

Footprinting a un objetivo usando maltego

Maltego es una aplicación de inteligencia y forense de código abierto. Recopila información sobre un objetivo y representa esta información de forma fácil.

Objetivos del laboratorio

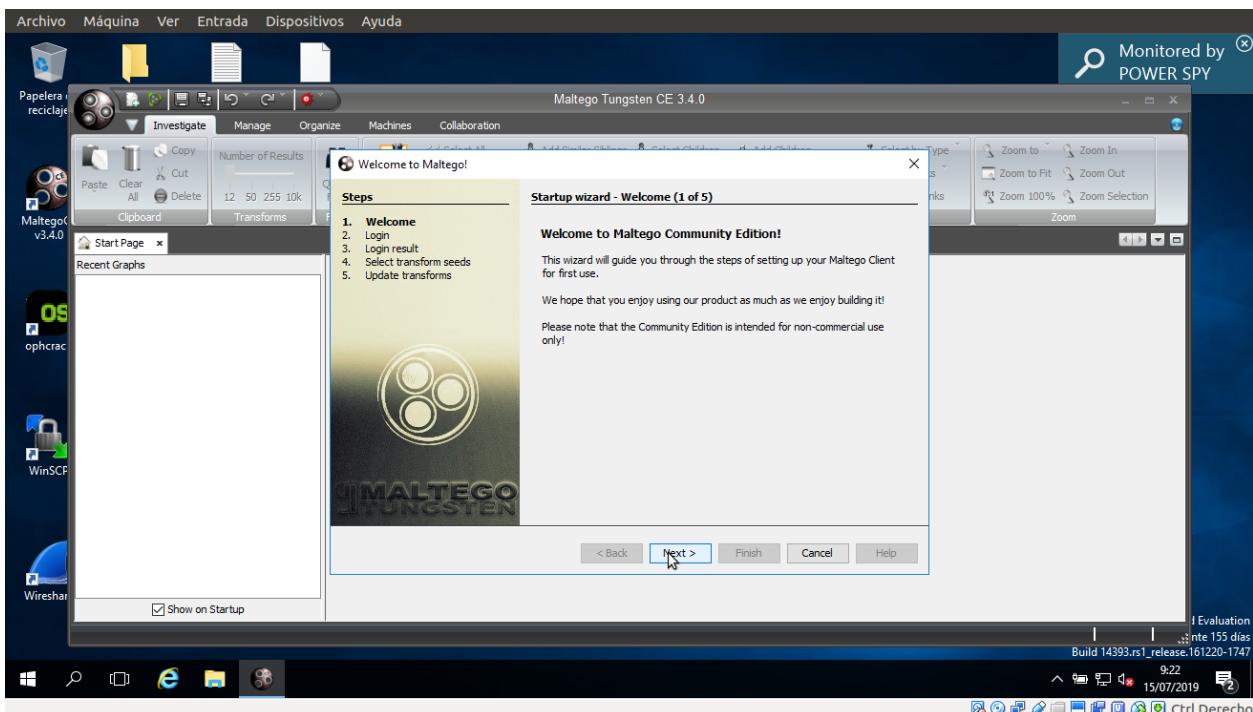
Este objetivo de este laboratorio es ayudar a los estudiantes a reunir la mayor cantidad de información posible sobre el objetivo. Con este laboratorio los estudiantes pueden:

- Identificar la tecnología del lado del servidor.
- Identificar el dominio
- Identificar el esquema de nombre de dominio.
- Identificar la información de la arquitectura orientada a servicios (SOA).
- Identificar el intercambiador de correo.
- Identificar el servidor de nombres.
- Identificar la dirección IP
- Identificar la ubicación geográfica.
- Identificar las entidades
- Encontrar la dirección de correo electrónico
- Averiguar los números de teléfono.

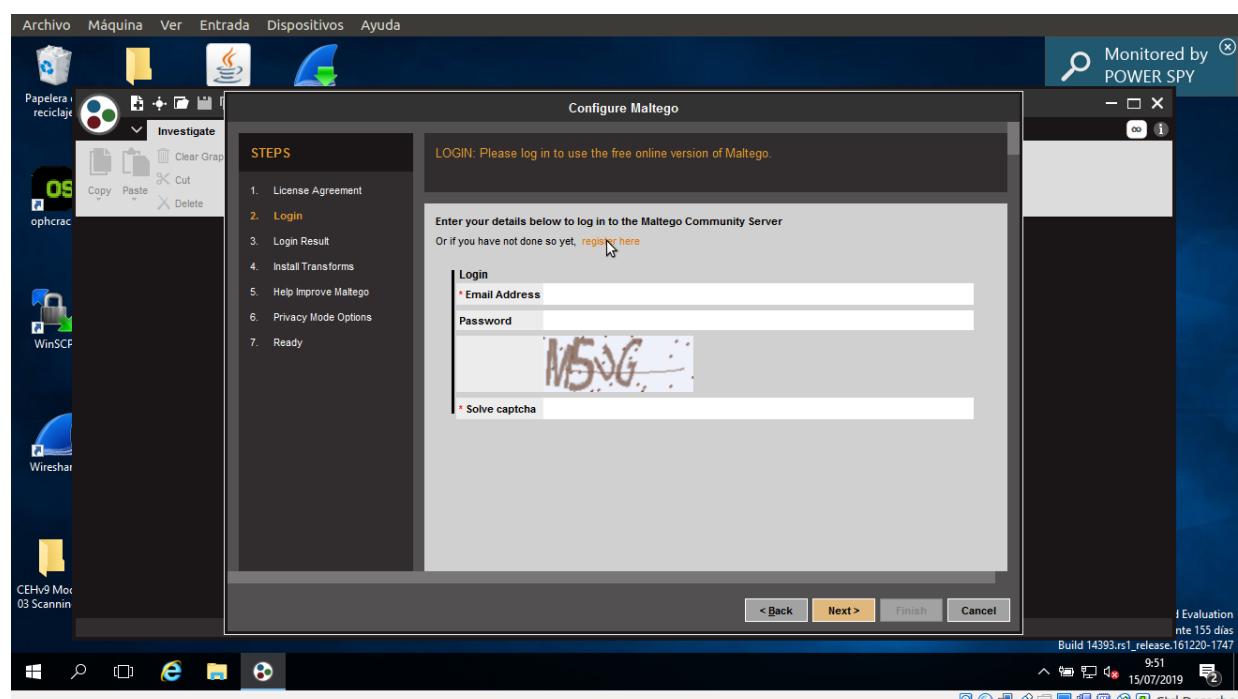
Tareas del laboratorio

1. Inicie un navegador web, escriba la URL **www.google.com** en la barra de direcciones y presione Intro

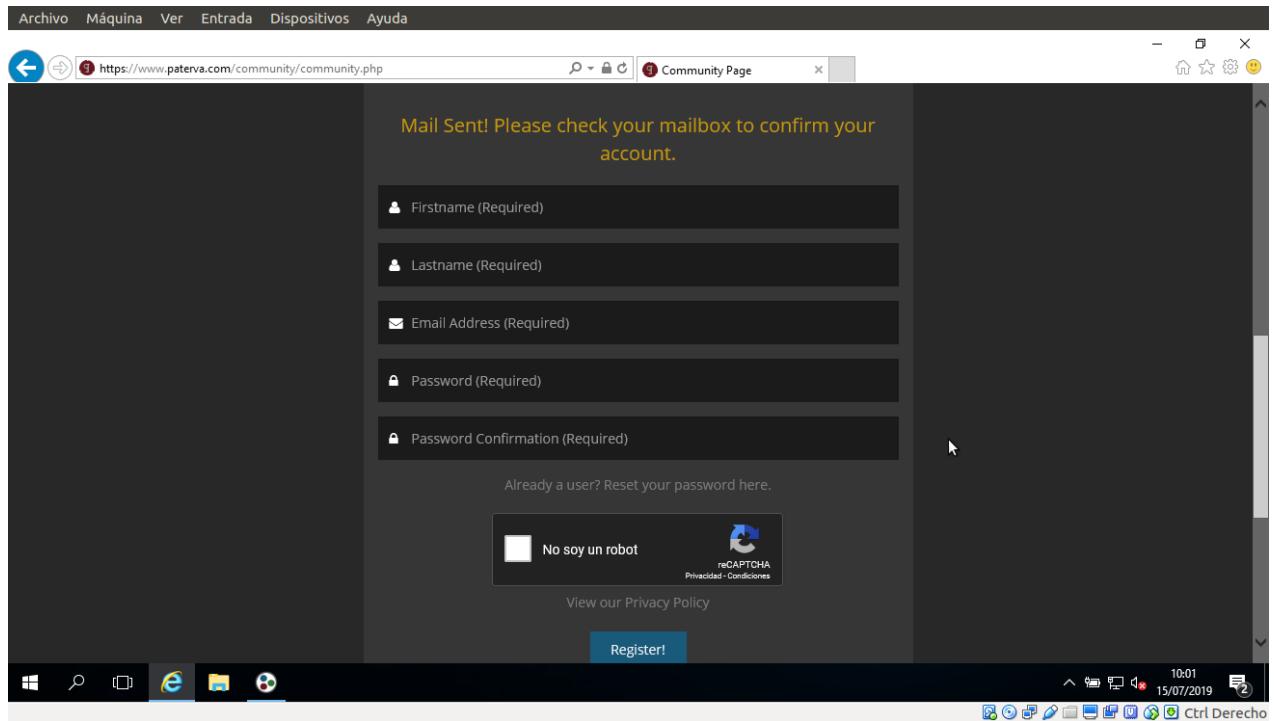
- Escriba el objetivo en el campo de búsqueda y presione Entrar. La URL es www.certifiedhacker.com.
- anote la URL y cierre el navegador web. Ejecute Maltego desde la pantalla de aplicaciones.
- Aparece un asistente de bienvenida en la GUI de Maltego. Haga clic en **Siguiente**.



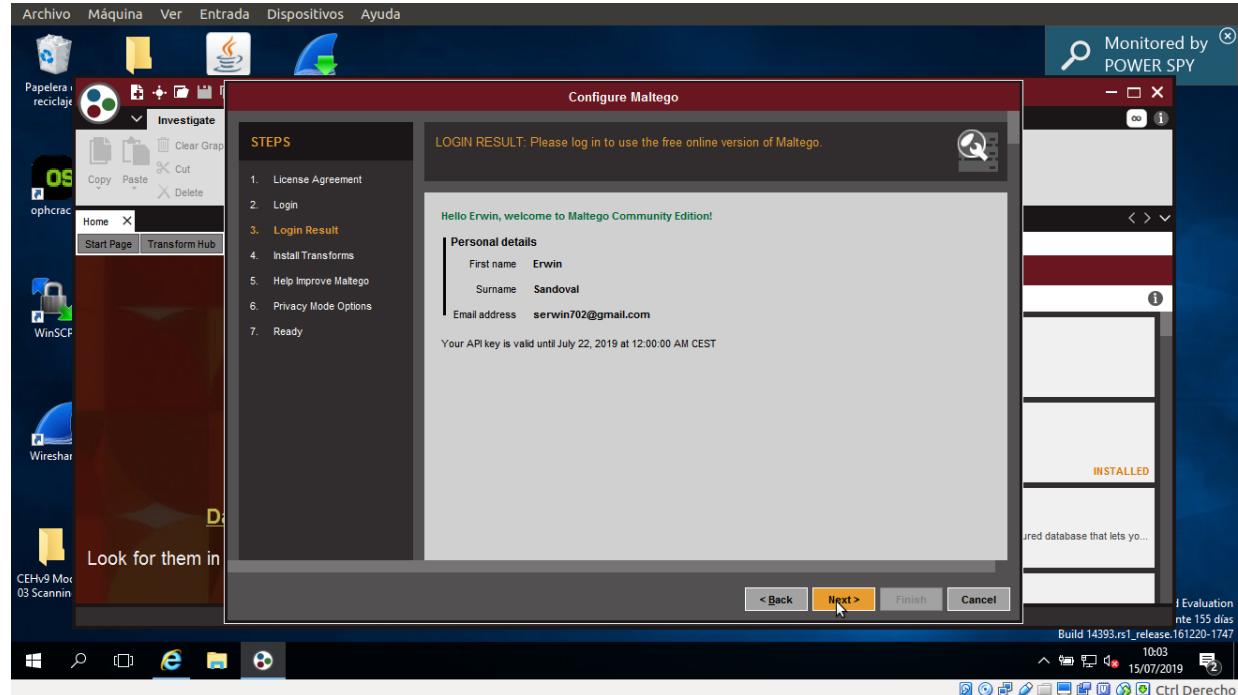
- Será redirigido a la sección de inicio de sesión. Haga clic en **registrarse aquí**



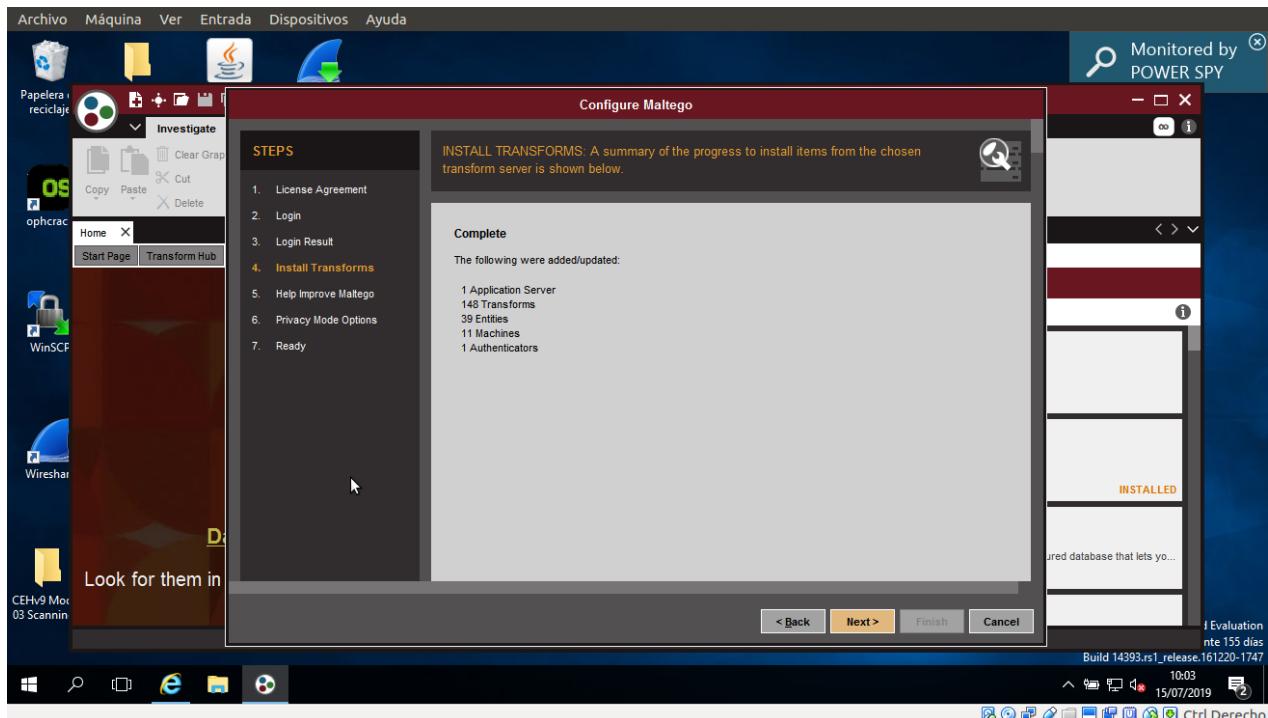
6. Registra tu cuenta y actívala.



7. Vuelva al asistente de configuración e ingrese la dirección de correo electrónico y la contraseña especificadas al momento del registro, resuelva el captcha y haga clic en Siguiente.
8. La sección de resultados de inicio de sesión muestra sus datos personales. Haga clic en Siguiente.



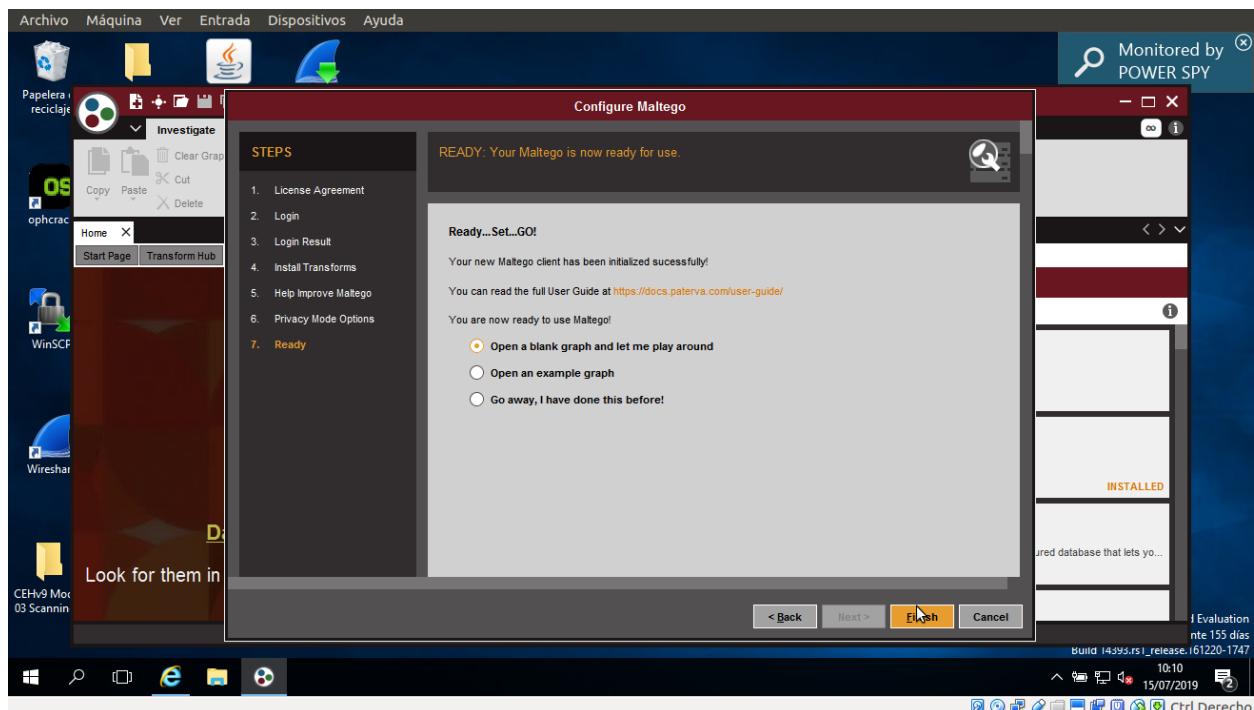
9. Aparece la sección Seleccionar semillas de transformación. Deje los ajustes por defecto y haga clic en siguiente.



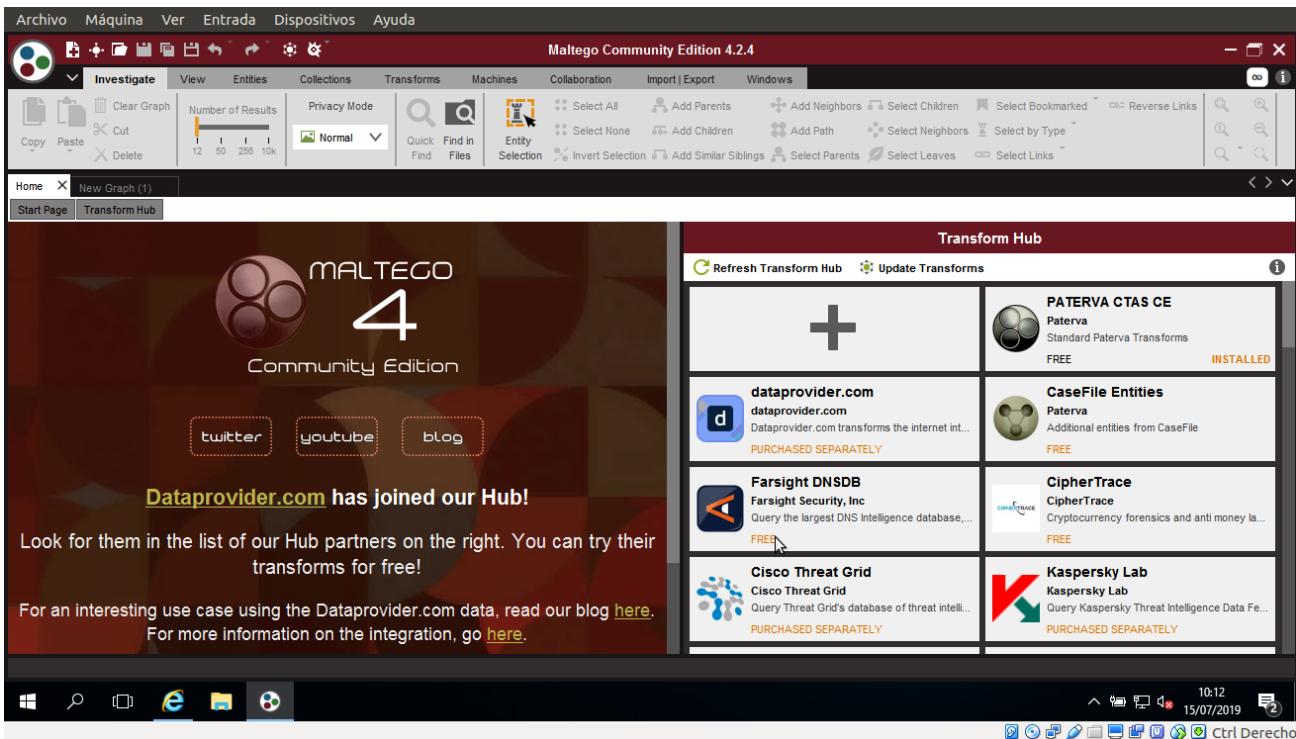
10. Aparece la sección Actualizar transformaciones. Deje la opción configurada como predeterminada y haga clic en Finalizar.

11. Aparece el asistente Iniciar una máquina. Haga clic en Cancelar para realizar la huella manualmente.

12. Seguido de esto damos finalizar.



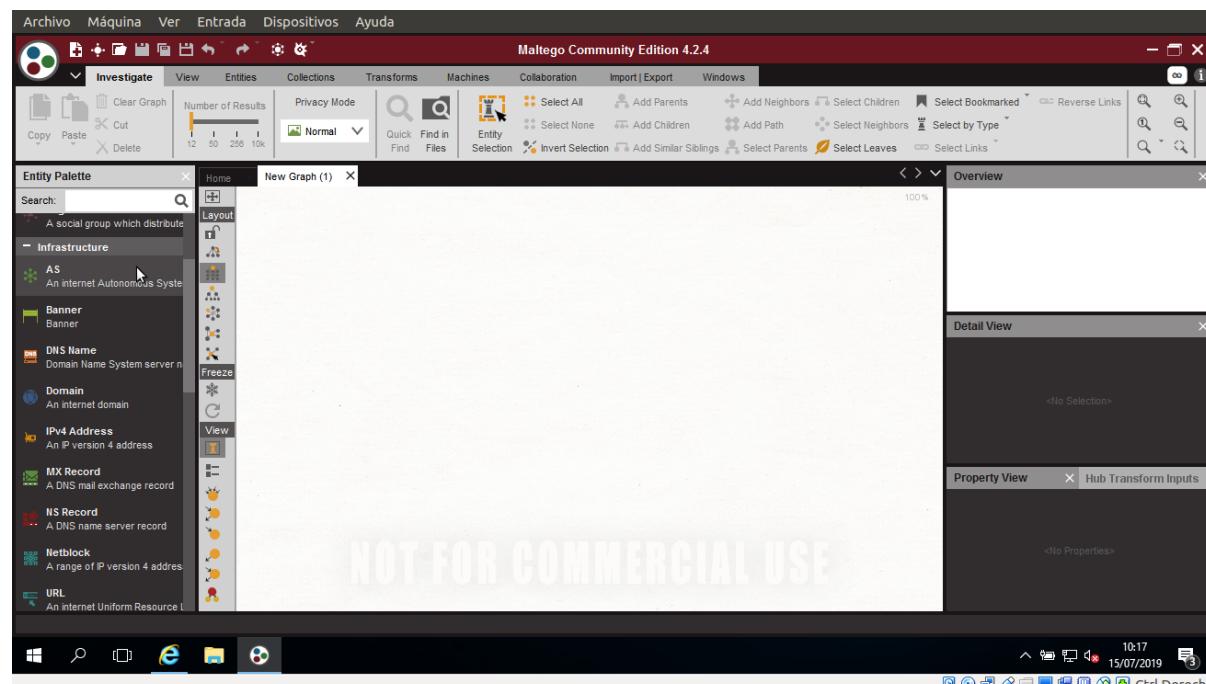
13. La interfaz gráfica de usuario de maltego aparece como se muestra en la siguiente captura de pantalla.



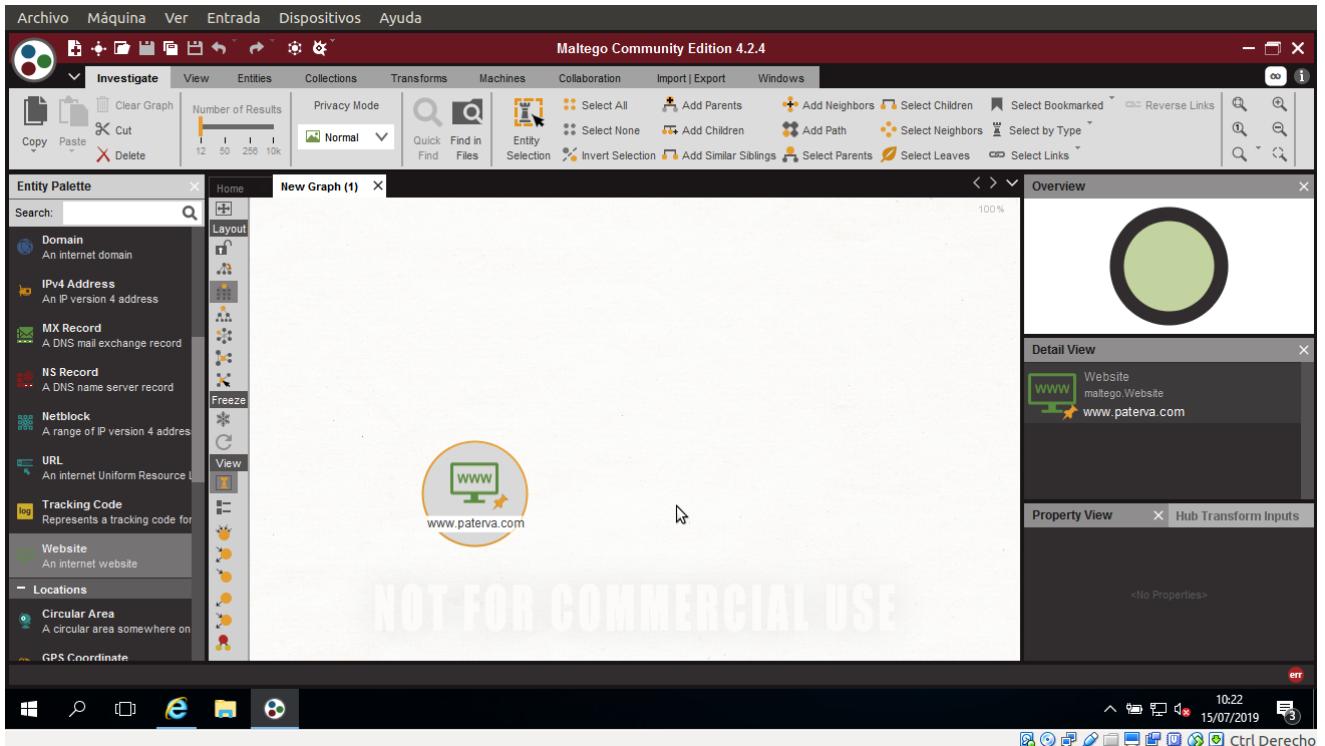
14. Haga clic en el icono ubicado en la esquina superior izquierda de la GUI (en la barra de herramientas) para comenzar un nuevo gráfico.

15. La ventana Nuevo gráfico (1) aparece junto con una Paleta en el panel izquierdo. Contiene una lista de transformaciones integradas predeterminadas.

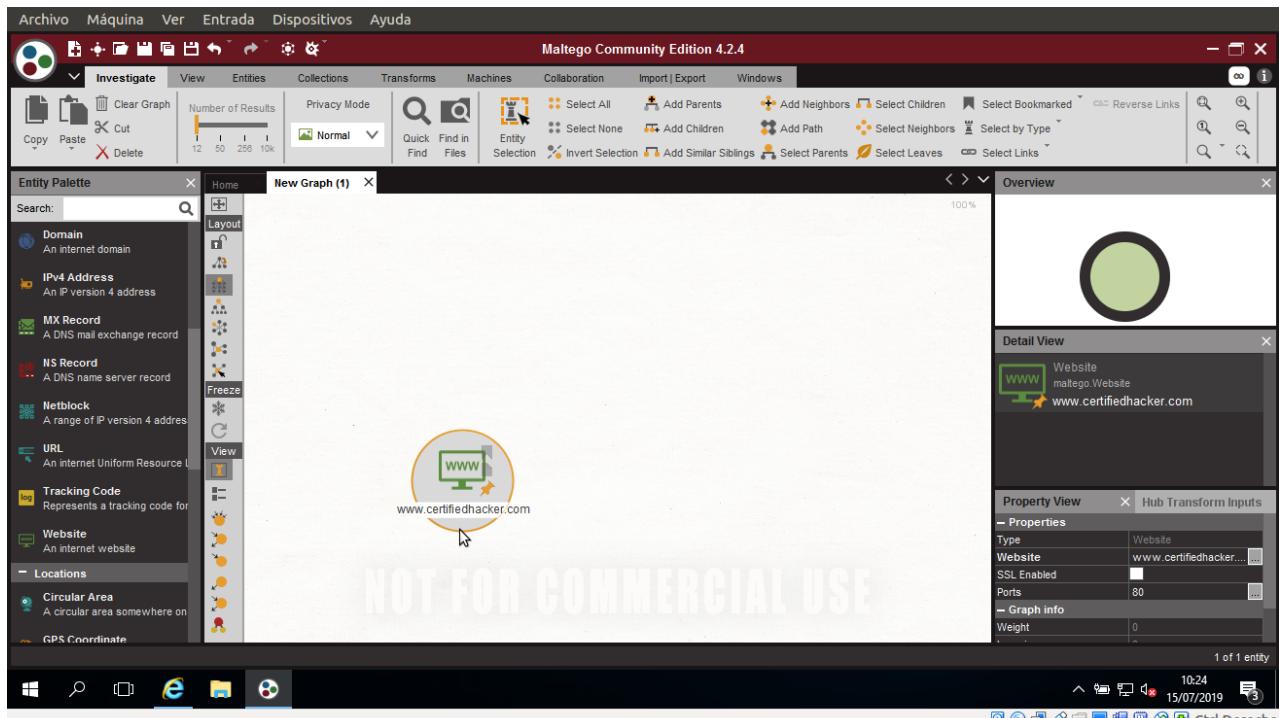
16. Expanda el nodo **Infraestructura** bajo **Paleta**.



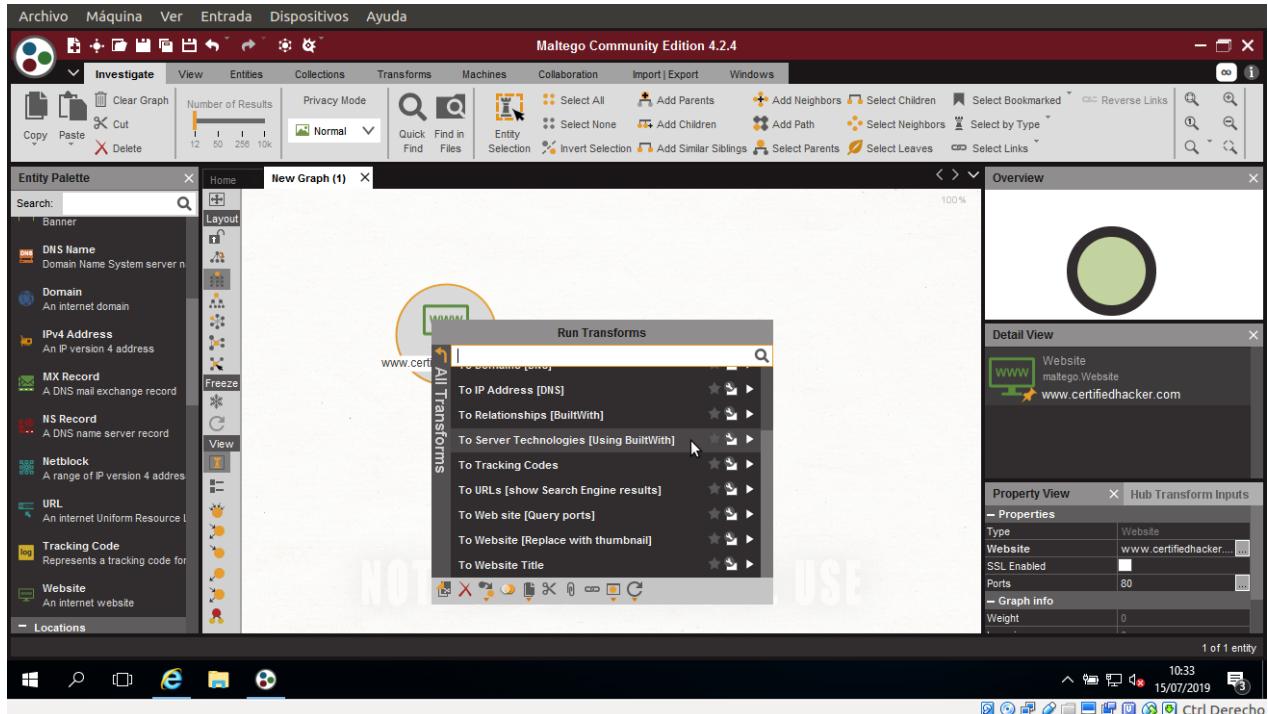
17. Expanda el nodo y observe una lista de entidades como AS, Nombre DNS, Dominio, etc.
18. Arrastre la entidad del sitio web a la sección Nuevo gráfico (1)
19. La entidad aparece en el nuevo gráfico, con la URL www.paterva.com seleccionada de forma predeterminada.



20. Haga doble clic en paterva.com y cambie el nombre del dominio a www.certifiedhacker.com. Presiona enter

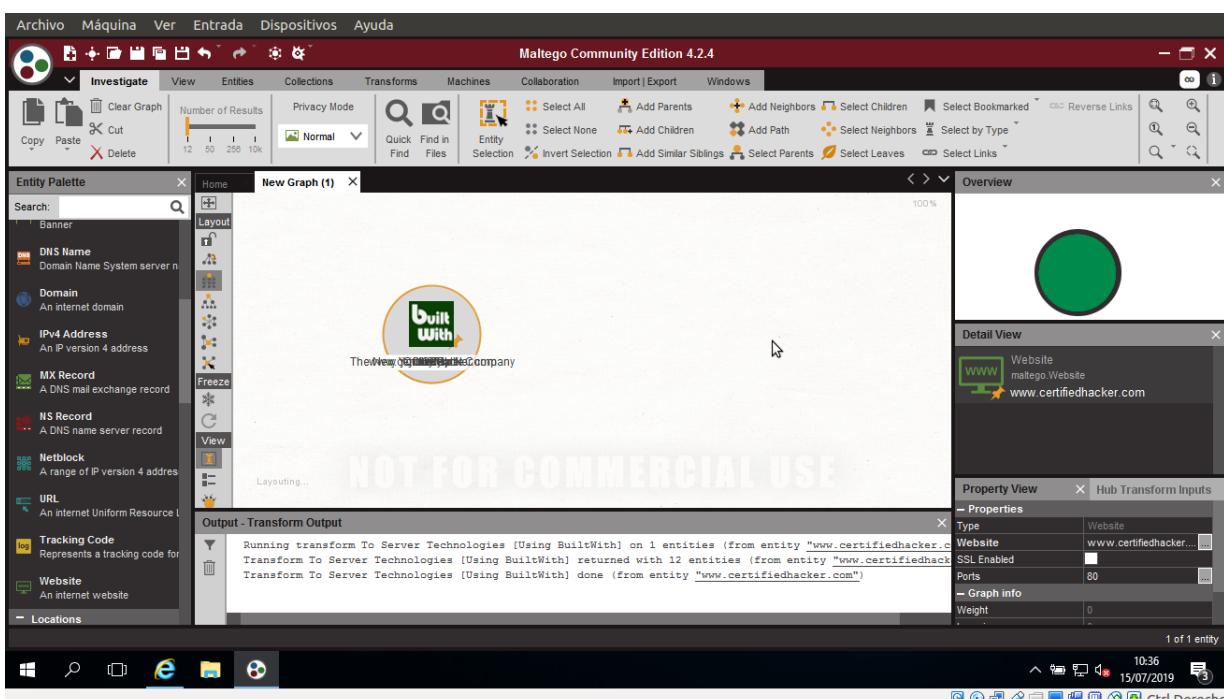


21. Haga clic con el botón derecho en la entidad y seleccione **Ejecutar transformación → Todas las transformaciones → ToServerTechnologies**

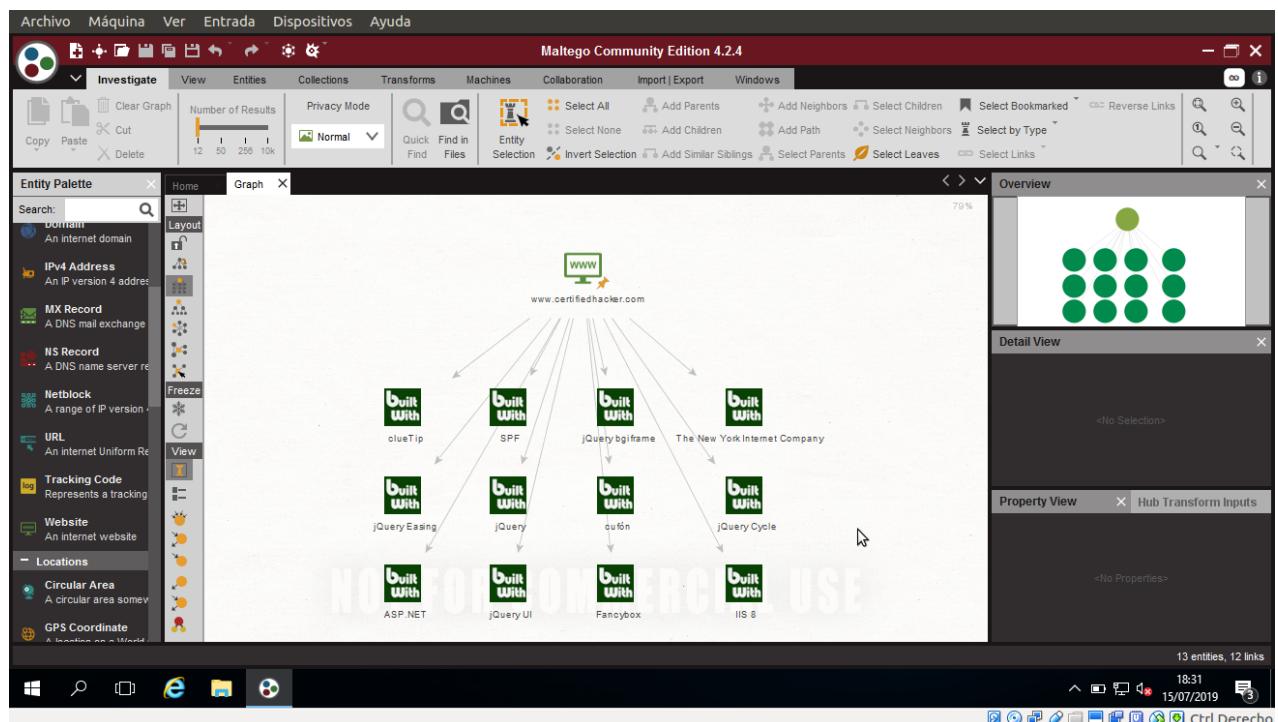


22. Aparece la ventana emergente requerida. Marque **Acepto el descargo de responsabilidad anterior y recordar estas configuraciones**. Haga clic en **Ejecutar!**.

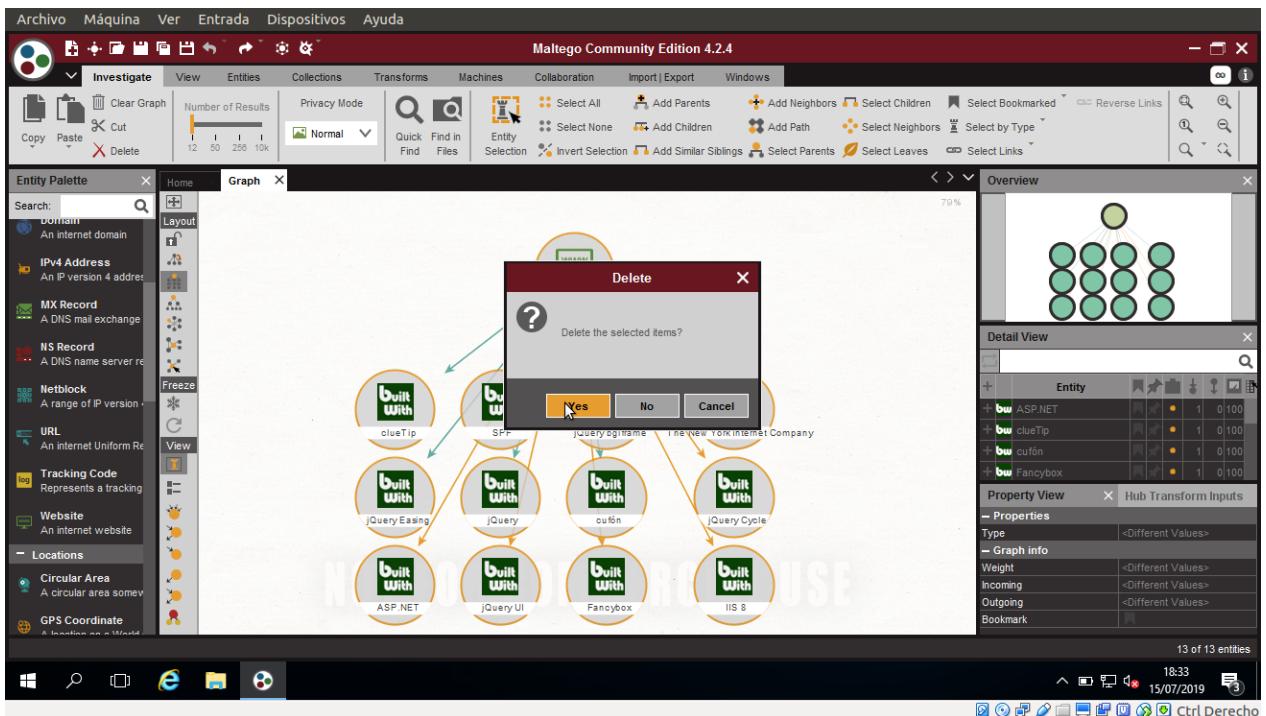
23. Maltego comienza a ejecutar la transformación ToServerTechnologies. Observa el estado en la barra de progreso.



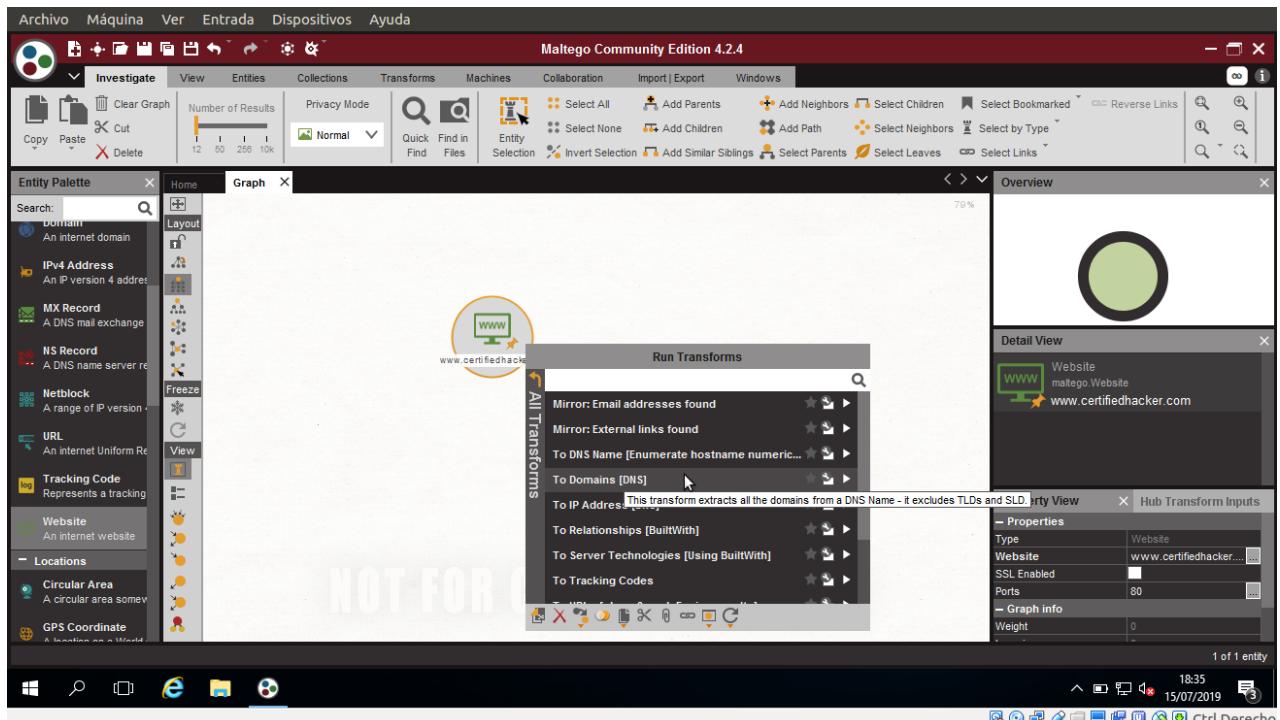
24. Una vez que Maltego completa Transforming Server Side Technologies, muestra las tecnologías implementadas en el servidor que aloja el sitio web, como se muestra en la siguiente captura de pantalla.



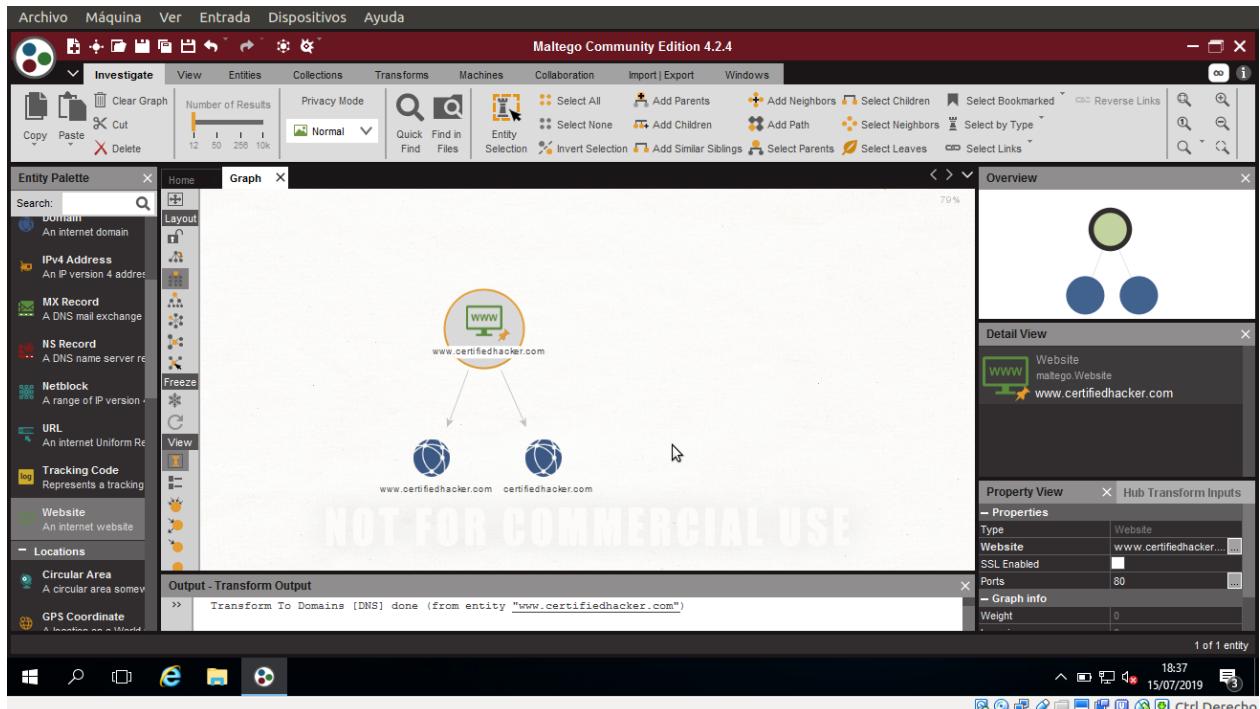
25. Después de obtener las tecnologías integradas del servidor, los atacantes pueden buscar vulnerabilidades relacionadas con cualquiera de ellas y simular técnicas de explotación para piratearlas.
26. Para iniciar una nueva transformación, seleccione todas las entidades presionando Ctrl + A en el teclado y presione Eliminar.
27. Aparece una ventana emergente de eliminación. haga clic en Sí.



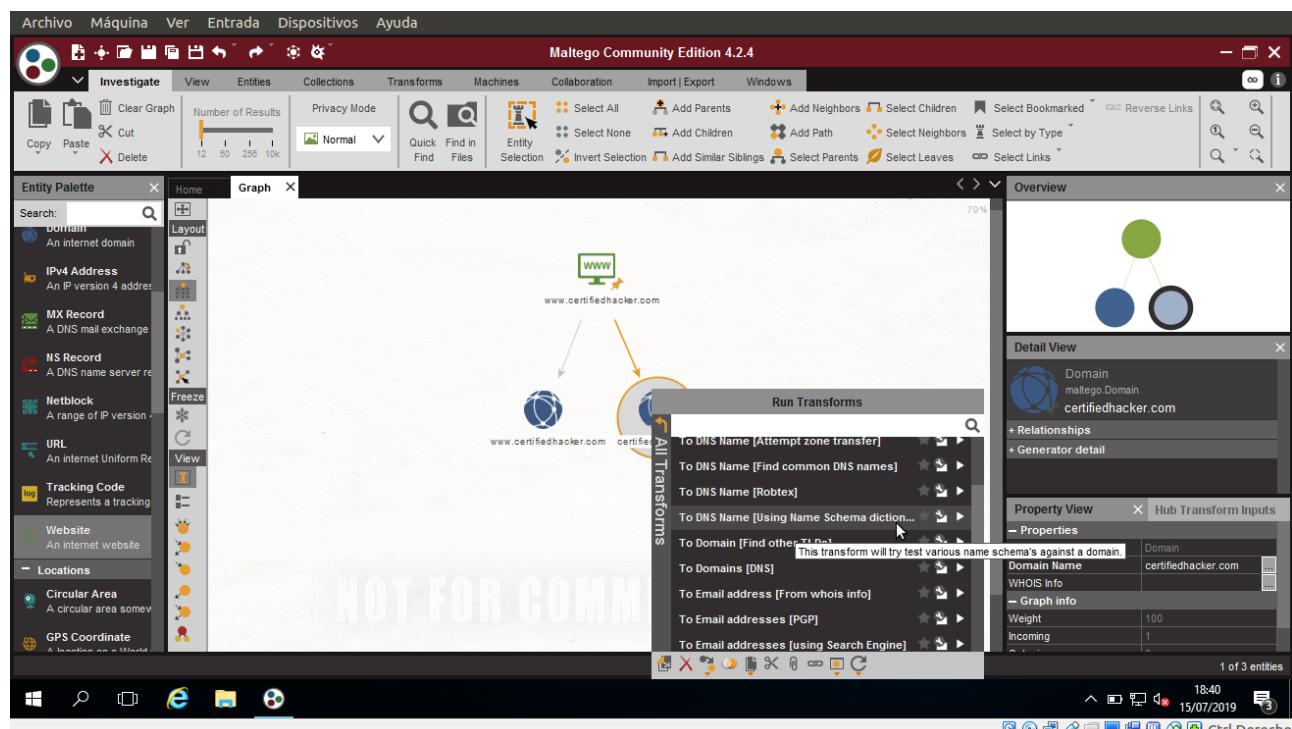
28. Siga los pasos 18-20 para crear un sitio web completo con la URL www.certifiedhacker.com.
29. Haga clic con el botón derecho en la entidad y seleccione **Ejecutar transformación -> Todas las transformaciones -> A dominios (DNS)**



30. El dominio correspondiente al sitio web se muestra, como se muestra en la siguiente captura de pantalla.

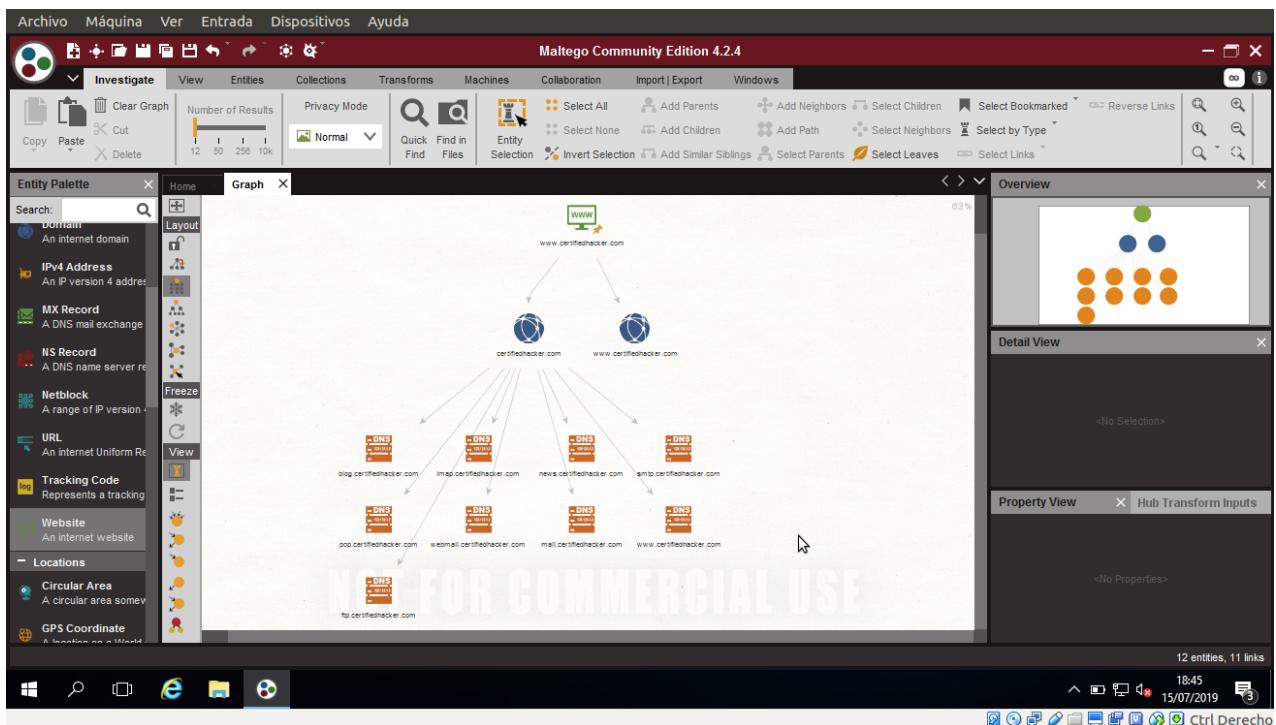


31. Haga clic con el botón derecho en la entidad y seleccione **Ejecutar transformación -> Todas las transformaciones -> DomainToDNSNameSchema**.



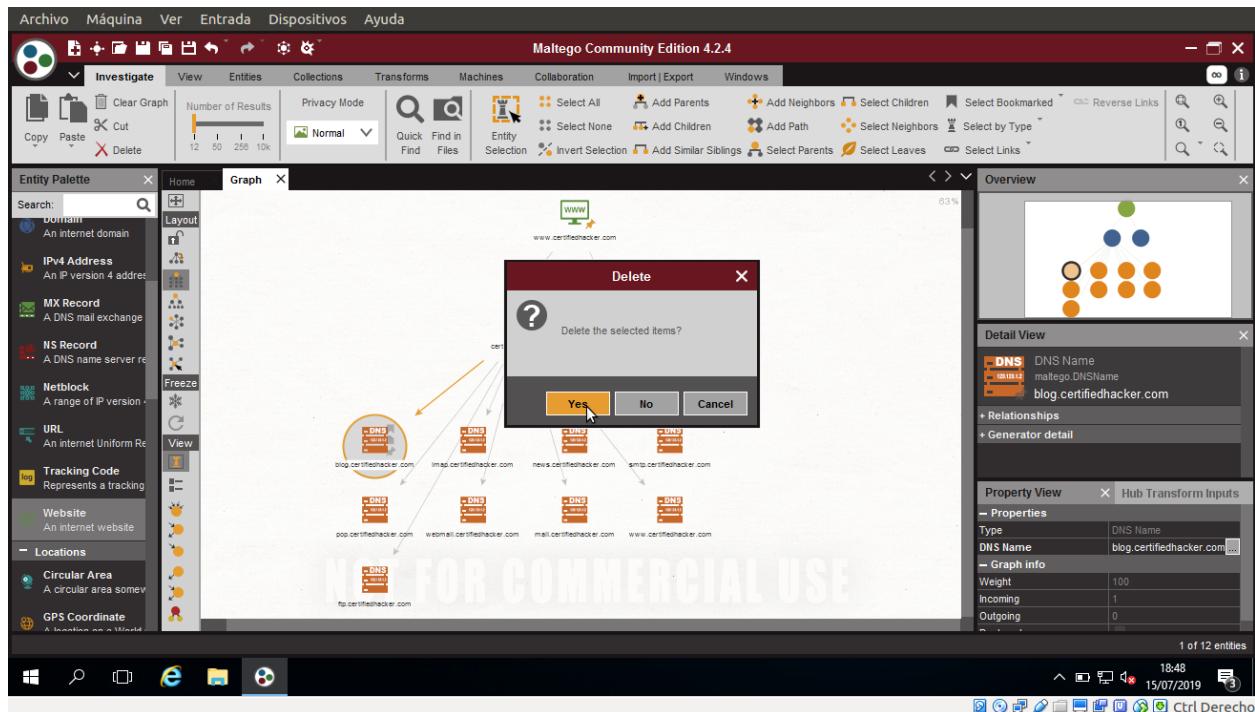
32. Aparece la ventana emergente de entrada requerida. Marque **Acepto el descargo de responsabilidad anterior y recordar estas configuraciones**. Haga clic en **Ejecutar!**

33. Esta transformación intentará probar varios esquemas de nombre contra un dominio e intentará identificar un esquema de nombre específico para el dominio como se muestra en la siguiente captura de pantalla.

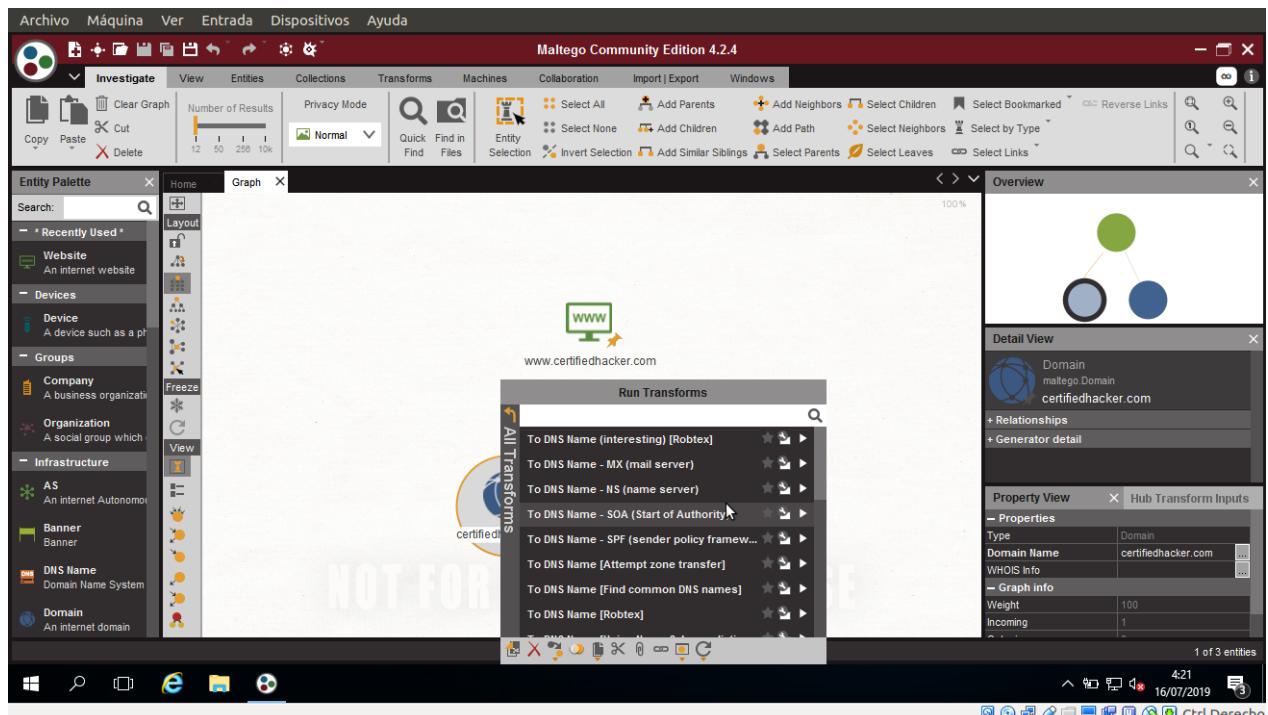


34. Después de identificar el esquema de nombres, los atacantes intentan simular varias técnicas de explotación para obtener información confidencial relacionada con los esquemas de nombres resultantes. Por ejemplo, un atacante puede implementar un ataque de fuerza o diccionario para iniciar sesión en ftp.certifiedhacker.com y obtener información confidencial.

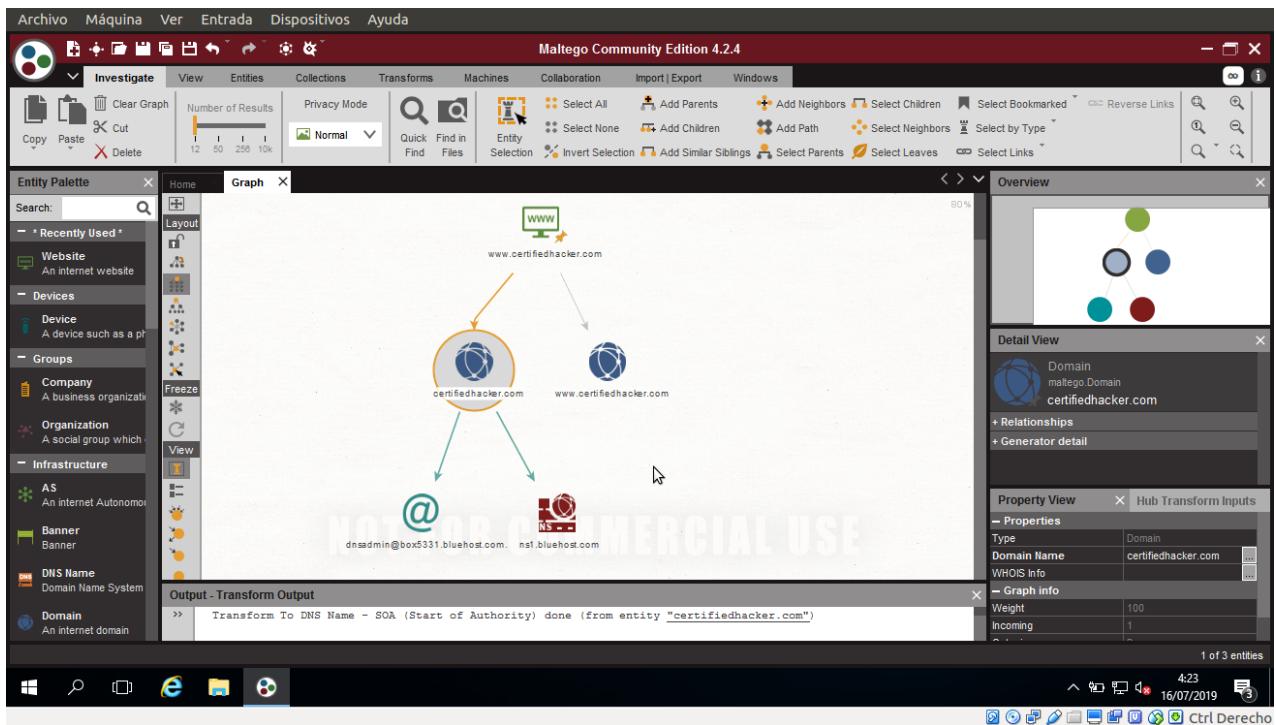
35. Seleccione solo los esquemas de nombre arrastrándolos y eliminándolos.



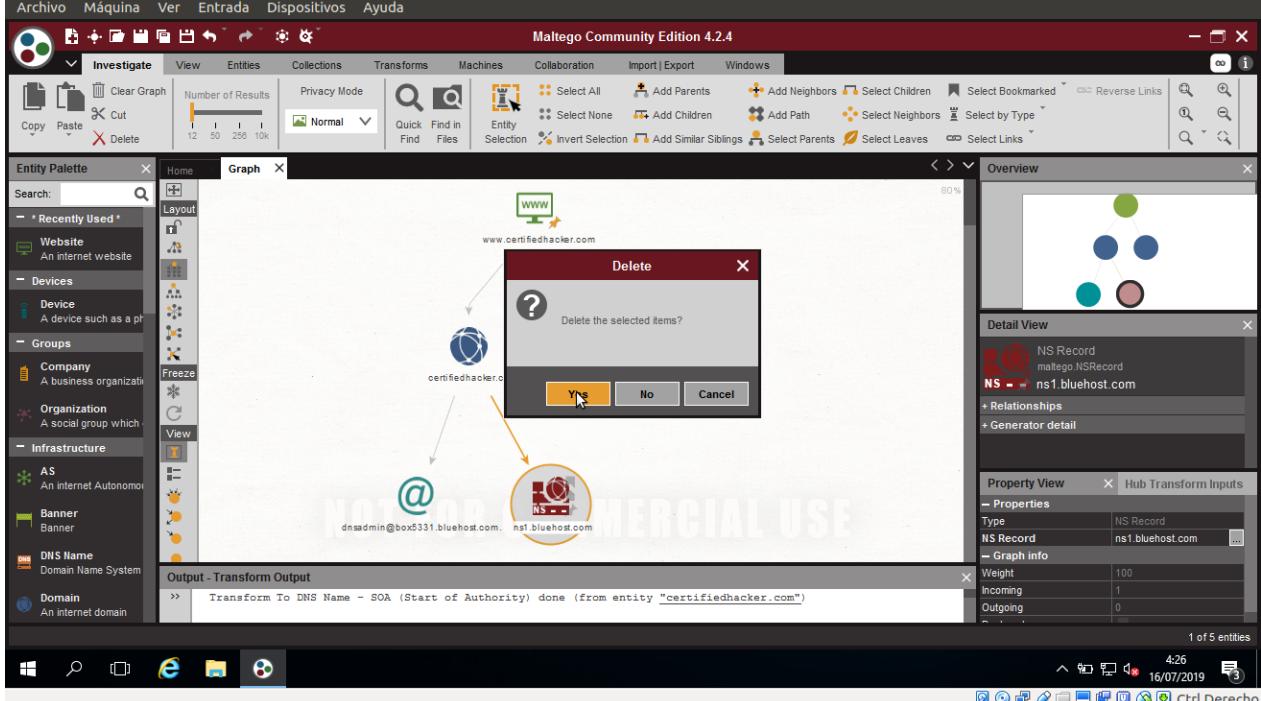
36. Haga clic con el botón derecho en la entidad y seleccione Ejecutar transformación -> Todas las transformaciones -> DomainToSOAInformation.



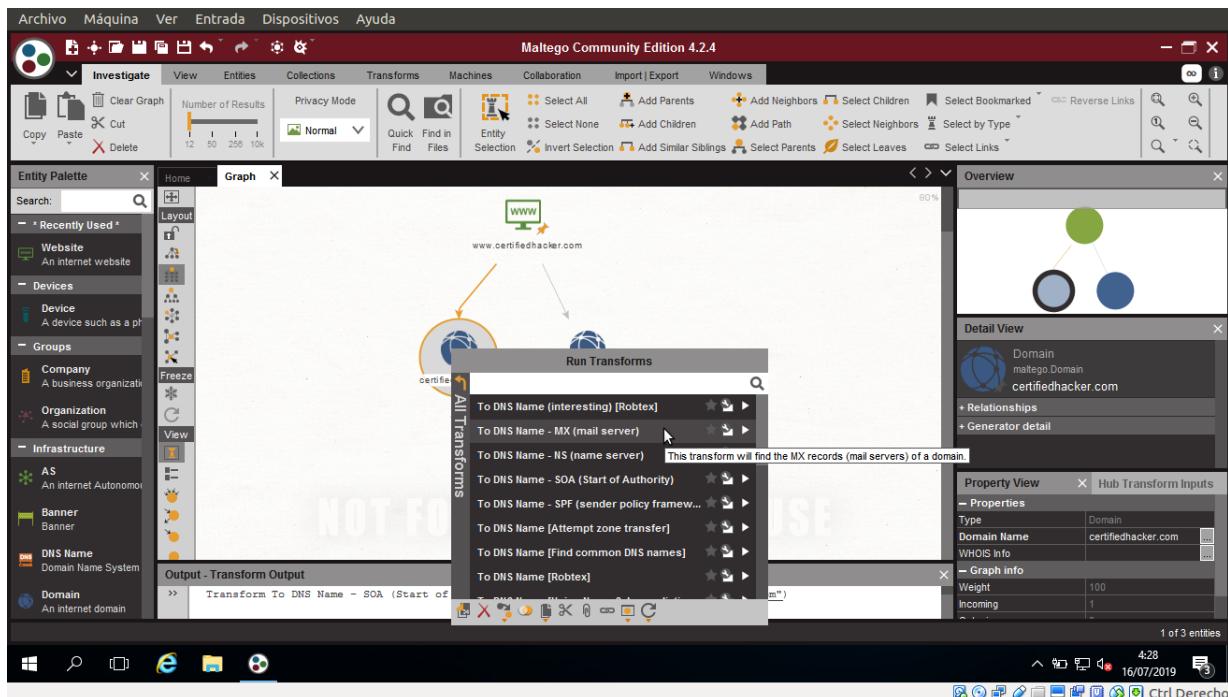
37. Esto devuelve el servidor de nombres primario y el correo electrónico del administrador del dominio. Como se muestra en la siguiente captura.



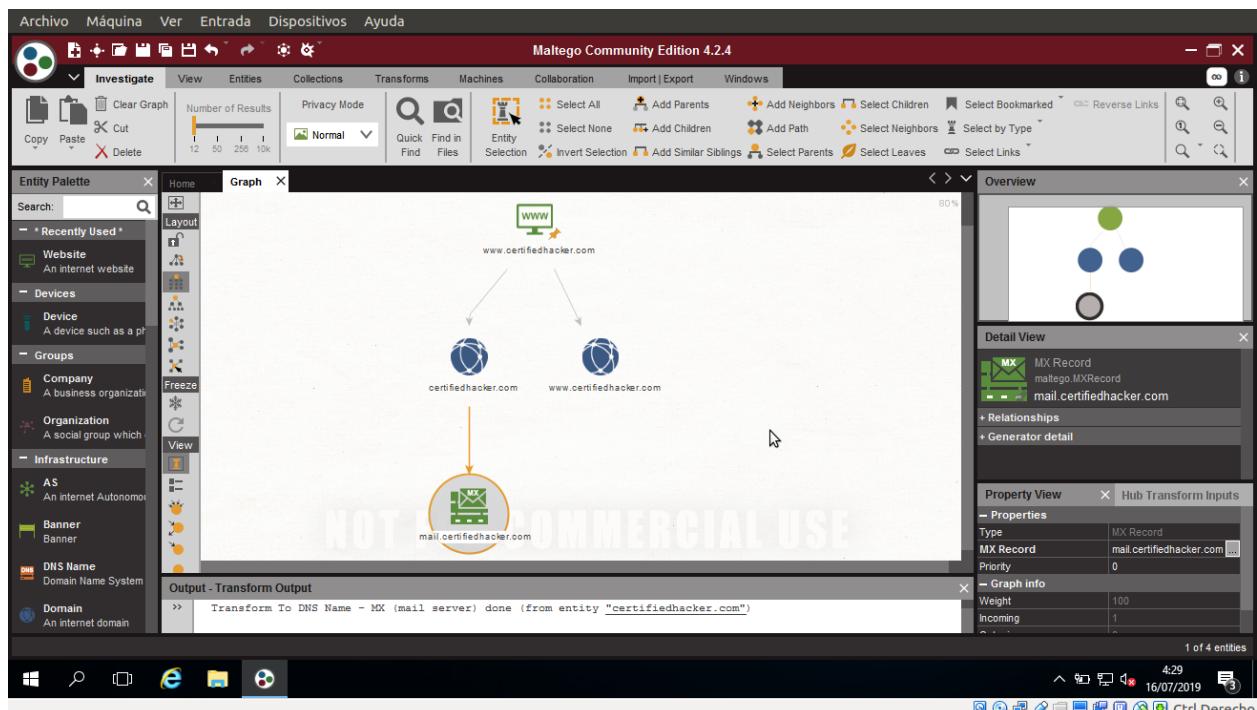
38. Al extraer la información relacionada con SOA, intente encontrar vulnerabilidades en sus servicios y arquitecturas y explotarlas.
39. Seleccione el servidor de nombres y el correo electrónico arrastrando para eliminarlos.



40. Haga clic con el botón derecho en la entrada y seleccione Ejecutar transformación → toda transformación → A DNS Name-MX (servidor de correo).

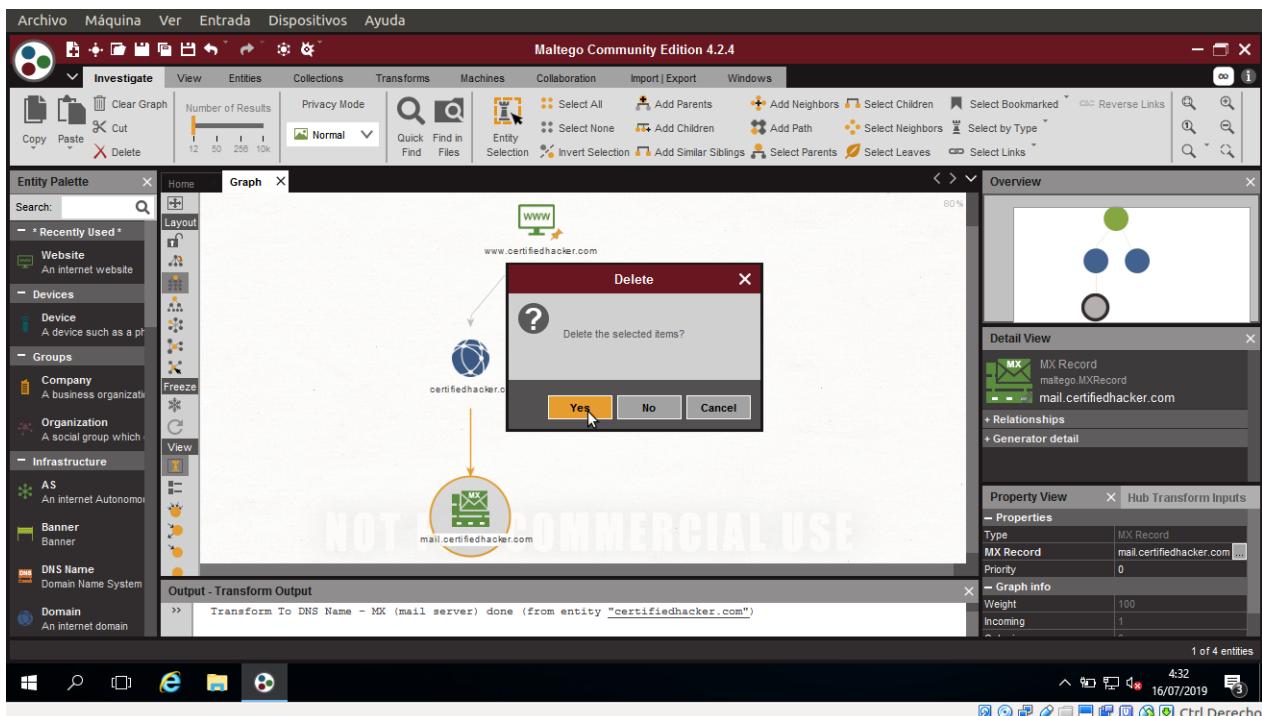


41. esta transformación devuelve el servidor de correo asociado con el dominio certifiedhacker.com, como se muestra en la siguiente captura:

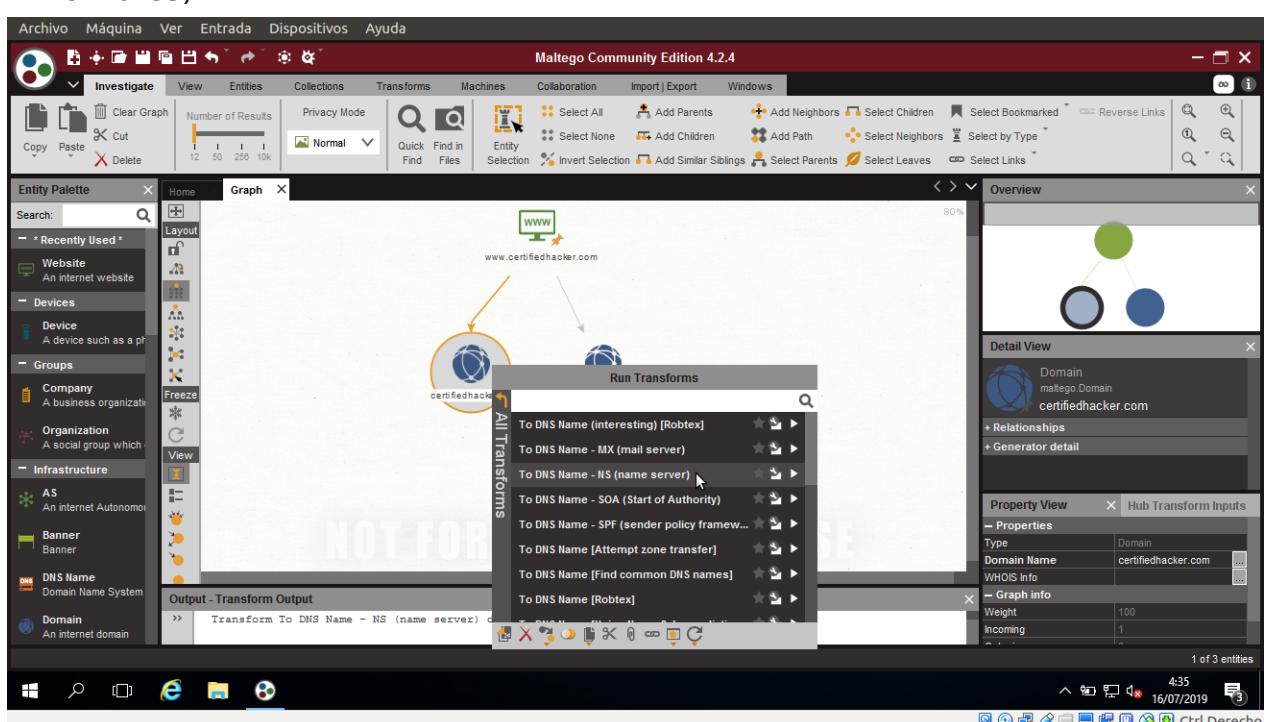


42. Al identificar el servidor de intercambio de correo, los atacantes intentan explotar las vulnerabilidades en el servidor y, por lo tanto, lo utilizan para realizar actividades maliciosas, como enviar correos electrónicos no deseados.

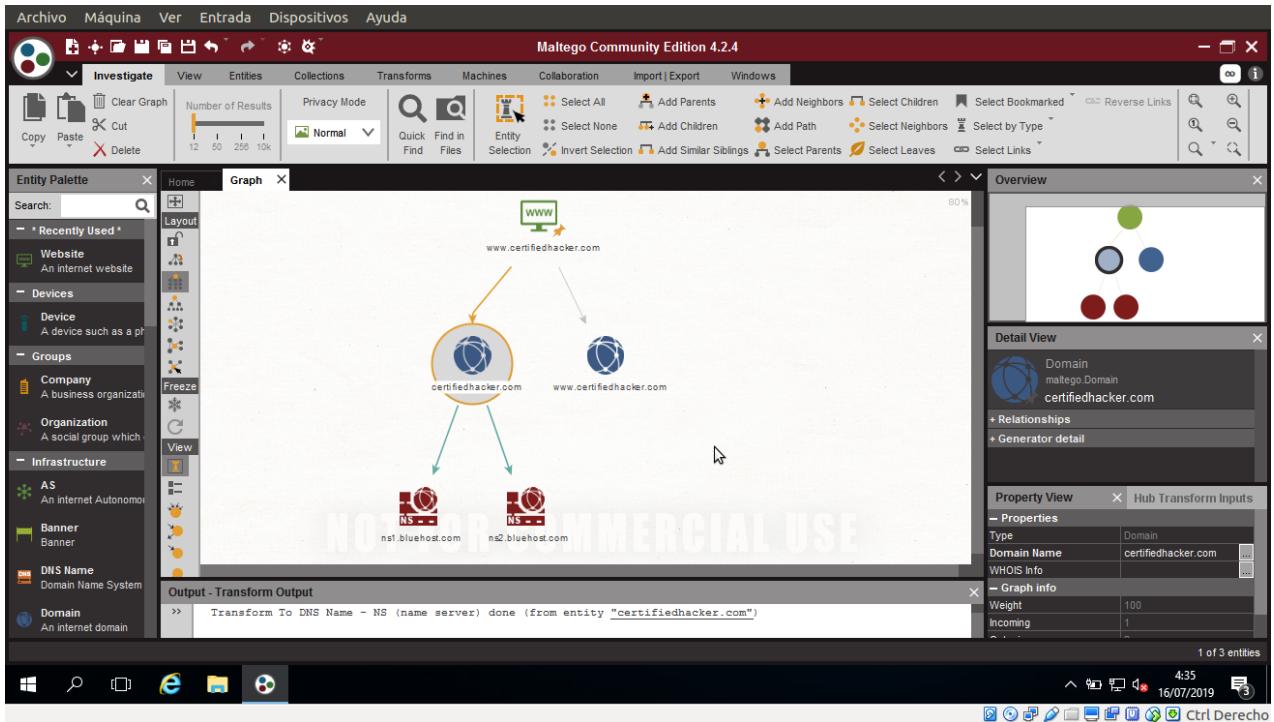
43. seleccione solo el servidor de correo arrastrándolo y eliminándolo.



44. Haga clic con el botón derecho en la entrada y seleccione Ejecutar transformación → toda transformación → A DNS Name-MX (servidor de nombres).



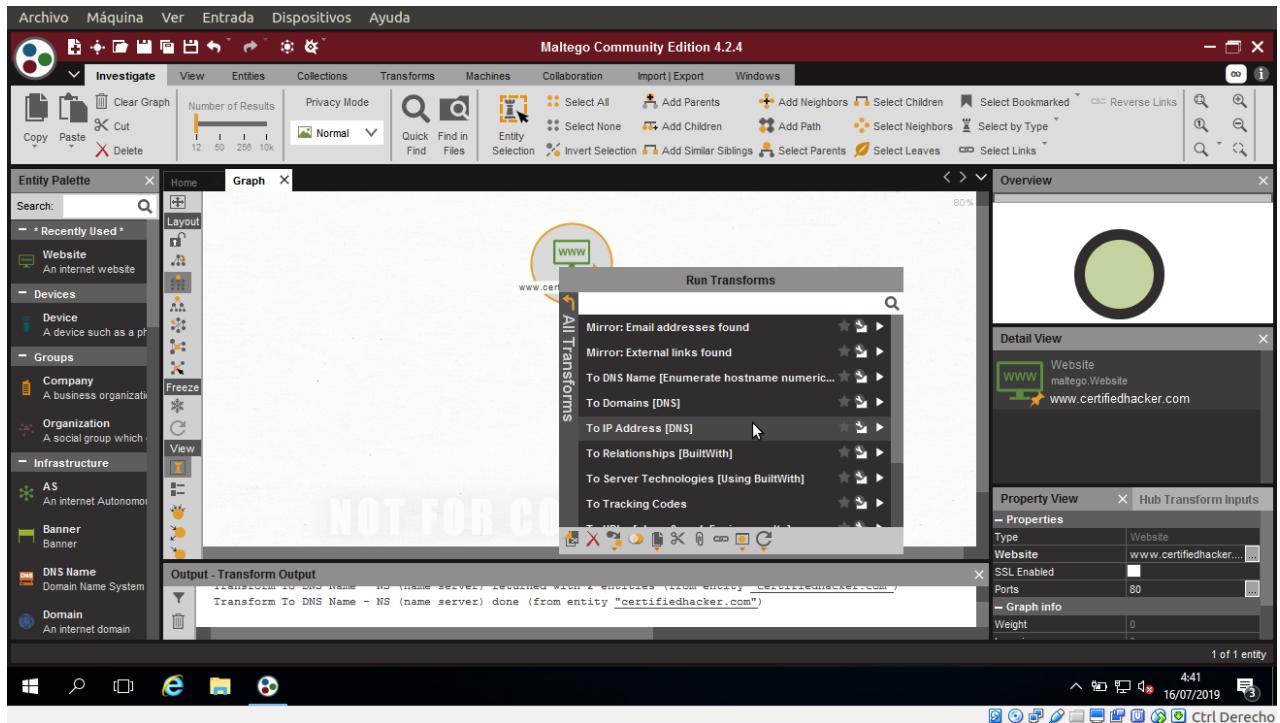
45. Esto devuelve los nombres asociados con el dominio. Como se muestra en la siguiente captura.



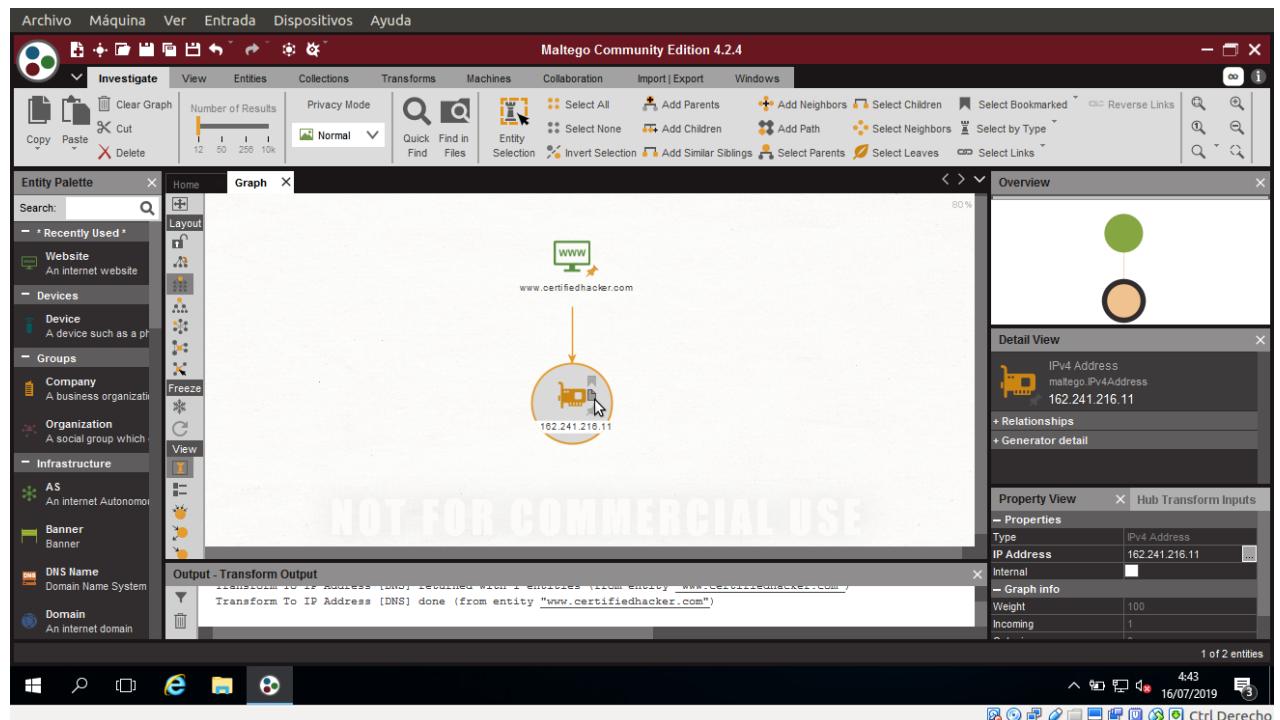
46. Al identificar el servidor de nombres primario, un atacante puede implementar varias técnicas para explotar el servidor y, por lo tanto, realizar actividades maliciosas, como el secuestro de DNS y la redirección de URL.

47. seleccione tanto el dominio como el servidor de nombres arrastrándolos y eliminándolos.

48. Haga clic con el botón derecho en la entrada y seleccione **Ejecutar transformación → toda transformación → A Dirección IP (DNS)**.

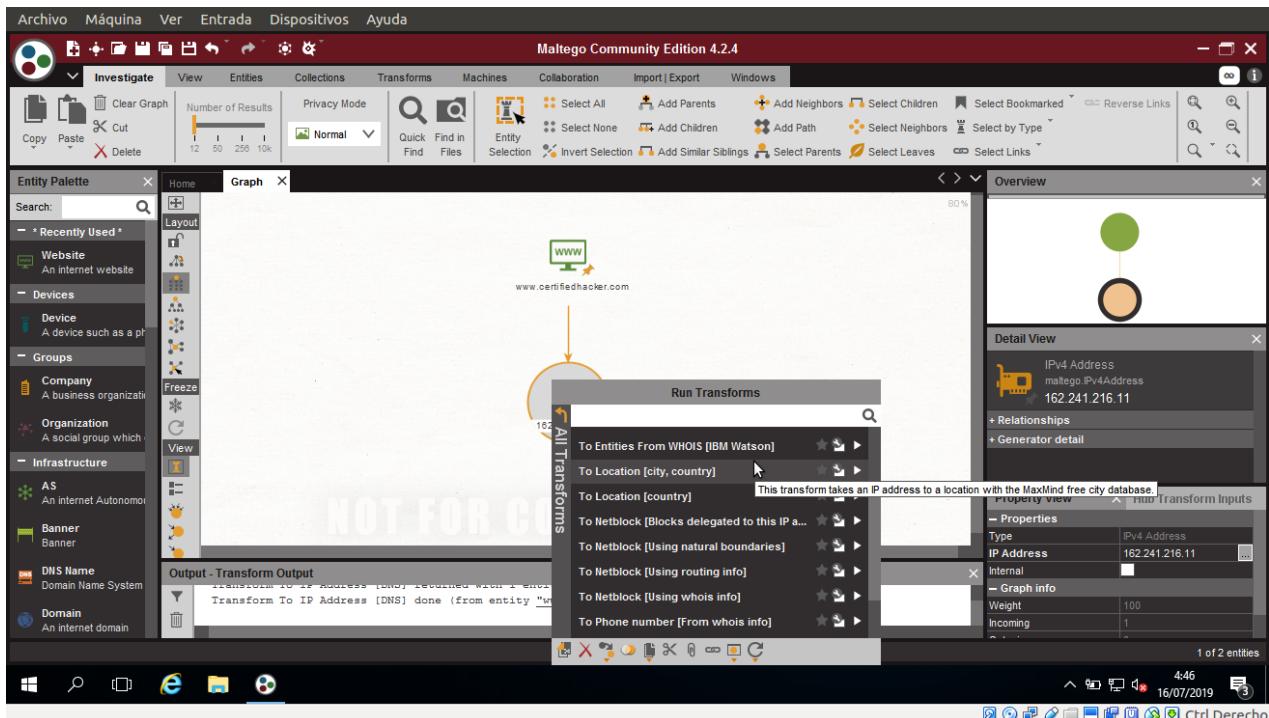


49. Esto muestra la dirección ip del sitio web, como se muestra en la siguiente captura.

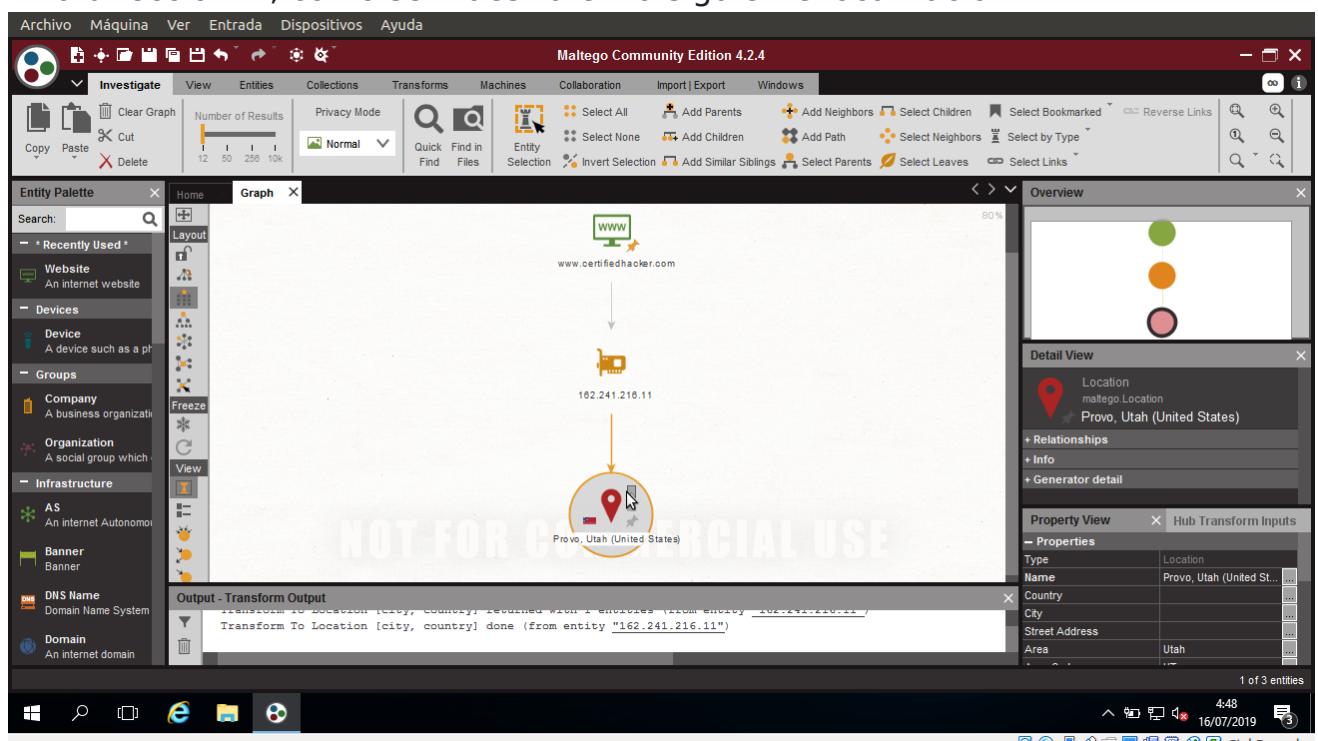


50. Al obtener la dirección IP del sitio web, un atacante puede simular varias técnicas de exploración para abrir y vulnerabilidades y, por lo tanto, intentar invadir la red y explotarlas.

51. Haga clic con el botón derecho en la entrada y seleccione **Ejecutar transformación** → **toda transformación** → **A localización (quien es API)**.



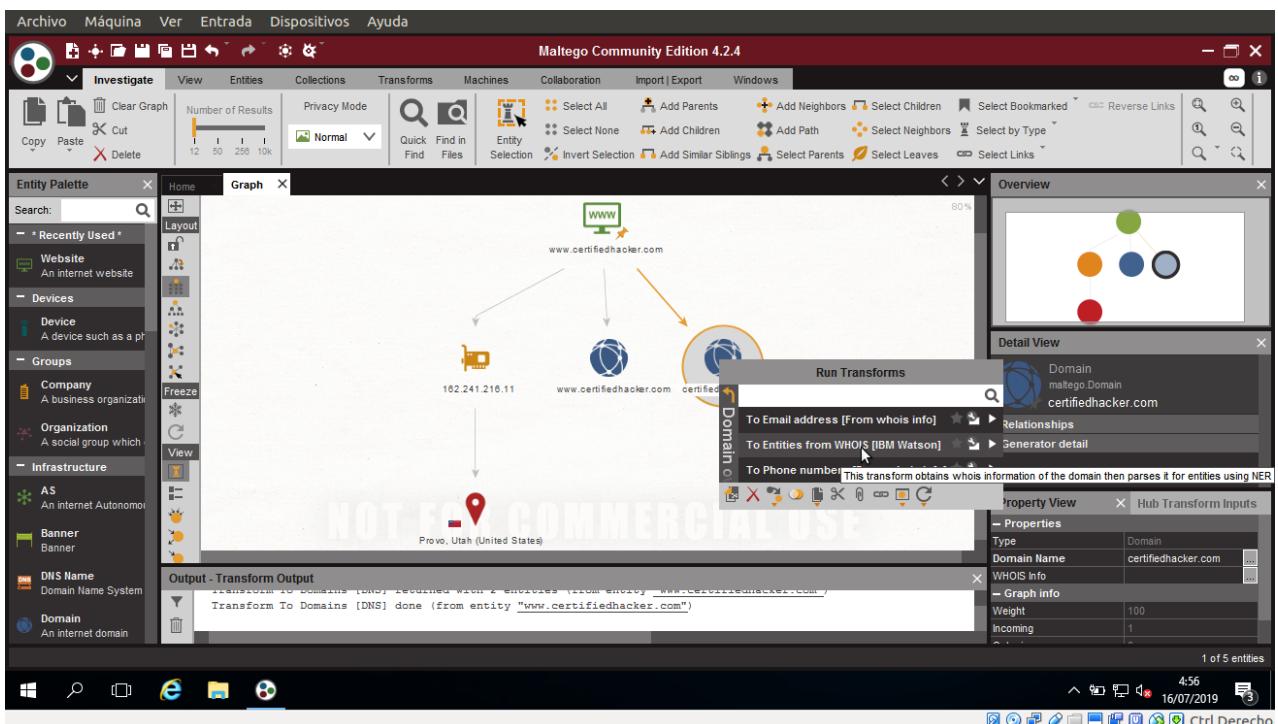
52. Esta transformación identifica la ubicación geográfica donde se encuentra la dirección IP, como se muestra en la siguiente localización.



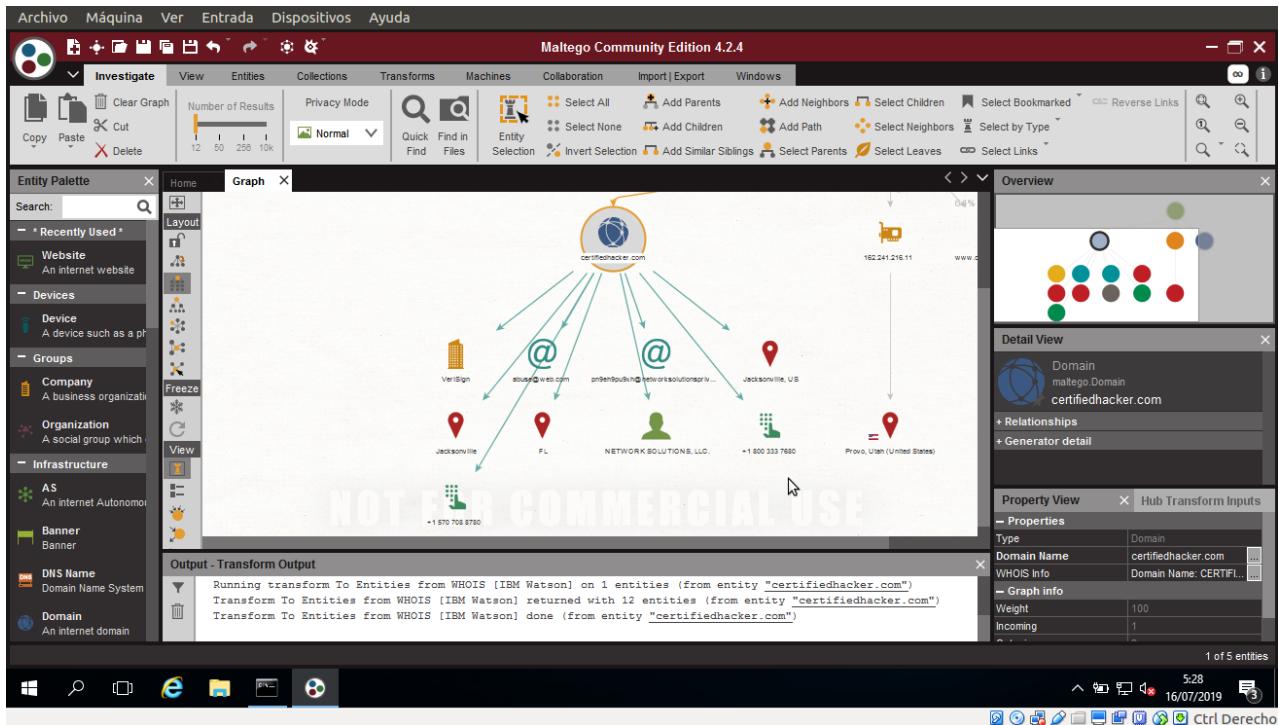
53. Al obtener la información relacionada con la ubicación geográfica, los atacantes pueden realizar ataques de ingeniería social haciendo llamadas de voz a un individuo en un intento de aprovechar información sensible.

54. Siga el paso 27 para resolver el nombre de dominio del sitio web.

55. Haga clic con el botón derecho en la entrada (certifiedhacker.com) y seleccione **Ejecutar transformación → detalle del propietario de dominio → a entidades [alchemy and Opencalais] via whois**.



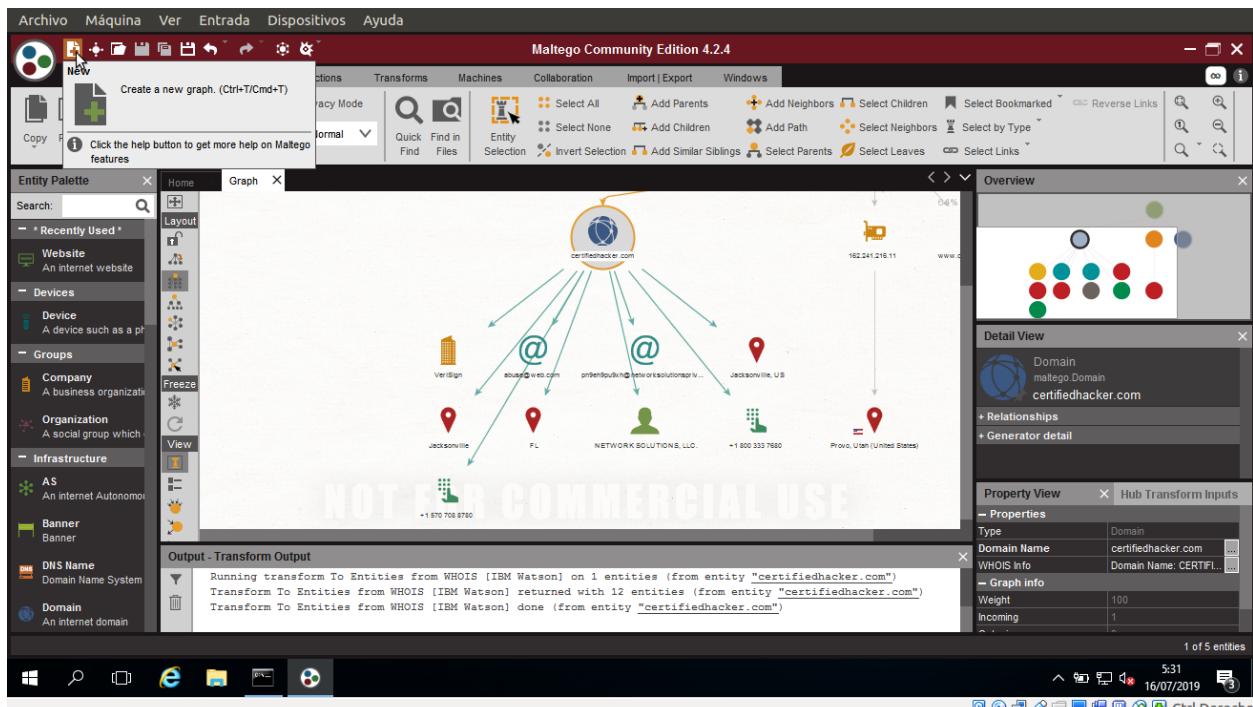
56. Esta transformación muestra las entidades pertenecientes al dominio del propietario, como se muestra en la siguiente captura.



57. Al obtener esta información, un atacante puede explotar los servidores mostrados en los resultados o simular una fuerza bruta o cualquier otra técnica de hack en la cuenta de correo del administrador y correos de phishing a los contactos en esa cuenta.

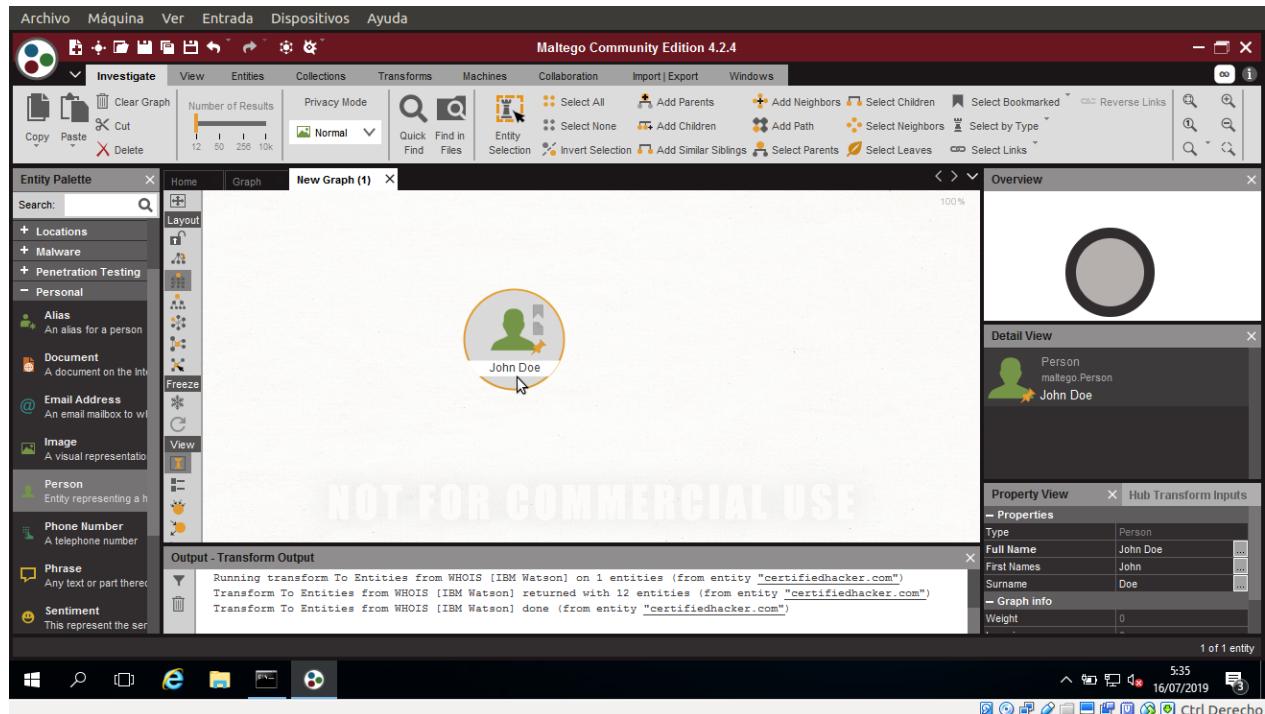
58. Realice la huella en una persona de destino para obtener la dirección de correo electrónico y el número de teléfono.

59. Haga clic en el ícono ubicado en la esquina superior izquierda de la GUI (en la barra de herramientas) para comenzar un nuevo gráfico.

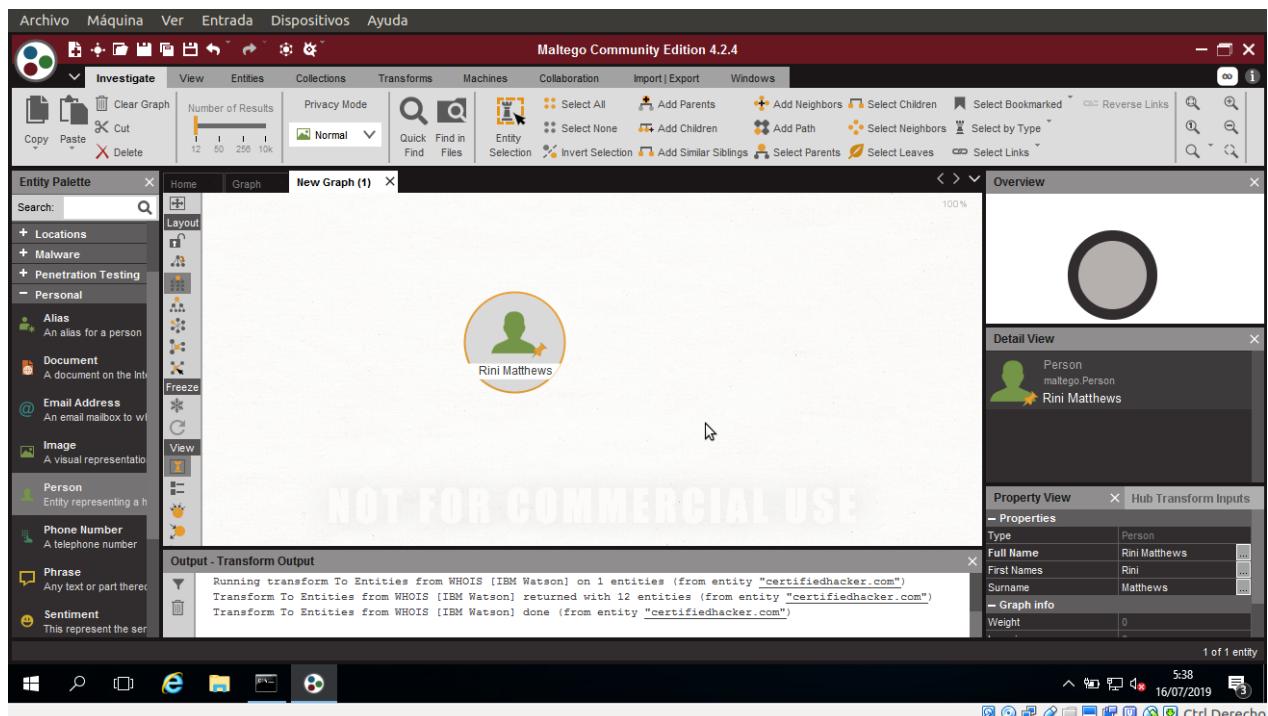


60. Aparece una nueva gráfica en maltego. expanda la pestaña **personal** de la izquierda y arrastre la entidad de **persona** a la sección Nuevo gráfico.

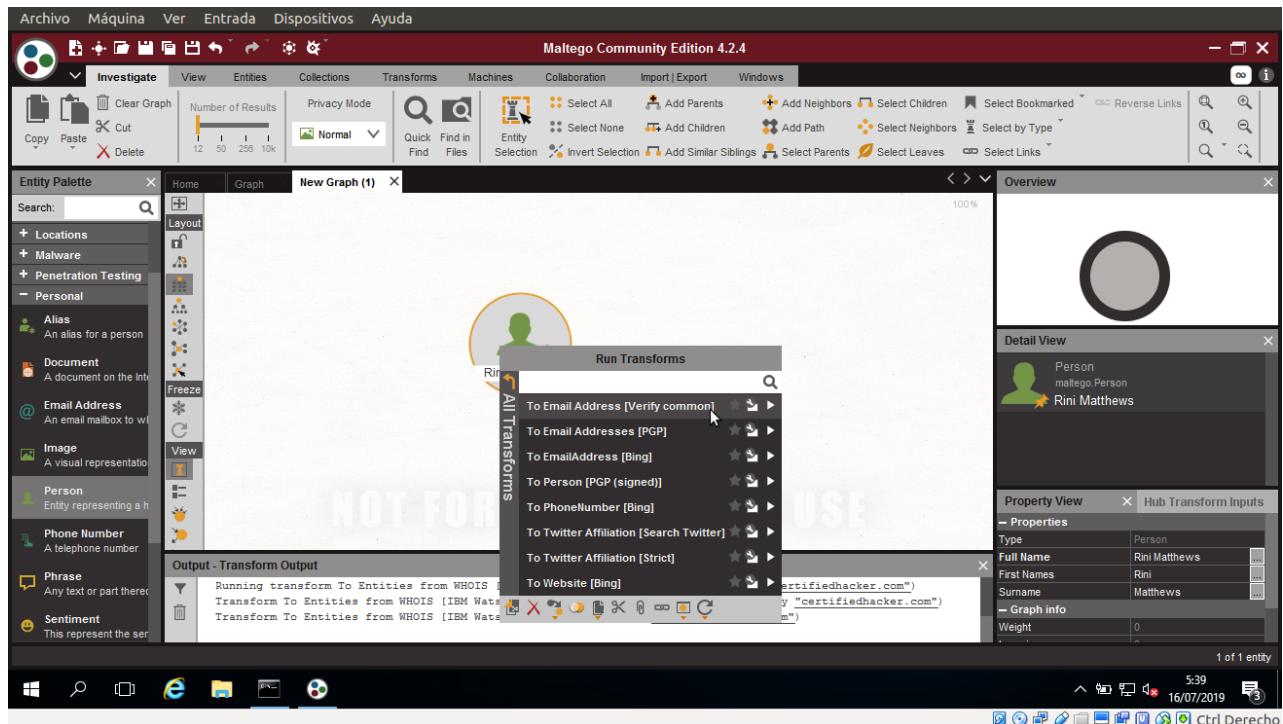
61. El nombre de la entidad se establece como John Doe por defecto.



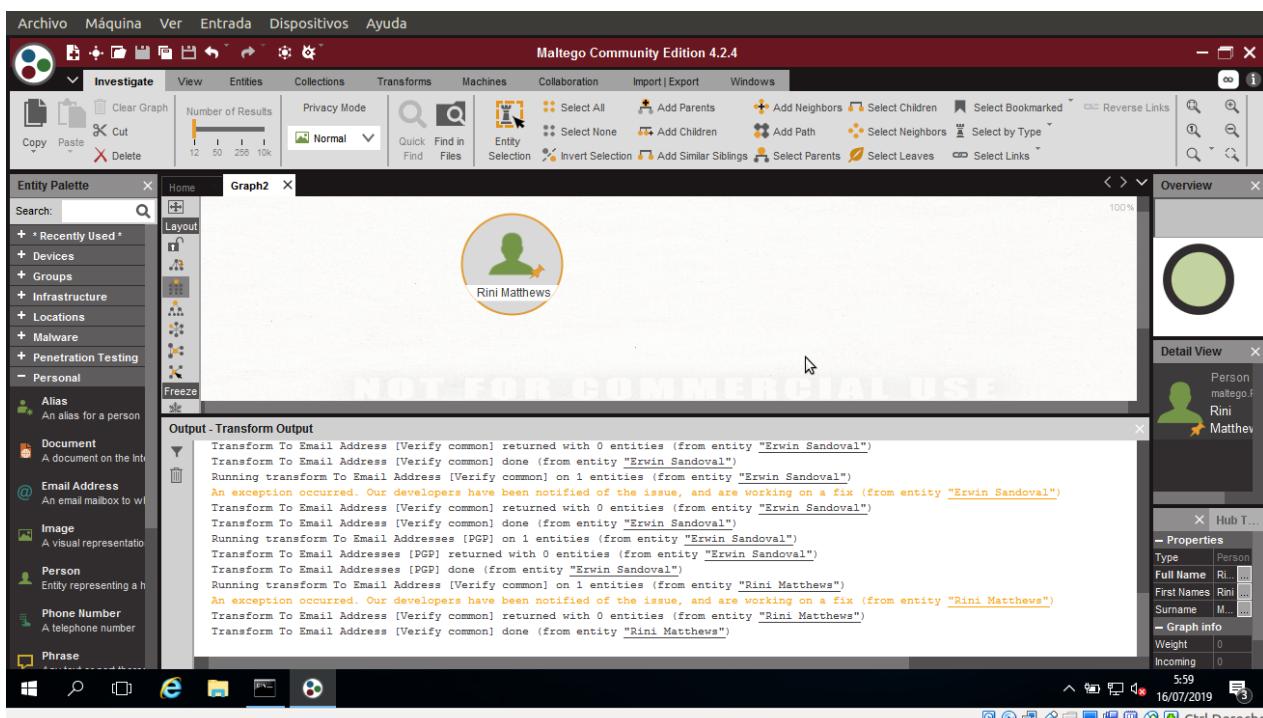
62. Para asignar el nombre de una persona objetivo, haga doble clic en John Doe y escriba el nombre de la persona (aquí, Rini Matthews).



63. Haga clic con el botón derecho en la entrada y seleccione **Ejecutar transformación** → **toda transformación** → **A Dirección de correo (verificación común)**.



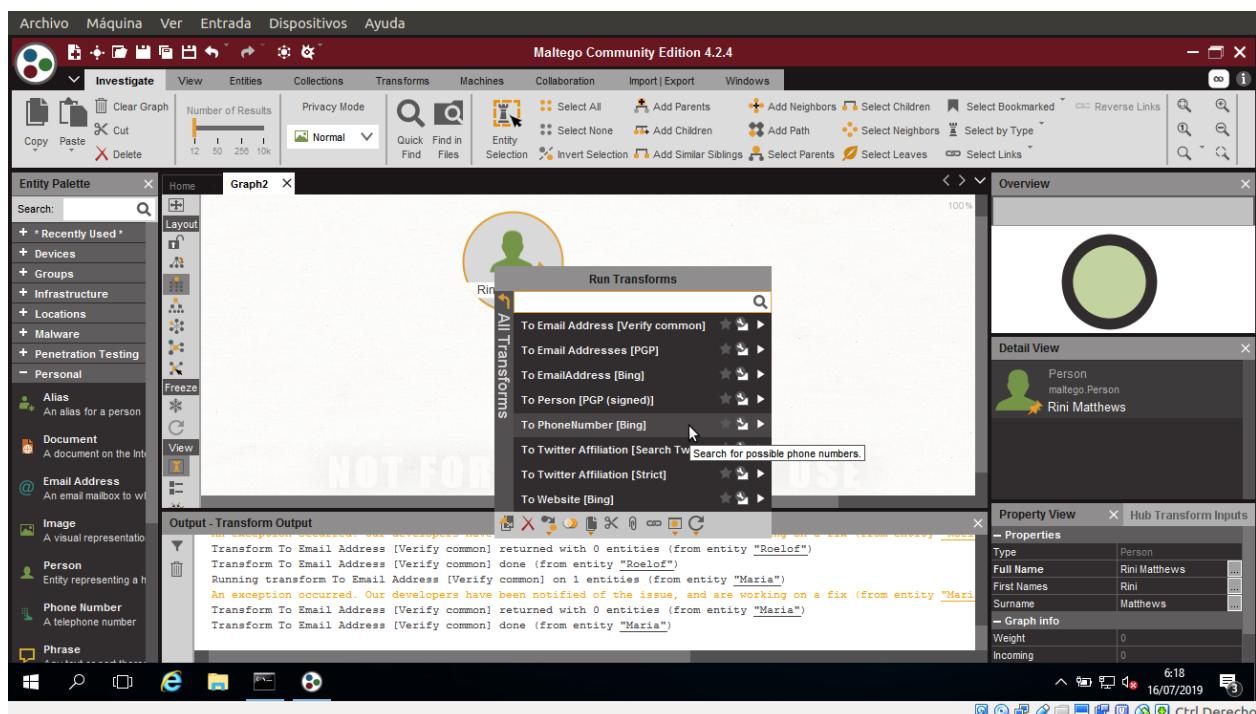
64. Maltego muestra todas las direcciones de correo electrónico válidas (que tienen el nombre en común) correspondientes al nombre dado, como se muestra en la siguiente captura.



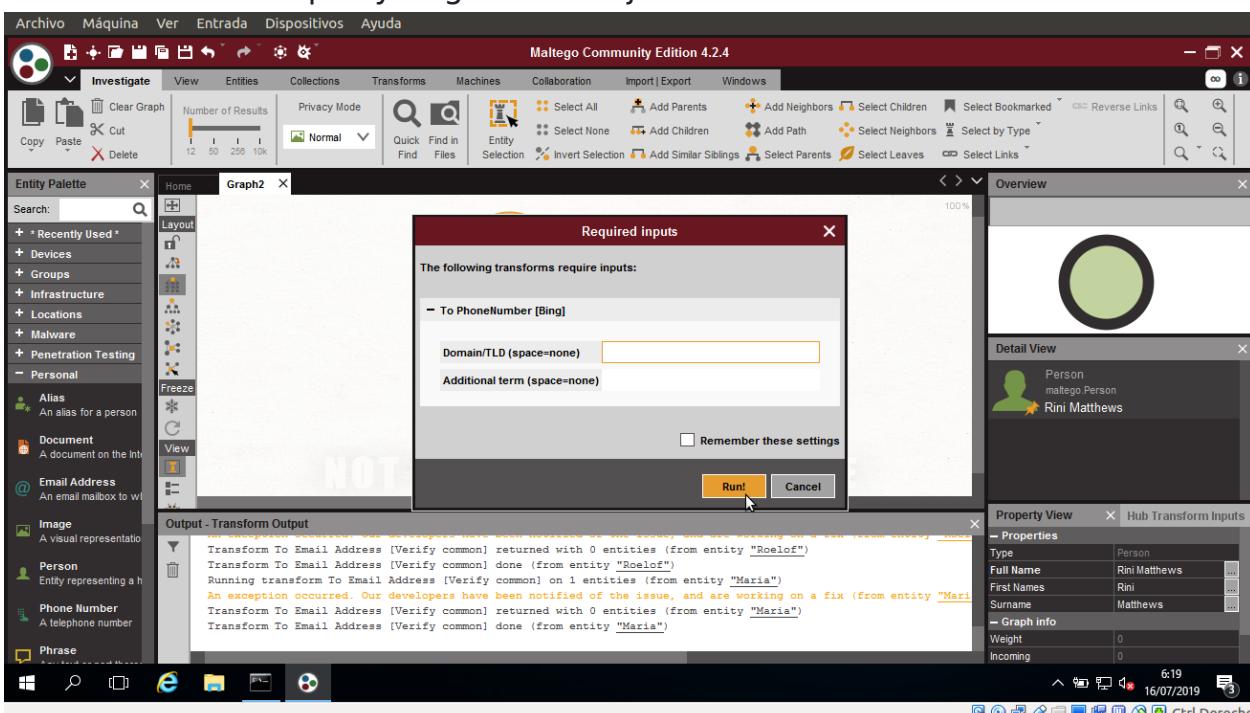
65. Evalúe las direcciones de correo electrónico y determine cuál pertenece a la persona objetivo.

66. Selecciona todas las direcciones de correo electrónico y elimínalas.

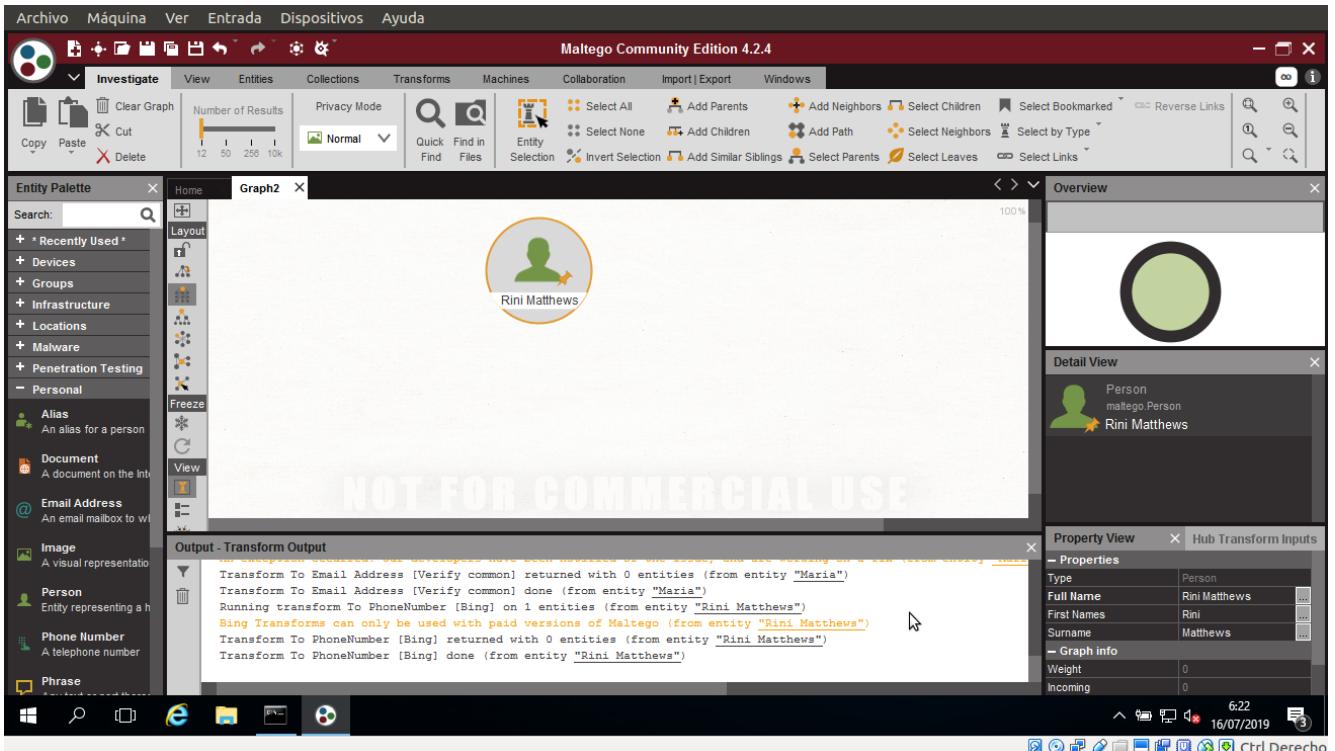
67. Haga clic derecho en la entidad persona y seleccione **Ejecutar transformación → toda transformación → A numero de telefono (usa el buscador)**.



68. Aparece una ventana emergente de entrada requerida, presione el espacio en ambos campos y haga clic en Ejecutar.



69. Maltego muestra una lista de numeros de telefonos asociados a una persona, como se muestra en la siguiente captura:



70. Verifique cada número con herramientas de búsqueda de personas en línea, como las páginas amarillas, para confirmar que un número de teléfono en particular pertenece a la persona objetivo.

71. Selecciona todas las entidades en la sección borralos.

72. Al extraer toda esta información, un atacante puede simular acciones como enumeración, ingeniería de piratería de aplicaciones web, etc. que pueden permitir el acceso a un sistema o red, obtener credenciales, etc.

73. Además de la transformación mencionada anteriormente, también hay una transformación que puede rastrear cuentas y conversaciones de personas que están registradas en sitios de redes sociales como Facebook y Twiter.