



**UNIVERSIDAD AUTÓNOMA DE CHIAPAS**

**SUBCOMPETENCIA 2**

**7° "M"**

**ANALISIS DE VULNERABILIDADES**

**ACT 2.1: ¿QUÉ ES WIRESHARK?**

**ESTUDIANTE: JESUS SALVADOR HERNANDEZ**

**ZARATE**

**PROFESOR: DR. LUIS GUTIERREZ ALFARO**

**TUXTLA GUTIERREZ CHIAPAS 19/02/2024**

## **¿Qué es Wireshark?**

Es un analizador, antes conocido como Ethereal, de protocolos de red de código abierto. Wireshark te permite registrar y buscar de manera interactiva el tráfico que atraviesa sobre una red. Es una herramienta con características poderosas que puede correr en casi cualquier plataforma como Windows.

Wireshark, al igual que cualquier otro analizador de protocolos, realiza determinadas acciones como:

- Captura/Registro de paquetes. Wireshark escucha la conexión de redes en tiempo real para, entonces, recolectar streams enteros de tráfico.
- Filtrado. Wireshark es capaz de cortar y fragmentar toda la información aleatoria utilizando filtros.
- Visualización. Wireshark permite entrometerse justo en medio de un paquete de red. Esto posibilita visualizar conversaciones enteras entre streams de red.
- Rastrear. Wireshark posibilita seguir el rastro de paquetes TCP stream, pudiendo ver todo lo relacionado con este paquete.
- Decodificación. Wireshark permite decodificar los paquetes y exportar a formatos específicos para guardar estos ítems.

## **¿Cuándo utilizar Wireshark?**

Wireshark es una herramienta de seguridad empleada por agencias gubernamentales, instituciones educativas, corporaciones, pequeños negocios y organizaciones sin fines de lucro para dar solución a problemas de red.

Esta herramienta puede ser utilizada para entender el análisis de tráfico de red, cómo se genera la comunicación cuando ciertos protocolos son utilizados y dónde pueden estar los errores cuando aparecen algunos problemas.

## Bibliografía

Wireshark · *Frequently asked questions.* (s. f.). Wireshark.

[https://www.wireshark.org/faq.html#\\_what\\_is\\_wireshark](https://www.wireshark.org/faq.html#_what_is_wireshark)

UCM-Proyecto de Innovación Software libre para ciencias e ingenierías. (s. f.).

<https://www.ucm.es/pimcd2014-free-software/wireshark>

Altube, R. (2023, 12 abril). Wireshark: Qué es y ejemplos de uso.

*OpenWebinars.net.*

<https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/>

*What Is Wireshark and How to Use It | Cybersecurity | CompTIA.* (s. f.).

CompTIA.org.

<https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it>