



MALTEGO

GUSTAVO FRANCISCO MÉNDEZ DE LA CRUZ

A01332475

¿QUÉ ES?

Es una herramienta de minería de datos que procesa gráficas dirigidas para el análisis de links. Es usada principalmente en investigación, para descubrir relaciones entre las piezas de información de varias fuentes ubicadas en internet.



- Identifica:
 - DNS (Domain Name Schema)
 - Nombre del Servidor
 - Mail
 - IP Address
 - Localización Geográfica
 - Entidades
 - Números Telefónicos

CREADOR

- Fue desarrollado por Paterva, compañía fue formada por Roelof Temmingh en el 2007, y esta integrada por 7 personas más. Y Maltego fue lanzada al público en 2008.



VERSIONES

Maltego V1 - 2008

Maltego V2 -
2009

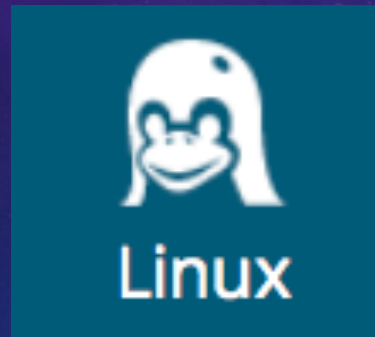
Maltego V3 -
2010

Maltego
V3.X.X -
2015

Maltego V4-
2016

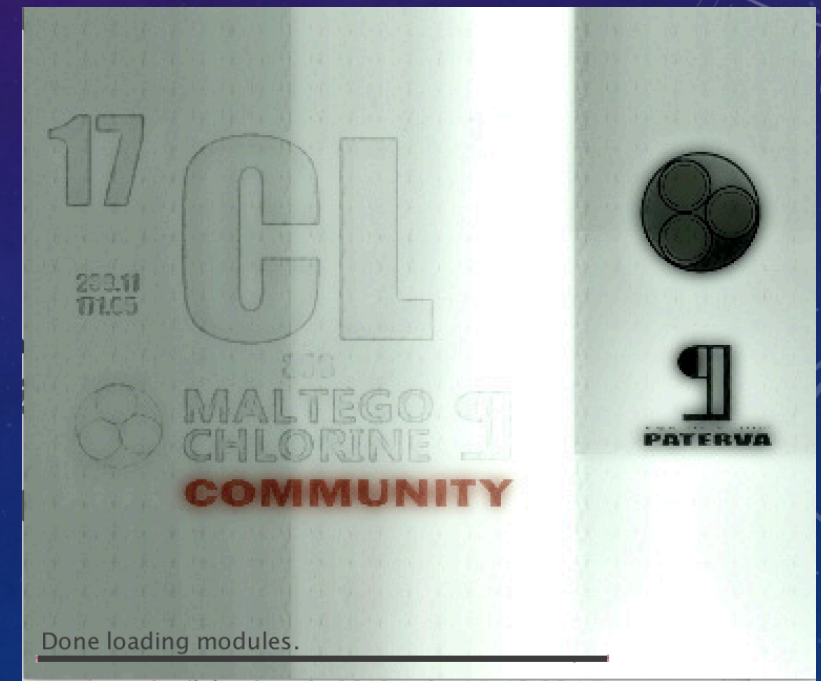
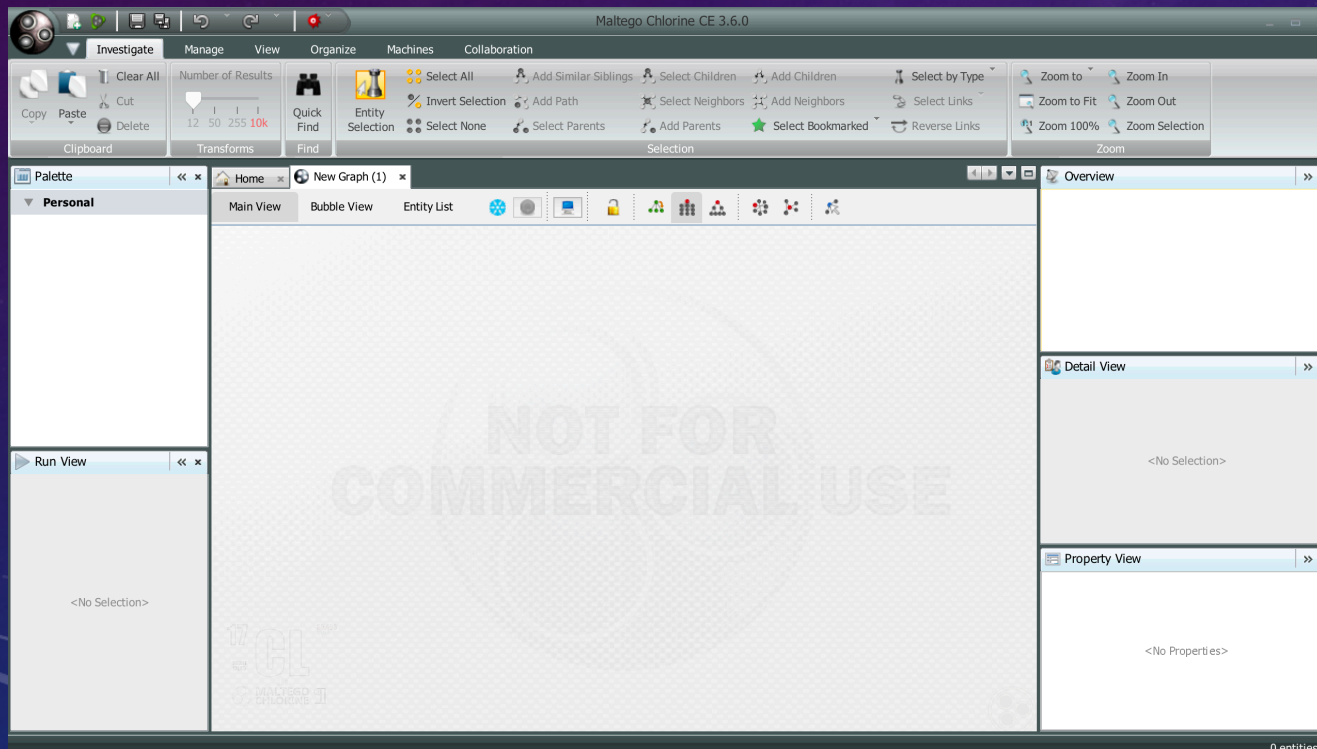
SISTEMAS OPERATIVOS

- Las 4 tipos de licencia trabajan en :



FUNCIONAMIENTO

- Funciona a través de una GUI pero se puede abrir en Linux desde la terminal



CÓDIGO



```
1 from Maltego import *
2
3 # Input - phrase entity
4 # Output - AS numbers
5 # NB: You need ISDIV defined as transform setting
6
7 def trx_EnumAS(m):
8     # construct a return vessel
9     TRX = MaltegoTransform()
10
11     #read the value, make sure its a digit
12     if (not m.Value.isdigit()):
13         # if not - complain
14         TRX.addUIMessage('Sorry but [' + m.Value + '] is not a whole number', UIM_PARTIAL)
15         return TRX.returnOutput()
16
17     #read the setting - you need ISDIV defined as transform setting in the TDS
18     isdiv = m.getTransformSetting('ISDIV')
19
20     #check if its a digit - else complain even more bitterly
21     if (not isdiv.isdigit()):
22         TRX.addUIMessage('Silly! We need a number', UIM_FATAL)
23         return TRX.returnOutput()
24
25     #here we know we're good to go.
26     #read the value of the node
27     howmany = int(m.Value);
28
29     # how many have accumulated?
30     accum=0;
31
32     for i in range(1,howmany+1):
33         if (i % int(isdiv) == 0):
34
35             # add an AS entity with the index as a value...
36             Ent = TRX.addEntity('maltego.AS', str(i))
37
38             # ... and set the weight
39             Ent.setWeight(howmany-i)
40
41             # add a property called 'div'
42             Ent.addProperty('div', 'Divisible by', 'strict', str(isdiv))
43
44             # see it's odd or even and set the link/note/bookmark properties
45             # this makes for a very ugly graph..but..ya
46             if (i%2==0):
47                 Ent.setLinkColor('0x00FF00')
48                 Ent.setNote('Even')
49                 Ent.setLinkLabel('Even link')
50                 Ent.setLinkStyle(LINK_STYLE_NORMAL)
51                 Ent.setLinkThickness(1)
52                 Ent.setBookmark(BOOKMARK_COLOR_GREEN)
53             else:
54                 Ent.setLinkColor('0xFF0000')
55                 Ent.setNote('Odd')
56                 Ent.setLinkLabel('Odd link')
57                 Ent.setLinkStyle(LINK_STYLE_DASHED)
58                 Ent.setLinkThickness(2)
59                 Ent.setBookmark(BOOKMARK_COLOR_RED)
60
61             accum=accum+1;
62             if accum>=m.Slider:
63                 break
64
65     # return the XML to the TDS server
```



WH IS



Consulting | Research | Development | Training

<http://www.blackhillsinfosec.com>

[recon-ng v4.6.3, Tim Tomes (@LaNMaSteR53)]

COMPETENCIA

LICENCIAS



Maltego XL
– 1800 USD



Maltego Classic
– 760 USD



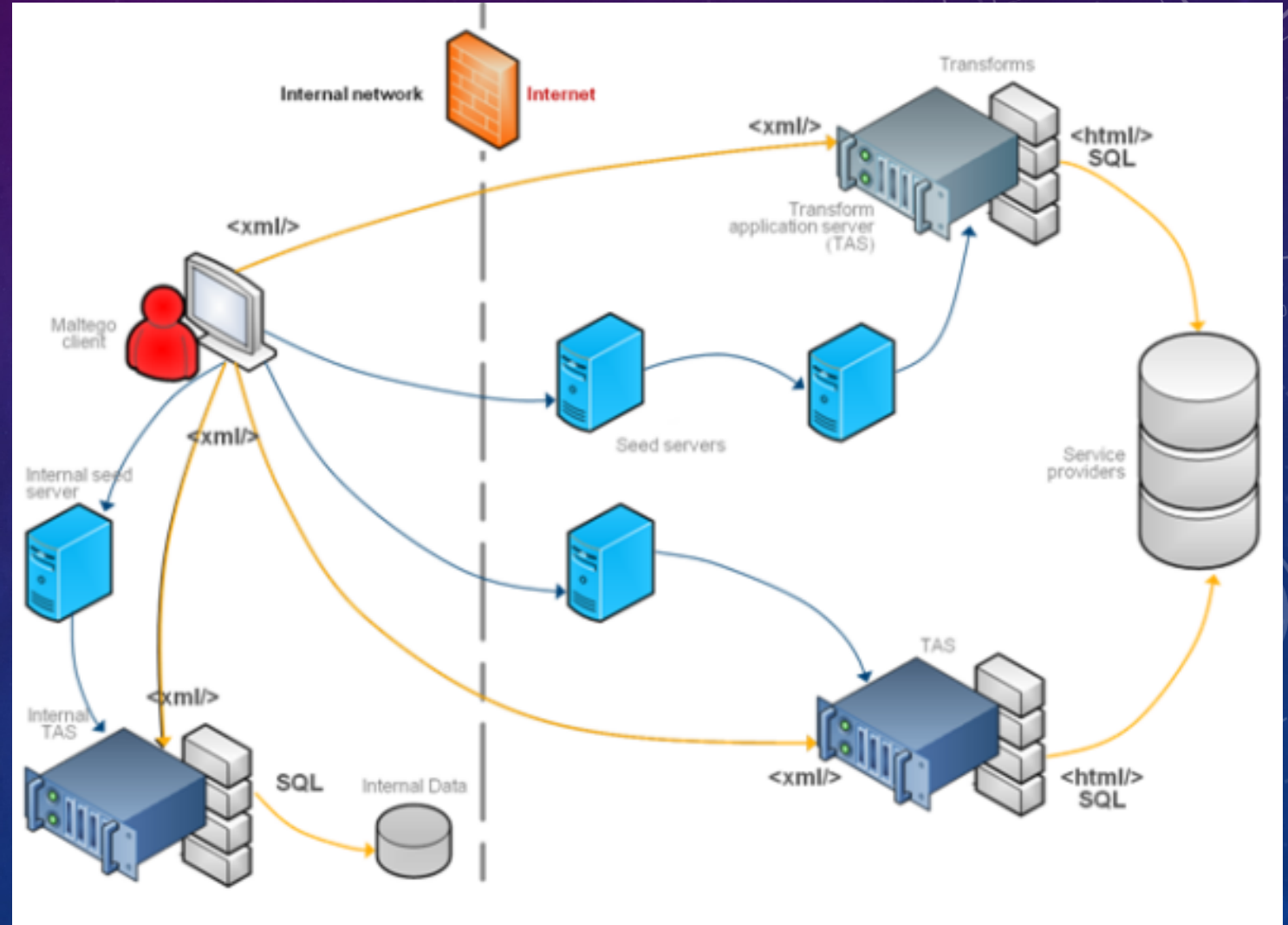
Maltego CE



Casefile

FUNCIONAMIENTO TÉCNICO

- Maltego envía la petición a los servidores semillas en formato XML a través de HTTPS
- La petición del servidor de la semilla se da a los servidores TAS que se transmiten a los proveedores de servicios
- Los resultados se envían de regreso



OTRAS TÉCNICAS

- Páginas de internet (Examina el código HTML y las cookies)
- Email (Examinar el header del email)

```
Delivered-To: [redacted]@gmail.com
Received: by 10.112.39.167 with SMTP id q7cs
Sat, 1 Jun 2013 21:24:01 -0700 (PDT)
Return-Path: <[redacted]erma@gmail.com>
Received-SPF: pass (google.com: domain of [redacted]
sender) client-ip=10.224.205.137;
Authentication-Results: mr.google.com; spf=pass (mail
10.224.205.137 as permitted sender) smtp.mail=
header.i=[redacted]erma@gmail.com
Received: from mr.google.com ([10.224.205.137])
by 10.224.205.137 with SMTP id fq9mr8578570qab.39.1
Sat, 01 Jun 2013 21:24:00 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20120113;
h=mime-version:in-reply-to:reference:
:content-type;
bh=TGEIPb4ti7gfQG+ghh7OkPjKx+Tt/iAC1
b=KguZLTlfg2+QZXzZKexlNnvRcnD/+P4+Nk5NKSptG/uHXDsiv/hGH46e2P+75MxDR8
blPK3eJ3Uf/CsaBZWDIT0XLak0AGrP3Bot92MCZFxeUUQ9uWl/xHALSnkeUIEEeKGqOC
oa9hD59D3oXI8KAC7ZmkblGzXmV4D1WfCL894RaMBOUoMzRwOWWIib95a1I38cqt1fP
ZhrWFKh5xSnZXsE73xZPEYzp7yecCeQuYHZNgs1Kxc07xQjeZuw+HWK/vR6xChDjapZ4
K5ZAfYZmkIkFX+VdLZqu7YGFzy6oHcuP16yS/C2fXHVdsuYamMT/yecvhCVo8Og7FKt6
/Kzw==
MIME-Version: 1.0
Received: by 10.224.205.137 with SMTP id fq9m
Sat, 01 Jun 2013 21:24:00 -0700 (PDT)
Received: by 10.229.230.79 with HTTP; Sat, 1
In-Reply-To: <CAQYWATT1zdDXE3o8D2rhiE4Ber2ev
References: <CAQYWATT1zdDXE3o8D2rhiE4Ber2Mv0uhro6r+7Mu7c8ubp8Eg@mail.gmail.com>
Date: Sun, 2 Jun 2013 09:53:59 +0530
Message-ID: <CAMsv0X10qEjnfW8WJdSzQhNnO=EMJcgfgX+mUfjB_tt2sy2dXA@mail.gmail.com>
Subject: ... SOLUTIONS ...
From: [redacted] Mirza <[redacted]erma@gmail.com>
To: [redacted]an@gmail.com,
[redacted]OLUTIONS <[redacted]olutions@gm
[redacted]er@yahoo.com>
```

The address from which the message was sent

Sender's IP address

Sender's mail server

Date and time received by the originator's email servers

Authentication system used by sender's mail server

Date and time of message sent

A unique number assigned by mr.google.com to identify the message

Sender's full name

DEMO

- Entidades
- Transform
- Maquinas

