Reuniendo información Personal usando Online People Search Services

Online People Search Services ofrece información en tiempo real sobre una persona, estas herramientas ayudan a descubrir información sobre las personas.

Escenario del Laboratorio:

Durante la reunión de la información, necesitas reunir información de los empleados que trabajan en posiciones críticas en la organización de la víctima, como los administradores de la red., Recepcionistas, etc. La información recolectada puede ser de mucha ayuda. En este laboratorio vamos a demostrar como puedes realizar tus propias búsquedas de información personal usando online people search services.

Objetivos de Laboratorio

Los objetivos de este laboratorio es reunir información persoal usando **whitepages**, una utilidad que puede ser encontrada en https://www.whitepages.com

Desarrollo del Laboratorio:

En este laboratorio necesitas:

Un buscador web con conección a internet

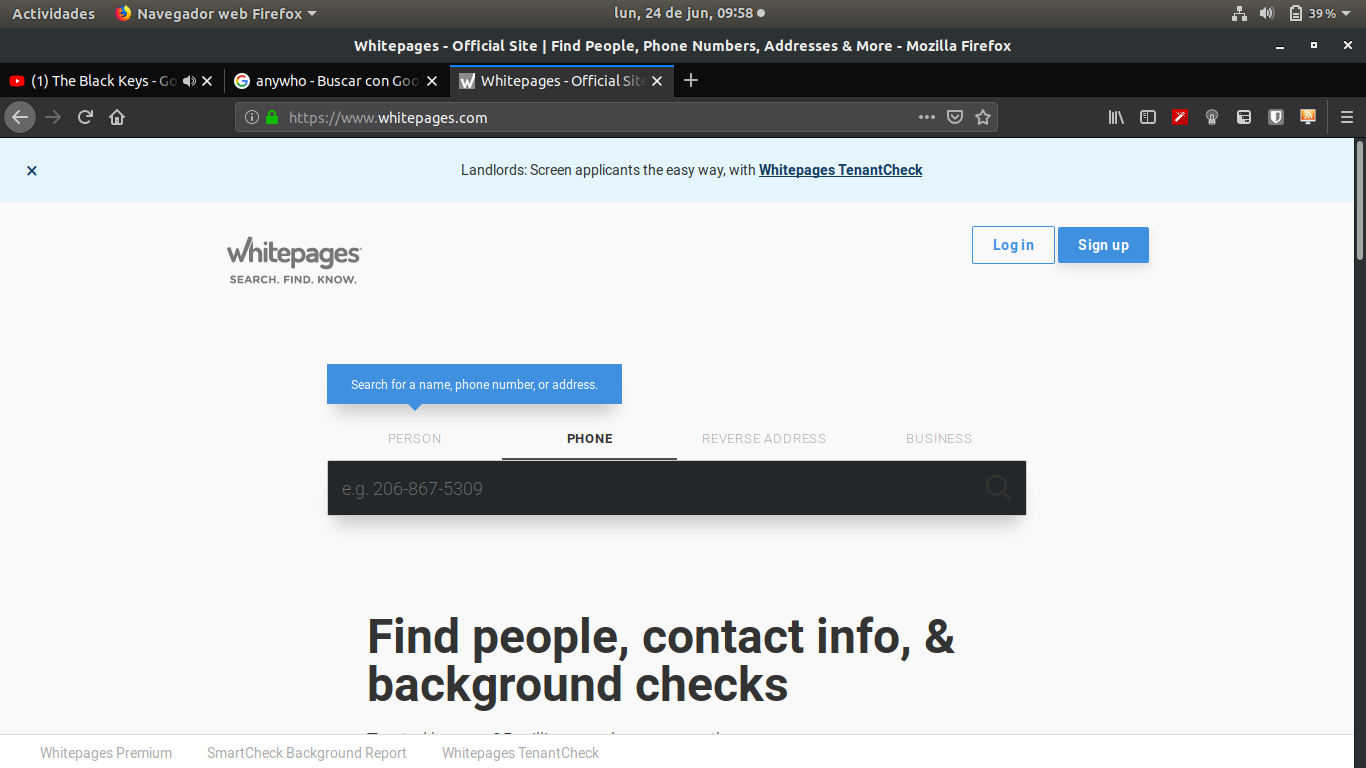
Privilegios de administrador en las herramientas que se están ejecutando.

Windows Server 2012

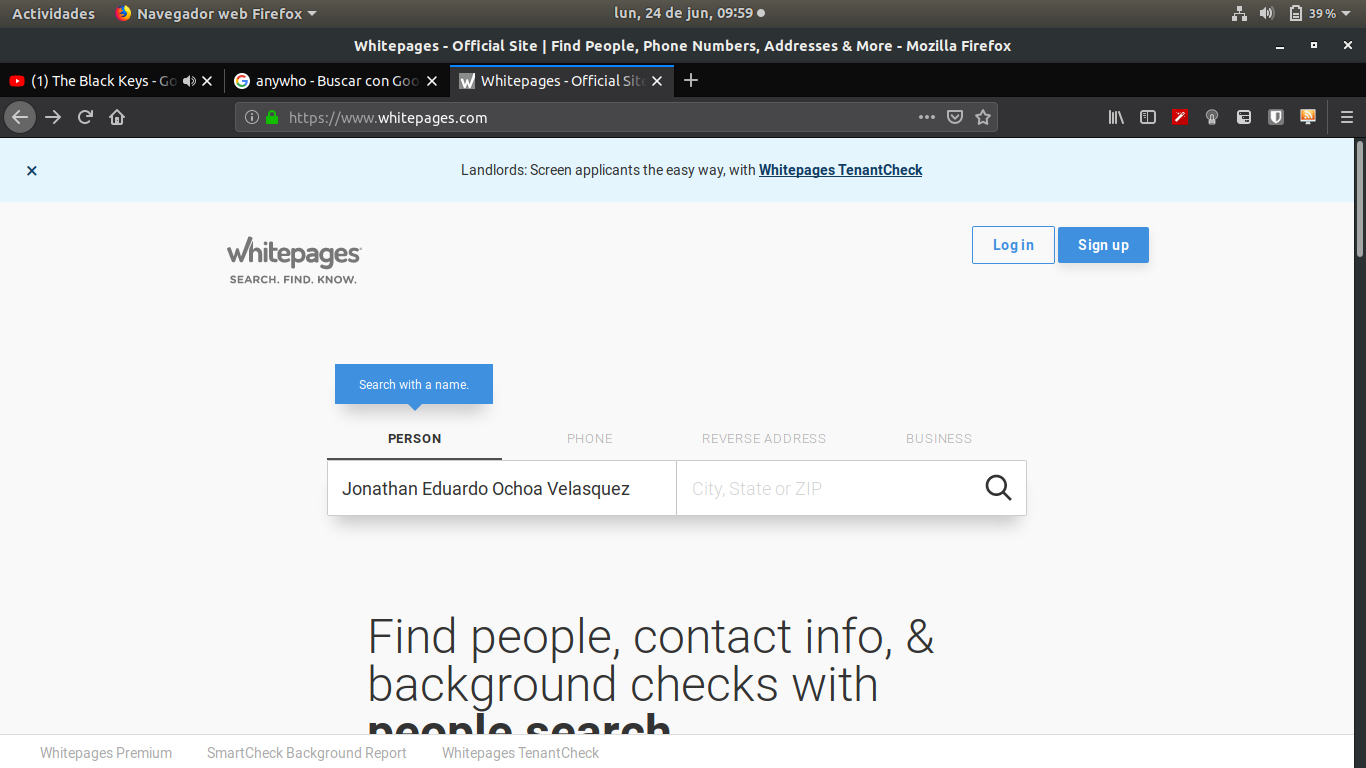
Tareas del Laboratorio:

5. Abre un navegador e ingresa a la página de **whitepages.**

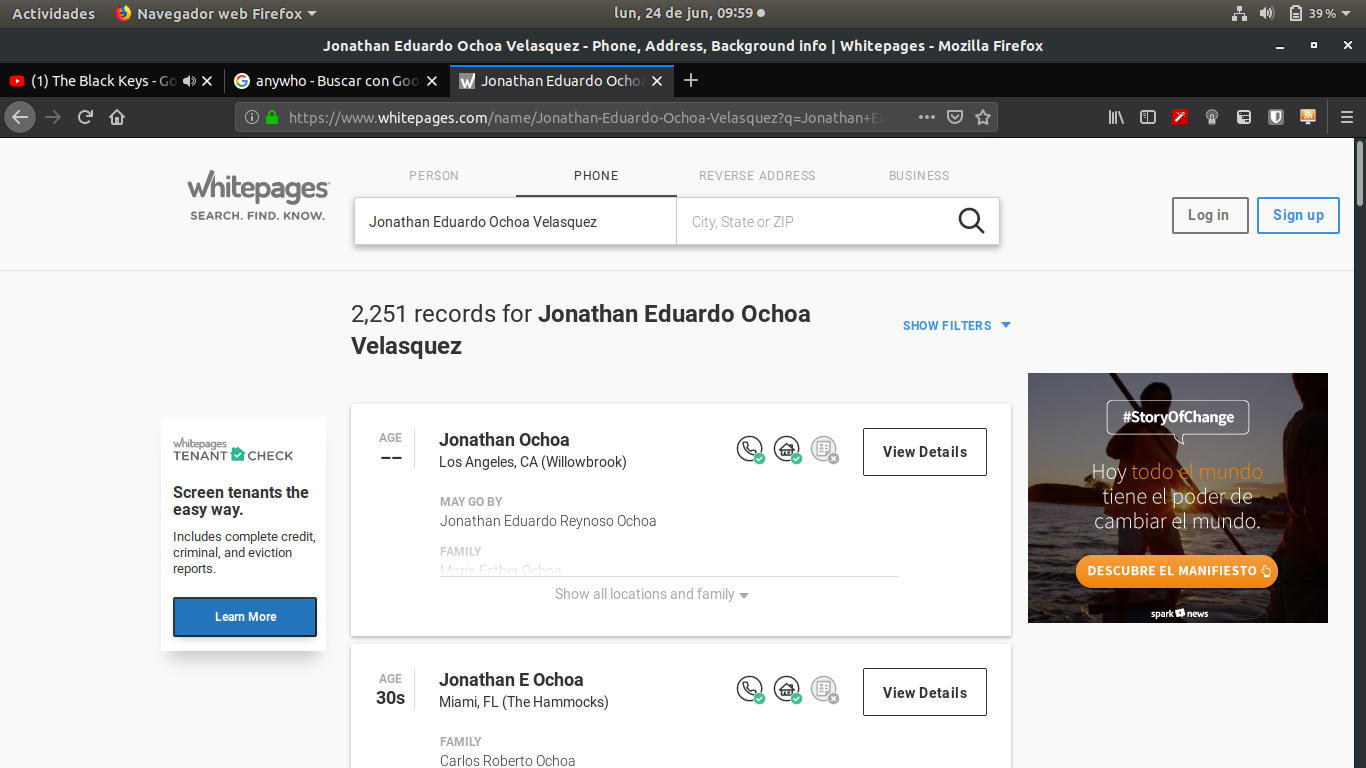
6. La página de whitepages aparecerá, como se muestra en la captura.



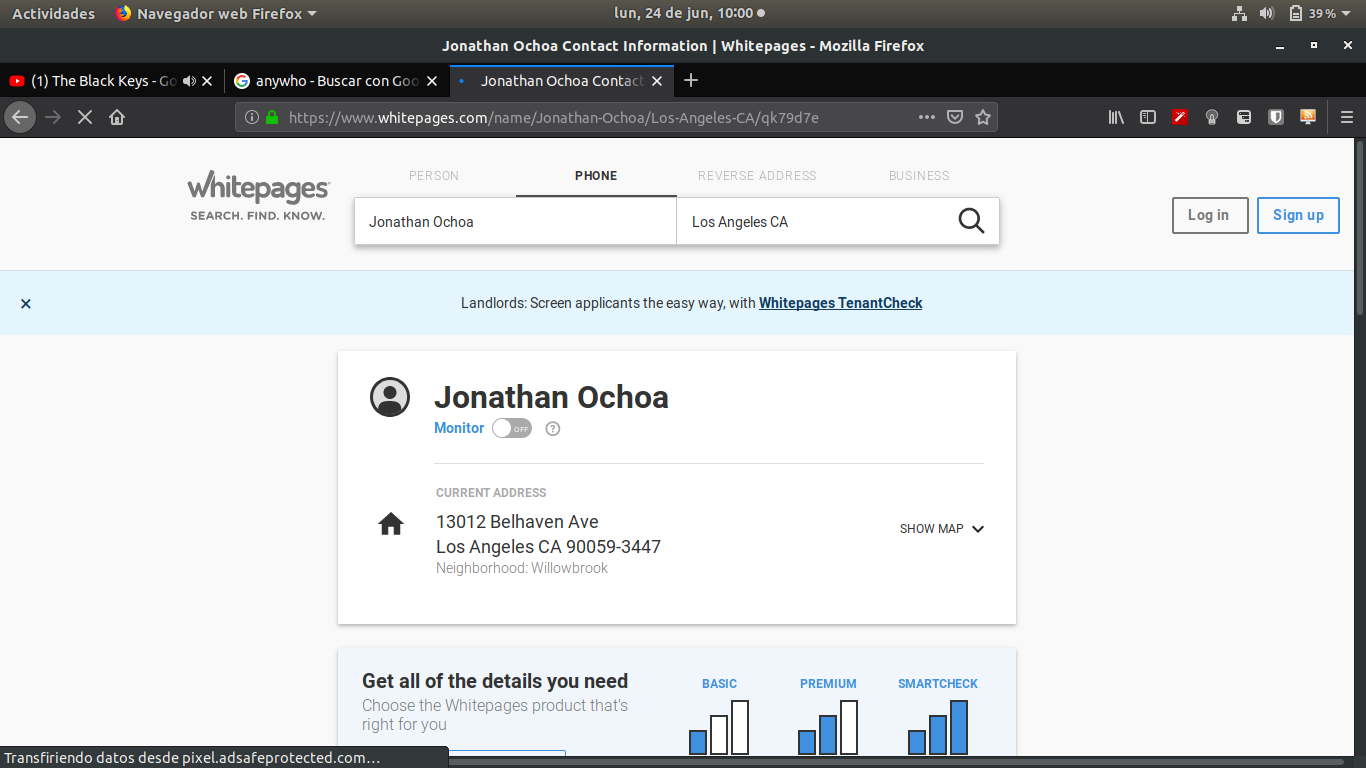
7. Para empezar la búsqueda ingresa los detalles de la persona que deseas buscar, por nombre, correo, usuario o teléfono, da click en el botón de buscar.



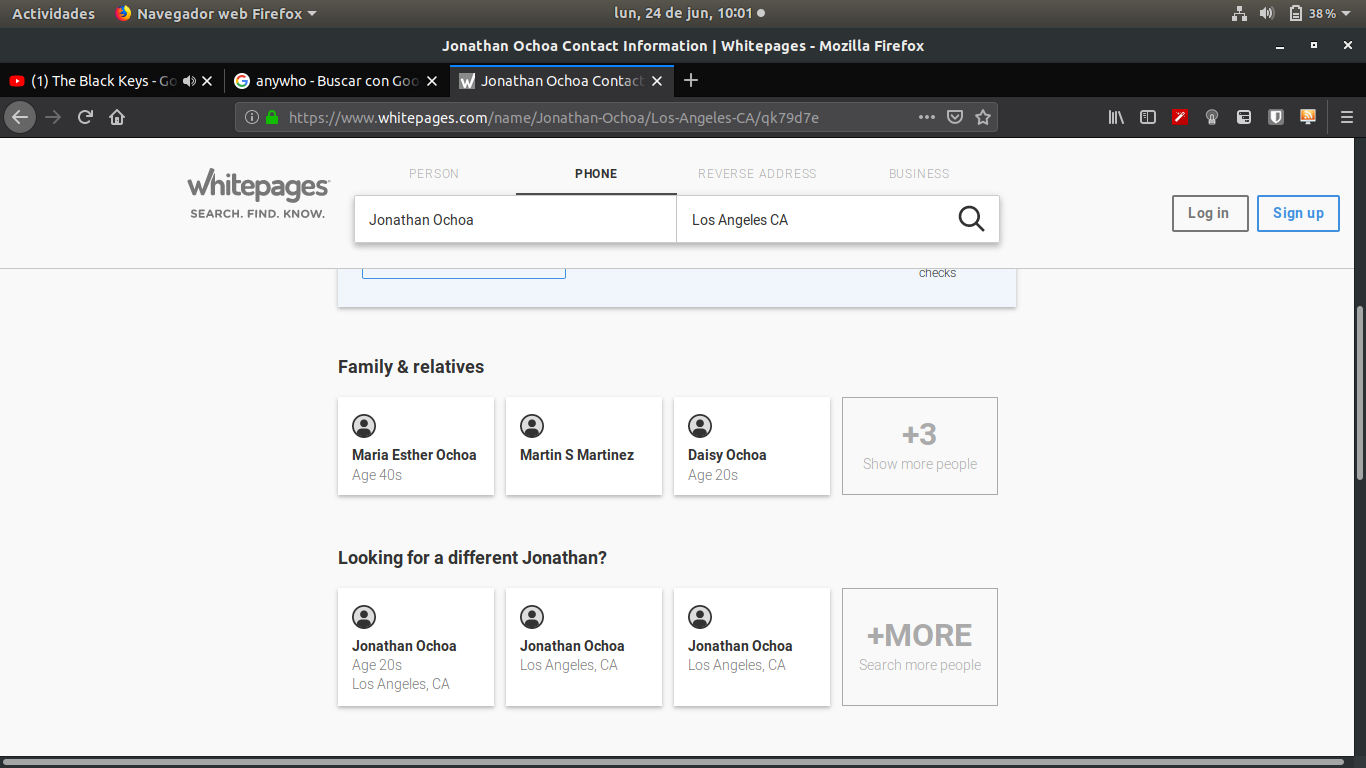
8. whitepages retornará los resultados con el nombre que has introducido.

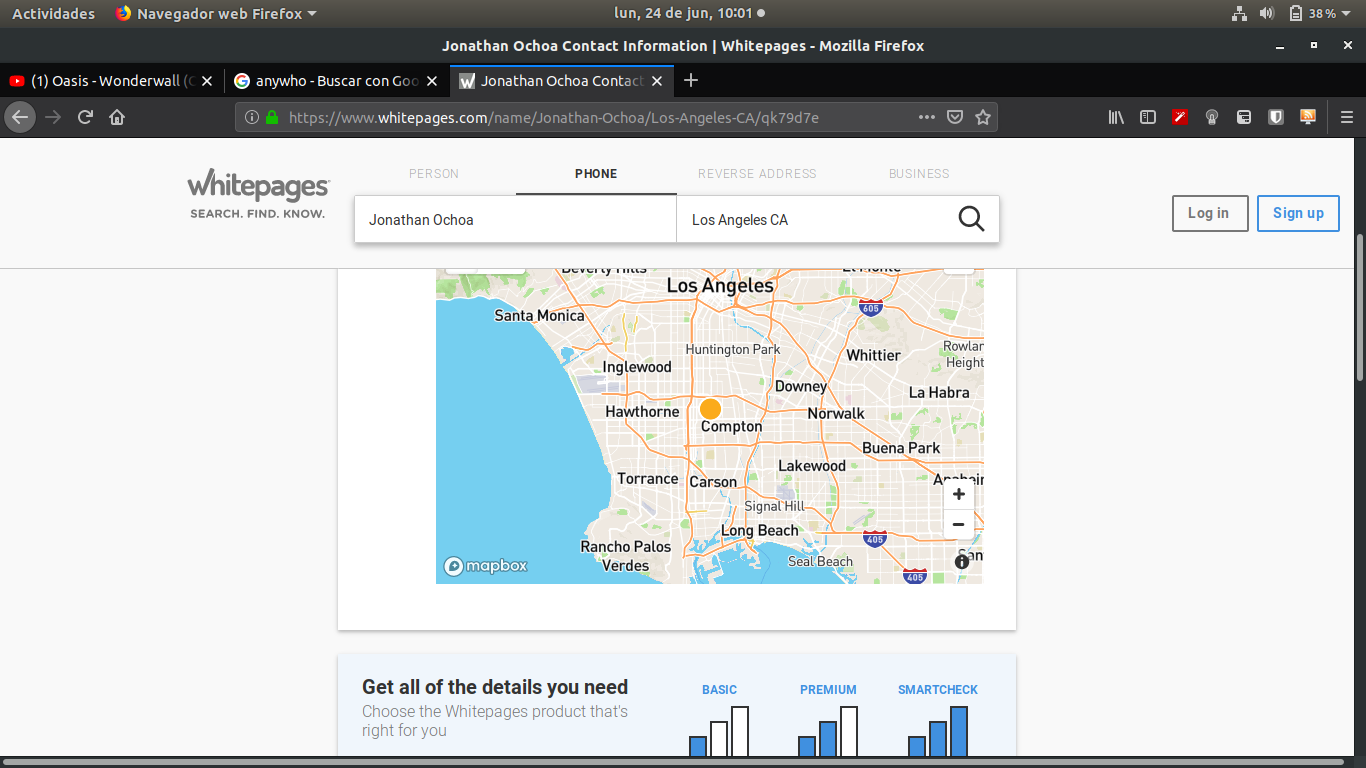


9. Da click en cualquiera de los links para ver más información.



10. whitepages muestra la información completa como se muestra en la siguiente captura.





**Extracción de Información de Compañias usando un Web Data Extractor.**

Escenario del laboratorio:

En los procesos de la obtención de información, tu siguiente tarea será extraer información del sitio web de una organización.

Objetivos del laboratorio:

Los objetivos de este laboratorio son demostrar como se extrae información de una compañía usando un Web Data Extractor.

Desarrollo del laboratorio:

Para llevar a cabo este laboratorio necesitas:

* Web Data Extractor que puede ser adquirido de D:\CEH-Tools\CEHv9 Module 2 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor. También puedes descargar la versión más reciente de su página oficial.
* Windows Server 2012

Tareas de Laboratorio:

1. Ejecutar el programa.

2. Sigue los pasos para su correcta instalación.

3. Abre la aplicación.

4. Da click en New para empezar una nueva sesión.

5. Click en new para abrir los ajustes de sesión.

6. Escribe la URL [**http://www.certifiedhacker.com**](http://www.certifiedhacker.com/)in el campo de URL y chequea todas las opciones que se muestran, da click en OK.

7. Click en Start para empezar la Extracción de datos.

8. Web Data Extractor empezará a recolectar la información (telefonos, correos, etc).

9. Una vez que los datos son extraidos, aparecerá una caja de diálogo, da click en OK.

10. Puedes ver la información extraida.

11 Selecciona Meta Tags para ver la URI, host, dominio, etc.

12. Selecciona la fila de emails para ver las direcciones de correo, nombre, URI, host y toda la información relacionada a los emails.

13. Selecciona la fila de Phones para ver todo lo relacionado con Teléfonos.

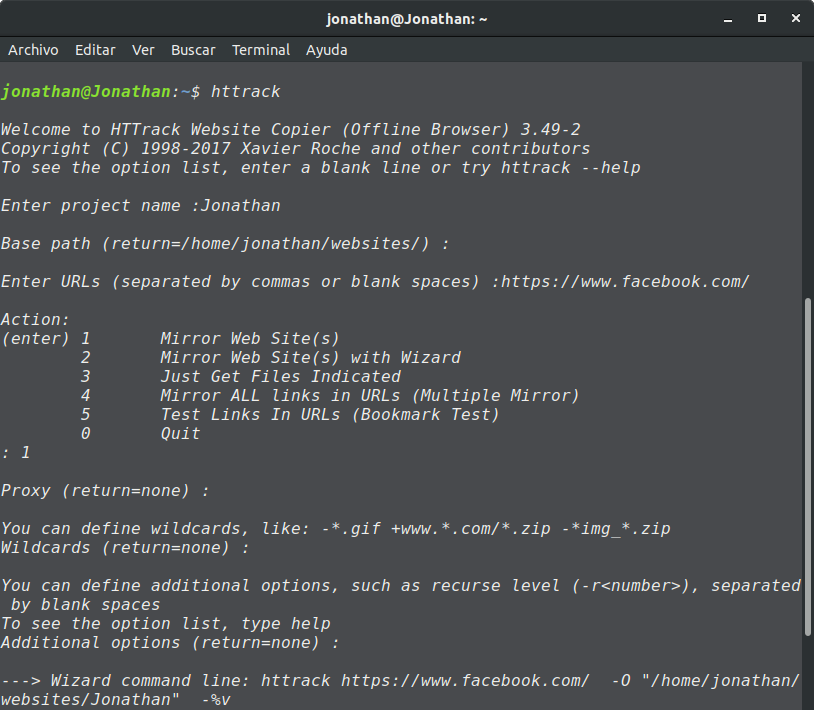
14. Para guardar, escoge File y da click en Save Session.

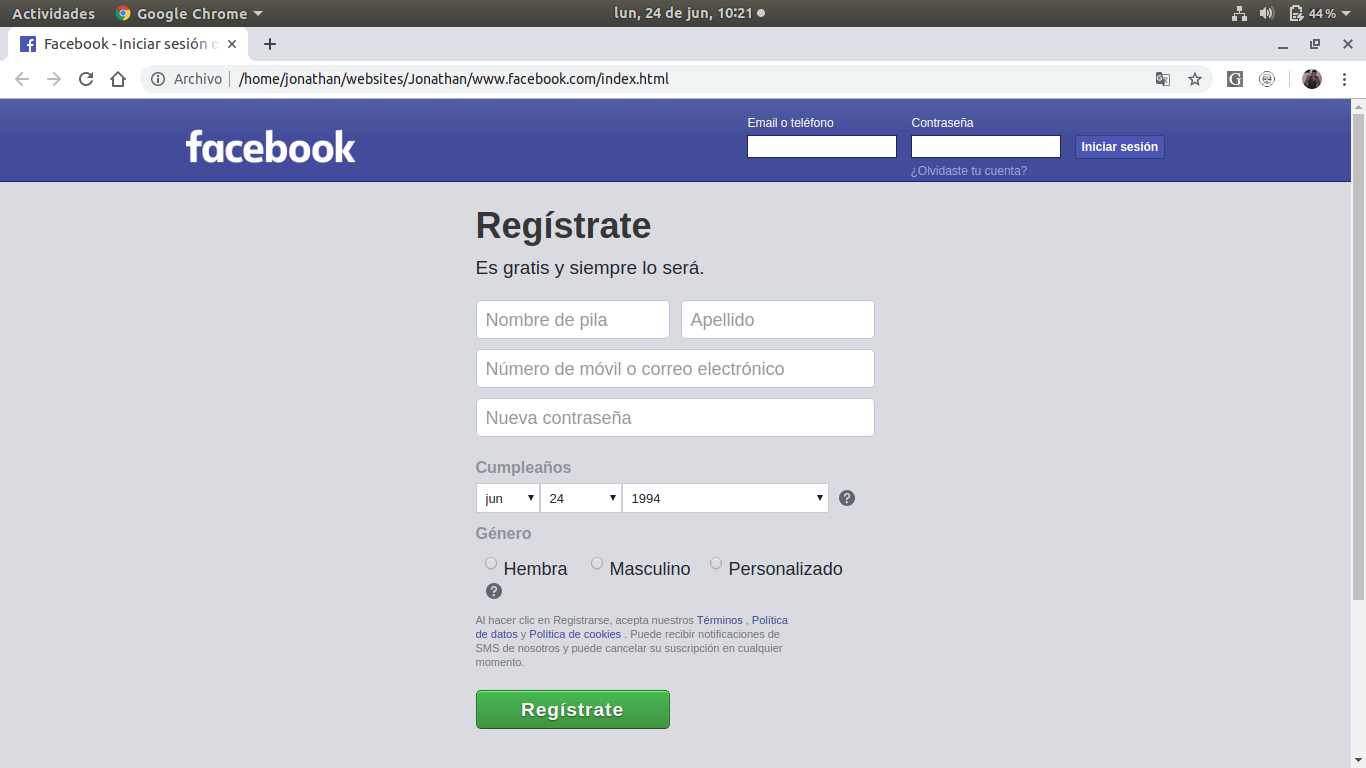
**Reflejando un sitio web usando HTTrack**

**Copiador se sitios web.**

Objetivos del laboratorio:

Los objetivos de este laboratorio son que los estudiantes aprendar a copiar sitios web usando HTTrack.

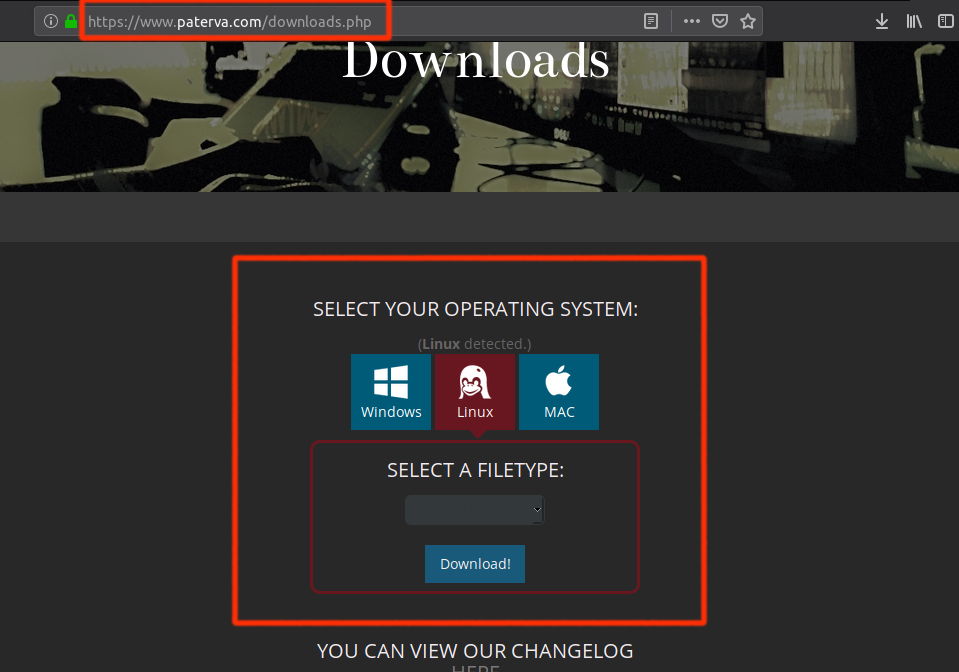




Recolección de información utilizando Maltego:

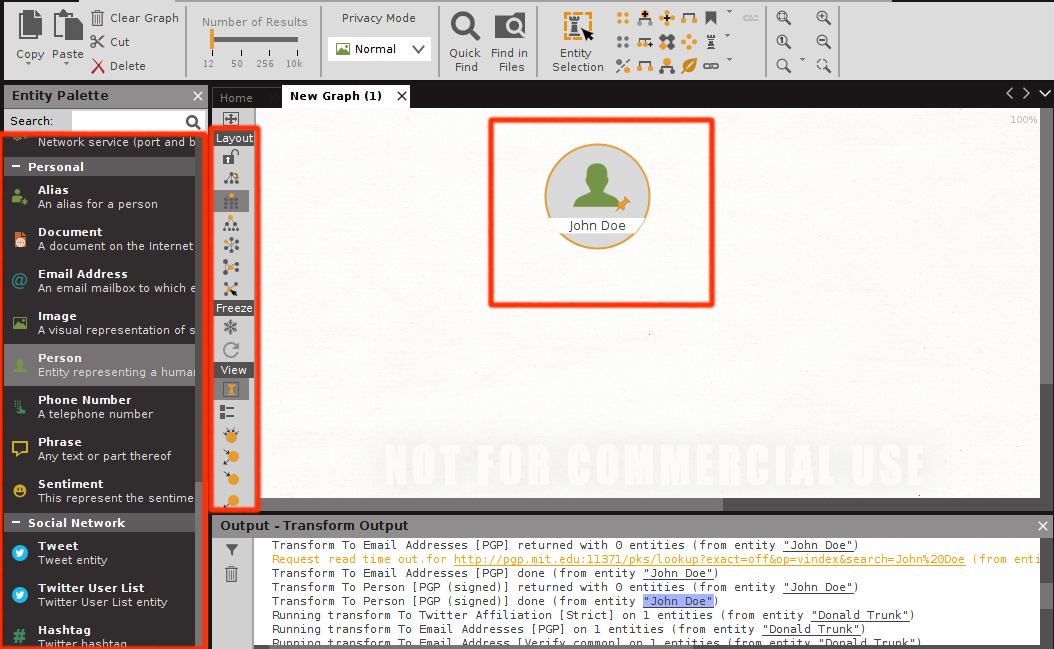
Maltego, es un servicio que tiene el potencial de encontrar información sobre personas y empresas en Internet, permitiendo cruzar datos para obtener perfiles en redes sociales, servidores de correo, etc.

Para usar Maltego es necesario instalarlo y registrarse en su página web, creando una cuenta que nos va a permitir usar la aplicación junto con sus servidores gratuitos.



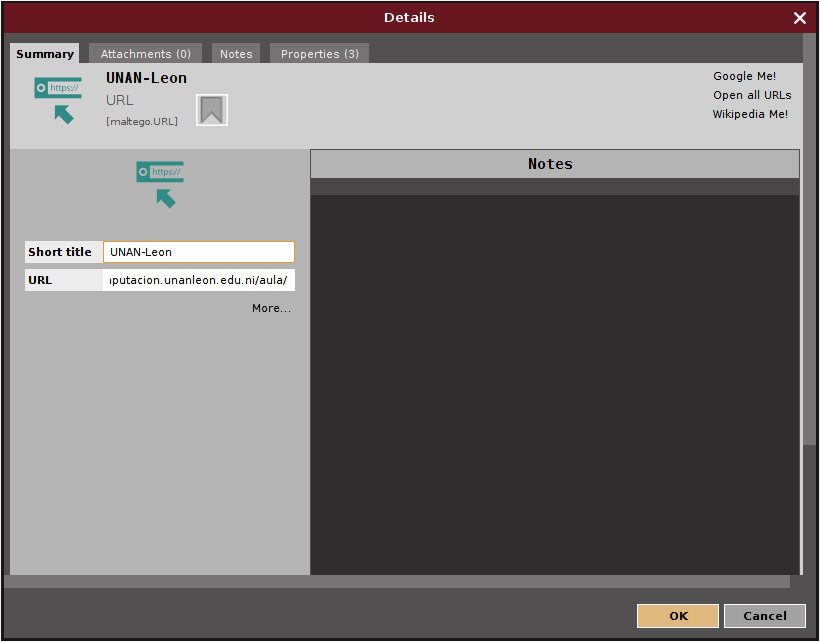
La captura nos muestra la página web donde podemos realizar la descarga de Maltego para los diferentes SO existentes en el mercado.

Una vez realizada la instalación e iniciada la sesión, deberemos crear una hoja de búsqueda nueva y arrastrar la entidad (es el tipo de búsqueda que queremos hacer, en este caso una persona), para luego hacer la búsqueda y ver qué resultados arroja.

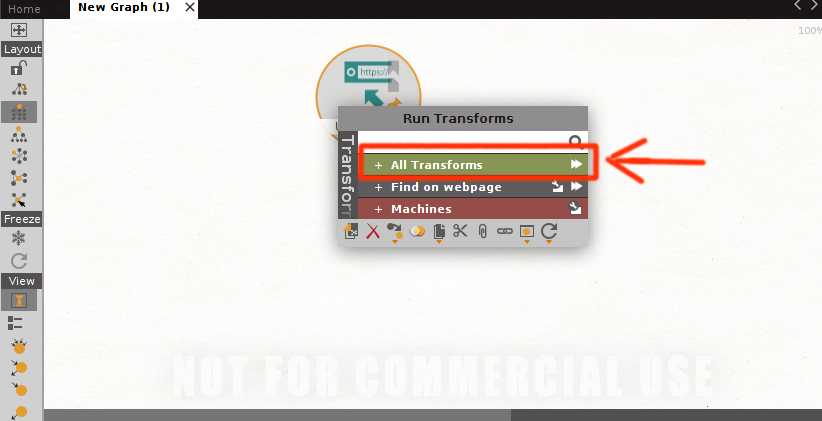


En la parte izquierda podemos ver los tipos de búsqueda que podemos hacer (personas, organizaciones, URL, etc), a la par de este menú se encuentra un layout donde podemos decir la jerarquía en que se va a mostrar la búsqueda y más a la derecha tenemos la ventana donde se cargarán los resultados.

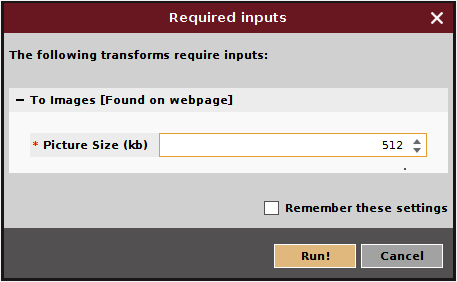
Una vez seleccionado el tipo de búsqueda a realizar, daremos doble clic sobre el icono de la url para acceder a la configuración y, una vez configurada la url a buscar.



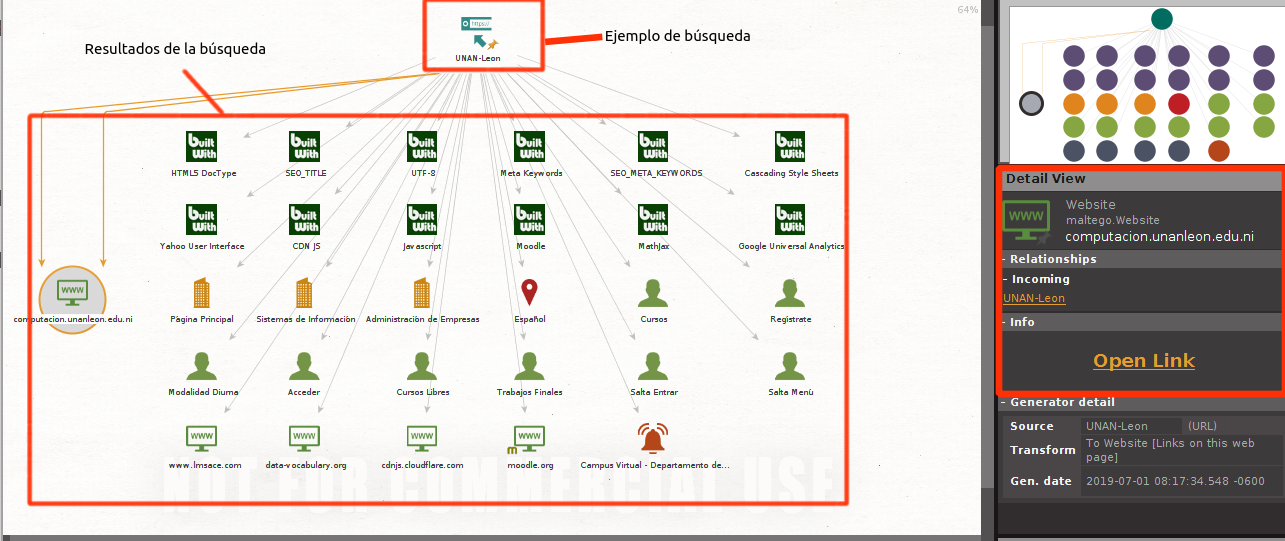
Por último solo queda dar clic derecho en el icono de la entidad seleccionada y seleccionar la opción que queramos buscar, en mi caso quiero buscar todo lo relacionado a este url, por lo tanto elegiré la opcion **All Transforms.**



Luego de dar clic nos aparecerá una pequeña ventana donde nos pide que indiquemos la calidad con la que se mostrarán las imágenes obtenidas de la búsqueda, en mi caso escogeré 512.

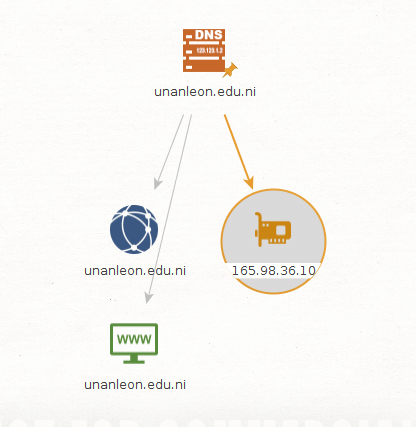


Damos clic en Run.

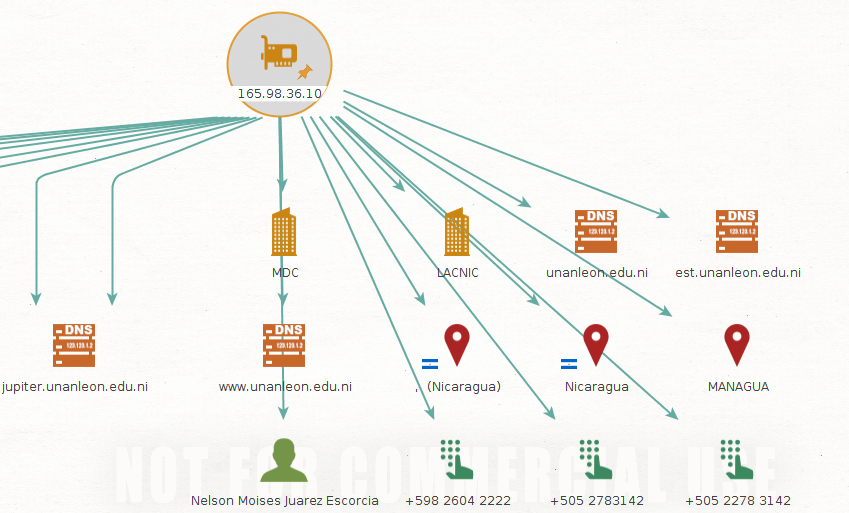


En la captura podemos ver los resultados que obtuvimos, en los que se encuentran: los servicios que ofrece el sitio web, como está estructurado, de que otros servicios hace uso (en este caso, el aula virtual de la UNAN-León hace uso de Edmodo), se ven sitios donde se hace mención o donde hay información relacionada a la url que introducimos. Si damos clic en uno de los íconos de la vista obtenida, por ejemplo en el ícono que dice **computacion.unanleon.edu.ni**, a la parte derecha obtenemos información específica de ese elemento seleccionado.

En este caso solo mostramos cómo buscar información de una url, pero con esta poderosa herramienta, pero también se pueden hacer búsquedas de dominios, direcciones de correo electrónico, números telefónicos, servidores DNS, entre otros datos.



Podemos usar la ip del resultado obtenido de la captura antenior para obtener más información:



En esta caso pudimos obtener información muy detallada de la ip de UNAN-LEÓN como es: ubicación, servidor DNS, información de LACNIC (El Registro de Direcciones de Internet de América Latina y Caribe).