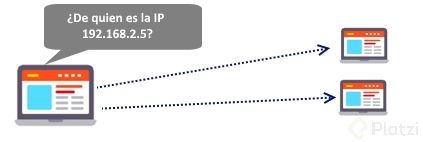
[Curso de Hacking Ético](https://platzi.com/clases/ethical-hacking/)

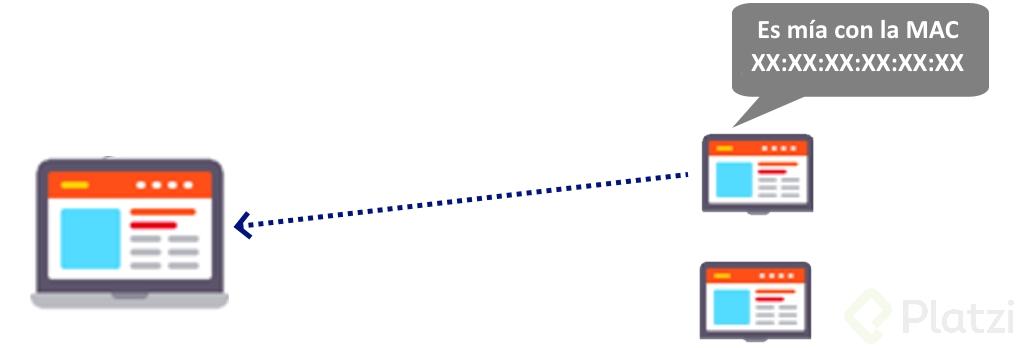
**ArtículoSniffing y Cómo realizar un ataque Man in the middle automatico**

[**Alan Joaquín Baeza Meza**](https://platzi.com/@ajbaeza)

26 de Abril de 2019

Los fundamentos de la arquitectura TCP/IP condicionan tanto las vulnerabilidades, que pueden ser explotadas en diversos ataques, como el tipo de mecanismos y herramientas que pueden ser utilizados para su protección.  
Como se vio en clases anteriores el modelo TCP funciona en capas que son:

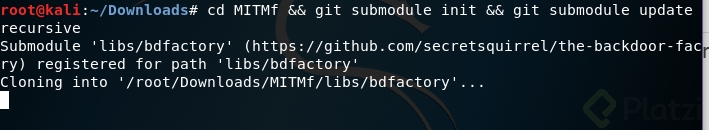
**El protocolo ARP (Address Resolution Protocol)**  
Es un protocolo de la capa física que se encarga de encontrar la dirección hardware (MAC) que corresponde a una determinada dirección lógica (IP).  
Por lo cual desde su concepción en el RFC 826 su funcionamiento se basa en el envío de un paquete (ARP request) a la dirección de difusión de red a (broadcast) el cual contiene la IP por la que se pregunta.  


El equipo que contenga la dirección responderá con un paquete (ARP reply) junto con la dirección Ethernet que le corresponde.  


Existe un tipo de **ataque** que se aprovecha del protocolo ARP y que **permite a un atacante suplantar a otro usuario de la red de área local (LAN)**, teniendo acceso a los paquetes de datos para él destinados y pudiendo, incluso, modificarlos o bloquearlos.  
Esta técnica se conoce como ARP Spoofing o ARP Poisoning y consiste en enviar falsos mensajes **ARP reply** a la red para que el atacante reciba los paquetes destinados al usuario que el atacante quiere suplantar, ya que como fue concebido no se requieren un ARP request mandar una respuesta.

**Herramientas necesarias:**  
Para la realización de esta práctica se requiere los siguiente:

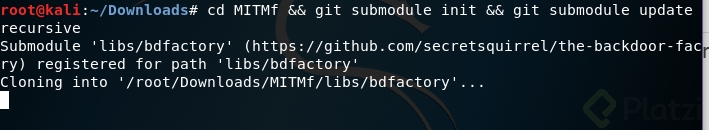
* VirtualBox 6.0.4.  
  <https://www.virtualbox.org/wiki/Downloads>
* Kali Linux 2019.1a.  
  <https://www.kali.org/downloads/>
* Metasploitable 3  
  <https://sourceforge.net/projects/metasploitable/>

**Instalación de MITMf**  
Es una herramienta que proporciona una gran cantidad de ataques de manera simple al uso de plugins.  
Para la instalación se requiere la instalación desde su dirección el Github que es:  
<https://github.com/byt3bl33d3r/MITMf>  
Acceder a la carpeta Download y se descarga el git con el comando: git clone https://github.com/byt3bl33d3r/MITMf.git  


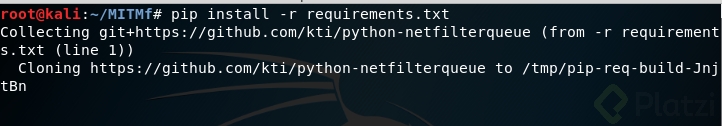
Se ingresa a la carpeta con el comando cd. Cd MITMf  

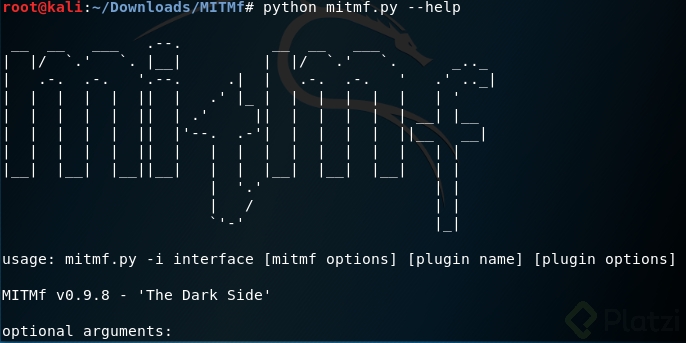

Es necesario instalar las siguientes dependencias que MITMf requiere.

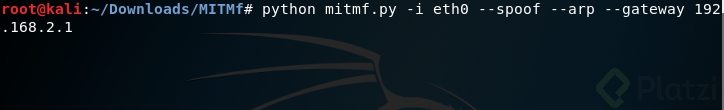
apt-get install python-dev python-setuptools libpcap0.8-dev libnetfilter-queue-dev libssl-dev libjpeg-dev libxml2-dev libxslt1-dev libcapstone3 libcapstone-dev libffi-dev file

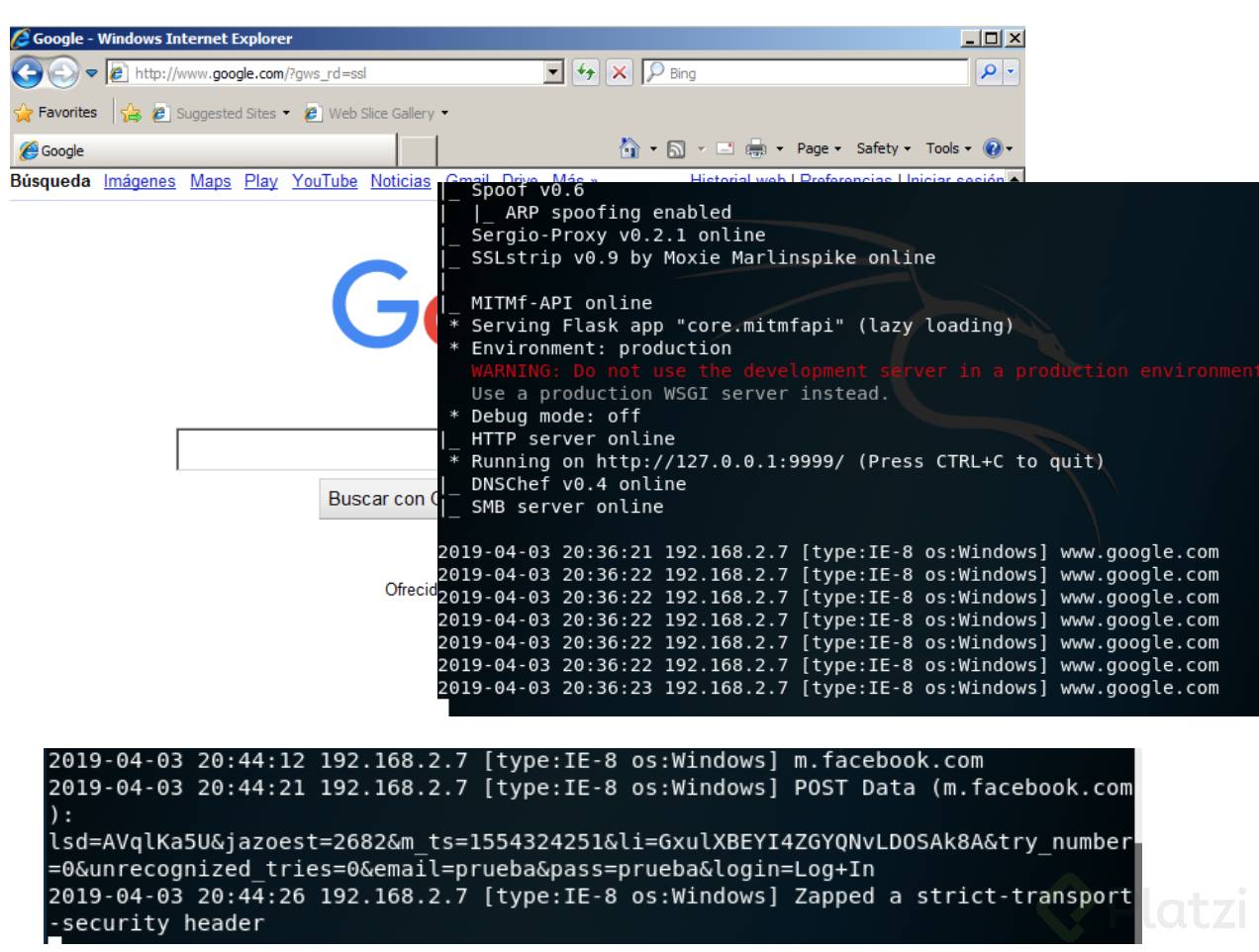
Se ingresa a la carpeta, además de inicializar y clone los submódulos con:  
cd MITMf && git submodule init && git submodule update –recursive  


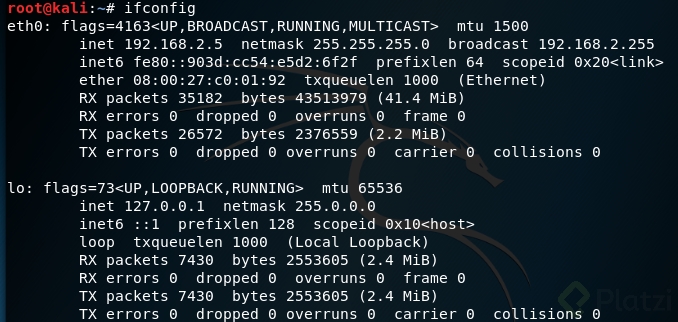
Con las dependencias instaladas, se prosigue a instalar la herramienta.

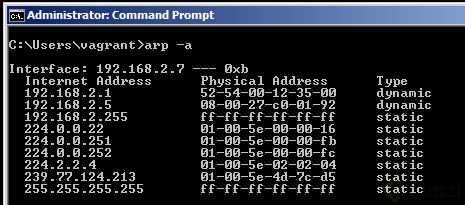
pip install -r requirements.txt  


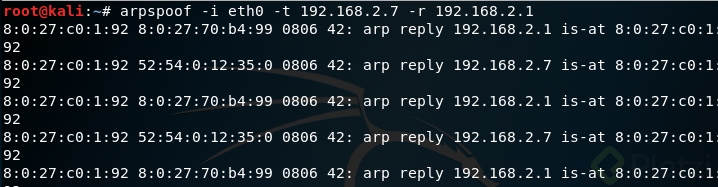
Para probar que se instaló correctamente, se debe correr lo siguiente:  


Se realiza un ataque que involucre todos los equipos.  


Para verificar su funcionamiento en el equipo con Metasploitable 3, se ingresa al navegador.  


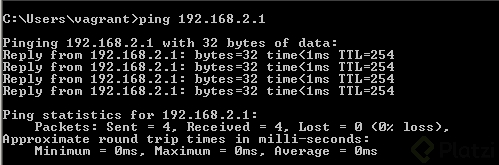
Iniciando con el ataque de forma manual:  
En la máquina con Kali Linux es necesario determinar cuál es la interfaz de red que se utilizara, para esto se hace uso del comando **ifconfig** que para esta prueba es “eth0”.  


En la máquina donde está instalado Metasploitable 3 se recomienda realizar un ping al equipo atacante para probar que están visibles. Después revisar su tabla ARP con el comando en cmd de “arp -a”, donde cada equipo tiene una dirección física única.  


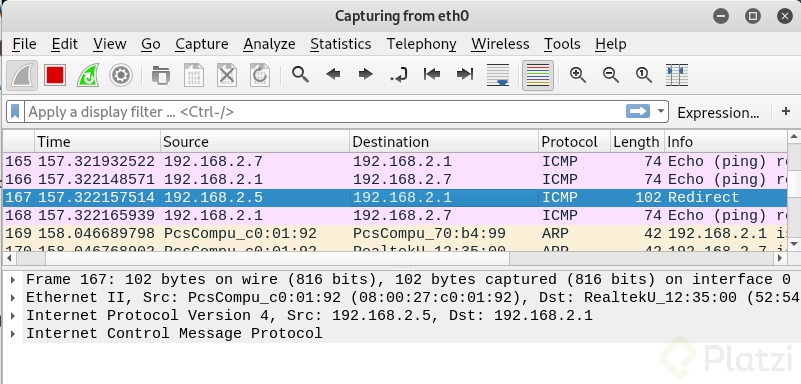
El paso siguiente es mandar tantos paquetes **ARP reply** a nuestra víctima con el objetivo de suplantar la identidad del Gateway que tiene la dirección 192.168.2.1, con el comando:  
arpspoof -i eth0 -t IPVíctima -r DefaultGateway  


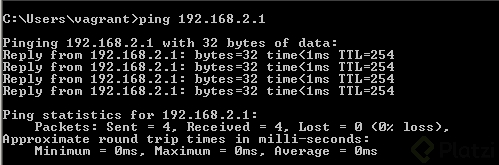
Nota: Es necesario dejar que esta terminal continúe mandando paquetes:  
Donde:

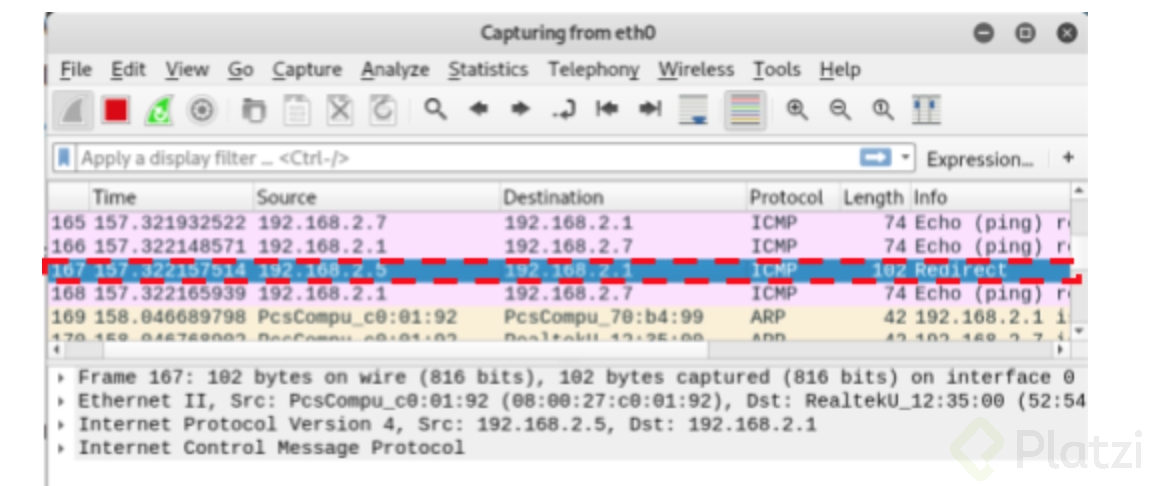
* i: corresponde a la interfaz de red.
* t: La dirección IP de la víctima.
* r: El Gateway por default.

Para constatar su funcionamiento, nuevamente se ejecuta el comando “arp -a” en el equipo objetivo para ver si se realizó algún cambio. ¿Qué pueden notar?  


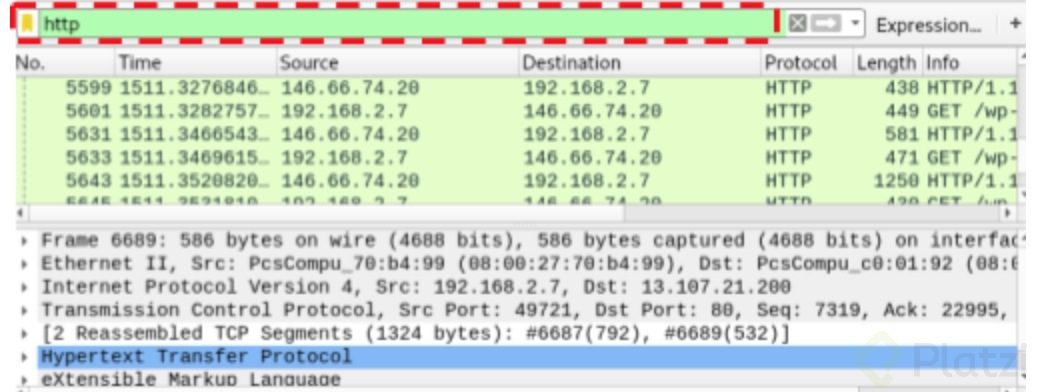
Con el paso anterior los paquetes llegan a nuestro equipo, pero es necesario saber qué hacer con ellos, Linux tiene la funcionalidad de reenviar los paquetes que recibe, pero esta desactivada por default para estos es necesario ejecutar en otra terminal lo siguiente:  
echo 1 > /proc/sys/net/ipv4/ip\_forward  

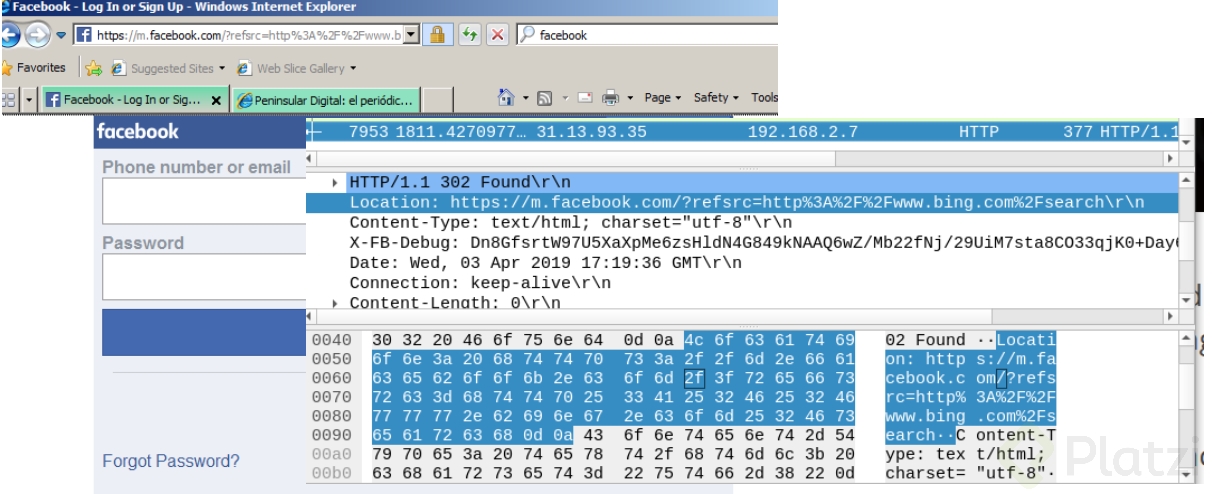

Para conocer a detalle el funcionamiento de este ataque en el equipo donde se encuentra Kali, abrir la herramienta Wireshark y seleccionar la interfaz “eth0” o en la cual estén realizando el ataque.  


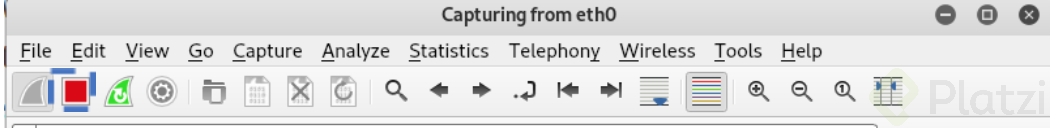
Se manda un ping de la máquina objetivo a la dirección Gateway para ver qué sucede.  


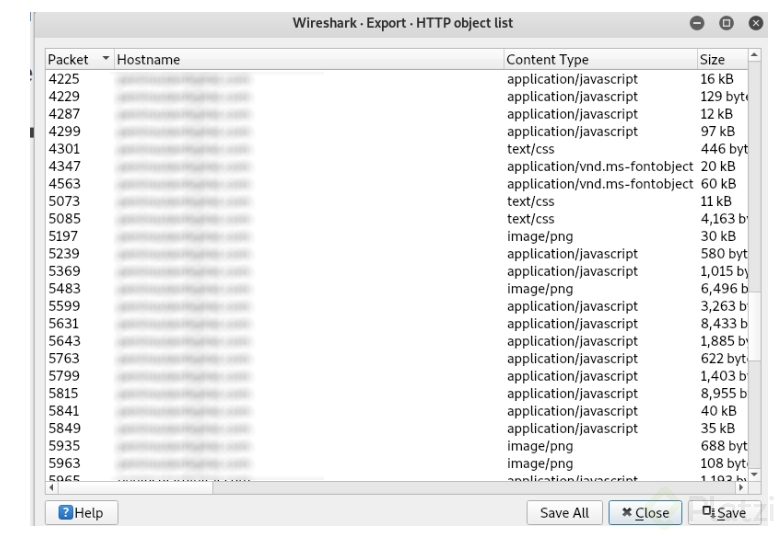
Al revisar las tramas en Wireshark se puede notar que llegan al destino, pero también son recibidas y reenviadas por nuestro equipo.  


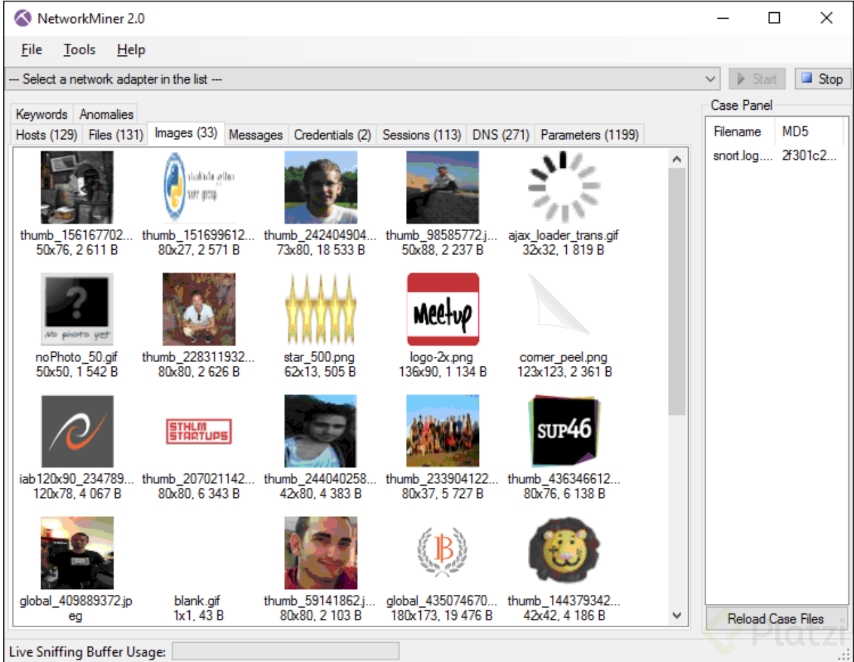
Para seguir jugando con este ataque se abre un navegador en la máquina objetivo y se ingresa a una página de internet.  


En el equipo donde se encuentra corriendo wireshark, se añade un filtro el cual solamente mostrará las peticiones HTTP, agregando solamente el nombre del protocolo en este apartado.  


Si se agrega Facebook podemos ver dentro de Wireshark como automáticamente redirecciona a la página con el protocolo HTTPS.  


Para finalizar nuestro sniffing detenemos en el cuadro rojo que se muestra en la imagen de abajo y se guarda todo el tráfico analizado en la opción:  
File->Save as  


Podemos exportar los objetos en el menú: File->Export Objects->HTTP.  


Otra opción es guardar la captura como archivo. pcap y agregarlo a la herramienta Network Minner que organiza de mejor manera la información resultante del análisis.  


Nota: imagen ilustrativa  
Hay que recordar que una página que implemente el protocolo HTTP toda la información viaja en “texto claro” y una persona malintencionada puede obtener las credenciales sin problemas si se encuentra inspeccionando el tráfico por lo que se recomienda utilizar página con el distintivo de HTTPS.  
Claro, existen herramientas que te permiten hacer un bypass a este protocolo también como lo es MiTmF