Module 03: Open Source Intelligence (OSINT) Methodology

Objective

The objective of this lab is to help students learn different techniques to gather information about a company; you will learn how to:

- Extract a company's information
- Perform network tracerouting
- Perform passive OS fingerprinting

Scenario

Penetration testing is much more than just running exploits against vulnerable systems. In fact, a penetration test begins before penetration testers have even contacted the victim's systems. Rather than blindly throwing out exploits and praying that one of them returns a shell, a penetration tester meticulously studies the environment for potential weaknesses and their mitigating factors. By the time a penetration tester runs an exploit, he or she is nearly certain that it will be successful. Since failed exploits can in some cases cause a crash or even damage to the target system, or at the very least make the target un-exploitable in the future, penetration testers won't get the best results, or deliver the most thorough report to their clients, if they blindly turn an automated exploit machine on the target network with no preparation.

A penetration tester collects the information of a company such as internal and external links of the company's website, people working in the company, geographical location, DNS information, competitive intelligence, network range etc. This information is collected in order to search for vulnerabilities, to exploit and sniff valuable information. In order to become an expert penetration tester and security auditor, you must know various techniques to gather a company's information.

Exercise 1: Performing Information Gathering on a Target Organization using OSINT Framework

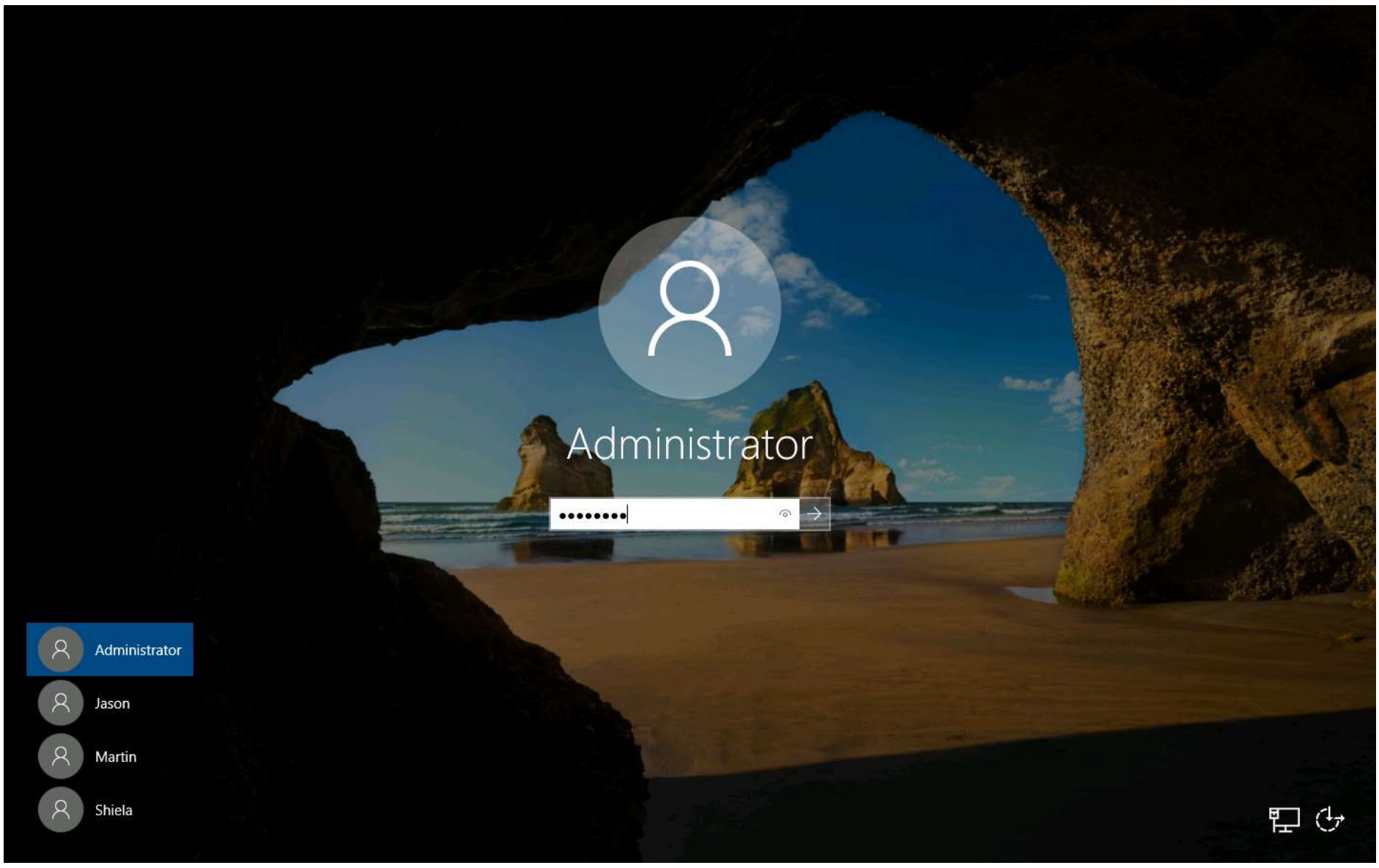
Scenario

Penetration testing is much more than just running exploits against vulnerable systems. In fact, a penetration test begins before penetration testers have even contacted the victim's systems. Rather than blindly throwing out exploits and praying that one of them returns a shell, a penetration tester meticulously studies the environment for potential weaknesses and their mitigating factors. By the time a penetration tester runs an exploit, he or she is nearly certain that it will be successful. Since failed exploits can, in some cases, cause a crash or even damage the target system, or at the very least make the target un-exploitable in the future, penetration testers do not get the best results. Moreover, they cannot deliver the most thorough report to their clients, if they blindly turn an automated exploit machine on the target network with no preparation.

A penetration tester collects a company's information such as internal and external links of the company's website, people working in the company, its geographical location, DNS information, competitive intelligence, and network range etc. This information is collected in order to search for vulnerabilities, to sniff and exploit valuable information. In order to become an expert penetration tester and security auditor, you must know the various techniques required to gather a company's information.

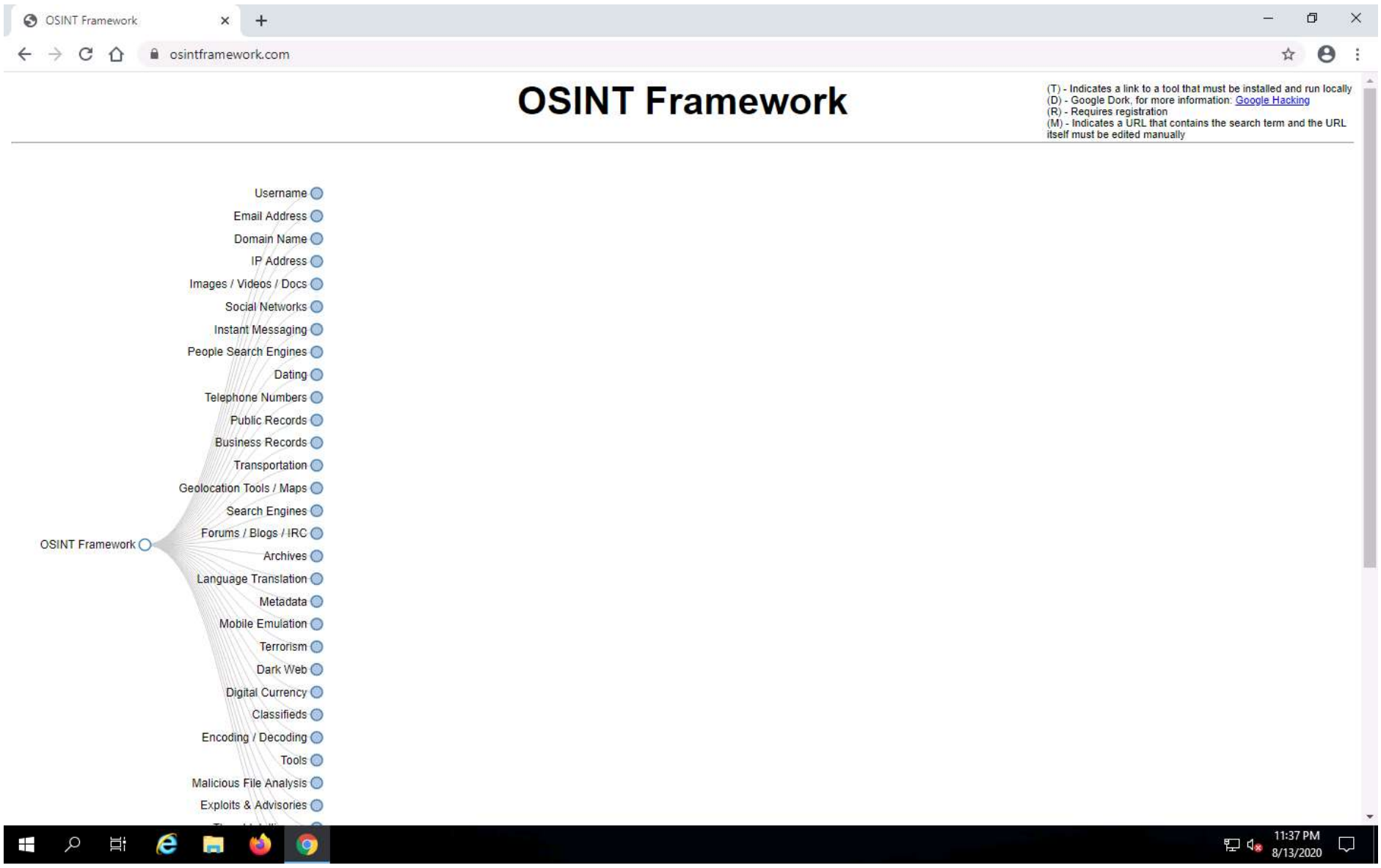
1. By default **CPENT-M3 Windows Server 2019** machine is selected, click **Ctrl+Alt+Del**.

2. In the password field type **Pa$$w0rd** and press **Enter**



3. Open any browser, here in this we lab we are using **Google Chrome** browser.

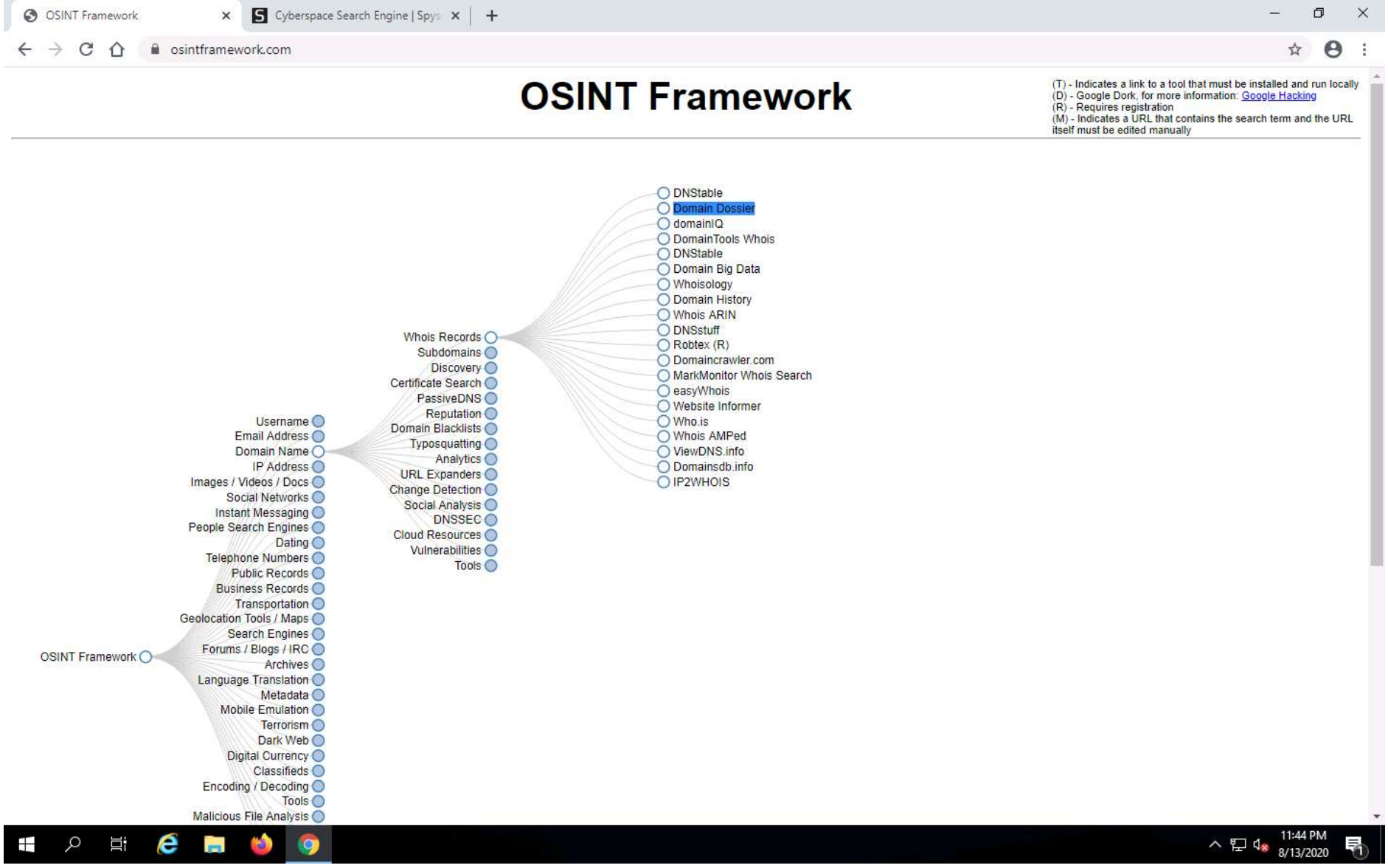
4. In the address bar of the browser, type **https://osintframework.com/** and press **Enter**. OSINT Framework page appears as shown in the screenshot.



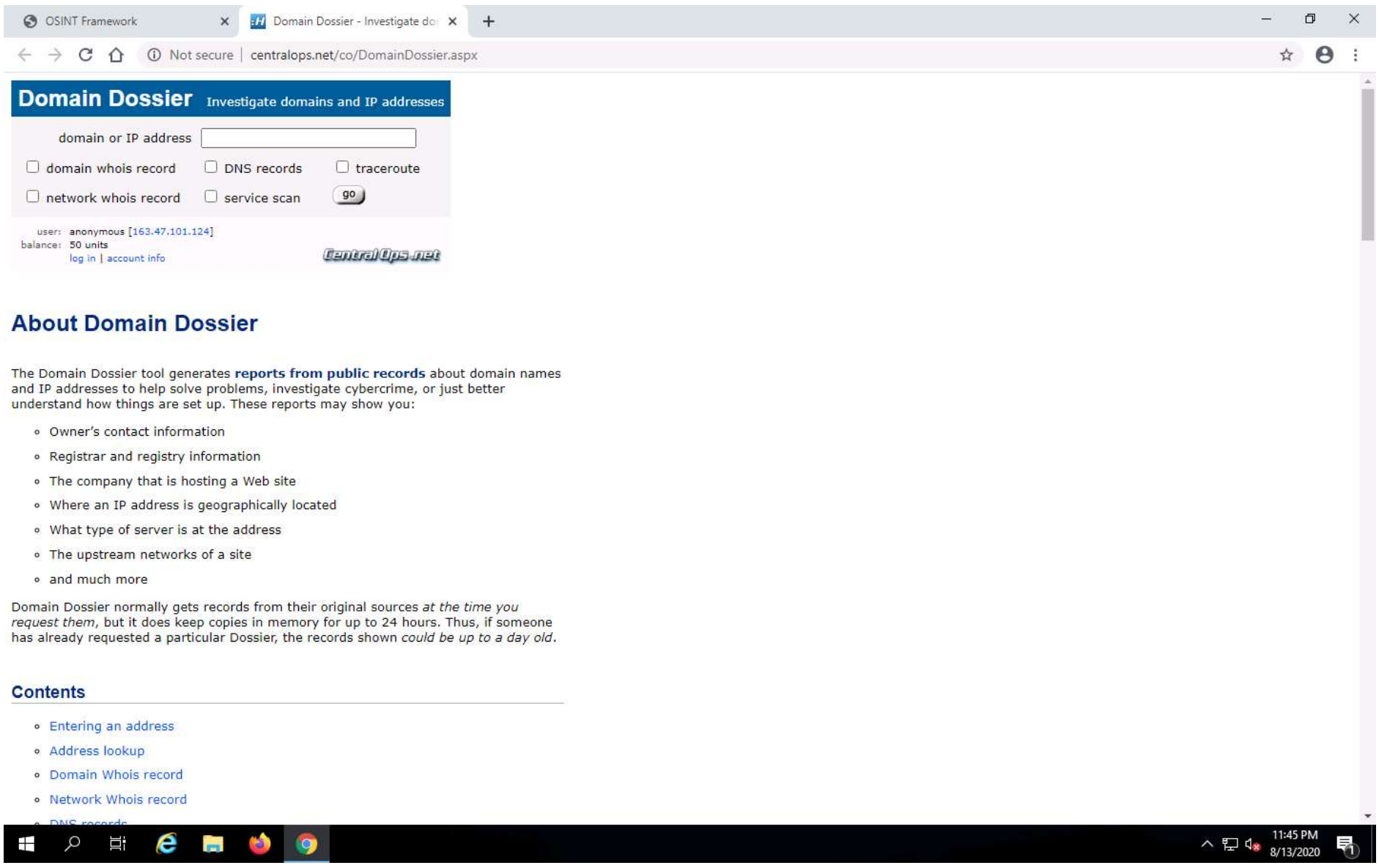
5. In the OSINT Framework page, click **Domain Dossier**. The Domain Dossier helps us to create the report from the public records, investigate cybercrimes, or just better understand how things will be setup.

6. The report will show you the follow details:

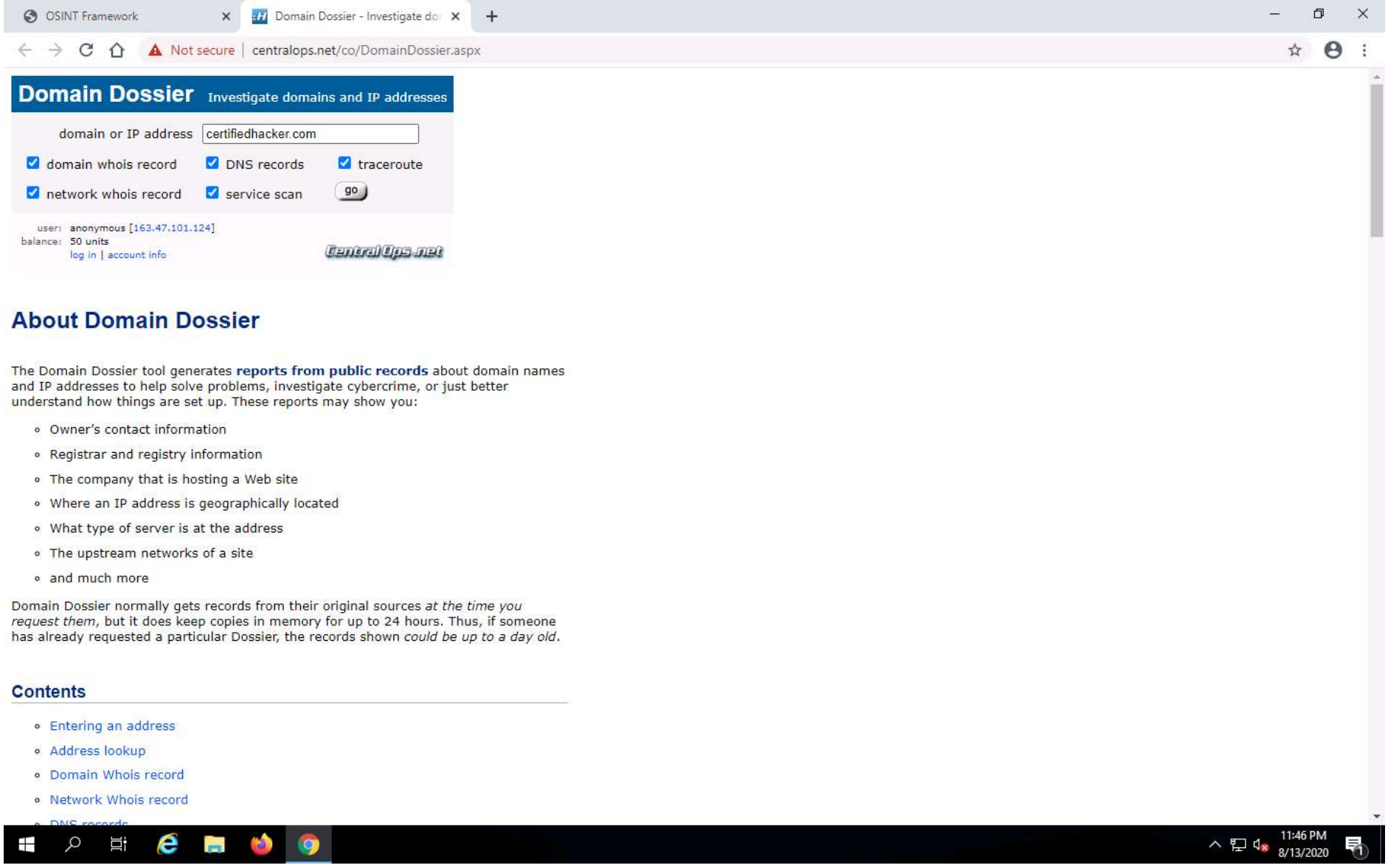
    - Contact information of the Owner
    - Registrar and Registry information
    - The company that is hosting a website
    - IP Address geographical location
    - Type of the Server
    - Network upstream of the sites



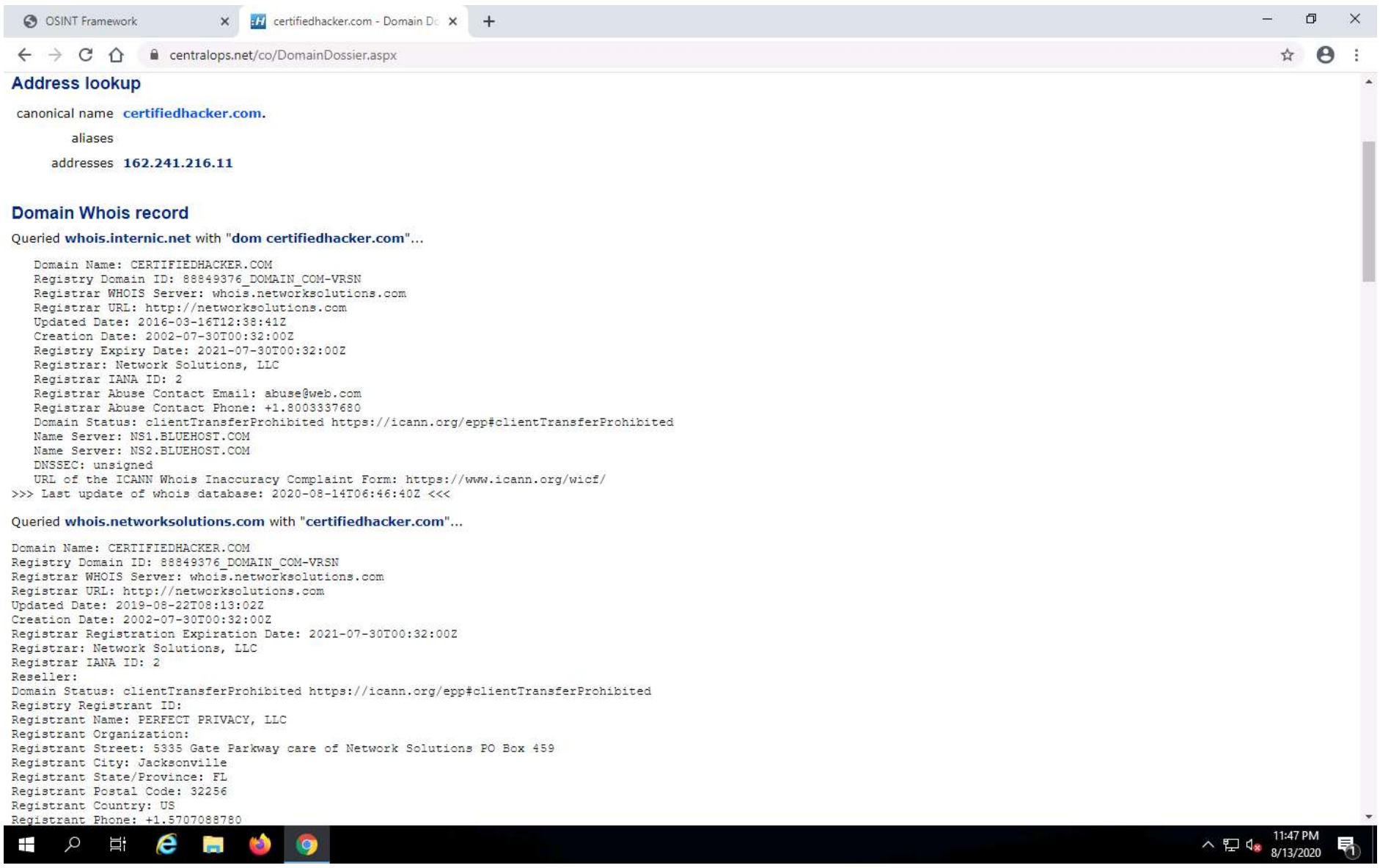
7. The **Domain Dossier** opens in a new tab as shown in the screenshot.



8. In the **domain or IP address** field type the target website and check all the options and then click **go** to perform the Domain Dossier.

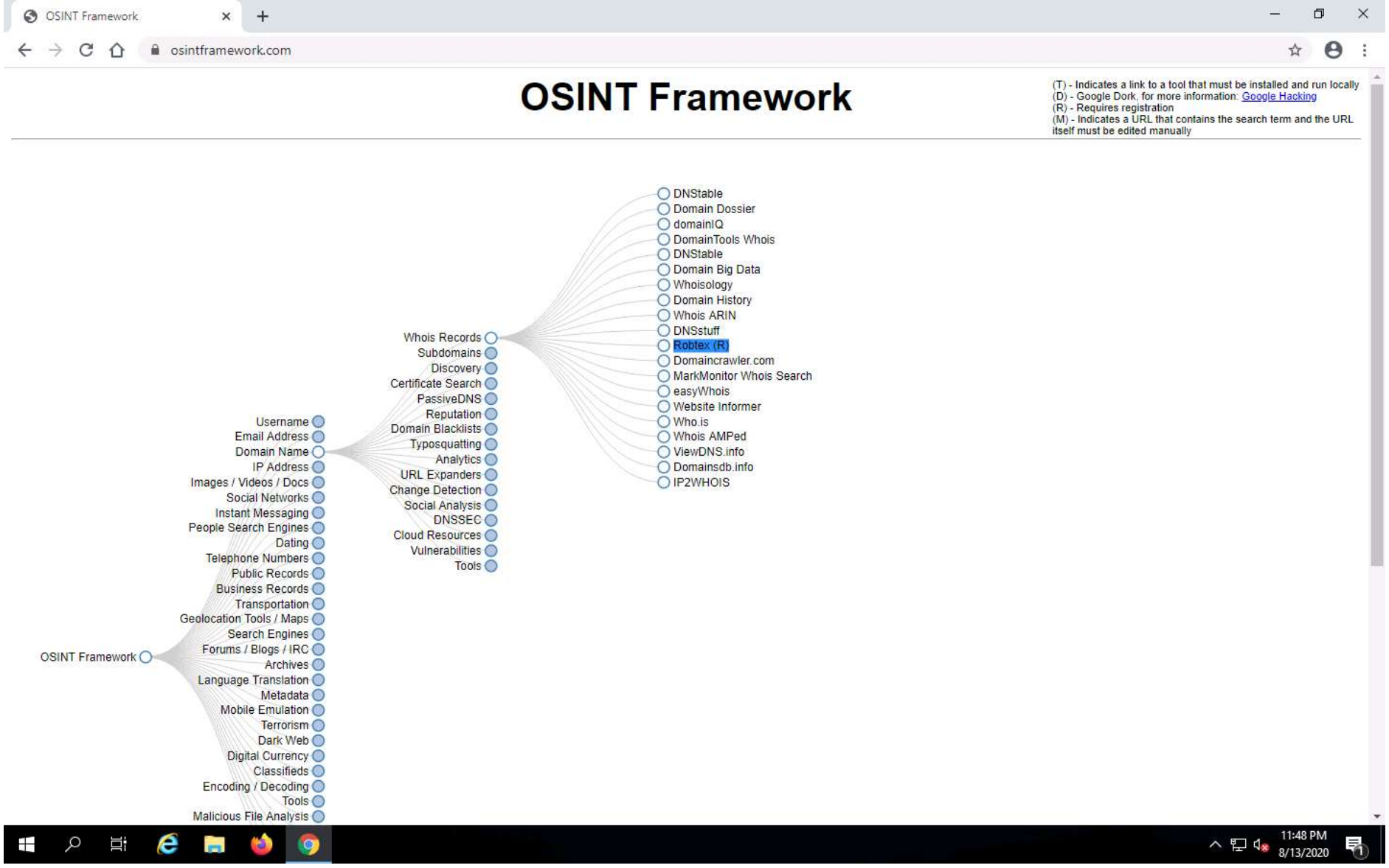


9. The Domain Dossier performs the scan on the target machine and collects the complete details of the targeted website as shown in the screenshot. Scroll down to view the complete details of the targeted website.

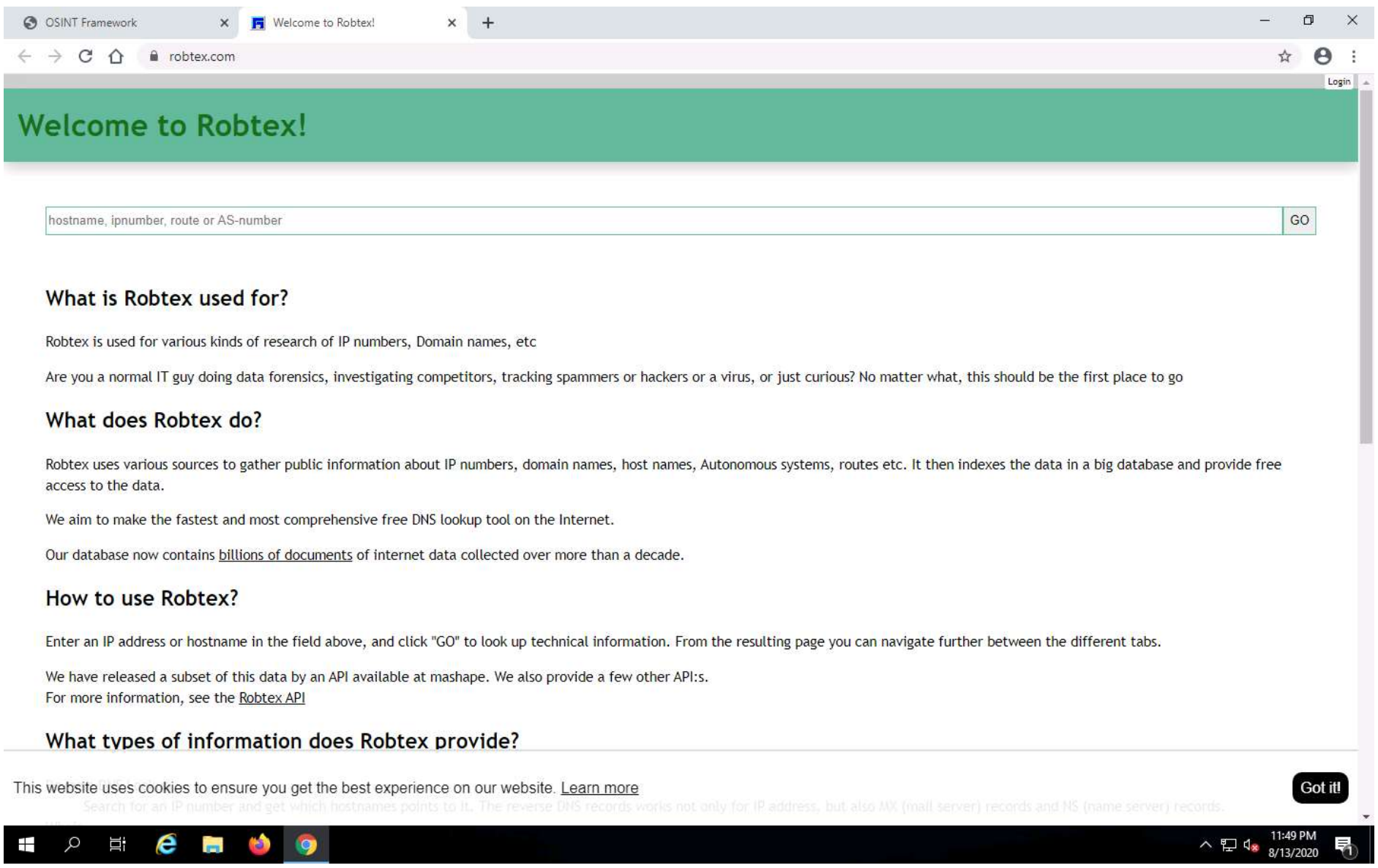


10. Close the **Domain Dossier** tab, and switch to **OSINT Framework** tab.

11. In the OSINT Framework click **Robtex (R)**.

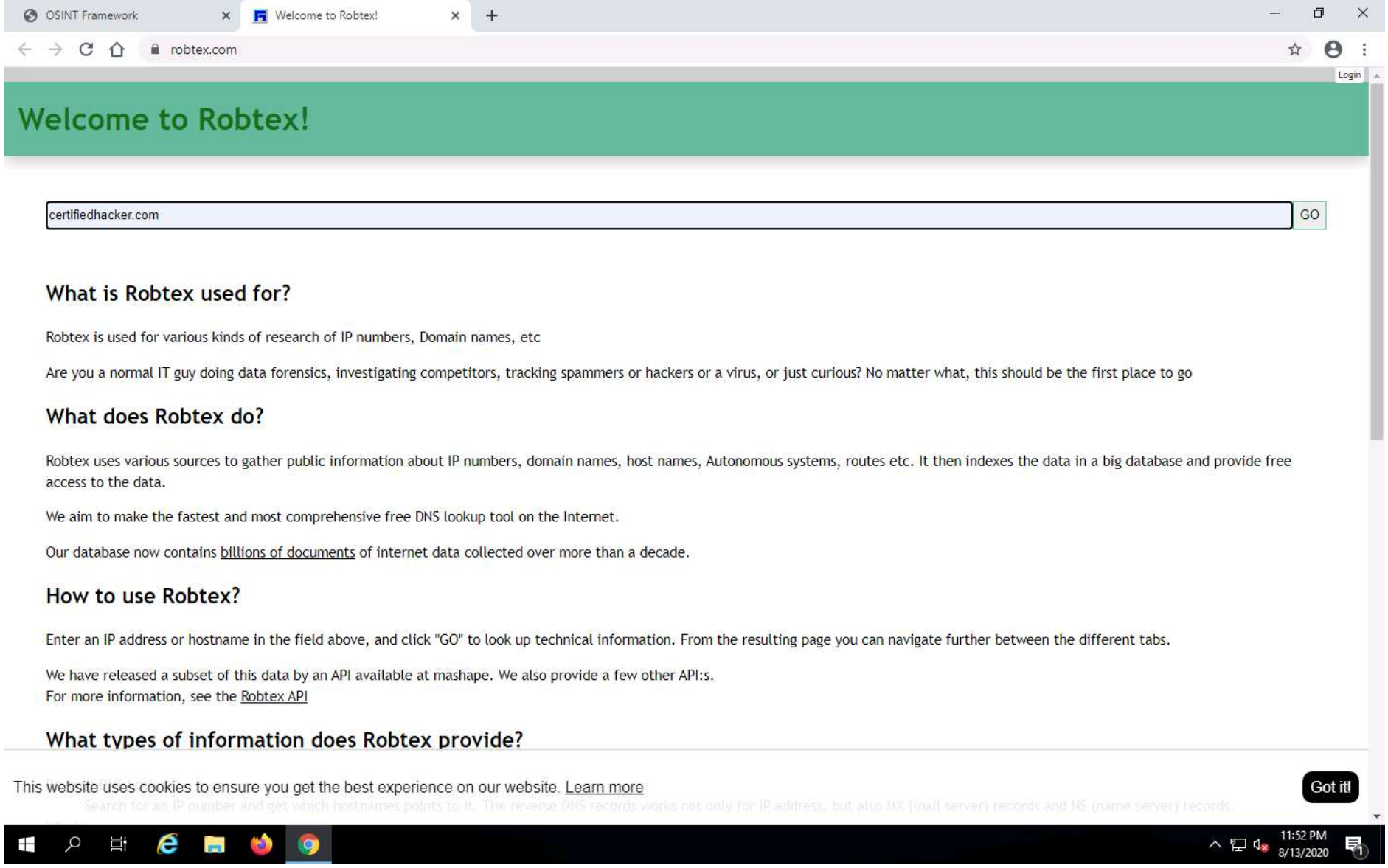


12. Robtex is used for different types of **investigation of IP numbers, Domain names,** etc.

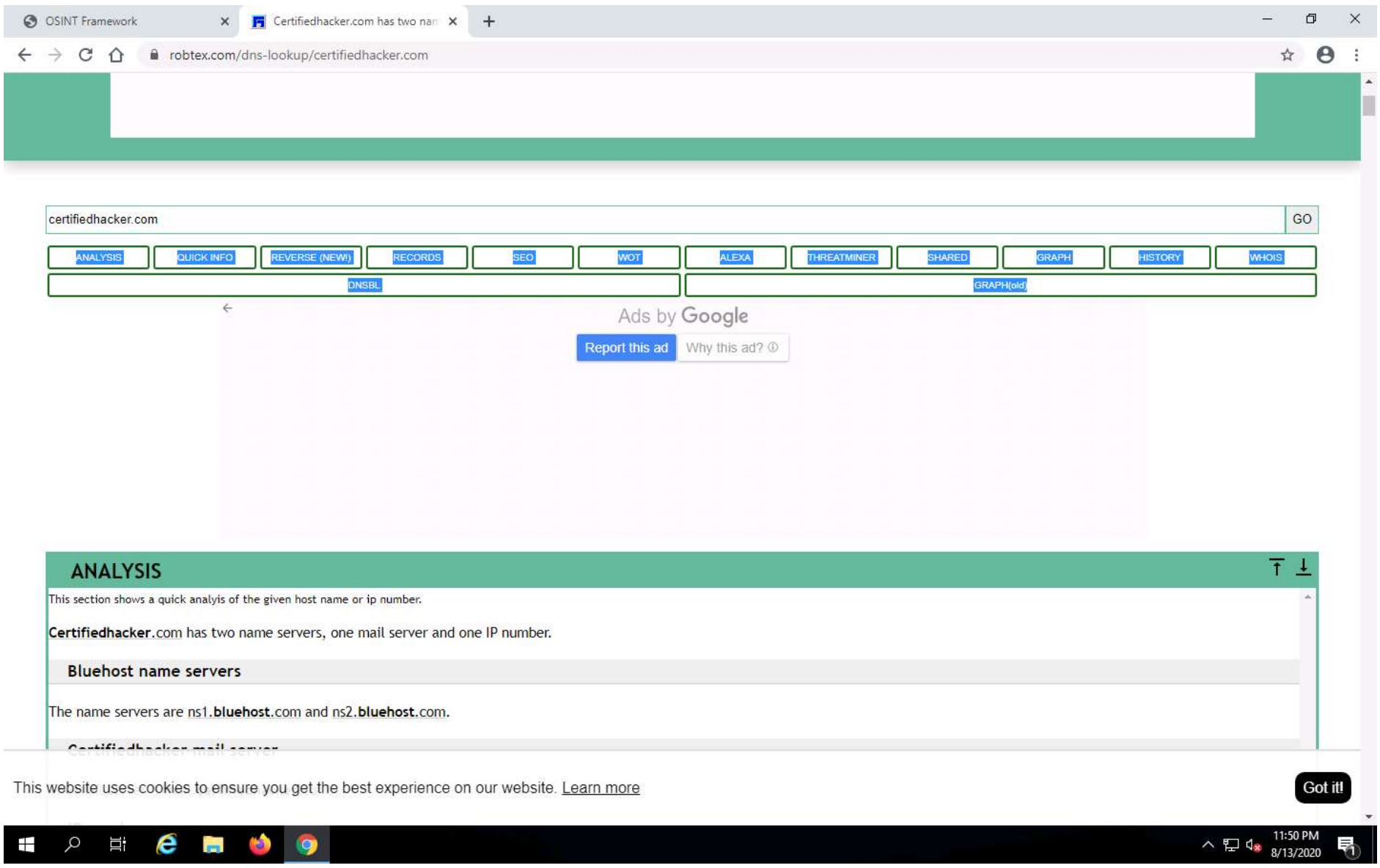


13. Robtex uses numerous sources to gather public information about **IP Addresses, Domain, host names, Autonomous systems, routes** etc. Robtex catalogs the information in a huge database and gives you with the free access to the data.

14. Type the target website in the Robtex field and click **GO**.



15. As soon as you click on GO button, the Robtex provides you with the output as shown in the screenshot.



16. The **Analysis** section shows you with the complete analysis of the provided target website.

OSINT Framework | Certifiedhacker.com has two nan | robtex.com/dns-lookup/certifiedhacker.com

ANALYSIS

This section shows a quick analyis of the given host name or ip number.

Certifiedhacker.com has two name servers, one mail server and one IP number.

Bluehost name servers

The name servers are ns1.**bluehost**.com and ns2.**bluehost**.com.

Certifiedhacker mail server

The mail server is mail.**certifiedhacker**.com.

IP number

The IP number is 162.241.216.11. The PTR of the IP number is box5331.**bluehost**.com. The IP number is in Provo, United States. It is hosted by JS.

We investigated two host names that cnames to **certifiedhacker**.com.

Results found

Certifiedhacker.net, **certifiedhacker**.org, certifiedhacker.com.**ipaddress**.com, **hackercertified**.com and **hackercertified**.net.

QUICK INFO

Quick summary of the host name

11:52 PM 8/13/2020

17. Next, in the **Records** section, it provides the hierarchical analysis of the provided entity.

OSINT Framework | Certifiedhacker.com has two nan | robtex.com/dns-lookup/certifiedhacker.com

Domain Name	certifiedhacker.com
Registry	com
TLD	com
DNS	
IP numbers	162.241.216.11
Name servers	ns1.**bluehost**.com ns2.**bluehost**.com
Mail servers	mail.**certifiedhacker**.com

REVERSE (NEW!)

Reverse DNS reports of the queried and related entities

Please login to see this section

RECORDS

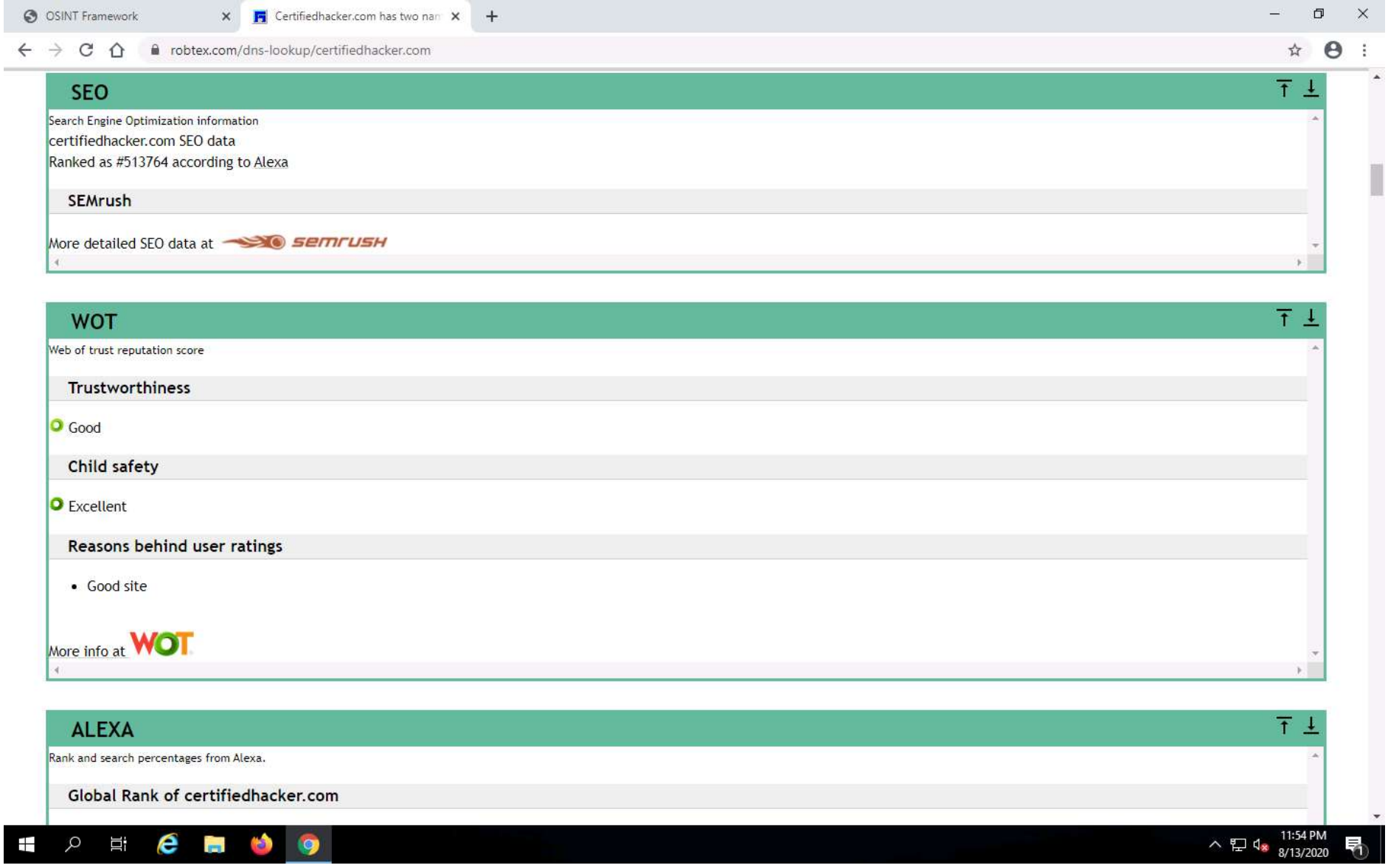
Hierarchical analysis of the entity

certifiedhacker.com

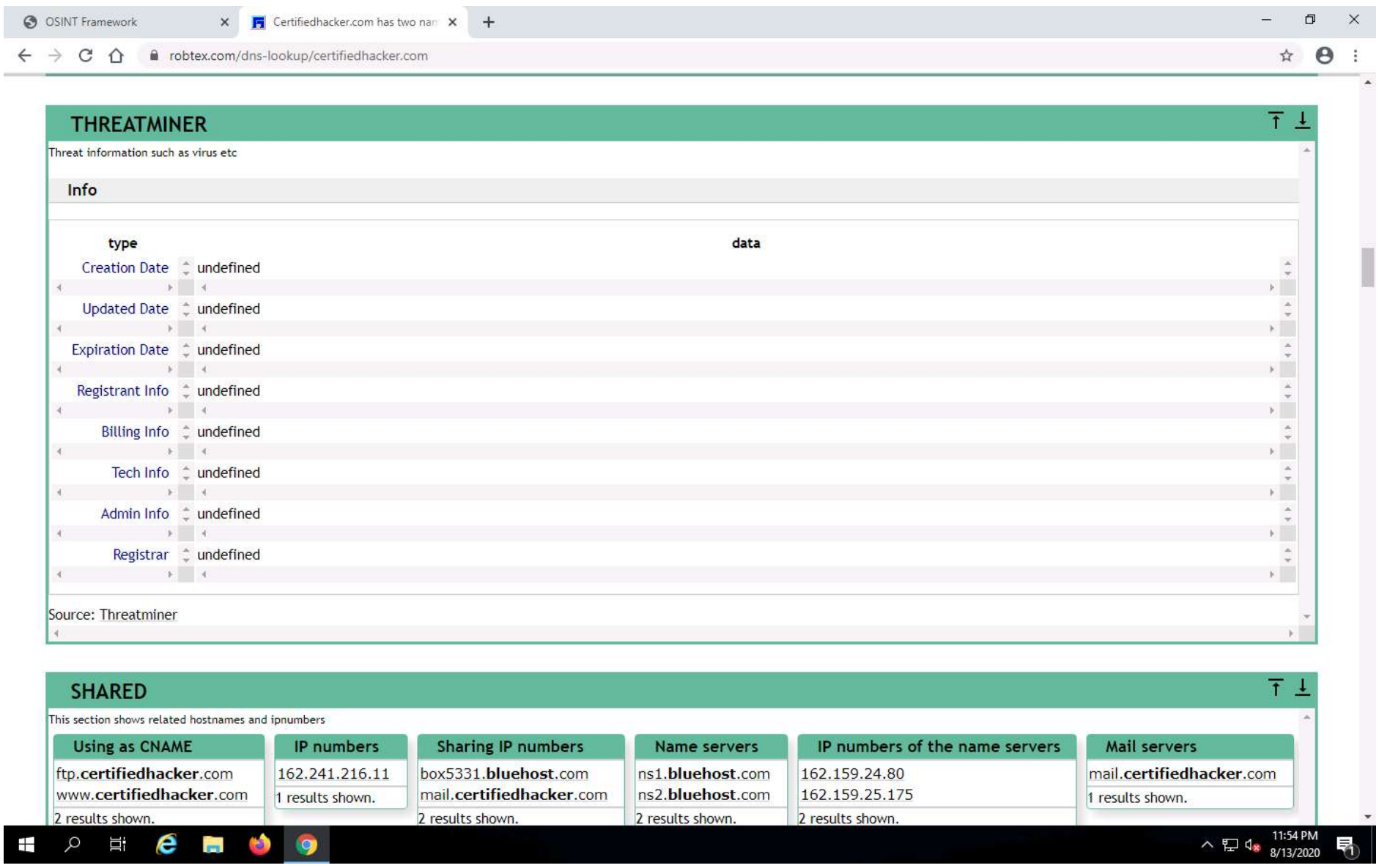
- a 162.241.216.11
  - whois Unified Layer (BLUEH-2)
  - route 162.241.0.0/16
    - bgp AS46606
      - asname EIGI Endurance International Group, Inc
  - descr JS
  - location Provo, United States

11:53 PM 8/13/2020

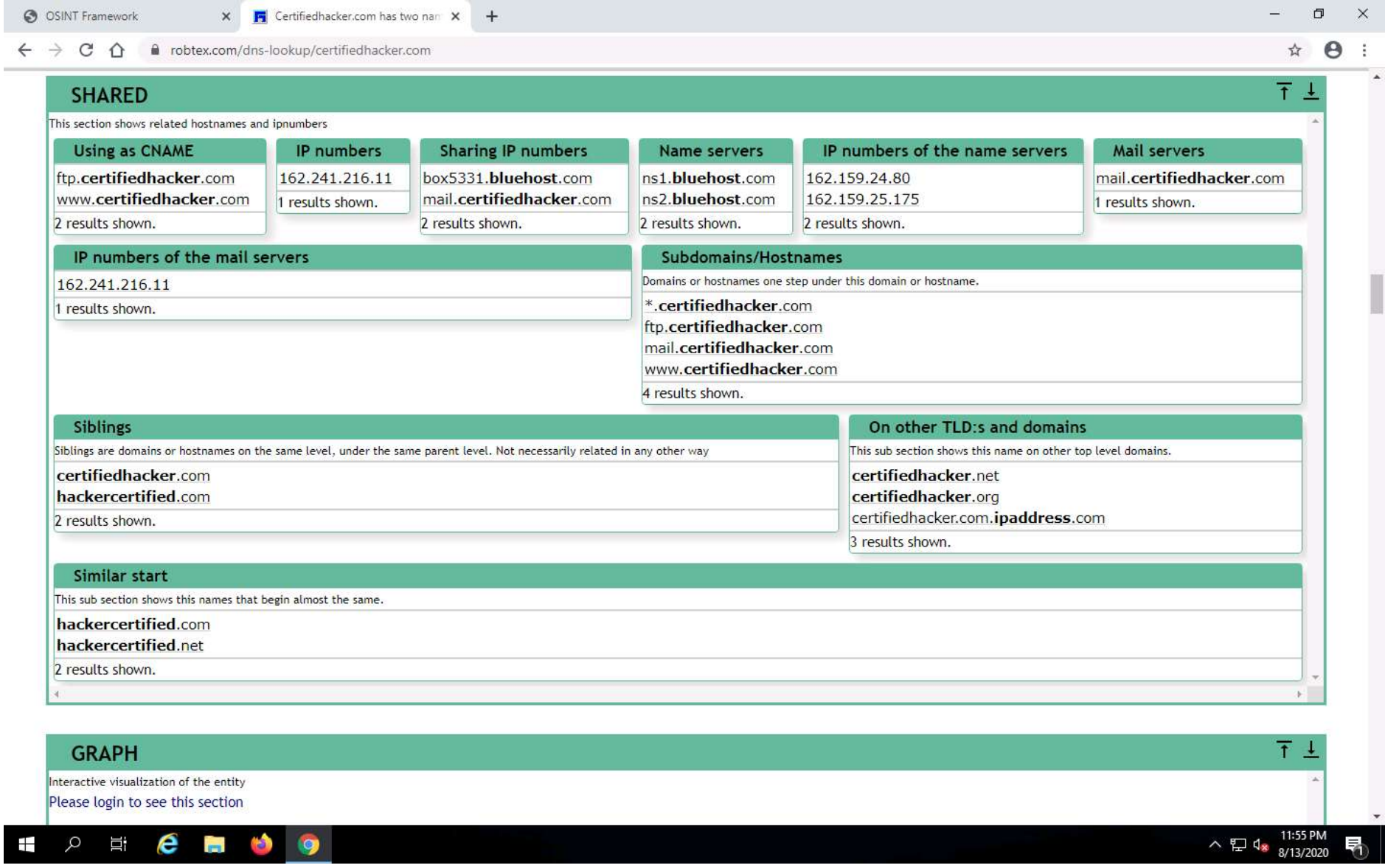
18. It also provides the **SEO, WOT, Alexa** as shown in the screenshot.



19. Scroll down to view **THREATMINER** section where Robtex gives you the threat information such as virus etc if any.



20. To view the related hostnames and IP numbers of the provided target website, scroll down to **SHARED** section.



21. Similarly scroll down to view other results for the target website. Close the Robtex tab after the analysis.

Exercise 2: Footprinting a Target using Maltego

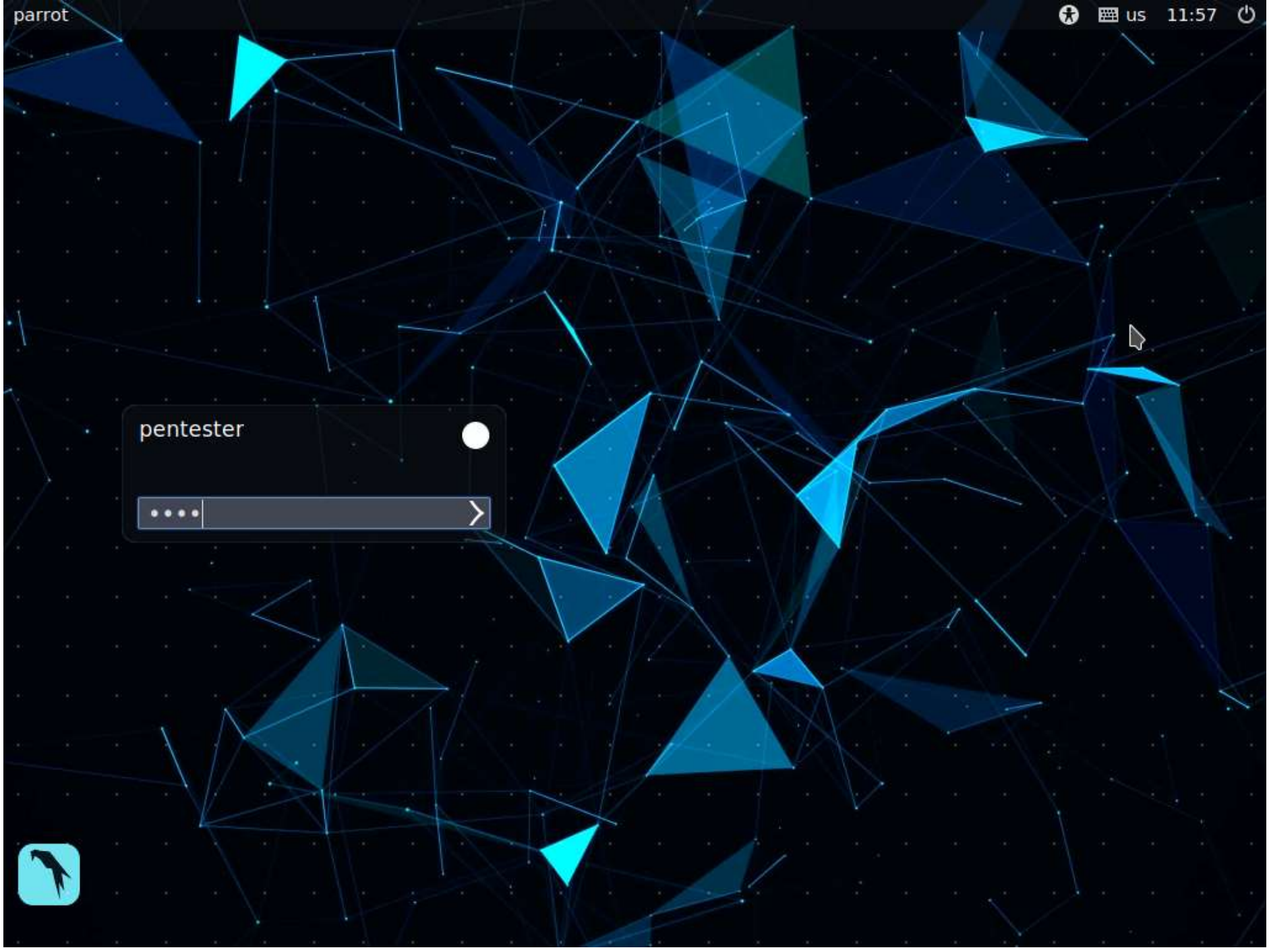
Scenario

Maltego is a footprinting tool used to gather maximum information for the purpose of ethical hacking, computer forensics, and pentesting. It provides a library of transforms to discover data from open sources and visualizes that information in a graph format, suitable for link analysis and data mining. Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate, and even making it possible to see hidden connections.

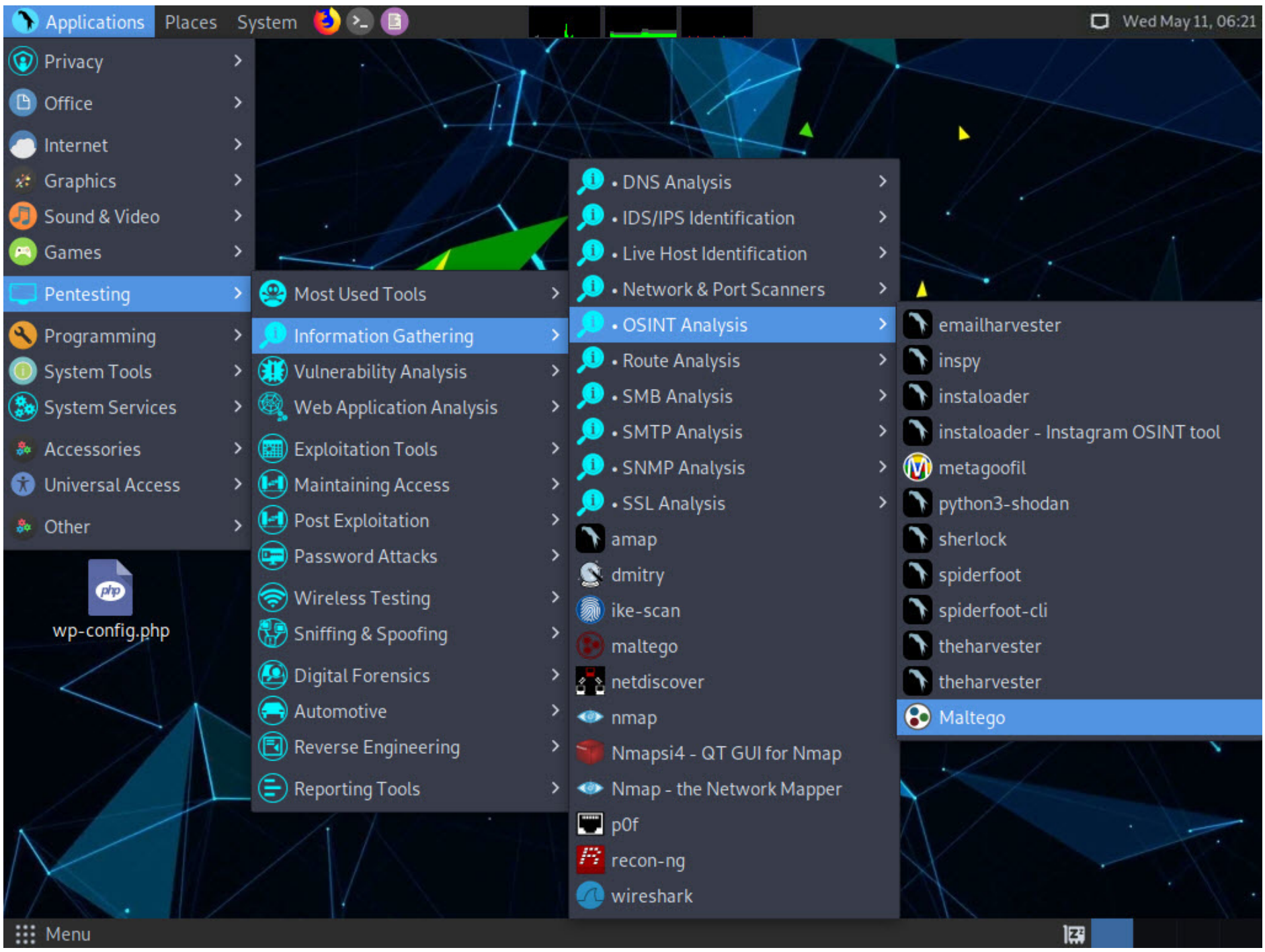
Here, we will gather a variety of information about the target organization using Maltego.

Note: The screenshots will differ while performing the lab tasks.

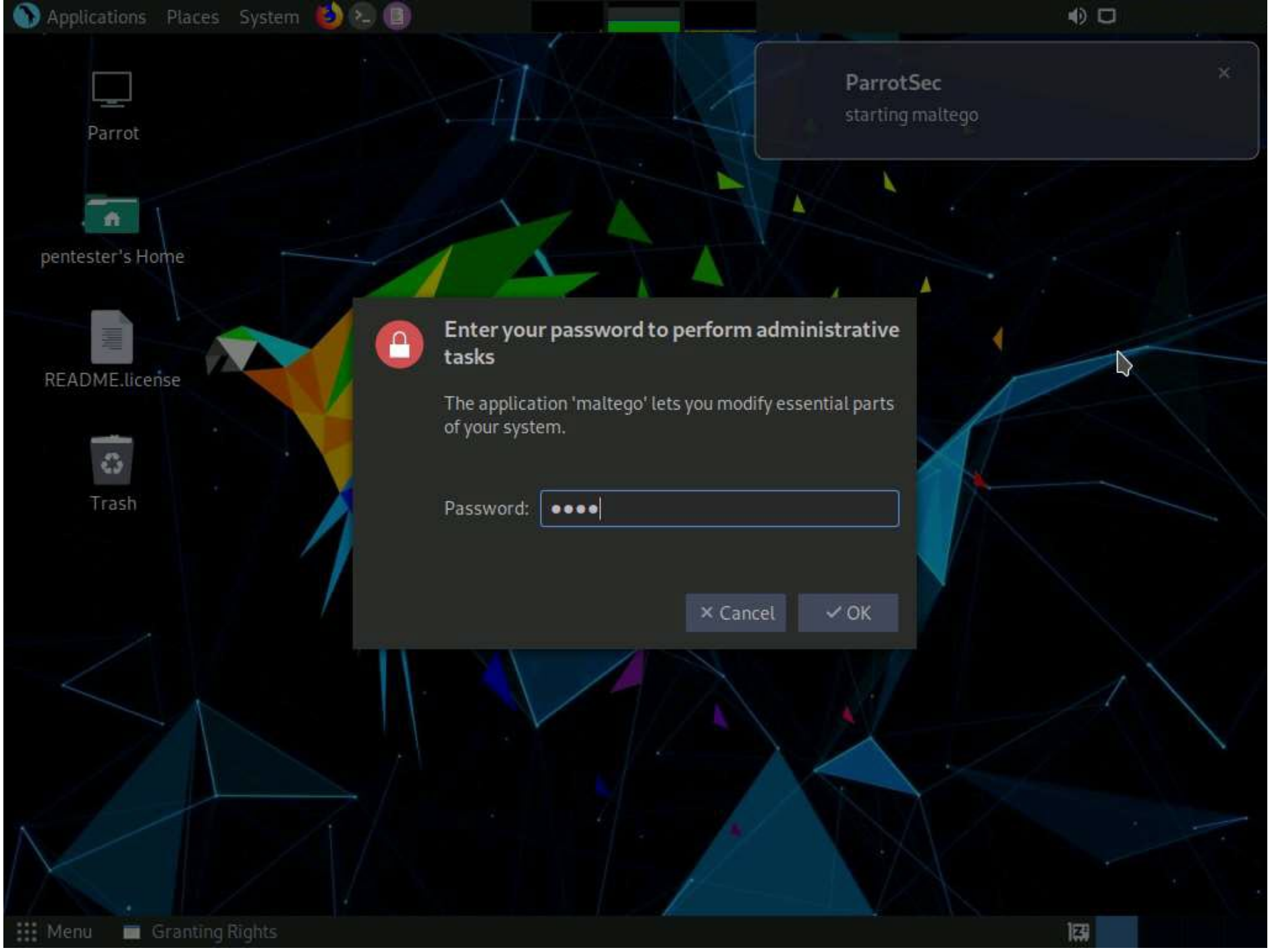
1. Click **CPENT-M3 Parrot Security**. Type **toor** in the **Password** field and press **Enter**.



2. Launch **Maltego** by navigating to **Applications** -> **Pentesting** -> **Information Gathering** -> **OSINT Analysis** -> **maltego**, as shown in the screenshot.

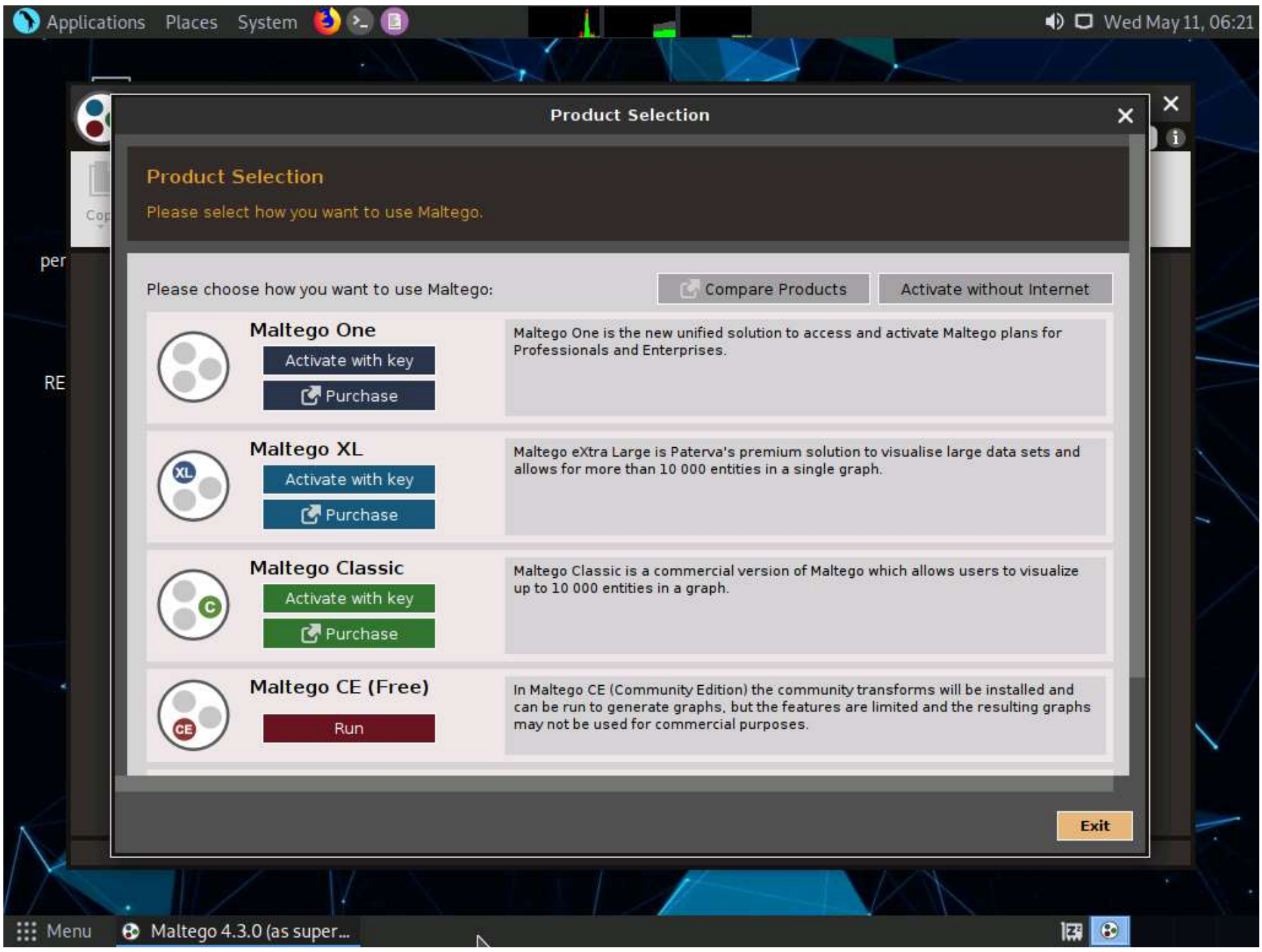


3. Enter your password to perform administrative tasks window appears, type **toor** in the Password field and click **OK**.

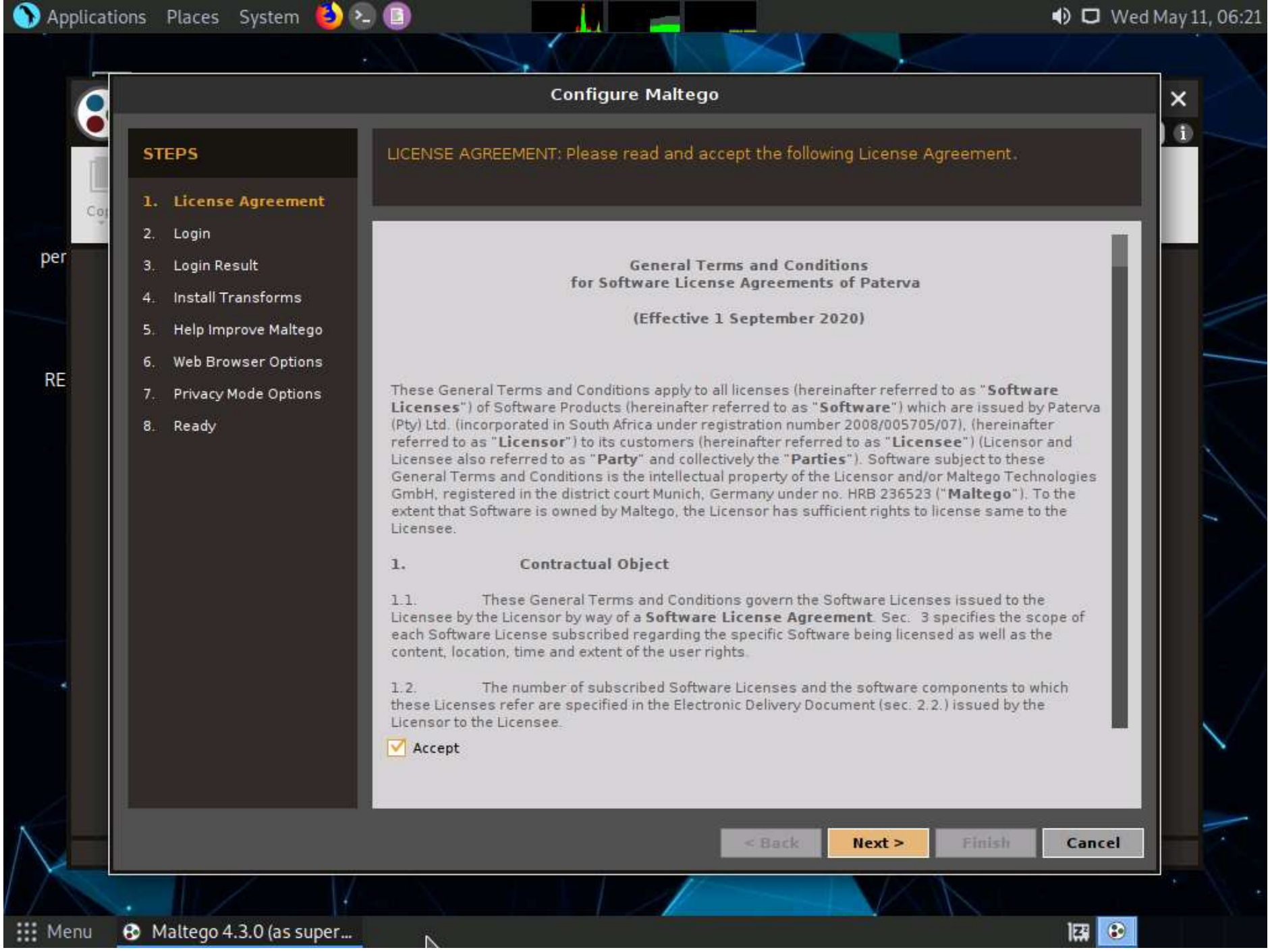


4. A **Product Selection wizard** appears on the **Maltego** GUI; click **Run** from **Maltego CE (Free)** option.

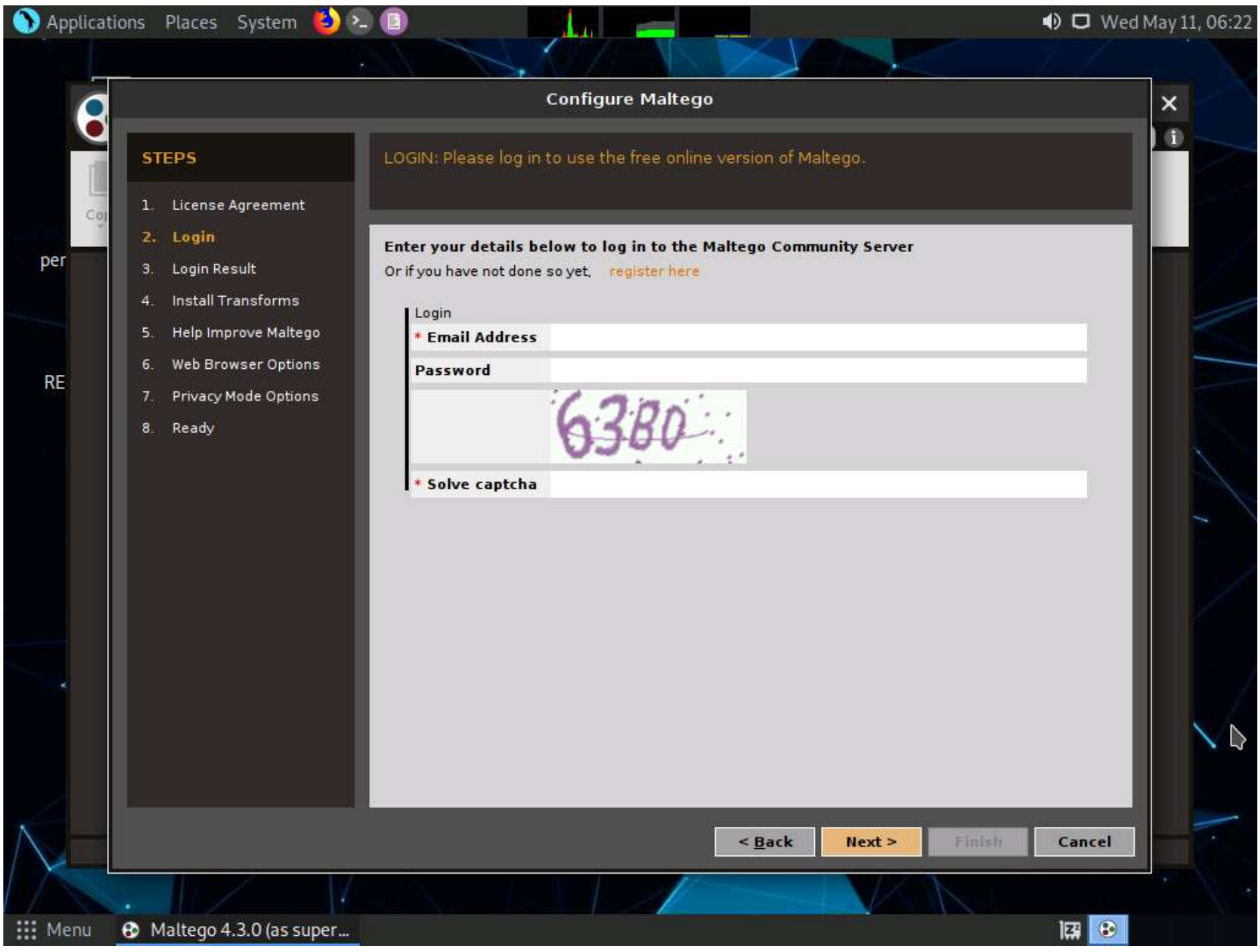
Note: If the Memory Settings Optimized pop-up appears, click **Restart Now**.



5. As the **Configure Maltego** window appears along with a **LICENSE AGREEMENT** form, check the **Accept** checkbox and click **Next**.

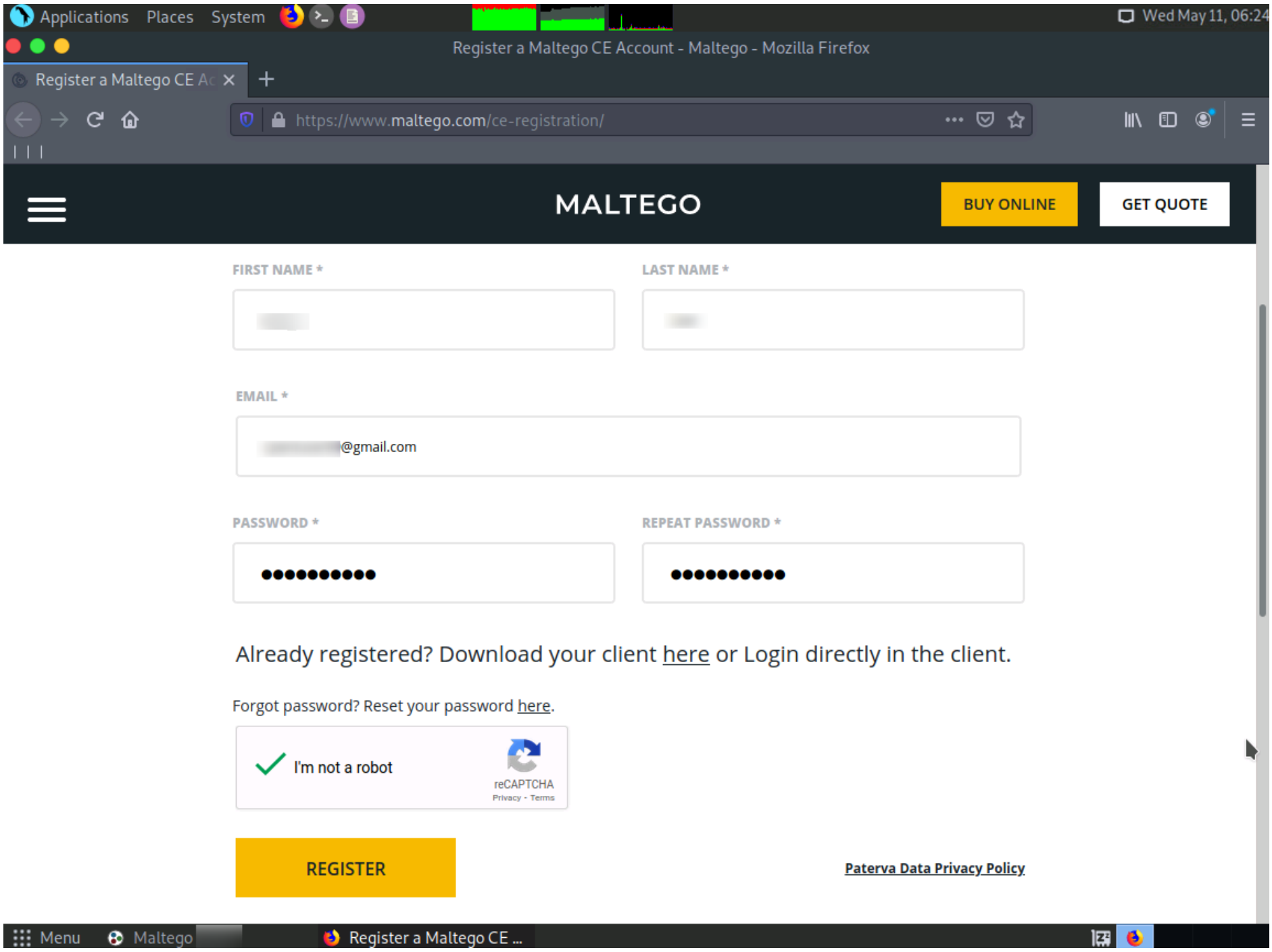


6. You will be redirected to the **Login** section; as shown in the screenshot.

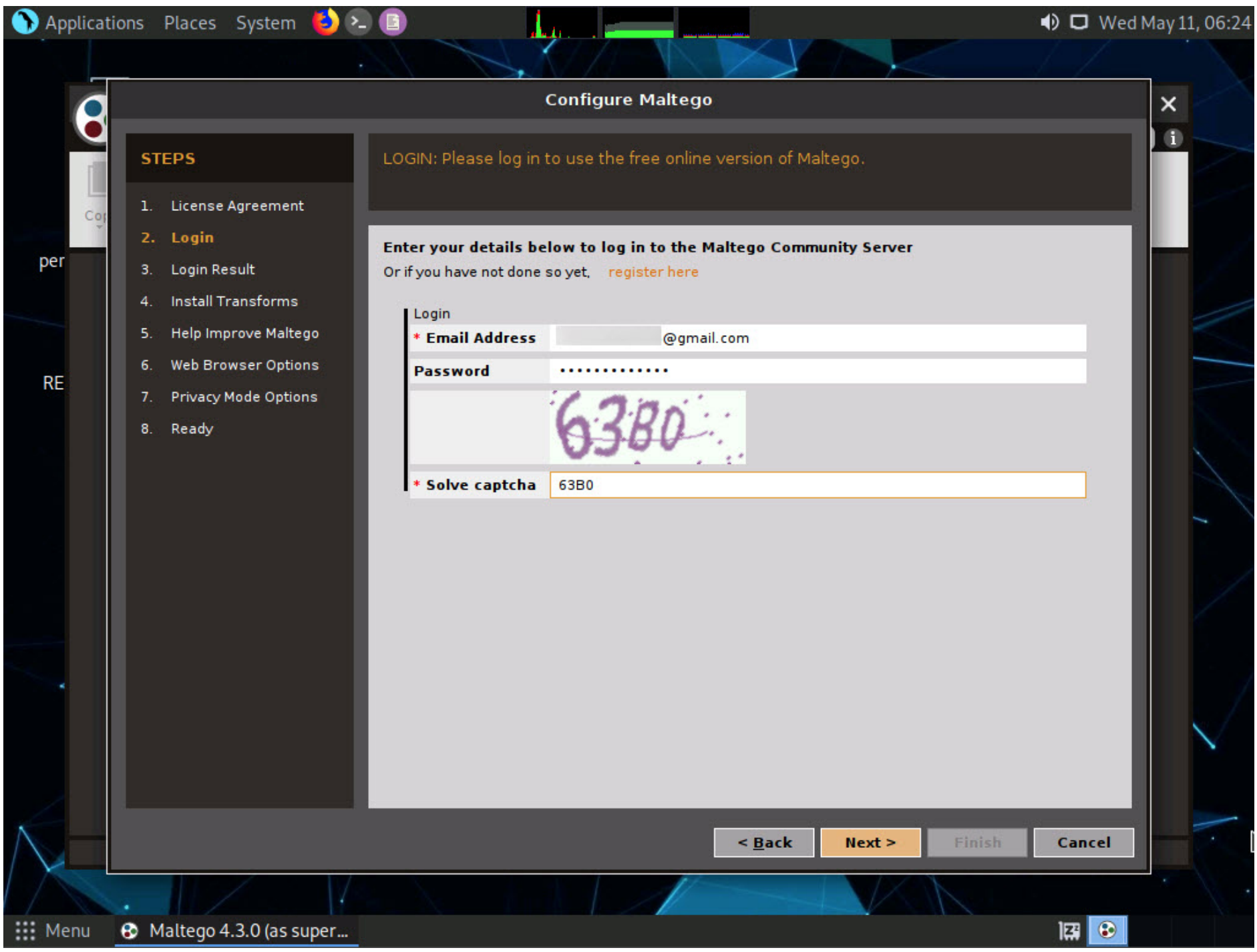


7. Now open a browser and type https://www.maltego.com/ce-registration in the address bar of the browser and press **Enter**. **Register a Maltego CE Account** page appears, enter your details and confirm the captcha, and click **REGISTER** button to register your account and activate it.

Note: If cookie notification appears in the lower section of the browser, click **Accept**.

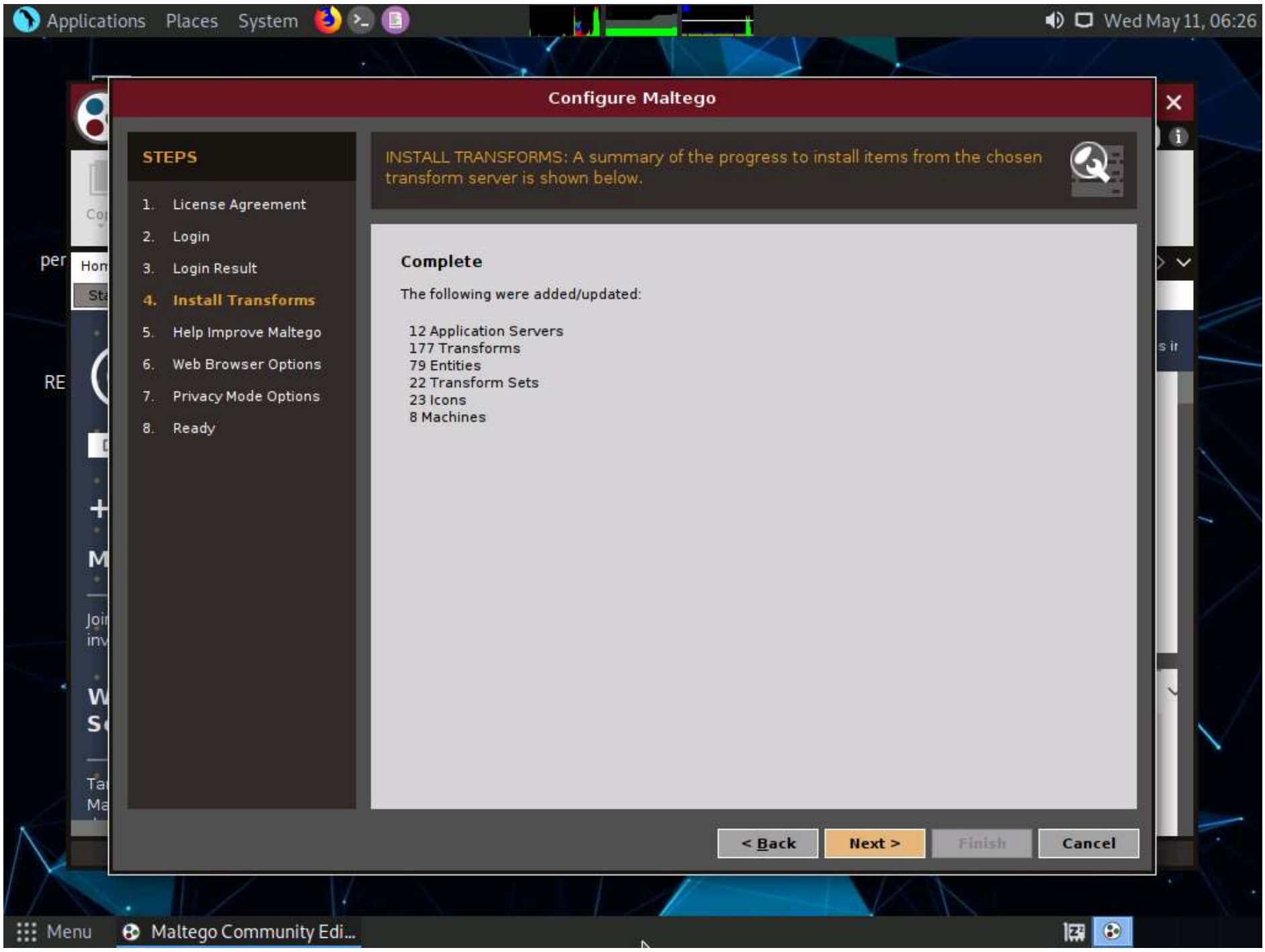


8. Minimize the **web browser** and go back to the **setup wizard** and enter the **Email Address** and **Password** specified at the time of registration; solve the captcha and click **Next**.

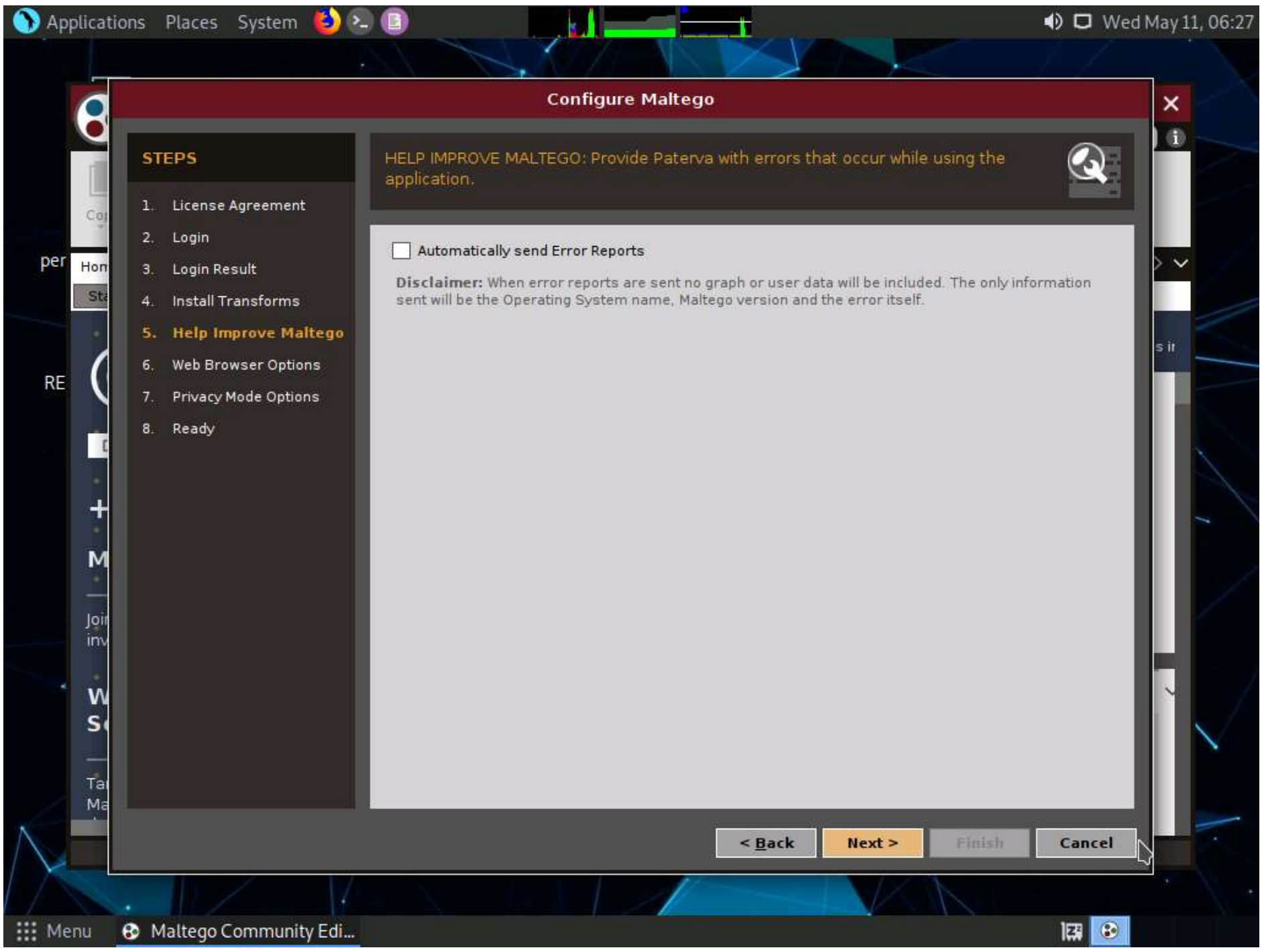


9. The **Login Result** section displays your personal details; click **Next**.

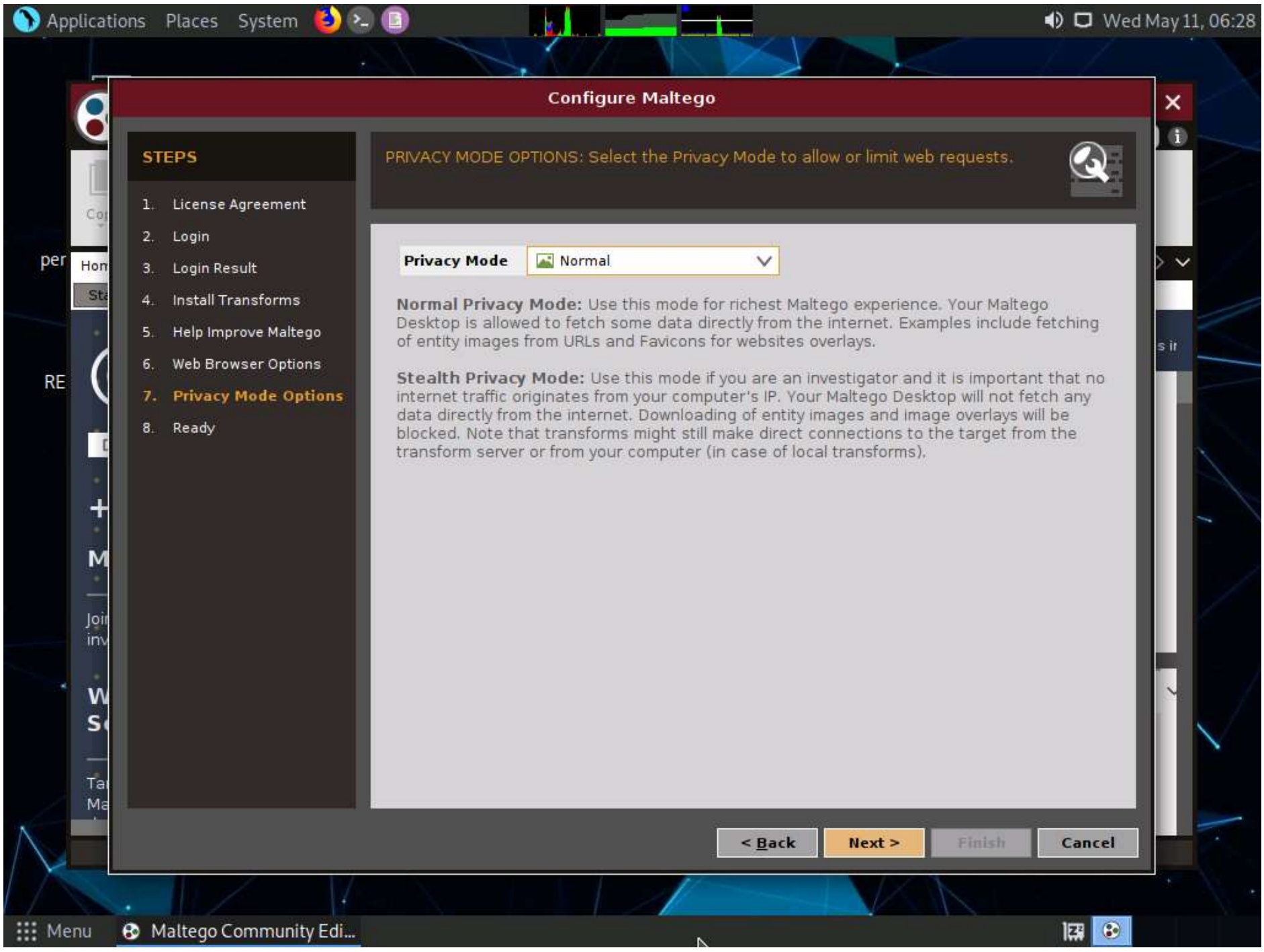
10. The **Install Transforms** section appears, which will install items from the chosen transform server. Leave the settings to default and click **Next**.



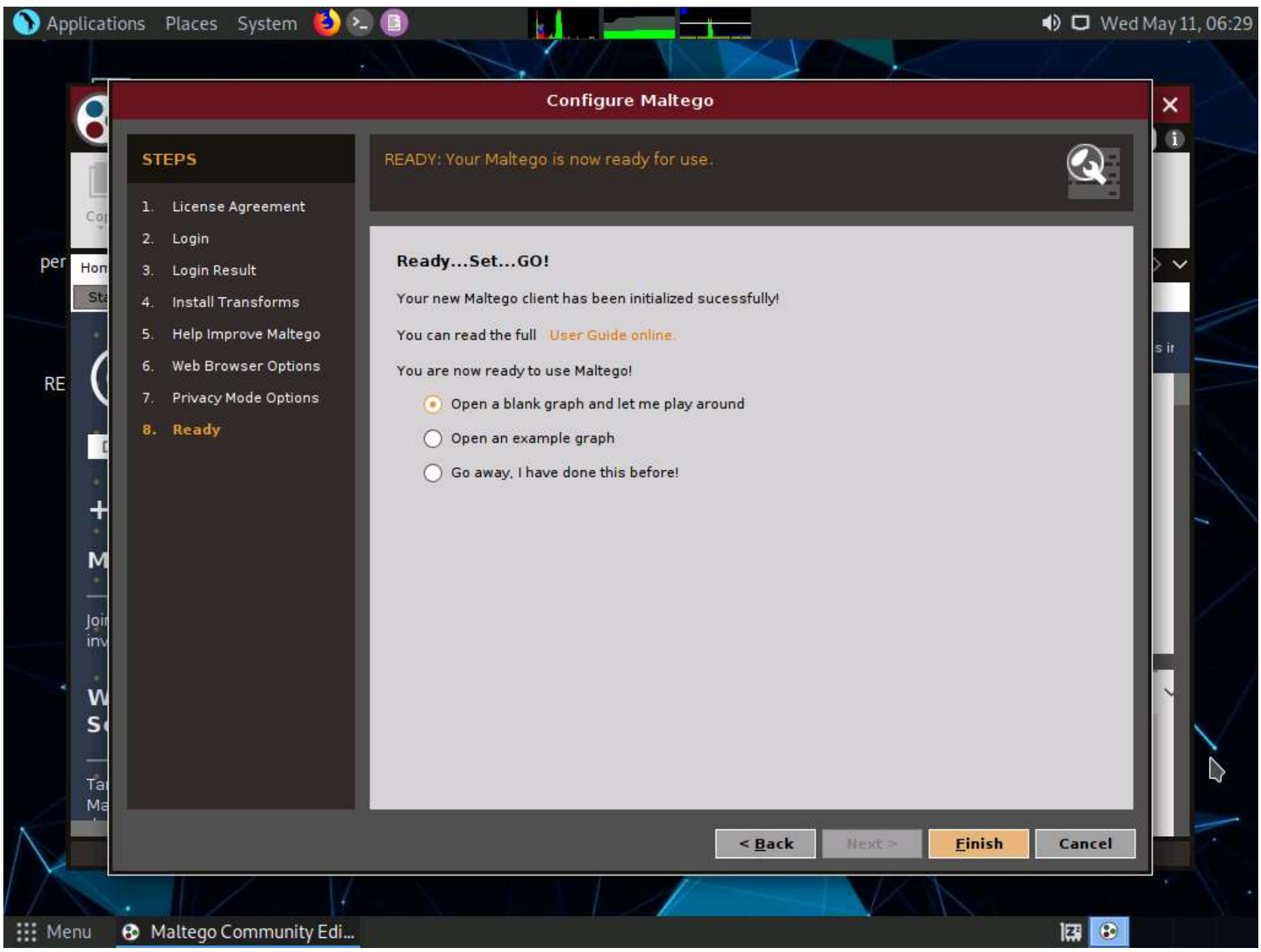
11. The **Help Improve Maltego** section appears. Leave the options set to default and click **Next**.



12. In **Web Browser Options** click **Next** and then in the **Privacy Mode Options** section appears. Leave the options set to default and click **Next**.



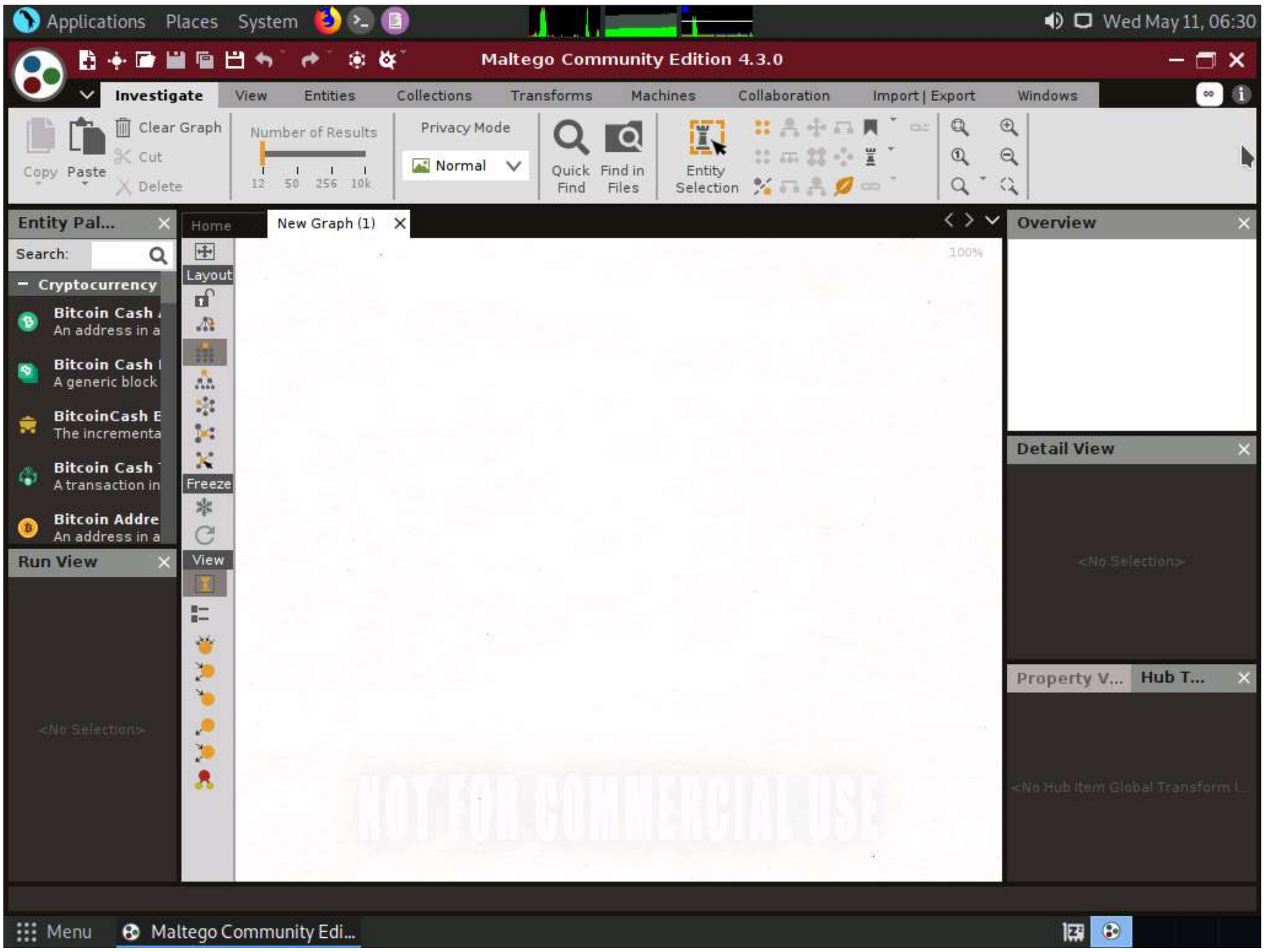
13. The **Ready section** appears. Select the radio button of **Open a blank graph and let me play around** and click **Finish** to perform footprinting manually.



14. The Maltego Community Edition GUI appears, and the **New Graph (1)** window will be automatically launched, as shown in the screenshot.

Note: If the **New Graph (1)** window does not open automatically, click the **Create a new graph** icon located at the top-left corner of the GUI (in the toolbar) to start a new graph.

Note: Previous Configuration Found pop-up appears, click **No**.

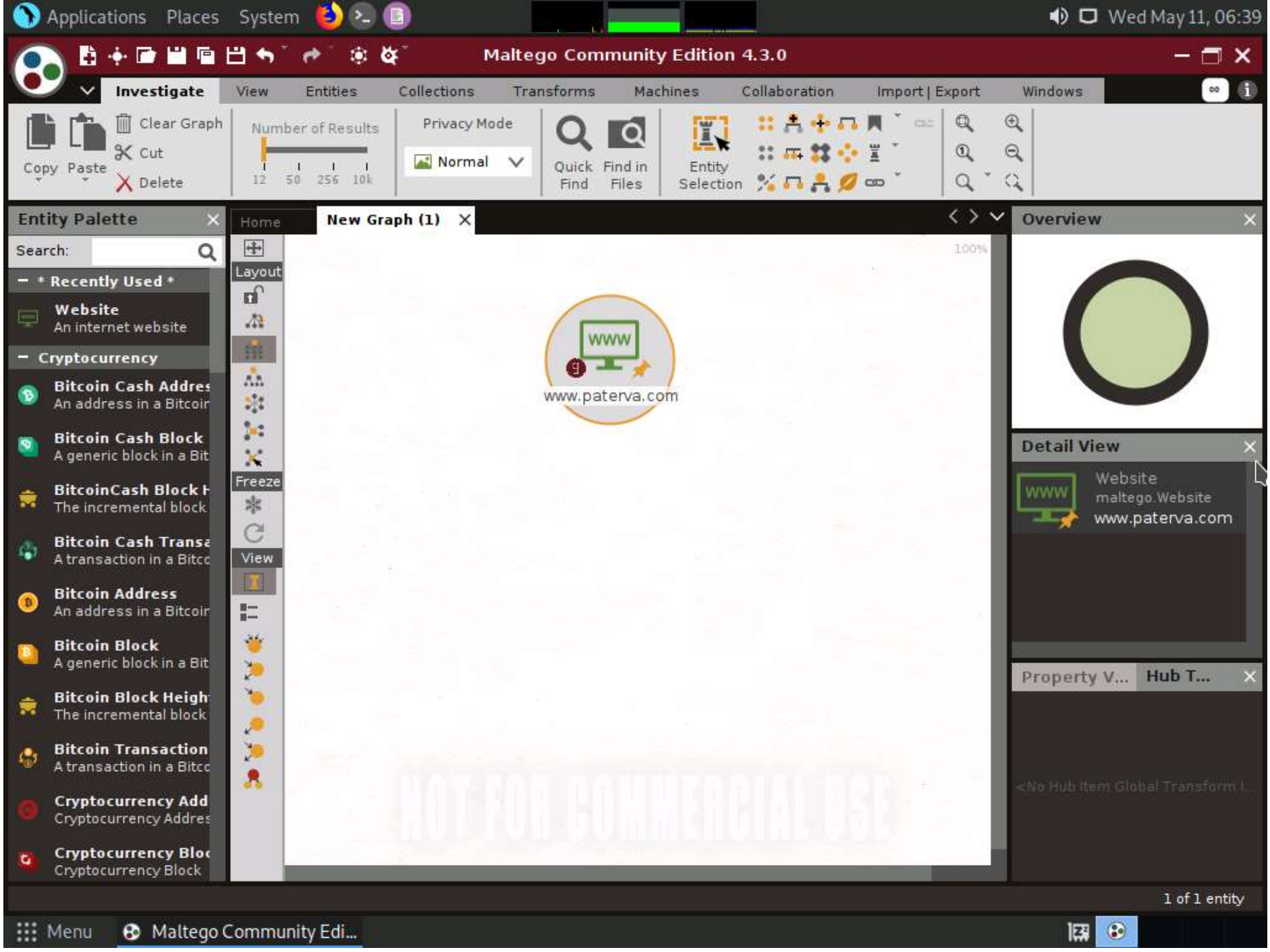


15. In the left-pane of **Maltego GUI**, you can find the **Entity Palette** box, which contains a list of default built-in transforms. In the **Infrastructure** node under **Entity Palette**, observe a list of entities such as **AS, DNS Name, Domain, IPv4 Address, URL, Website,** etc.

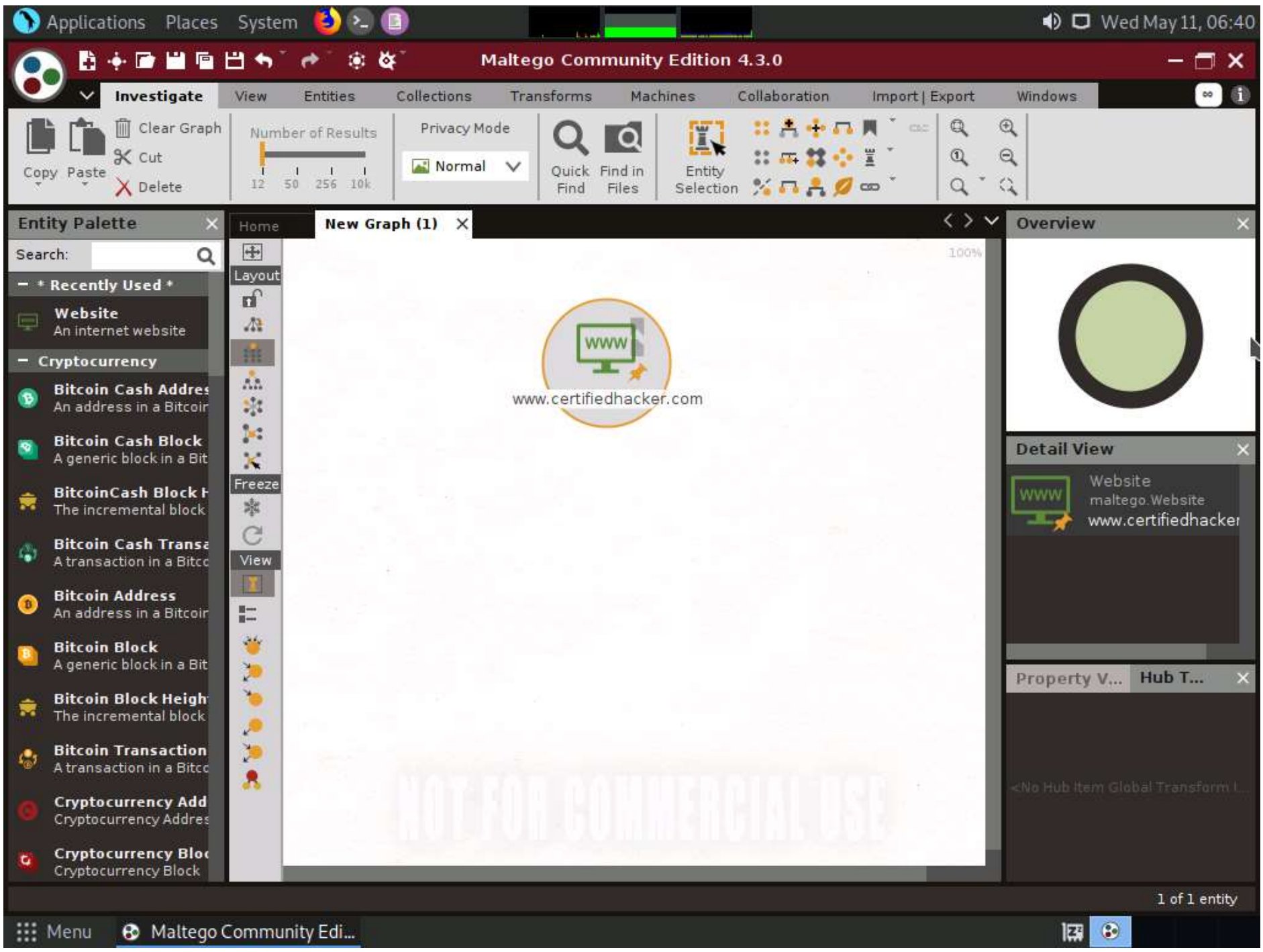
16. Drag the **Website entity** onto the **New Graph (1)** window.

17. The entity appears on the new graph, with the **www.paterva.com** URL selected by default.

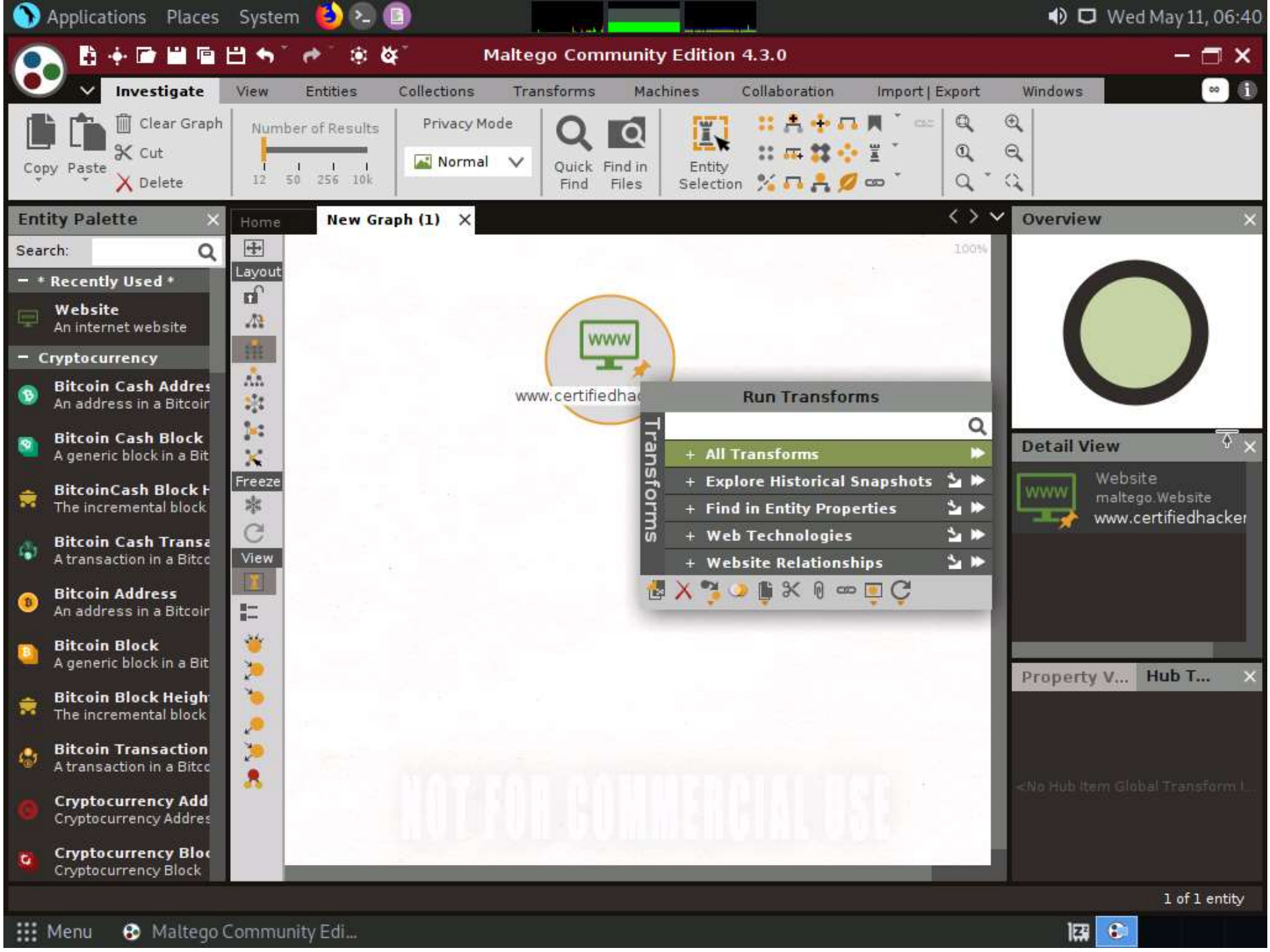
Note: If you are not able to view the entity as shown in the screenshot, click in the New Graph (1) window and scroll up, which will increase the size of the entity.



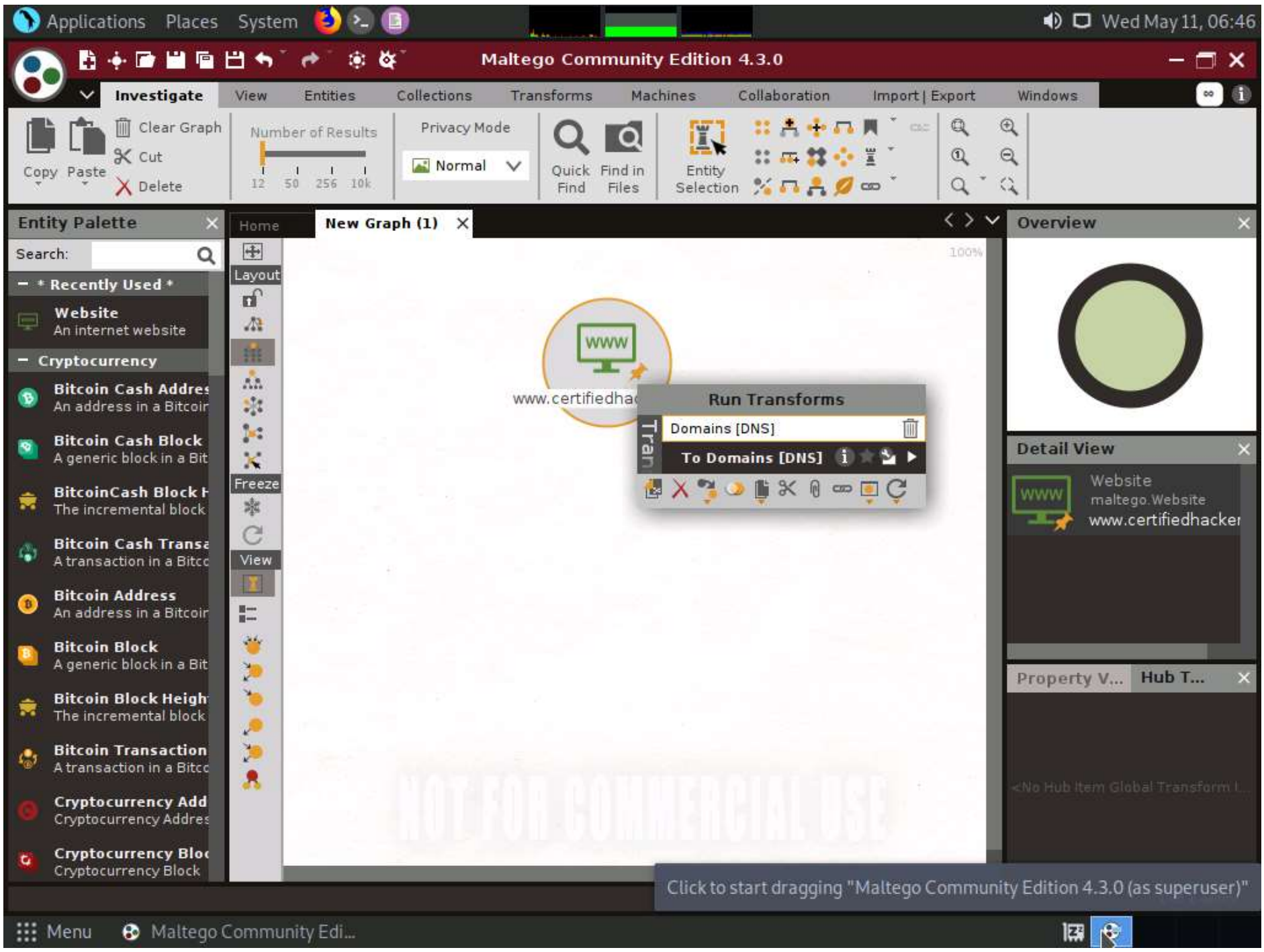
18. Double-click the name **www.paterva.com** and change the domain name to **www.certifiedhacker.com**; press **Enter**.



19. Right-click the **entity** and select **All Transforms**.

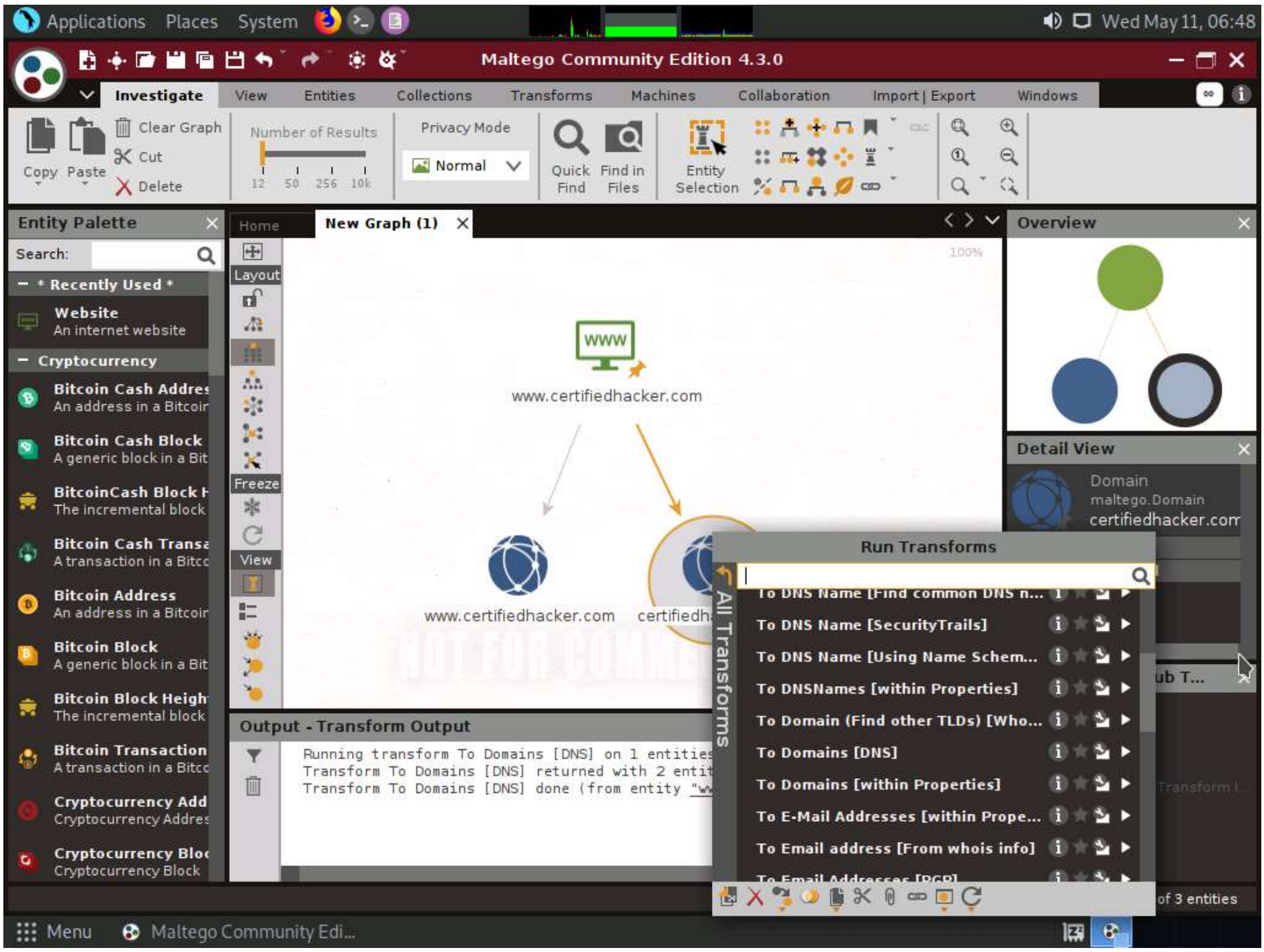


20. Now, right-click the **www.certifiedhacker.com** website entity and select **All Transforms** --> **To Domains [DNS]**.

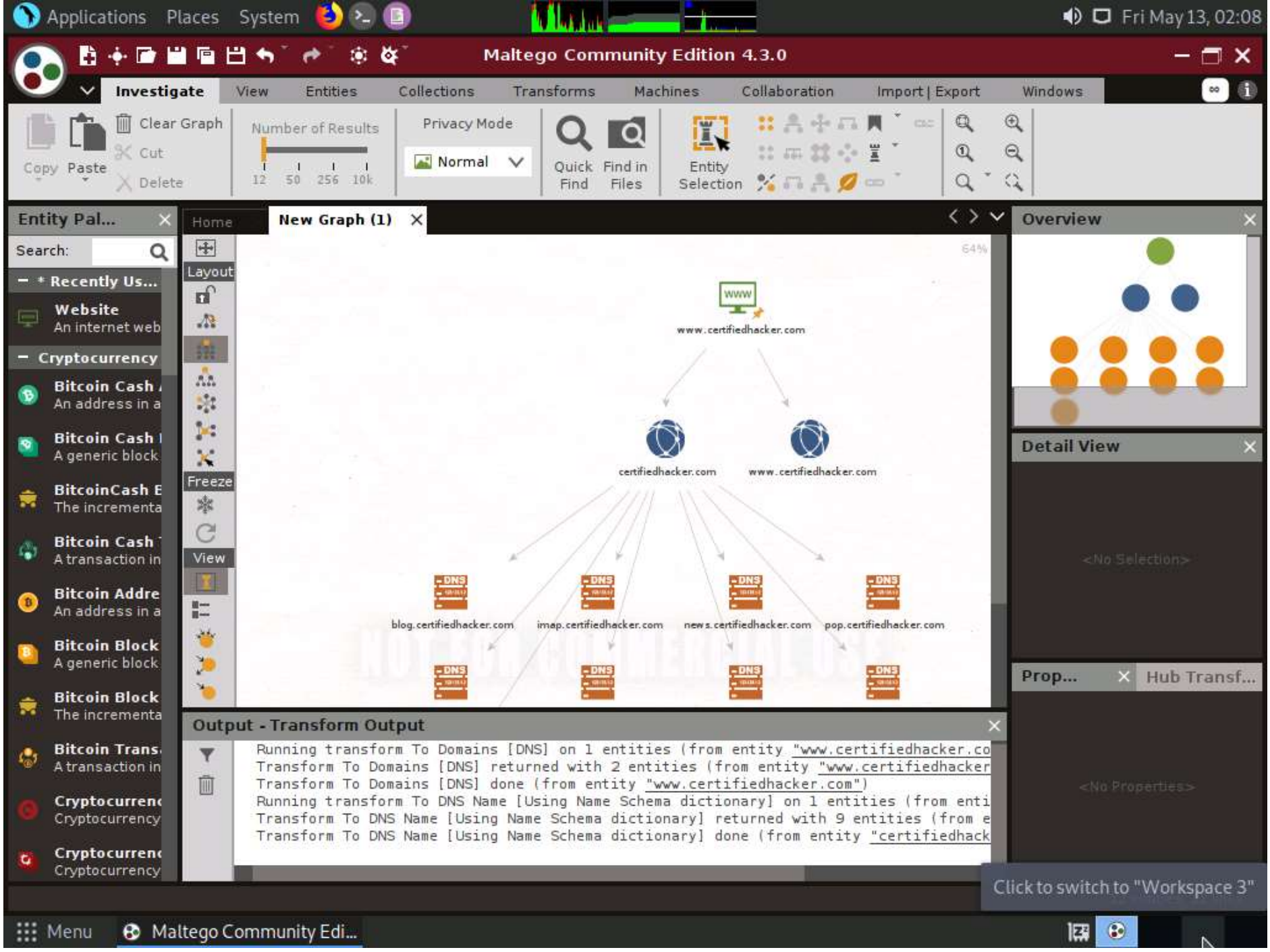


21. The domain corresponding to the website displays, as shown in the following screenshot.

22. Right-click the **certifiedhacker.com** entity and select **All Transforms** ---> **To DNS Name [Using Name Schema diction...]**.



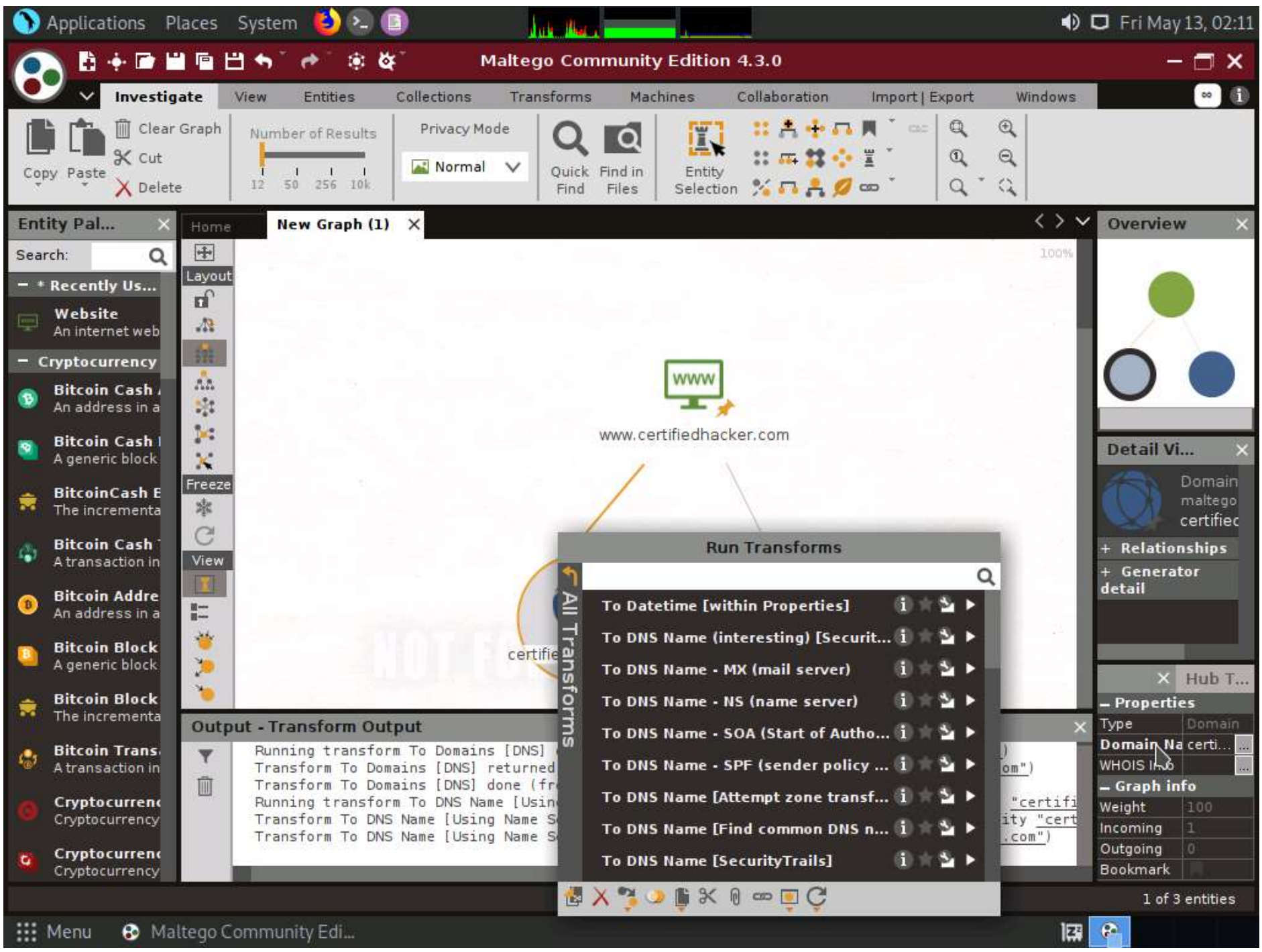
23. Observe the status in the progress bar. This transform will attempt to test various name schemas against a domain and try to identify a specific name schema for the domain, as shown in the following screenshot.



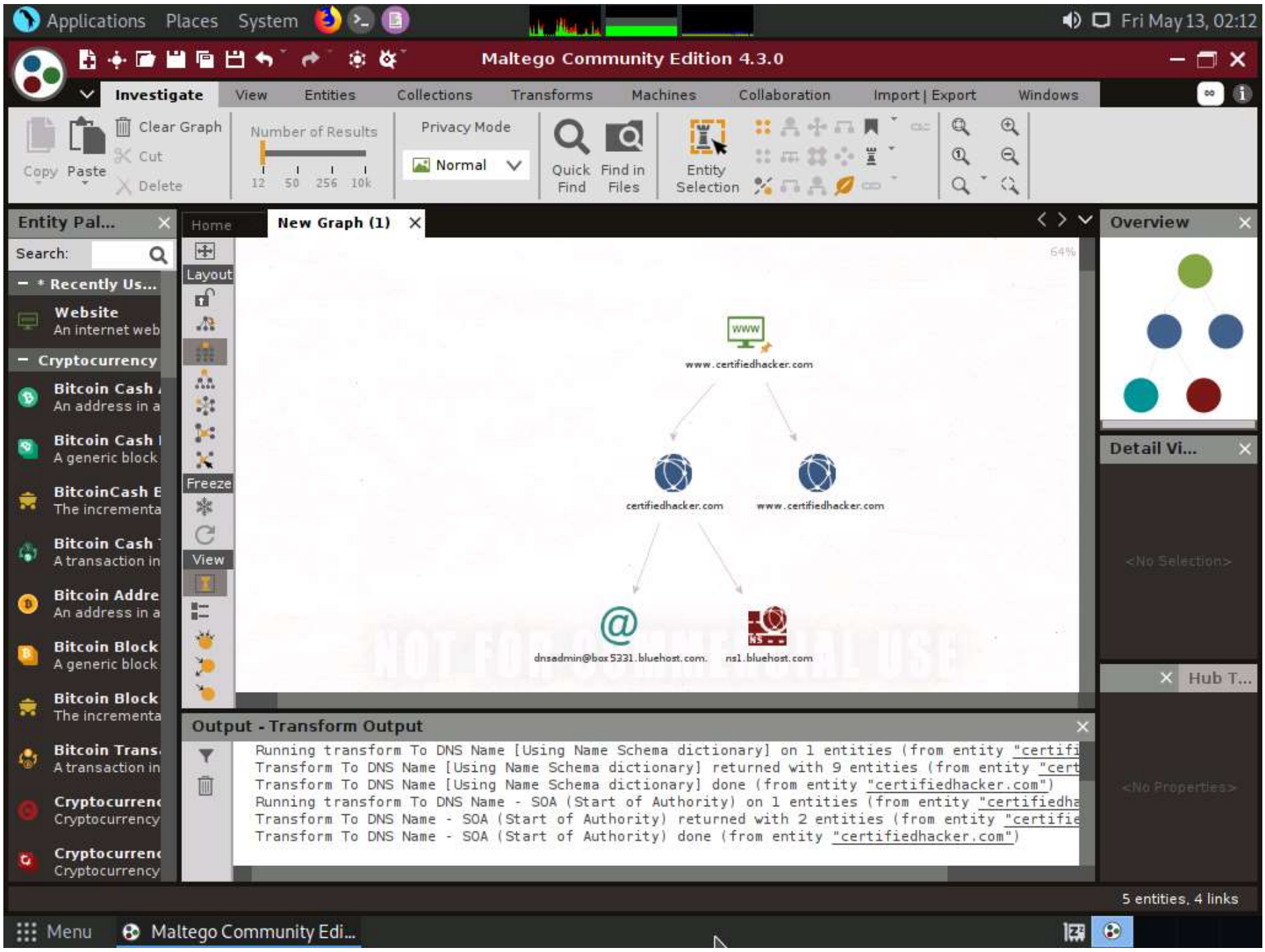
24. After identifying the name schema, attackers attempt to simulate various exploitation techniques to gain sensitive information related to the resultant name schemas. For example, an attacker may implement a brute-force or dictionary attack to log in to **ftp.certifiedhacker.com** and gain confidential information.

25. Select only the name schemas by dragging and deleting them.

26. Right-click the **certifiedhacker.com** entity and select **All Transforms** --> **To DNS Name - SOA (Start of Authority)**.

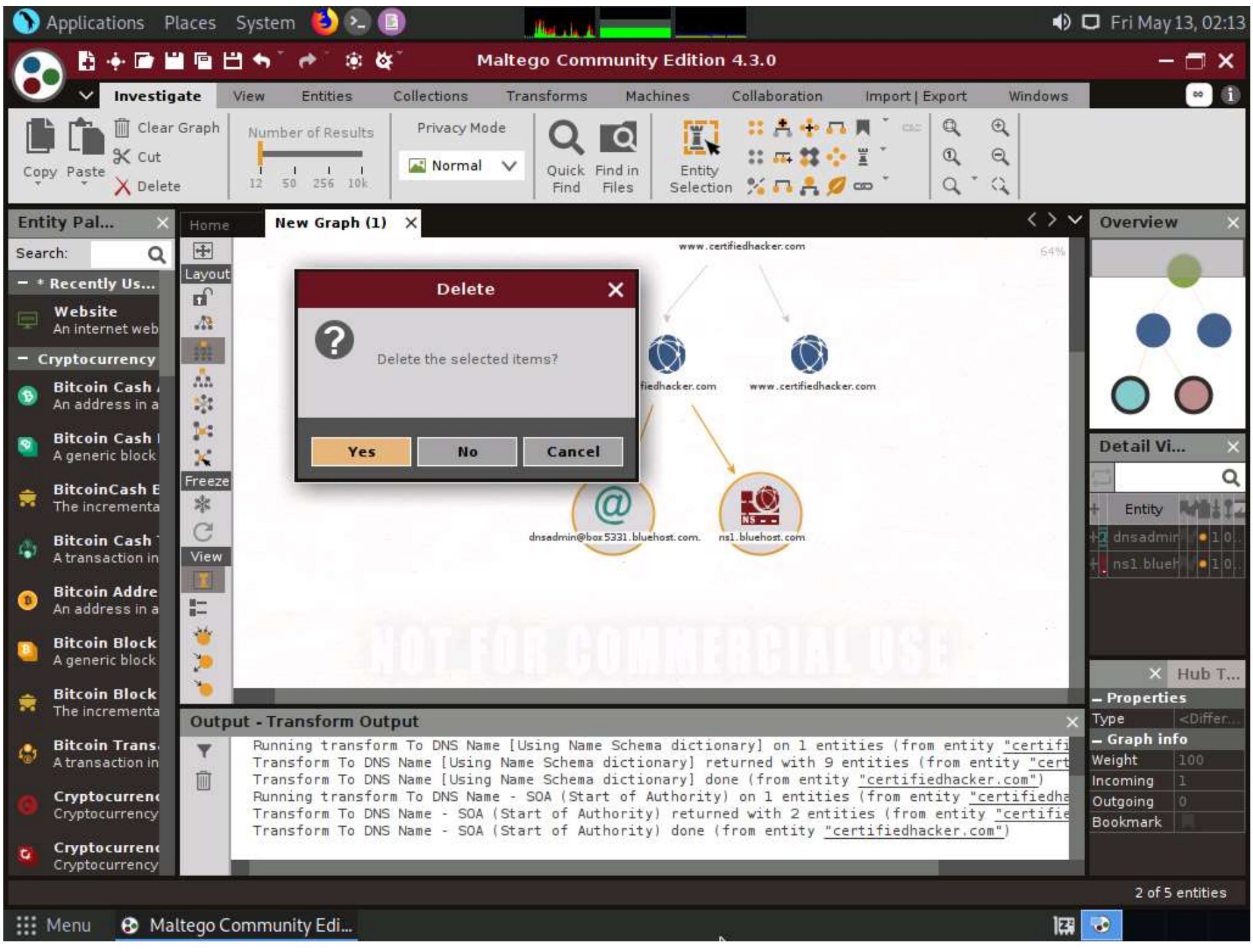


27. This returns the primary name server and the email of the domain administrator, as shown in the following screenshot.

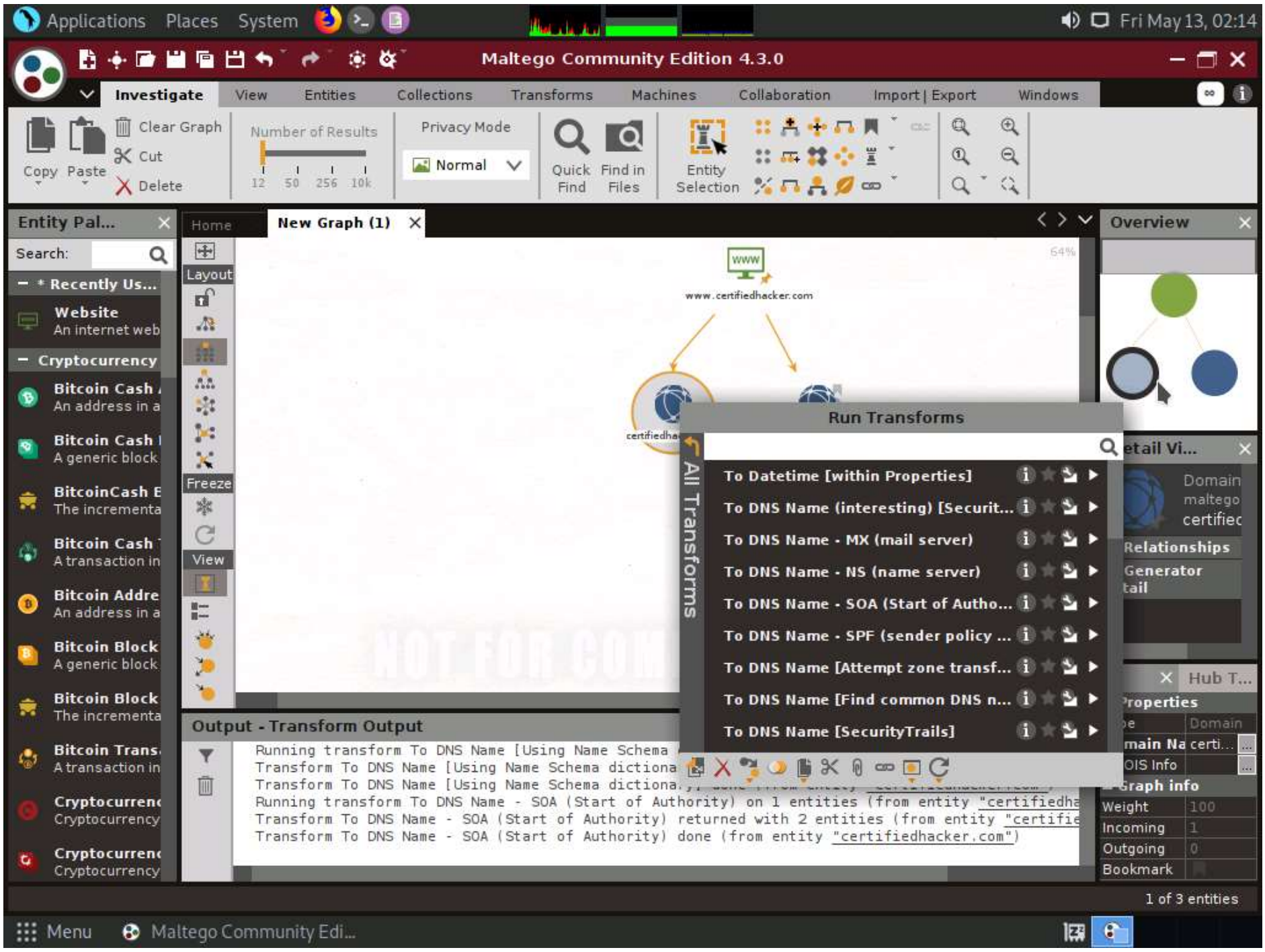


28. By extracting the SOA related information, attackers attempt to find vulnerabilities in their services and architectures and exploit them.

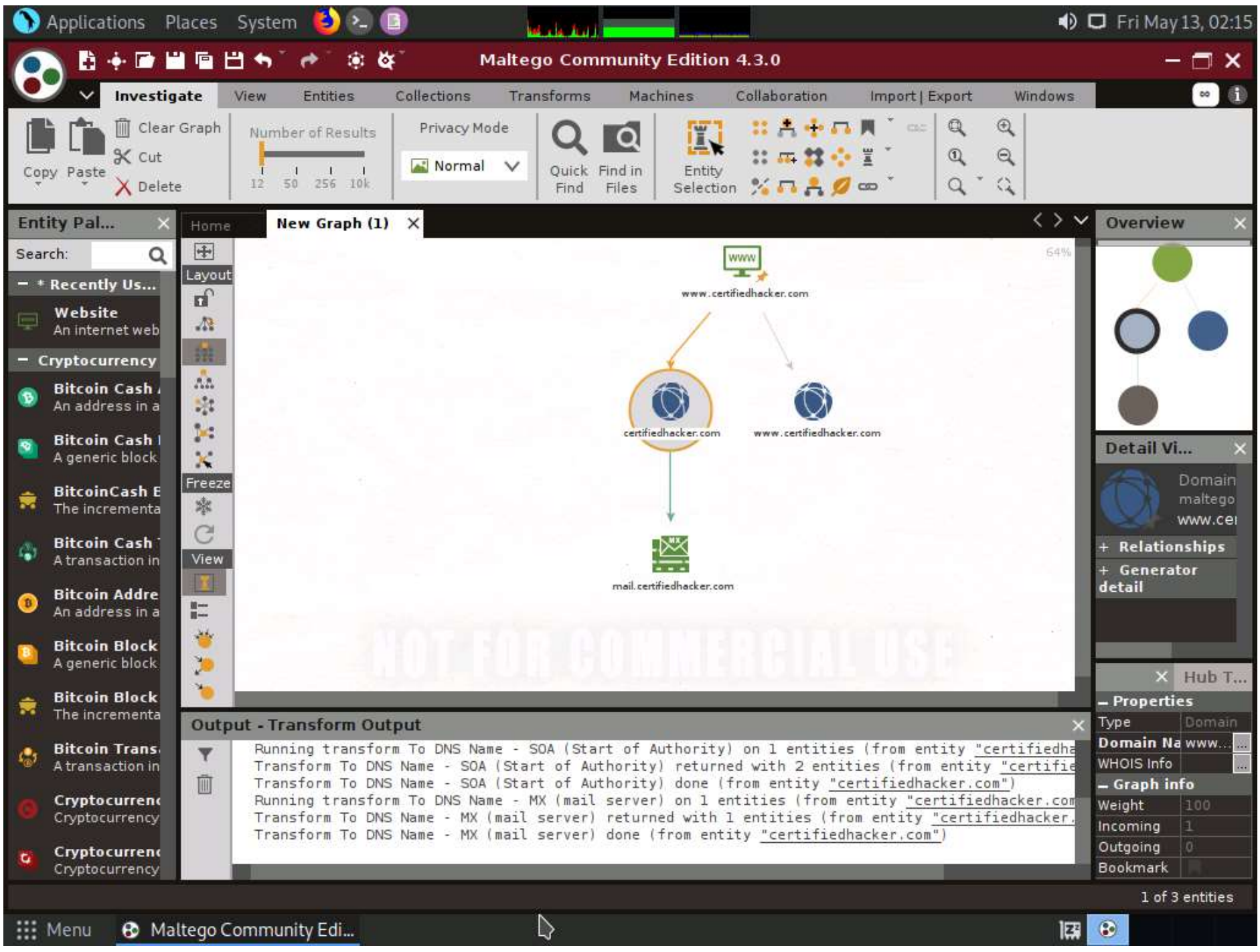
29. Select both the name server and the email by dragging and deleting them.



30. Right-click the **certifiedhacker.com** entity and select **All Transforms** --> **To DNS Name - MX (mail server)**.

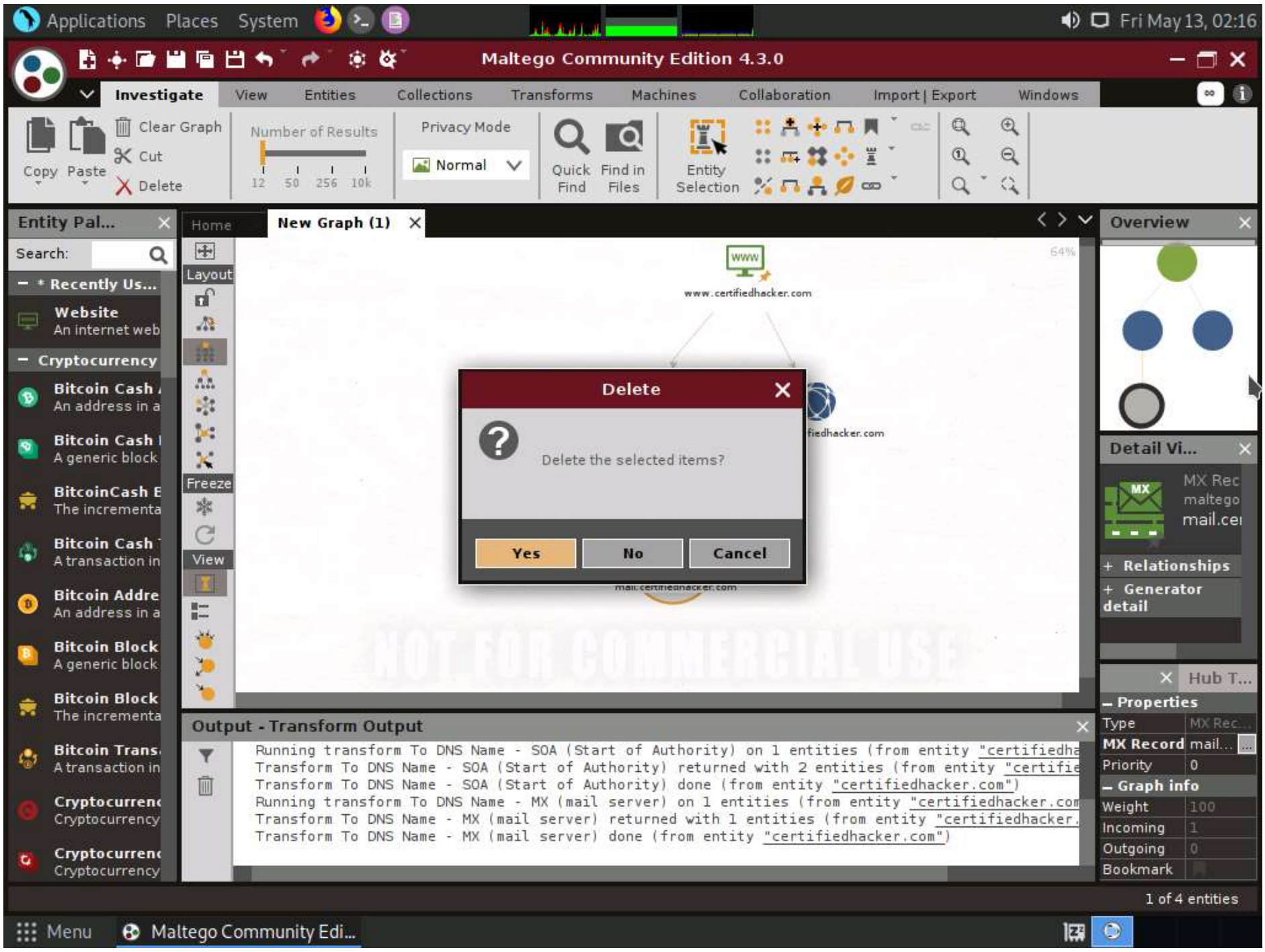


31. This transform returns the mail server associated with the **certifiedhacker.com** domain, as shown in the following screenshot.

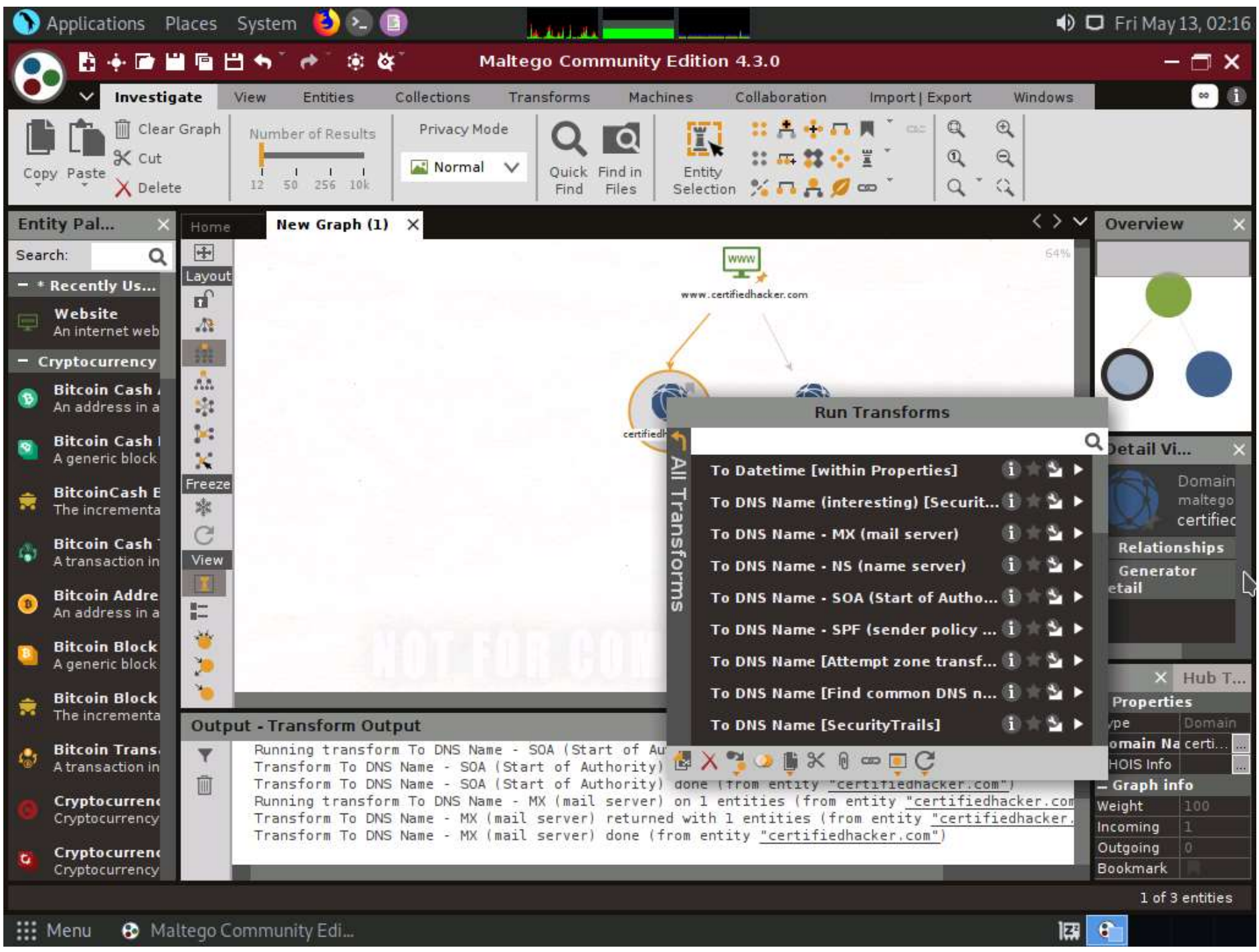


32. By identifying the mail exchanger server, attackers attempt to exploit the vulnerabilities in the server and, thereby, use it to perform malicious activities such as sending spam e-mails.

33. Select only the mail server by dragging and deleting it.



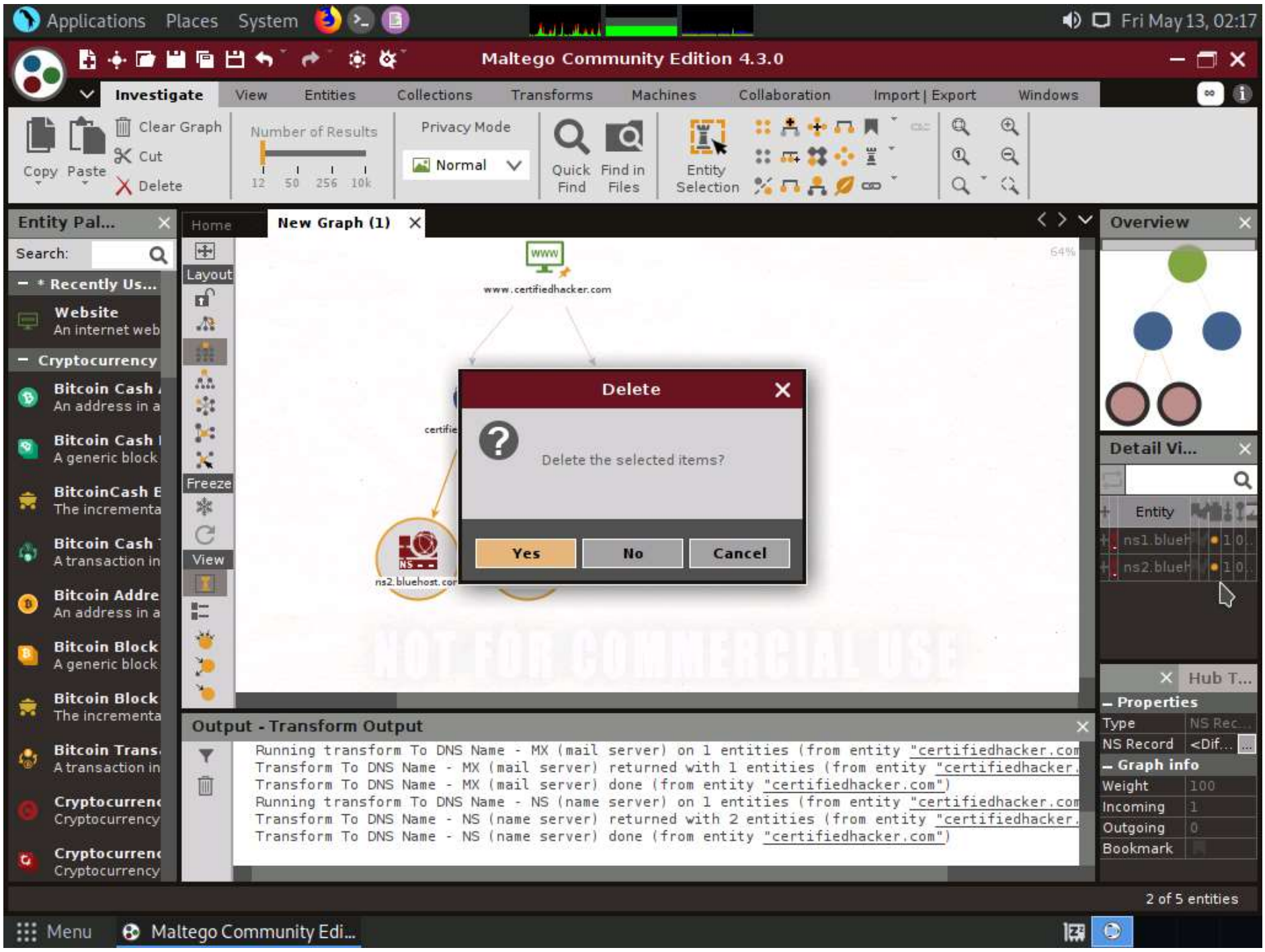
34. Right-click the **certifiedhacker.com** entity and select **All Transforms** --> **To DNS Name - NS (name server)**.



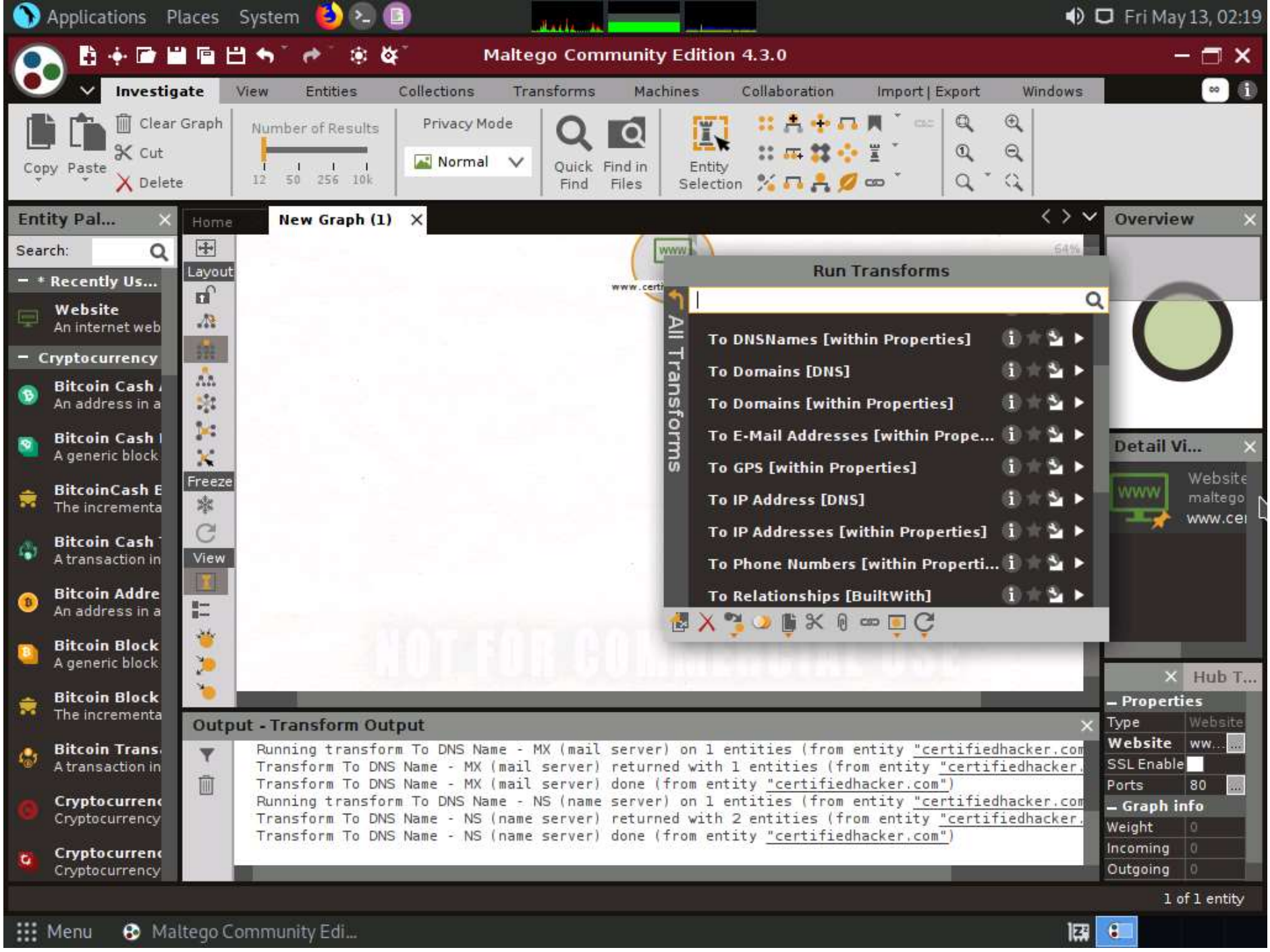
35. This returns the name servers associated with the domain, as shown in the following screenshot.

36. By identifying the primary name server, an attacker can implement various techniques to exploit the server and thereby perform malicious activities such as DNS Hijacking and URL redirection.

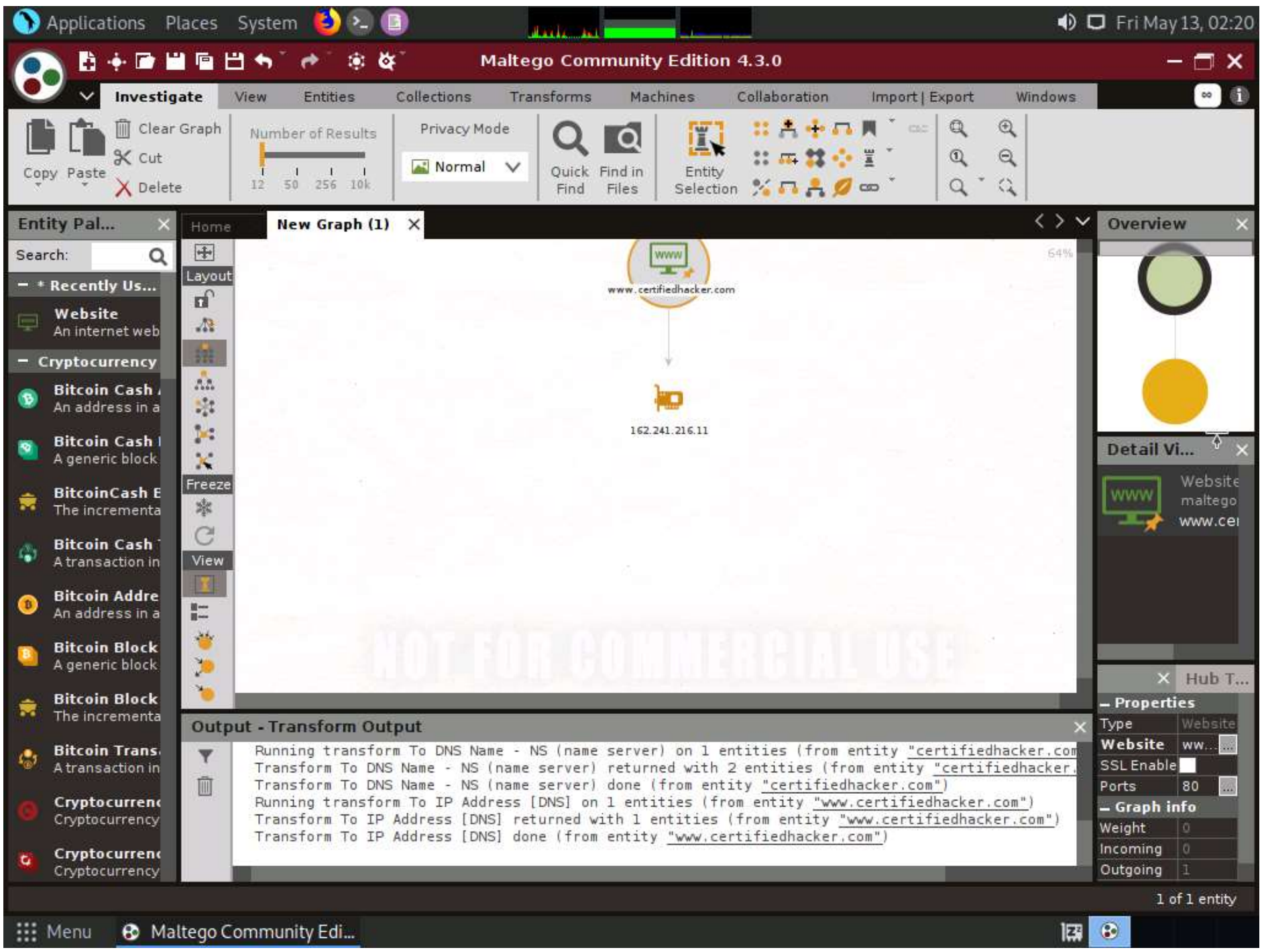
37. Select both the domain and the name server by dragging and deleting them. In the same way delete **certifiedhacker.com** and **www.certifiedhacker.com** entities.



38. Right-click the entity and select **All Transforms** --> **To IP Address [DNS]**.

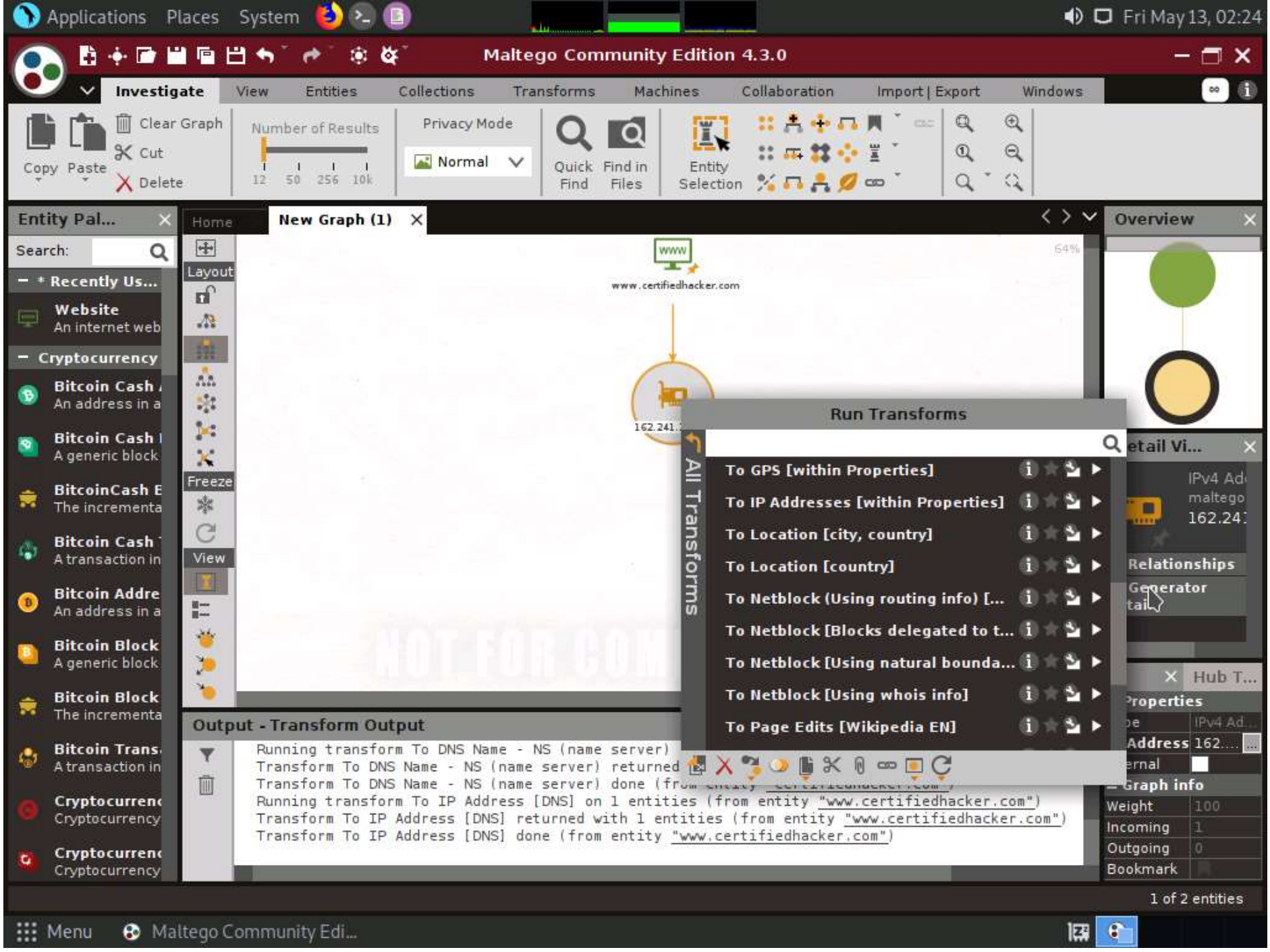


39. This displays the **IP address** of the website, as shown in the following screenshot.

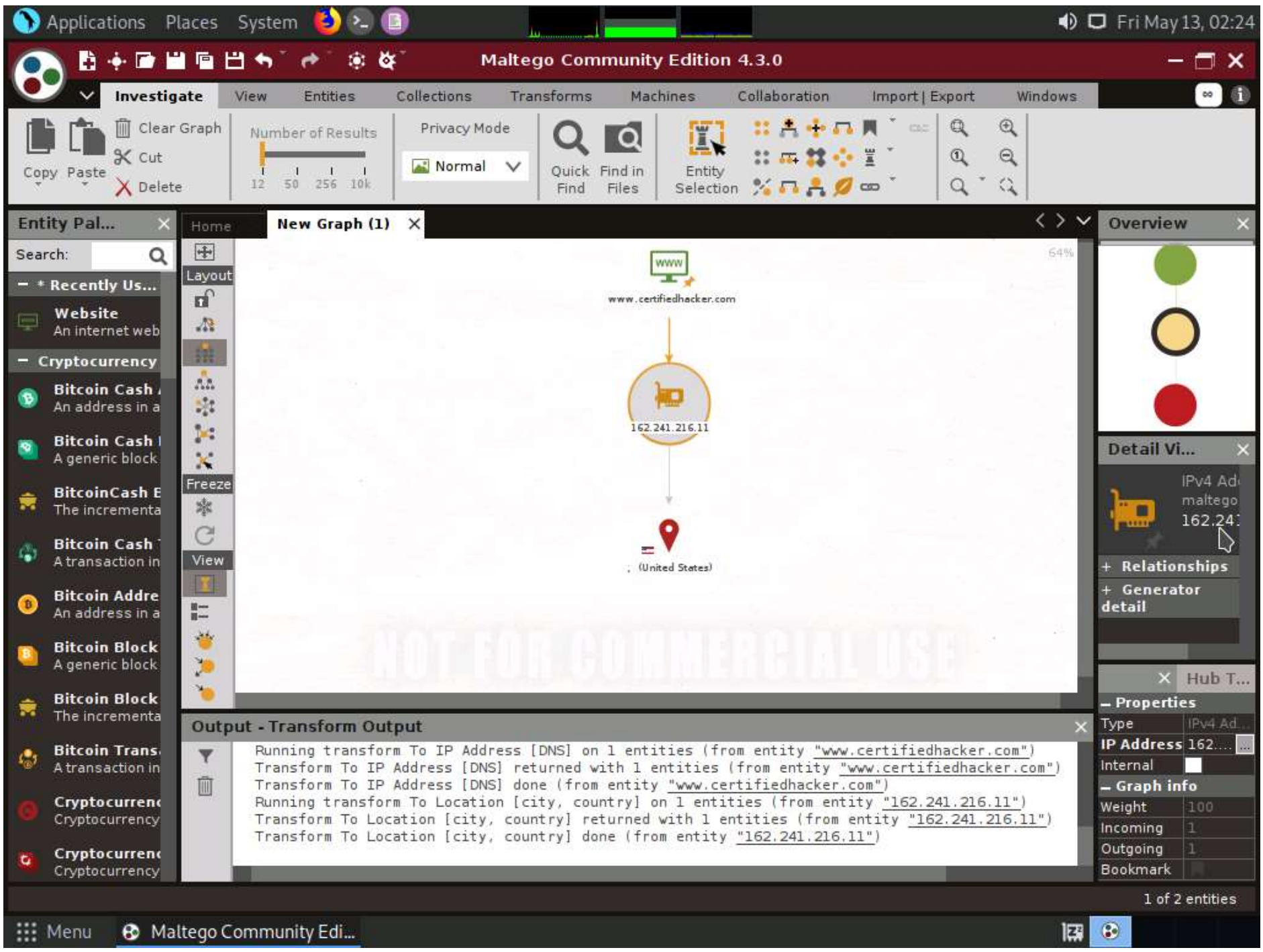


40. By obtaining the IP address of the website, an attacker can simulate various scanning techniques to find open ports and vulnerabilities and, thereby, attempt to intrude in the network and exploit them.

41. Right-click the **IP address entity** and select **All Transforms** --> **To location [city, country]**.

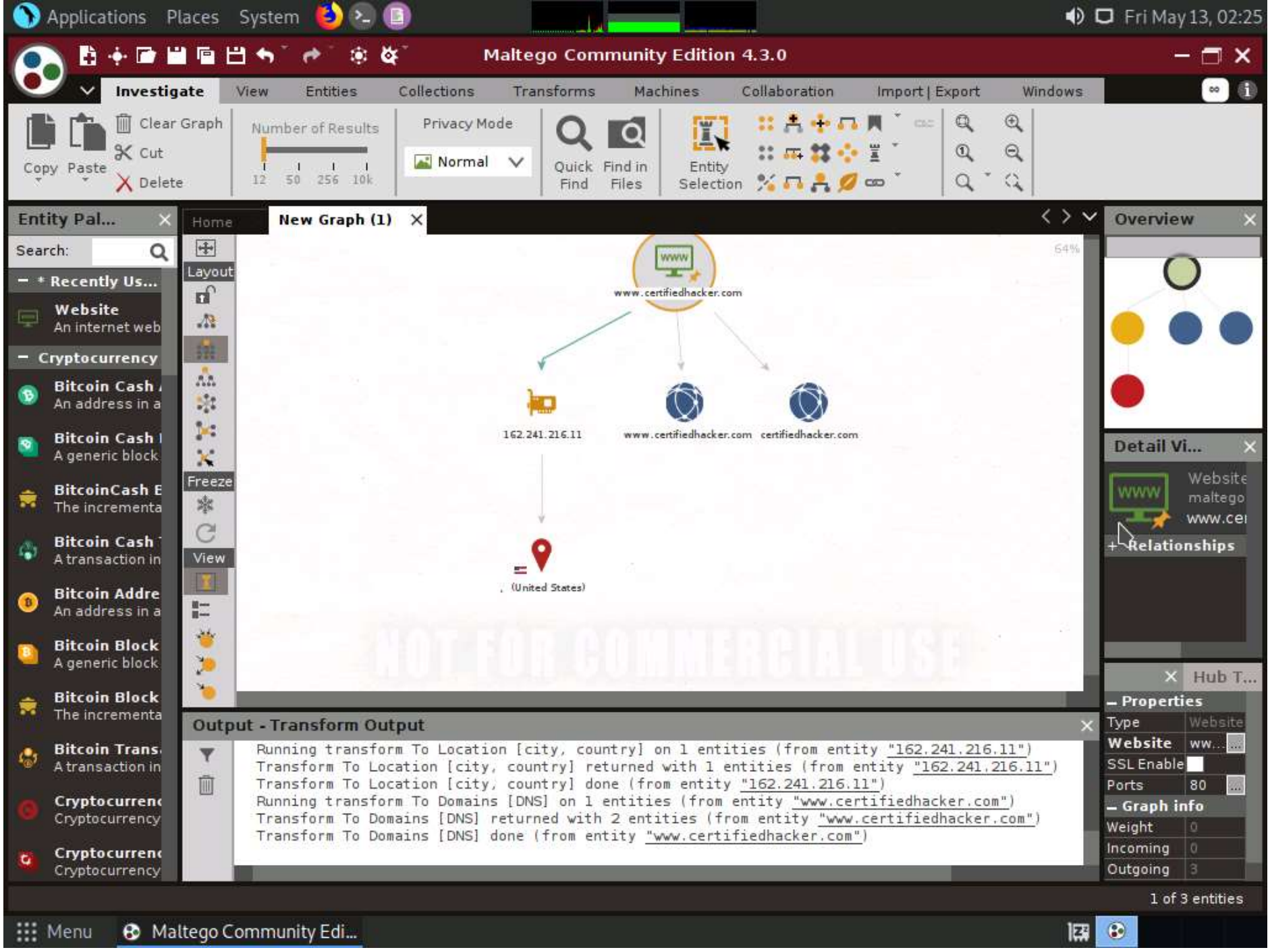


42. This transform identifies the geographical location of the IP address, as shown in the following screenshot.

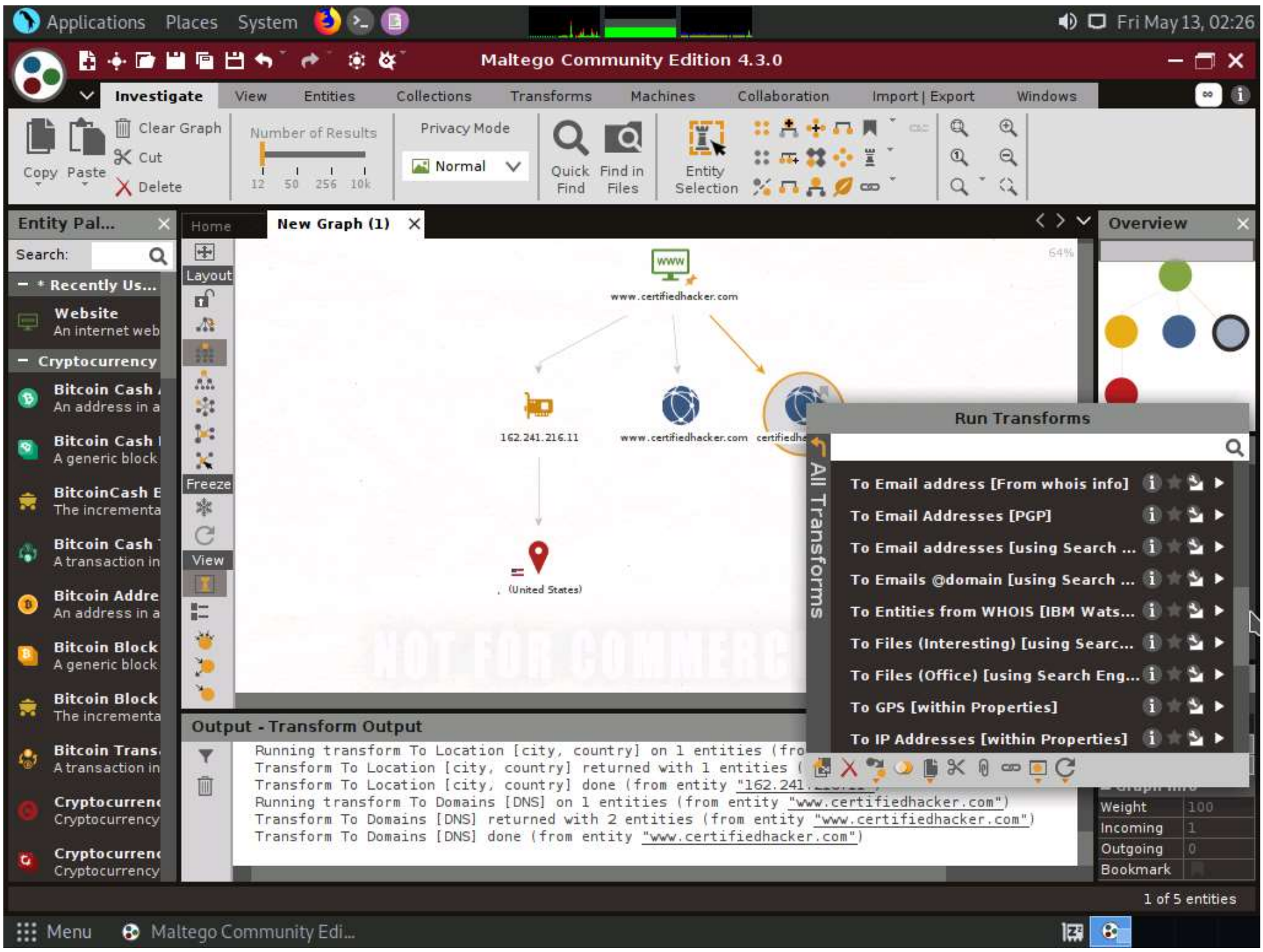


43. By obtaining the information related to geographical location, attackers can perform social engineering attacks by making voice calls (vishing) to an individual in an attempt to leverage sensitive information.

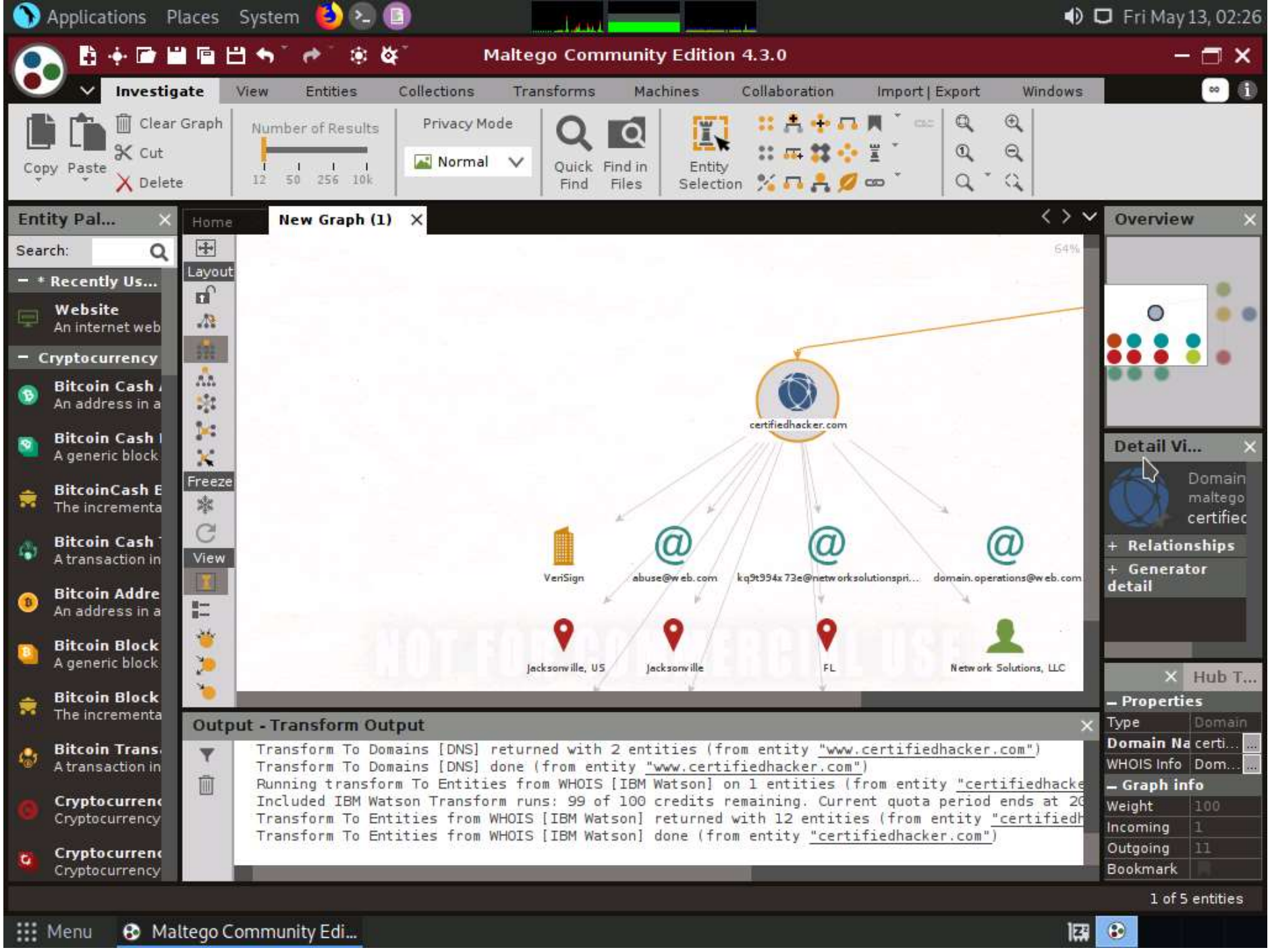
44. Now, right-click the **www.certifiedhacker.com** website entity and select **All Transforms** --> **To Domains [DNS]**. The domains corresponding to the website display, as shown in the screenshot.



45. Right-click the **domain entity (certifiedhacker.com)** and select **All Transform** --> **To Entities from WHOIS [IBM Watson]**.



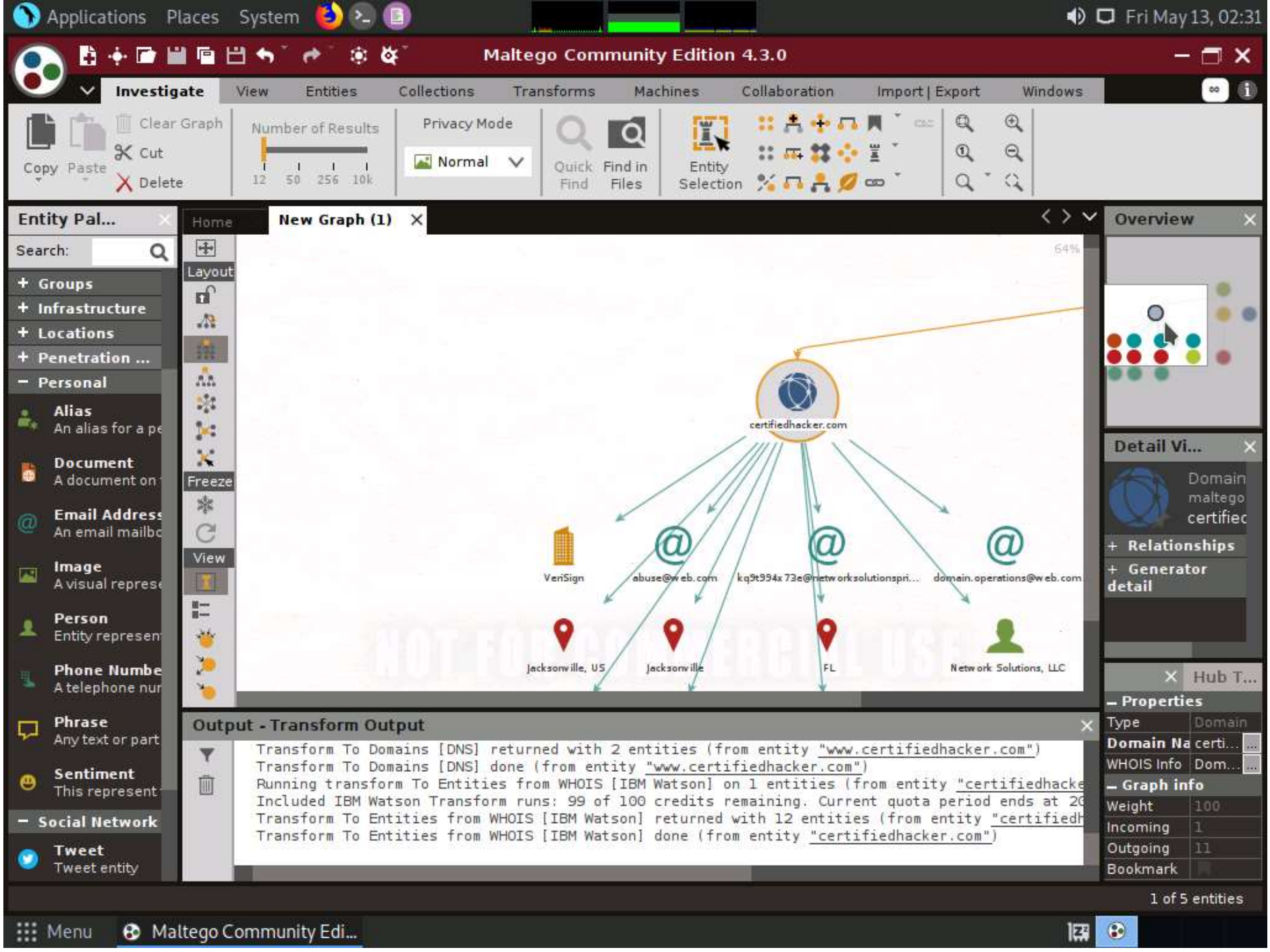
46. This transform returns the entities pertaining to the owner of the domain, as shown in the following screenshot.



47. By obtaining this information, you can exploit the servers displayed in the result or simulate a brute force attack or any other technique to hack into the admin mail account and send phishing emails to the contacts in that account.

48. Apart from the aforementioned methods, you can perform footprinting on the critical employee from the target organization to gather additional personal information such as email addresses, phone numbers, personal information, image, alias, phrase, etc.

49. In the left-pane of the Maltego GUI, click the **Personal** node under **Entity Palette** to observe a list of entities such as **Email Address, Phone Numbers, Image, Alias, Phrase,** etc.



50. Apart from the transforms mentioned above, other transforms can track accounts and conversations of individuals who are registered on social networking sites such as Twitter. Extract all possible information.

51. By extracting all this information, you can simulate actions such as **enumeration, web application hacking, social engineering,** etc., which may allow you access to a **system or network, gain credentials,** etc.

52. This concludes the demonstration of **footprinting a target using Maltego**.

53. Close all open windows and document all the acquired information. ego**.

54. Close all open windows and document all the acquired information.