

## Maltego e como usar no Kali Linux

Já ouviu falar na expressão “data mining”? Provavelmente sim, porém, caso ainda não tenha vou resumir brevemente o que é.

“Data mining”, ou simplesmente mineração de dados, é a ação de encontrar e correlacionar fragmentos de dados ao ponto de poder relacioná-las detectando assim informações relevantes.

No campo de Análise Forense ou Pentest essas informações podem ser utilizadas para detectar rastros deixados pelo atacante ou no caso do atacante encontrar vulnerabilidades ou informações sigilosas que não deveriam estar expostas.

### O que é o Maltego?

Basicamente o Maltego é uma ferramenta totalmente interativa de código fonte aberto focado em inteligência e análise forense. Normalmente ela é muito utilizada durante investigações para buscar e relacionar informações que estão espalhadas pela internet.

O seu funcionamento é simplesmente incrível! Por ser automatizada, a ferramenta tem a habilidade de buscar fragmentos de dados e transformá-los em gráficos estruturados e de fácil entendimento.

Como comentei acima, ferramenta é de código fonte aberto, porém, possui algumas versões que são para uso comercial e são pagas. Mas não se preocupe, pois existe uma versão não comercial gratuita. Abaixo seguem as versões do Maltego:

- Maltego CE – livre, uso não comercial
- Maltego Classic – pago, uso comercial
- Maltego XL – pago, uso comercial
- Maltego One – uso comercial pago
- Maltego CaseFile – gratuito, comercial

O Maltego vem instalado por padrão no Kali Linux,

### O que é possível fazer com o Maltego?

Devido ao Maltego ter a habilidade de correlacionar informações, ele pode trazer dados objetivos sobre possíveis ameaças em uma rede corporativa.

Seja um dispositivo conectado à internet que está “vazando” configurações ou informações ou até mesmo dados sobre pessoas, e-mails e até mesmo DNS.

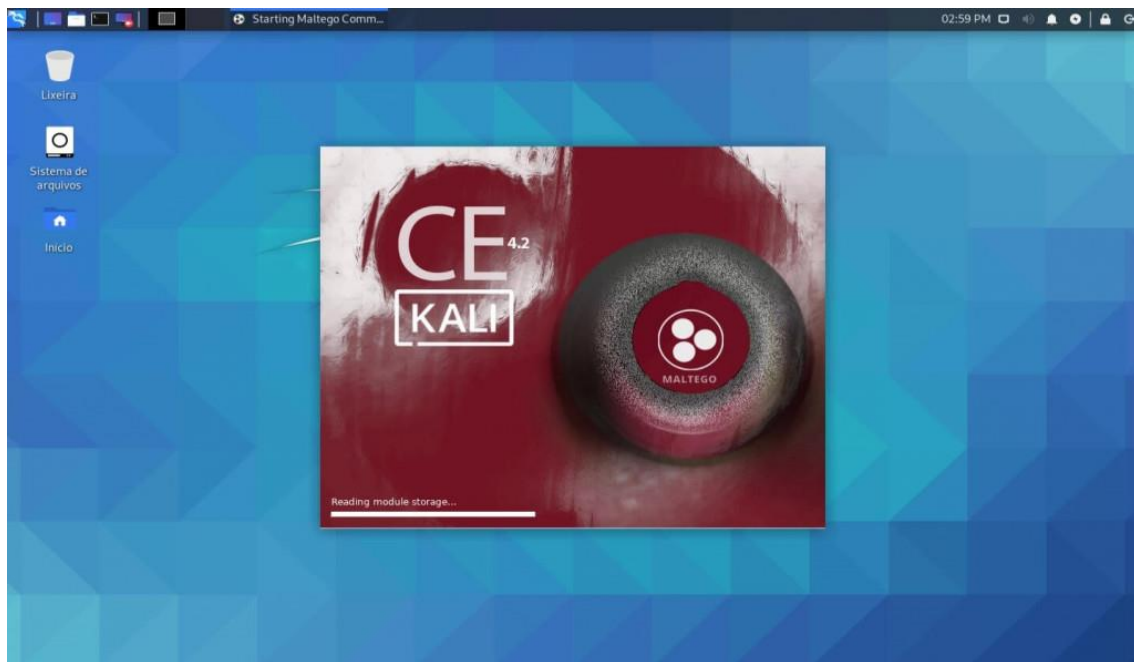
Se você busca detectar possíveis falhas em sua rede de uma forma profunda e fundamental, o Maltego é a ferramenta certa.

Através do Maltego você pode determinar as seguintes relações e conexões entre a sua rede e o mundo externo, veja abaixo algumas das funcionalidades de forma bem resumida:

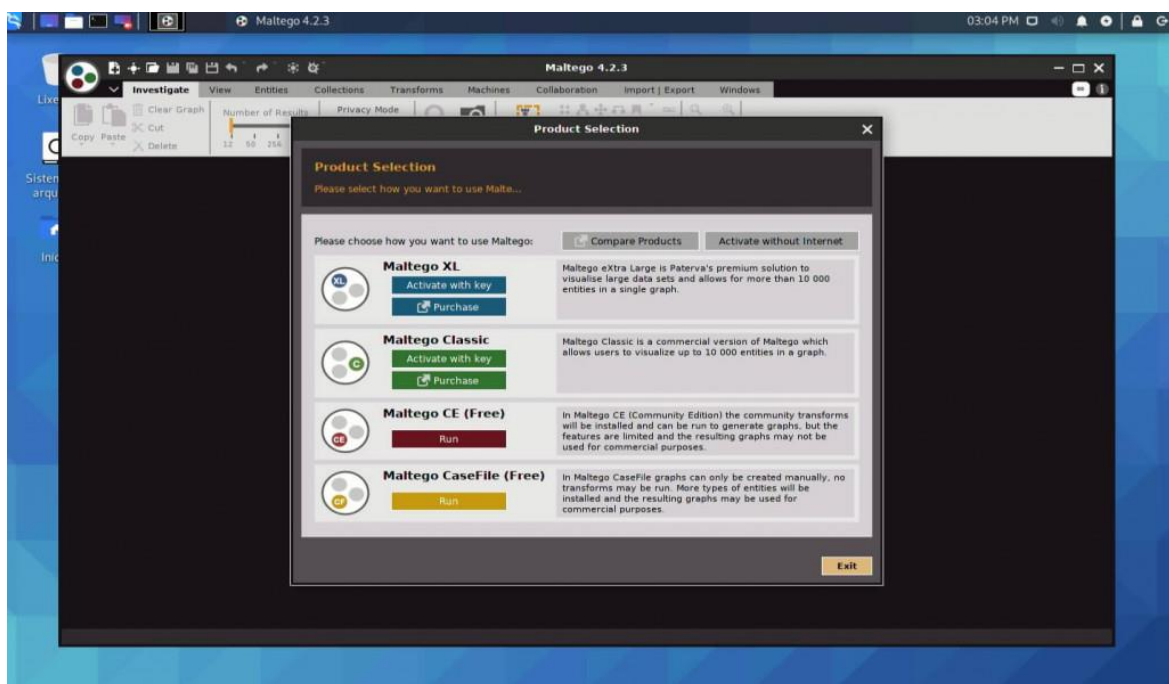
- Pessoas, grupos de pessoas, redes sociais e etc.
- Empresas, dados referentes a proprietários, organizações e muito mais.
- Sites, DNS, registradores de domínios e servidores.
- Documentos, e-mails, endereços, telefones.

Como instalar e usar o Maltego no Kali Linux

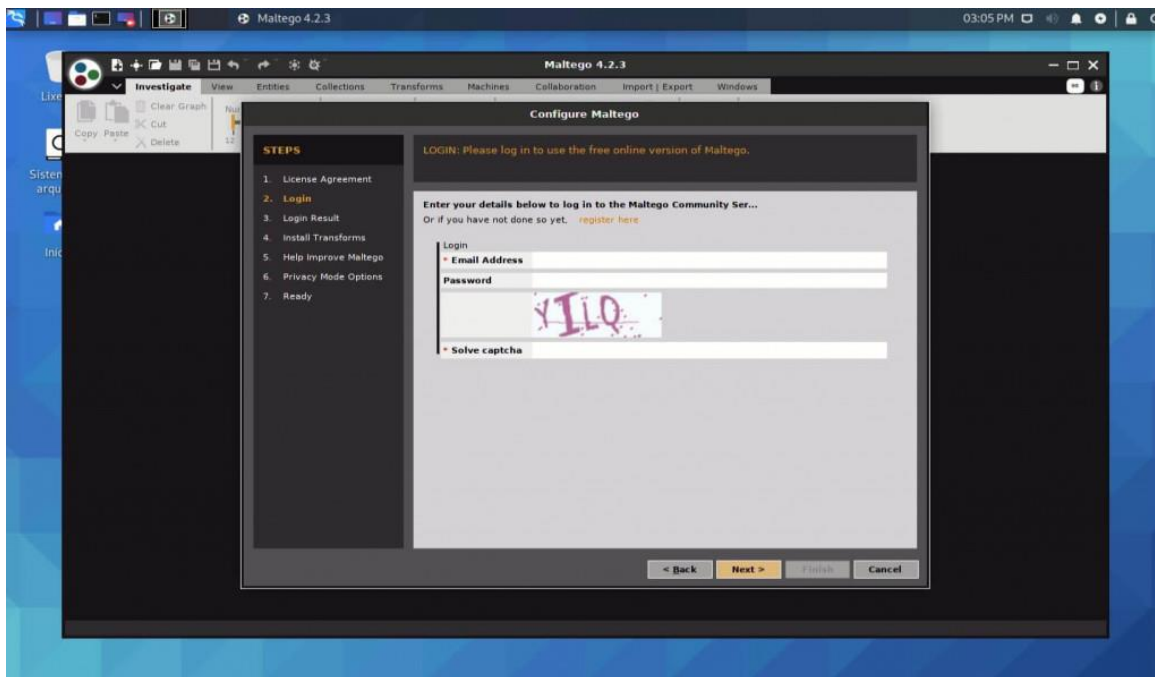
Com o seu Kali Linux devidamente instalado, basta procurar na guia de programas por “Maltego” e clicar em executar.



Uma vez que o Maltego carregar, será exibida as opções das versões disponíveis, para este tutorial utilizaremos a versão CE – Free.



Ao selecionar a versão CE (Free), você será direcionado para uma tela de login ou registro no caso de novos usuários. Sendo assim efetue o seu registro e ative a sua conta



Para o registro são exigidas apenas algumas informações, como nome, sobrenome, e-mail e uma senha.

**Register a Maltego CE Account**

Welcome to the Maltego Community Edition page, here you will be able to register an account that you can use with the latest community edition of Maltego!

FIRST NAME \*

LAST NAME \*


EMAIL \*

PASSWORD \*

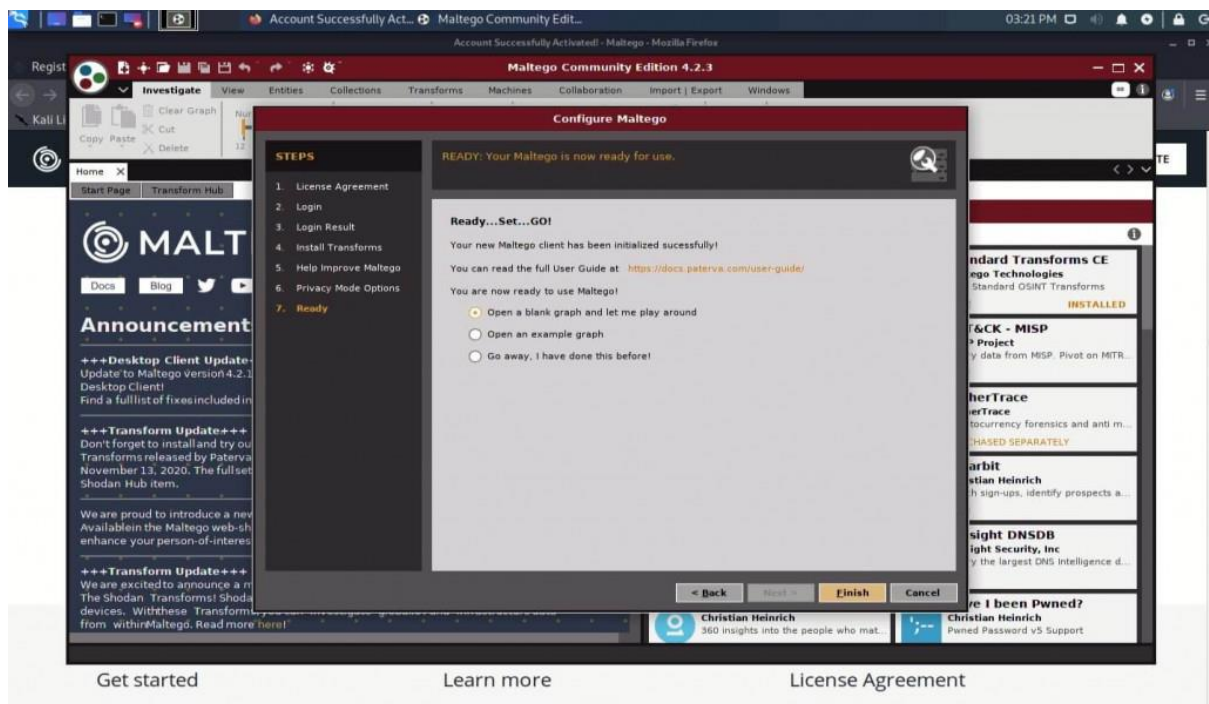
REPEAT PASSWORD \*

Already registered? Download your client [here](#) or Login directly in the client.

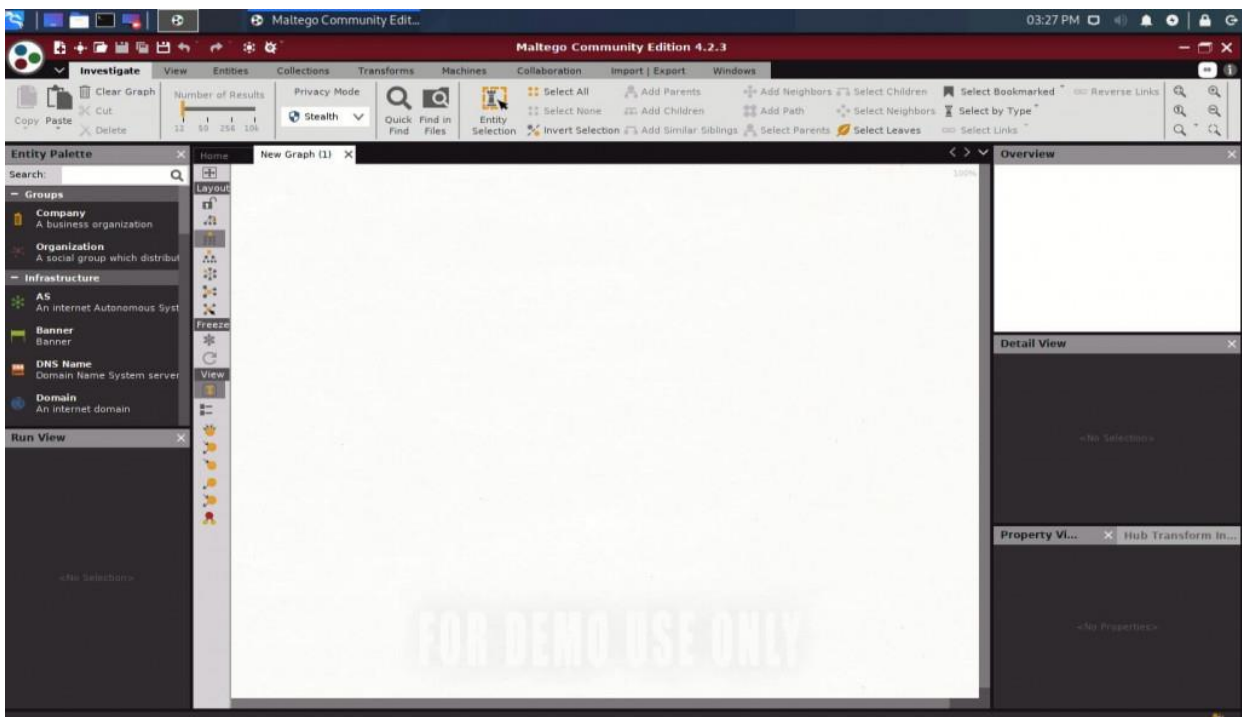
Forgot password? Reset your password [here](#).

☐ I'm not a robot 

Após registrar e confirmar o seu e-mail, basta colocar o usuário e senha cadastrados no Maltego, clicar em “Next”, “Next” novamente e “Finish”.



Uma vez que você finalizar a instalação do Maltego, uma tela em branco será exibida e estaremos prontos para começarmos a usar o Maltego no Kali Linux!



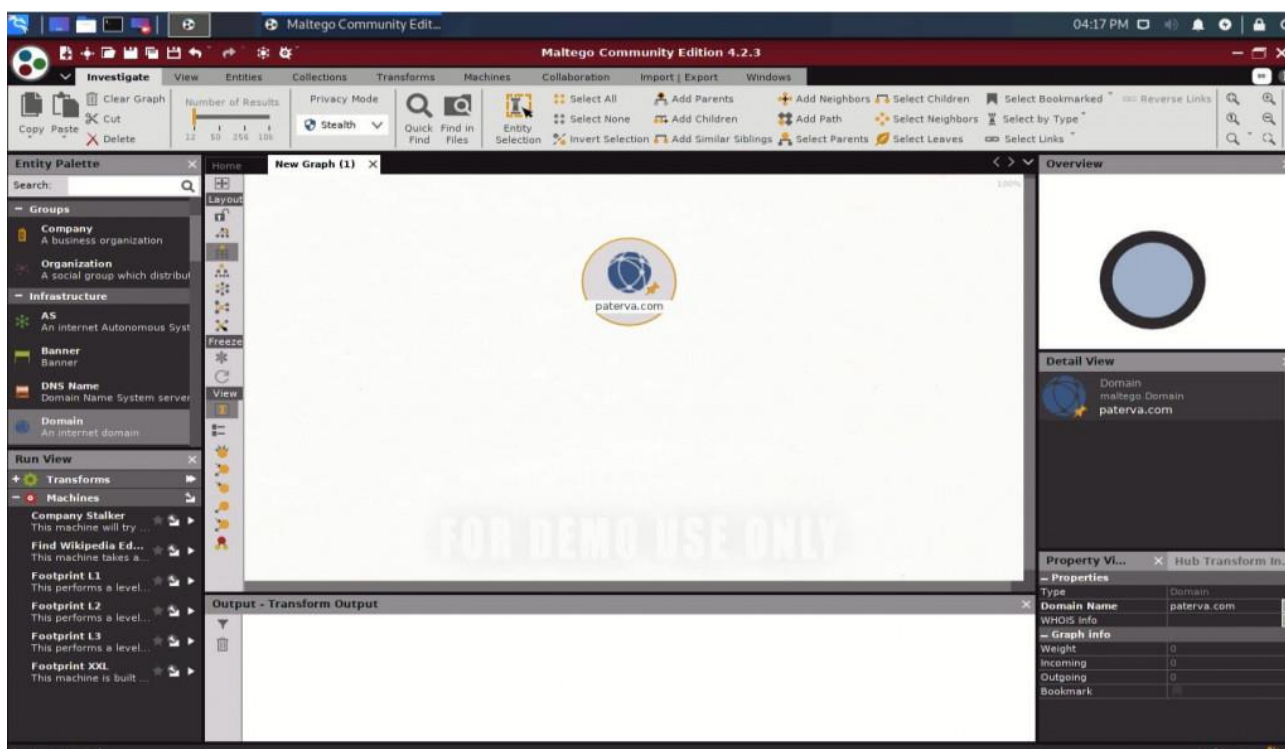
## Como levantar informações sobre um domínio usando o Maltego

Certamente o Maltego é uma ferramenta extremamente avançada com diversos recursos e seria impossível reproduzi-los todos em um único artigo.

Portanto, para este artigo irei focar no levantamento de informações referentes a um domínio, sem mais demoras vamos ver do que o Maltego é capaz!

Ao seu lado esquerdo, existem diversos ícones que na verdade são atalhos para funções extremamente poderosas, para usá-las basta clicar e arrastar para o quadro branco.

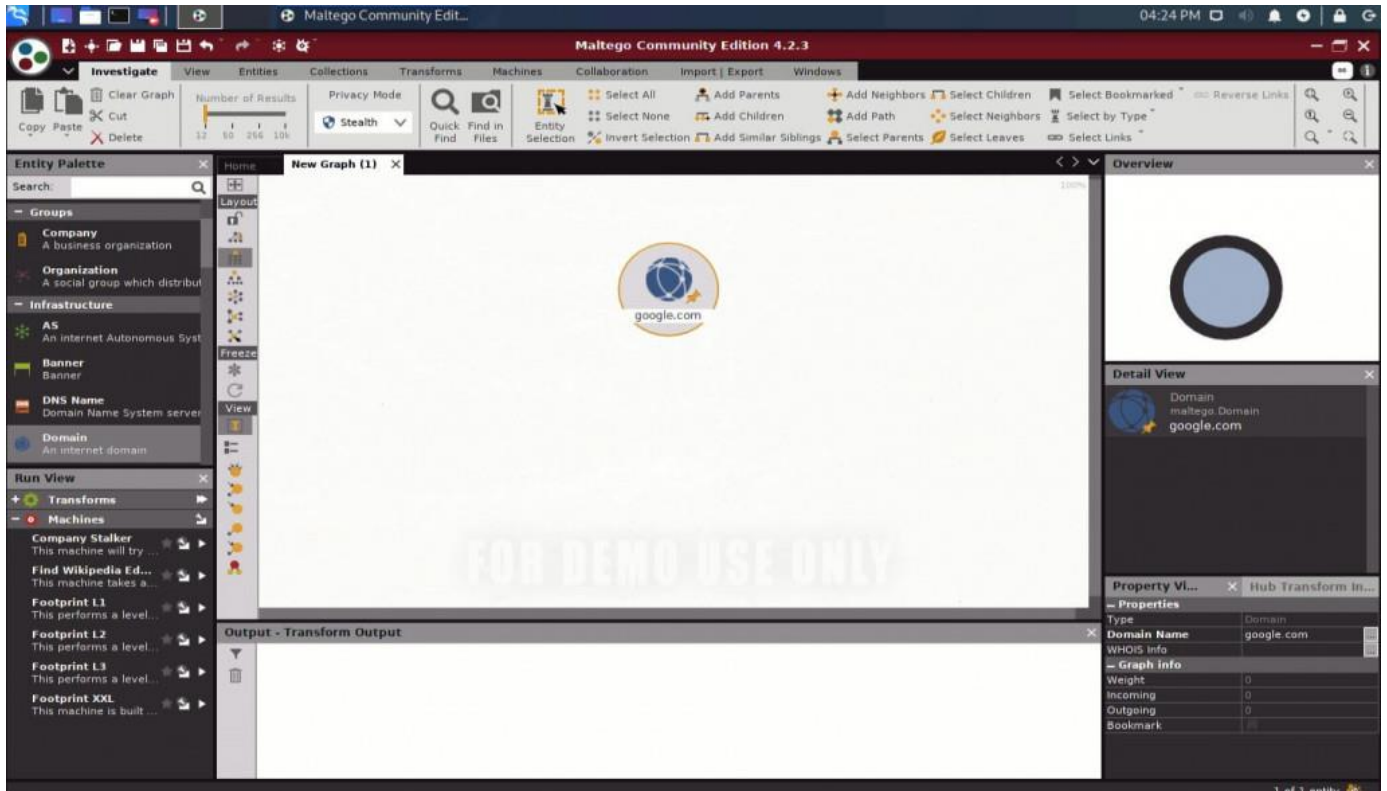
A função responsável pelo levantamento de informações sobre um domínio é a “Domain”, sendo assim clique e arraste ela para o quadro ao lado



Repare que o domínio padrão é o da paterva.com, empresa responsável pelo desenvolvimento do Maltego. Para alterar basta mudar o campo “Domain Name” ao lado esquerdo.

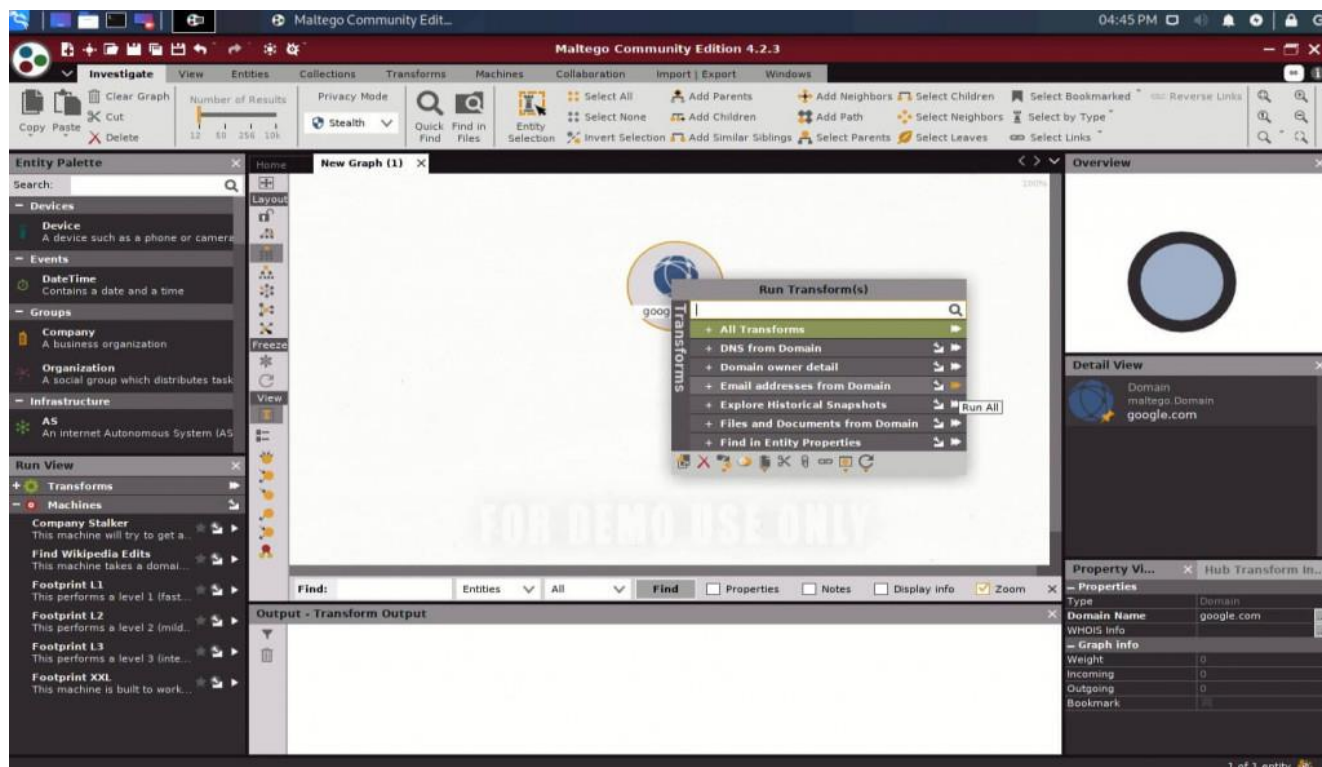
Você pode colocar o domínio que quiser, lembrando-se sempre de usar a ferramenta com responsabilidade, ok?

Apenas com o intuito de demonstração, vamos fazer uma varredura no domínio da Google.com e ver quais informações o Maltego consegue levantar.



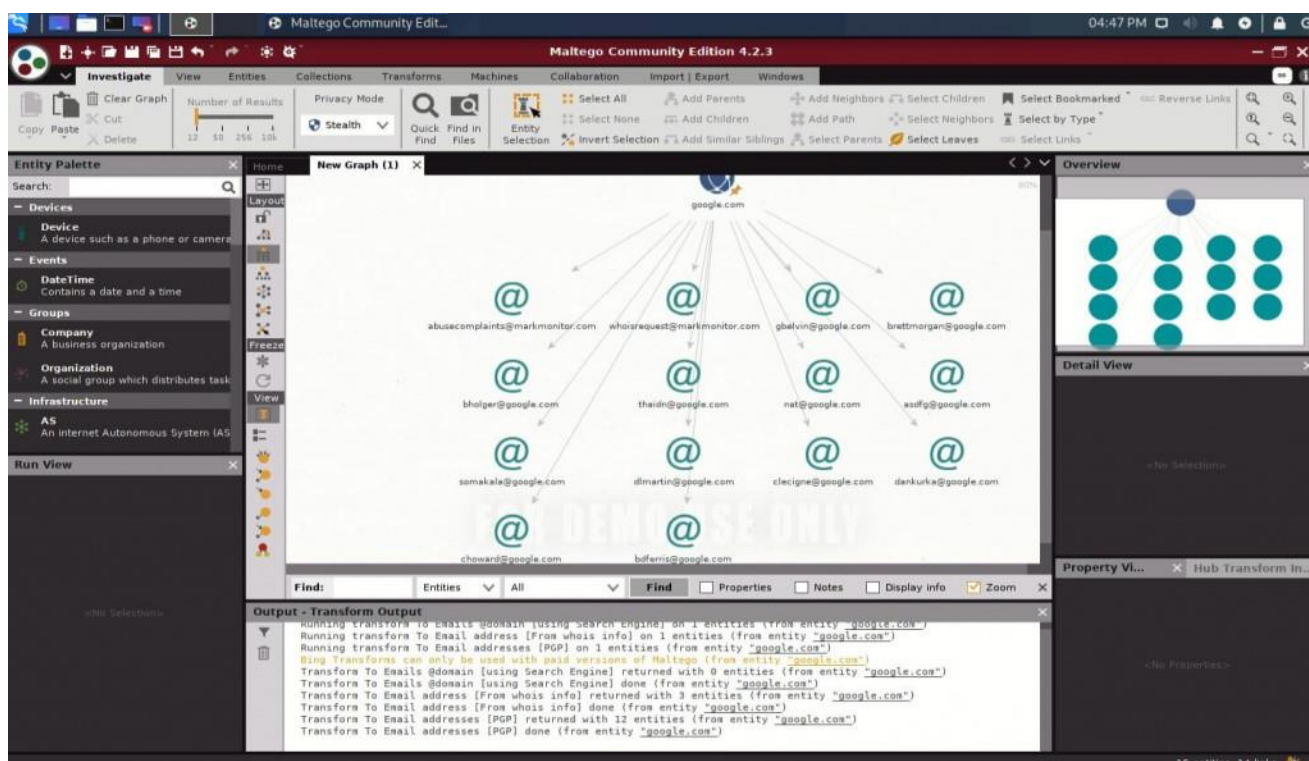
Para isso clique com o botão direito sobre a propriedade que adicionamos para termos acesso as ferramentas de mineração de dados disponíveis no Maltego.





Repare que no menu exibido teremos acesso a buscas de informações relacionadas ao DNS do domínio, proprietário, endereços de email entre outras funções. Entretanto vamos ver como a ferramenta se comporta ao realizar uma busca de emails, para isso clique na setinha “Run all” em “Email addresses from Domain”.





Como podemos observar o Maltego executa uma varredura completa, tentando levantar endereços de email vinculados ao domínio “google.com” e os exibe de forma organizada correlacionando-os com a propriedade principal adicionada.

### Maltego e as poderosas “Machines”

Dentro do Maltego existem funções chamadas de “machines” ou “máquinas” que são nada mais do que scripts poderosos pré-configurados para buscar informações e relacioná-las entre as propriedades de forma automatizada.

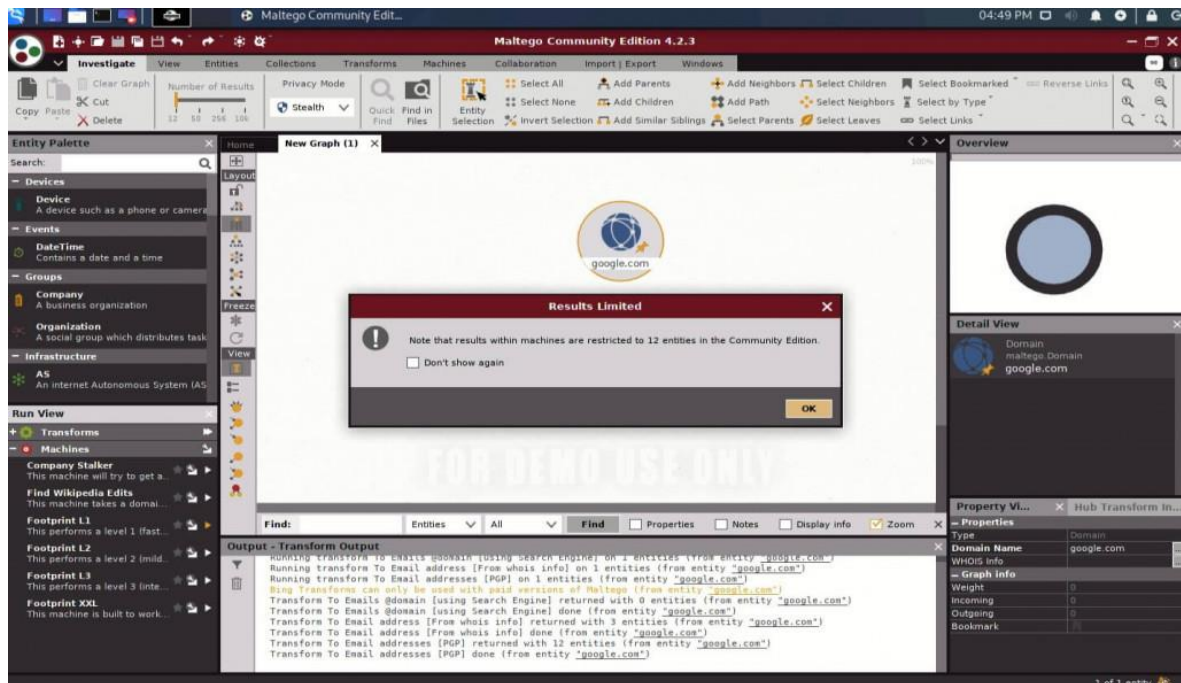
Para usá-los na versão gratuita existe uma pequena limitação de propriedades, que não será um problema para você que está iniciando o aprendizado na ferramenta.

Portanto, para usá-la, selecione a propriedade adicionada inicialmente, no caso “google.com” e ao seu lado esquerdo, repare que existe uma abada escrita “Machines”.

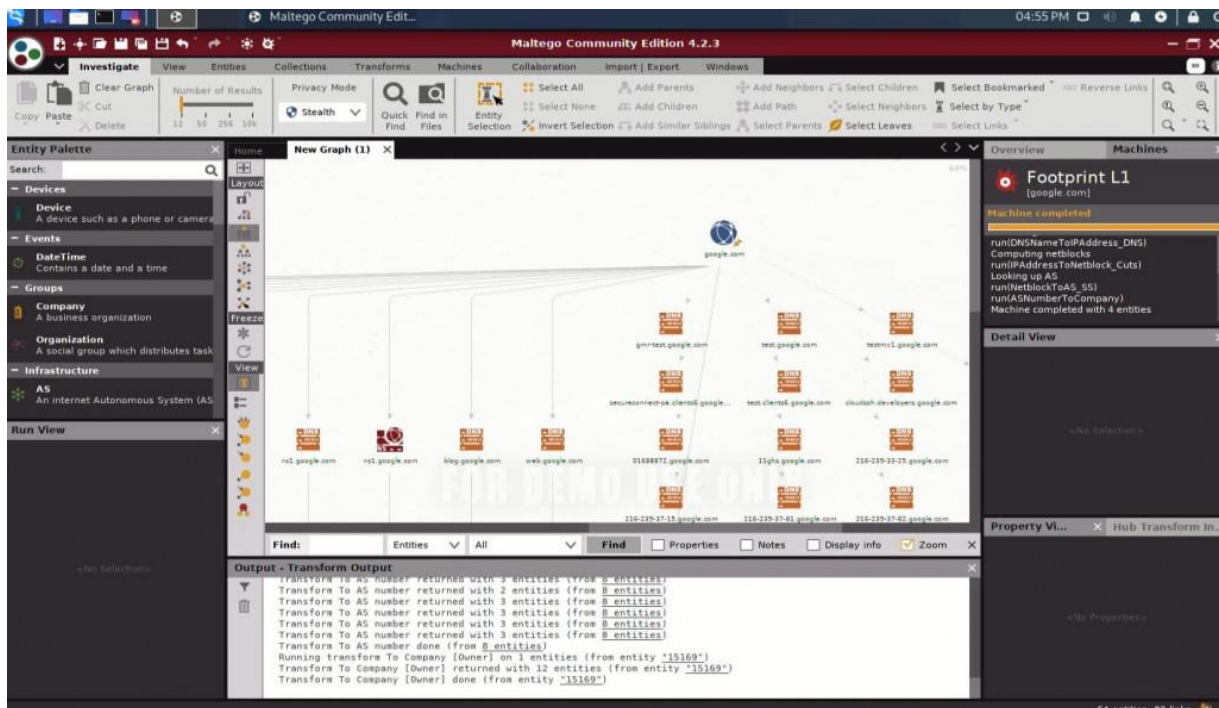
Ali são listados alguns scripts padrões do Maltego que possuem funções variadas, aconselho a ir testando cada uma para observar o poder da ferramenta.

Porém, para exemplificar, vamos utilizar a “Footprint L1” que vai realizar uma varredura, buscando relações entre servidores, números de IP’s e até mesmo localizações.

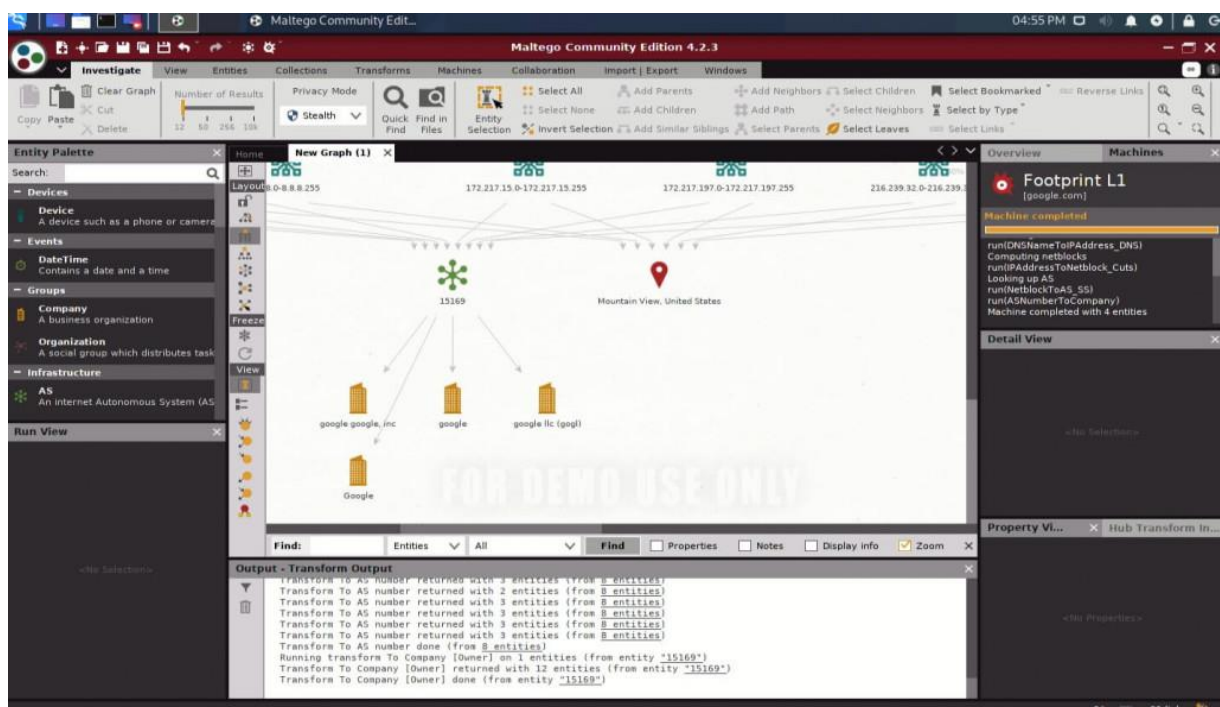
Clique na “setinha” conforme a notificação referente ao limite de entidades na versão Community (gratuita) e observe os resultados.



Uma vez que a varredura foi finalizada, será possível observar de uma forma clara e objetiva informações preciosas que interligam o domínio com uma infraestrutura, veja abaixo:

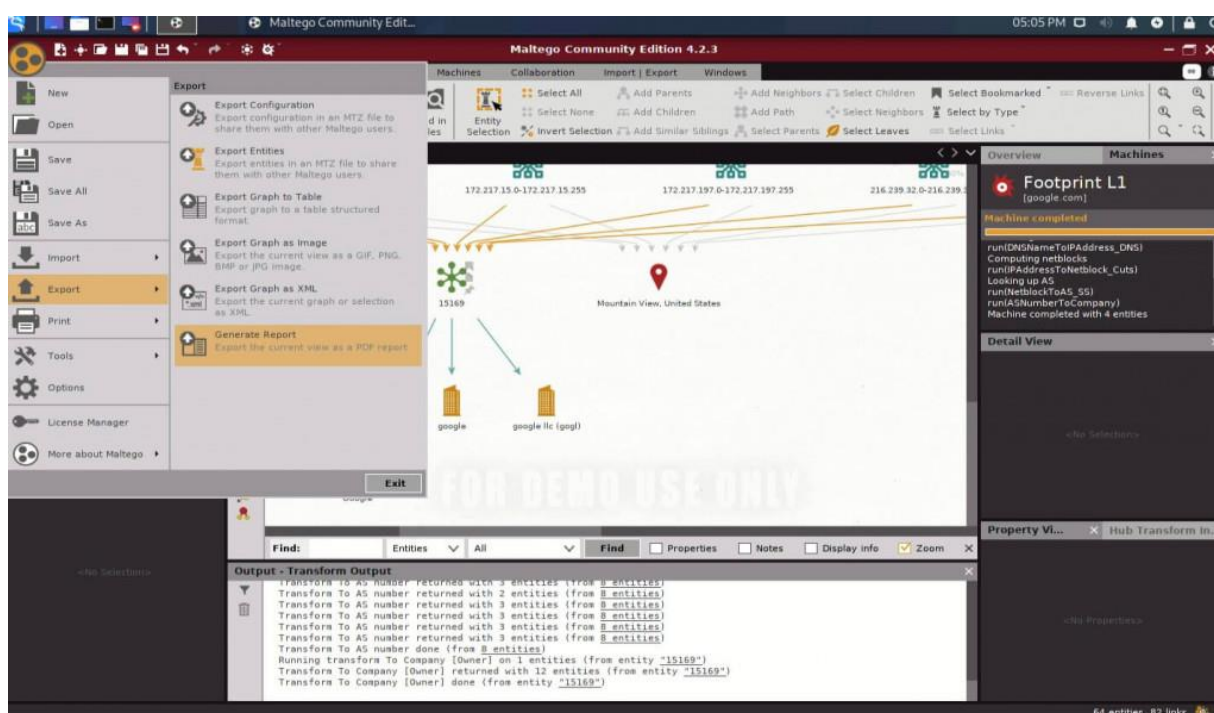


Podemos observar os registros de DNS interligados ao domínio principal “google.com” e como a infraestrutura se comunica entre si, isso tudo apenas “pressionando um botão”.



Além de localizações físicas relacionadas ao domínio pesquisado, o que sem sombra de dúvidas nos trás uma noção do poder desta ferramenta incrível.

Caso queira gerar um relatório, o Maltego permite exportar a consulta realizada para o formato de PDF, XML ou até mesmo imagem.



E como em um “passe de mágica” você tem um relatório totalmente estruturado e devidamente organizado.

**1. Top 10 Entities**

Total number of entities: 64  
Total number of links: 82

**Ranked by Incoming Links**

Rank	Type	Value	Incoming links
1	AS	15169	8
2	Location	Mountain View, United States	6
3	IPv4 Address	216.239.32.10	3
4	Website	www.google.com	2
5	Netblock	172.217.197.0-172.217.197.255	2
6	Netblock	172.217.164.0-172.217.164.255	2
7	Netblock	172.217.15.0-172.217.15.255	2
8	Netblock	172.217.8.0-172.217.8.255	2
9	IPv4 Address	172.217.164.174	1
10	IPv4 Address	172.217.197.26	1

**Ranked by Outgoing Links**

Rank	Type	Value	Outgoing links
1	Domain	google.com	37
2	AS	15169	4
3	DNS Name	smtp.google.com	3

## Conclusão final

Se você tem buscado uma ferramenta para realizar o levantamento de informações de uma forma avançada e automatizada, certamente o Maltego é a melhor opção do mercado.

Com uma interface intuitiva e recursos robustos ele se destaca por tornar uma tarefa demorada em algo extremamente rápido e eficaz.

E claro, seria impossível listar todos os recursos presentes nesta ferramenta, sendo assim aconselho ir experimentando cada uma das funcionalidades para ir conhecendo melhor o Maltego