|  |  |  |
| --- | --- | --- |
|  | **UNIVERSIDAD**  **NACIONAL**  **DE LOJA** | CIS-UNL |
|  |  |  |

***Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables***

***Integrantes:***

***Paralelo:*** “A”

***Fecha:***

***Docente:*** Ing. Mario Cueva **# Actividad de trabajo Práctico Nro:**

***Fecha***

1. **Tema: Análisis de Tráfico utilizando la herramienta Wireshark.**
2. **Abstract**

Contener información de cada parte del artículo, incluyendo los resultados.

Siempre debe tener un párrafo de longitud y nunca debe tener encabezados.

Ser revisado cuidadosamente una vez que se ha terminado de escribir el Trabajo

No contener citas ni referencias..

1. **INTRODUCION**

**Antecedentes**

Al momento de estudiar acerca de cómo se comunican las aplicaciones informáticas en la red es esencial tener el conocimiento básico de los protocolos y datos que utilizan, así como la estructura de los paquetes que envía y recibe (Mu, lozano )

**Objetivos**

* Describir el funcionamiento de la herramienta Wireshark
* Analizar el comportamiento del envio de tramas de datos

1. **Metodologia**

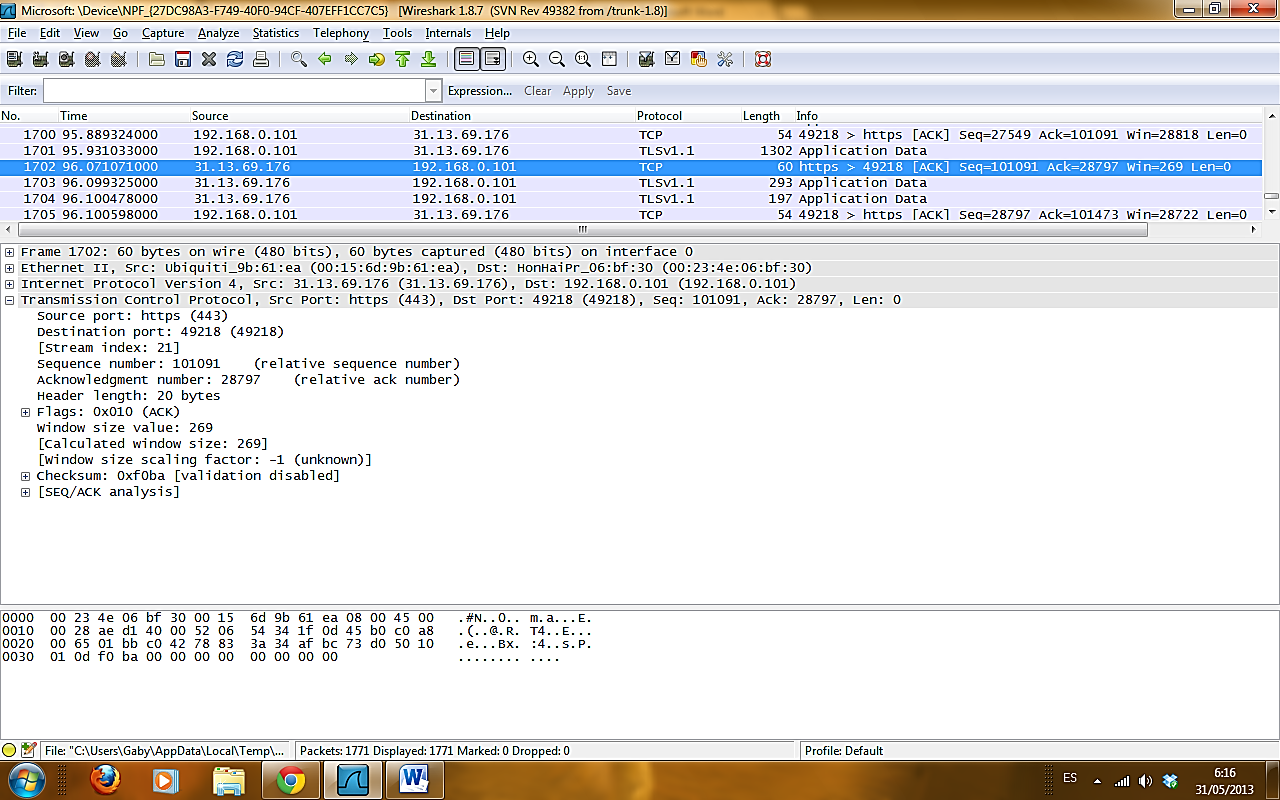
Materiales, tecnicas y metodos, metodologia de desarrollo

1. **Resultados y discusiones**

**Hallazgos(resultados) del estudio.**

A continuación, se detalla el desarrollo de la práctica, luego de usar wireshark para hacer un análisis del tráfico de cada uno de los protocolos, hemos obtenido lo siguiente:

**PROTOCOLO HTTPS.**

El protocolo HTTPS lo encontramos encriptado dentro del protocolos TCP, nos permite la tranferencias de datos de una maner segura.

**El protocolo HTTPS está utilizando el puerto 443 por defecto y está enviando un mensaje ACK: 28797 para la transmisión de datos.**

**Que significa los hallazgos (discusión)**

1. **Conclusiones: (cuatro conclusiones)**

* Wireshark es un programa muy útil ya que por medio de los filtros se puede capturar el protocolo que se desee para utilizarlo como objeto de estudio y de esta manera saber su funcionamiento que se realiza durante la transmisión de datos y de todos los procesos que este utiliza.

1. **Bibliografía: (Estandar APA O IEEE)**

Mu, F., Zhang, J., Du, J., & Lin, J. (2011). Application of the Secure Transport SSL Protocol in Network Communication. http://doi.org/10.1109/ISCID.2011.25

Ordean, M., & Giurgiu, M. (2010). Implementation of a security layer for the SSL/TLS protocol. *2010 9th International Symposium on Electronics and Telecommunications, ISETC’10 - Conference Proceedings*, 209–212. http://doi.org/10.1109/ISETC.2010.5679350

Riffo, M. A. (2008). Vulnerabilidades de las Redes TCP/IP y Principales Mecanismos de Seguridad. *In Vitro*, *3*(2), 1–23. Retrieved from http://www.ncbi.nlm.nih.gov.myaccess.library.utoronto.ca/pubmed/11720961

Subías, M. P. (n.d.). Desfalcos por “Phishing,” 25–26.

Wagner, D., & Schneier, B. (1996). Analysis of the SSL 3.0 protocol. *Proceedings of the 2nd Conference on Proceedings of the Second USENIX Workshop on Electronic Commerce - Volume 2*, 4. http://doi.org/10.1.1.29.9990