# TAREA 2 – ATACANDO Y DEFENDIENDO

JHON SEBASTIAN ZUÑIGA LOPEZ

TUTOR SERGIO LUIS LUDO ARGUMEDO

GRUPO 55

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA
INGENIERIA EN SISTEMAS
Argelia – Cauca
febrero 2022

## Objetivo

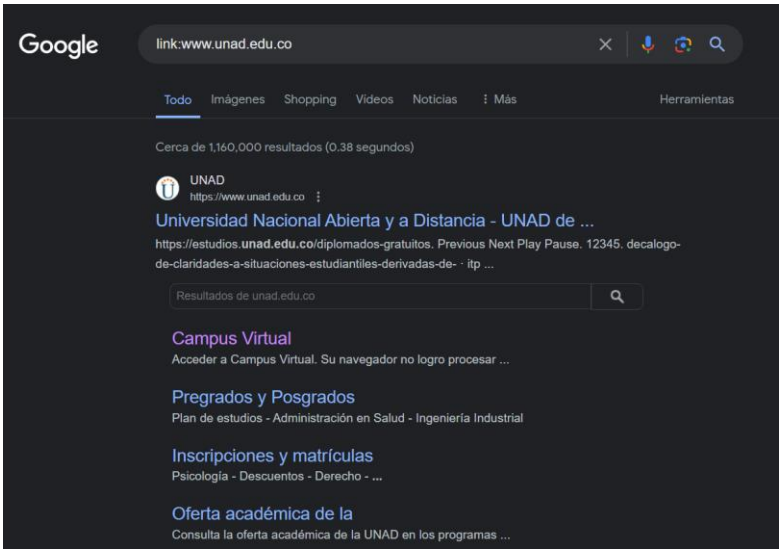
Realizar una evaluación de los riesgos y vulnerabilidades presentes en el entorno web. Para lograrlo, se utilizarán medios avanzados como las búsquedas avanzadas en Google con operadores específicos, que permiten obtener resultados más precisos y relevantes para identificar posibles amenazas. Además, se recurrirá a metabuscadores, herramientas que permiten obtener información de múltiples fuentes simultáneamente, agilizando así el proceso de identificación de riesgos y vulnerabilidades de manera más eficiente y completa en el entorno. Por último, web se empleará el navegador TOR para garantizar el anonimato y la privacidad durante la navegación, lo que facilitará la detección de vulnerabilidades sin revelar la identidad del evaluador.

## Desarrollo

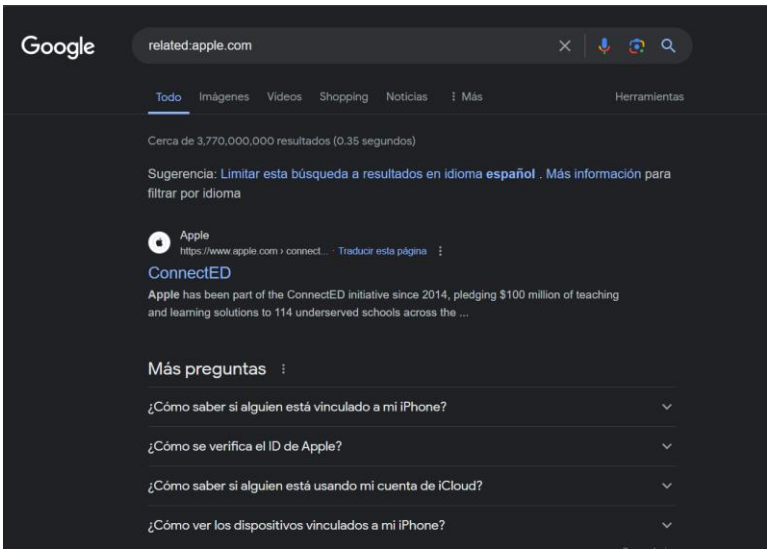
**Enlace de la presentación:**
https://www.canva.com/design/DAGAZDSNUh4/vSdWtSjATfYjGRujxa6gbA/edit?utm_content=DAGAZDSNUh4&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

**Parte uno: herramientas OSINT**

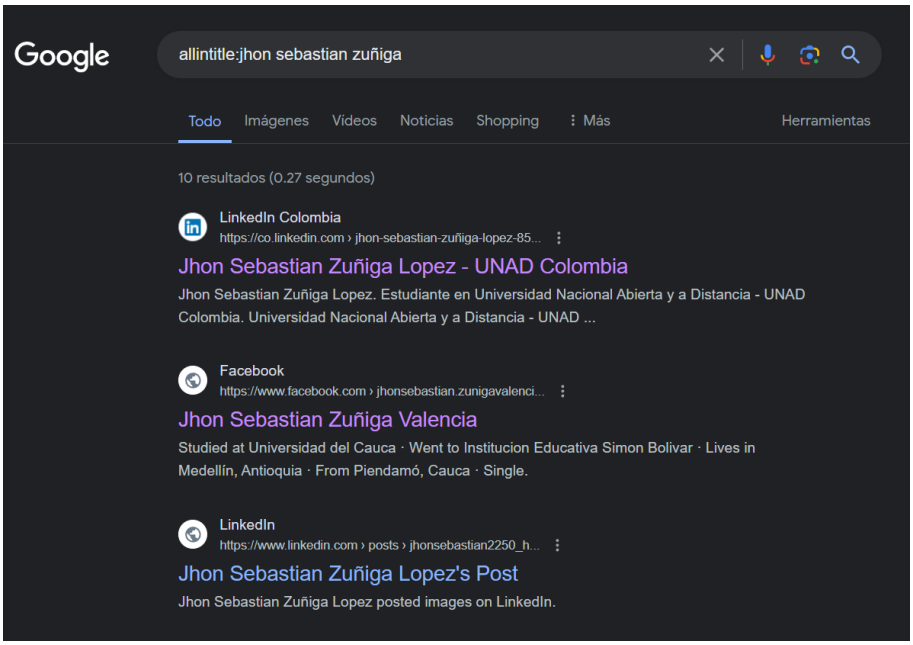
**Link**: Es un operador que se utiliza para obtener un listado de todas las páginas que se refieran a una dirección URL determinada. Por ejemplo, link:www.unad.edu.co

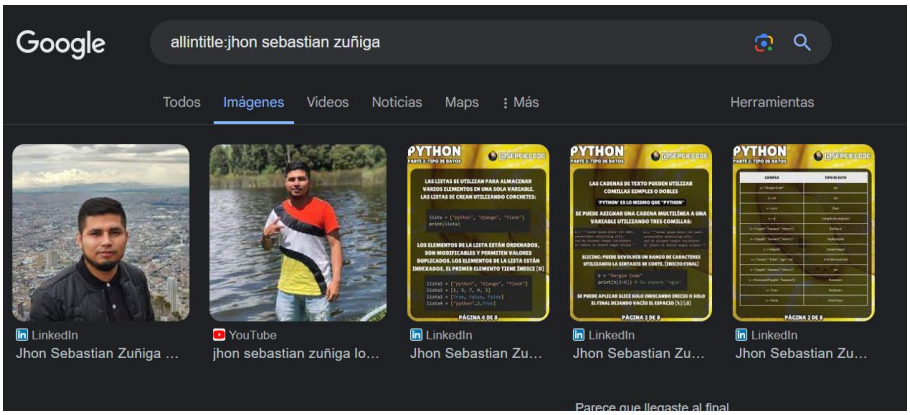



**Related**: Con este operador se pueden listar todas aquellas páginas que tengan algún tipo de relación o sean similares a un sitio determinado, por ejemplo, related:apple.com

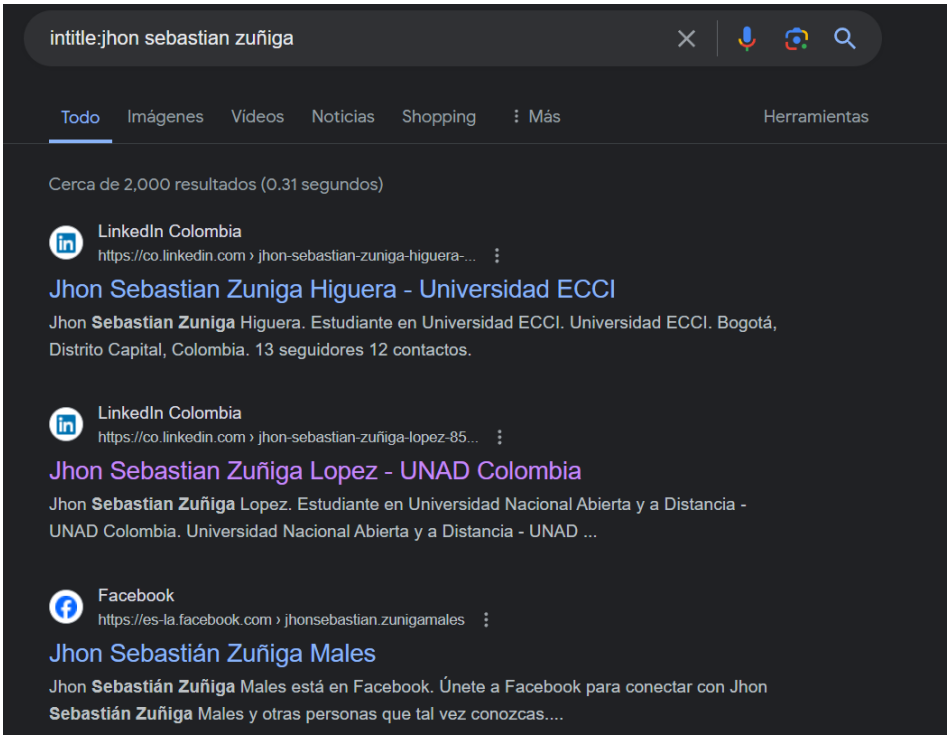


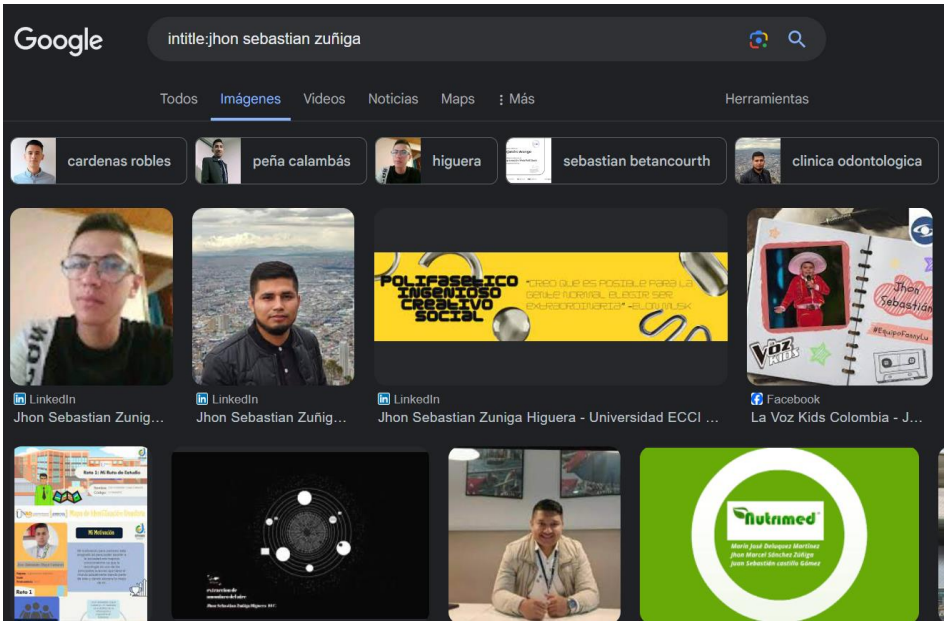

**Allintitle**: Con este operador se puede enfocar una búsqueda exclusivamente a los títulos. El operador busca el metatitle en las páginas o documentos y solo muestra los que coincidan con la búsqueda. Ejemplo, allintitle:jhon sebastian Zuñiga buscara aquellas páginas en donde el titulo contenga todas las palabras ingresadas



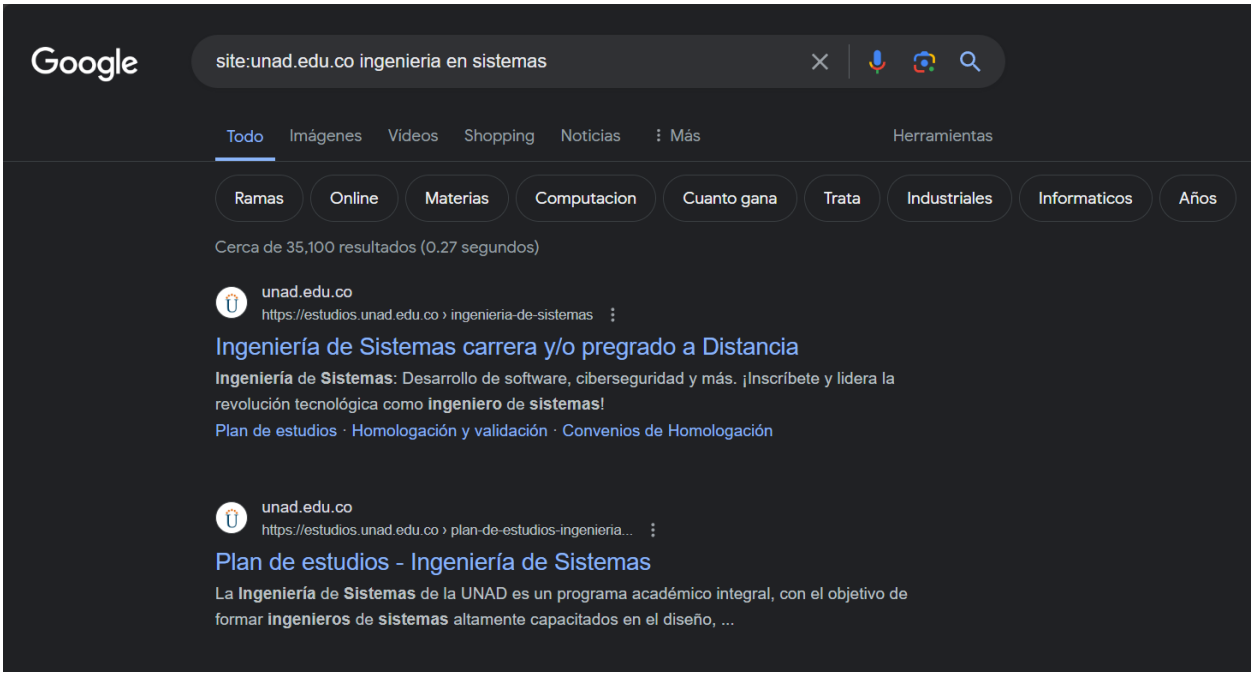



**Intitle**: al igual que el allintitle busca documentos, fotos, video, paginas, etc, en donde su título coincida con la busque, a diferencia del operador anterior este busca la primera palabra en el titulo y si se ingresan más palabras serán buscadas en el contenido. Ejemplo, intitle:jhon sebastian Zuñiga, esto buscar la primer palabra en el titulo y el resto de palabras en su contenido.

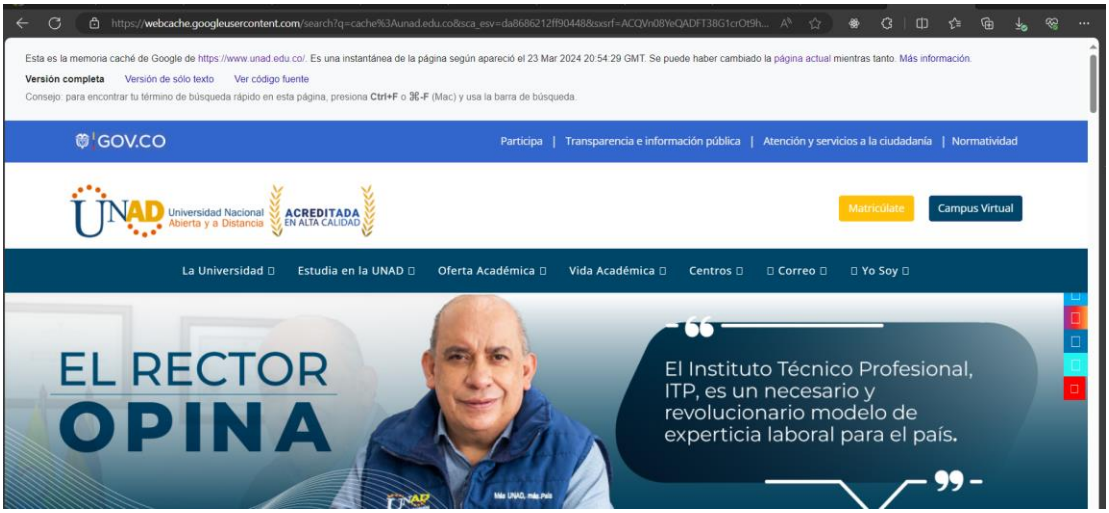





**Site**: Este operador es útil para realizar búsquedas de una página en específico, si se quiere buscar toda la información sobre un tema en específico de una página, basta con escribir el tema inmediatamente después del sitio, ejemplo sitie:unad.edu.co ingeniería en sistemas.

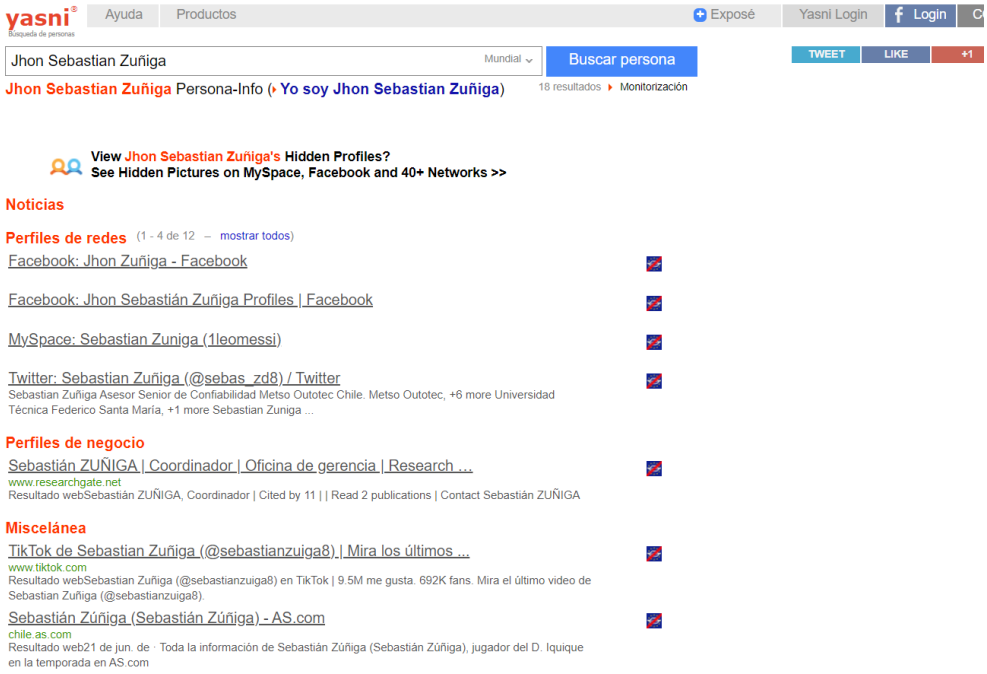


**Cache**: Google guarda una copia en cache de las páginas, por lo cual con este operador podemos acceder a esa copia, por ejemplo cache:unad.edu.co

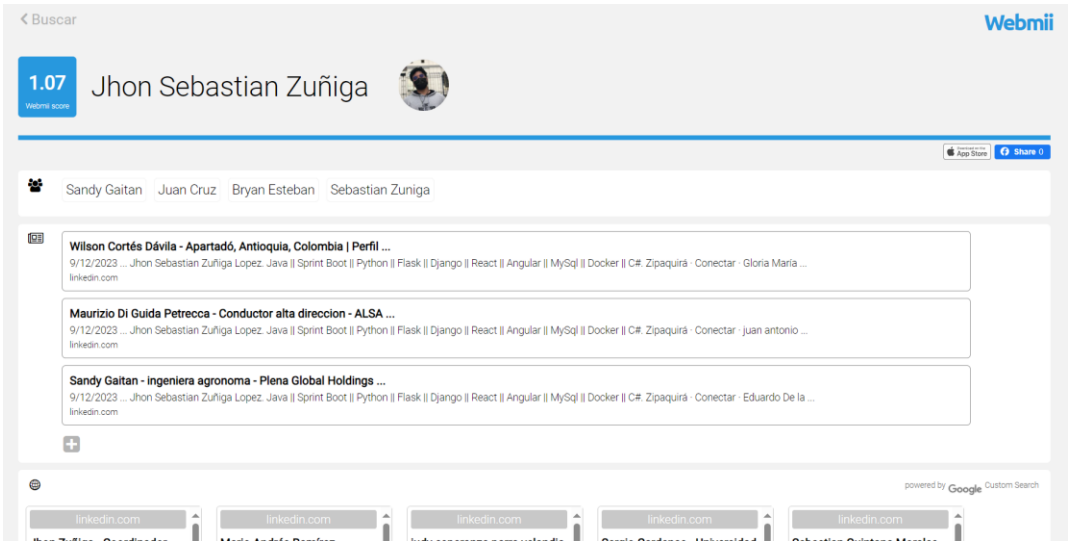



## Metabuscadores

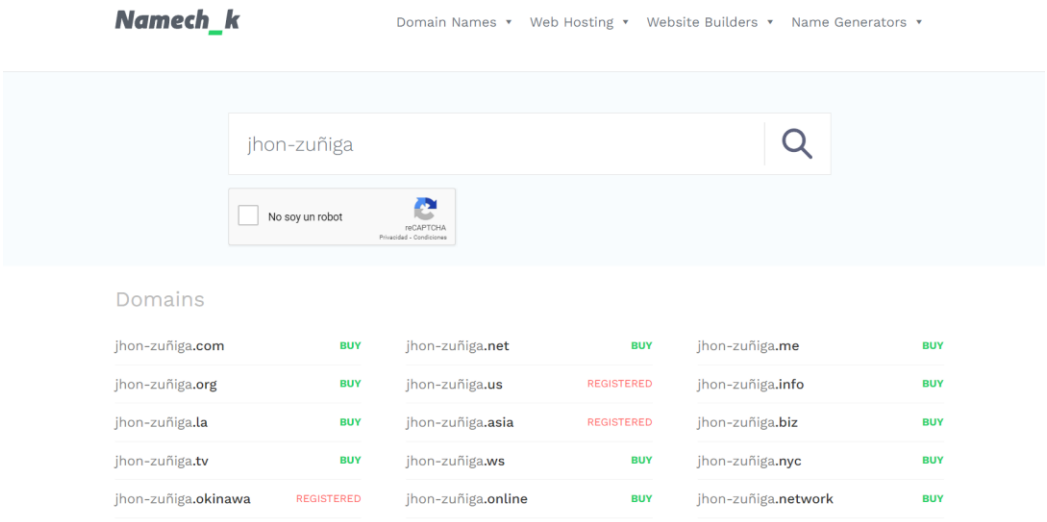
**Yasni**: es buscador especializado en el rastreo de personas mediante la información publica en internet, solo basta con indicar nombre y apellidos y el buscador realizara el rastreo.

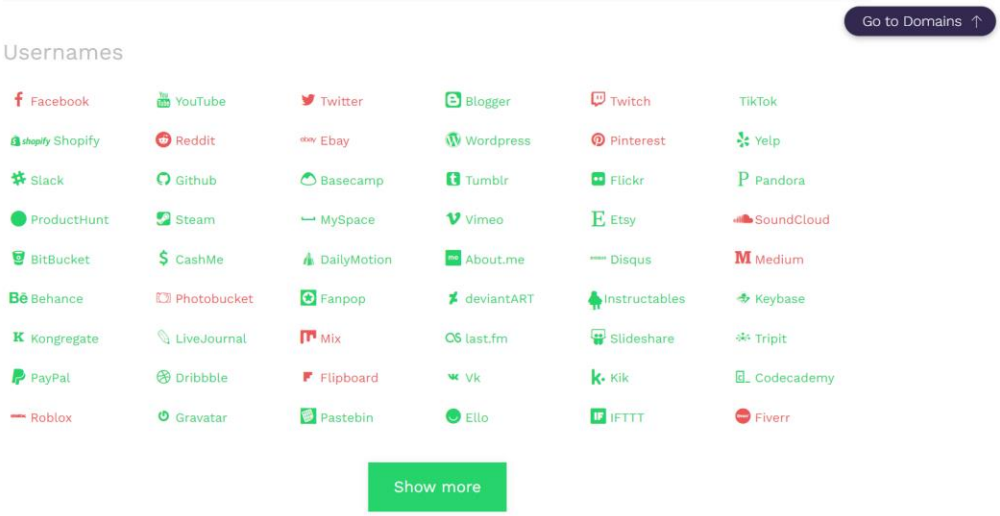


**Webmii**: Es un motor de búsqueda que recopila información publica en la web y de diversos sitios web.




**Namech_k**: es una pagina desarrollada para verificar si un nombre de usuario o dominio esta se encuentra disponible o esta siendo usado en algún lugar.






## Conclusión

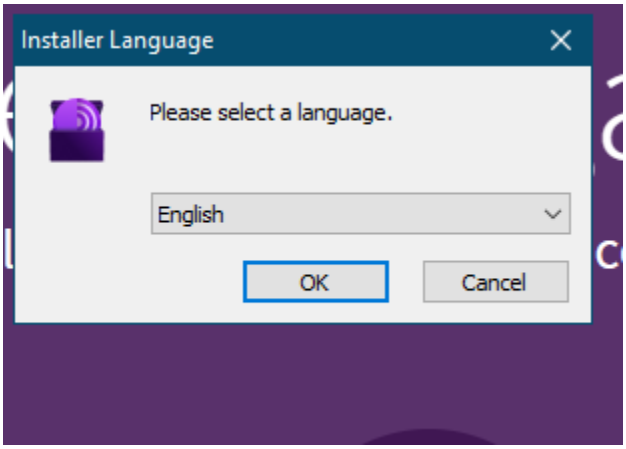
Los resultados del ejercicio permiten concluir que por medio de la web fácilmente se puede implementar la ingeniería social con el objetivo de realizar un ataque ya sea a un persona, grupo o entidad, por este motivo es muy importante tener en cuenta la información que se está publicando en las diferentes redes sociales o páginas web ya que después de que la mayor parte de datos publicada es accesible por los atacantes.

**Segunda parte - Atacando**

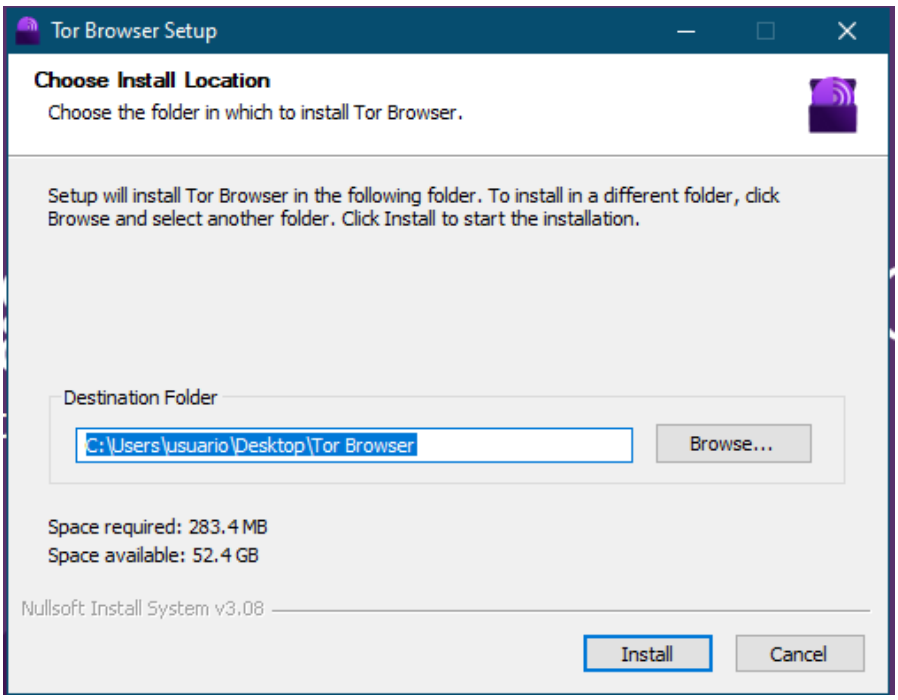
**Instalación de TOR**

Se ingresa a la pagina principal de Tor, en esta se encuentra la descarga para los diferentes sistemas operativos, para el ejercicio se escoge el SO Windows

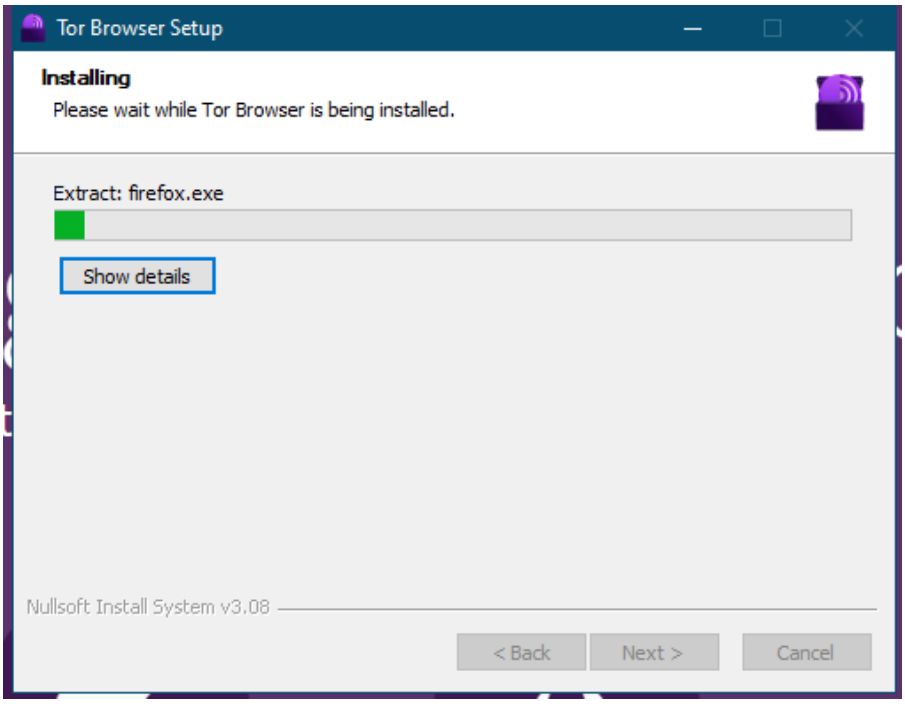

Finalizada la descarga, se ejecuta el archivo descargado, inicialmente se configura el idioma de instalación.



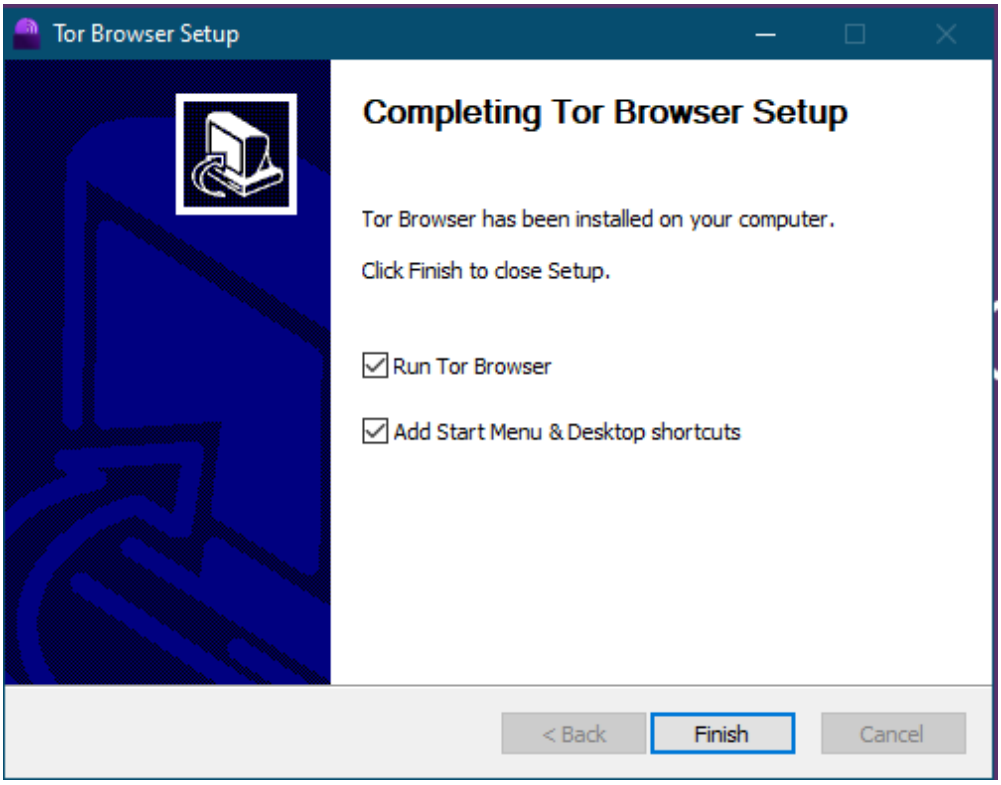
Por defecto el instalador ya tiene una ruta de instalación. Si se requiere se puede escoger otra ruta, para el ejercicio se deja por defecto.




La instalación ha comenzado.

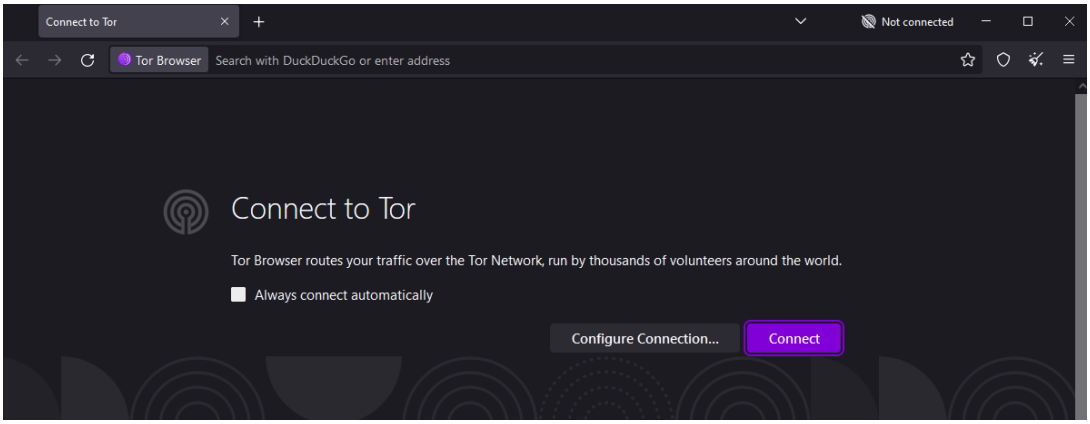


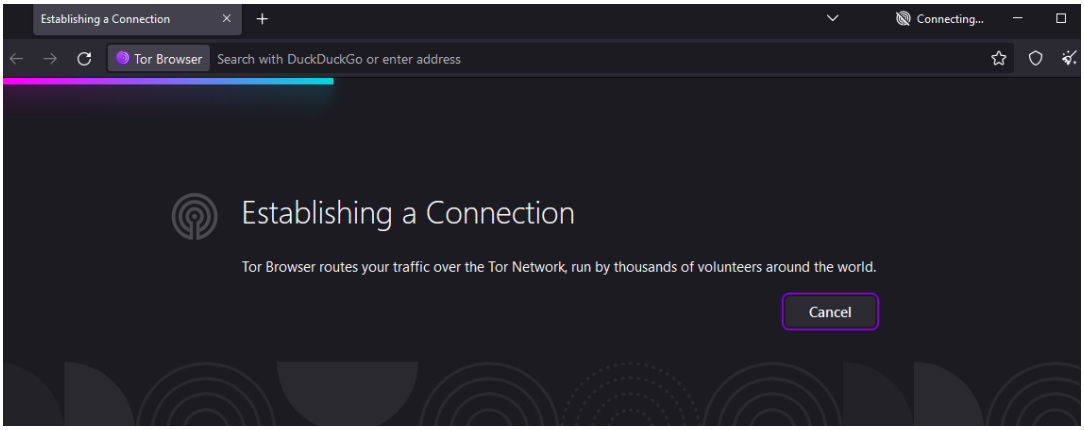
Cuando la instalación finaliza, tenemos esta interfaz.



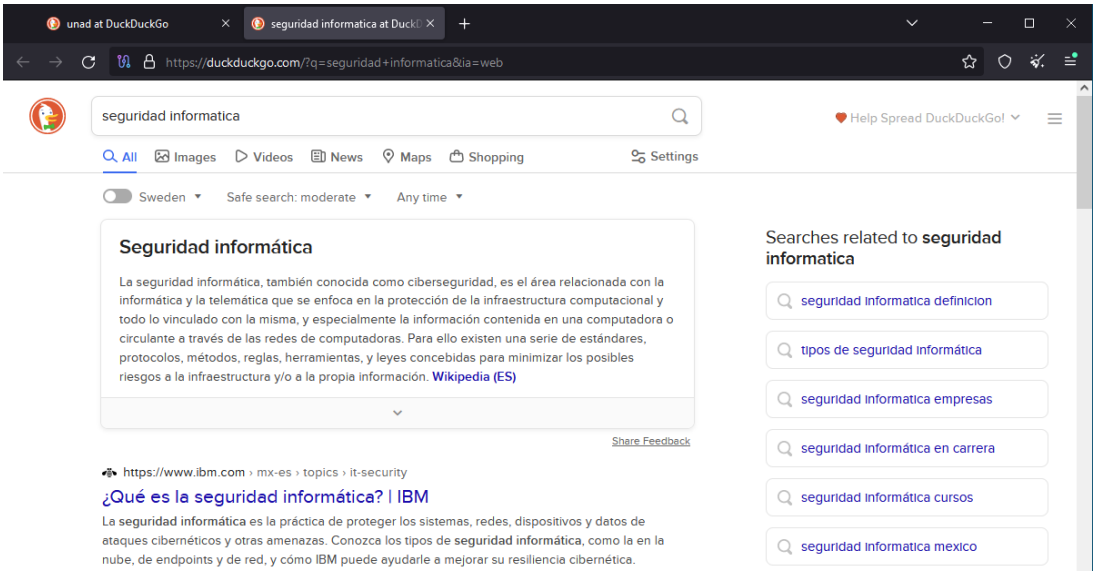

En este momento ya se tiene instalado el navegador TOR, solo queda ejecutarlo.

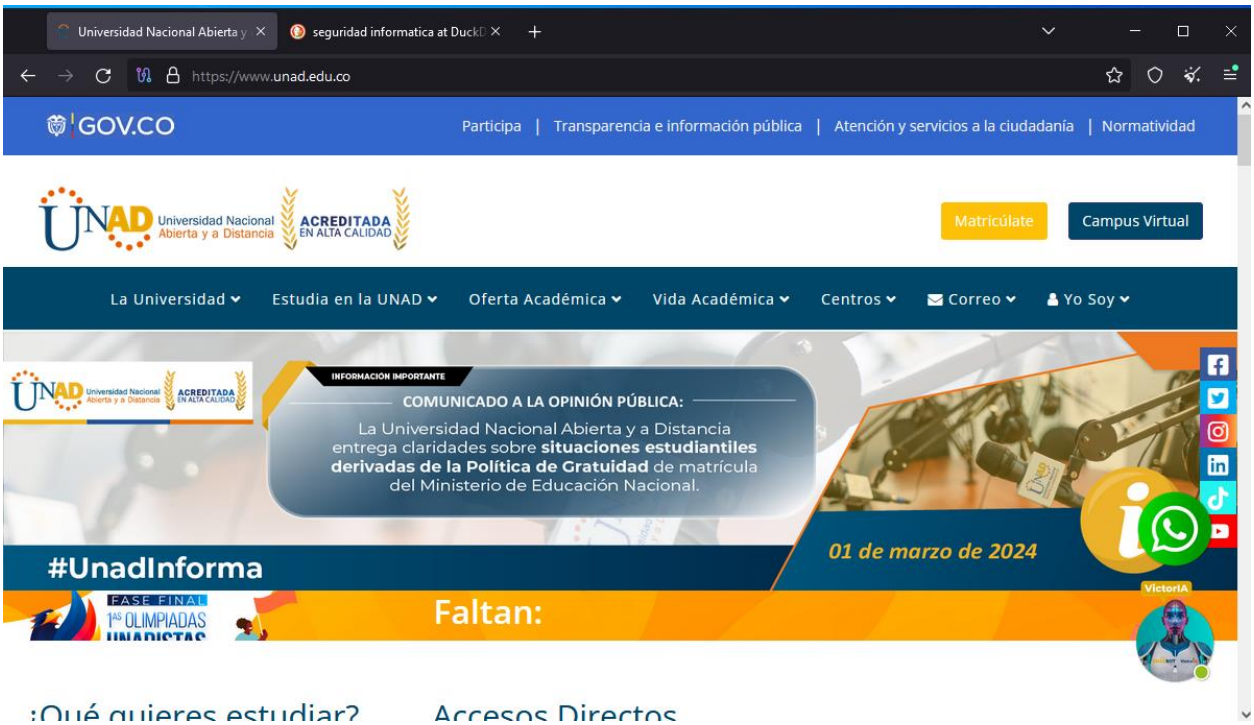
Al momento de ejecutarlo pedirá conexión con TOR.






**Listo ya podemos navegar con TOR.**






**Conclusión**

El navegador TOR permite navegar de forma anónima y segura por la web enmascarando la dirección IP del usuario y enrutando el trafico por medio de diferentes nodos distribuidos por todo el mundo. Este protege la identidad en línea, permitiendo el acceso de forma segura y sin rastreo de terceros, sin embargo, en necesario tener en cuenta que esto no garantiza el anonimato l 100 por ciento, por lo cual es necesario utilizado con precaución y tener en cuenta las diferentes implicaciones legales que puede acarrear.

En Colombia no hay una ley que prohíba el uso de TOR, pero eso no quiere decir que todo lo que hagas dentro de Tor sea legal, si un usuario se ve envuelto en un asesinato, expendio de drogas, venta de armas o muchos otros delitos puede ser judicializado sin importar que el medio de acción haya sido el navegador TOR.

## Referencias Bibliográficas


23 operadores de búsqueda para usar Google como Profesional. (2021, mayo 1). Platzi. https://platzi.com/blog/23-operadores-de-google/

Fernández, Y. (2023, octubre 20). 39 operadores de búsqueda para Google para afinar al máximo el buscador. Xataka.com; Xataka Basics. https://www.xataka.com/basics/operadores-busqueda-para-google

Padallan, J. O. (2019). Ciber Security Ant Its C. En Arcler Press (Eds), Cyber Security (pp. 29-49). Canadá: Arcler Press. https://eds-s-ebscohost-com.bibliotecavirtual.unad.edu.co/eds/ebookviewer/ebook?sid=74ed1b82-395e-4e33-9ab1-c7b780f3f849%40redis&ppid=pp_Cover&vid=0&format=EB

Padallan, J. O. (2019).Social Media, Botnet, and Intrusion Detection En Arcler Press (Eds), Cyber Security (pp. 117-139). Canadá: Arcler Press. https://eds-s-ebscohost-com.bibliotecavirtual.unad.edu.co/eds/ebookviewer/ebook?sid=74ed1b82-395e-4e33-9ab1-c7b780f3f849%40redis&ppid=pp_Cover&vid=0&format=EB