

CURSO *ONLINE* DE CIBERSEGURIDAD__

Taller 2

Unidad 2. Aspectos básicos de ciberseguridad



VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

 **incibe**
INSTITUTO NACIONAL DE CIBERSEGURIDAD



Contenidos

1	EL USO DE HERRAMIENTAS DE RECONOCIMIENTO OSINT	3
2	INSTALACIÓN Y CONFIGURACIÓN DE THEHARVESTER	5
3	ENUNCIADO EJERCICIO PRÁCTICO 1	10
4	SOLUCIÓN EJERCICIO PRÁCTICO 1	12
5	MALTEGO	16

Duración total del taller: 1 hora.

EL USO DE HERRAMIENTAS DE RECONOCIMIENTO OSINT

1



EL USO DE HERRAMIENTAS DE RECONOCIMIENTO OSINT

A través de este ejercicio, vas a comprender cómo recopilar información de diferentes fuentes públicas, como correos electrónicos, subdominios, *hosts*, puertos abiertos, etc., a través del uso de TheHarvester.

Primero vamos a conocer el concepto de OSINT y qué utilidad tiene. OSINT (del inglés *Open Source INTelligence* o Inteligencia de código abierto) hace referencia a una serie de técnicas y/o procesos que permiten la recopilación de información de fuentes públicas, con el objetivo de analizar dicha información y darle una utilidad, es decir, es un conjunto de herramientas y actividades que permiten recopilar información, analizar los datos recopilados, correlacionarlos y darles utilidad.

Se puede recopilar información muy valiosa de diferentes fuentes. Imagina la cantidad de datos que un usuario genera en Internet, en blogs, foros, noticias, y sobre todo, en redes sociales.

Por ello, con esta práctica vas a aprender a utilizar alguna de las herramientas OSINT más conocidas y utilizadas.

INSTALACIÓN Y CONFIGURACIÓN DE THEHARVESTER

2



2 INSTALACIÓN Y CONFIGURACIÓN DE THEHARVESTER

TheHarvester es una de las principales herramientas OSINT dentro de la *suite* Kali Linux y ya viene instalada por defecto en este SO, por lo que no es necesario realizar ninguna acción de instalación para poder trabajar con ella.

- Dentro de la máquina virtual de Kali Linux, abre una terminal de comandos. Es importante que sepas que a la terminal de comandos también se la conoce como «terminal», «*Shell*» «consola de comandos» o, simplemente, «consola».
- Ejecuta theHarvester. Para ello, basta con que en la terminal escribas el comando «**theHarvester**». Para ver todas las opciones que ofrece TheHarvester ejecuta el comando «**theHarvester-h**».

2 INSTALACIÓN Y CONFIGURACIÓN DE THEHARVESTER

```
(incibe@kali)-[~]
$ theHarvester -h

*****
*
*  THE HARVESTER  *
*
* theHarvester 4.0.3
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-g] [-p] [-s] [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-t DNS_TLD] [-r] [-n] [-c] [-f FILENAME] [-b SOURCE]

theHarvester is used to gather open source intelligence (OSINT) on a company or domain.

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Company name or domain to search.
  -l LIMIT, --limit LIMIT
                        Limit the number of search results, default=500.
  -S START, --start START
                        Start with result number X, default=0.
  -g, --google-dork      Use Google Dorks for Google search.
  -p, --proxies          Use proxies for requests, enter proxies in proxies.yaml.
  -s, --shodan          Use Shodan to query discovered hosts.
  --screenshot SCREENSHOT
                        Take screenshots of resolved domains specify output directory: --screenshot output_directory
  -v, --virtual-host     Verify host name via DNS resolution and search for virtual hosts.
  -e DNS_SERVER, --dns-server DNS_SERVER
                        DNS server to use for lookup.
  -t DNS_TLD, --dns-tld DNS_TLD
                        Perform a DNS TLD expansion discovery, default False.
  -r, --take-over        Check for takeovers.
  -n, --dns-lookup       Enable DNS server lookup, default False.
  -c, --dns-brute        Perform a DNS brute force on the domain.
  -f FILENAME, --filename FILENAME
                        Save the results to an XML and JSON file.
  -b SOURCE, --source SOURCE
                        anubis, baidu, bing, binaryedge, bingapi, bufferoverrun, censys, certspotter, crtsh, dnsdumpster, duckduckgo, fullhunt, github-code, google, hackertarget, hunter, intelx, linkedin, linkedin_links, n45ht,
                        omniscint, otx, pentesttools, projectdiscovery, qwant, rapiddns, rocketreach, securityTrails, spyse, sublist3r, threatcrowd, threatminer, trello, twitter, urlscan, virustotal, yahoo, zoomeye
```

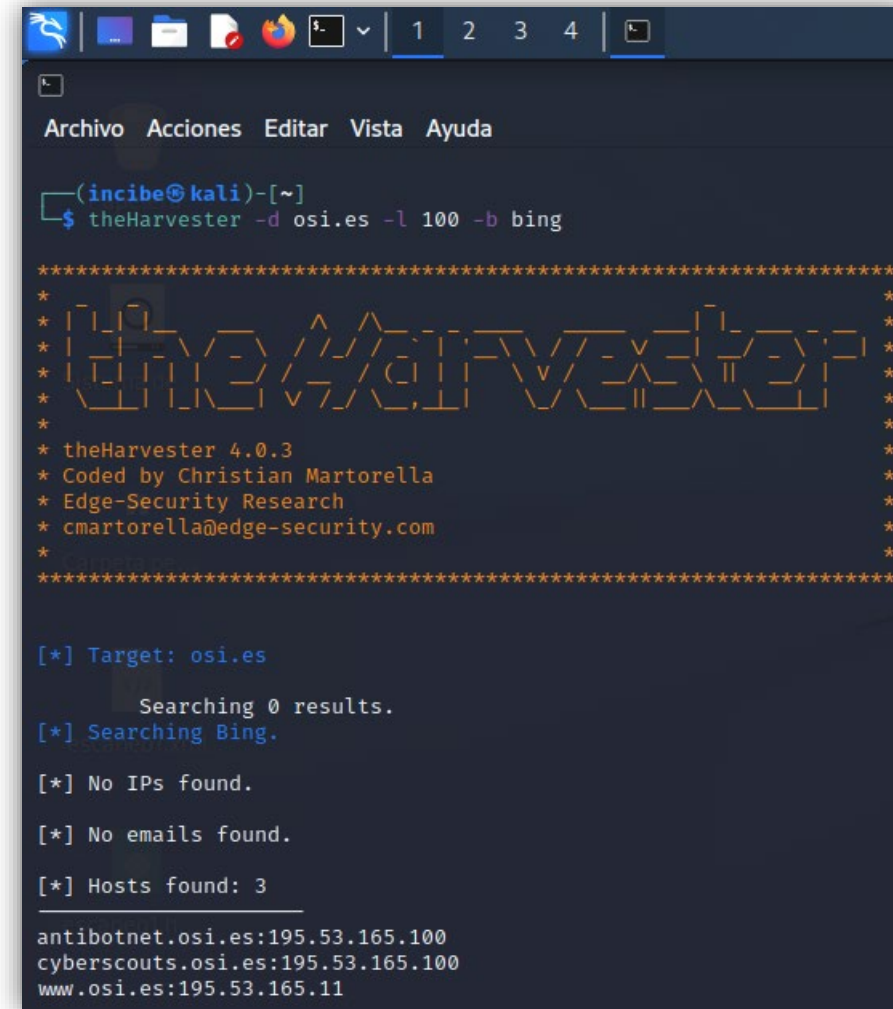
Ilustración 1: Escribir el comando « theHarvester » en la terminal.

2 INSTALACIÓN Y CONFIGURACIÓN DE THEHARVESTER

- Puedes visualizar los principales comandos:
 - **-d**: dominio objetivo sobre el que se quiere realizar el análisis. Por ejemplo, `osi.es`.
 - **-l**: límite para evitar que la búsqueda colapse. Se puede limitar a un número determinado de resultados, por ejemplo, al límite `-l 100`.
 - **-f**: archivo. Si se quiere exportar los resultados a un archivo, los formatos más habituales son `.xml` o `.json`, por ejemplo, `-f resultados.xml`.
 - **-b**: fuente. Se pueden especificar uno o varios motores de búsqueda con los que se realizará el análisis. Por ejemplo, `-b bing`.

2 INSTALACIÓN Y CONFIGURACIÓN DE THEHARVESTER

- ¿Cómo se escanean los 100 primeros resultados del dominio `osi.es` en Bing? Para ello, ejecuta el comando «**theHarvester -d osi.es -l 100 -b bing**».



```
(incibe@kali)-[~]
$ theHarvester -d osi.es -l 100 -b bing

*****
*                                     *
* theHarvester 4.0.3                  *
* Coded by Christian Martorella       *
* Edge-Security Research             *
* cmartorella@edge-security.com      *
*                                     *
*****

[*] Target: osi.es

    Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

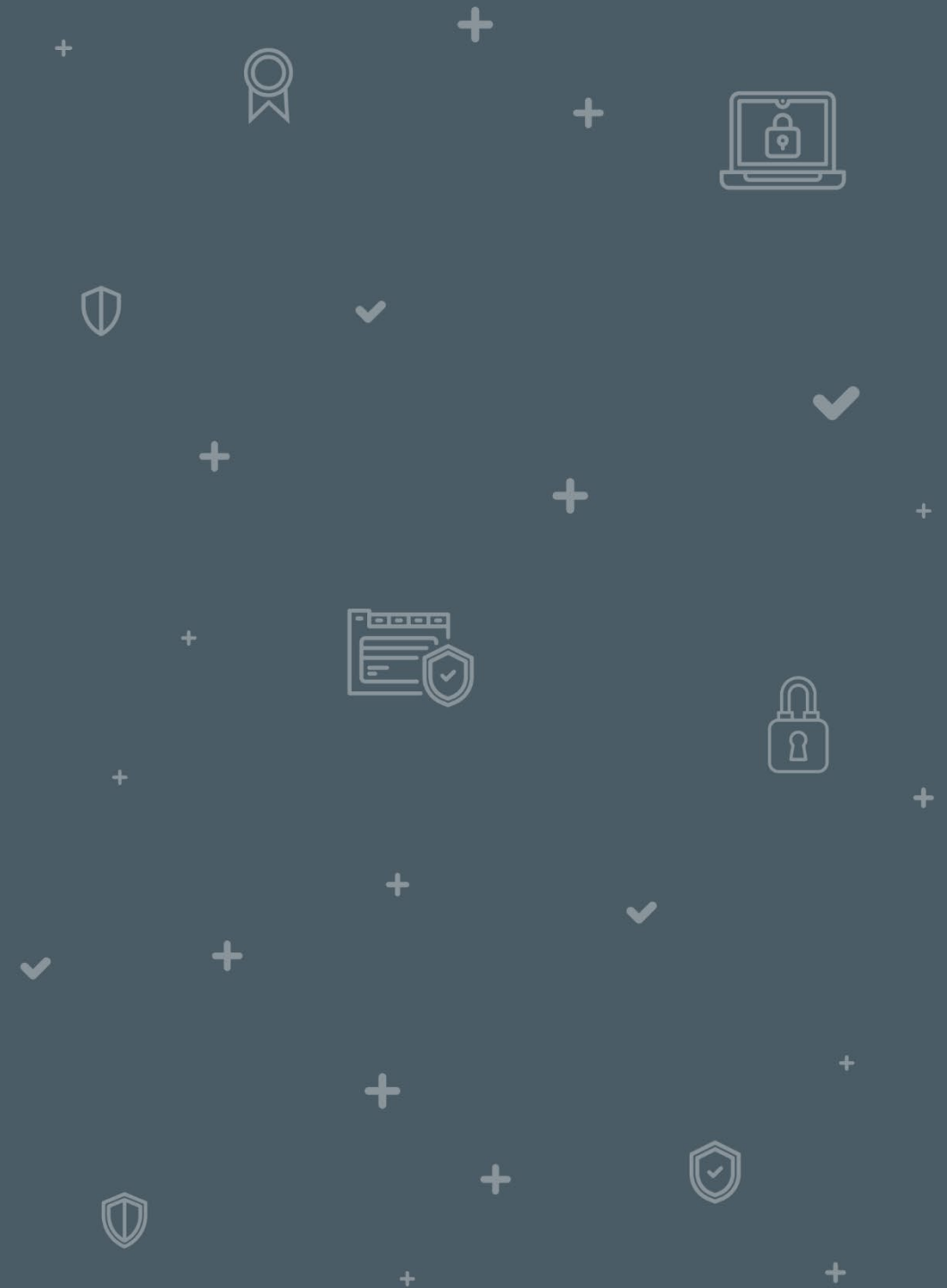
[*] No emails found.

[*] Hosts found: 3
-----
antibotnet.osi.es:195.53.165.100
cyberscouts.osi.es:195.53.165.100
www.osi.es:195.53.165.11
```

Ilustración 2: Ejecuta el comando «theHarvester -d osi.es -l 100 -b bing».

ENUNCIADO EJERCICIO PRÁCTICO 1

3



ENUNCIADO EJERCICIO PRÁCTICO 1

Realiza un análisis de los 100 primeros resultados del dominio incibe.es en Google mediante el uso de la herramienta OSINT.

SOLUCIÓN EJERCICIO PRÁCTICO 1

4



4 SOLUCIÓN EJERCICIO PRÁCTICO 1

- Realiza un análisis de los 100 primeros resultados del dominio incibe.es en Google mediante el uso de la herramienta OSINT.
- Ejecuta el comando «**theHarvester -d incibe.es -l 100 -b Google**».

```
(incibe@kali)-[~]
$ theHarvester -d incibe.es -l 100 -b google

*****
*                                     *
*  theHarvester                      *
*  theHarvester 4.0.3                *
*  Coded by Christian Martorella     *
*  Edge-Security Research            *
*  cmartorella@edge-security.com     *
*                                     *
*****

[*] Target: incibe.es

[*] Searching 0 results.
[*] Searching 100 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 6
-----
espaciosciberseguridad@incibe.es
espacioscs_profesores@incibe.es
info@incibe.es
jornadas.pyme@incibe.es
talento.ciberseguridad@incibe.es
x22talento.ciberseguridad@incibe.es

[*] Hosts found: 3
-----
estudioherramientas.incibe.es
www.incibe.es:195.53.165.153
x22www.incibe.es
```

Ilustración 3: Ejecuta el comando «theHarvester -d incibe.es -l 100 -b Google».

4 SOLUCIÓN EJERCICIO PRÁCTICO 1

- En la siguiente imagen podemos ver los mismos resultados en un fichero XML. Los resultados que te aparezcan a ti podrán ser diferentes a los que se muestran aquí.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
--<theHarvester>
  <email>espaciosciberseguridad@incibe.es</email>
  <email>espacioscs_profesores@incibe.es</email>
  <email>info@incibe.es</email>
  <email>talento.ciberseguridad@incibe.es</email>
  <email>x22talento.ciberseguridad@incibe.es</email>
  <host>estudioherramientas.incibe.es</host>
--<host>
  <ip>195.53.165.153</ip>
  <hostname>www.incibe.es</hostname>
</host>
<host>x22www.incibe.es</host>
</theHarvester>
```

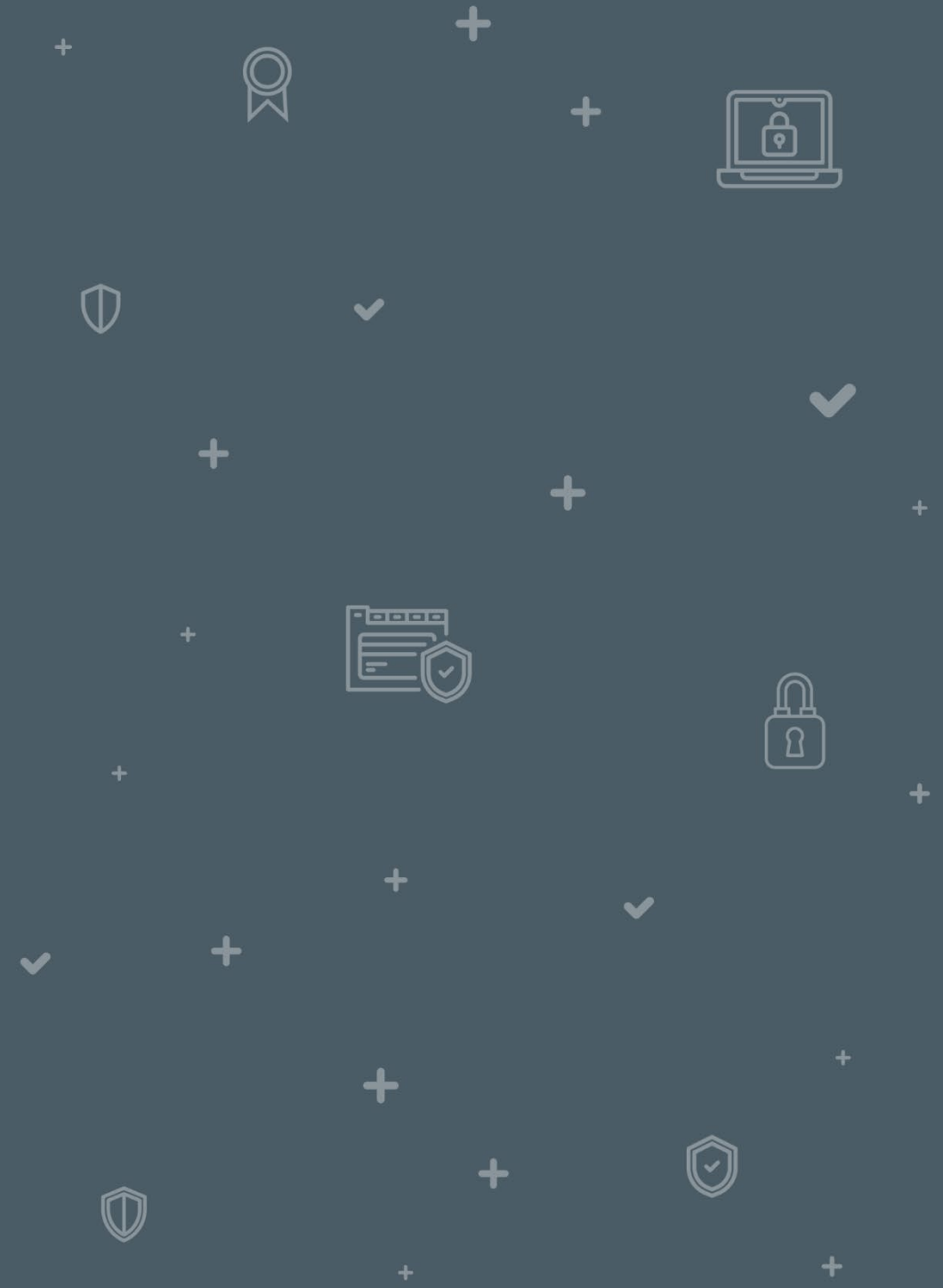
Ilustración 4: Imagen de los resultados del ejercicio mostrados en fichero XML.

SOLUCIÓN EJERCICIO PRÁCTICO 1

- Con los resultados, observa que se han encontrado 6 correos electrónicos y 3 *host* (son los nombres de dominio) de los cuales, uno de ellos, tiene información acerca de la dirección IP pública. El uso de herramientas OSINT es de gran utilidad en la fase 1 de reconocimiento del ciclo de vida de un ciberataque, guardando relación con el *footprinting*. Las cuentas de correo electrónico encontradas pueden utilizarse para realizar ataques de *phishing*, la relación con otros dominios se puede emplear debido a que, en ocasiones, los administradores olvidan actualizar estos dominios secundarios o, si se encuentran formularios, se pueden utilizar para realizar ataques XSS, entre otros. Por ello, conocer el funcionamiento de técnicas y herramientas OSINT resulta tan útil.

MALTEGO

5



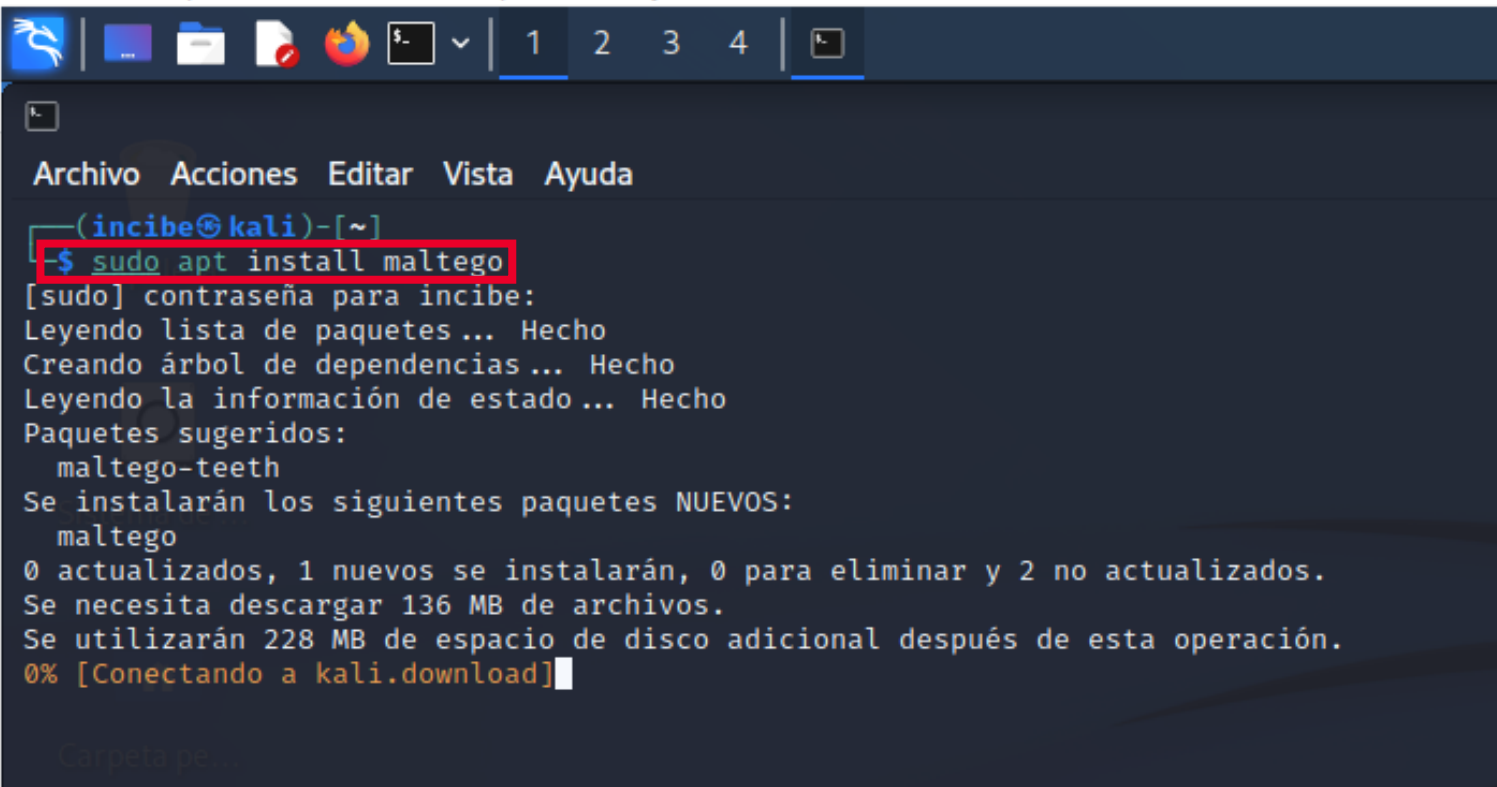
5 MALTEGO

Ahora, vas a aprender a recopilar información de diferentes fuentes públicas, como correos electrónicos, subdominios, *hosts*, puertos abiertos, etc., a través del uso de herramientas de reconocimiento OSINT. En este caso, Maltego, una de las herramientas OSINT más usadas, nos permite ver de manera gráfica y ordenada nuestro descubrimiento de datos y fuentes y analizar las relaciones entre diferentes equipos, personas, dominios, correo, etc.

5 MALTEGO

Instalación y configuración

- Abre un nuevo terminal en la máquina Kali Linux. Una vez hecho esto, ejecuta el siguiente comando: **sudo apt install maltego**.
- Deberás introducir tu contraseña pues la ejecución de este comando requiere de permisos de superusuario.



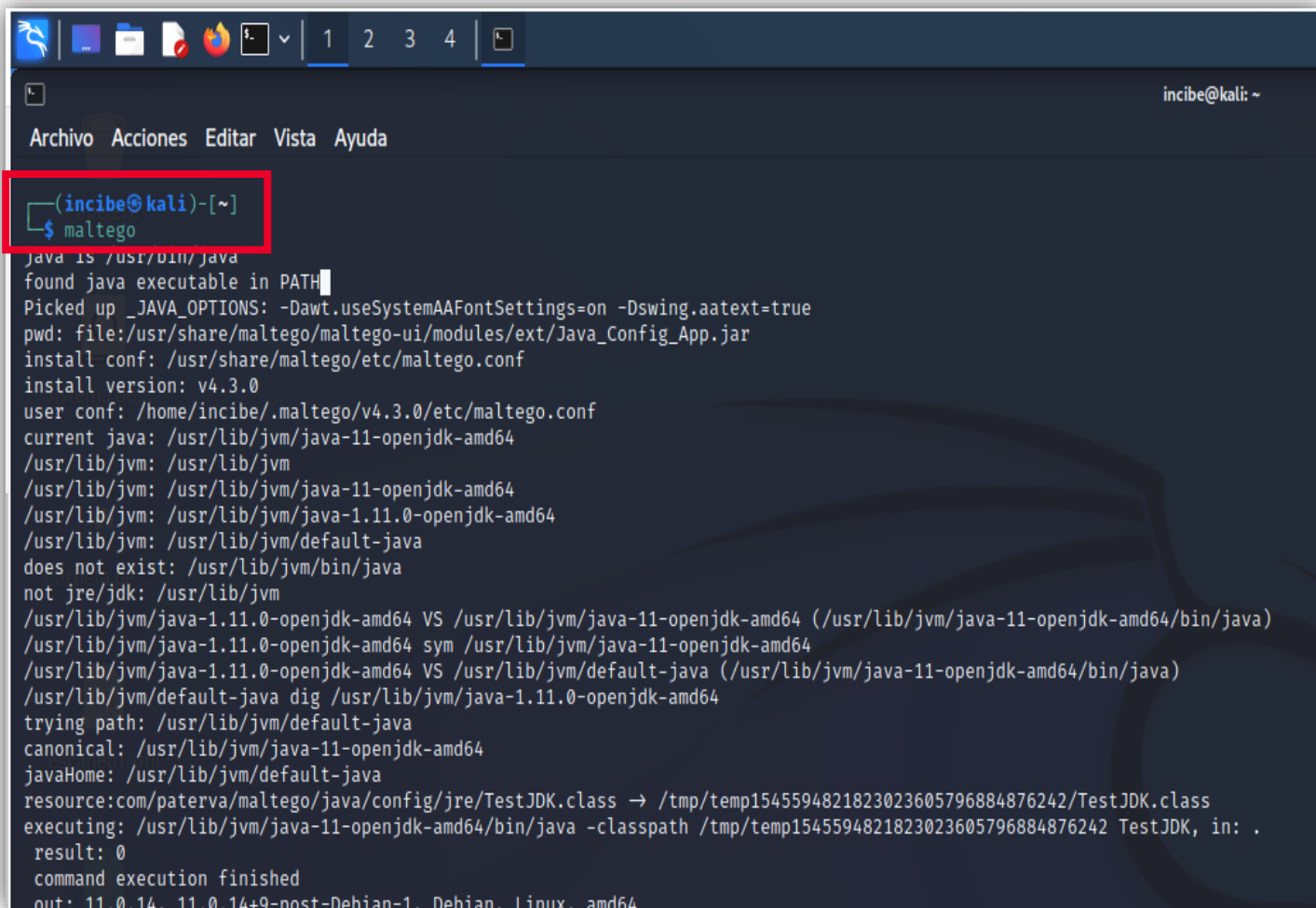
```
Archivo Acciones Editar Vista Ayuda
(incibe@kali)-[~]
$ sudo apt install maltego
[sudo] contraseña para incibe:
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias ... Hecho
Leyendo la información de estado ... Hecho
Paquetes sugeridos:
  maltego-teeth
Se instalarán los siguientes paquetes NUEVOS:
  maltego
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 2 no actualizados.
Se necesita descargar 136 MB de archivos.
Se utilizarán 228 MB de espacio de disco adicional después de esta operación.
0% [Conectando a kali.download]
```

Ilustración 5: Imagen de la instalación de Maltego mediante el comando «sudo apt install maltego». Para utilizar ese comando es necesario introducir la contraseña.

5 MALTEGO

Instalación y configuración

- Una vez instalado, para ejecutar la herramienta utiliza el comando maltego.



```
(incibe@kali)-[~]
$ maltego
java is /usr/bin/java
found java executable in PATH
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
pwd: file:/usr/share/maltego/maltego-ui/modules/ext/Java_Config_App.jar
install conf: /usr/share/maltego/etc/maltego.conf
install version: v4.3.0
user conf: /home/incibe/.maltego/v4.3.0/etc/maltego.conf
current java: /usr/lib/jvm/java-11-openjdk-amd64
/usr/lib/jvm: /usr/lib/jvm
/usr/lib/jvm: /usr/lib/jvm/java-11-openjdk-amd64
/usr/lib/jvm: /usr/lib/jvm/java-1.11.0-openjdk-amd64
/usr/lib/jvm: /usr/lib/jvm/default-java
does not exist: /usr/lib/jvm/bin/java
not jre/jdk: /usr/lib/jvm
/usr/lib/jvm/java-1.11.0-openjdk-amd64 VS /usr/lib/jvm/java-11-openjdk-amd64 (/usr/lib/jvm/java-11-openjdk-amd64/bin/java)
/usr/lib/jvm/java-1.11.0-openjdk-amd64 sym /usr/lib/jvm/java-11-openjdk-amd64
/usr/lib/jvm/java-1.11.0-openjdk-amd64 VS /usr/lib/jvm/default-java (/usr/lib/jvm/java-11-openjdk-amd64/bin/java)
/usr/lib/jvm/default-java dig /usr/lib/jvm/java-1.11.0-openjdk-amd64
trying path: /usr/lib/jvm/default-java
canonical: /usr/lib/jvm/java-11-openjdk-amd64
javaHome: /usr/lib/jvm/default-java
resource:com/paterva/maltego/java/config/jre/TestJDK.class → /tmp/temp1545594821823023605796884876242/TestJDK.class
executing: /usr/lib/jvm/java-11-openjdk-amd64/bin/java -classpath /tmp/temp1545594821823023605796884876242 TestJDK, in: .
result: 0
command execution finished
out: 11.0.14_11.0.14+9-post-Debian-1, Debian, Linux, amd64
```

Ilustración 6: Una vez instalado, es necesario introducir el comando «maltego» para ejecutar la herramienta.

5 MALTEGO

Instalación y configuración

- Te aparecerá una pantalla como la siguiente, donde deberás seleccionar la opción de «*Community Edition*» que se muestra con el nombre «CE (Free)». Esta edición es gratuita y la más completa que ofrece Maltego, pero exige registrarse en su portal. Al hacer clic en «*Run*», automáticamente te redirigirá a la página de registro de Maltego.

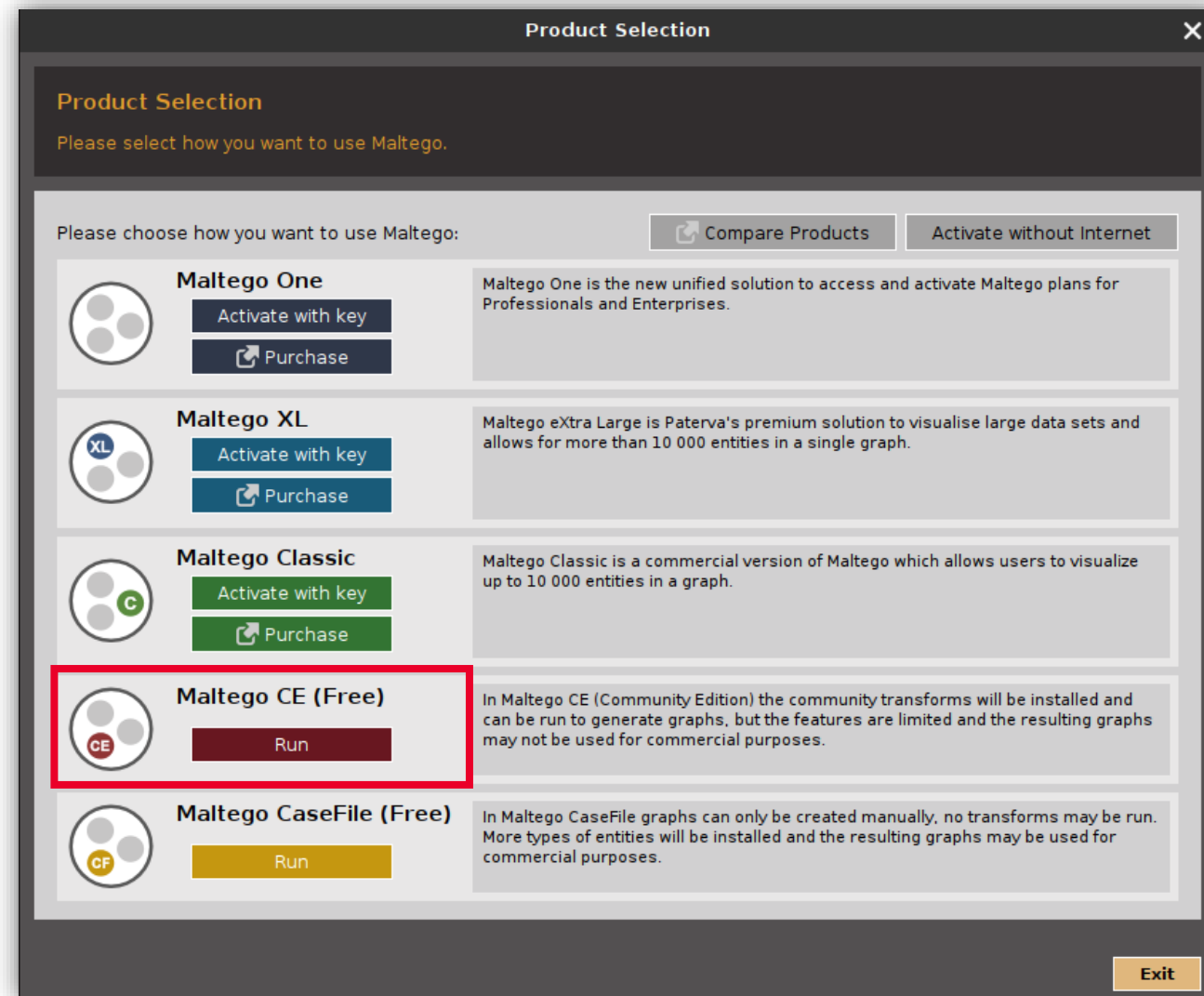


Ilustración 7: Captura de la pantalla donde se podrá elegir la versión gratuita del programa.

5 MALTEGO

Instalación y configuración

- Una vez realizados todos los pasos de registro y hayas activado la cuenta con el enlace que te han enviado al correo, podrás seguir con la configuración de la herramienta.

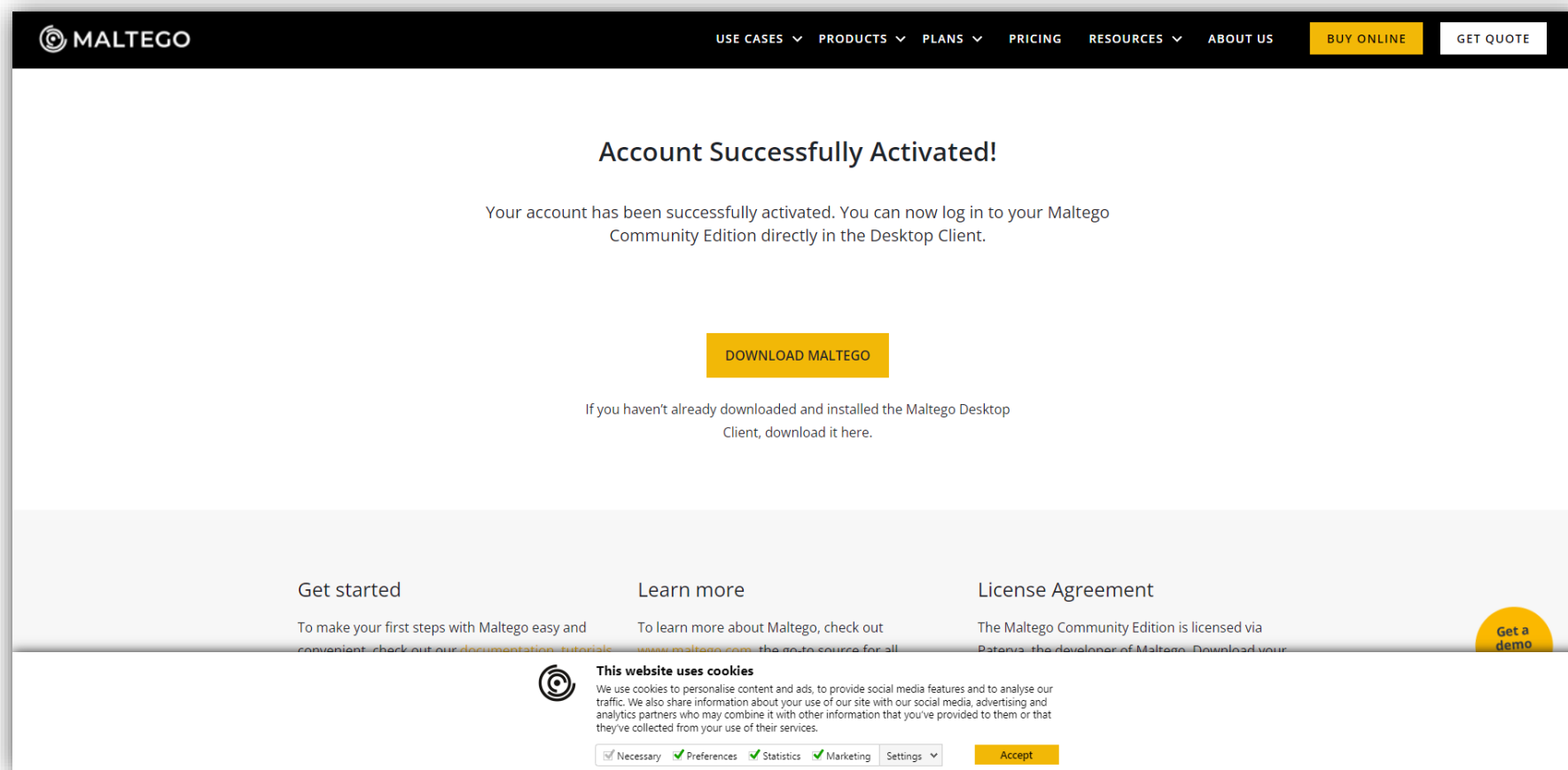


Ilustración 8: Imagen de la confirmación de la correcta activación de la cuenta.

5 MALTEGO

Instalación y configuración

- Volviendo a la interfaz de Maltego, debes aceptar los términos de licencia activando la casilla «**Accept**» y haciendo clic en «**Next**».

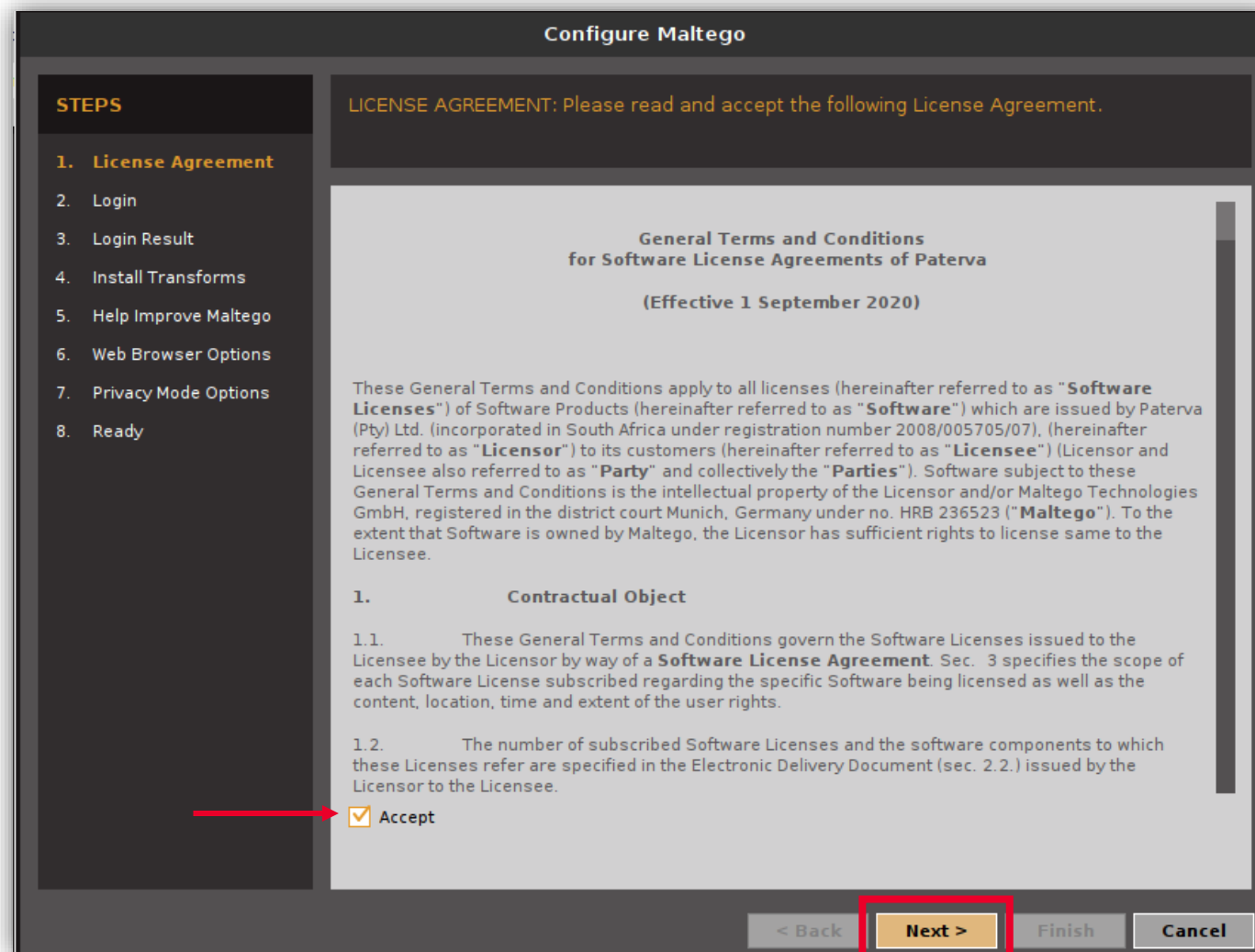


Ilustración 9: Captura de la página en la que se aceptan los términos y condiciones del programa.

5 MALTEGO

Instalación y configuración

- En la siguiente pantalla, introduce los datos de *login* con los que te has registrado en la página de Maltego.

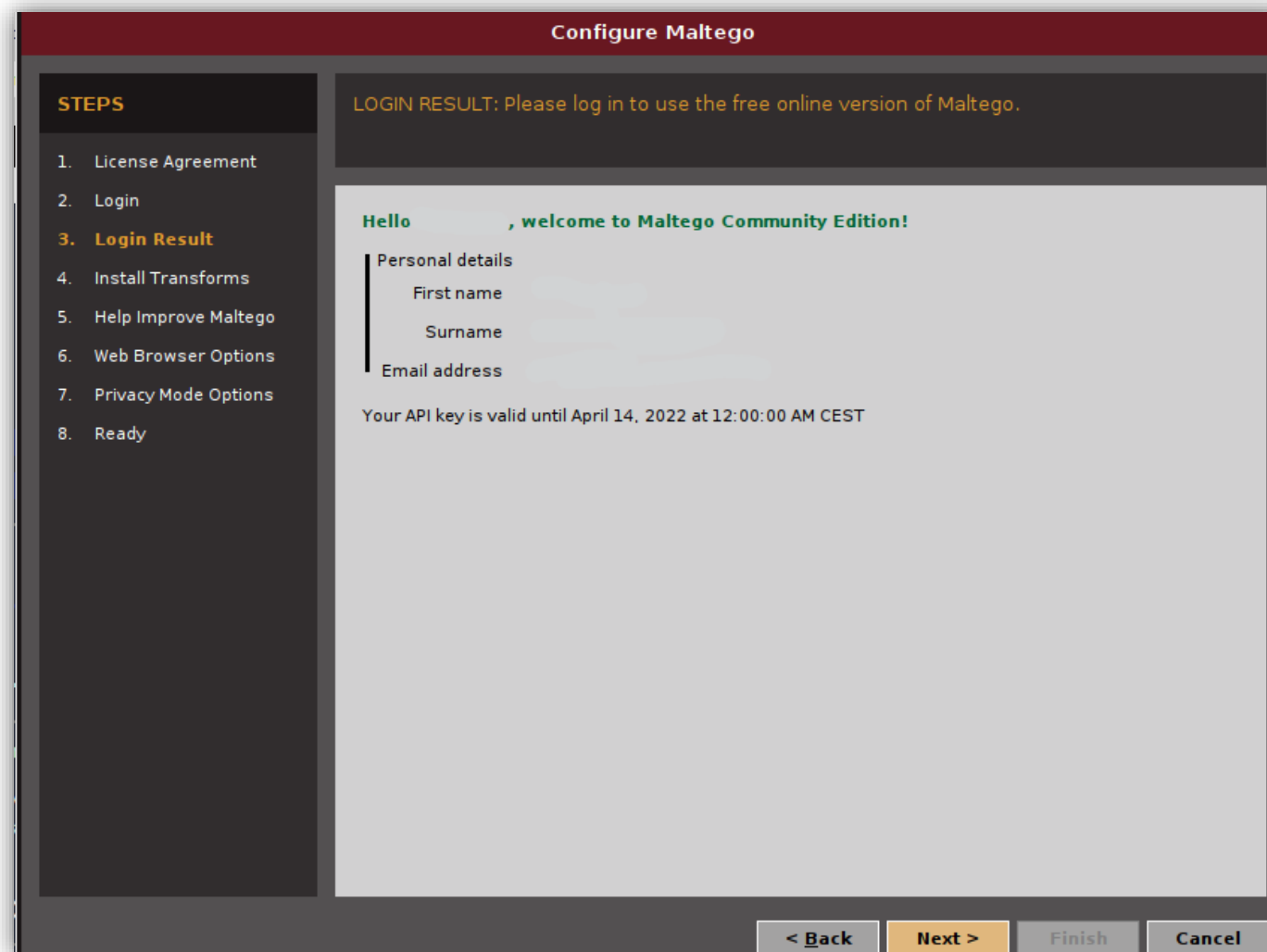


Ilustración 10: Imagen con la pantalla en la que introducir los datos de acceso.

5 MALTEGO

Instalación y configuración

- A continuación, aparecerá una pantalla donde debes confirmar la instalación de las «Transformadas». Las transformadas de Maltego son funciones que te ayudarán a tratar la información de diversas maneras y a buscar resultados en diversas fuentes. Por el momento, deja todo por defecto, aprenderás más adelante a instalar Transformadas bajo demanda.

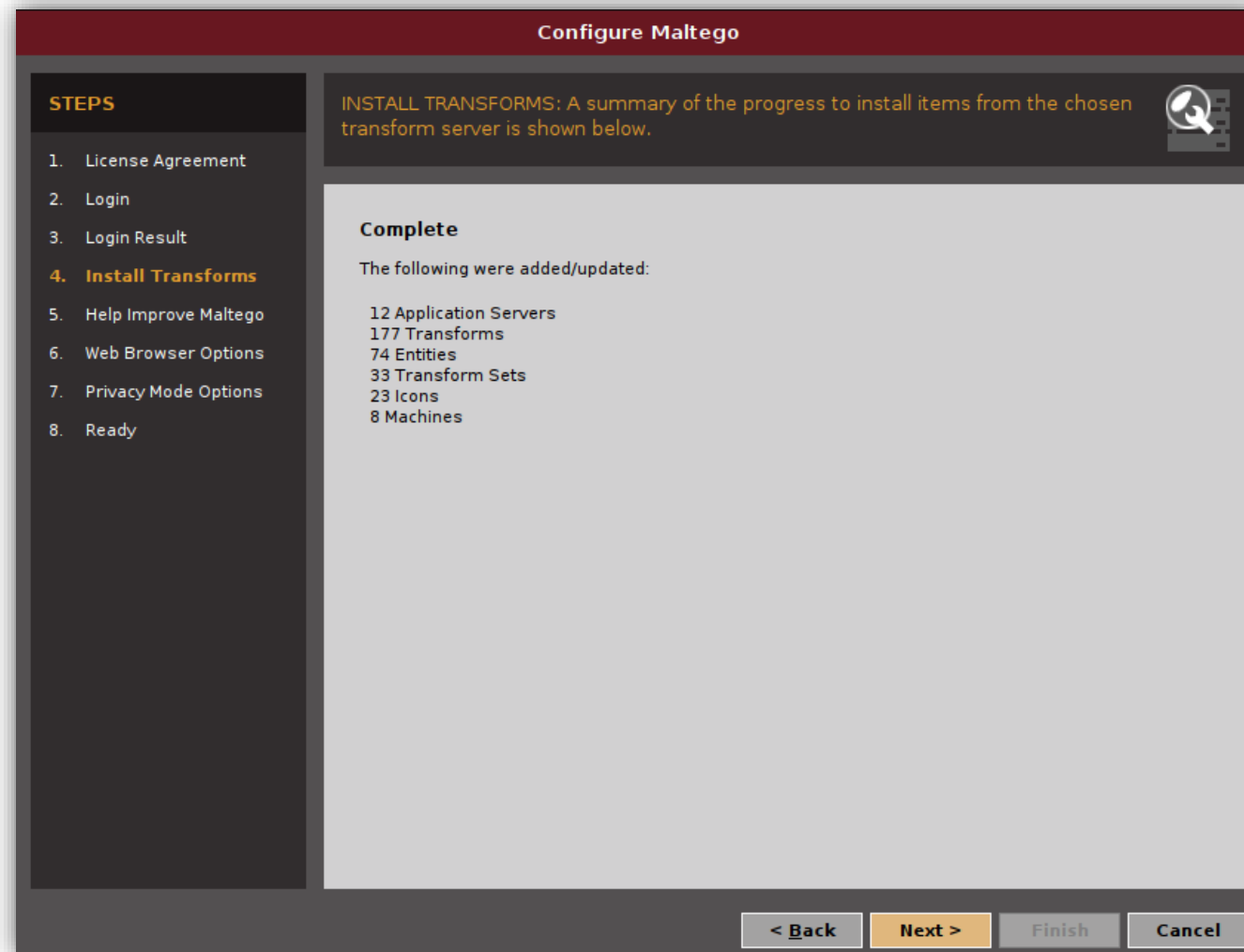


Ilustración 11: Imagen de la pantalla donde se confirma la instalación de las «Transformadas», funciones que ayudan a tratar la información.

5 MALTEGO

Instalación y configuración

- En esta pantalla el programa pregunta por la posibilidad de que los desarrolladores puedan recibir automáticamente un informe de error cuando la aplicación tenga algún fallo. Decide si quieres permitirlo o no y pulsa «Next».

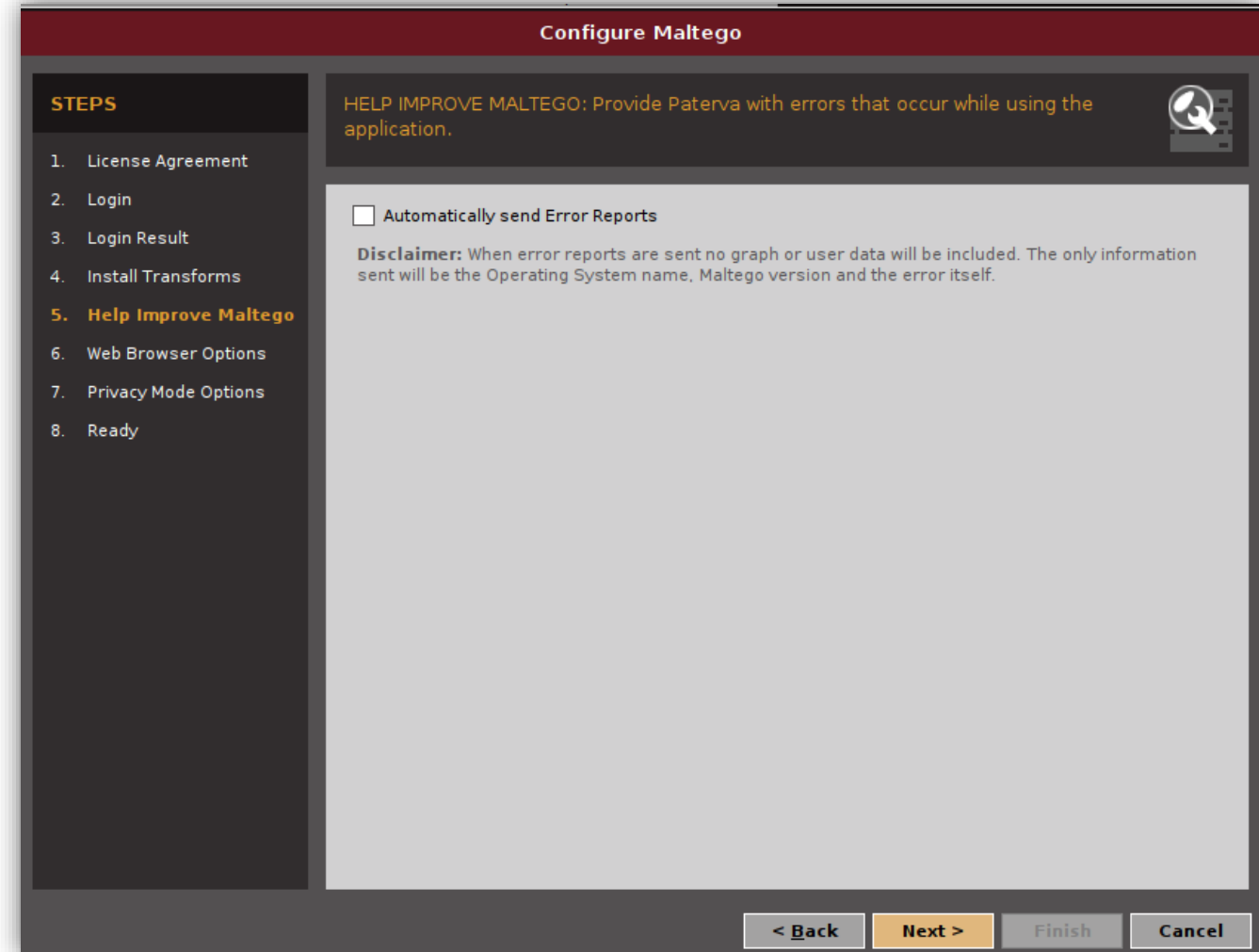


Ilustración 12: Pantalla donde se da la opción de marcar que la herramienta envíe automáticamente los errores que puedan surgir en ella.

5 MALTEGO

Instalación y configuración

- Ahora debes seleccionar el navegador web para poder abrir y acceder directamente a los enlaces descubiertos en Maltego. En este caso, usa el navegador por defecto del sistema seleccionando la opción «**Default System Browser**» y haciendo clic en «**Next**».

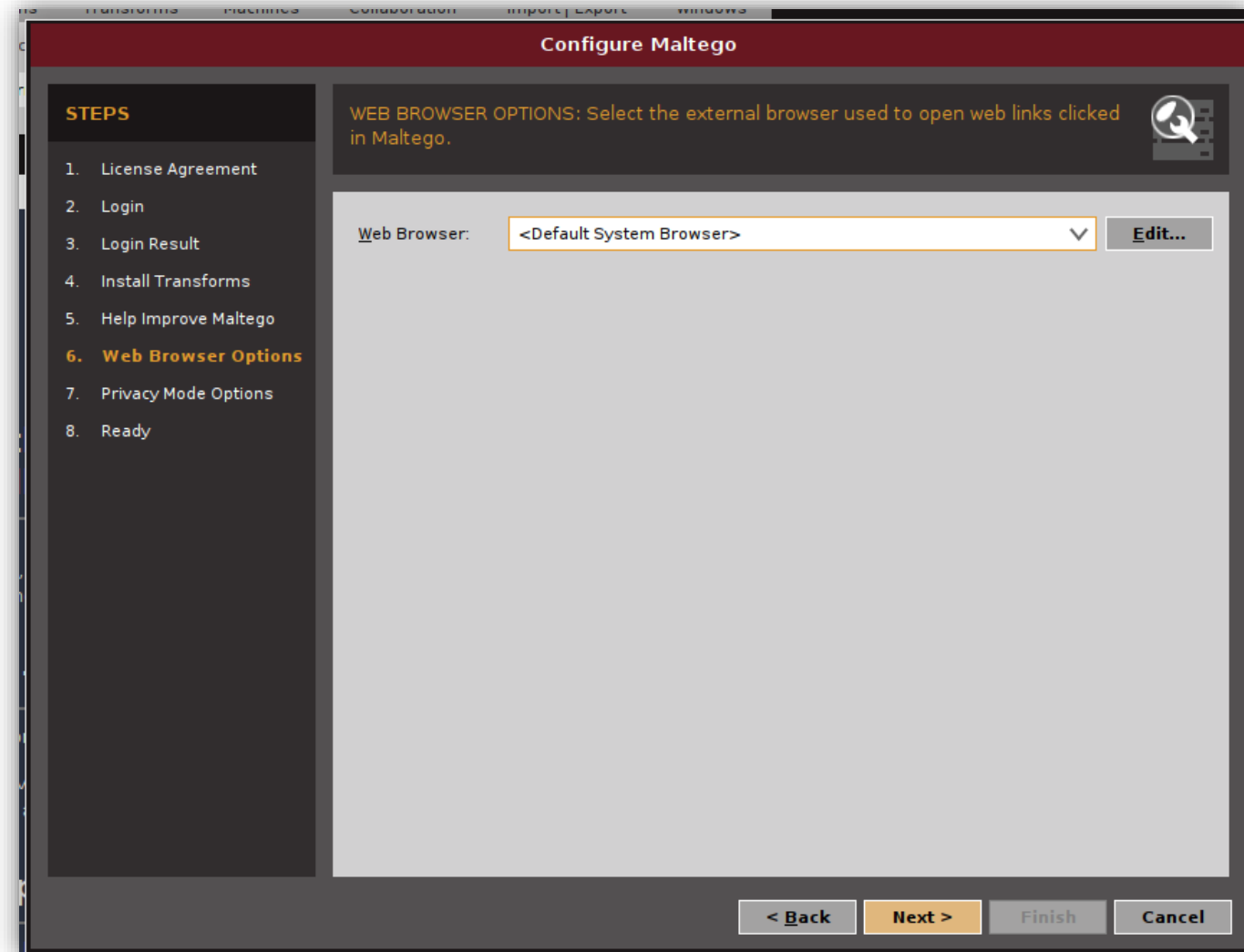


Ilustración 13: Navegador web para poder abrir y acceder directamente a los enlaces descubiertos en Maltego

5 MALTEGO

Instalación y configuración

- A continuación, configura el nivel de privacidad de Maltego durante tus investigaciones. Para una investigación profesional la opción a seleccionar es «*Stealh Privacy Mode*», sin embargo, como aquí vamos a realizar una práctica meramente educativa, es suficiente y recomendable el modo «*Normal*». Selecciónalo y haz clic en «*Next*».

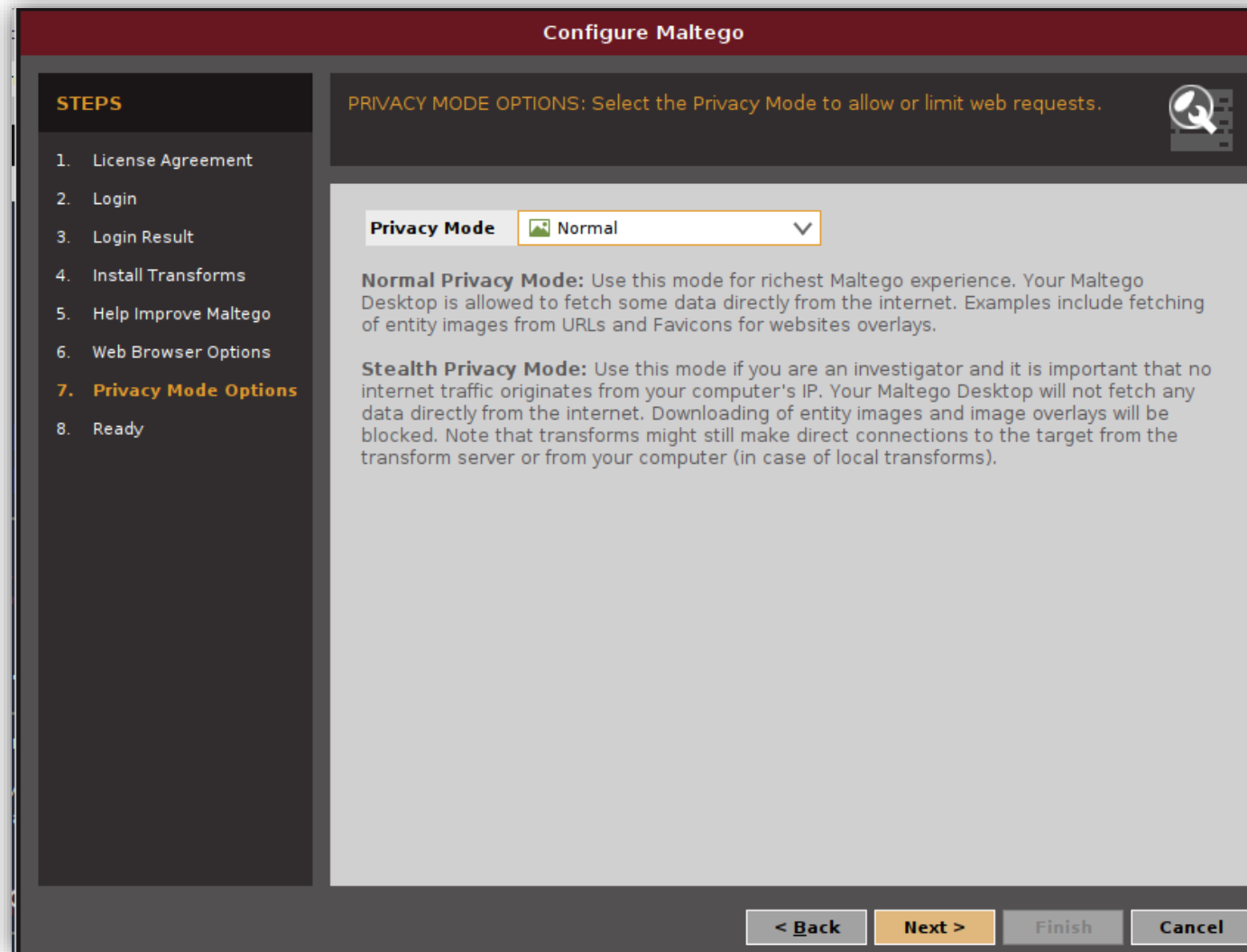


Ilustración 14: Pantalla donde se selecciona el modo de privacidad.

5 MALTEGO

Instalación y configuración

- En la pantalla final, da la opción de abrir un nuevo gráfico donde llevarás a cabo tu investigación. Selecciona la opción «*Open a blank graph*» y haz clic en «*Finish*».

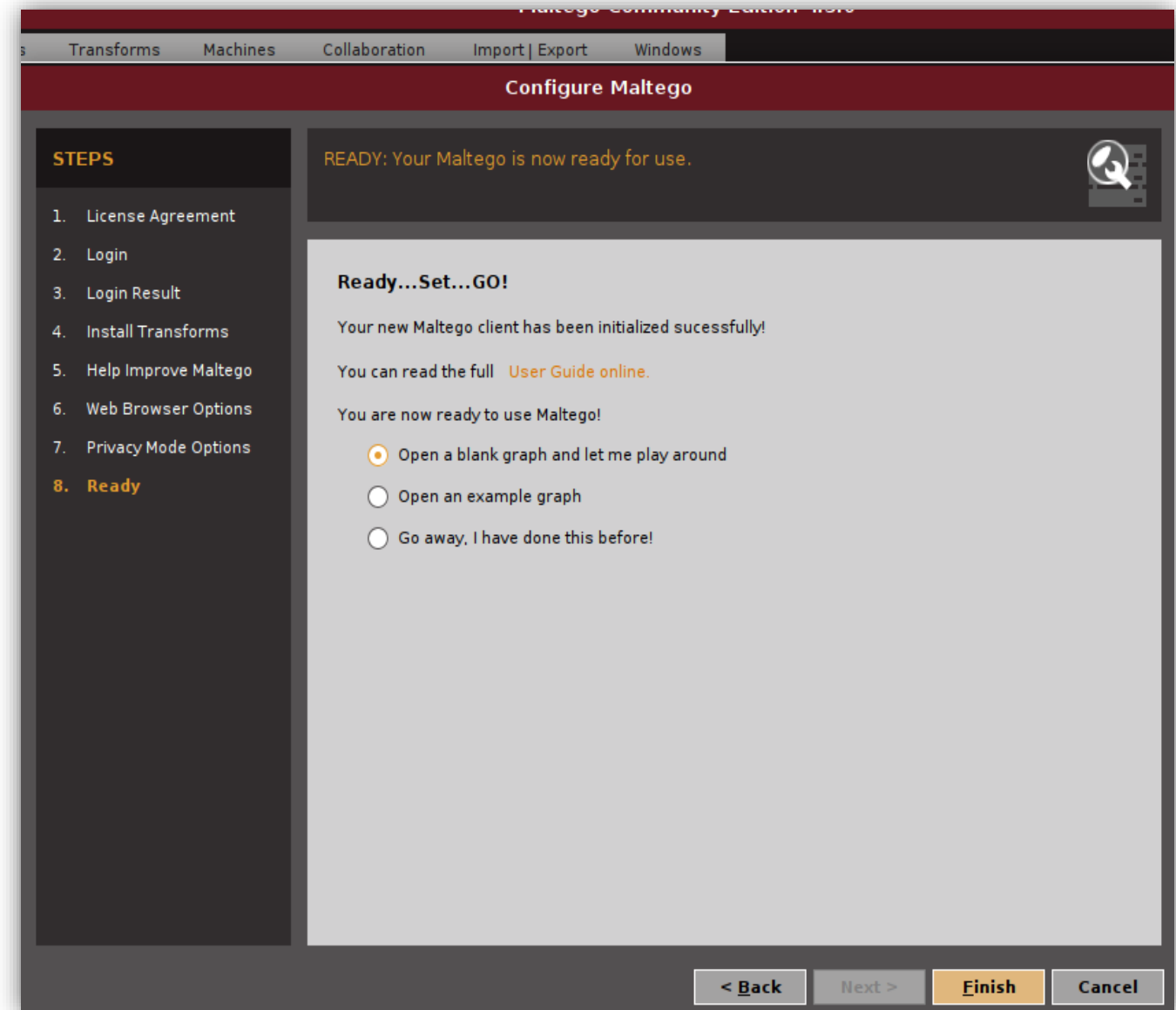


Ilustración 15: Imagen donde se abre el tipo de gráfico elegido para realizar la investigación.

5 MALTEGO

Instalación y configuración

- Esta es la pantalla principal de la herramienta.

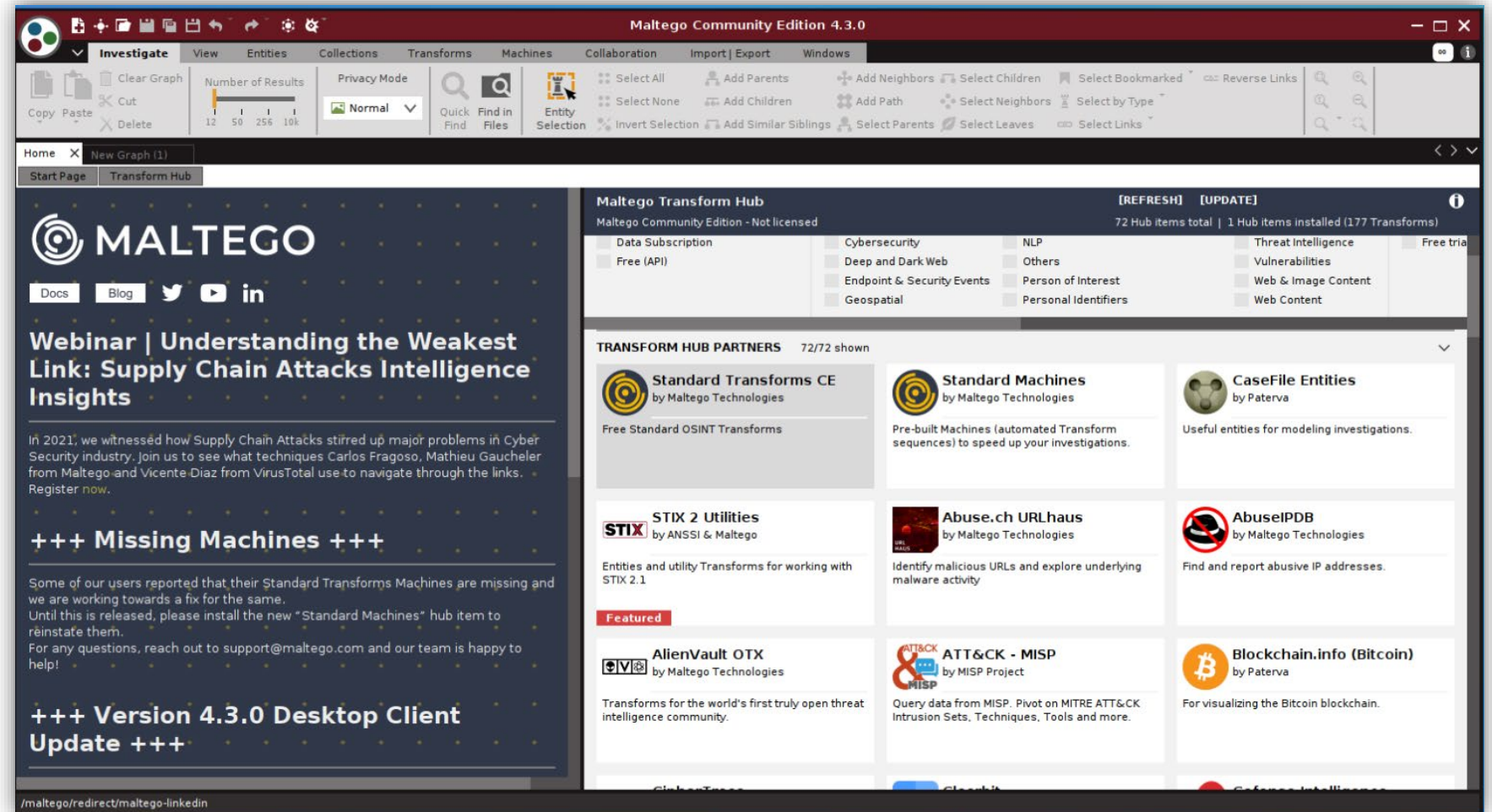


Ilustración 16: Imagen que muestra la pantalla principal de Maltego.

5 MALTEGO

Instalación y configuración

- Antes de empezar la investigación deberás instalar algunas «Transformadas» o funciones que darán más resultados y más detalles a tu análisis. Para ello, haz clic en la pestaña superior, «**Home**».
- Como podrás observar en la siguiente imagen [ilustración 17], en la parte derecha, verás un área llamada «**Transform Hub Partners**». Hay transformadas de pago, otras que requieren de una API key como Shodan y otras gratuitas. Podemos filtrar por todas y cada una de las categorías con la ayuda del panel superior.
- En tu caso, instala las siguientes transformadas haciendo clic en «**Install**» en cada una de ellas.
 - *Standard Transforms CE.*
 - *CaseFile Entities.*
 - *Farsight DNSDB.*
 - *Have I Been Pawned?*
 - *Social Links CE.*

5 MALTEGO

Instalación y configuración

- Siempre puedes volver a esta pantalla y hacer un repaso de todas las transformadas y sus funciones para adaptarlo a tus necesidades.

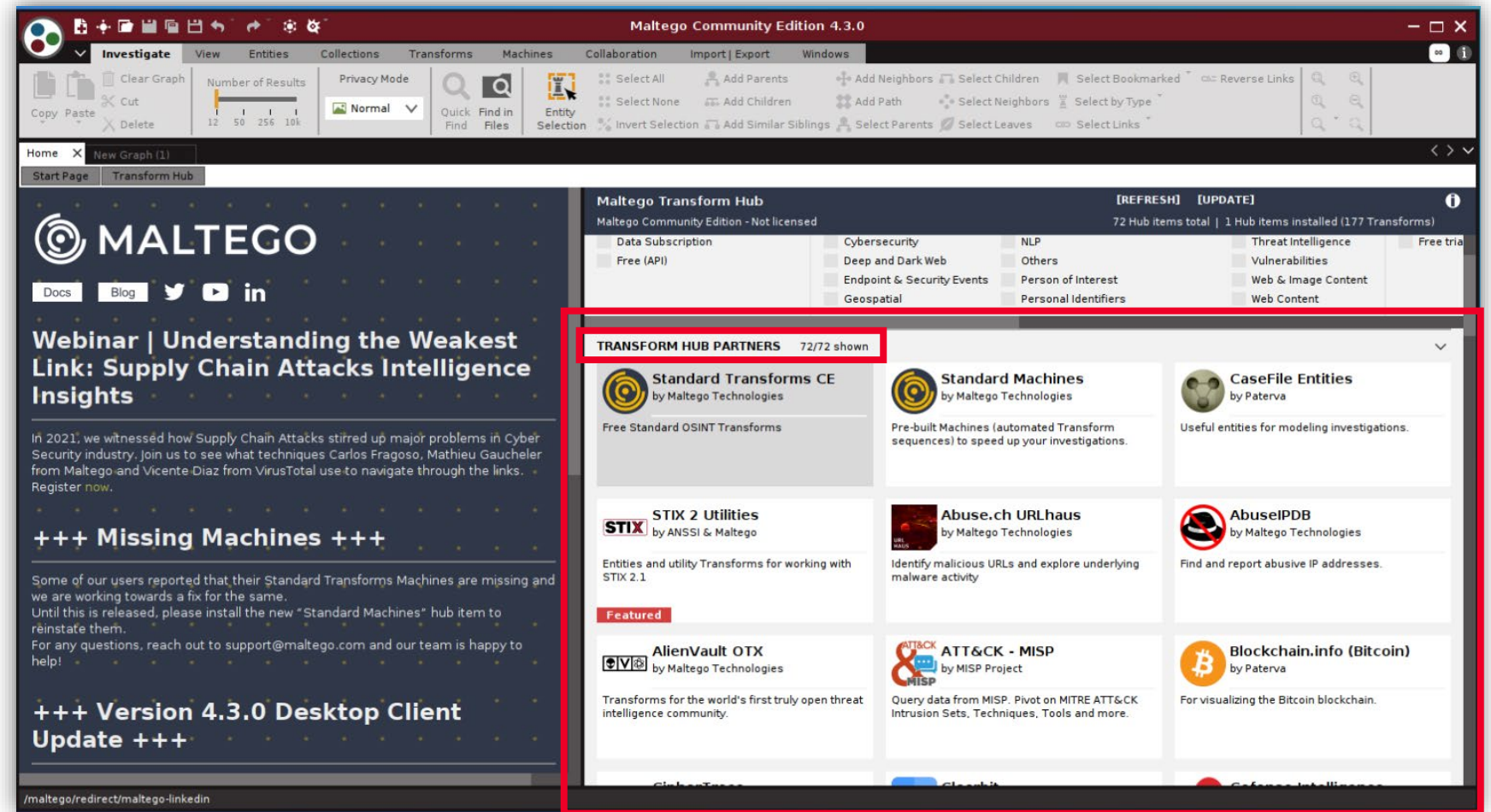


Ilustración 17: Imagen que muestra ejemplos de las diferentes transformadas que se pueden elegir.

5 MALTEGO

Instalación y configuración

- Dirígete a la pestaña «**New Graph**». Este es el panel donde llevarás a cabo la investigación sobre el dominio «**paterva.com**».
- Para empezar, dentro de la paleta de «**Entidades**» de la parte izquierda, debes buscar la entidad «**Domain**» ya que lo que quieres analizar es un Dominio.
 - Igualmente, dispones de entidades para buscar textos, correos electrónicos, IP, etc.
- Busca «**domain**» en la caja de búsqueda destinada a ello.

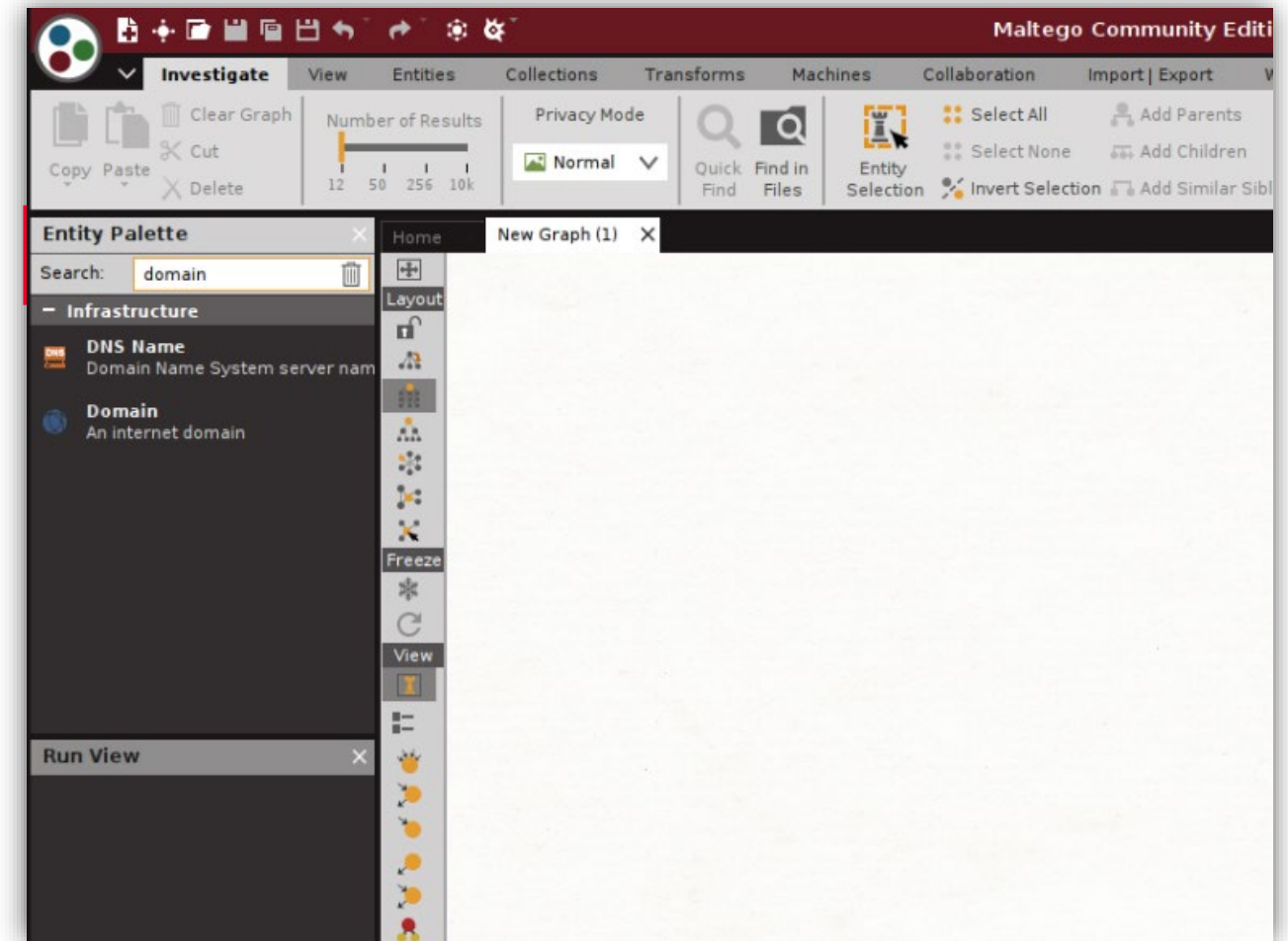


Ilustración 18: Imagen del buscador en el que se introduce el término «domain».

5 MALTEGO

Instalación y configuración

- Haz clic y arrastra el elemento «*domain*» a tu panel. Puedes hacer zoom en el panel con la rueda del ratón o moverte libremente haciendo clic derecho y arrastrando.

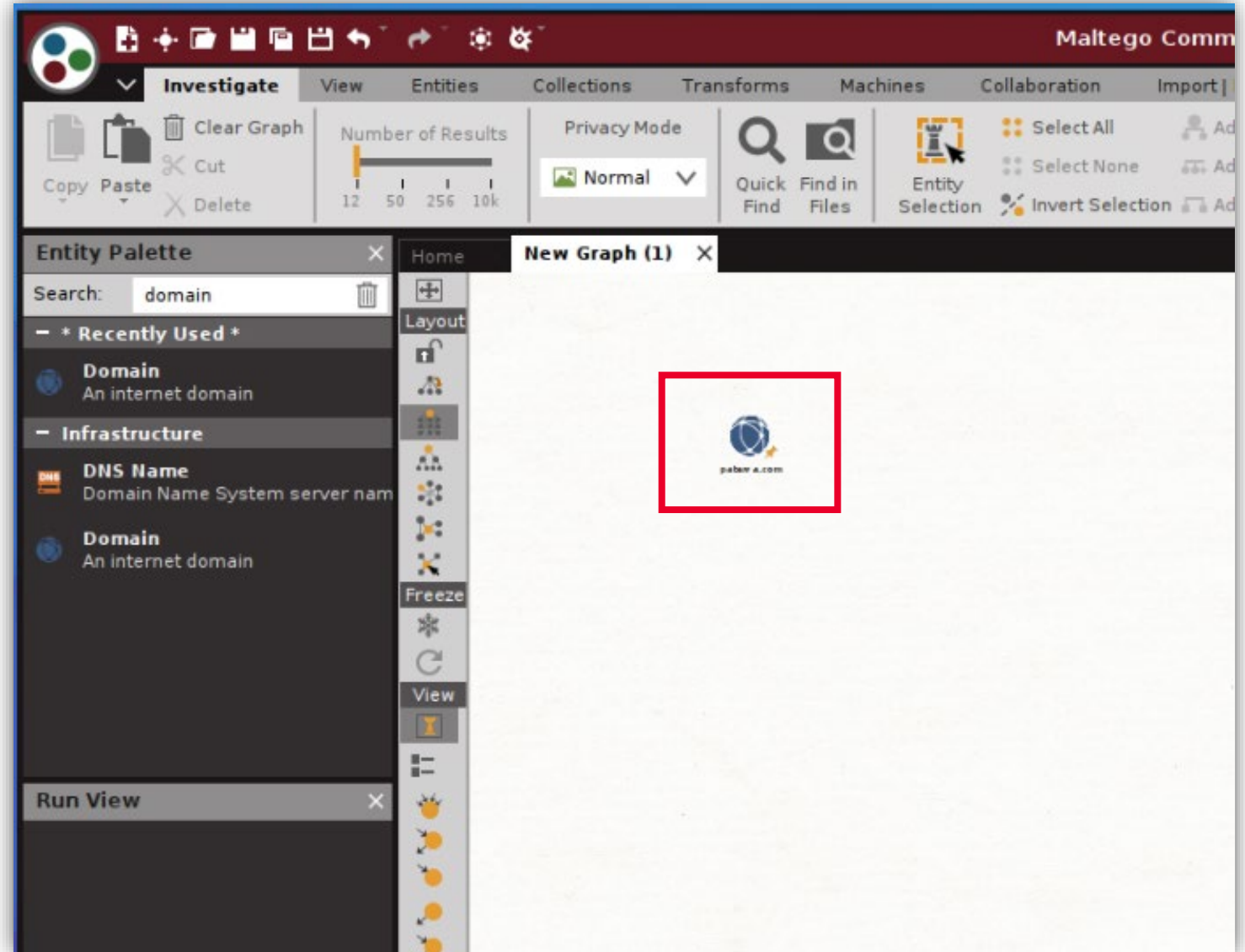


Ilustración 19: Imagen de la pantalla donde se arrastra el elemento «domain» a tu panel.

5 MALTEGO

Instalación y configuración

- Haciendo clic en el elemento, puedes ver como aparece en la esquina inferior derecha el panel de propiedades. Aquí, sobre el campo «**Domain name**», escribe el dominio sobre el que quieras iniciar la investigación. En este caso, utilizarás el dominio que nos ofrece Maltego, «paterva.com».

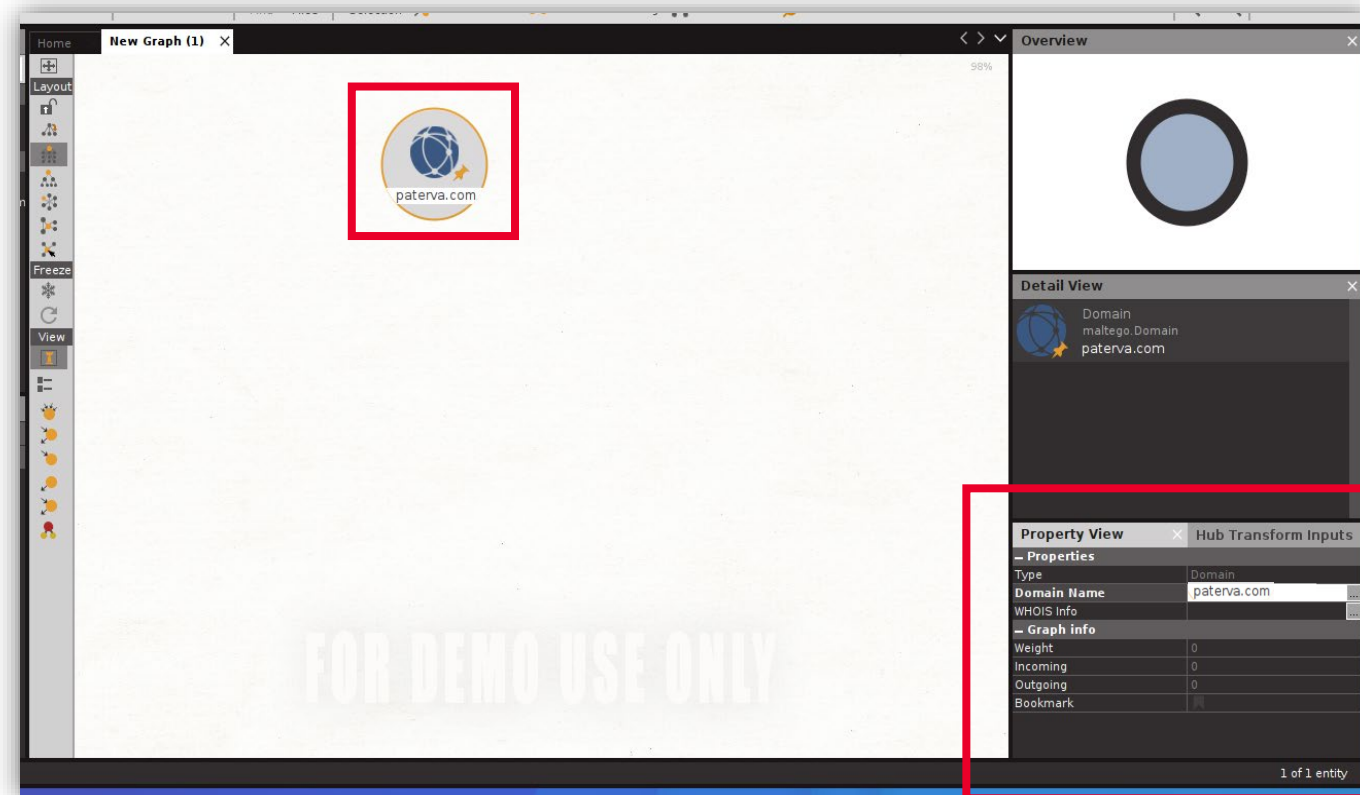


Ilustración 20: Pantalla en la que se escribe el dominio sobre el que se realiza la investigación.

5 MALTEGO

Instalación y configuración

- A continuación, haz clic derecho sobre el elemento y pulsa en «+ **All Transforms**» para aplicar todas las transformadas de una sola vez. Cabe destacar que, en una investigación ordenada, deberás seleccionar y aplicar solo aquellas transformadas que te interesen.

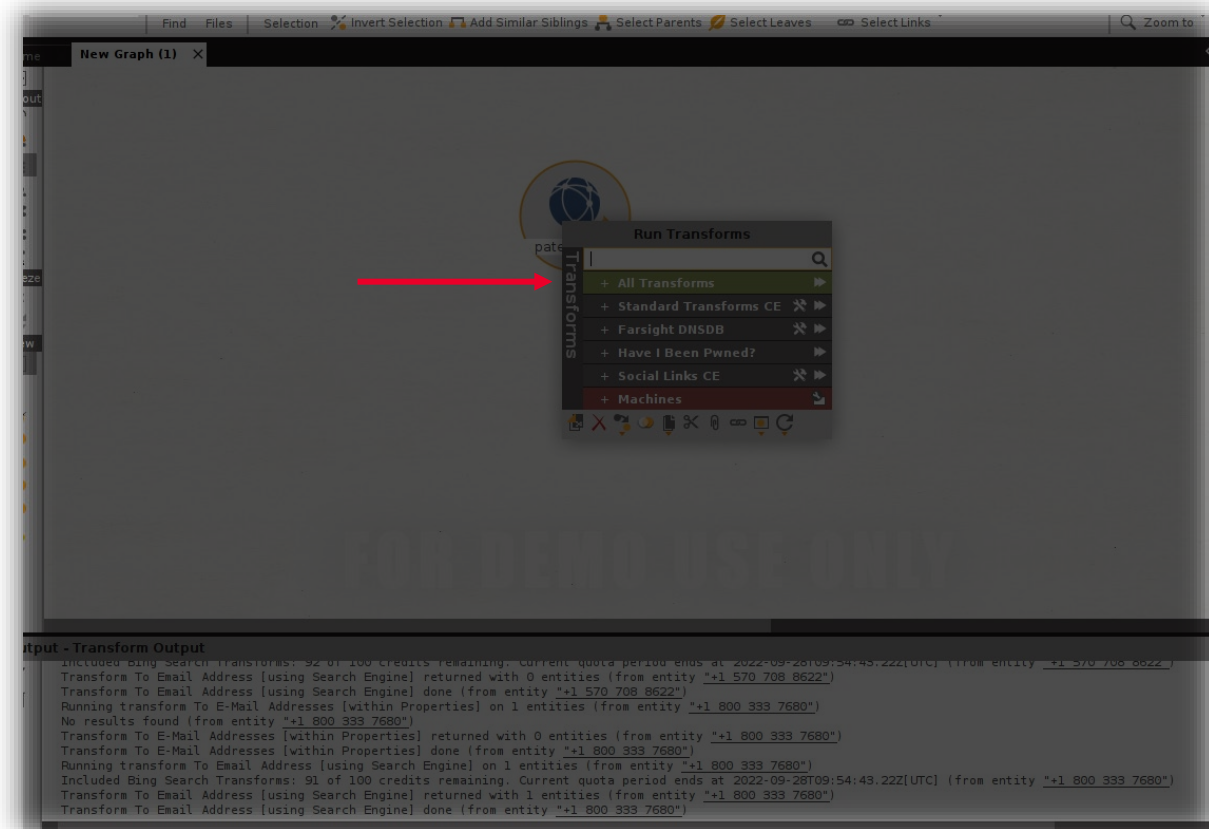


Ilustración 21: Captura del apartado en el que se aplica la selección de las transformadas.

5 MALTEGO

Instalación y configuración

- Es probable que te aparezca una ventana donde pidan algunos datos necesarios para algunas de las transformadas. Simplemente, **deja los campos por defecto** y haz clic en **«Run»**.

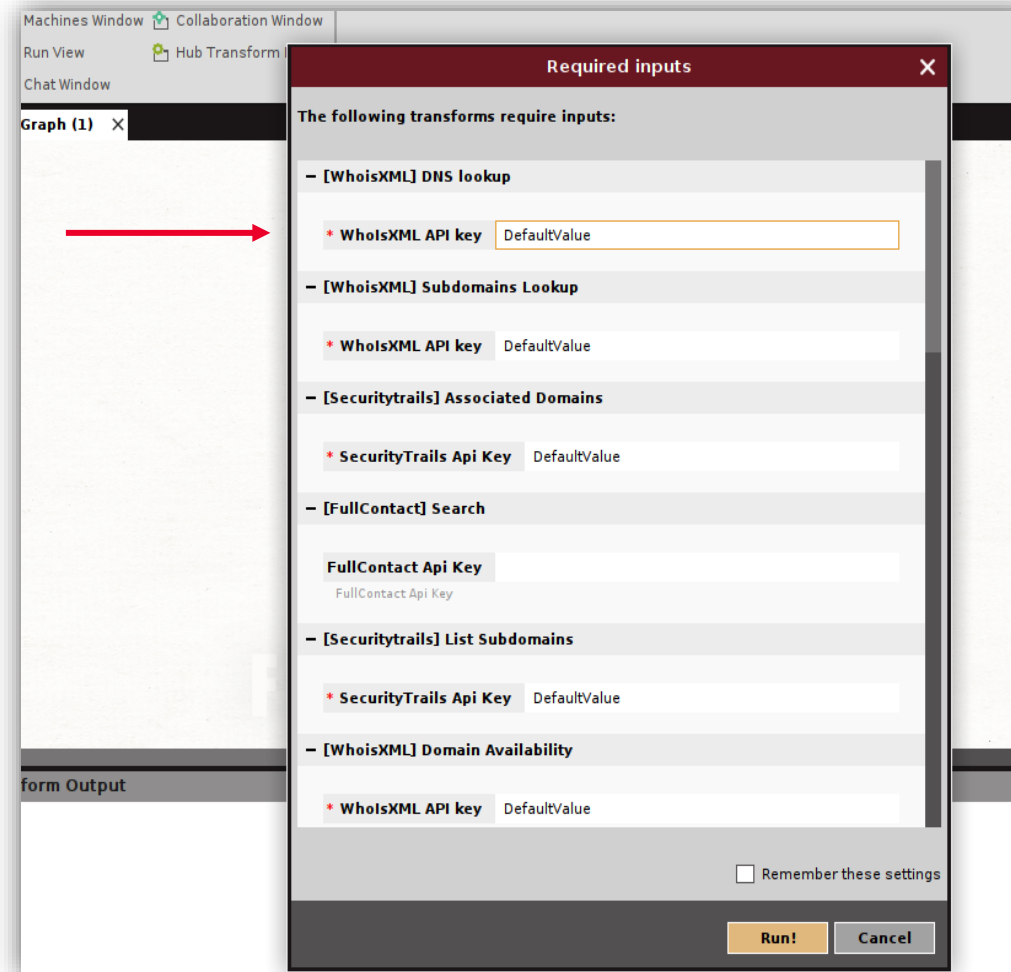


Ilustración 22: Ventana en la que se mantienen los campos por defecto de las transformadas.

5 MALTEGO

Instalación y configuración

- Una vez que haya terminado el análisis (lo sabrás porque en la consola inferior aparecerá un mensaje con la palabra «**done**»), verás un diagrama con los resultados divididos por categorías y colores. En tu caso, sobre el dominio «**paterva.com**» se han encontrado web, direcciones de email, números de teléfono, registros DNS, etc.

5 MALTEGO

Instalación y configuración

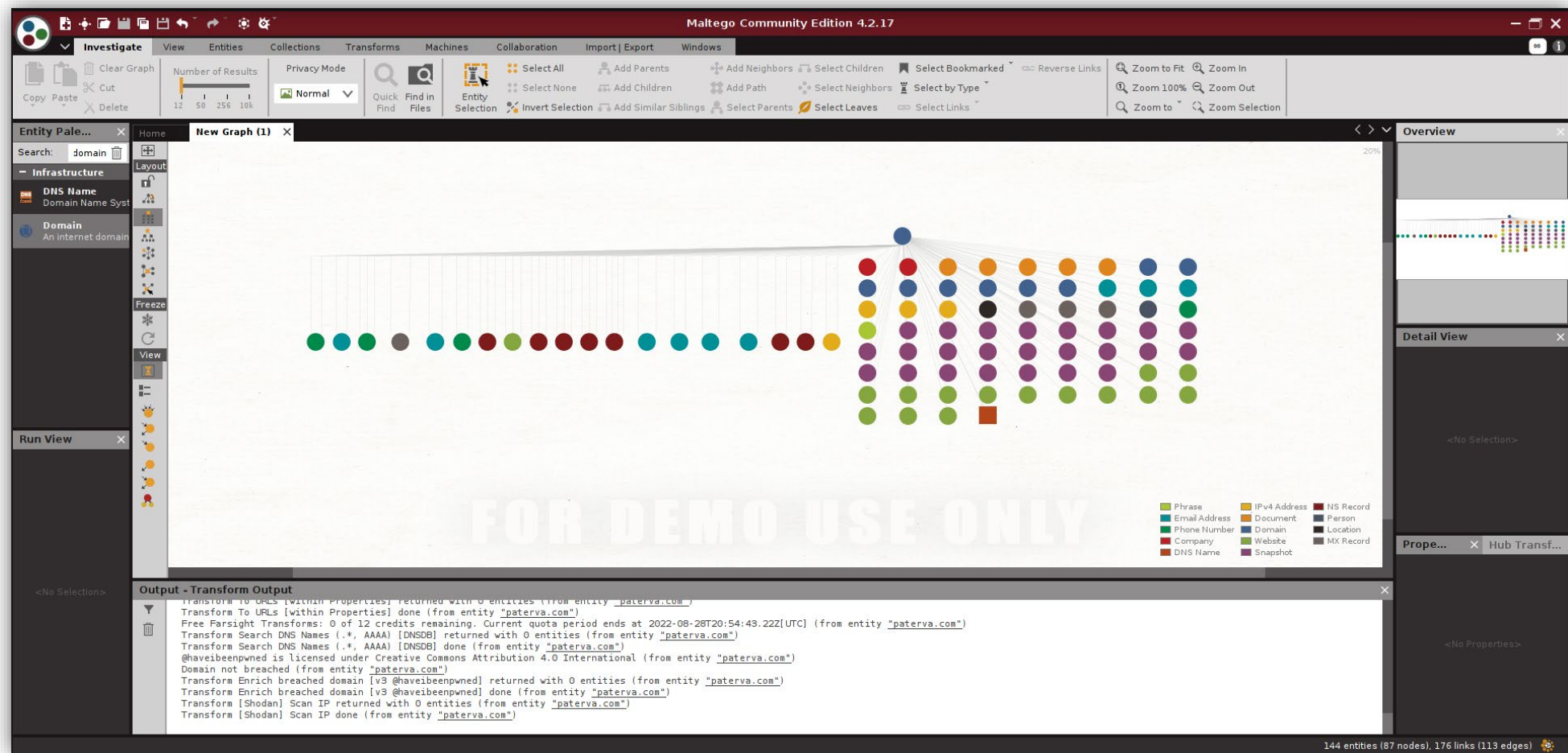


Ilustración 23: Imagen con los resultados del análisis.

5 MALTEGO

Instalación y configuración

- En el menú lateral izquierdo, en el gráfico «**Layout**» puedes cambiar la vista entre las diferentes tipologías que mejor se adapten a tus necesidades.

5 MALTEGO

Instalación y configuración

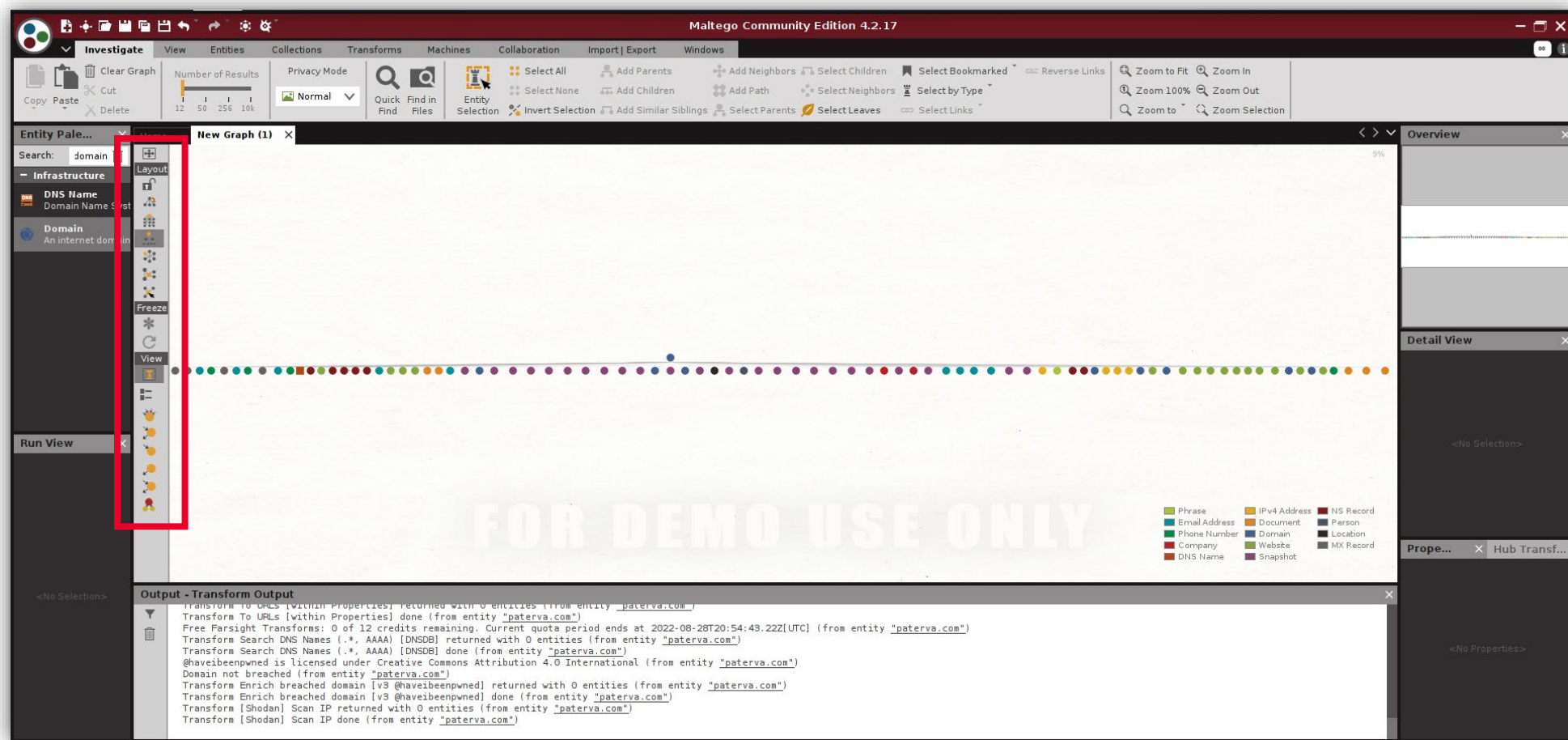


Ilustración 24: Vista del gráfico «Layout».

5 MALTEGO

Instalación y configuración

- Para obtener más detalle sobre los resultados, puedes hacer *zoom* con la rueda del ratón sobre el gráfico y hacer clic sobre cada uno para obtener detalles sobre el origen, datos extraídos, URL, etc.

5 MALTEGO

Instalación y configuración

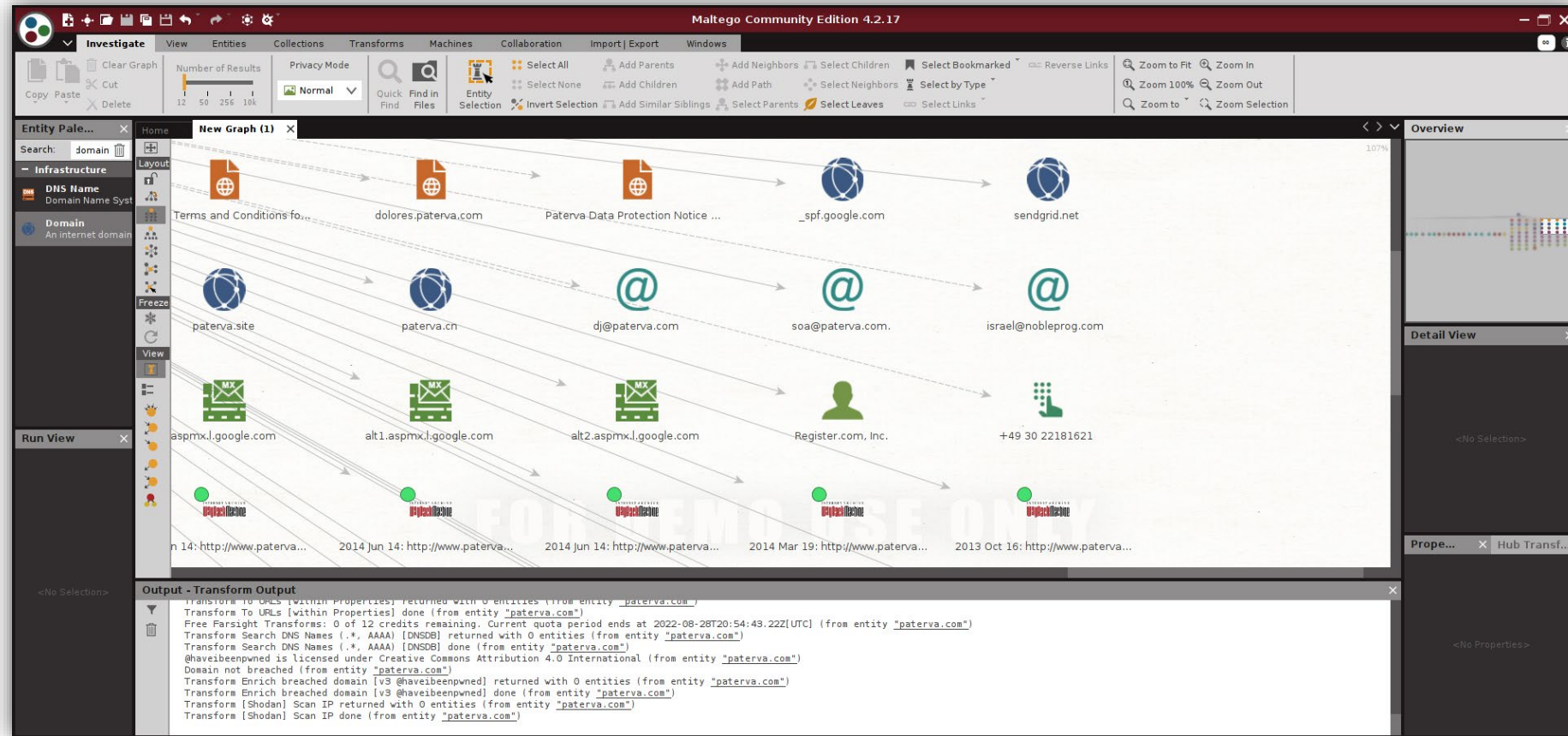


Ilustración 25: Al hacer zoom sobre el gráfico y hacer clic sobre cada uno de los iconos, se obtienen detalles de estos.

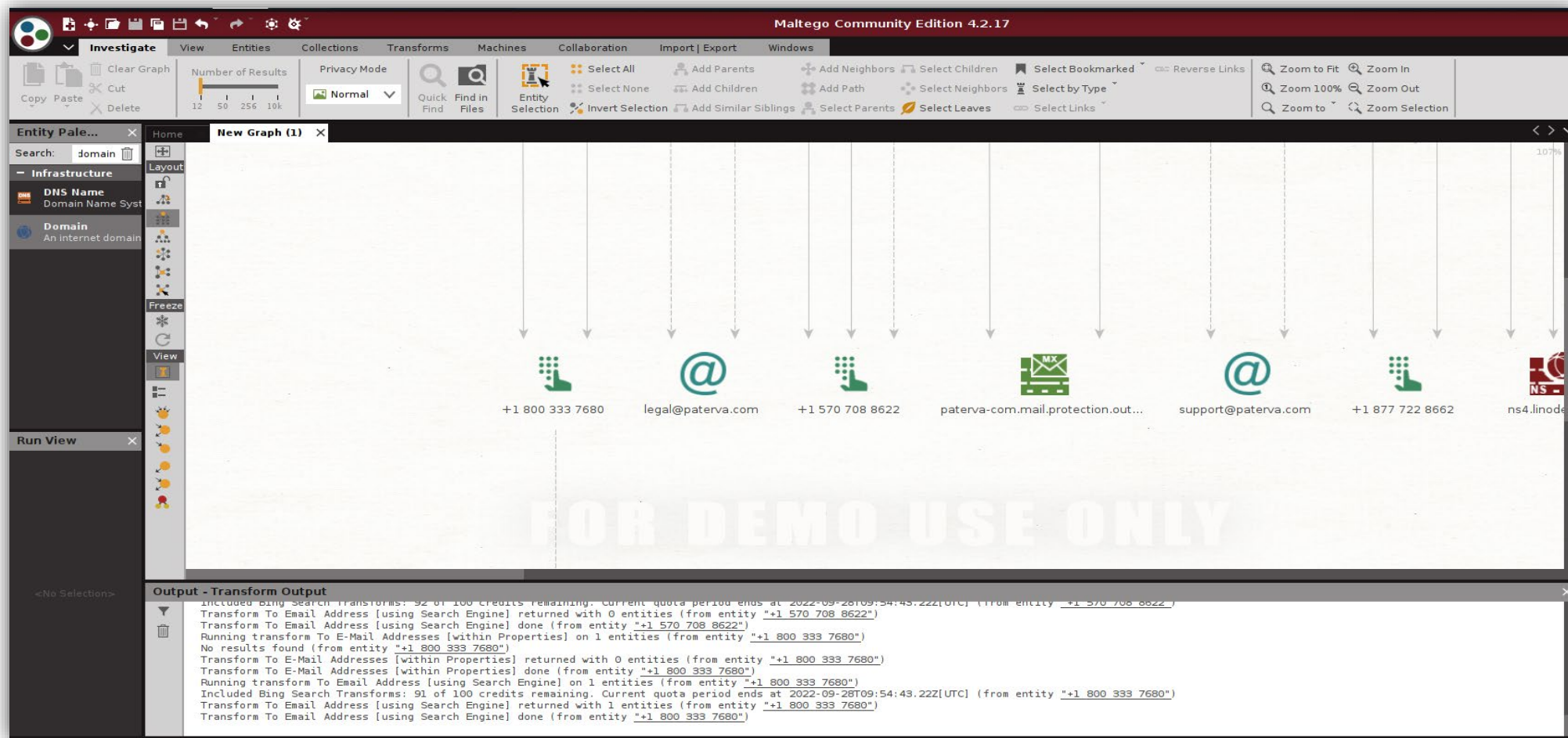
5 MALTEGO

Instalación y configuración

- En nuestro caso, si centramos la atención sobre el bloque de «**Phone number**», vemos que se han encontrado varios números de teléfono en el dominio «**paterva.com**».

5 MALTEGO

Instalación y configuración



5 MALTEGO

Instalación y configuración

- Para poder obtener más detalles sobre los *emails* asociados a este número de teléfono, puedes volver a hacer clic derecho en el elemento «**Phone number**» y aplicar la transformada «**To Email Addresses [using search Engine]**».

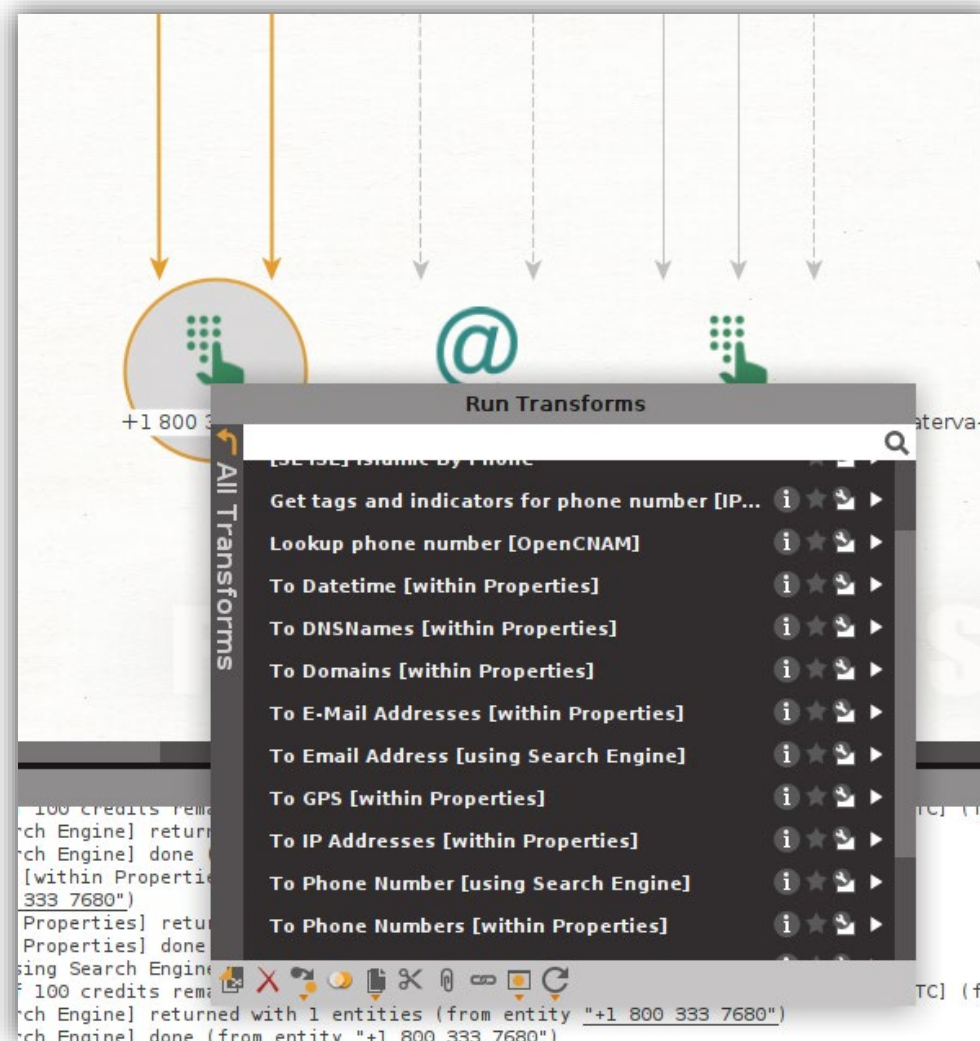


Ilustración 27: Aplicación de la transformada «*To Email Addresses [using search Engine]*» para ver más detalles de los elementos asociados a los números de teléfono

5 MALTEGO

Instalación y configuración

- Verás que, ahora, para este número de teléfono identifica un *email*. Sobre cada *email*, a su vez, podrías volver a realizar las transformadas adecuadas y encontrar si tiene alguna web a su nombre, sus perfiles en redes sociales, contraseñas filtradas, etc., hasta alcanzar el nivel de detalle deseado.

5 MALTEGO

Instalación y configuración

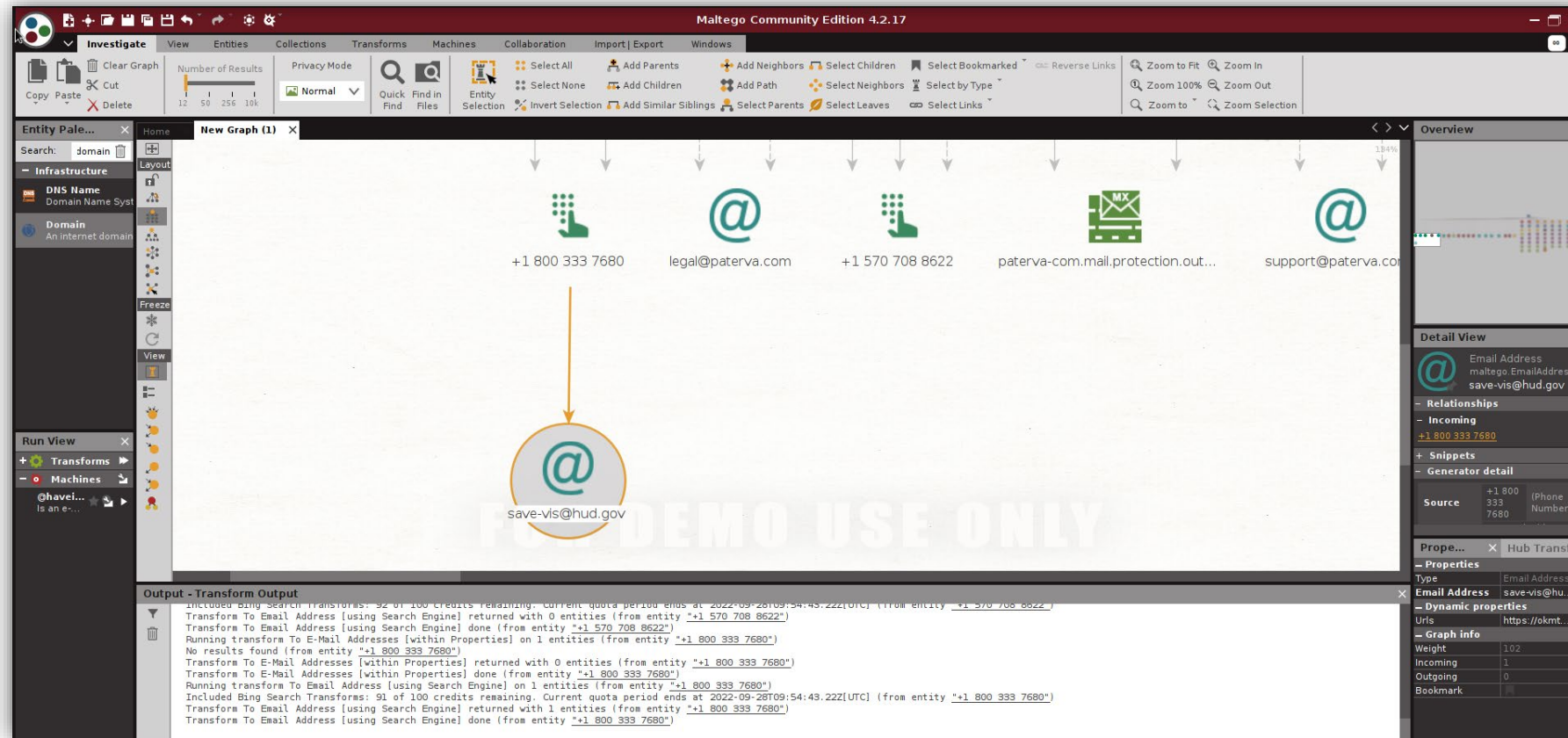


Ilustración 28: Imagen con el nivel de detalle que se puede obtener si cada vez que obtenemos un dato, se vuelve a solicitar información sobre el mismo.

¡GRACIAS!



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

