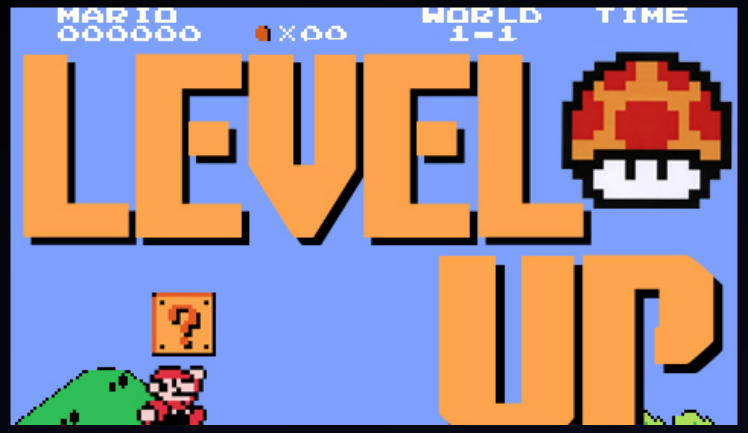


WITH MALTEGO

4TH OCTOBER 2017, EUCOM (TLP: WHITE)

TOM LANCASTER

@TLANSEC

paloalto NETWORKS®

WHY GIVE A TALK ABOUT MALTEGO?

- I do not work for Paterva.
- I use this tool a lot.
- I think people could be using it better, or give up too easily.

CONTENTS

- WHAT?
- WHY?
- Our Setup
- Writing your own transforms
- Post Processing graph data
- Tips for using Maltego

WHAT?

MALTEGO OVERVIEW

- Application; $$ for licenses;
- Visualisation tool with automation;
- Highly customisable;

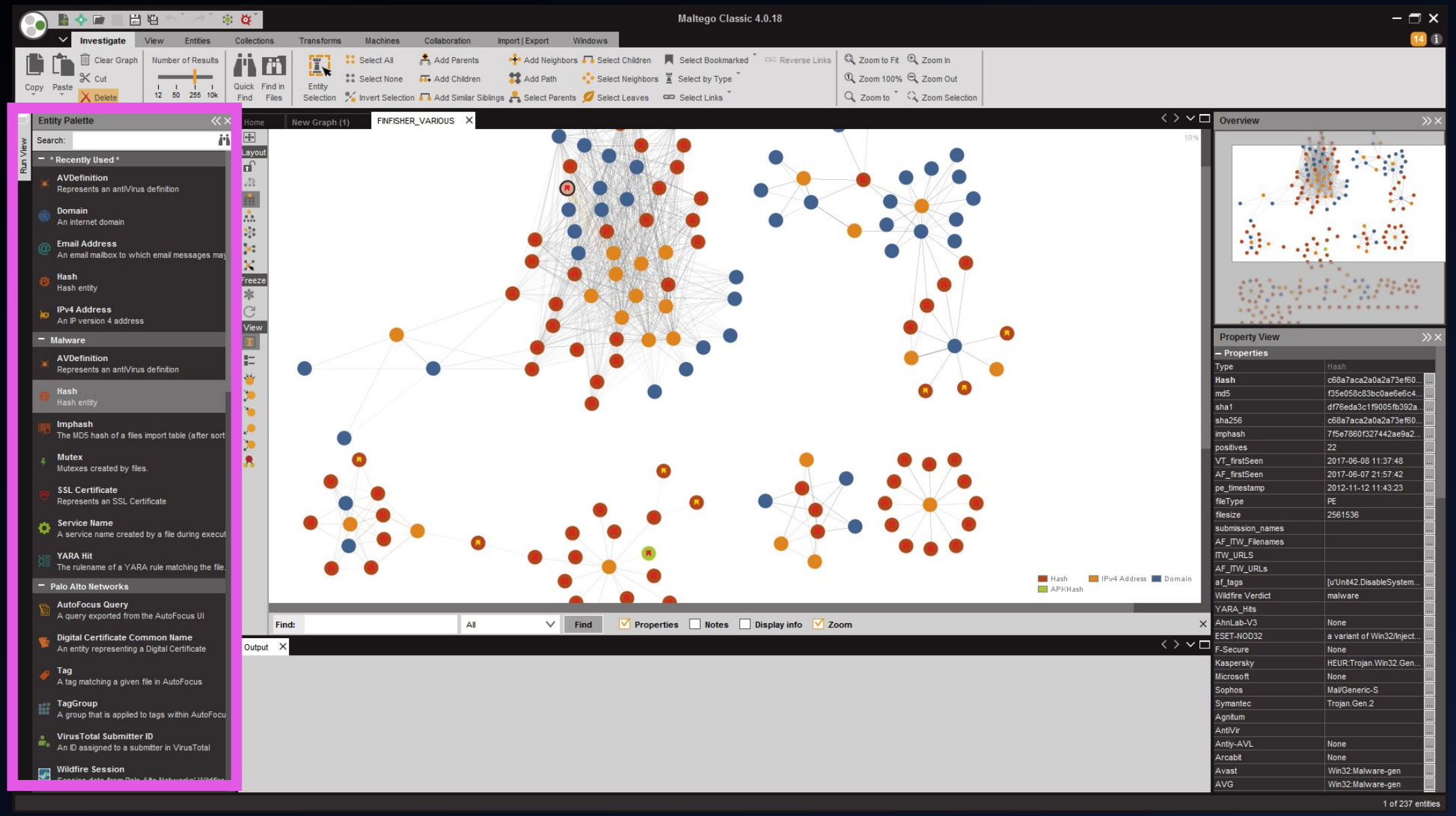
KEY CONCEPTS - ENTITIES

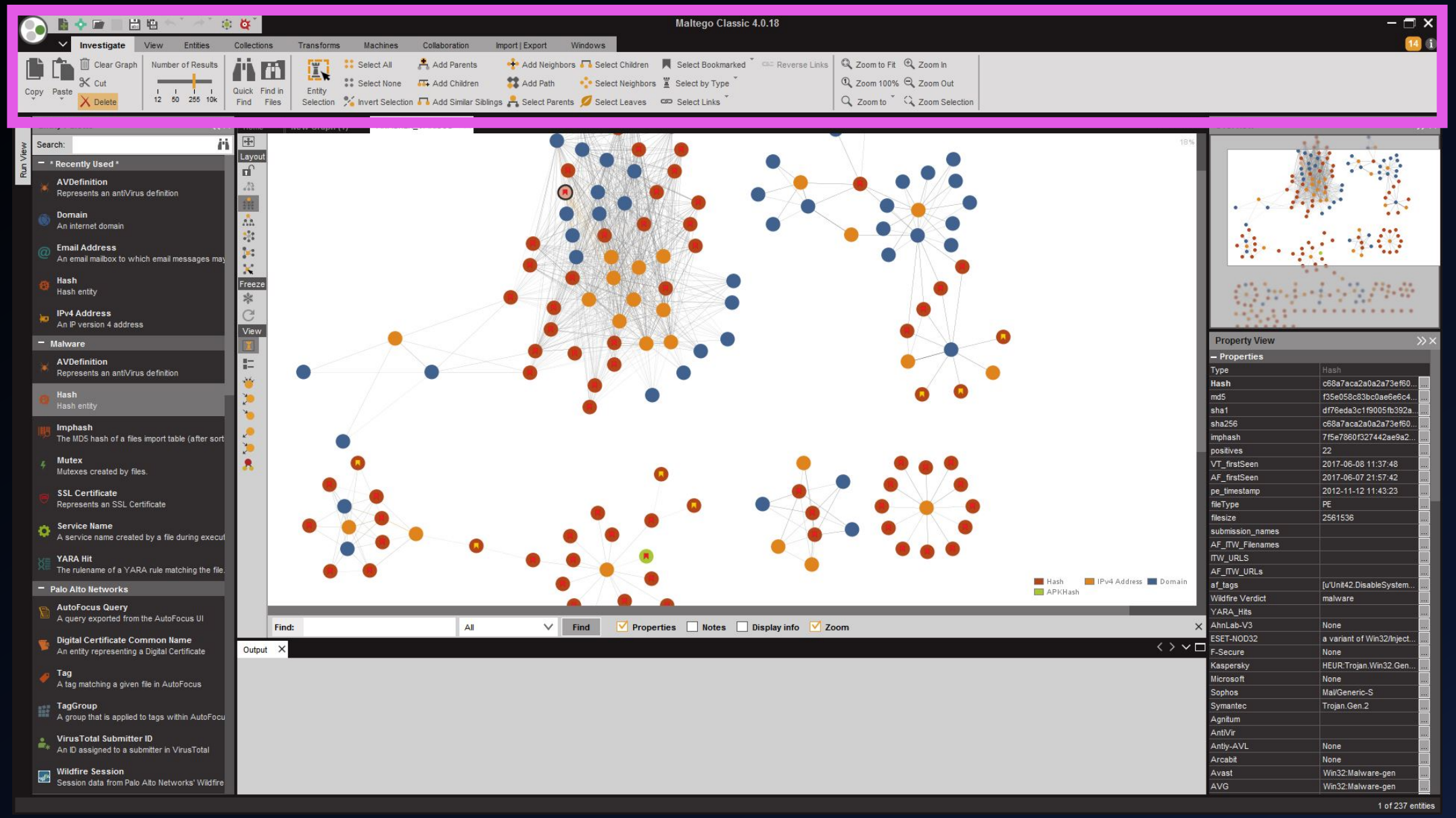
- Can be anything you want.
- Value, Icon, properties.
- Make your own!

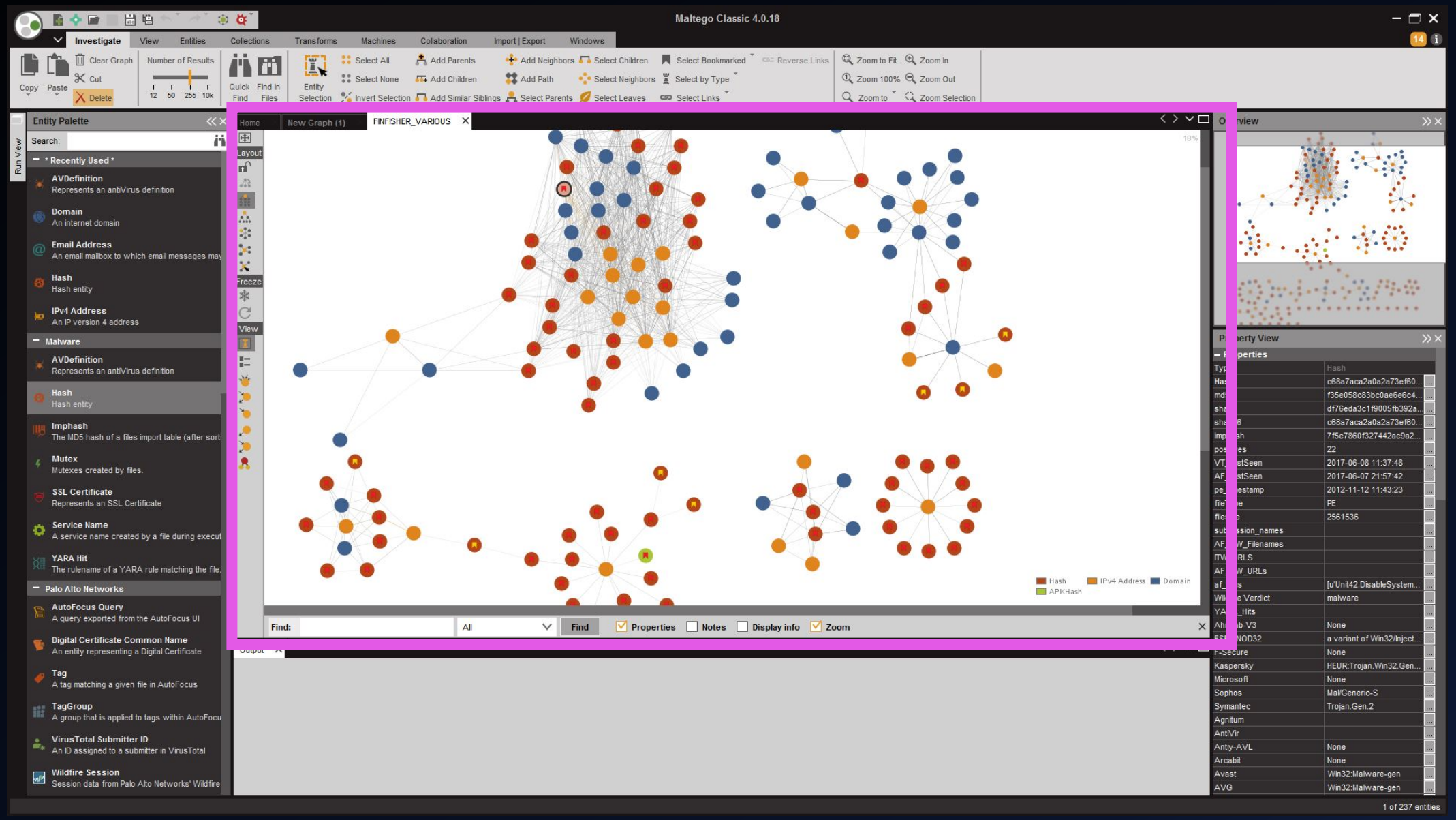
– Properties	
Type	Hash
Hash	33c187cfd9e3b68c3089...
md5	96b47c5af8652ac99150...
sha1	6524f8a29c7fd0190f53d...
sha256	33c187cfd9e3b68c3089...
imphash	None
positives	15
VT_firstSeen	2017-08-24 08:50:55
AF_firstSeen	2017-08-24 02:06:48
pe_timestamp	2017-08-16 12:04:33
fileType	PE
filesize	227328
submission_names	PolicyConverter.exe,Cry...

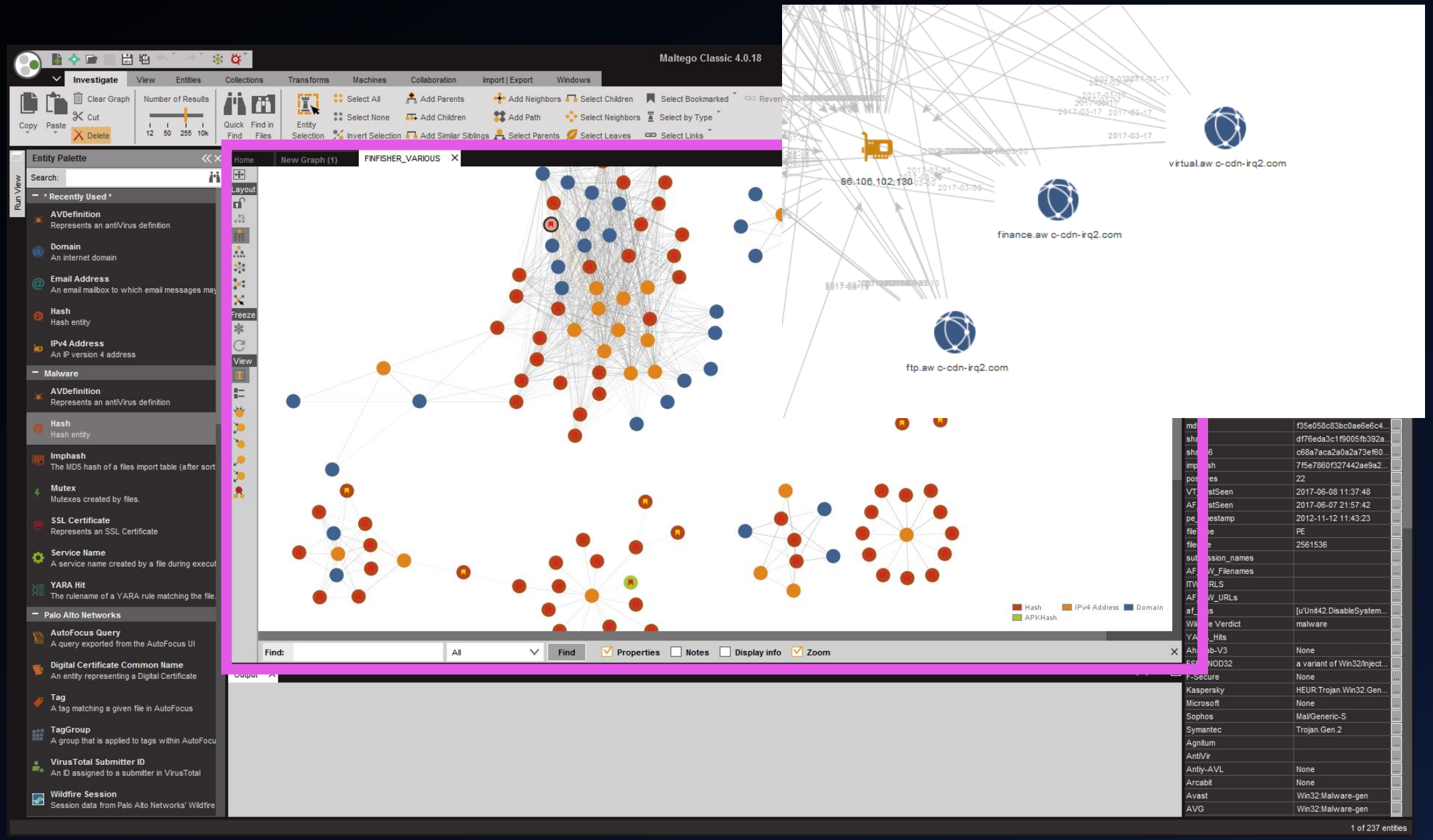
KEY CONCEPTS - TRANSFORMS

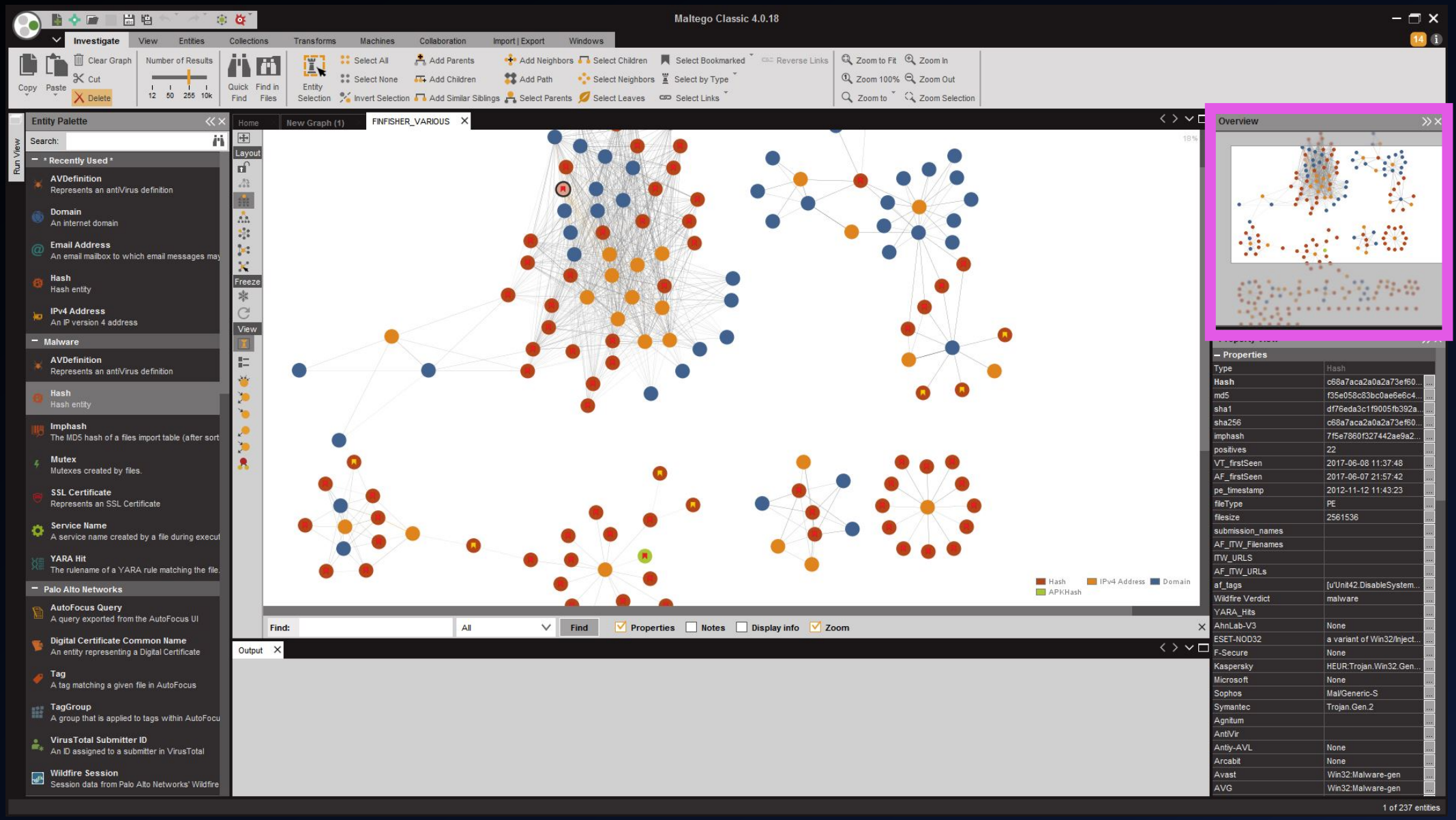
- Run some code, using an entity as an input.
- Return data to graph based on results.
- Code can run locally or remotely.

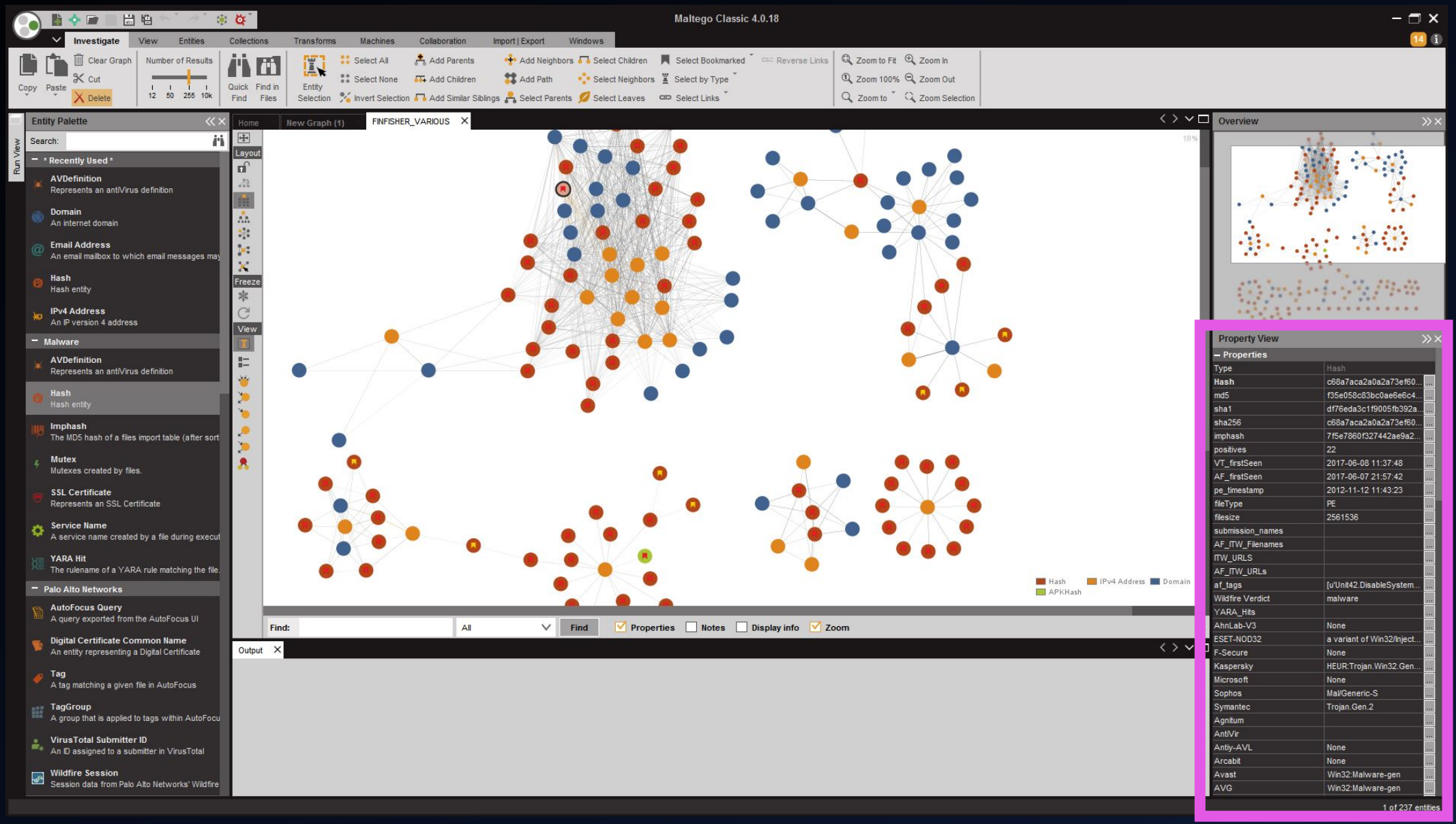

Maltego Classic 4.0.18
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
Search:
* Recently Used *
AVDefinition
Represents an antiVirus definition
Domain
An internet domain
Email Address
Hash
Hash entity
IPv4 Address
An IP version 4 address
Malware
Imphash
Mutex
Mutexes created by files.
SSL Certificate
Represents an SSL Certificate
Service Name
YARA Hit
Palo Alto Networks
AutoFocus Query
Digital Certificate Common Name
An entity representing a Digital Certificate
Tag
A tag matching a given file in AutoFocus
TagGroup
VirusTotal Submitter ID
An ID assigned to a submitter in VirusTotal
Wildfire Session
Home
New Graph (1)
FINFISHER_VARIOUS
Overview
Property View
Properties
Type
Hash
md5
sha1
sha256
imphash
positives
VT_firstSeen
AF_firstSeen
pe_timestamp
fileType
filesize
submission_names
AF_ITW_Filenames
ITW_URLS
AF_ITW_URLs
af_tags
Wildfire Verdict
YARA_Hits
AhnLab-V3
ESET-NOD32
F-Secure
Kaspersky
Microsoft
Sophos
Symantec
Agnitum
AntiVir
Antiy-AVL
Arcabit
Avast
AVG
Find:
Properties
Notes
Display info
Zoom
Output
1 of 237 entities


Maltego Classic 4.0.18
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Search:
* Recently Used *
AVDefinition
Represents an antiVirus definition
Domain
An internet domain
Email Address
Hash
Hash entity
IPv4 Address
An IP version 4 address
Malware
Imphash
Mutex
Mutexes created by files.
SSL Certificate
Represents an SSL Certificate
Service Name
YARA Hit
Palo Alto Networks
AutoFocus Query
A query exported from the AutoFocus UI
Digital Certificate Common Name
An entity representing a Digital Certificate
Tag
A tag matching a given file in AutoFocus
TagGroup
VirusTotal Submitter ID
An ID assigned to a submitter in VirusTotal
Wildfire Session
Session data from Palo Alto Networks' Wildfire
Property View
Properties
Type
Hash
md5
sha1
sha256
imphash
positives
VT_firstSeen
AF_firstSeen
pe_timestamp
fileType
filesize
submission_names
AF_ITW_Filenames
ITW_URLS
AF_ITW_URLs
af_tags
Wildfire Verdict
malware
YARA_Hits
AhnLab-V3
None
ESET-NOD32
F-Secure
Kaspersky
Microsoft
Sophos
Mal/Generic-S
Symantec
Trojan.Gen.2
Agnitum
AntiVir
Antiy-AVL
Arcabit
Avast
Win32:Malware-gen
AVG
Find:
Properties
Notes
Display info
Zoom
Output
1 of 237 entities


Maltego Classic 4.0.18
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
Search:
* Recently Used *
AVDefinition
Represents an antiVirus definition
Domain
An internet domain
Email Address
Hash
Hash entity
IPv4 Address
An IP version 4 address
Malware
Imphash
Mutex
Mutexes created by files.
SSL Certificate
Represents an SSL Certificate
Service Name
YARA Hit
Palo Alto Networks
AutoFocus Query
Digital Certificate Common Name
Tag
TagGroup
VirusTotal Submitter ID
Wildfire Session
Home
New Graph (1)
FINFISHER_VARIOUS
Hash
IPv4 Address
Domain
APKHash
Find:
All
Find
Properties
Notes
Display info
Zoom
Property View
Hash
Kaspersky
HEUR:Trojan.Win32.Gen...
Microsoft
None
Sophos
Mal/Generic-S
Symantec
Trojan.Gen.2
Agnitum
AntiVir
Antiy-AVL
None
Arcabit
None
Avast
Win32:Malware-gen
AVG
Win32:Malware-gen
1 of 237 entities


Maltego Classic 4.0.18
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
Search:
* Recently Used *
AVDefinition
Represents an antiVirus definition
Domain
An internet domain
Email Address
Hash
Hash entity
IPv4 Address
An IP version 4 address
Malware
Imphash
Mutex
Mutexes created by files.
SSL Certificate
Represents an SSL Certificate
Service Name
YARA Hit
Palo Alto Networks
AutoFocus Query
Digital Certificate Common Name
Tag
TagGroup
VirusTotal Submitter ID
Wildfire Session
Home
New Graph (1)
FINFISHER_VARIOUS
Find:
All
Find
Properties
Notes
Display info
Zoom
Hash
IPv4 Address
Domain
APKHash
86.106.102.130
virtual.aw c-cdn-irq2.com
finance.aw c-cdn-irq2.com
ftp.aw c-cdn-irq2.com
Verdict
malware
None
Kaspersky
HEUR:Trojan.Win32.Gen...
Microsoft
None
Sophos
Mal/Generic-S
Symantec
Trojan.Gen.2
Antiy-AVL
None
Arcabit
None
Avast
Win32:Malware-gen
AVG
Win32:Malware-gen
1 of 237 entities


Maltego Classic 4.0.18
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
Search:
* Recently Used *
AVDefinition
Represents an antiVirus definition
Domain
An internet domain
Email Address
An email mailbox to which email messages may
Hash
Hash entity
IPv4 Address
An IP version 4 address
Malware
AVDefinition
Represents an antiVirus definition
Hash
Hash entity
Imphash
The MD5 hash of a files import table (after sort
Mutex
Mutexes created by files.
SSL Certificate
Represents an SSL Certificate
Service Name
A service name created by a file during execut
YARA Hit
The rulename of a YARA rule matching the file.
Palo Alto Networks
AutoFocus Query
A query exported from the AutoFocus UI
Digital Certificate Common Name
An entity representing a Digital Certificate
Tag
A tag matching a given file in AutoFocus
TagGroup
A group that is applied to tags within AutoFocu
VirusTotal Submitter ID
An ID assigned to a submitter in VirusTotal
Wildfire Session
Session data from Palo Alto Networks' Wildfire
Home
New Graph (1)
FINFISHER_VARIOUS
Layout
Freeze
View
Hash
IPv4 Address
Domain
APKHash
Find:
All
Find
Properties
Notes
Display info
Zoom
Output
Overview
Properties
Type
Hash
Hash
c68a7aca2a0a2a73ef60...
md5
f35e058c83bc0ae6e6c4...
sha1
df76eda3c1f9005fb392a...
sha256
c68a7aca2a0a2a73ef60...
imphash
7f5e7860f327442ae9a2...
positives
22
VT_firstSeen
2017-06-08 11:37:48
AF_firstSeen
2017-06-07 21:57:42
pe_timestamp
2012-11-12 11:43:23
fileType
PE
filesize
2561536
submission_names
AF_ITW_Filenames
ITW_URLS
AF_ITW_URLs
af_tags
[u'Unit42.DisableSystem...
Wildfire Verdict
malware
YARA_Hits
AhnLab-V3
None
ESET-NOD32
a variant of Win32/Inject...
F-Secure
None
Kaspersky
HEUR:Trojan.Win32.Gen...
Microsoft
None
Sophos
Mal/Generic-S
Symantec
Trojan.Gen.2
Agnitum
AntiVir
Antiy-AVL
None
Arcabit
None
Avast
Win32:Malware-gen
AVG
Win32:Malware-gen
1 of 237 entities

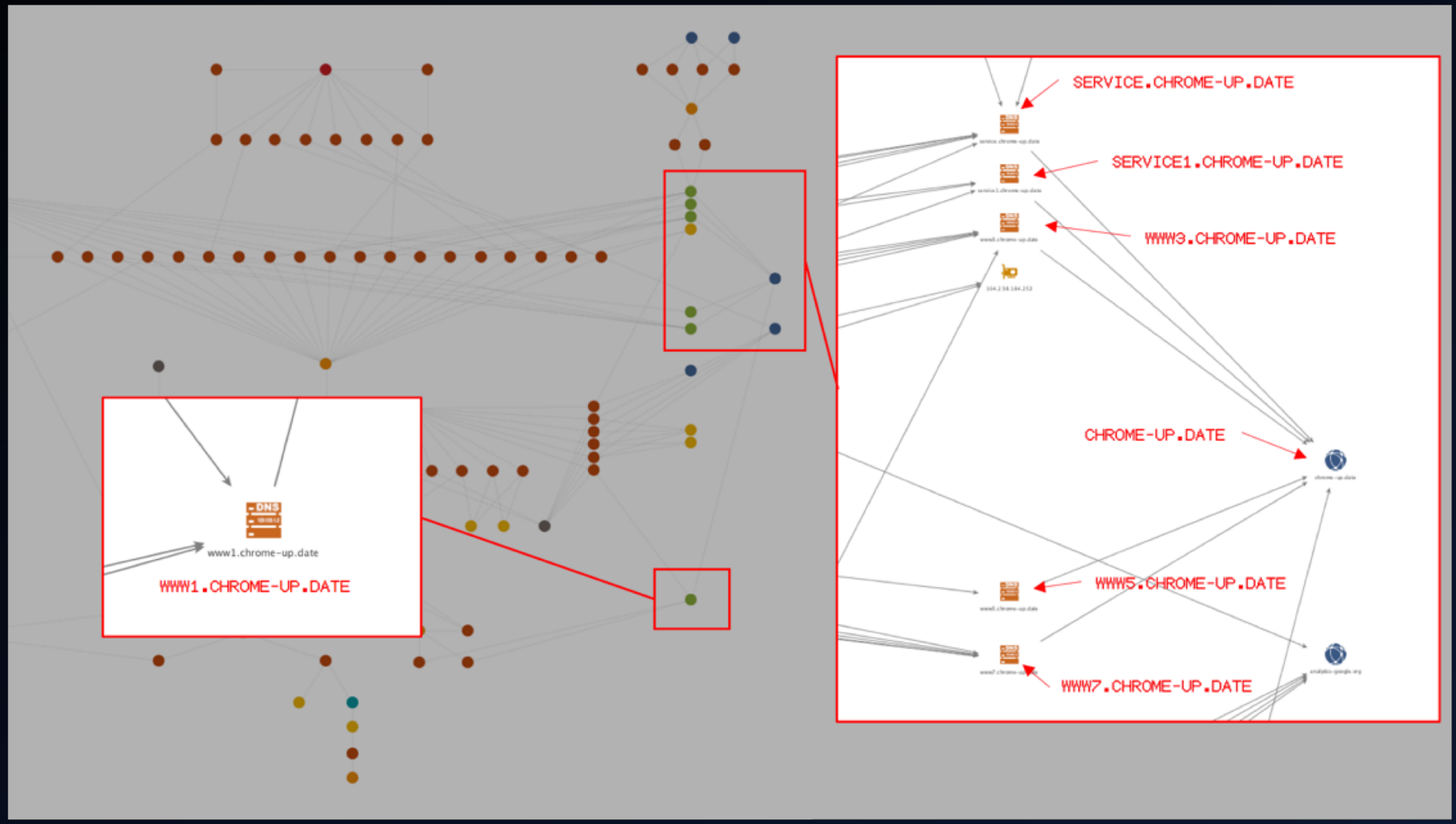

Maltego Classic 4.0.18
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
Search:
* Recently Used *
AVDefinition
Represents an antiVirus definition
Domain
An internet domain
Email Address
Hash
Hash entity
IPv4 Address
An IP version 4 address
Malware
Palo Alto Networks
AutoFocus Query
Digital Certificate Common Name
Tag
TagGroup
VirusTotal Submitter ID
Wildfire Session
Home
New Graph (1)
FINFISHER_VARIOUS
Overview
Property View
Properties
Type
Hash
md5
sha1
sha256
imphash
positives
VT_firstSeen
AF_firstSeen
pe_timestamp
fileType
filesize
submission_names
AF_ITW_Filenames
ITW_URLS
AF_ITW_URLs
af_tags
Wildfire Verdict
malware
YARA_Hits
AhnLab-V3
None
ESET-NOD32
F-Secure
Kaspersky
Microsoft
Sophos
Symantec
Agnitum
AntiVir
Antiy-AVL
Arcabit
Avast
Win32:Malware-gen
AVG
Find:
Properties
Notes
Display info
Zoom
Output
1 of 237 entities

WHY?

USE CASE #1 :: SHOWING YOUR WORKING

How did you get that result?

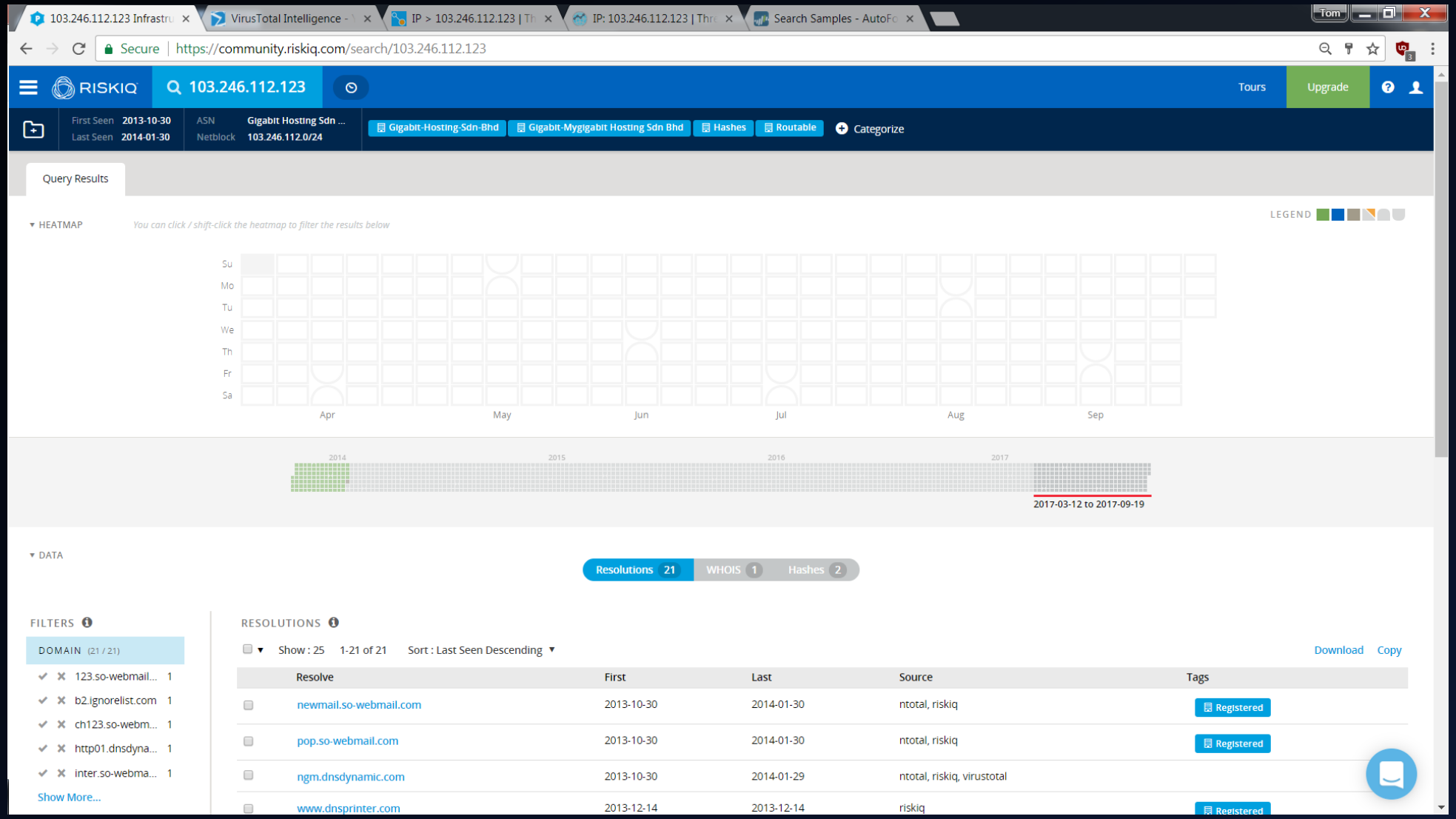
USE CASE #1 :: SHOWING YOUR WORKING



USE CASE #2 :: PIVOTING AND EXPLORING

Tell me more about 103.246.112.123

USE CASE #2 :: PIVOTING AND EXPLORING

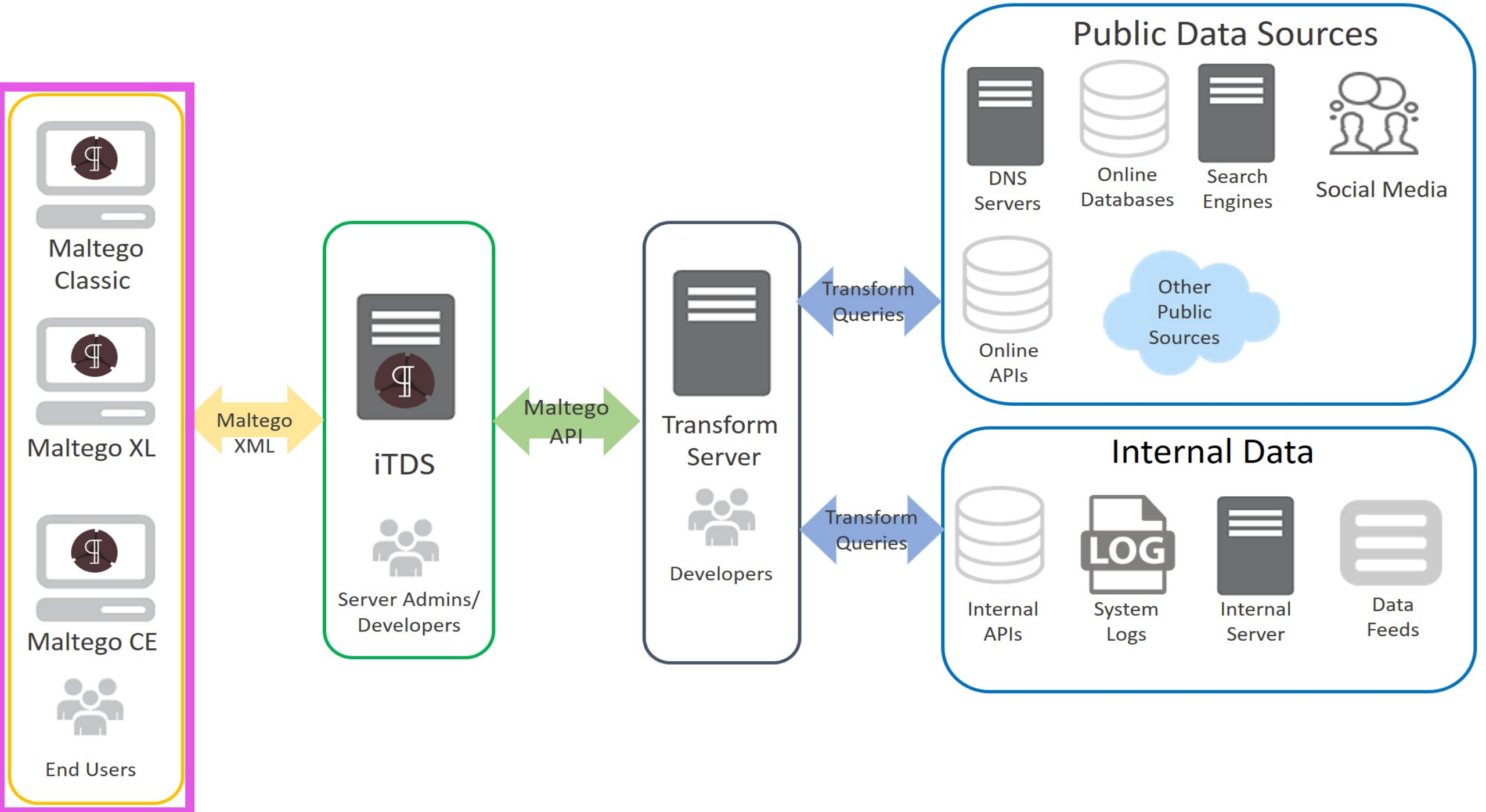


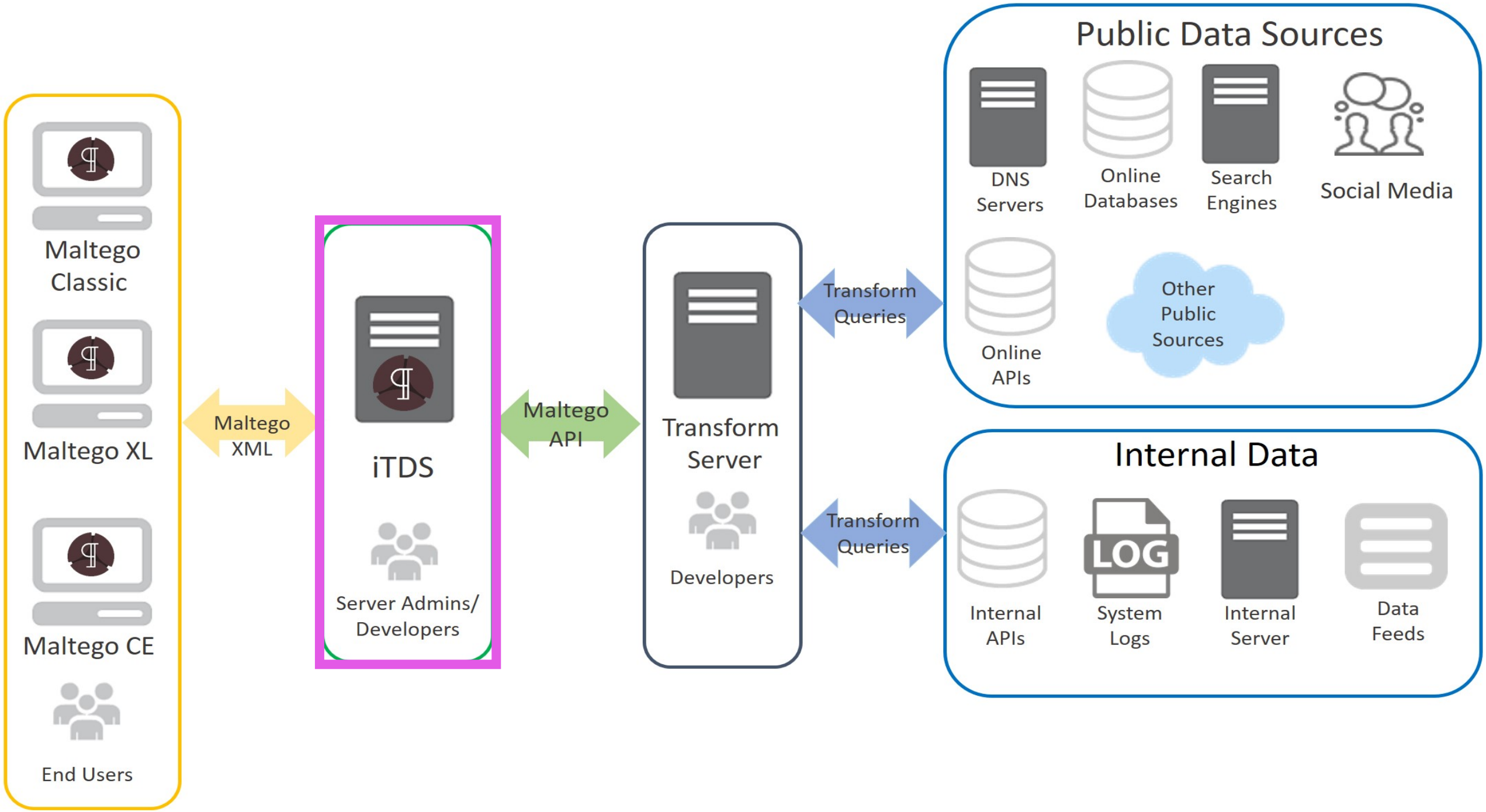
USE CASE #2 :: PIVOTING AND EXPLORING

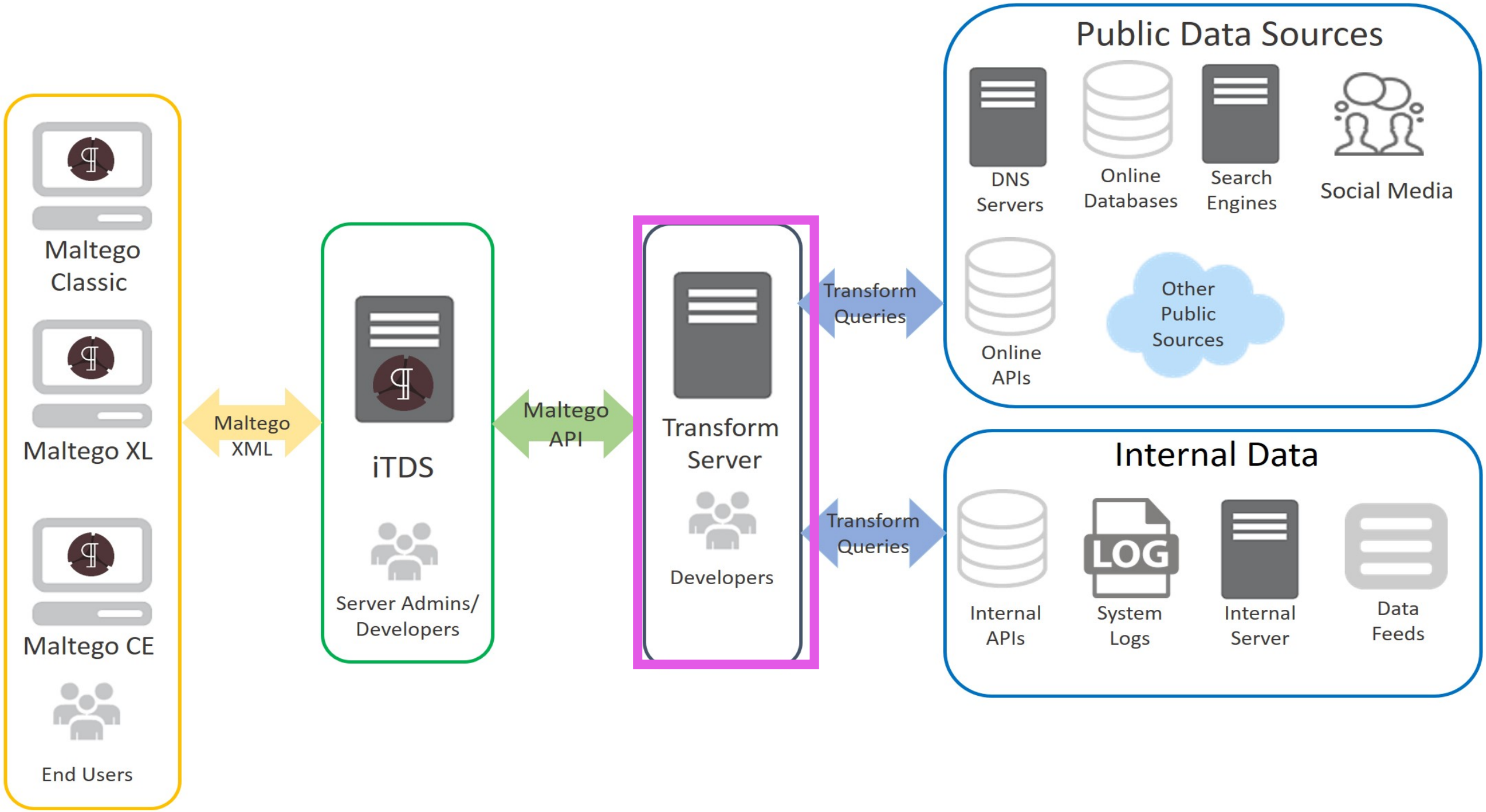
USE CASE #2 :: PIVOTING AND EXPLORING

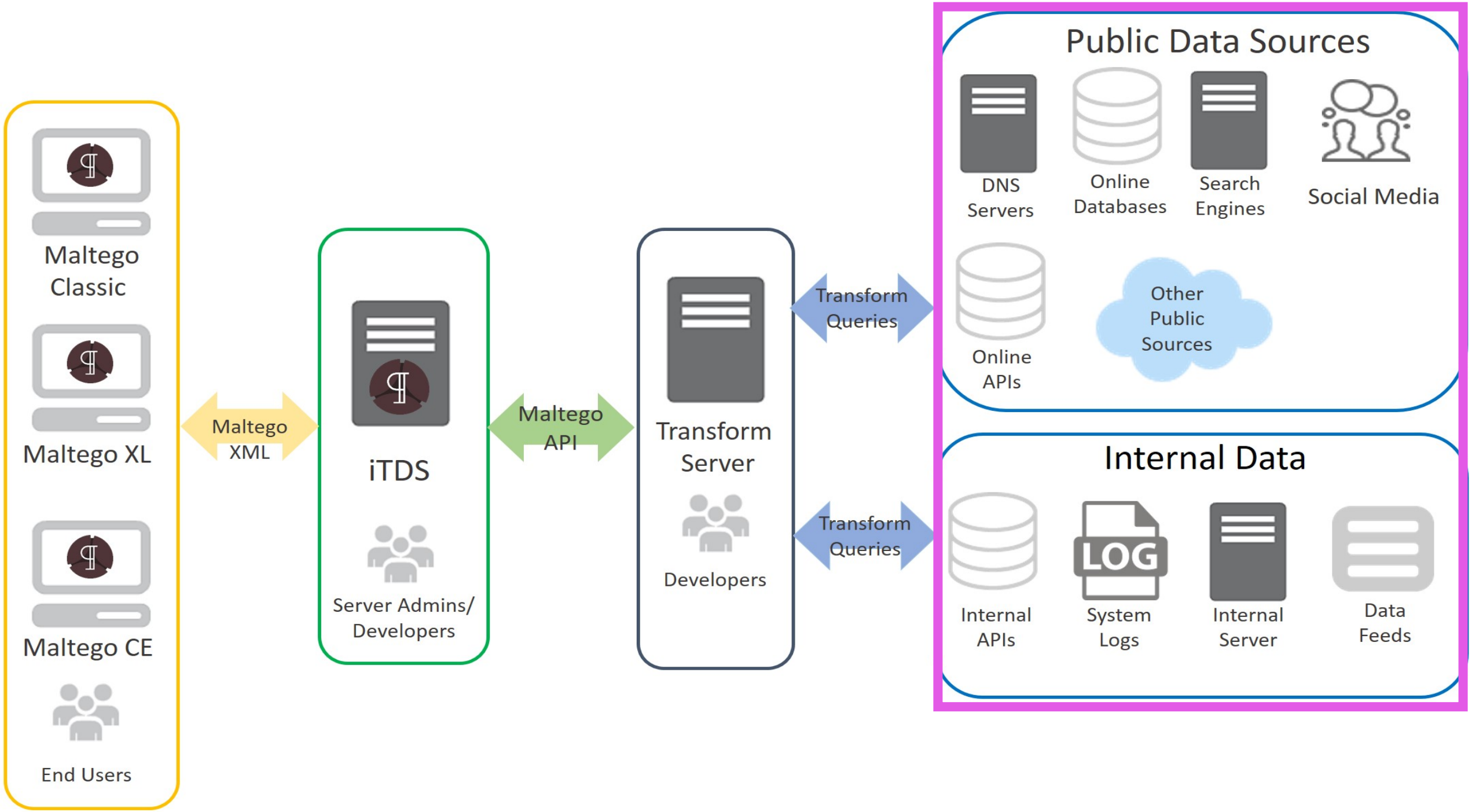
- Check n data sources in 1 click.
- Easy visualisation of links; highlight for context.
- Easy to remove bad data from the view.

The Setup


Public Data Sources
DNS Servers
Online Databases
Search Engines
Social Media
Online APIs
Other Public Sources
Transform Queries
Internal Data
Internal APIs
System Logs
Internal Server
Data Feeds
Transform Queries
Transform Server
Developers
Maltego API
iTDS
Server Admins/ Developers
Maltego XML
Maltego Classic
Maltego XL
Maltego CE
End Users


Public Data Sources
DNS Servers
Online Databases
Search Engines
Social Media
Online APIs
Other Public Sources
Transform Queries
Internal Data
Internal APIs
System Logs
Internal Server
Data Feeds
Transform Queries
Transform Server
Developers
Maltego API
iTDS
Server Admins/ Developers
Maltego XML
Maltego Classic
Maltego XL
Maltego CE
End Users


Public Data Sources
DNS Servers
Online Databases
Search Engines
Social Media
Online APIs
Other Public Sources
Internal Data
Internal APIs
System Logs
Internal Server
Data Feeds
Transform Queries
Transform Queries
Transform Server
Developers
Maltego API
iTDS
Server Admins/ Developers
Maltego XML
Maltego Classic
Maltego XL
Maltego CE
End Users


Maltego Classic
Maltego XL
Maltego CE
End Users
Maltego XML
iTDS
Server Admins/ Developers
Maltego API
Transform Server
Developers
Transform Queries
Transform Queries
Public Data Sources
DNS Servers
Online Databases
Search Engines
Social Media
Online APIs
Other Public Sources
Internal Data
Internal APIs
System Logs
Internal Server
Data Feeds

WE USE

- 100% inhouse written transforms (no public transforms).

- Our own TDS server (access to internal only data sets).

REQUIREMENTS

- 4-5 weeks of dev time;
- access to useful data sources;
- 1 or 2 servers and $$$ for licenses.

WHAT ABOUT THE HUB?

+

PATERVA CTAS — *From Transform Hub*
Paterva
Standard Paterva Transforms
FREE

CaseFile Entities — *From Transform Hub*
Paterva
Additional entities from CaseFile
FREE

SocialLinks — *From Transform Hub*
SocialLinks
Social Networks, Search Engines, People and Companies
COMMERCIAL

Recorded Future — *From Transform Hub*
Recorded Future Inc.
Query Recorded Future for threat intelligence information
COMMERCIAL

Kaspersky Lab — *From Transform Hub*
Kaspersky Lab
Query Kaspersky Threat Intelligence Data Feeds. Note that Data F...
COMMERCIAL

ThreatConnect — *From Transform Hub*
ThreatConnect
ThreatConnect Platform Transform Set
COMMERCIAL

Palo Alto Networks AutoFocus — *From Transform Hub*
Palo Alto Networks
Query Palo Alto Networks' AutoFocus API.
COMMERCIAL

ThreatGRID — *From Transform Hub*
Malformity Labs
Query the ThreatGRID malware platform
COMMERCIAL

Shodan — *From Transform Hub*
Andrew MacPherson (Paterva)
Query Shodan data from within Maltego!
FREE

Flashpoint — *From Transform Hub*
Flashpoint
Business Risk Intelligence (BRI) from the Deep and DarkWeb.
COMMERCIAL

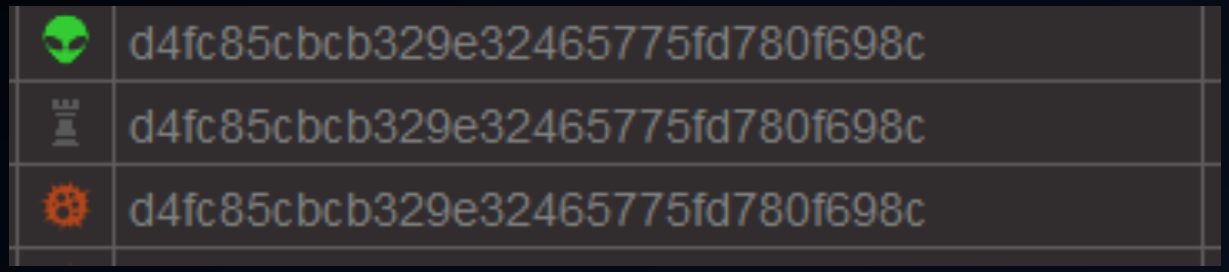
Intel 471 — *From Transform Hub*
Intel 471
Query Intel 471 for actor-centric intelligence information.
COMMERCIAL

CrowdStrike Intel — *From Transform Hub*
CrowdStrike
CrowdStrike Intelligence API Transforms
COMMERCIAL

CrowdStrike ThreatGraph — *From Transform Hub*
CrowdStrike
CrowdStrike ThreatGraph API Transforms
COMMERCIAL

VirusTotal Public API — *From Transform Hub*
Malformity Labs
Query the VirusTotal Public API
FREE

PROBLEMS WITH PUBLIC TRANSFORMS

- 

- Context menu problems
- Link Labels
- Properties

WRITING TRANSFORMS

HELLO WORLD

```
'''
hello world transform
'''
from Maltego import MaltegoTransform
me = MaltegoTransform()
me.addEntity("maltego.emailAddress", "hello@world.com")
me.returnOutput()
```

WRITING YOUR OWN TRANSFORMS

- Relatively easy!
- Add a wrapper around the base Maltego library.
- Wrapper makes for easy bulk changes

PALO MALTEGO HELLO WORLD

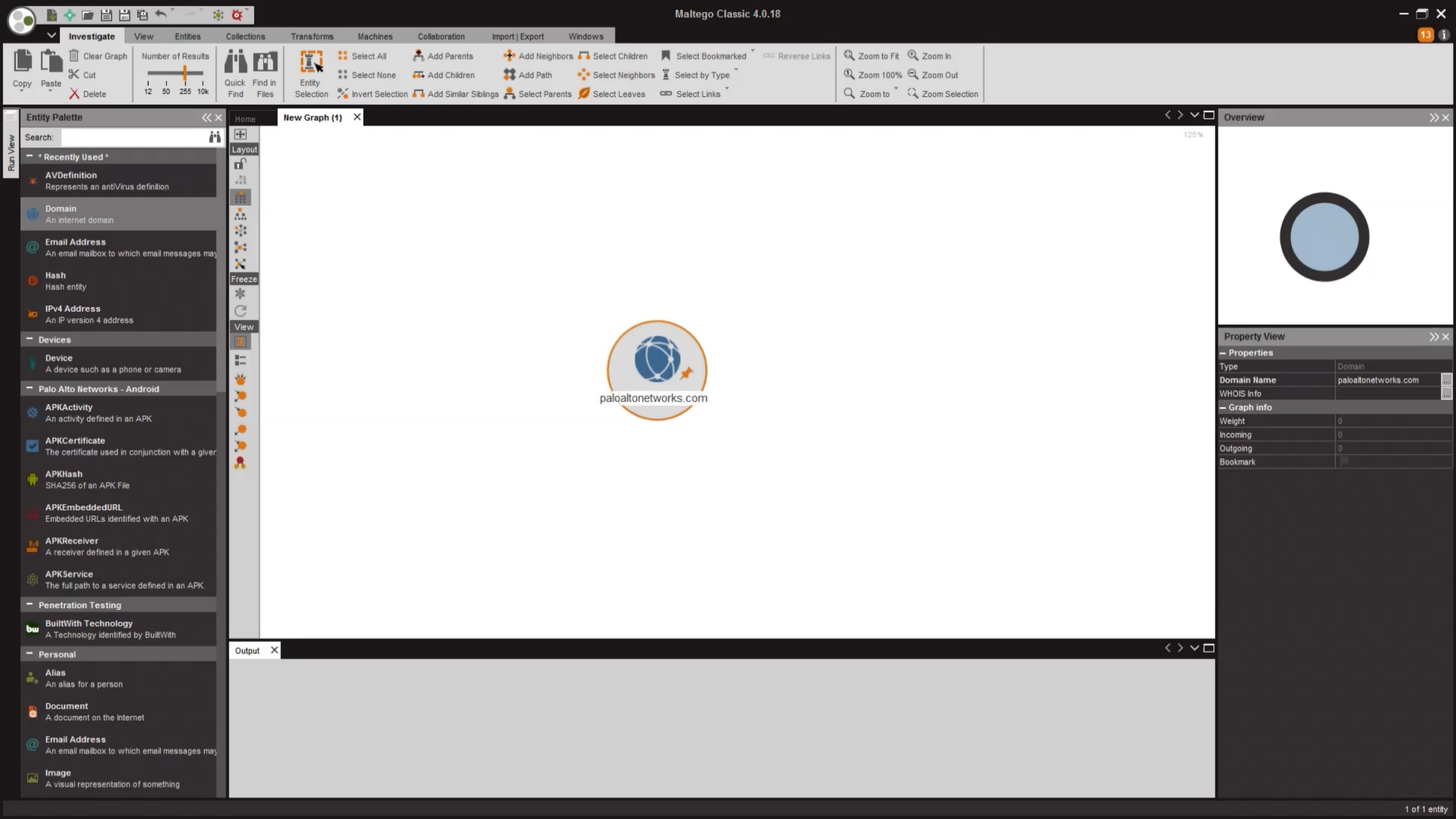
```
from PaloMaltego import PaloMaltego as pm

def PaloHelloWorld(m):
    '''
     m :: the XML passed to the function by the server
    '''
    retObj = pm(m, "Hello World", transformType="example")
    prop = retObj.defineProperty("Run Date", retObj.TransformRunDate)
    retObj.returnEmail("hello@world.com", properties=prop)
    retObj.returnOutput()
```

PRE-FILTERING

```
def returnEmail(self, value, properties=None,):
    '''
    value : the value we wish to return
    properties : a list of properties
    '''
    # Check if the supplied value is blacklisted, if it is, stop executing.
    if self.isBlacklistedEmail(value) is True:
        return
    # A function that actually a returns something to the graph
    self.returnEntity(value, ipEntity, properties)
```

PRE-FILTERING IN ACTION


Maltego Classic 4.0.18
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
12
50
255
10k
Quick Find
Find in Files
Entity Selection
Select All
Select None
Invert Selection
Add Parents
Add Children
Add Similar Siblings
Add Neighbors
Add Path
Select Parents
Select Children
Select Neighbors
Select Leaves
Select Bookmarked
Select by Type
Select Links
Reverse Links
Zoom to Fit
Zoom In
Zoom 100%
Zoom Out
Zoom to
Zoom Selection
Run View
Entity Palette
Search:
* Recently Used *
AVDefinition
Represents an antiVirus definition
Domain
An internet domain
Email Address
An email mailbox to which email messages may
Hash
Hash entity
IPv4 Address
An IP version 4 address
Devices
Device
A device such as a phone or camera
Palo Alto Networks - Android
APKActivity
An activity defined in an APK
APKCertificate
The certificate used in conjunction with a giver
APKHash
SHA256 of an APK File
APKEmbeddedURL
Embedded URLs identified with an APK
APKReceiver
A receiver defined in a given APK
APKService
The full path to a service defined in an APK.
Penetration Testing
BuiltWith Technology
A Technology identified by BuiltWith
Personal
Alias
An alias for a person
Document
A document on the Internet
Email Address
An email mailbox to which email messages may
Image
A visual representation of something
Home
New Graph (1)
Layout
Freeze
View
125%
paloaltonetworks.com
Output
Overview
Property View
Properties
Type
Domain
Domain Name
paloaltonetworks.com
WHOIS Info
Graph info
Weight
0
Incoming
0
Outgoing
0
Bookmark
1 of 1 entity

POST PROCESSING

KEEP YOUR GRAPHS

- Don’t throw your graphs away.
- They contain useful, structured data.
- Make them searchable.

MTGX --> OTHER SYSTEMS

Save graphs to common location

Watch for changes

Index graph and log changes

Forward data to other systems

OTHER SYSTEMS --> MTGX

- Someone shares some domains with you…

diaco-tools\.com

technical-notes\.com

mj-notes\.com

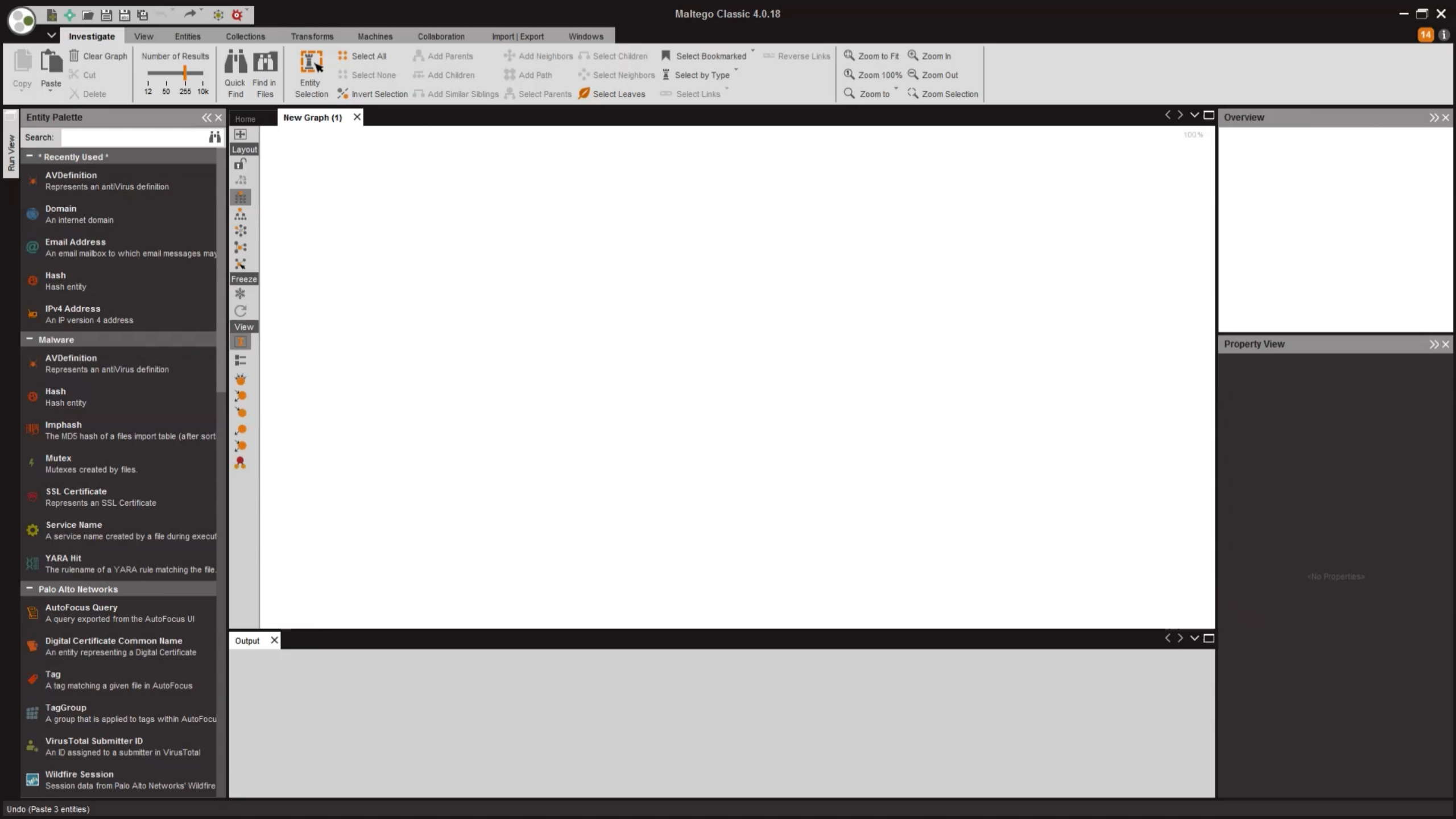
OTHER SYSTEMS --> MTGX

What actor do these domains relate to?

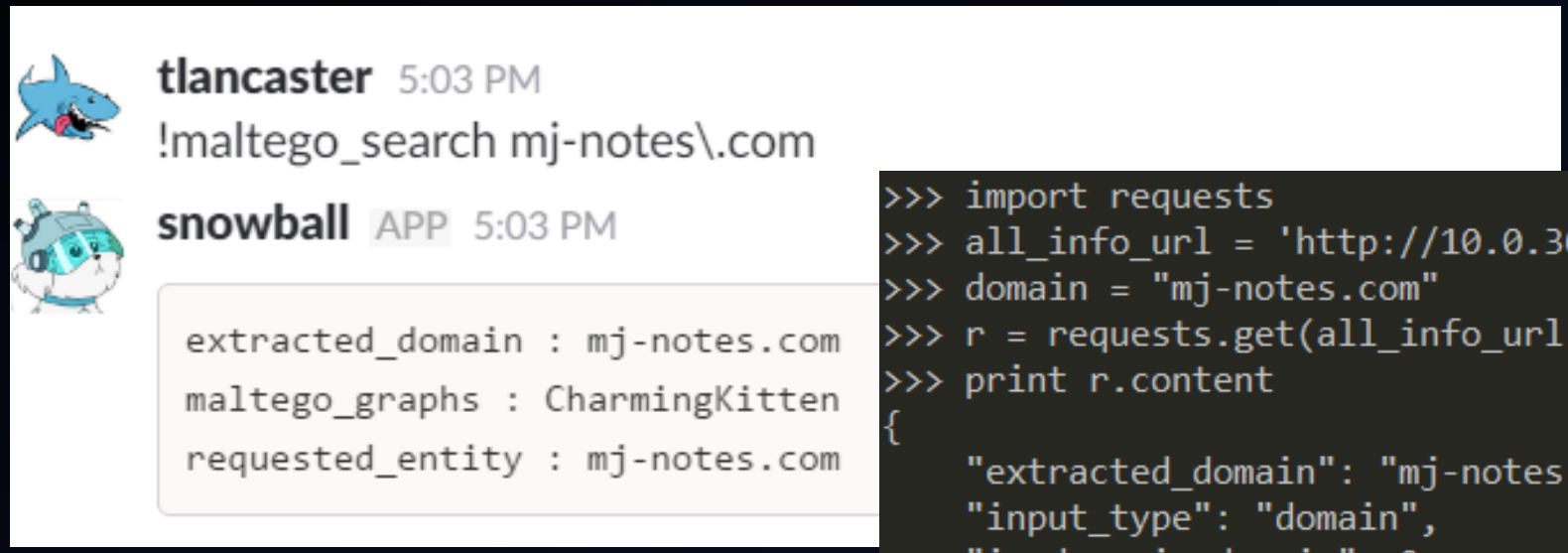
Can I illustrate this to someone else quickly?

How did I come to that conclusion?

SEARCHING GRAPH DATA


Maltego Classic 4.0.18
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
12
50
255
10k
Quick Find
Find in Files
Entity Selection
Select All
Select None
Invert Selection
Add Parents
Add Children
Add Similar Siblings
Add Neighbors
Add Path
Select Parents
Select Children
Select Neighbors
Select Leaves
Select Bookmarked
Select by Type
Select Links
Reverse Links
Zoom to Fit
Zoom In
Zoom 100%
Zoom Out
Zoom to
Zoom Selection
Run View
Entity Palette
Search:
* Recently Used *
AVDefinition
Represents an antiVirus definition
Domain
An internet domain
Email Address
An email mailbox to which email messages may
Hash
Hash entity
IPv4 Address
An IP version 4 address
Malware
AVDefinition
Represents an antiVirus definition
Hash
Hash entity
Imphash
The MD5 hash of a files import table (after sort
Mutex
Mutexes created by files.
SSL Certificate
Represents an SSL Certificate
Service Name
A service name created by a file during execut
YARA Hit
The rulename of a YARA rule matching the file.
Palo Alto Networks
AutoFocus Query
A query exported from the AutoFocus UI
Digital Certificate Common Name
An entity representing a Digital Certificate
Tag
A tag matching a given file in AutoFocus
TagGroup
A group that is applied to tags within AutoFocu
VirusTotal Submitter ID
An ID assigned to a submitter in VirusTotal
Wildfire Session
Session data from Palo Alto Networks' Wildfire
Home
New Graph (1)
Layout
Freeze
View
100%
Output
Overview
Property View
«No Properties»
Undo (Paste 3 entities)

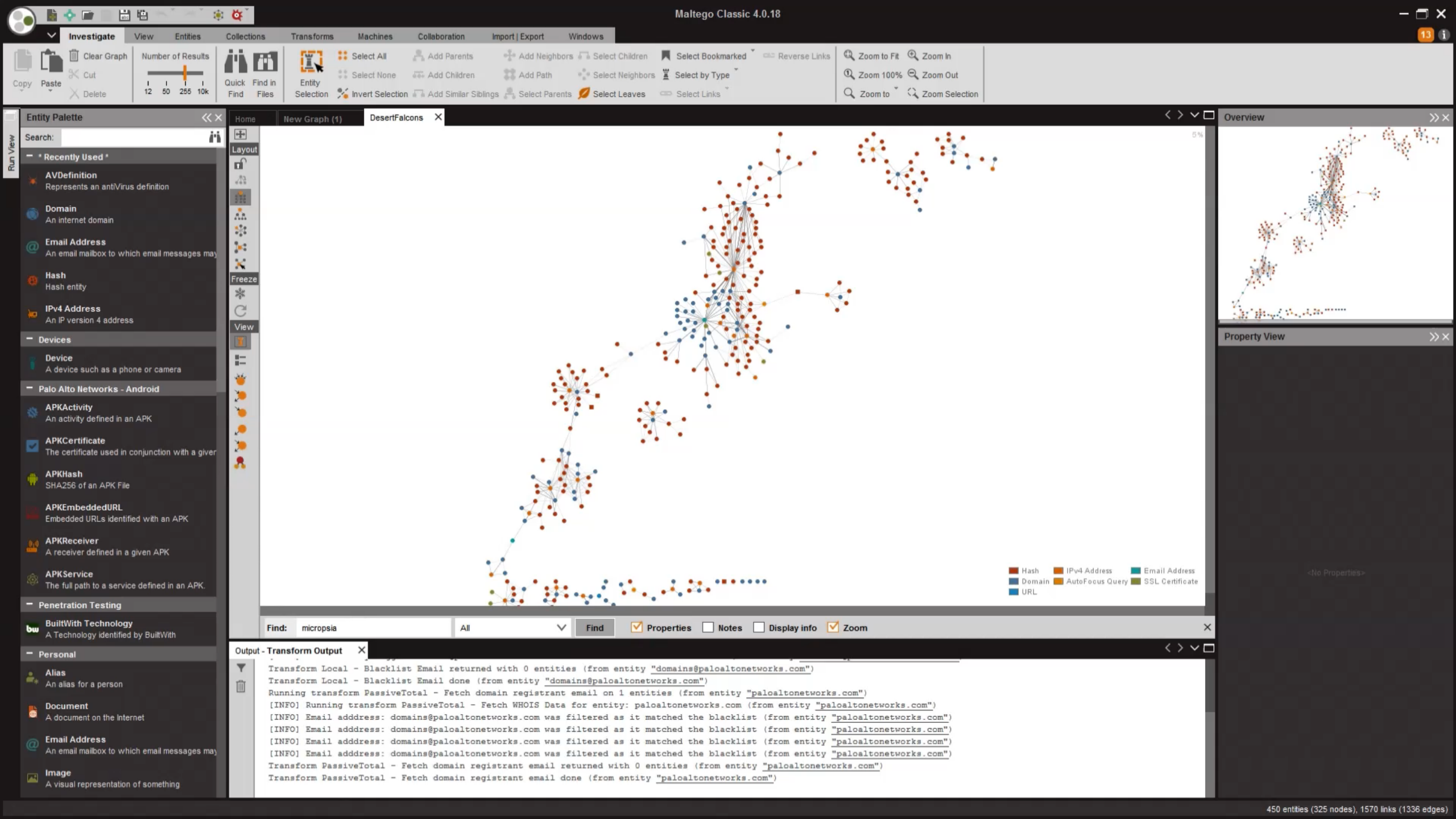
NOT JUST FOR MALTEGO




```
>>> import requests
>>> all_info_url = 'http://10.0.36.17:81/transform_api_v1/query/%s/%s'
>>> domain = "mj-notes.com"
>>> r = requests.get(all_info_url % ('domain' , domain))
>>> print r.content
{
    "extracted_domain": "mj-notes.com",
    "input_type": "domain",
    "is_dynamic_domain": 0,
    "is_generic_email_registrant": 0,
    "is_parking_ip": 0,
    "is_sinkhole": 0,
    "is_uninteresting_domain": 0,
    "maltego_graphs": [
        "CharmingKitten"
    ],
    "requested_entity": "mj-notes.com"
}
```

USING THE CLIENT

USING FIND MORE OFTEN


Maltego Classic 4.0.18
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
12 50 255 10k
Quick Find
Find in Files
Entity Selection
Select All
Select None
Invert Selection
Add Parents
Add Children
Add Similar Siblings
Add Neighbors
Add Path
Select Parents
Select Children
Select Neighbors
Select Leaves
Select Bookmarked
Select by Type
Select Links
Reverse Links
Zoom to Fit
Zoom In
Zoom 100%
Zoom Out
Zoom to
Zoom Selection
Run View
Entity Palette
Search:
* Recently Used *
AVDefinition
Represents an antiVirus definition
Domain
An internet domain
Email Address
An email mailbox to which email messages may
Hash
Hash entity
IPv4 Address
An IP version 4 address
Devices
Device
A device such as a phone or camera
Palo Alto Networks - Android
APKActivity
An activity defined in an APK
APKCertificate
The certificate used in conjunction with a giver
APKHash
SHA256 of an APK File
APKEmbeddedURL
Embedded URLs identified with an APK
APKReceiver
A receiver defined in a given APK
APKService
The full path to a service defined in an APK.
Penetration Testing
BuiltWith Technology
A Technology identified by BuiltWith
Personal
Alias
An alias for a person
Document
A document on the Internet
Email Address
An email mailbox to which email messages may
Image
A visual representation of something
Home
New Graph (1)
DesertFalcons
Layout
Freeze
View
Hash
IPv4 Address
Email Address
Domain
AutoFocus Query
SSL Certificate
URL
Find:
micropsia
All
Find
Properties
Notes
Display info
Zoom
Overview
Property View
<No Properties>
Output - Transform Output
Transform Local - Blacklist Email returned with 0 entities (from entity "domains@paloaltonetworks.com")
Transform Local - Blacklist Email done (from entity "domains@paloaltonetworks.com")
Running transform PassiveTotal - Fetch domain registrant email on 1 entities (from entity "paloaltonetworks.com")
[INFO] Running transform PassiveTotal - Fetch WHOIS Data for entity: paloaltonetworks.com (from entity "paloaltonetworks.com")
[INFO] Email adddress: domains@paloaltonetworks.com was filtered as it matched the blacklist (from entity "paloaltonetworks.com")
[INFO] Email adddress: domains@paloaltonetworks.com was filtered as it matched the blacklist (from entity "paloaltonetworks.com")
[INFO] Email adddress: domains@paloaltonetworks.com was filtered as it matched the blacklist (from entity "paloaltonetworks.com")
[INFO] Email adddress: domains@paloaltonetworks.com was filtered as it matched the blacklist (from entity "paloaltonetworks.com")
Transform PassiveTotal - Fetch domain registrant email returned with 0 entities (from entity "paloaltonetworks.com")
Transform PassiveTotal - Fetch domain registrant email done (from entity "paloaltonetworks.com")
450 entities (325 nodes), 1570 links (1336 edges)

MAKE AND USE TRANSFORM SETS

Maltego Classic 4.0.18

Investigate | View | Entities | Collections | Transforms | Machines | Collaboration | Import | Export | Windows

Copy | Paste | Clear Graph | Cut | Delete | Number of Results (12 50 255 10k) | Quick Find | Find in Files | Entity Selection | Select All | Select None | Invert Selection | Add Parents | Add Children | Add Similar Siblings | Add Neighbors | Add Path | Select Parents | Select Children | Select Neighbors | Select Leaves | Select Bookmarked | Select by Type | Select Links | Reverse Links | Zoom to Fit | Zoom In | Zoom 100% | Zoom Out | Zoom to | Zoom Selection

Run View

Entity Palette

Search:

* Recently Used *

- AVDefinition — Represents an antiVirus definition
- Domain — An internet domain
- Email Address — An email mailbox to which email messages may
- Hash — Hash entity
- IPv4 Address — An IP version 4 address

Devices

- Device — A device such as a phone or camera

Palo Alto Networks - Android

- APKActivity — An activity defined in an APK
- APKCertificate — The certificate used in conjunction with a given
- APKHash — SHA256 of an APK File
- APKEmbeddedURL — Embedded URLs identified with an APK
- APKReceiver — A receiver defined in a given APK
- APKService — The full path to a service defined in an APK.

Penetration Testing

- BuiltWith Technology — A Technology identified by BuiltWith

Personal

- Alias — An alias for a person
- Document — A document on the Internet
- Email Address — An email mailbox to which email messages may
- Image — A visual representation of something

Home | New Graph (1)

Layout | Freeze | View

125%

Output - Transform Output

```
Transform PassiveTotal - Fetch domain registrant email returned with 0 entities (from entity "paloaltonetworks.com")
Transform PassiveTotal - Fetch domain registrant email done (from entity "paloaltonetworks.com")
Running transform NetworkTotal - Get Subdomains on 1 entities (from entity "vpn.konamidata.com")
[INFO] Running transform NetworkTotal - Get Subdomains for entity: vpn.konamidata.com (from entity "vpn.konamidata.com")
Transform NetworkTotal - Get Subdomains returned with 0 entities (from entity "vpn.konamidata.com")
Transform NetworkTotal - Get Subdomains done (from entity "vpn.konamidata.com")
Running transform NetworkTotal - Get Subdomains on 1 entities (from entity "konamidata.com")
[INFO] Running transform NetworkTotal - Get Subdomains for entity: konamidata.com (from entity "konamidata.com")
Transform NetworkTotal - Get Subdomains returned with 246 entities (from entity "konamidata.com")
Transform NetworkTotal - Get Subdomains done (from entity "konamidata.com")
```

Overview

Property View

Properties	
Type	Domain
Domain Name	kvnn.konamidata.com
WHOIS Info	
Graph info	
Weight	0
Incoming	0
Outgoing	0
Bookmark	

1 of 1 entity

USING “COLLECTIONS” TO QUICKLY PRUNE BAD DATA

Maltego Classic 4.0.18

Investigate | View | Entities | Collections | Transforms | Machines | Collaboration | Import | Export | Windows

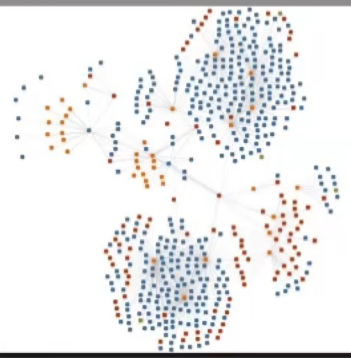
Copy | Paste | Clear Graph | Cut | Delete | Number of Results (12 50 255 10k) | Quick Find | Find in Files | Entity Selection | Select All | Select None | Invert Selection | Add Parents | Add Children | Add Similar Siblings | Add Neighbors | Add Path | Select Parents | Select Children | Select Neighbors | Select Leaves | Select Bookmarked | Select by Type | Select Links | Reverse Links | Zoom to Fit | Zoom In | Zoom 100% | Zoom Out | Zoom to | Zoom Selection

Run View | Entity Palette | Layout | Freeze | View

New Graph (1)

Hash | IPv4 Address | Domain | APKHash

Overview



Property View

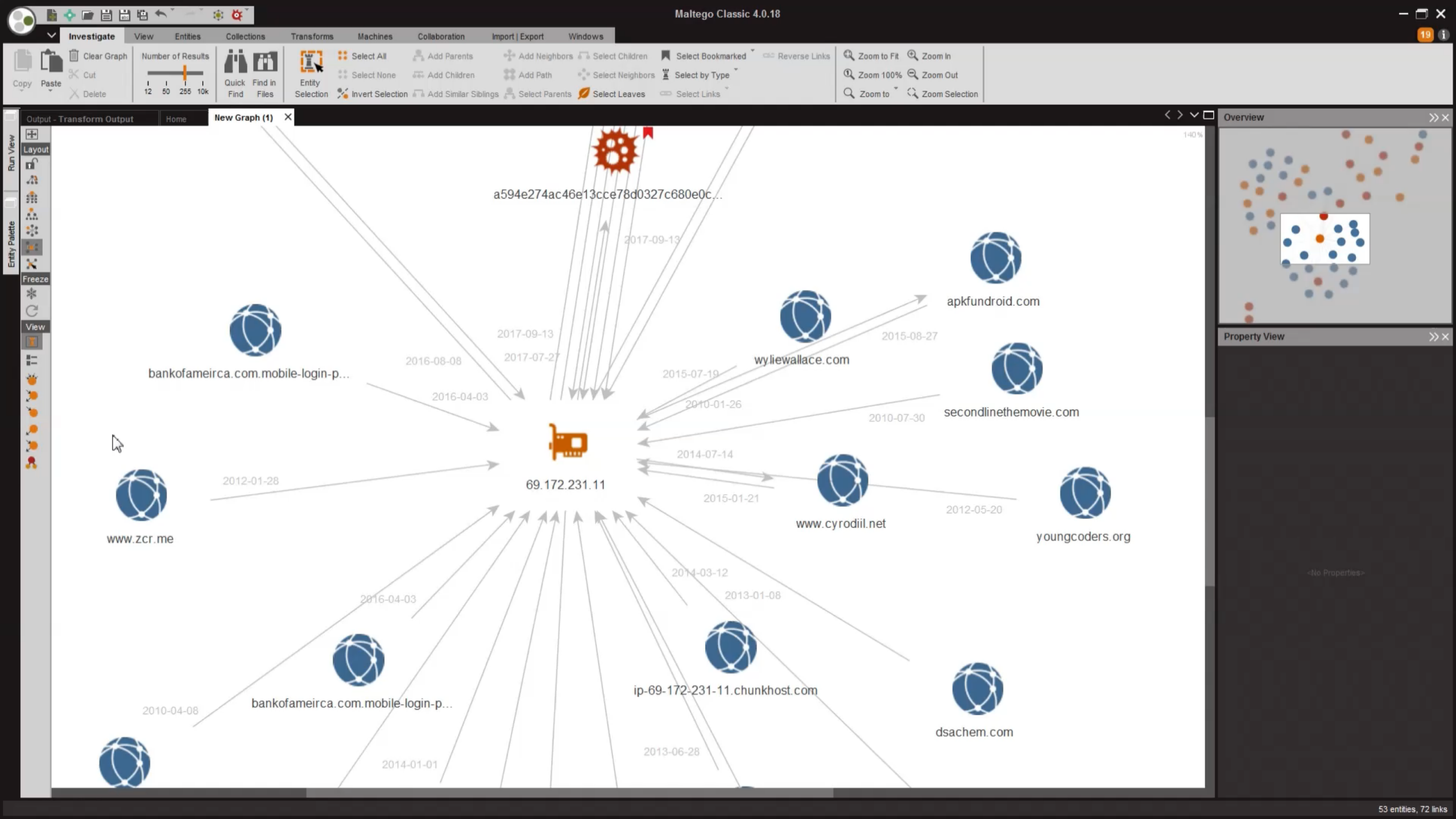
<No Properties>

Output - Transform Output

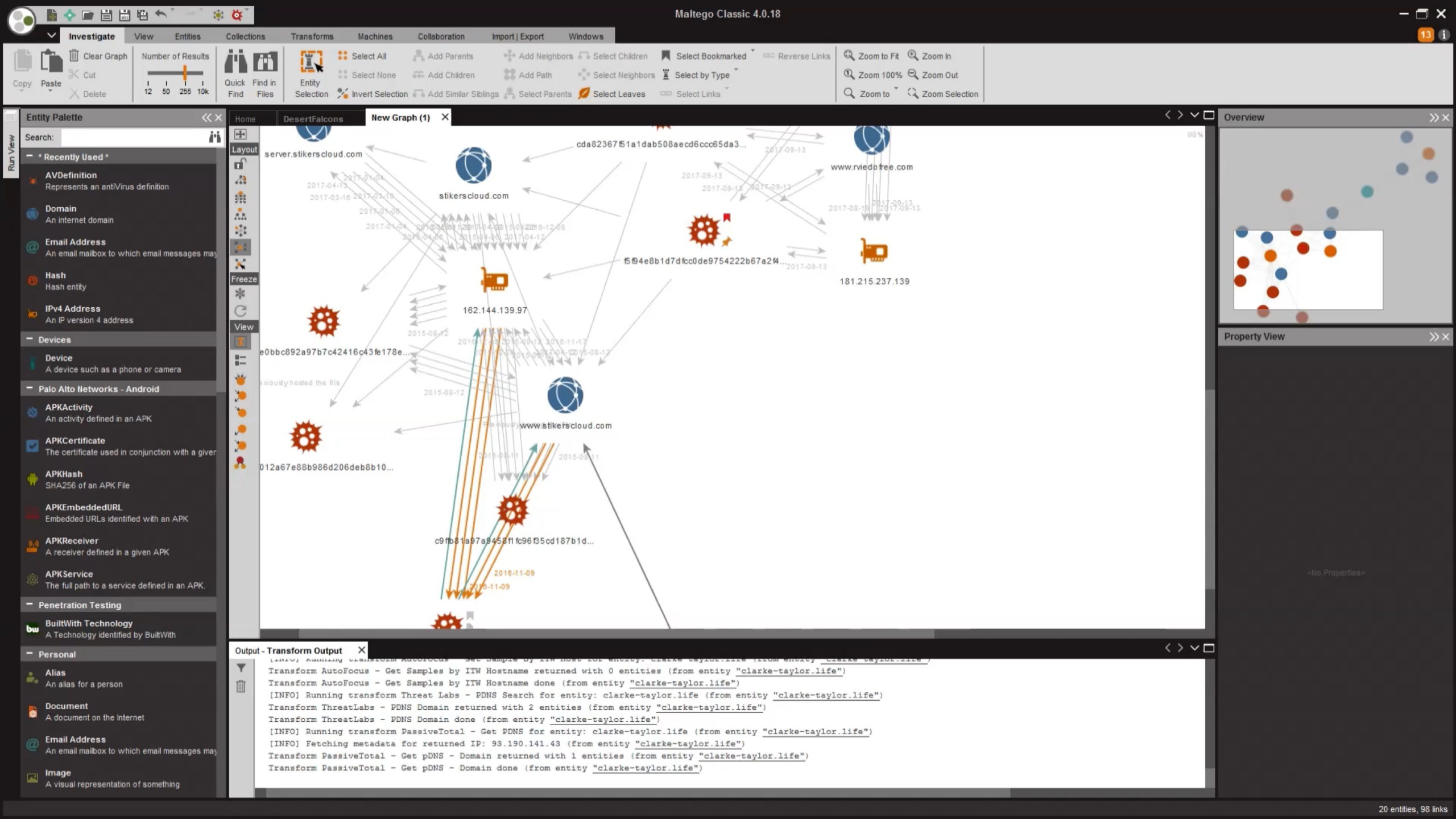
```
[INFO] Sample: bc6788471e639bf62208160a64fff8bd718b5d0418039643fbbf3b443057e022 was filtered.The tag Commodity.Virut is blacklisted (from entity "23.62.6.19")
[INFO] Sample: ba91d5b293d1cdf705f3a44bd3763b6de1191c3a8c5f0d8c13a1c83216c4803d was filtered.The tag Commodity.Virut is blacklisted (from entity "23.62.6.19")
[WARNING] Additional entities were available but could not be returned due to the slider limit (from entity "23.62.6.19")
Transform AutoFocus - Get Sample by IP returned with 255 entities (from entity "23.62.6.19")
[INFO] Running transform AutoFocus - Get Sample By C2 for entity: 23.62.6.18 (from entity "23.62.6.18")
[INFO] Sample: bc6788471e639bf62208160a64fff8bd718b5d0418039643fbbf3b443057e022 was filtered.The tag Commodity.Virut is blacklisted (from entity "23.62.6.18")
[INFO] Sample: ba91d5b293d1cdf705f3a44bd3763b6de1191c3a8c5f0d8c13a1c83216c4803d was filtered.The tag Commodity.Virut is blacklisted (from entity "23.62.6.18")
[WARNING] Additional entities were available but could not be returned due to the slider limit (from entity "23.62.6.18")
Transform AutoFocus - Get Sample by IP returned with 255 entities (from entity "23.62.6.18")
Transform AutoFocus - Get Sample by IP done (from 2 entities)
```

4565 entities (520 nodes), 6207 links (1082 edges)

USING LINK LABELS TO PRUNE BAD DATA FROM GRAPHS


Maltego Classic 4.0.18
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Clear Graph
Cut
Delete
Copy
Paste
Number of Results
12
50
255
10k
Quick Find
Find in Files
Entity Selection
Select All
Select None
Invert Selection
Add Parents
Add Children
Add Similar Siblings
Add Neighbors
Add Path
Select Parents
Select Children
Select Neighbors
Select Leaves
Select Bookmarked
Select by Type
Select Links
Reverse Links
Zoom to Fit
Zoom In
Zoom 100%
Zoom Out
Zoom to
Zoom Selection
Output - Transform Output
Home
New Graph (1)
Layout
Freeze
View
Run View
Entity Palette
Overview
Property View
<No Properties>
a594e274ac46e13cce78d0327c680e0c...
2017-09-13
apkfundroid.com
wyliewallace.com
2015-08-27
secondlinethemovie.com
2010-07-30
bankofameirca.com.mobile-login-p...
2017-09-13
2017-07-27
2016-08-08
2016-04-03
2015-07-19
2010-01-26
69.172.231.11
2014-07-14
2015-01-21
www.cyrodiil.net
2012-05-20
youngcoders.org
www.zcr.me
2012-01-28
2011-03-12
2013-01-08
2016-04-03
bankofameirca.com.mobile-login-p...
ip-69-172-231-11.chunkhost.com
dsachem.com
2010-04-08
2013-06-28
2014-01-01
53 entities, 72 links

PASTING ONTO EXISTING GRAPHS


Maltego Classic 4.0.18
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
12
50
255
10k
Quick Find
Find in Files
Entity Selection
Select All
Select None
Invert Selection
Add Parents
Add Children
Add Similar Siblings
Add Neighbors
Add Path
Select Parents
Select Children
Select Neighbors
Select Leaves
Select Bookmarked
Select by Type
Select Links
Reverse Links
Zoom to Fit
Zoom In
Zoom 100%
Zoom Out
Zoom to
Zoom Selection
Entity Palette
Search:
* Recently Used *
AVDefinition
Represents an antiVirus definition
Domain
An internet domain
Email Address
An email mailbox to which email messages may
Hash
Hash entity
IPv4 Address
An IP version 4 address
Devices
Device
A device such as a phone or camera
Palo Alto Networks - Android
APKActivity
An activity defined in an APK
APKCertificate
The certificate used in conjunction with a giver
APKHash
SHA256 of an APK File
APKEmbeddedURL
Embedded URLs identified with an APK
APKReceiver
A receiver defined in a given APK
APKService
The full path to a service defined in an APK.
Penetration Testing
BuiltWith Technology
A Technology identified by BuiltWith
Personal
Alias
An alias for a person
Document
A document on the Internet
Email Address
An email mailbox to which email messages may
Image
A visual representation of something
Home
DesertFalcons
New Graph (1)
Layout
Freeze
View
server.stikerscloud.com
stikerscloud.com
cda82367f51a1dab508aecd6ccc65da3...
www.rviedofree.com
f5f94e8b1d7dfcc0de9754222b67a2f4...
181.215.237.139
162.144.139.97
e0bbc892a97b7c42416c43fe178e...
www.stikerscloud.com
012a67e88b986d206deb8b10...
c9ffb81a97a8458f1fc96f35cd187b1d...
Overview
Property View
<No Properties>
Output - Transform Output
Transform AutoFocus - Get Samples by ITW Hostname returned with 0 entities (from entity "clarke-taylor.life")
Transform AutoFocus - Get Samples by ITW Hostname done (from entity "clarke-taylor.life")
[INFO] Running transform Threat Labs - PDNS Search for entity: clarke-taylor.life (from entity "clarke-taylor.life")
Transform ThreatLabs - PDNS Domain returned with 2 entities (from entity "clarke-taylor.life")
Transform ThreatLabs - PDNS Domain done (from entity "clarke-taylor.life")
[INFO] Running transform PassiveTotal - Get PDNS for entity: clarke-taylor.life (from entity "clarke-taylor.life")
[INFO] Fetching metadata for returned IP: 93.190.141.43 (from entity "clarke-taylor.life")
Transform PassiveTotal - Get pDNS - Domain returned with 1 entities (from entity "clarke-taylor.life")
Transform PassiveTotal - Get pDNS - Domain done (from entity "clarke-taylor.life")
20 entities, 98 links

OVERALL BENEFITS

- Faster analysis
- “Visual Breadcrumbs”.
- Easy export of relationships to 3rd party systems.
- Reconstruct historical investigations more easily.

CONCLUSIONS

- Write your own transforms.
- Use transform sets.
- Store and post-process your graphs.

GOT CODE?

- No public code. For now.
- Happy to help/advise.
- If you’re a power user, come join our user group

ANY QUESTIONS?

@TLANSEC