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

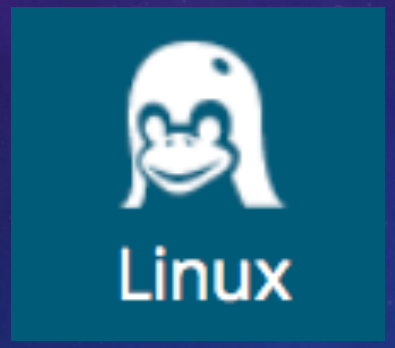
- Fue desarrollado por Paterva, compañía fue formada por Roelof Temmingh en el 2007, y esta integrada por 7 personas más. Y Maltego fue lanzada al público en 2008.

VERSIONES


Maltego V1 - 2008
Maltego V2 - 2009
Maltego V3 - 2010
Maltego V3.X.X - 2015
Maltego V4- 2016

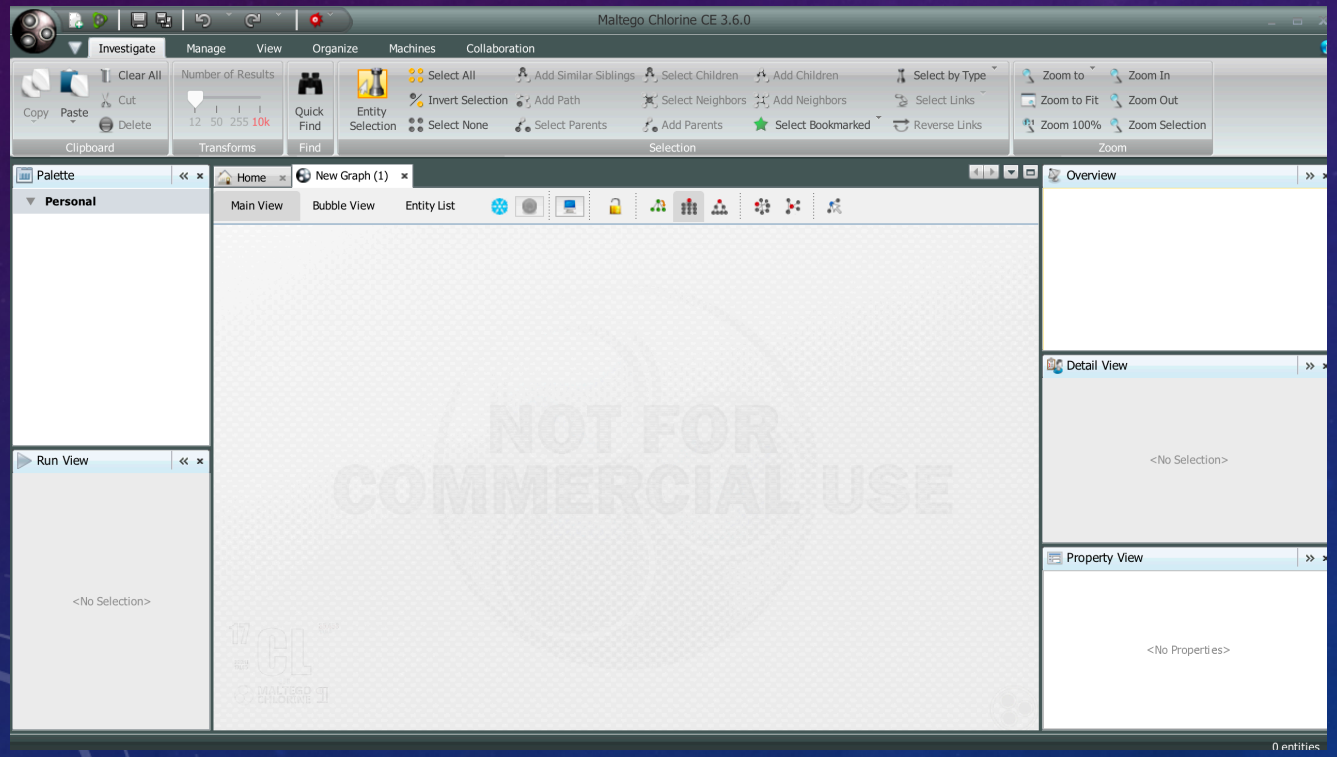
SISTEMAS OPERATIVOS

- Las 4 tipos de licencia trabajan en :



FUNCIONAMIENTO

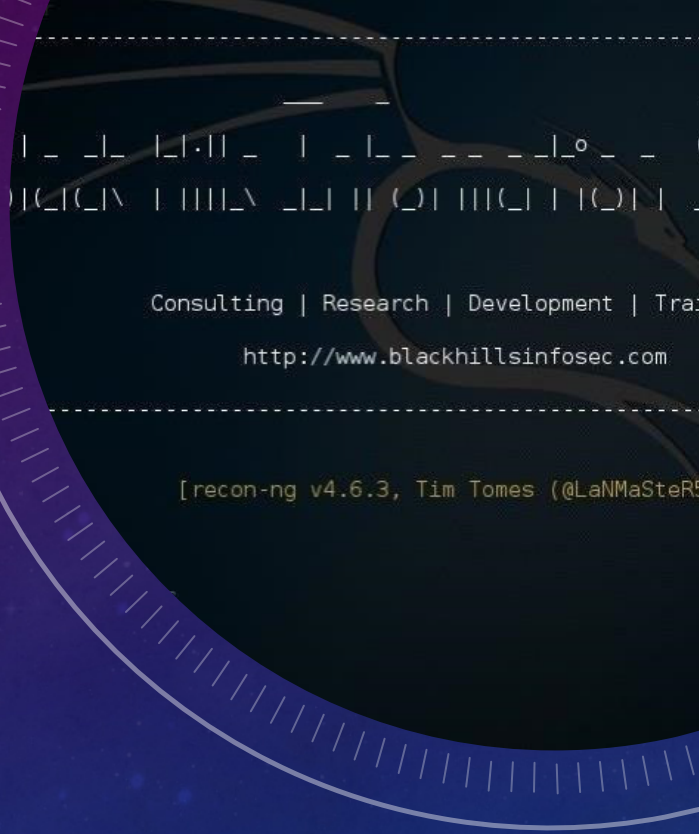
- Funciona a través de una GUI pero se puede abrir en Linux desde la terminal



CÓDIGO

```python
from Maltego import *

# Input -  phrase entity
# Output - AS numbers
# NB: You need ISDIV defined as transform setting

def trx_EnumAS(m):
    # construct a return vessel
    TRX = MaltegoTransform()

    #read the value, make sure its a digit
    if (not m.Value.isdigit()):
        # if not - complain
        TRX.addUIMessage('Sorry but ['+m.Value+'] is not a whole number',UIM_PARTIAL)
        return TRX.returnOutput()

    #read the setting - you need ISDIV defined as transform setting in the TDS
    isdiv = m.getTransformSetting('ISDIV')

    #check if its a digit - else complain even more bitterly
    if (not isdiv.isdigit()):
        TRX.addUIMessage('Silly! We need a number',UIM_FATAL)
        return TRX.returnOutput()

    #here we know we're good to go.
    #read the value of the node
    howmany = int(m.Value);

    # how many have accumulated?
    accum=0;

    for i in range(1,howmany+1):
        if (i % int(isdiv) == 0):

            # add an AS entity with the index as a value...
            Ent = TRX.addEntity('maltego.AS', str(i))

            # ... and set the weight
            Ent.setWeight(howmany-i)

            # add a property called 'div'
            Ent.addProperty('div','Divisible by','strict',str(isdiv))

            # see it's odd or even and set the link/note/bookmark properties
            # this makes for a very ugly graph..but..ya
            if (i%2==0):
                Ent.setLinkColor('0x00FF00')
                Ent.setNote('Even')
                Ent.setLinkLabel('Even link')
                Ent.setLinkStyle(LINK_STYLE_NORMAL)
                Ent.setLinkThickness(1)
                Ent.setBookmark(BOOKMARK_COLOR_GREEN)
            else:
                Ent.setLinkColor('0xFF0000')
                Ent.setNote('Odd')
                Ent.setLinkLabel('Odd link')
                Ent.setLinkStyle(LINK_STYLE_DASHED)
                Ent.setLinkThickness(2)
                Ent.setBookmark(BOOKMARK_COLOR_RED)

            accum=accum+1;
            if accum>=m.Slider:
                break

    # return the XML to the TDS server
```

WHOIS



COMPETENCIA

LICENCIAS

Maltego XL
– 1800 USD

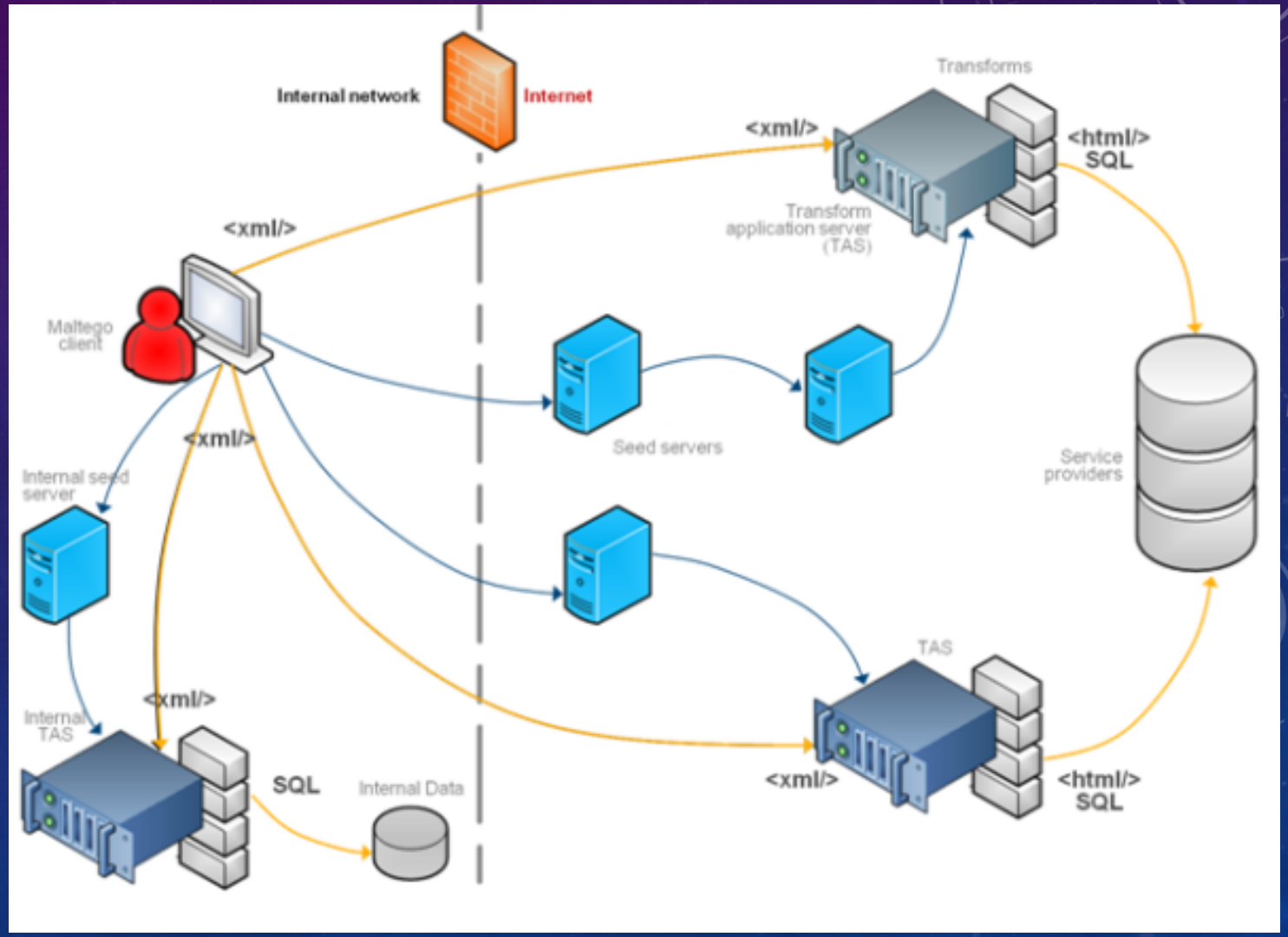
Maltego Classic
– 760 USD

Maltego CE

Casefile

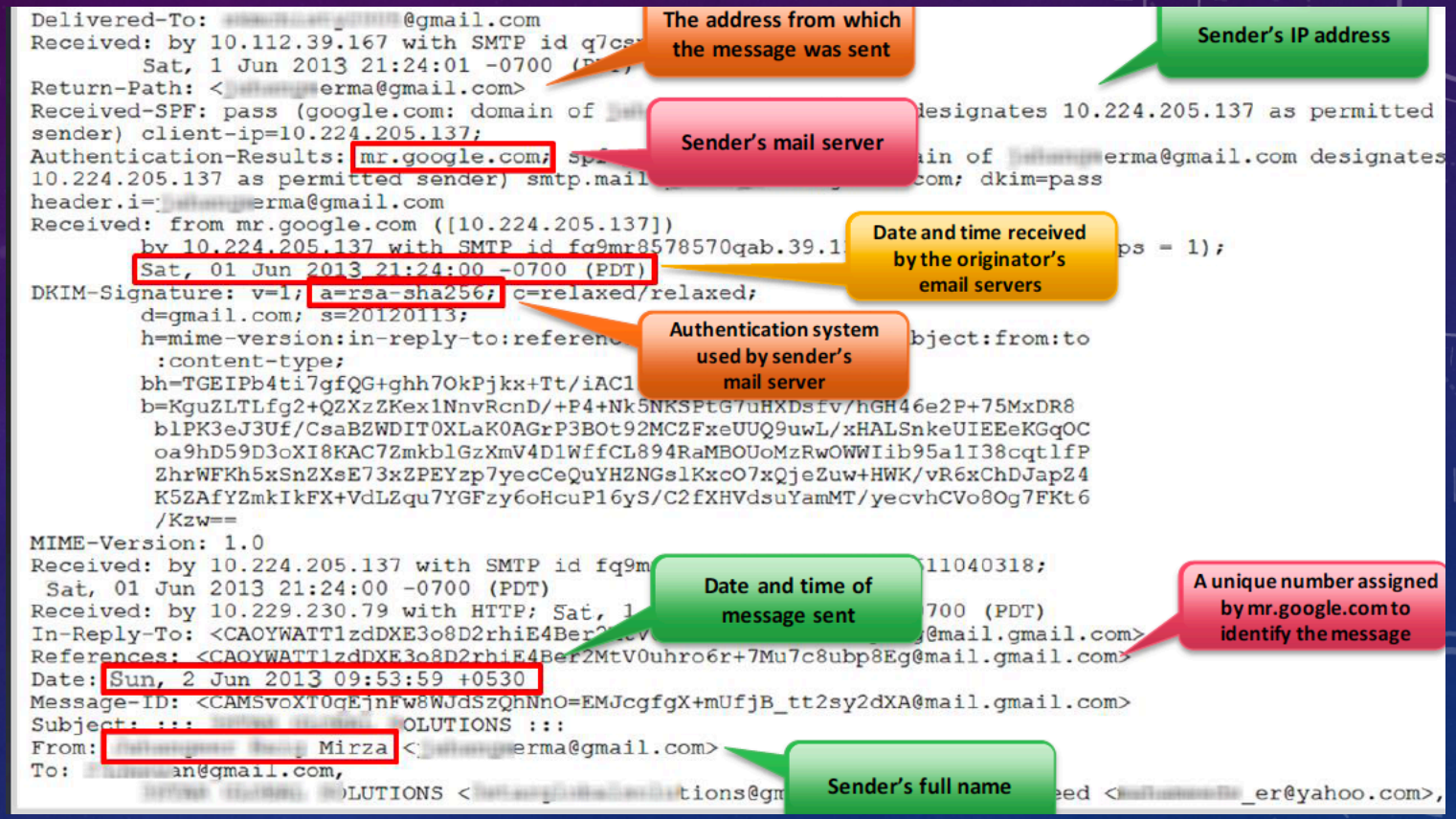
FUNCIONAMIENTO TÉCNICO

- 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)



DEMO

- Entidades
- Transform
- Maquinas