Rodrigo Castillo Camargo
Taller de Footprinting

1: Footprinting:
Toda actividad que nosotros hacemos, creamos o buscamos en internet deja una huella digital que es accequible para cualquier persona que tenga a disposición el internet.
El “Footprinting” hace referencia al regateo de información que se puede ejecutar a a travéz de técnicas de busqueda con el fin de encontrar información sensible de algún objetivo en específico, para fines del taller , haré Footprinting sobre la escuela colombiana de ingeniería julio garavito.

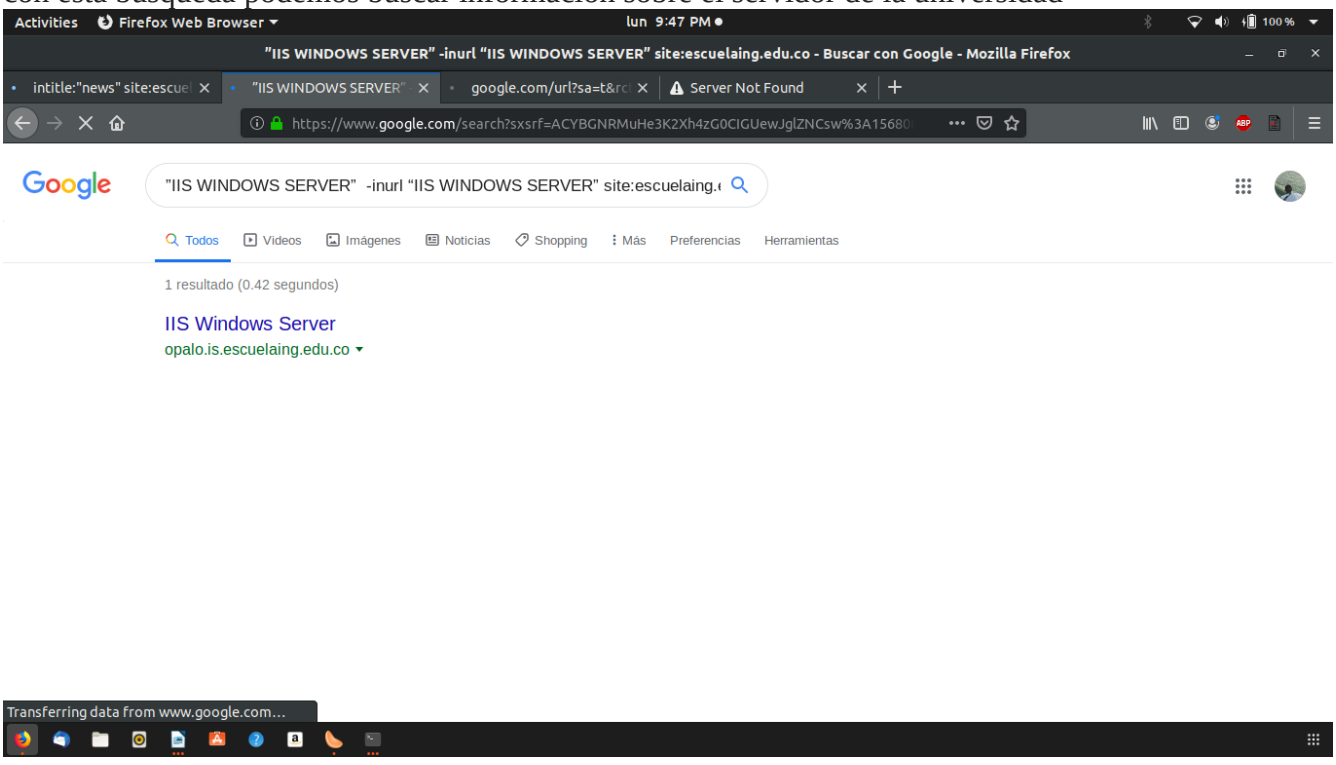
Parte 1- Busquedas avanzadas en google

Primera busqueda: intitle:"news" site:escuelaing.edu.co

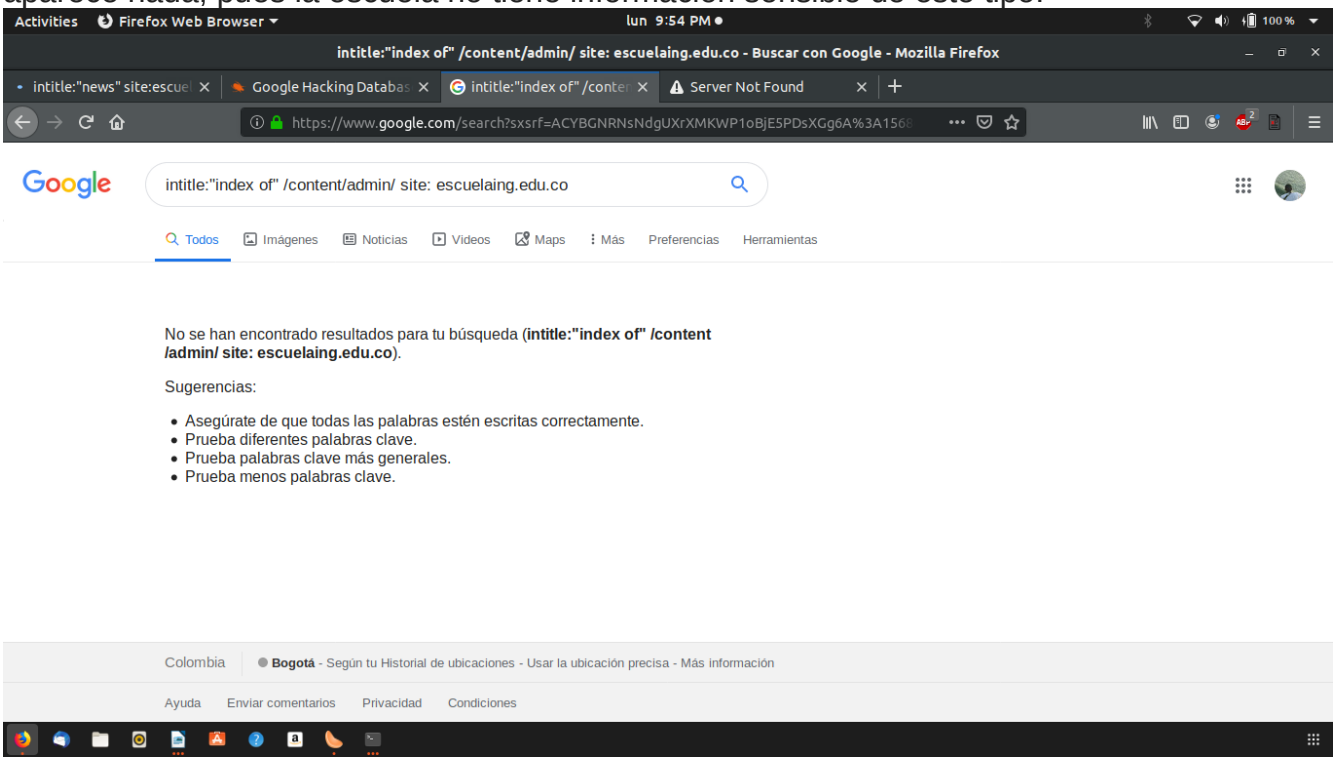
con ésta busqueda, podemos buscar información sobre noticias del laboratorio de la escuela colombiana de ingeniería, acá nos podemos informar sobre los lugares a los que tienen acceso los estudiantes en el laboratorio, sobre los dispositivos que éste posee, sobre la información del laboratorio que poseen los estudiantes, sobre los estudiantes de ingeniería que tienen acceso a la sala de sistemas puesto que fueron posicionados como monitores de ésta...etc.

Segunda Busqueda :Intitle:”IIS WINDOWS SERVER” -inurl “IIS WINDOWS SERVER” site:escuelaing.edu.co

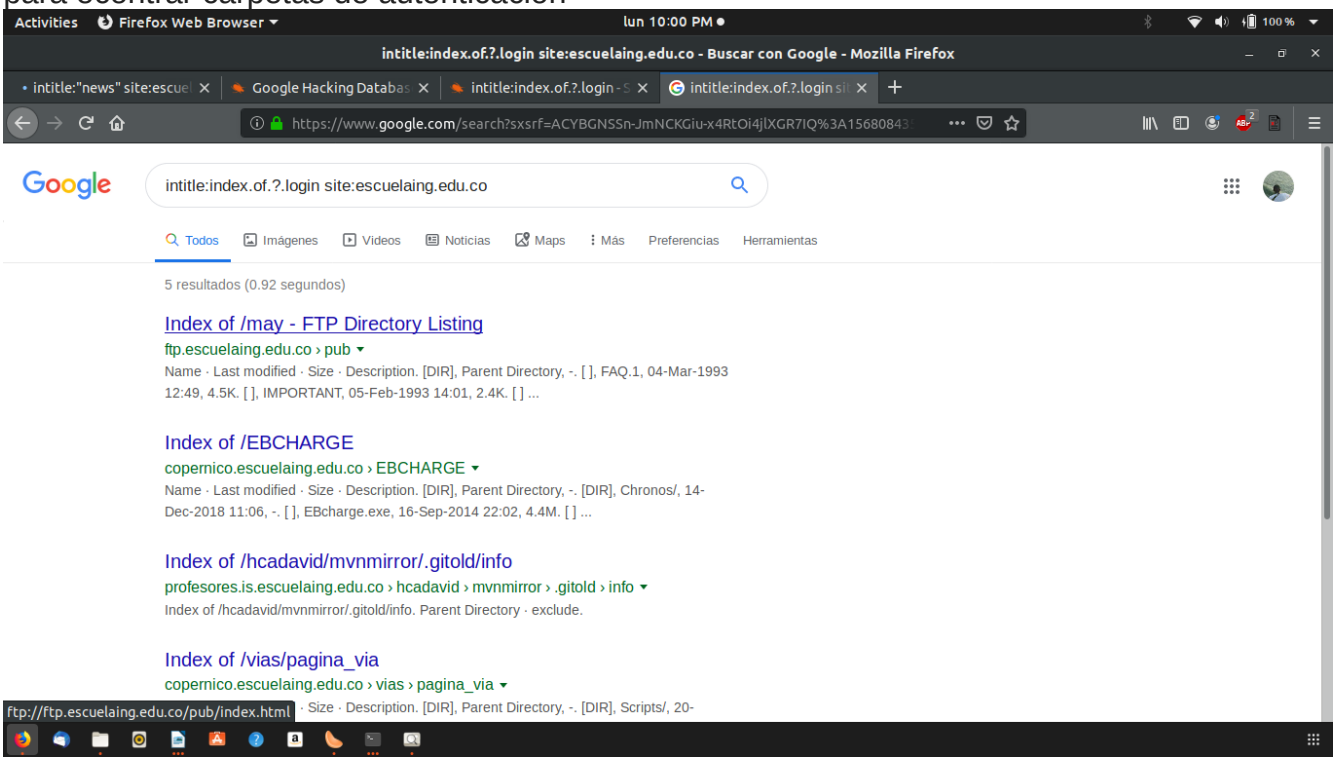
con esta busqueda podemos buscar información sobre el servidor de la universidad

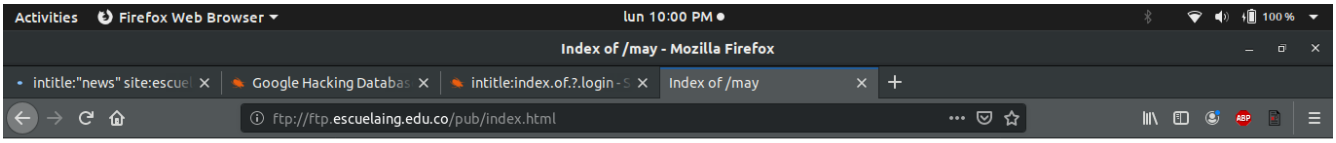


tercera busqueda: intitle:"index of" /content/admin/ site:escuelaing.edu.co
por ejemplo, en esta busqueda de directorios sensibles del contenido del administrador, no aparece nada, pues la escuela no tiene información sensible de este tipo.



Cuarta búsqueda:intitle:index.of.?.login site:escuelaing.edu.co es un comando que se usa para econtrar carpetas de autenticación

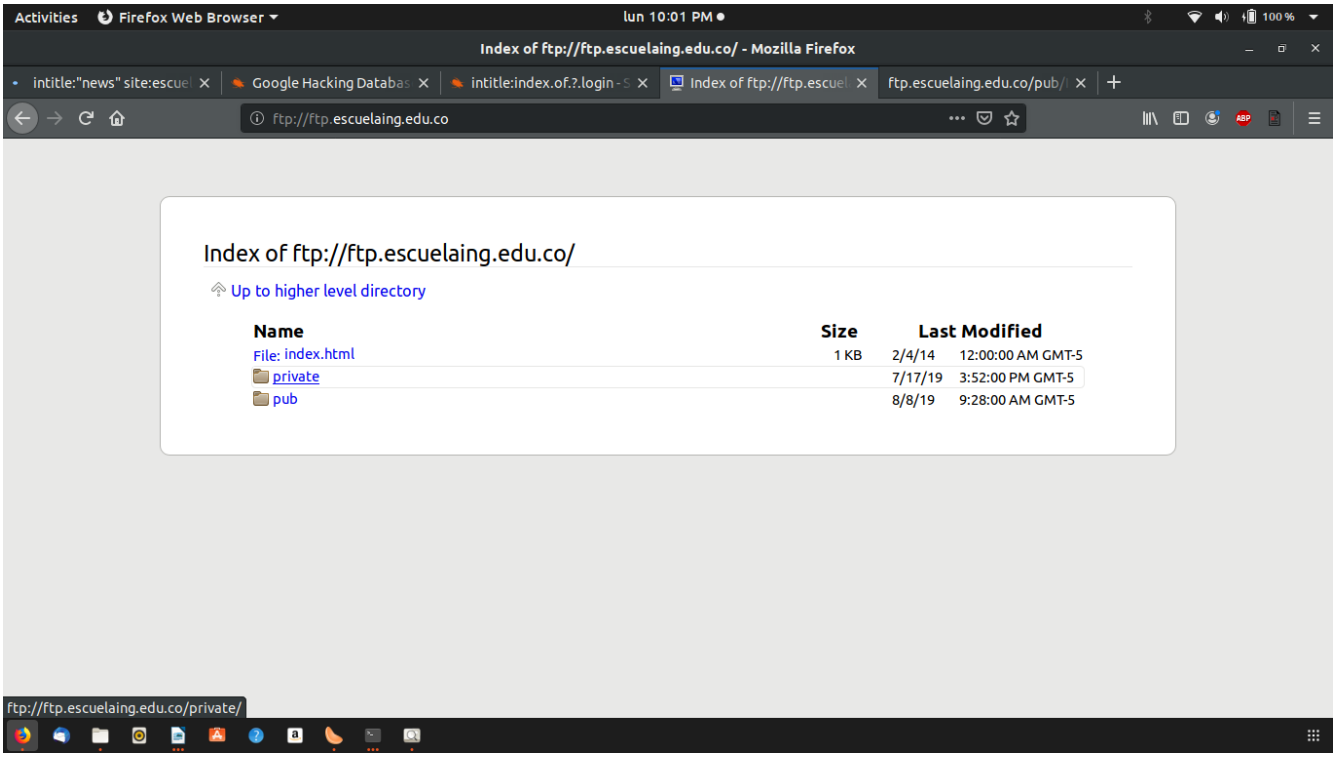


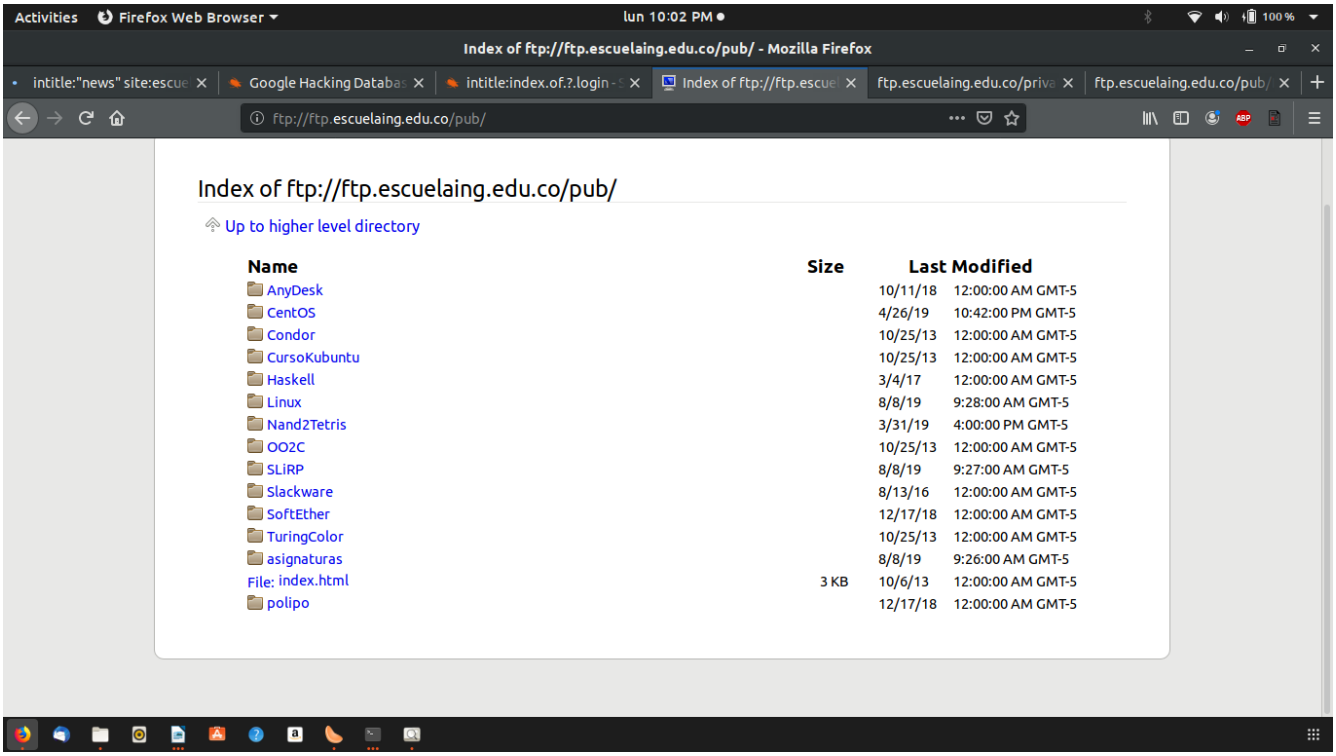


Index of /may

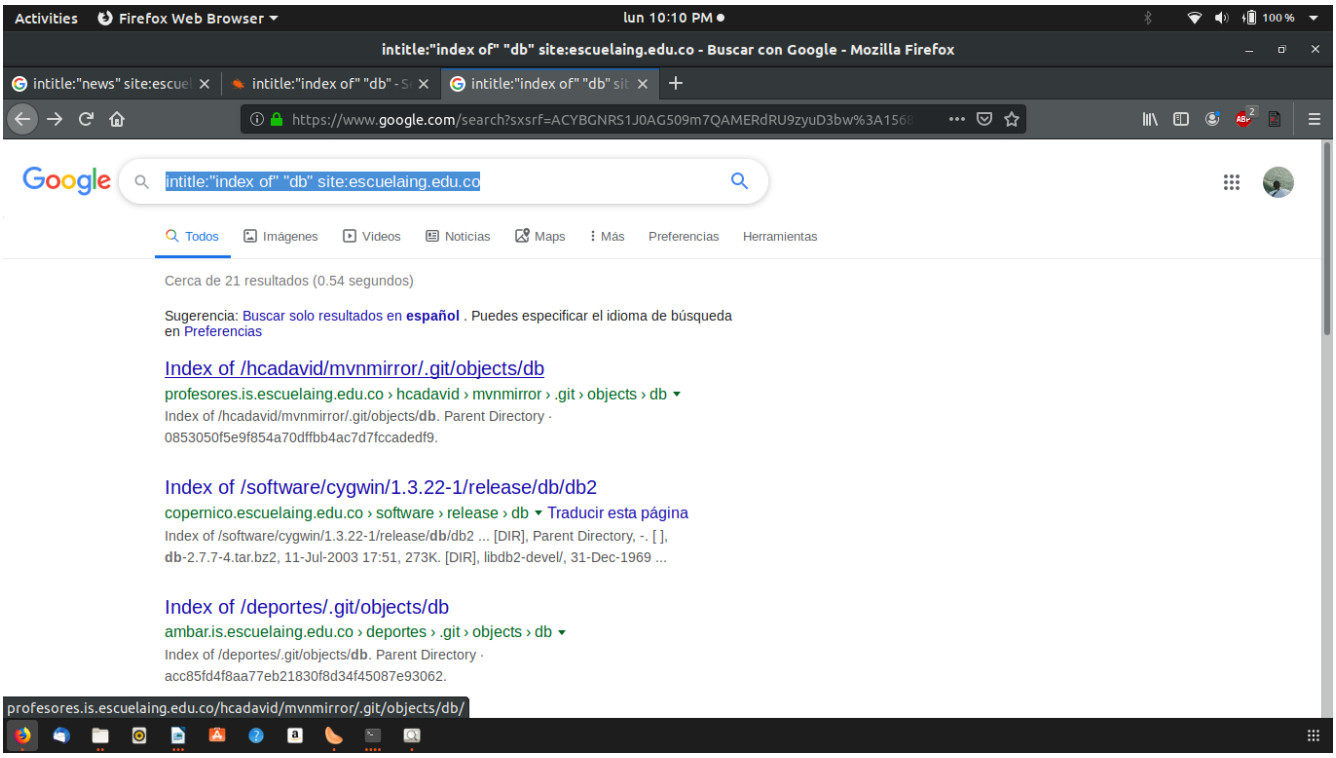
[ICO]	Name	Last modified	Size	Description
[DIR]	Parent Directory		-	
[ ]	FAQ.1	04-Mar-1993 12:49	4.5K	
[ ]	IMPORTANT	05-Feb-1993 14:01	2.4K	
[ ]	INTRO	11-Mar-1993 20:21	18K	
[ ]	REFRENCE	05-Mar-1993 20:18	24K	
[ ]	TBD	18-Jan-1993 21:10	765	
[ ]	USER-GUIDE	12-Mar-1993 16:23	19K	
[ ]	examples	07-Jan-1993 18:06	556	
[ ]	may-2.09.tar.gz	23-Mar-1997 14:27	83K	

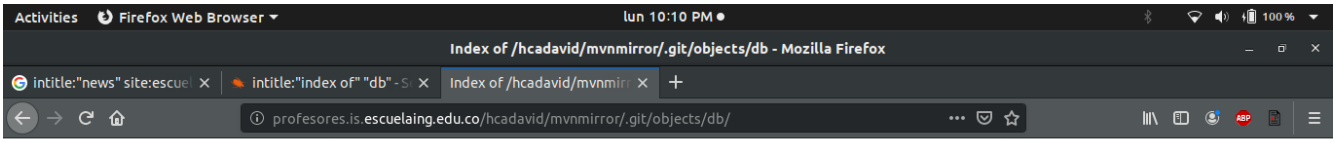
Apache/2.2.14 (Ubuntu) Server at linas.org Port 80





quinta busqueda:intitle:"index of" "db" site:escuelaing.edu.co
esta busqueda permite encontrar directorios sensibles que usen la palabra “db” que quiere decir data bases, da acceso a información sobre los servidores de la escuela de ingenieros que puede ser usada para futuros ataques



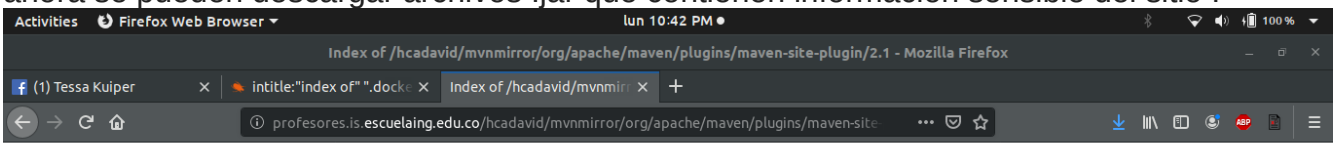


Index of /hcadavid/mvnmirror/.git/objects/db

- Parent Directory
- 0853050f5e9f854a70dffbb4ac7d7fccadedf9

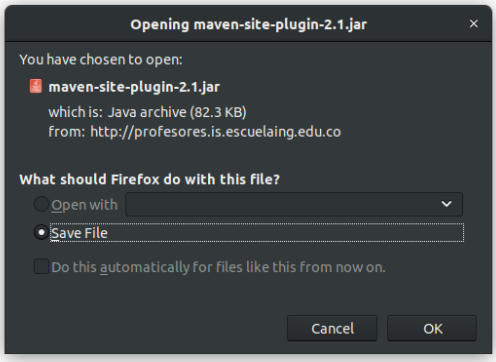
con lo que tenemos acceso a bases de datos sensibles de los estudiantes y profesores de la universidad.

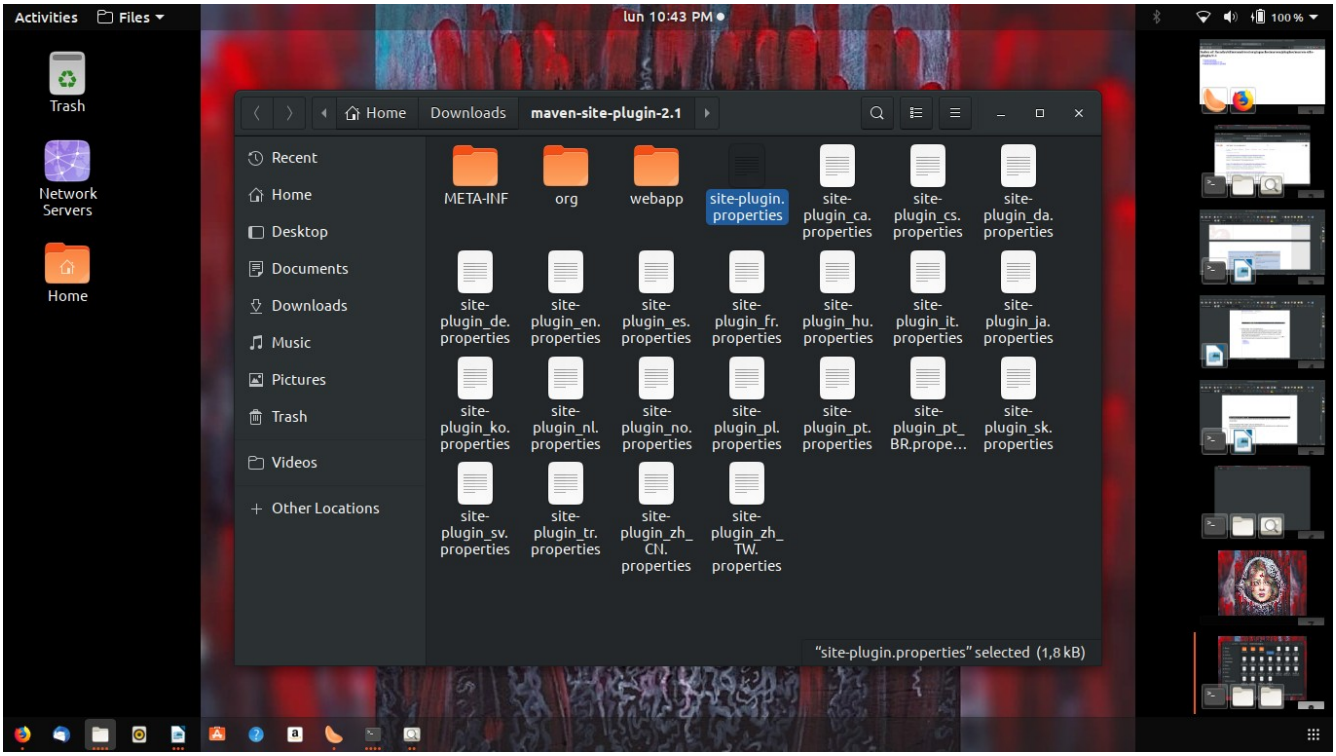
Sexta busqueda:intitle:"plugin" site :escuelaing.edu.co
en esta busqueda, aparecen directorios parecidos a los anteriores,con la diferencia de que ahora se pueden descargar archivos .jar que contienen información sensible del sitio .



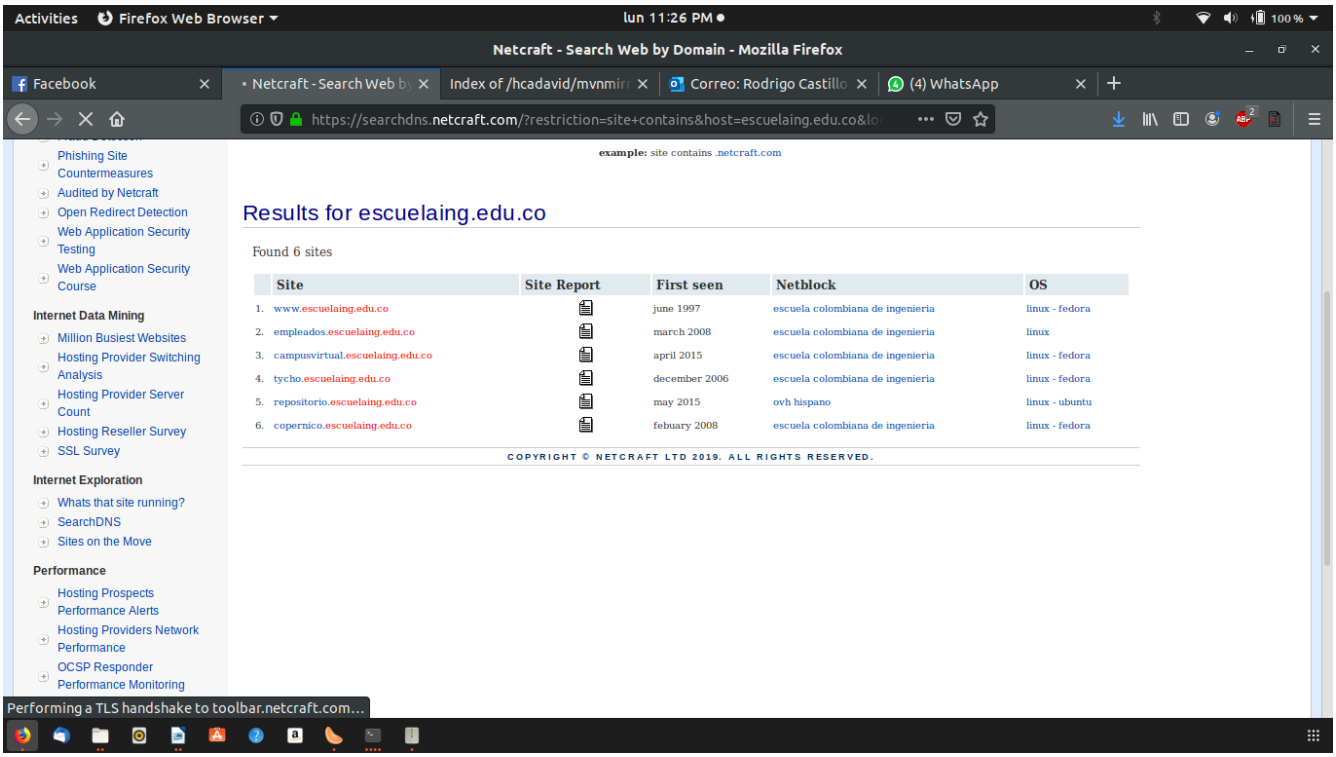
Index of /hcadavid/mvnmirror/org/apache/maven/plugins/maven-site-plugin/2.1

- Parent Directory
- maven-site-plugin-2.1.jar
- maven-site-plugin-2.1.jar.sha1

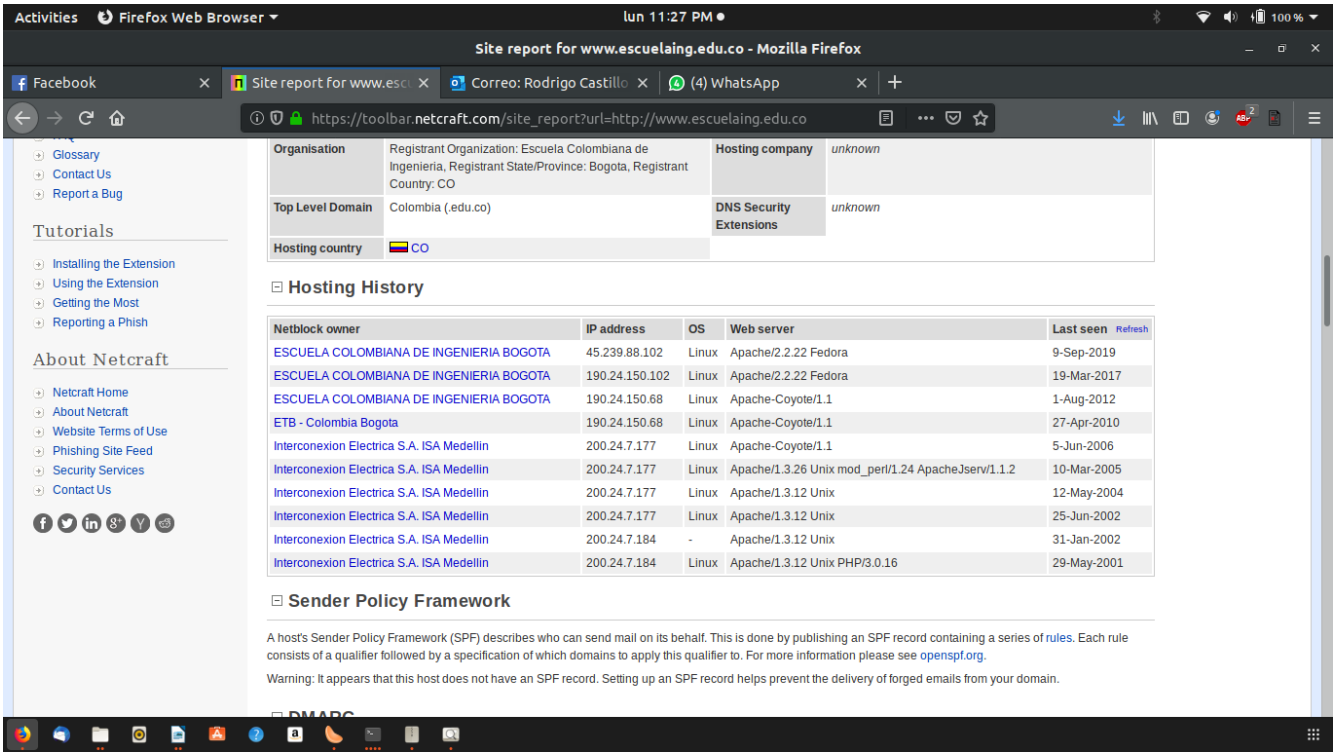




Segunda Parte: Netcraft

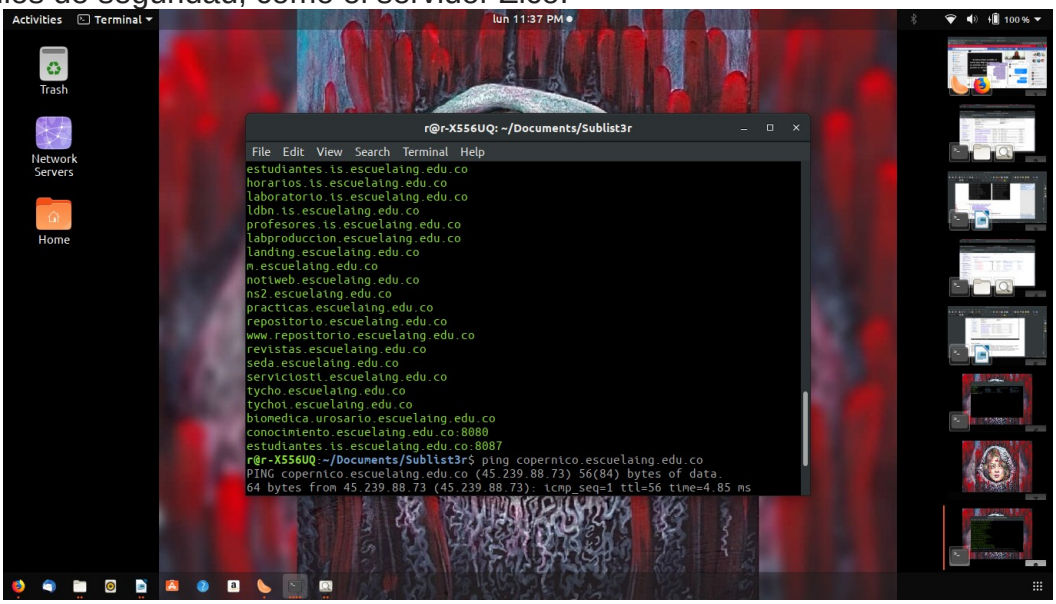


En netcraft podemos encontrar información referente a los servidores de la pagina , acerca del administrador de la pagina, acerca de los ips de los dominios de los servidores de la pagina, los sistemas operativos que usan y sus revisiones, esta información puede ser util para encontrar servidores desactualizados y vulnerabilidades en ellos



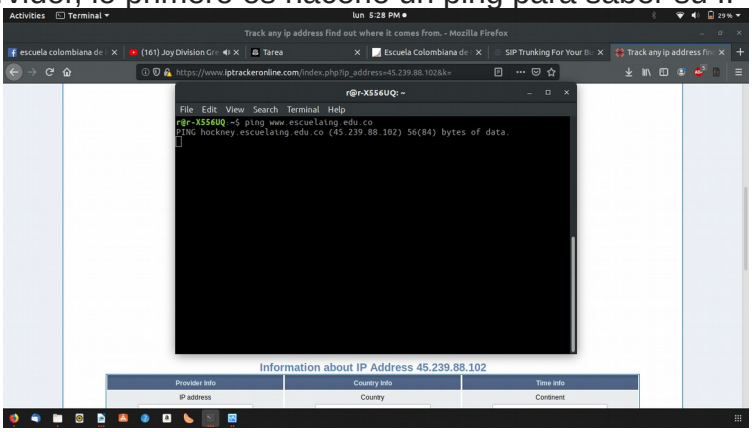
Parte 3: Sublist3r :

Sublist3r es un Script en python desarrollado por Ahmed Aboul-Ela , lo que hace es analizar en distintos sitios como en google, bing, baidu, yahoo...etc para averiguar por los subdominios del dominio objetivo que están abiertos, éstos subdominios a veces pueden ser vulnerables puesto que pueden ser subdominios olvidados que estén desactualizados o tengan fallos de seguridad, como el servidor Zico.

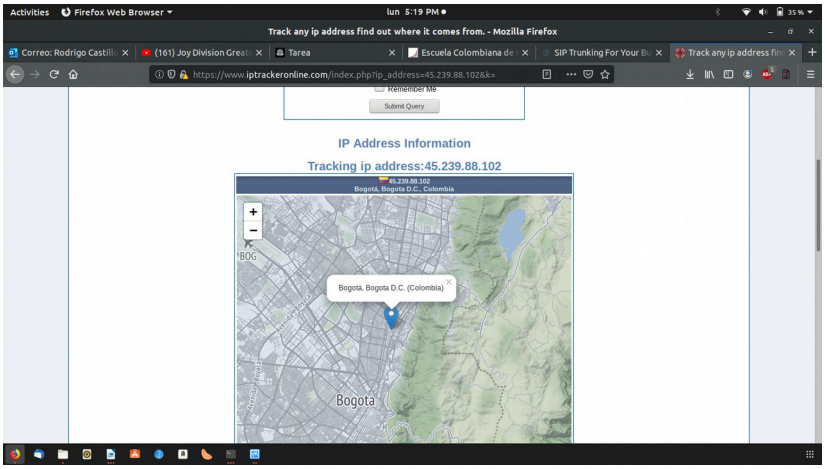


Parte 4: encontrar ubicación del servidor

para encontrar el servidor, lo primero es hacerle un ping para saber su IP

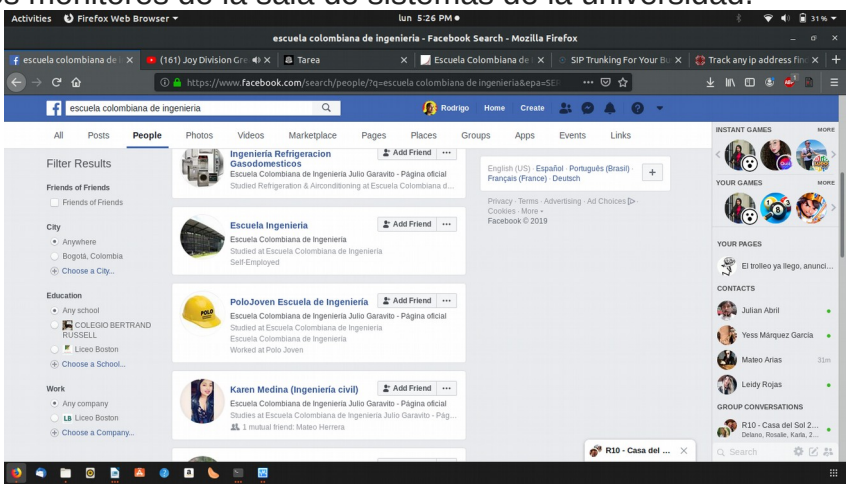


lo segundo es buscar algun localizador de ip en google, para el proposito de este curso, googleé IP-tracker en el buscador para acudir al servicio de alguno de los buscadores online, encontré que el servidor se encuentra ubicado cerca de la iglesia Lourdes, , la 63 con 8va (curiosamente, el servidor de la universidad El Rosario, se encuentra situado en la misma locación , por lo que no es descabellado deducir que ambas universidades acuden al mismo servicio de servidores.



Parte5 : Buscar en redes sociales.

Intenté buscar mediante el motor de búsqueda avanzada sobre gente que trabaja o estudia en la universidad minuto de dios, por ejemplo, busqué los monitores de la sala de sistemas, curiosamente, es gente que tiene amigos en común conmigo en facebook, por lo que, creo que para propósito del curso no tiene sentido, pero podría acudir a mis amigos para adquerir información de los monitores de la sala de sistemas de la universidad.



Parte 6: WebStractor y spadix

Con estas herramientas, es posible acceder a información sobre los empleados de la empresa, por ejemplo, a información de los profesores de la universidad, esta información puede ser util si se planea un ataque, pues a veces es mas facil atacar a los profesores y hacer ingeniería social.