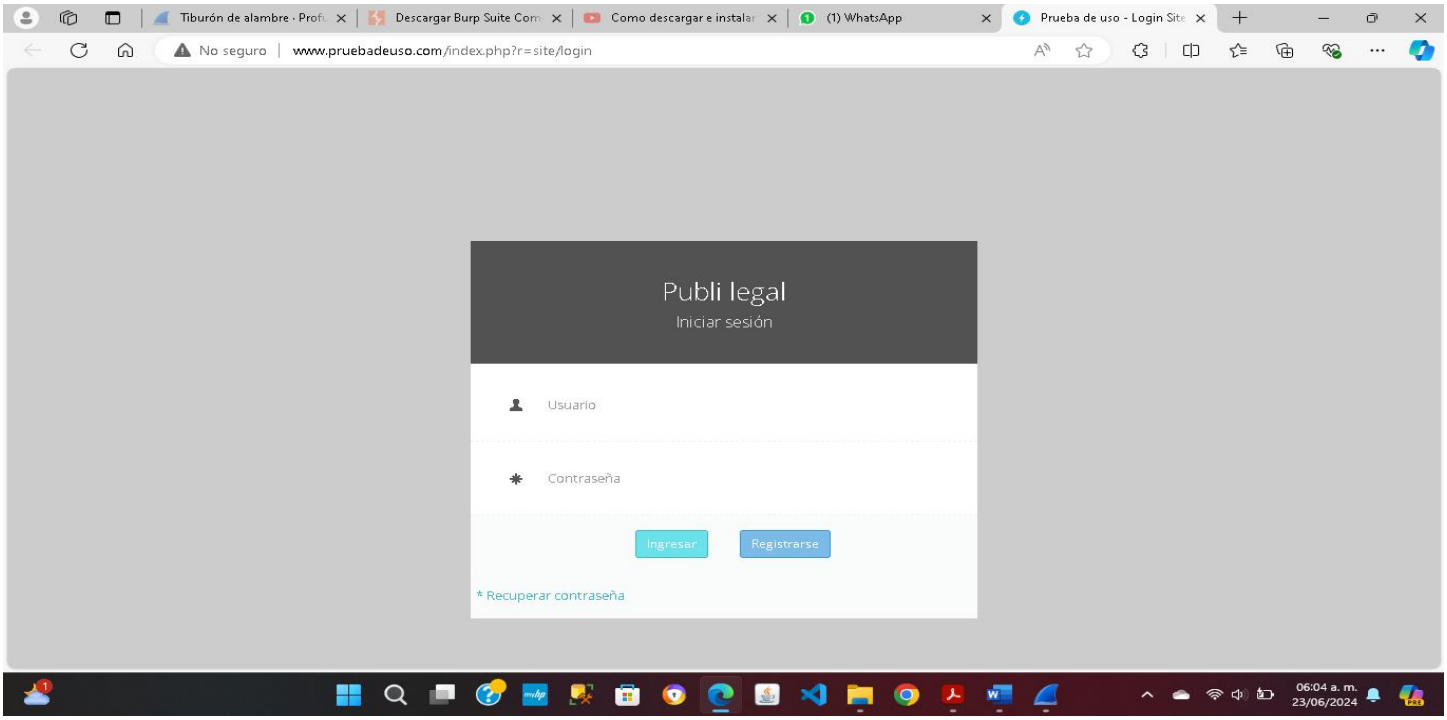


Una vez que ya logramos el ingreso a la opción *Wifi* nos permite visualizar la siguiente pantalla.

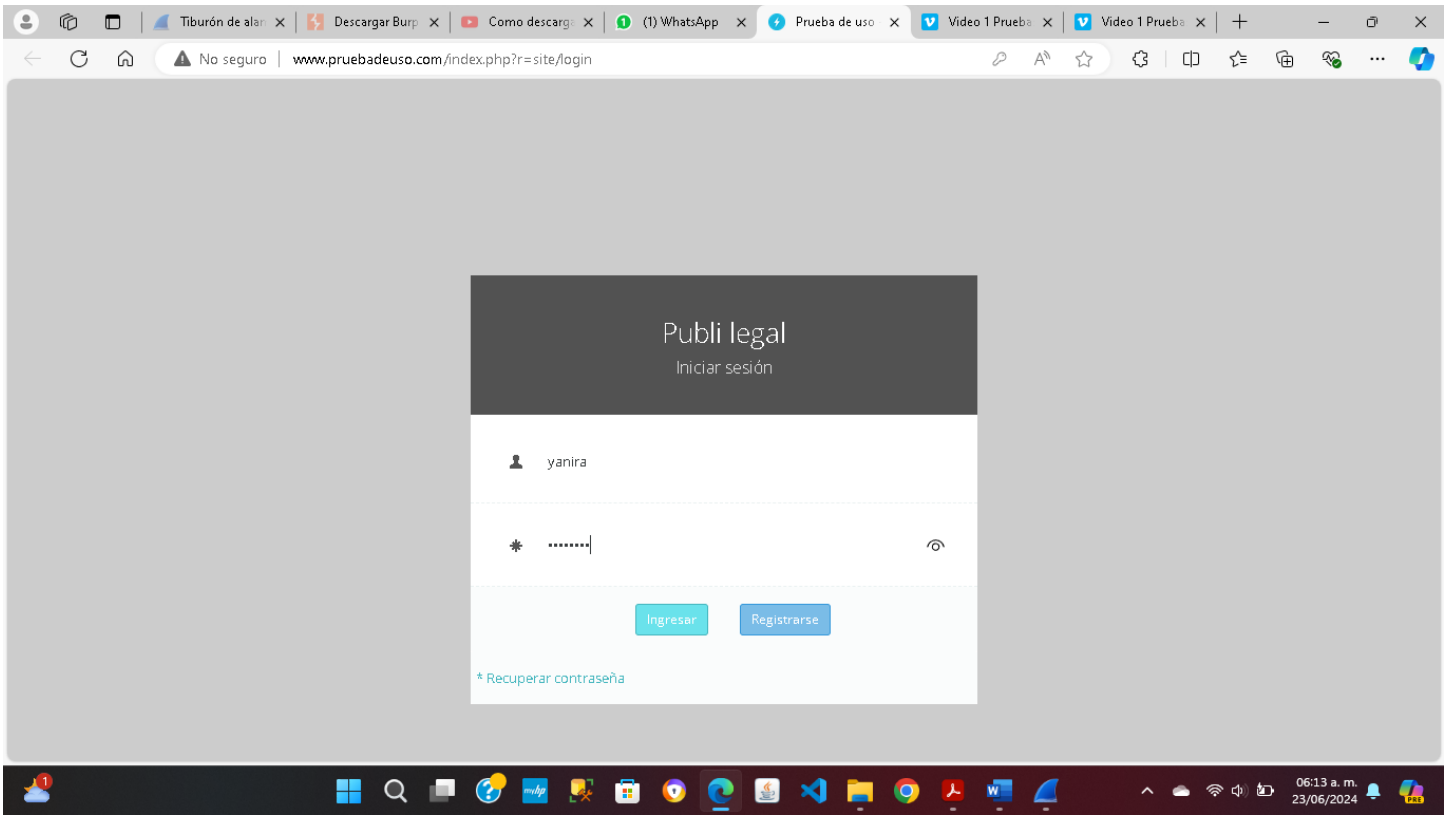



## Ataque al sitio

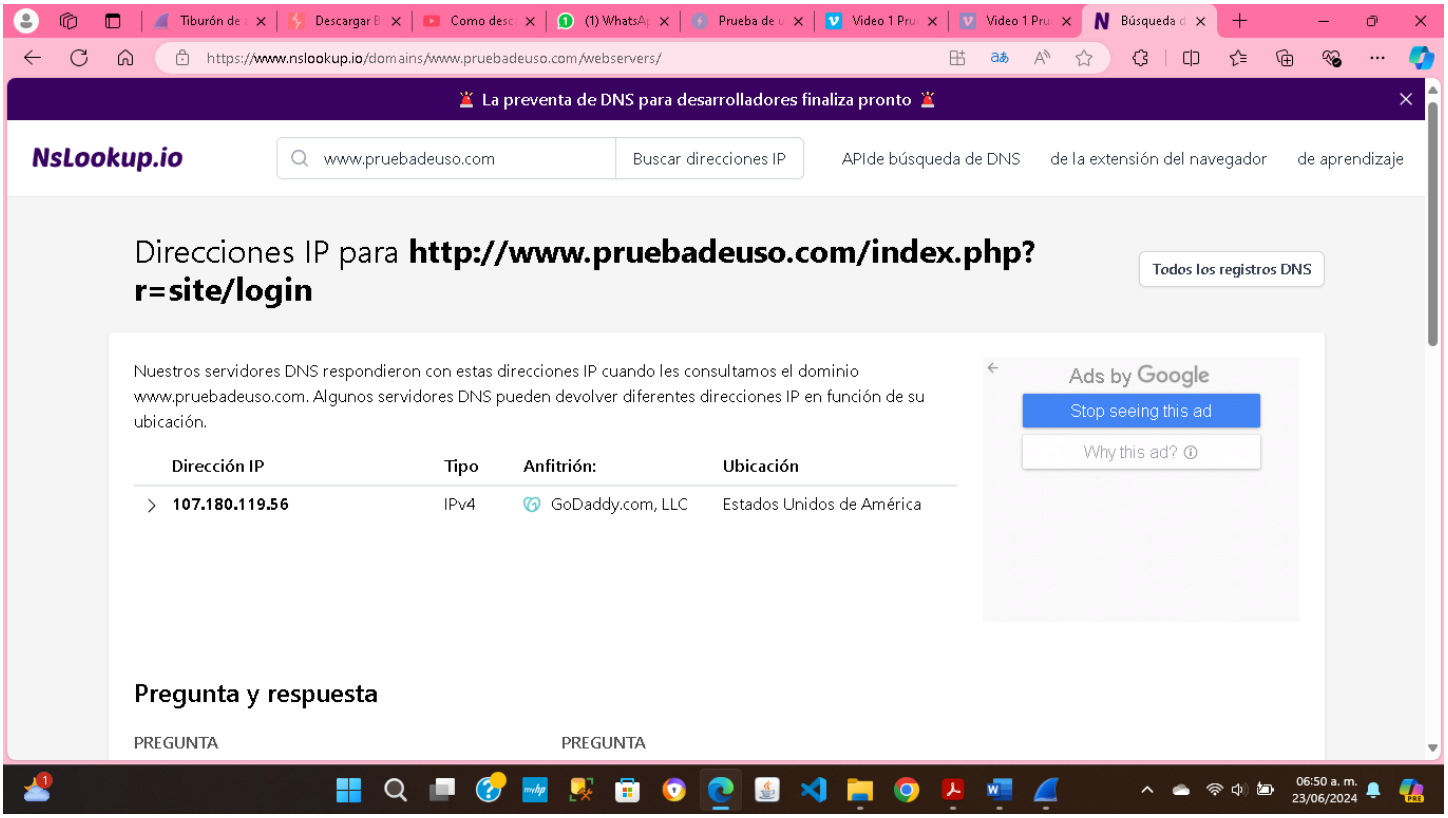
A continuación, ingresare al sitio web en el navegador de mi preferencia mediante el siguiente link http://www.pruebadeuso.com/index.php?r=site/login, en el cual llevare a cabo el ataca al sitio web.



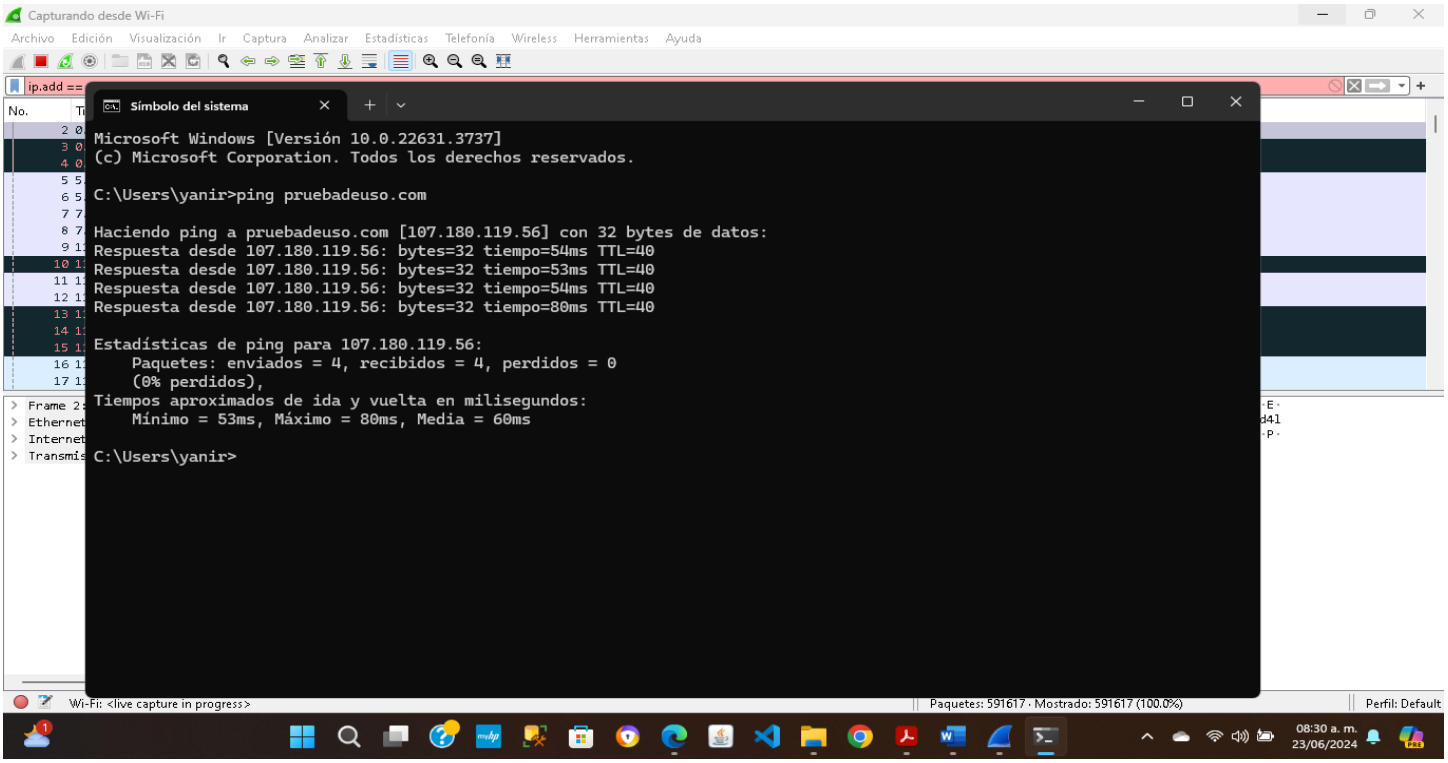
A continuación, intentare iniciar sesión utilizando credenciales incorrectas (esto no permitirá iniciar sesión).




En la siguiente imagen podemos observar que se logró entrar a la configuración del servidor de la sitio web, y buscar su dirección IP.

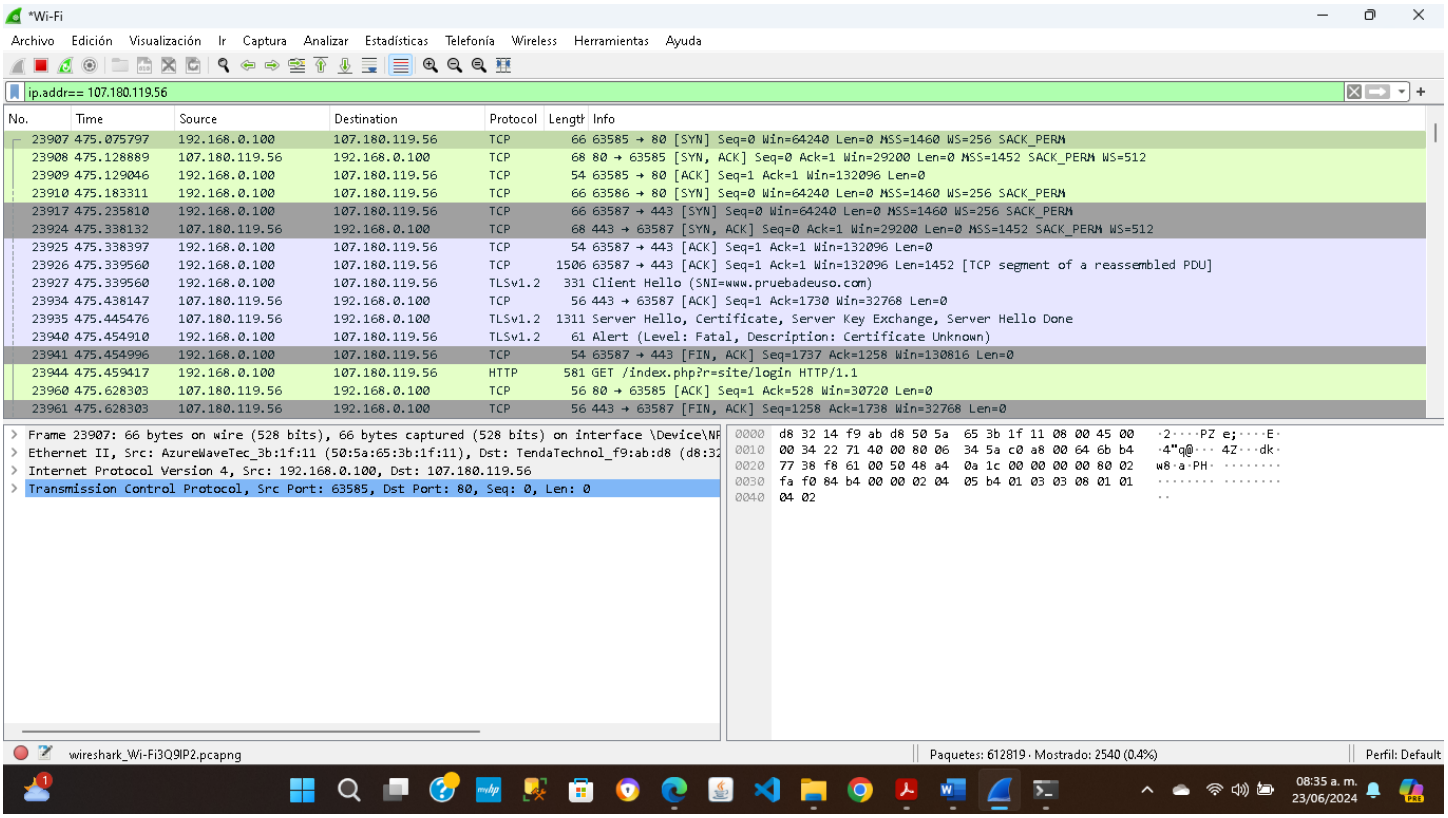


Aun cuando ya conocemos la ip del sitio web que vamos a atacar realice una confirmación de que la ip es correcto mediante el CMD de mi computadora.

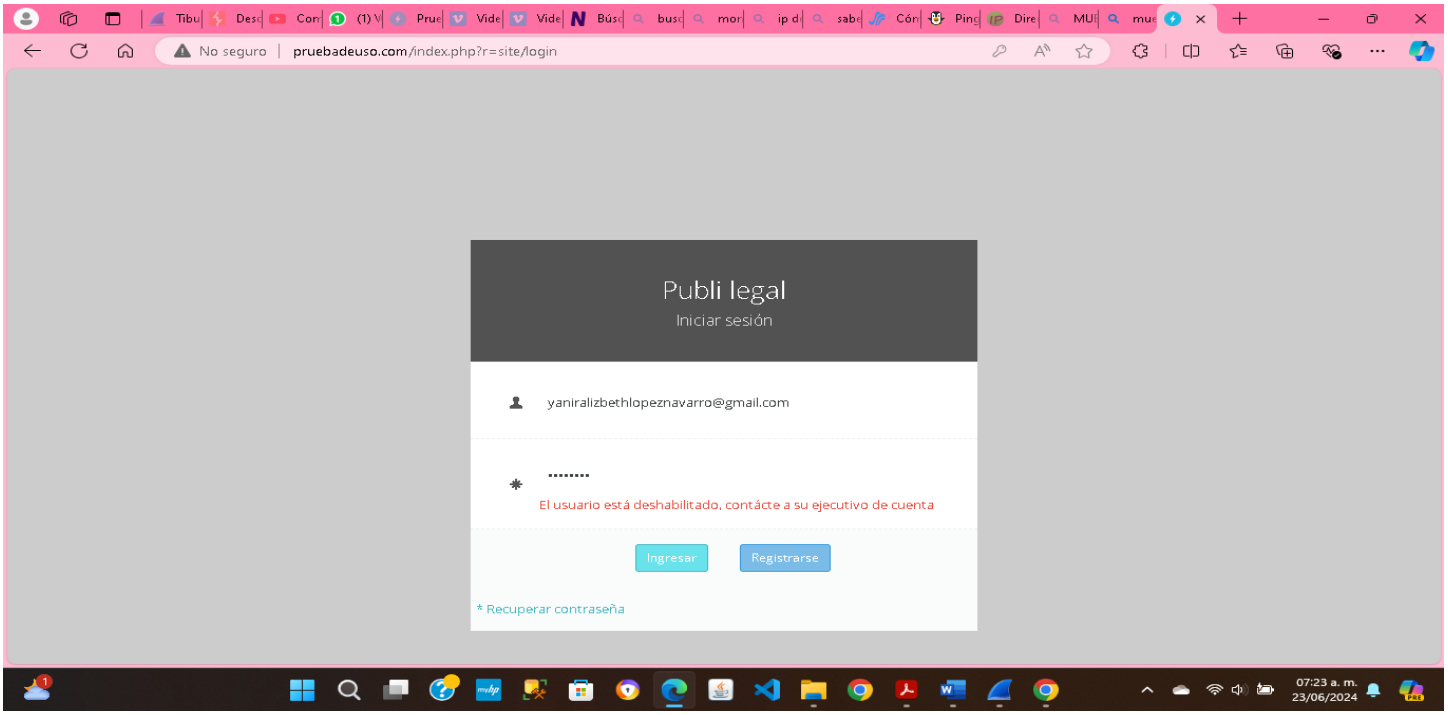



A continuación, se realizó la *búsqueda* de la dirección IP en *WireShark* mediante el siguiente comando:

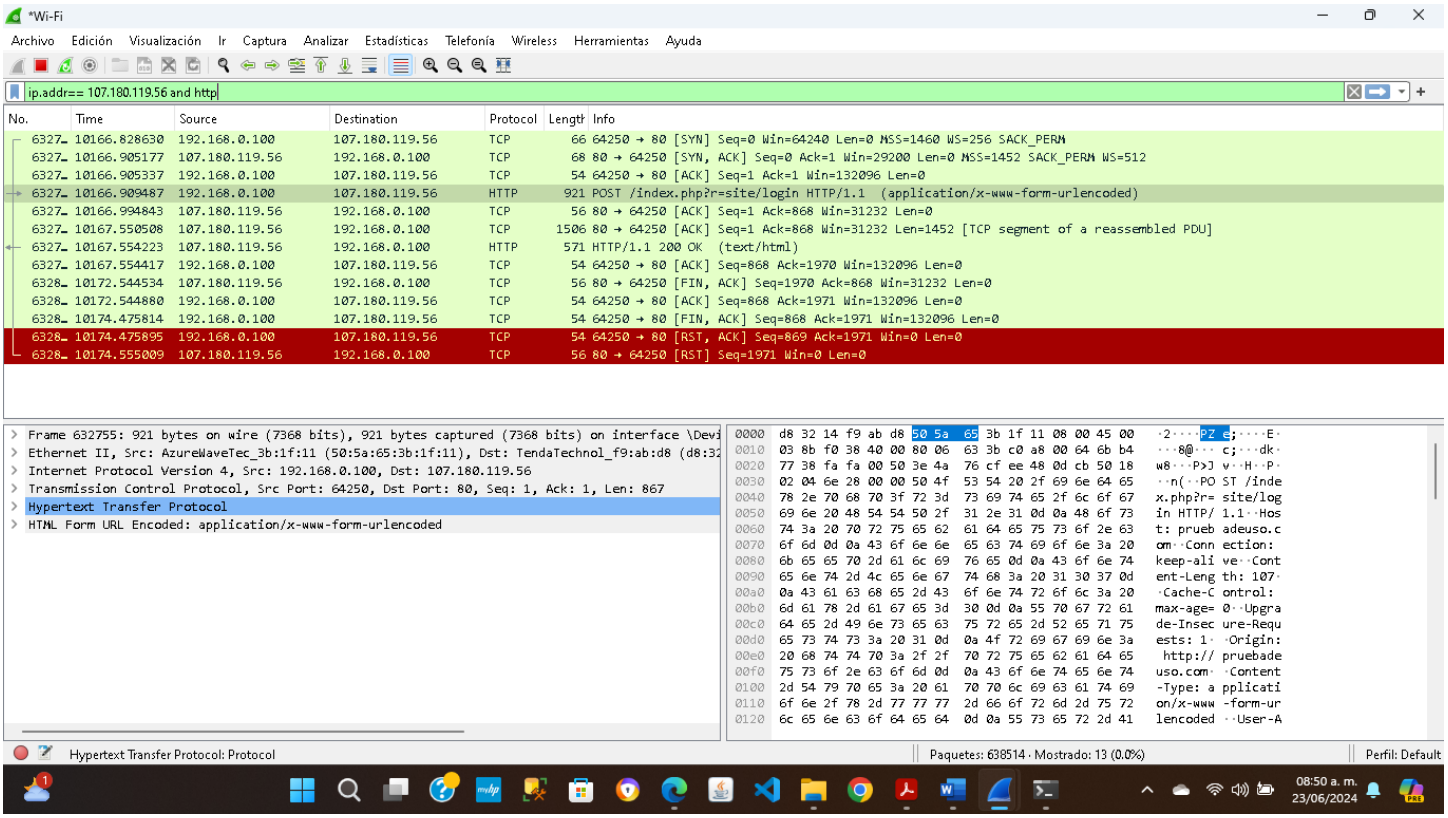
ip. Add == dirección IP



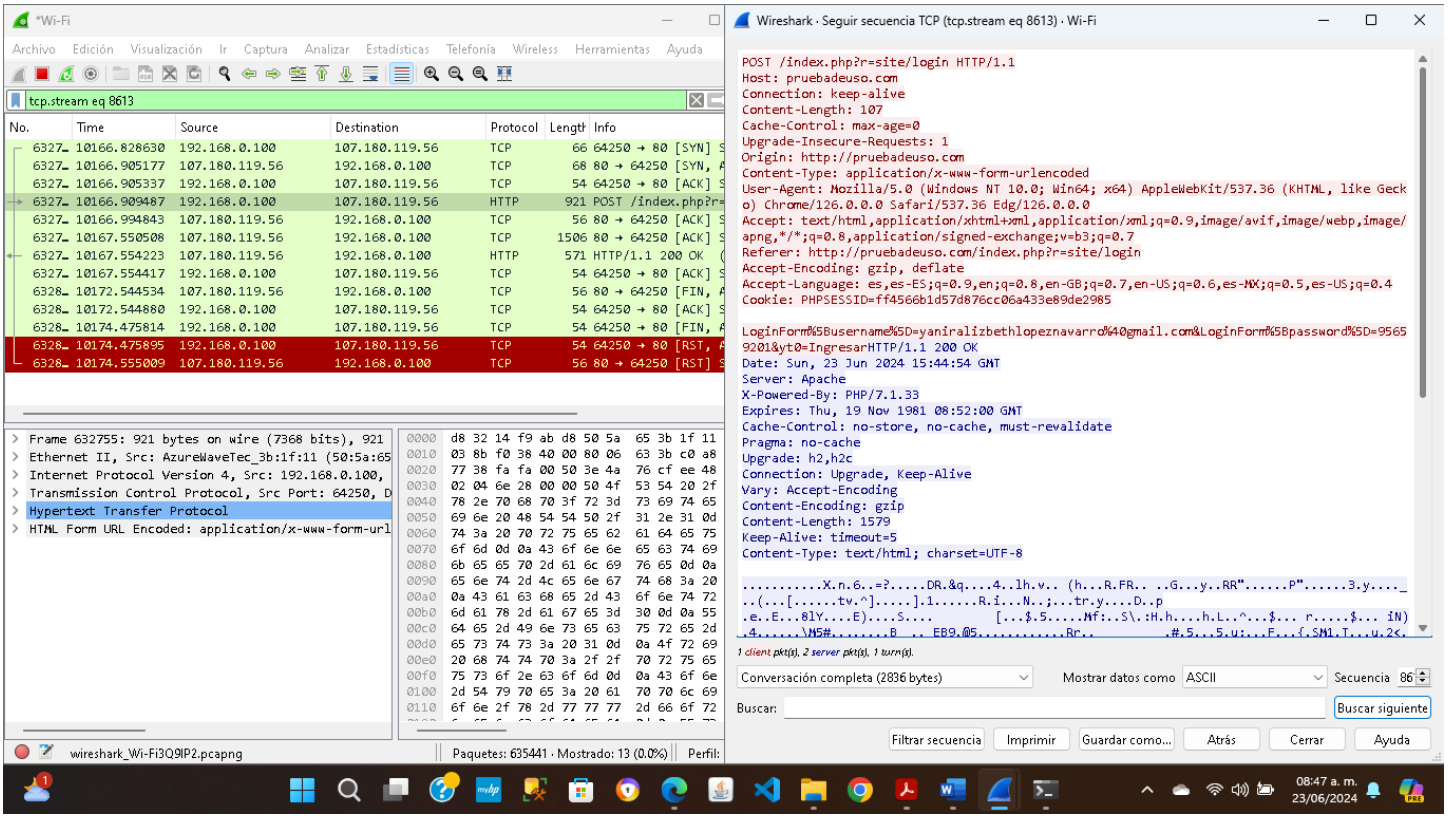
Intentamos volver al sitio web e ingresar los datos de manera correcta aun que no nos permite debido a que el sitio web no es de mi propiedad y no cuento con las credenciales correctas.




A continuación, se muestra en *Wireshark* se puede ver las acciones que ha realizado la dirección IP del sitio web.  Buscar mediante una opción que en protocolo tenga HTTP, así como la palabra POST.



A continuación, se muestra el resultado una vez que se dio clic derecho sobre la opción con las características anteriores y seleccionar *Seguir*.




Con esto nos permite visualizar el usuario/correo y contraseña con el que se intentó el inició sesión en el sitio web.

# Conclusión

La realización de esta actividad ha sido fundamental para comprender de manera profunda las vulnerabilidades que existen en las aplicaciones web sin medidas de seguridad adecuadas. En el ámbito laboral, adquirir esta experiencia nos capacita para identificar y corregir fallos en la seguridad de los sistemas que desarrollamos, asegurando que las aplicaciones que lanzamos al mercado protejan eficazmente la información de los usuarios.

En nuestra vida cotidiana, este conocimiento nos hace más conscientes de los riesgos a los que estamos expuestos al navegar por internet y utilizar diferentes servicios en línea. Entender cómo los datos pueden ser interceptados y utilizados de manera indebida nos motiva a ser más cuidadosos con la información que compartimos y a preferir sitios web que implementen medidas de seguridad robustas como el SSL.

Además, esta actividad nos ha demostrado la importancia de estar siempre actualizados y preparados para enfrentar los desafíos de la ciberseguridad. En un mundo cada vez más interconectado, proteger la información personal y corporativa es una responsabilidad compartida. A través de ejercicios prácticos como este, fortalecemos nuestras habilidades y contribuimos a un entorno digital más seguro y confiable para todos.

# Referencias


Ingeniería en desarrollo de software. Universidad México Internacional. Recuperado el día 10 de junio de 2024, umi.edu.mx/coppel/IDS/mod/scorm/player.php

*Video conferencing, web conferencing, webinars, screen sharing*. (s. f.). Zoom. https://academiaglobal-mx.zoom.us/rec/play/1MpPOitg1mPH7hMrQbeKHuOfNATsJi8d-11SrXSJAu47yV86hS2ucF5HuPqQNqN-5pZJMImBn4JUyp-k.dq6TBS1J-S98frpn?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FMpClRdjf8kiSF7ceZKjOQ_bXHsOk1vjK9p0eC9-NBgN1d51EH3XfjvPqcYahxers.doPPNRS_HIQiVvgg

Global, A. (2024, 23 junio). *Video 1 Pruebas de Vulnerabilidades Pérdida de Autenticación y Gestión de Sesiones.mp4* [Vídeo]. Vimeo. https://vimeo.com/711845557/a5ae411ce9