BUBT

Bangladesh University of Business & Technology

Assignment On

Maltego

Course Title ***: Cyber Security and Digital Forensic Lab***

Course Code ***: CSE-414***

Submitted By:

Md Sahrial Alam(17182103334)

Intake 38, Section 05

CSE Department

Submitted To:

Tanvir Hassan Zoha

Lecturer , Department of CSE

Bangladesh University of Business & Technology(BUBT)

Maltego

Introduction: Maltego is a powerful OSINT information gathering tool. For effective and successful penetration testing, information gathering is a prime aspect, and must be therefore given utmost importance. An attacker would attempt to gather as much information as he can about the target before executing an attack. Information gathering constitutes of about 80% part of the attack. Maltego enables the attack to be more refined and efficient than if it were carried out without much information about the target. "Maltego is a software used for open-source intelligence and forensics, developed by Paterva from Pretoria, South Africa. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format". Maltego is one of the best information gathering and data mining tools. In Maltego alone, users can query all types of data thanks to data integrations with Shodan, WHOIS, TinEye, The Wayback Machine, VirusTotal, ATT&CK, and MISP, Pipl, Orbis, and more.

Objective of Maltego:

- **Cyber Threat Intelligence:** Visualize and understand the attack surface. Help prevent potential threats to infrastructure.
- **Digital Risk Protection:** Investigate and help protect against unwanted asset exposure resulting from Digital Transformation efforts.
- **Business Risk Intelligence:** Reduce an organizational risk by visualizing Intel from illicit communities where threat actors discuss how to access and monetize proprietary data.
- **Cryptocurrency and the block chain:** Gather and link digital evidence on suspicious use of crypto currencies.

Maltego User: Maltego is pre-installed in Kali Linux. We can always download maltego for Windows, Linux or Mac.

Maltego has 3 different packs-

1. Community
2. Professionals
3. Enterprises

Community version is free to use and others are paid with more features.

Feature of Maltego Tools:

- The ability to perform link analyses on up to 10,000 Entities on a single graph.
- The capability to return up to 10,000 results per Transform run
- Includes collection nodes which automatically group entities together with common features allowing you to see past the noise and find the key relationships you are looking for
- Includes the ability to share graphs in real-time with multiple analysts in a single session
- Graph export options include:
- Images - jpg, bmp, and png.
- Generate PDF reports
- Tabular formats - csv, xls and xlsx
- GraphML
- Entity lists
- Graph import options include:
- Tabular formats - csv, xls and xlsx
- Copy and paste

Step by Step Work Process:

Starting the Maltego : Go to **Applications → Information Gathering → Maltego.**

Or In command Shell write maltego

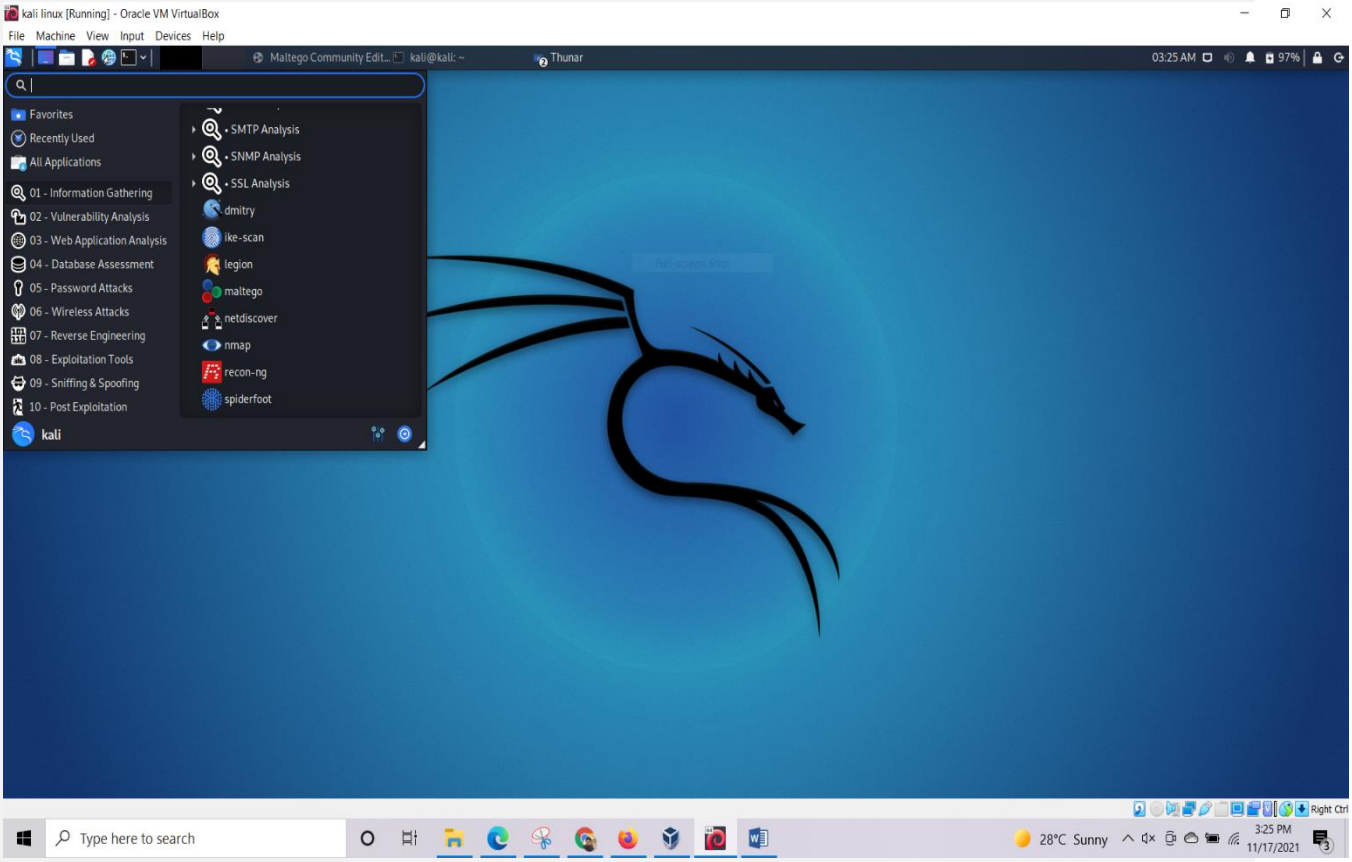

Fig 1: To find Maltego

Fig 2: To find Maltego in Command Line

Now at the start Maltego ask for Product Selection. Here , I'm choosing the CE version. After running the instance we'll be asked to register or login if we already have a account.

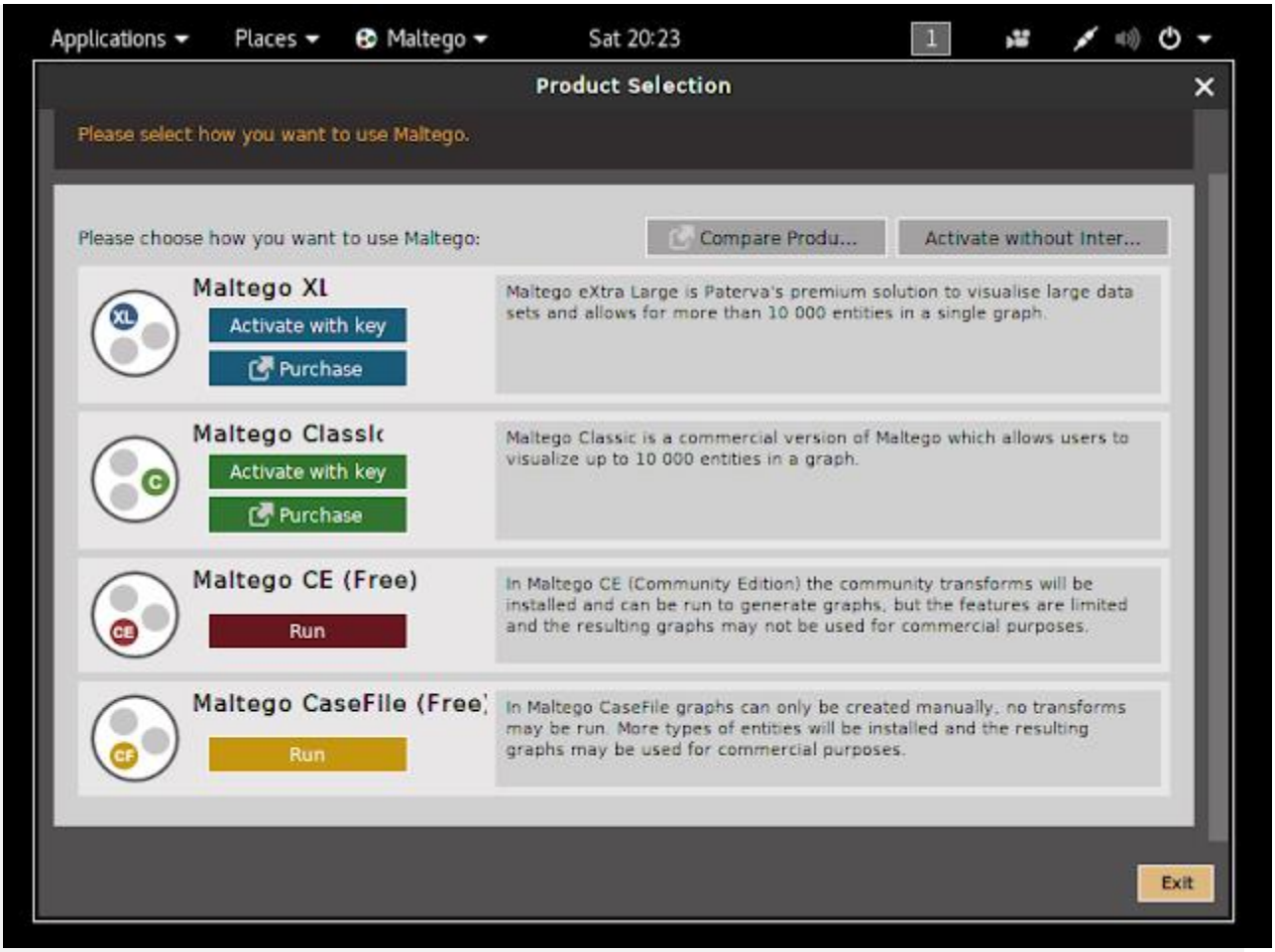

Fig 3: Maltego CE(Free)

Here, in these examples I'm showing we how to use Maltego for infrastructural reconnaissance.

After entering all the credentials we''ll see maltego home screen.

When we open the maltego after setting it up there are some buttons at top left corner. let's talk about them.

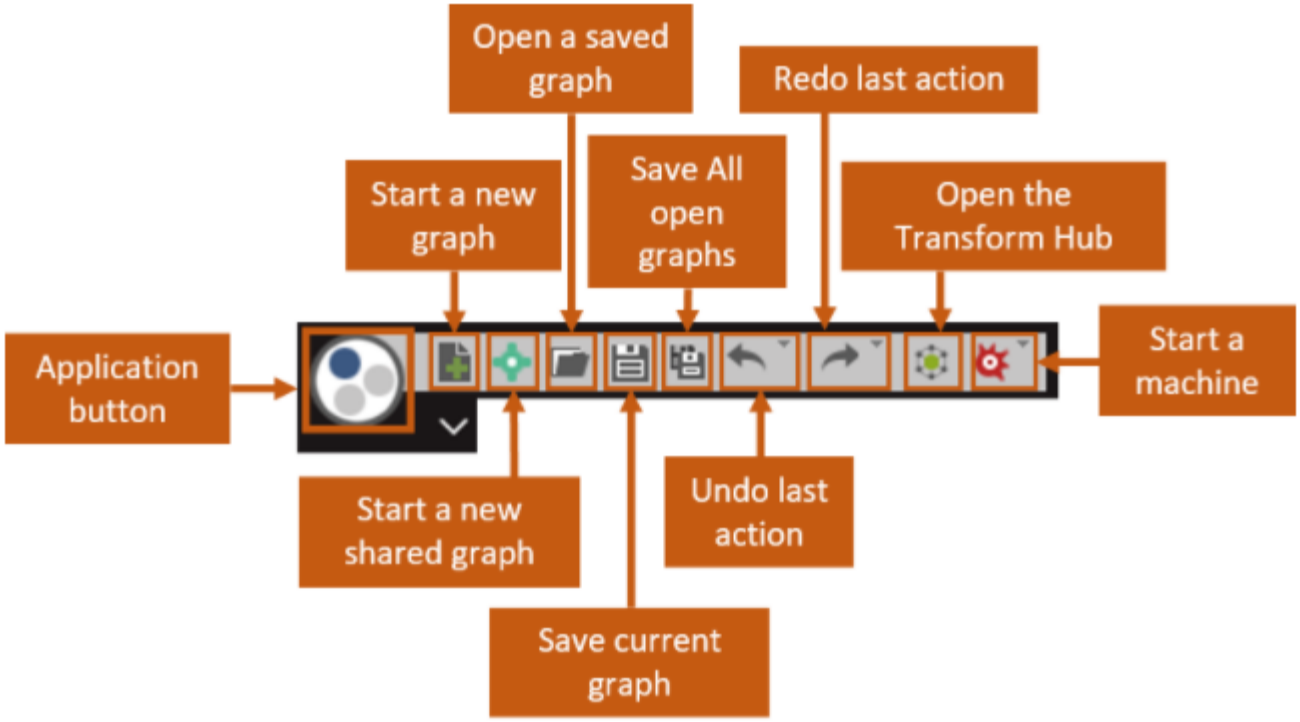

Fig 4.1: Maltego Feature info

The Application button will open a application menu.

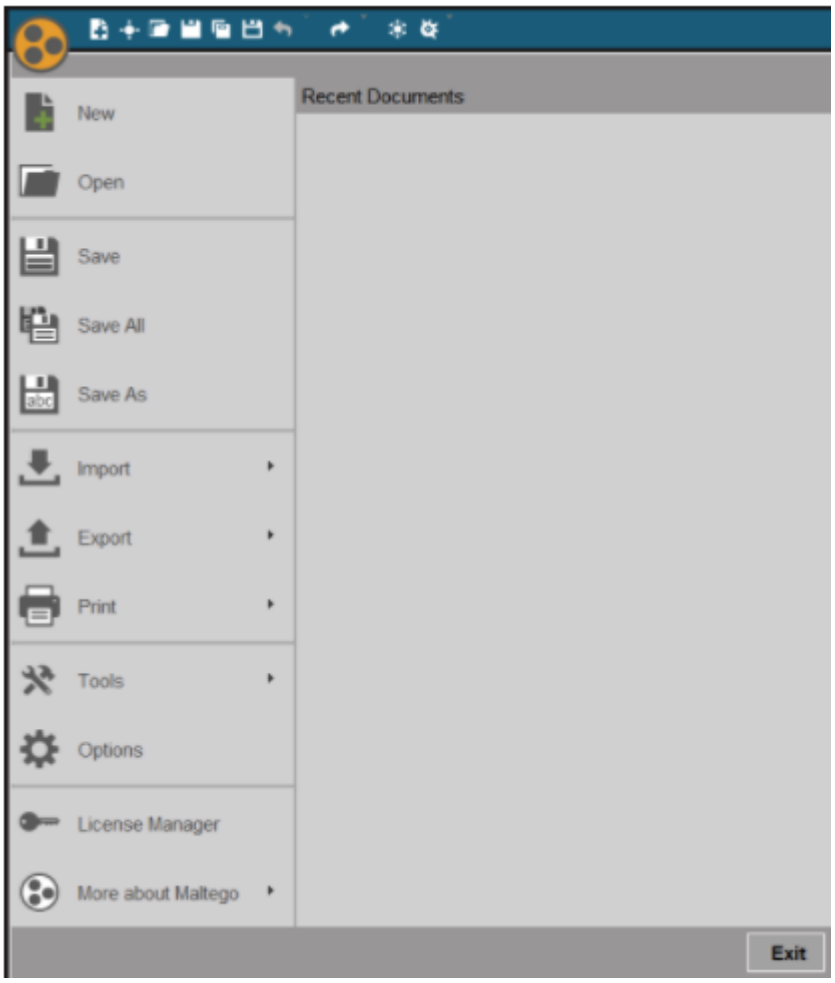

Fig 4.2: Maltego Feature info

Maltego uses graphs to show data and information it collects. Now, let's see how to how to create a new graph.

Graphs in Maltego

To create new graph.

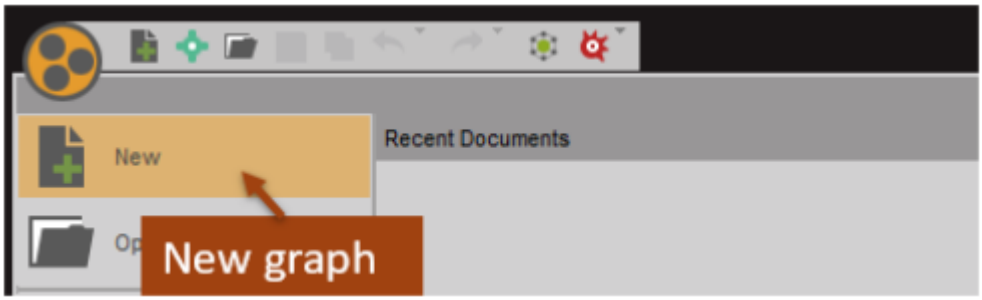

Fig 5: Create New File

To create a new graph we can go to application tab and click on new graph or we can also select new graph option from top left corner

Now Navigate to Entry Palette and just drag the ‘Domain’ icon to the center of the screen. Change ‘paterva.com’ to ‘any_website_we_want_gather_info_about’ by double clicking on it.

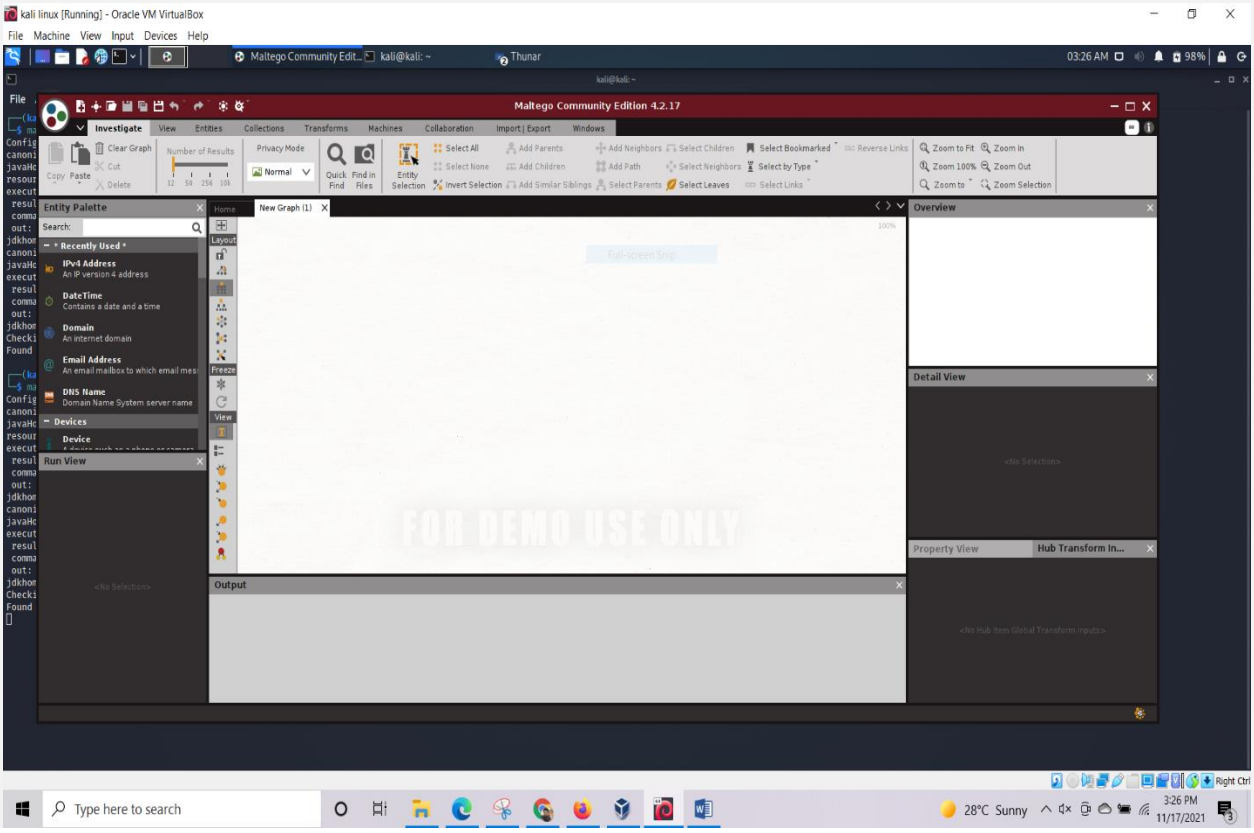

Fig 6: Maltego New File

Now,, right click the icon and press right arrow to run all transformations. at bottom of the screen a bar goes from 0 to 100% when all the transforms are done and our graph gets filled.

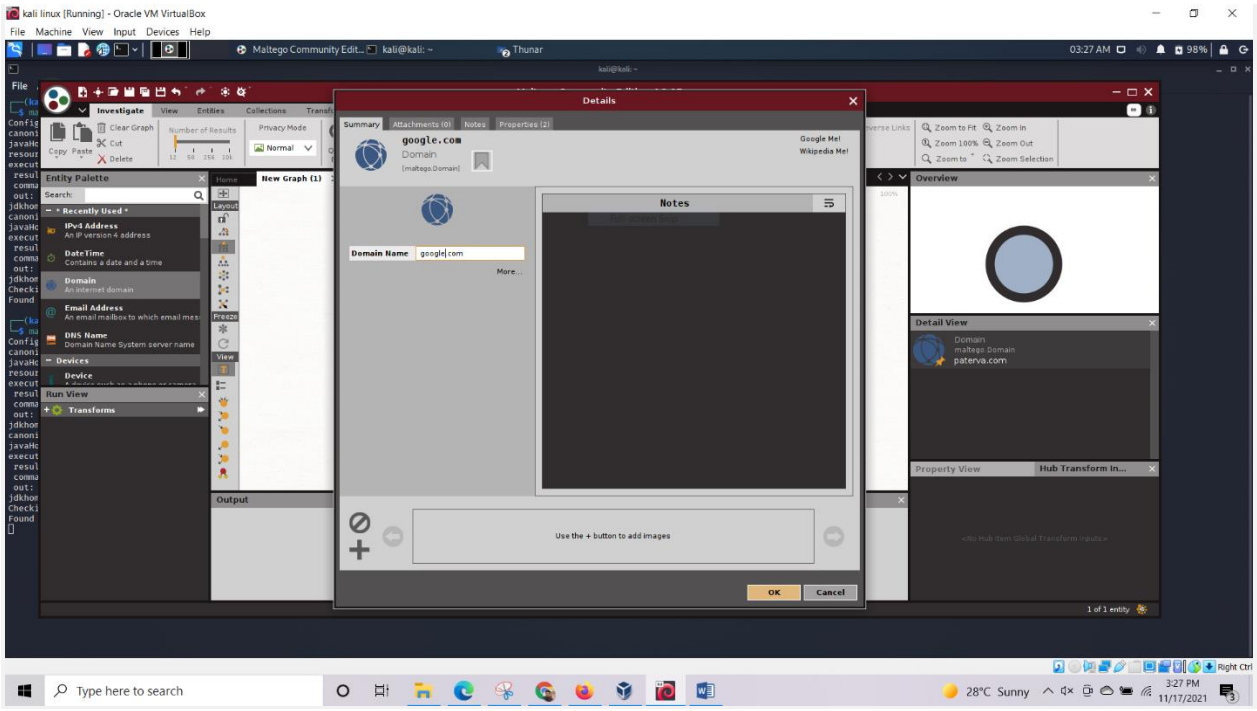

Fig 7: Domain Name

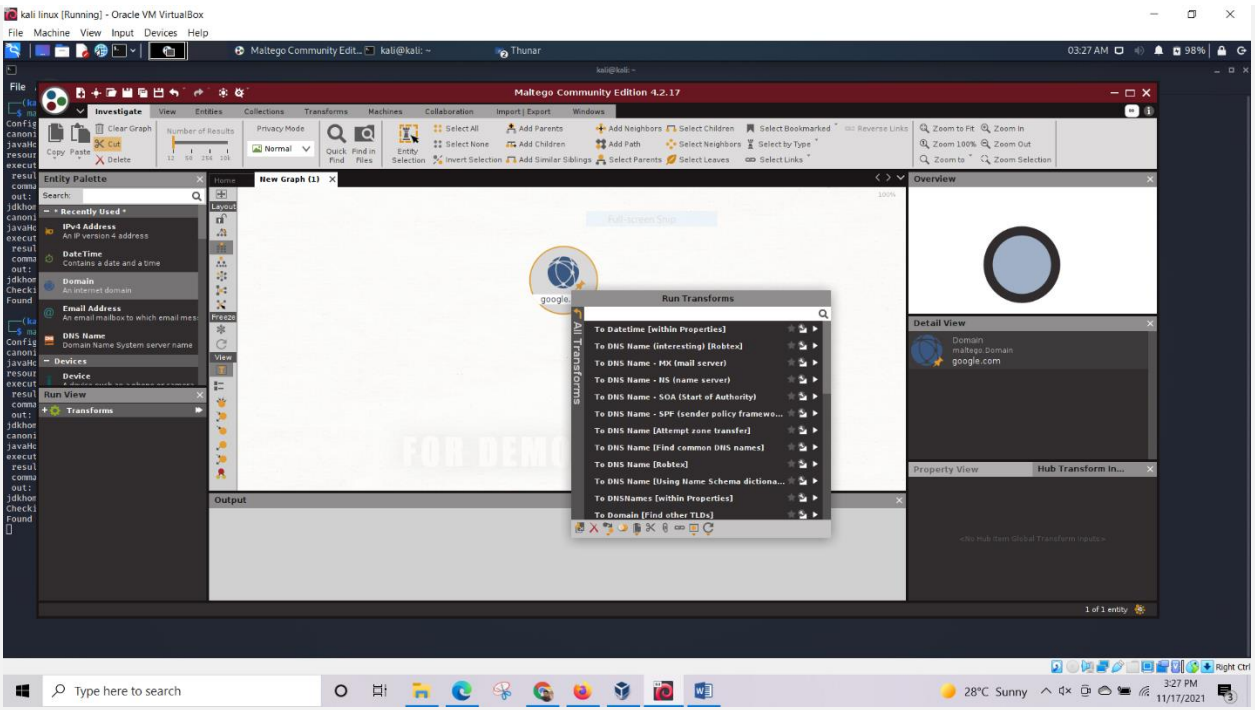

Fig 8: Domain Name Info

After running all the transforms we”ll notice that the graph is expanding. This expansions gives information about the related entities.

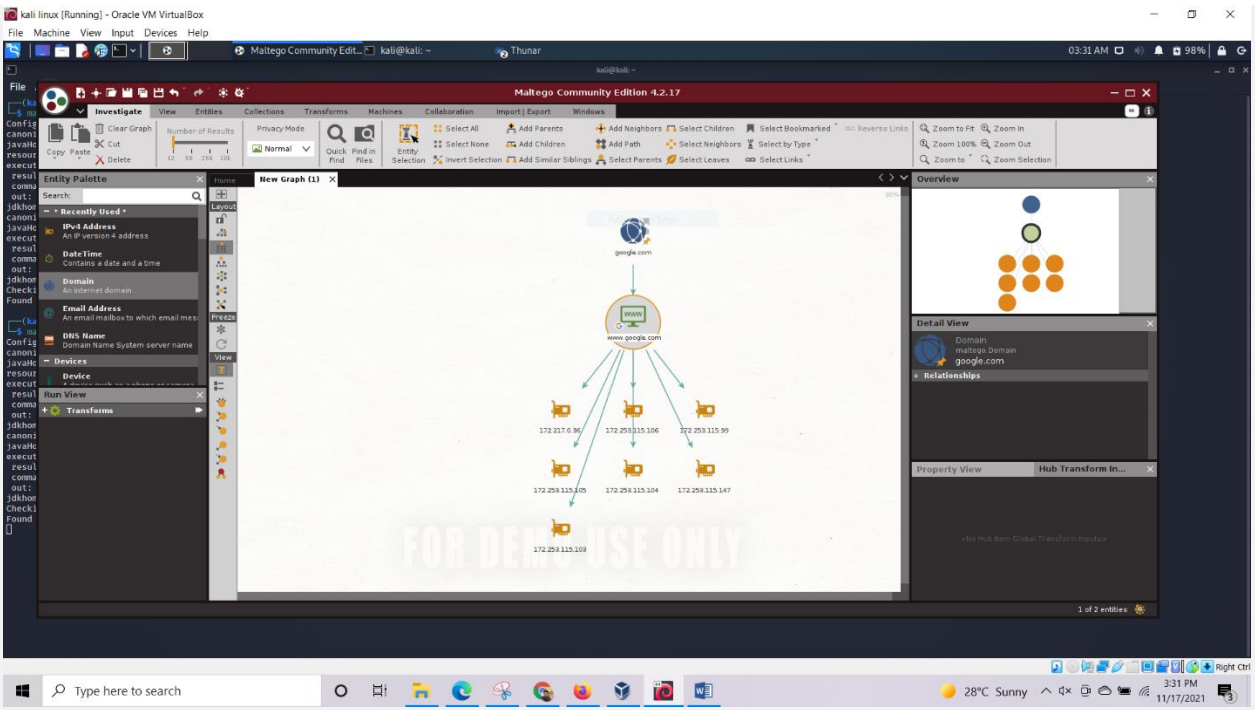

Fig 9: Domain Name Ip

Further expanding the targeted domain we''ll come to know on which server the site is hosted and various details like when the site was created and when the domain was purchased.

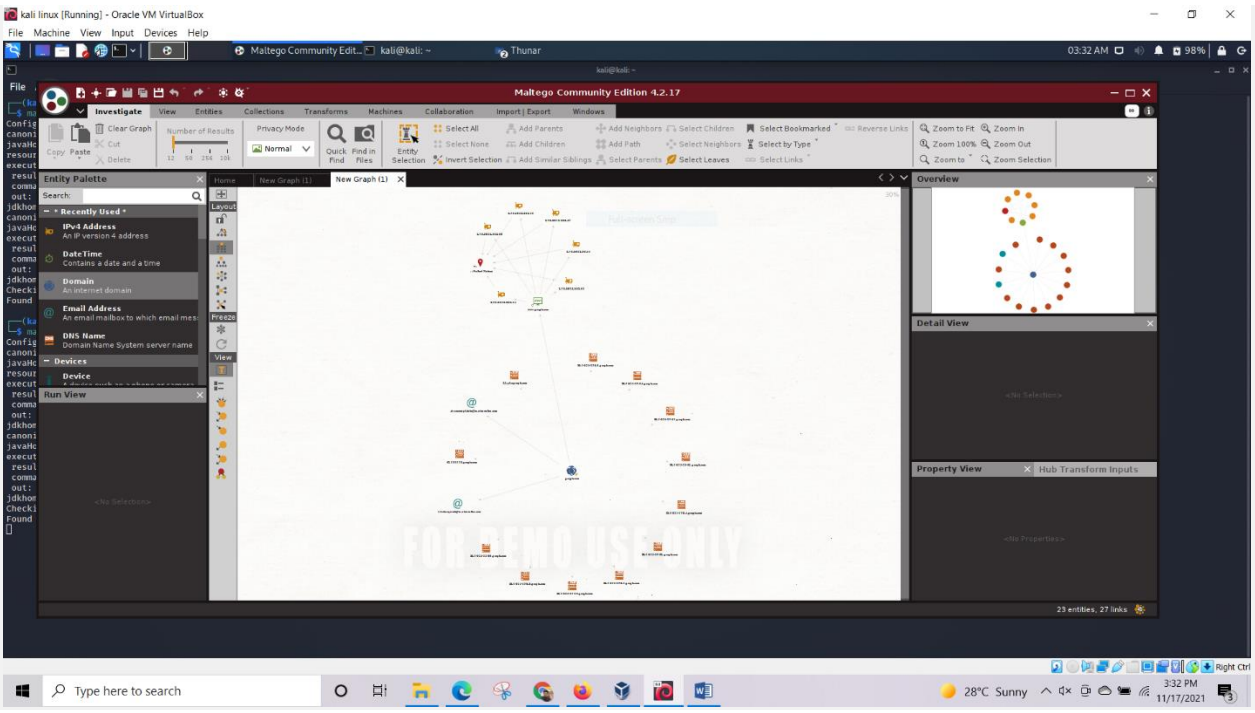

Fig 10: Domain all information

Conclusion: Maltego is a powerful tool and one of the best for information gathering. Although it's numerous features can be overwhelming at times, but once we get a grip on the tool, it will prove it's worth.