

**Colectando información acerca de un objetivo web usando Firebug**

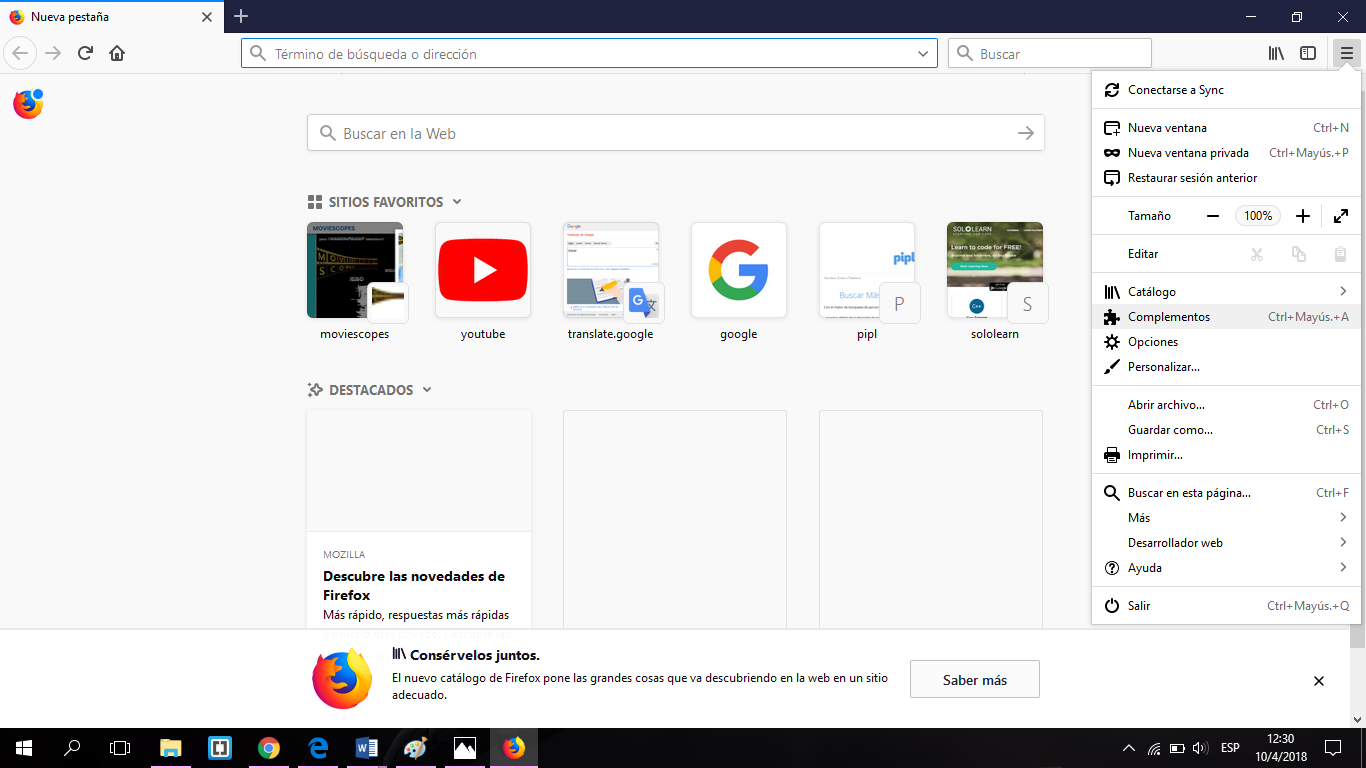
*Firebug se integra con Firefox proporcionando una gran cantidad de herramientas de desarrollo para editar y monitorear el CSS, HTML y JavaScript en vivo en cualquier página web.*

Objetivos del laboratorio:

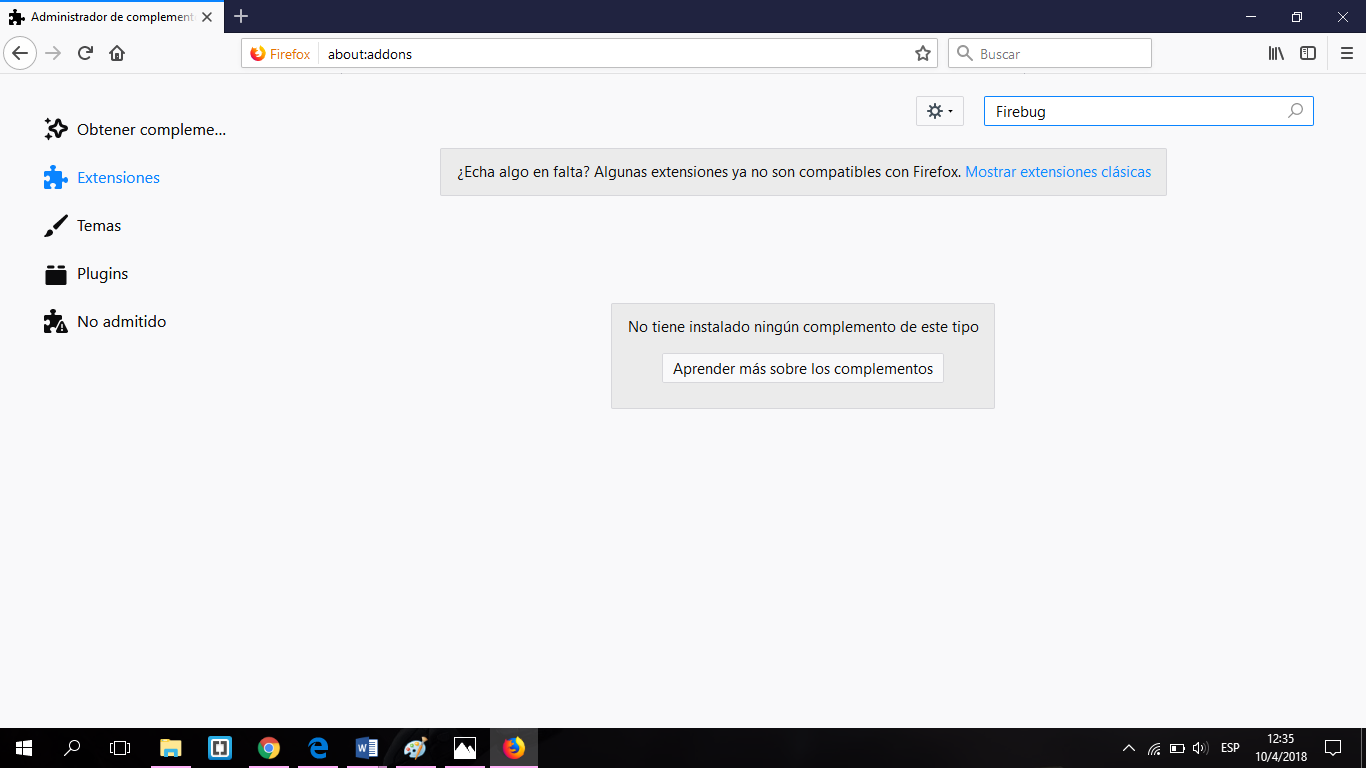
El objetivo del laboratorio es explicar cómo editar, depurar y monitorizar el CSS, HTML y JavaScript y además obtener tecnologías del lado del servidor y cookies.

Tareas de laboratorio:

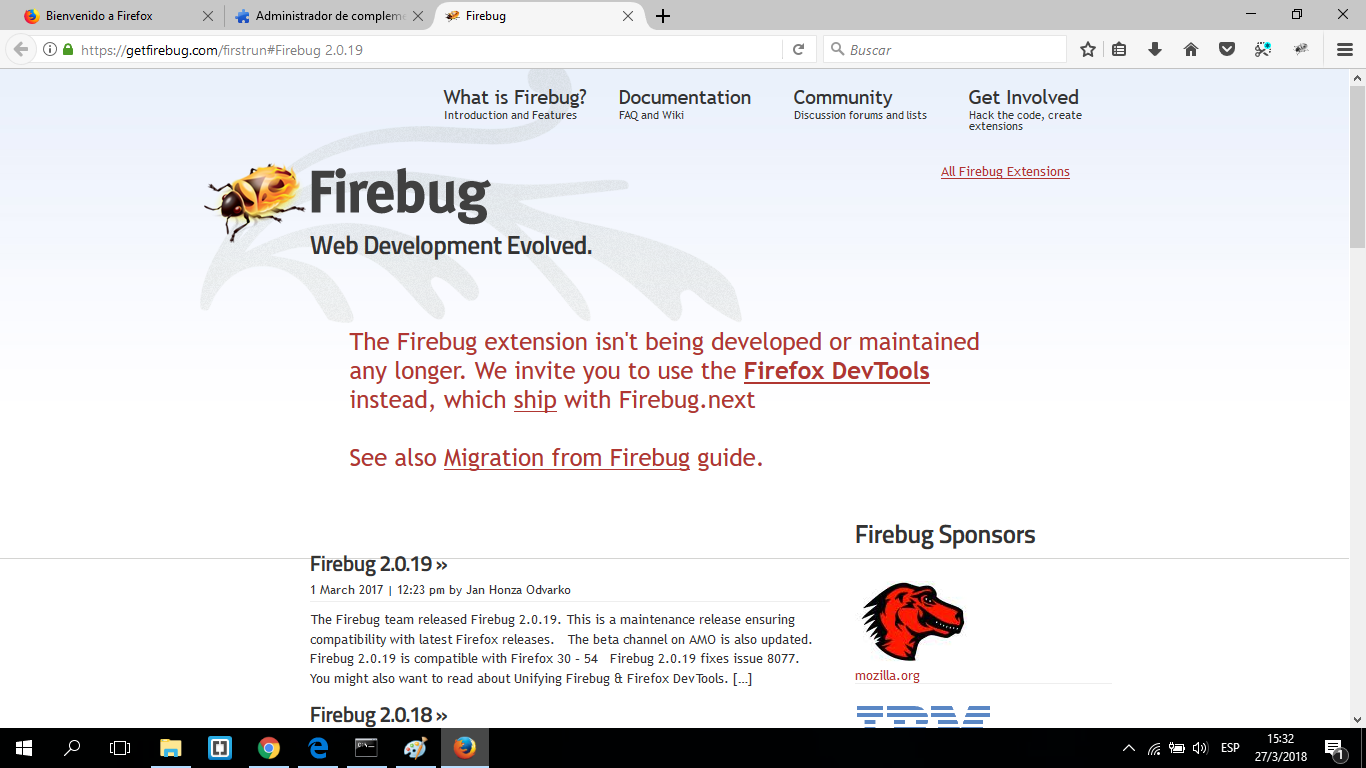
1. Abriremos nuestro navegador web Firefox y escribiremos <https://addons.mozilla.org/en-US/firefox/addon/firebug> en nuestra barra de direcciones y presionaremos **Enter**.
2. Si esto no resulta es probable que Firebug ya no se encuentre disponible en las nuevas versiones, para hacer estas pruebas usaremos la versión 56.0, también como otra alternativa se puede usar Firefox para desarrolladores ya que en este viene incorporado Firebug
3. Para la instalación de Firebug nos iremos a la sección complementos del navegador esta se encuentra en la parte superior derecha de la venta de nuestro navegador



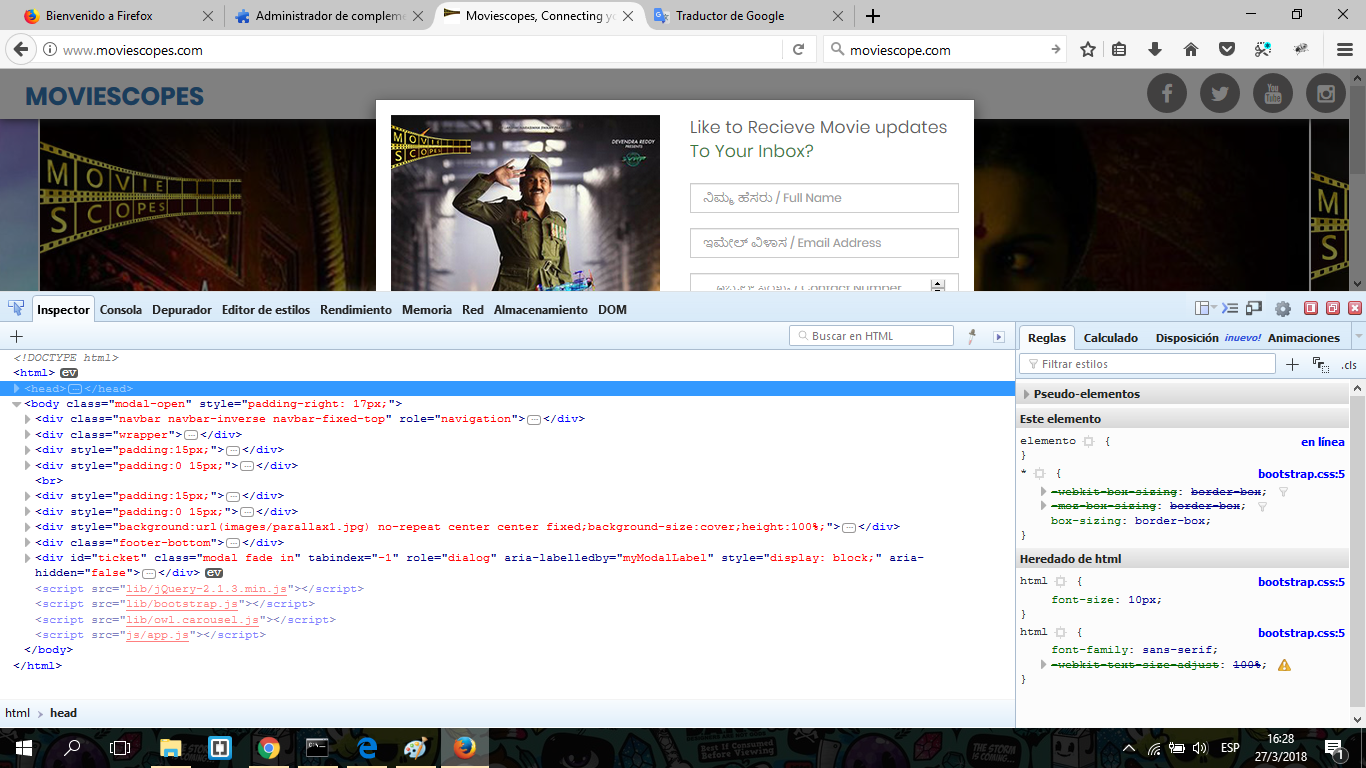
1. Luego nos vamos a **Extensiones** y buscamos Firebug



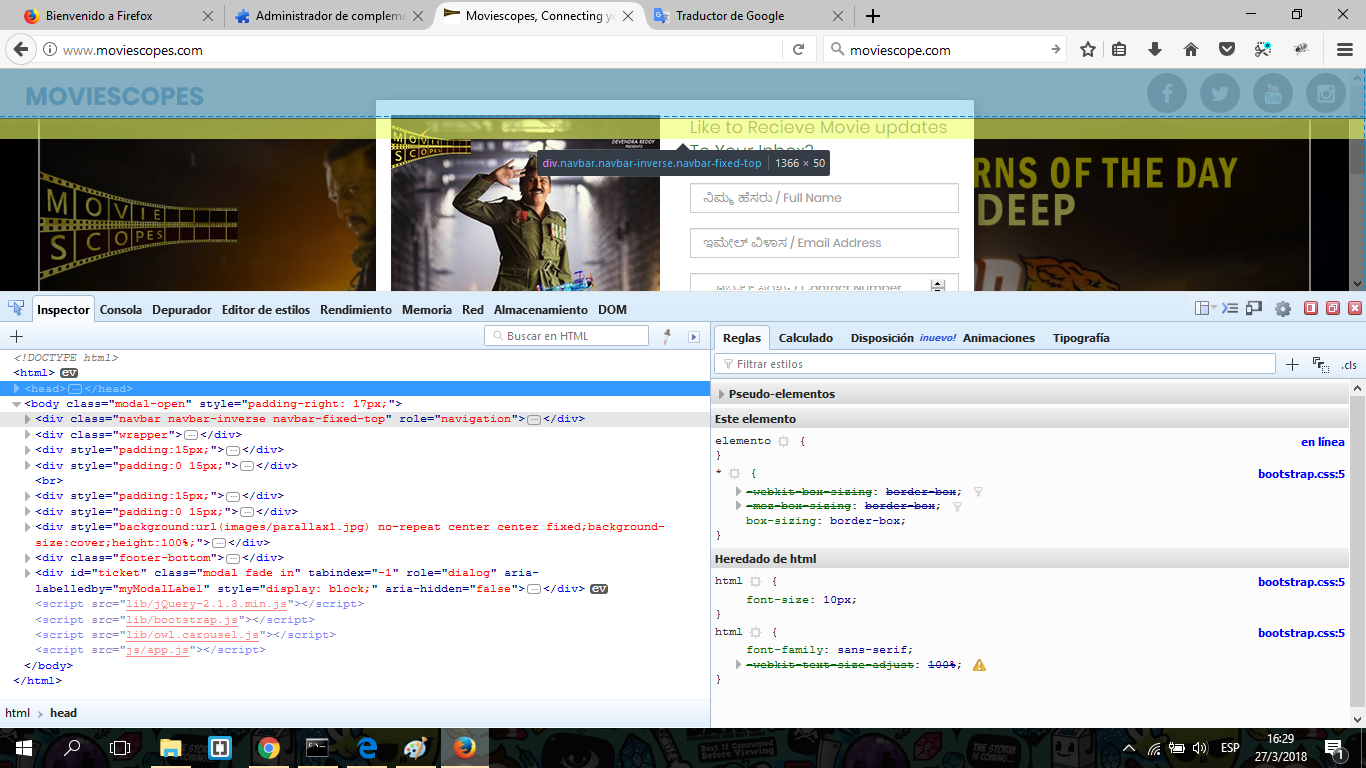
1. Una vez instalado Firebug se deberá mostrar la siguiente pestaña



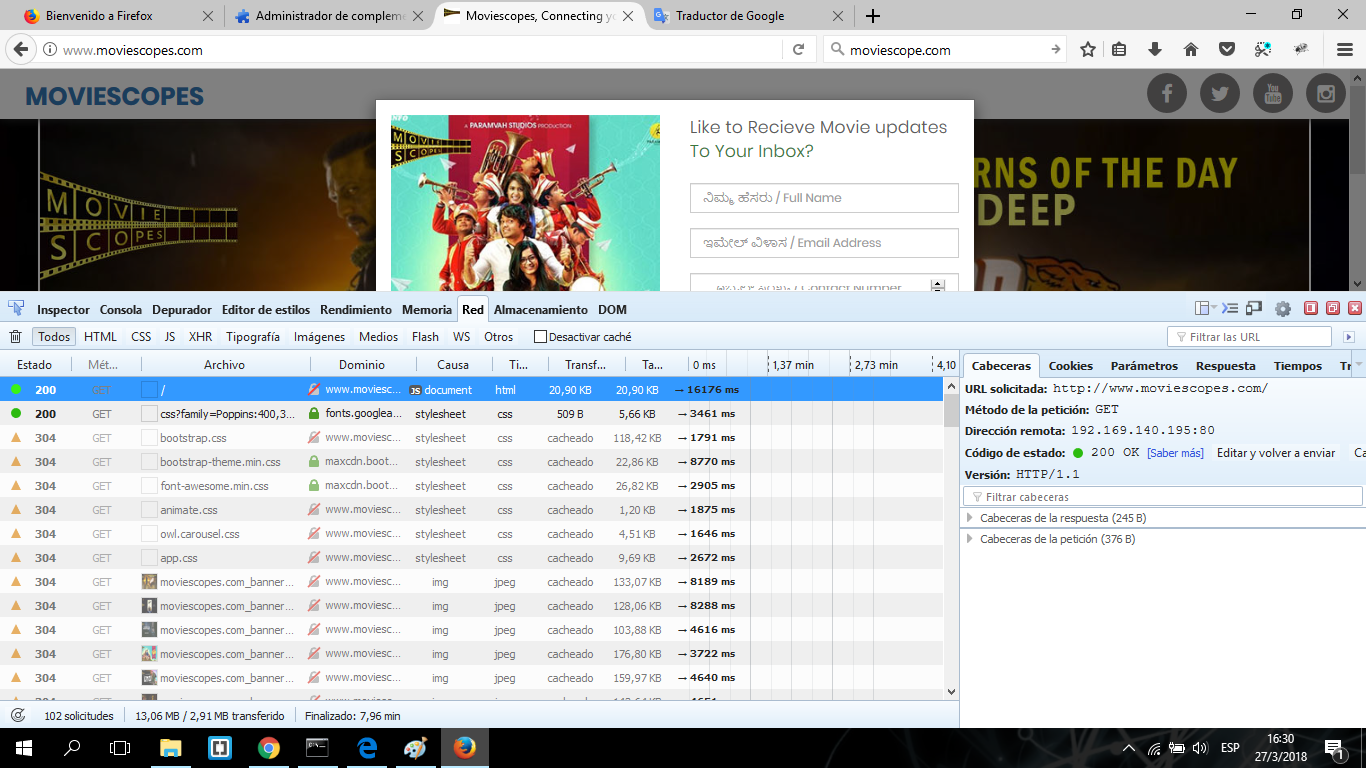
1. Luego de haber concluido su instalación escribiremos la URL del sitio web objetivo en la barra de direcciones [https://www.moviescopes.com](https://www.moviescopes.com/)
2. Una vez hecho esto deberá ejecutar Firebug, para esto daremos clic en el botón que está en la parte superior derecha de la ventana de nuestro navegador
3. Ahora nos vamos al modo inspector y observaremos que nos carga todo el código HTML de la página como se ve en la siguiente imagen.

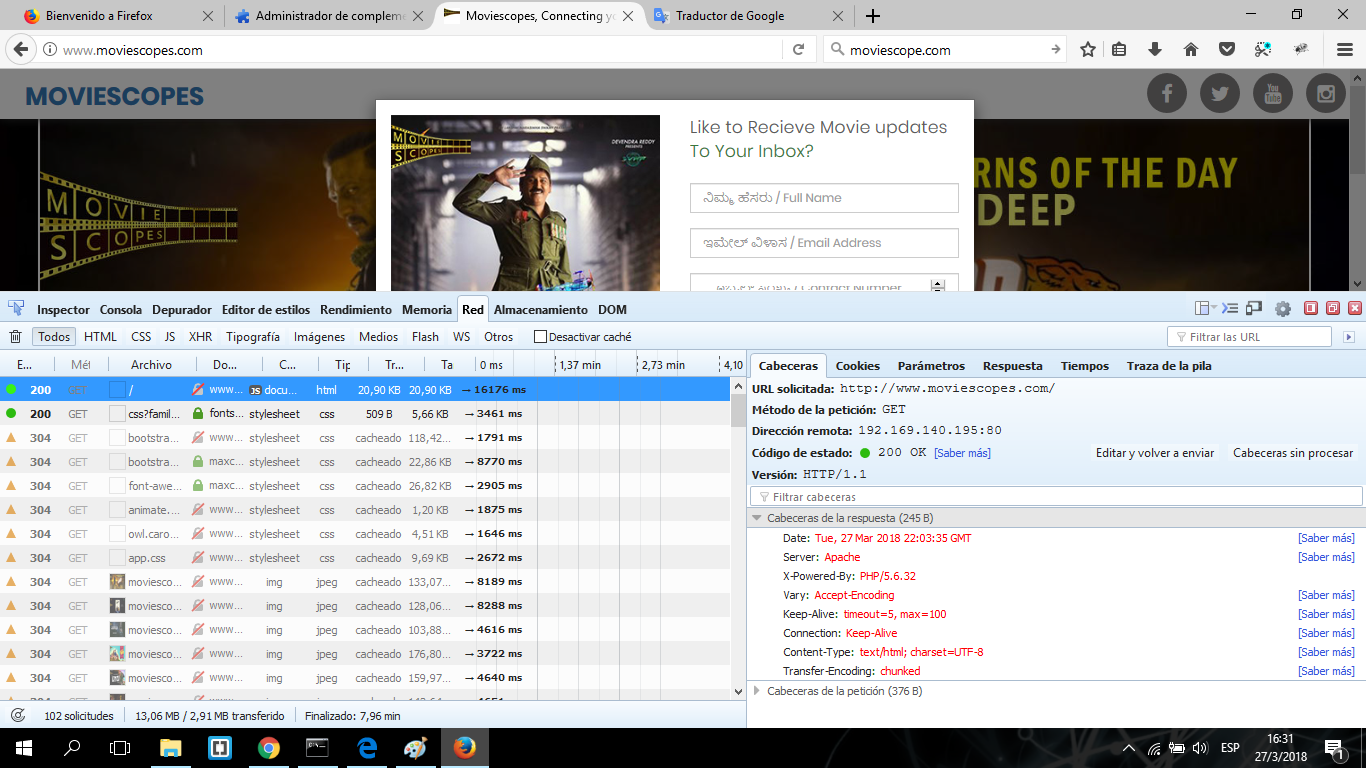


1. Como podemos observar al lado derecho de esta ventana también nos muestra el código CSS y nos muestra la posible herencia de este.



1. Ahora nos dirigimos a la pestaña **Red** del panel de control de Firebug, le damos la opción **Todos**
2. Esta pestaña nos muestra todas las peticiones GET y respuestas para todos los ítems en la sección **Net** tales como **HTML**, **CSS** etc. A lo largo con su tamaño, estado, línea de tiempo, dominio e IP.





1. Clic en la pestaña **almacenamiento** del panel de control de **Firebug**
2. En esta pestaña observaremos todas las cookies almacenadas en nuestro navegador cada vez que accedemos a una página web.
3. Un atacante puede utilizar técnicas de sniffing para robar las cookies y entonces manipularlas. De este modo se hackea la sesión de autenticación de un usuario sin necesidad de entrar legítimamente con las credenciales.
4. Un atacante puede obtener script relacionados con la web, identificar tecnologías del lado del servidor y manipular cookies. Donde permite realizar actividades fraudulentas tales como clonar sitios web, hackear sesiones, robar información de bases de datos etc.

