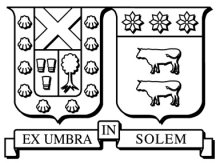



UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

# Informe de Proyecto Redes de Computadores (**ELO322**): FreeVPN v/s VPN de Pago

José Catalán (201551010-5)

Marcelo González (201430028-K)

Camilo Fernández (2014300040-9)

Jorge Fernández (201504100-8)

Universidad Técnica Federico Santa Maria,

Valparaiso, Chile

1 de Julio del 2016.

# Resumen

En el presente proyecto analizamos de manera teórica y práctica las principales diferencias que existen entre VPNs gratuitas y pagadas. Utilizando la VPN HMA (pagada) y Hola (gratuita), testeamos cada una de forma independiente accediendo a un sitio web especifico con el software Wireshark, el cual nos permite visualizar el tráfico de paquetes en conjunto a información de tráfico para cada caso y así observar las diferencias entre ellas.

Por otro lado estudiamos los diversos protocolos que existen en el mundo de las VPNs para así establecer cual es la que otorga mayor seguridad y tenerlo presente para su uso. Luego recaudamos información sobre cuales son las principales características que se deben conocer al momento de utilizar las VPNs.

Como resultado mediante Wireshark se obtuvo que las VPNs pagadas utilizan protocolo UDP en la transferencia de paquetes, mientras que las gratuitas utilizan TPC. De esto se puede extraer que las gratuitas utilizan solo el protocolo PPTP, el cuál es rápido y sencillo pero es el más vulnerable de los protocolos para VPNs, ya que es el primero en la historia de estas. También se logra concluir que el protocolo más seguro en las VPNs es OpenVPN en conjunto a Chameleon y la importancia que tiene el leer los términos y condiciones al momento de utilizar una VPN.

# Introducción

En el mundo de la internet siempre estamos propensos a constantes y diversos ataques o privación de contenidos por localización geográfica y/o seguridad. Es por este motivo que nacen la VPNs que son la herramienta perfecta para solucionar en gran medida a nivel usuario estos problemas. Pero a raíz de esto han surgido diversas VPNs, algunas pagadas y otra gratuitas, aquí es donde nace la siguiente pregunta ¿En que se diferencia una pagada de una gratuita? O ¿Qué tan seguras son las VPNs?.

Dadas estas incógnitas surge el tema central de nuestro proyecto, en el cual haremos uso de 2 VPNs por separado (una gratuita y otra pagada) y luego realizaremos seguimiento de paquetes con cada una al ingresar a un sitio web y así observar que protocolos se utilizan, que tanta información encriptan, etc. También saber qué factores considerar al momento de comenzar a utilizar una VPN.

## Tipos de Protocolos

- **PPTP**: Diseñado por Microsoft en 1999 en base al protocolo PPP. Causó gran impacto porque permitia ingresar a sitios que restringian las IP que podian ingresar, ademas de codificar la informacion.
  Es altamente vulnerable, debido a que esta prácticamente obsoleto en seguridad (cuanta con una encriptacion de 128-bits), hoy es usado debido a su rapida y secilla implementacion.

- **L2TP/IPSec**: Se crea L2TP a partir de PPTP, y este se apoya en IPSec, debido a que no cuenta con una encriptacion por si mismo. IPsec cuenta con una encriptación de muy alto nivel (256 bits), el paquete se encapsula dos veces, esto genera una pérdida de velocidad pero se gana mucho en

seguridad. Es lo mejor en temas de seguridad si es que el dispositivo no soporta OpenVPN.

- **OpenVPN**: Utiliza certificados digitales, para que el receptor haga la desenscripcion de los datagramas, gracias a esto cuanta con una alta velocidad. Además cuenta con una encriptación de 256 bits, por lo que no solo es bastante rápida, sino que tambien es muy segura.

- **Chamaleon**: Una mejora al OpenVPN, surgió debido a que China comenzó a identificar los protocolos VPN y bloquearlos.

## Tips y Recomendaciones antes de comprar una VPN

- **Protocolo que ocupa dicha VPN**, ya que como vimos anteriormente, algunos protocolos son más seguros que otros. Los protocolos que más brindan seguridad en este aspecto son SSL e IPSec.

- **Localización de los servidores de salida de la VPN**. Si se quiere bypassear una restricción de ubicación se debe elegir una VPN que tenga servidores en dicha ubicación. Por otro lado, si el usuario está preocupado por posible espionaje o monitorización de la actividad de parte de agentes del estado, se debería elegir una VPN que tenga servidores fuera de la ubicación "espiada".

- **Registro de datos**. Al conectarse a una VPN, uno confía en el proveedor de servicios VPN entregandole mis datos. Puede que la comunicación `per se` esté a salvo, pero otros sistemas de la misma VPN (en especial el operador) puede registrar sus datos si asi lo desea. Si se quiere asegurar que eso no pase, el proveedor de servicios VPN debe especificar en sus politicas de privacidad,antes de inscribirse en dicha VPN, que si ejecuta ese tipo de

politicas. Si la VPN no registra las actividades que se hacen al conectarse, mejor aún.

- **Características Anti-Malware/Anti-Spyware**. El uso de VPN no significa invulnerabilidad. Estando conectada en ella, se debe asegurar que se esté usando HTTPS cuando sea posible, y tener cuidado con las descargas. Algunos proveedores de servicios VPN viene con escáneres anti-malware, como por ejemplo Hotspot Shield.

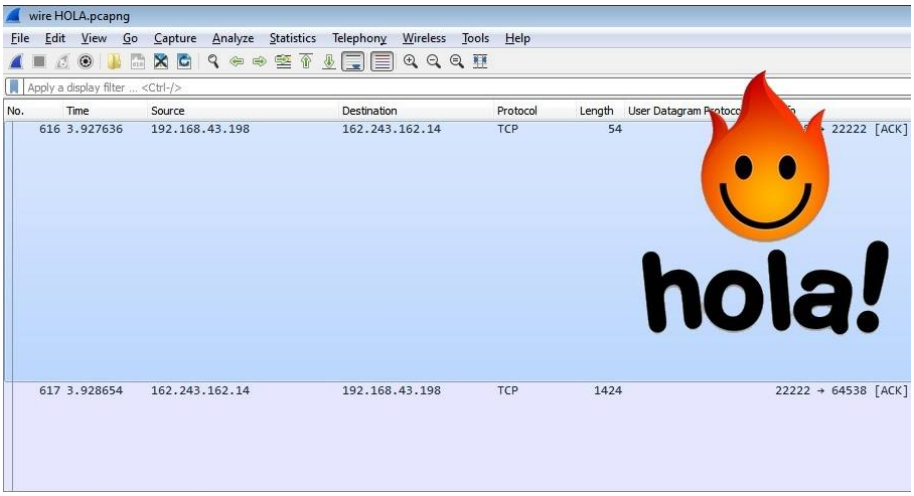
# Resultados parte práctica

Se compró una VPN pago de alta categoria y buena fama, para comprarla con una VPN gratuita muy conocida. El sitio utilizado para las pruebas fue `www.pandora.com` el cual está bloqueado para toda dirección IP fuera de U.S.A. A continuación se mostrarán y explicarán los resultados obtenidos.

## Capturas Wireshark

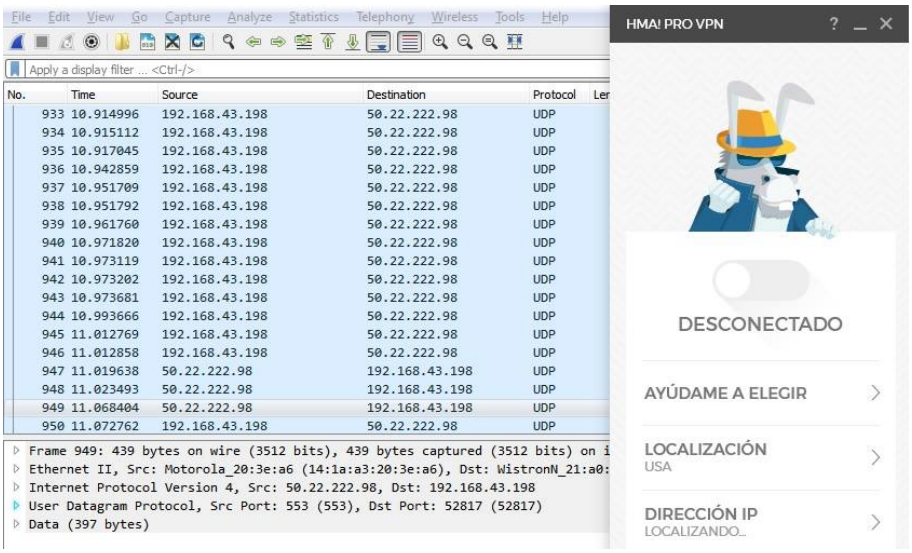
- **HOLA (Free VPN)**

  Luego de activar nuestro VPN nos introducimos en el sitio Pandora (el cual tiene el accceso bloqueado para las IPs fuera de USA). Al realizar la captura Wireshark hacia el servidor VPN, se da a conocer que los paquetes se enviaban via protocolo TCP, detalle bastante importante para nuestra investigación, ya que la interaccion USER- VPN SERVER via TCP solo es utilizada por el protocolo VPN PPTP, el cual es el más vulnerable (cuenta con un encriptación de 128- bits, la cual es la mas baja entre los protocolos VPN).




- **HideMyAss (VPN pago)**

  Esta VPN nos permite elegir el protocolo que deseamos usar; nosotros optamos elegir el protocolo L2TP/IPSec, el cual es de los más seguros (cuenta con una encriptación de 256 bits, además es encriptado dos veces, L2TP e IPSec). Nos fijamos que en la captura, las interacciones USER-VPNSERVER utilizan protocolo UDP, debido a que L2TP/IPSec trabaja sobre este protocolo.



# Conclusiones

Dejamos en claro la gran diferencia en seguridad entre VPN gratuitas y paga, pero se debe tener en consideracion que no siempre es necesario tanta seguridad, por tanto la VPN que el usuario utilizara dependera de lo que este quiera realizar.

Un usuario que esta dentro de China y quiere acceder a facebook, necesitara un VPN mas potente, por lo que debera pagar para obtener esa potencia, debido a que el firewall de china bloquea los protocolos VPN que intentan pasar, a excepcion de el protocolo Chamaleon.

Un usuario que solo desea acceder a una página como Pandora que restringe las IP fuera de USA podrá utilizar cualquier VPN ya que es una función bastante simple.

Una empresa que desea mantener conexion con sedes lejanas necesitará más seguridad para que los datos no sean cifrados por terceros, por lo que tendrán que pagar por una VPN que ofrezca un servicio con protocolo L2TP/IPSec o superior.

## Referencias

[1] http://es.giganews.com/vyprvpn/compare-vpn-protocols.html

[2] https://www.goldenfrog.com/ES/vyprvpn/chameleon

[3] http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs

[4] http://es.slideshare.net/JuanNoa/vpn-red-privada-virtual