

# SEMI-AUTOMATED CYBER THREAT INTELLIGENCE (ACT)

Training – FIRST CTI Symposium 2019 London

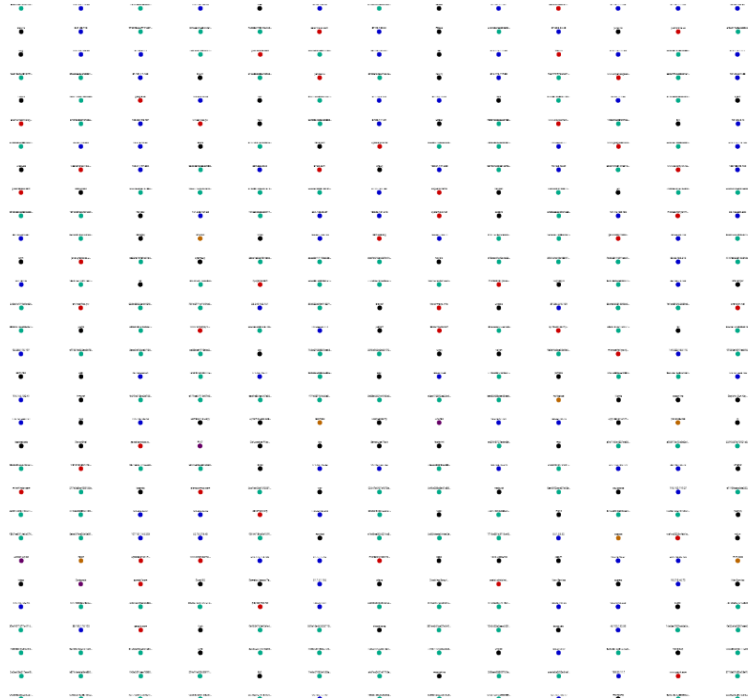
Martin Eian, Fredrik Borg, Geir Skjøtskift and Siri Bromander

■ Goal

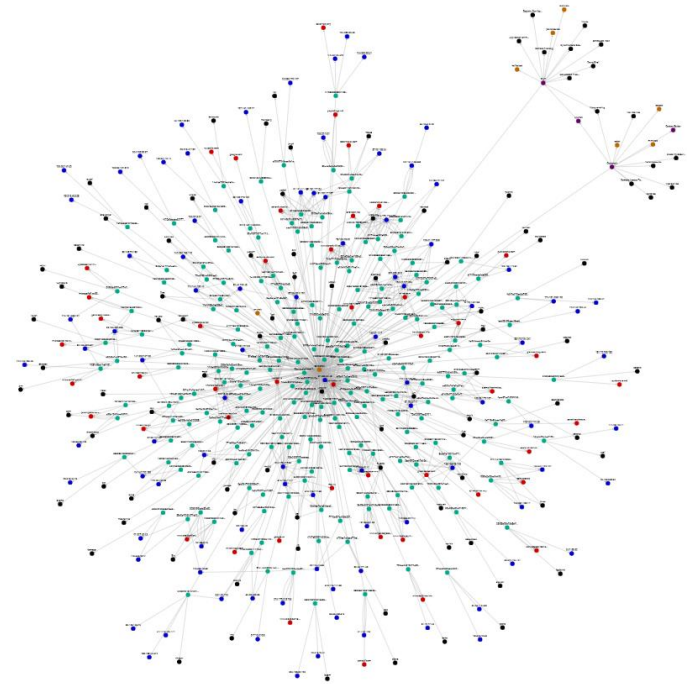
To collect and organize  
our knowledge of threats  
to make it useful

# Data and Information

## Data



## Information



## | Semi-Automated...

- Analysis
- Enrichment
- Information Sharing
- Countermeasures

# | Semi-Automated Cyber Threat Intelligence (ACT)

The main objective of the research project is to develop a *platform for cyber threat intelligence* to uncover cyberattacks, cyber espionage and sabotage.

The project will result in new methods for data *enrichment* and data *analysis* to enable *identification of threat agents*, their motives, resources and attack methodologies.

In addition, the project will develop new methods, work processes and mechanisms for the *generation and distribution of threat intelligence and countermeasures*, to stop ongoing and prevent future attacks.





# Models, Taxonomies and Vocabularies

- MITRE ATT&CK

- <https://attack.mitre.org>

- MITRE PRE-ATT&CK

- <https://attack.mitre.org/pre-attack/>

- MISP galaxy

- <https://github.com/MISP/misp-galaxy>

- STIX 2.0 vocabularies

- <https://oasis-open.github.io/cti-documentation/>

- Ryan Stillions' DML model

- [http://ryanstillions.blogspot.com/2014/04/the-dml-model\\_21.html](http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html)

ATT&CK Matrix

The MITRE ATT&CK Matrix™ is an overview of the tactics and techniques described in the ATT&CK model. It visually aligns individual techniques under the tactics in which they can be applied. Some techniques span more than one tactic because they can be used for different purposes.

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Automated Exfiltration	Commonly Used Port
Appinit DLLs	Appinit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Connection Proxy
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	PowerShell	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Component Firmware	Exploitation of Vulnerability	DLL Injection	Input Capture	Network Service Scanning	Remote Desktop Protocol	Process Hollowing	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Obfuscation
Component Object Model Hijacking	Legitimate Credentials	DLL Search Order Hijacking	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Regsvcs/Regasm	Email Collection	Exfiltration Over Other Network Medium	Failback Channels
DLL Search Order Hijacking	Local Port Monitor	DLL Side-Loading	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Regsvr32	Input Capture	Exfiltration Over Physical Medium	Multi-Stage Channels
Hyervisor	New Service	Disabling Security Tools		Process Discovery	Replication Through Removable Media	Rundll32	Screen Capture	Scheduled Transfer	Multiband Communication

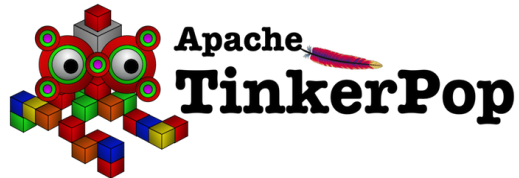
# Current OSINT Sources

- APTNotes
  - <https://github.com/aptnotes/data>
- APT & CyberCriminal Campaign Collection
  - [https://github.com/CyberMonitor/APT\\_CyberCriminal\\_Campagin\\_Collections](https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections)
- RSS Feeds
  - Infosec blogs
- mnemonic PassiveDNS
  - <https://passivedns.mnemonic.no/>
- Shadowserver IP-BGP
  - <https://www.shadowserver.org/wiki/pmwiki.php/Services/IP-BGP>
- VirusTotal
- MISP (circl.lu)



# THE ACT PLATFORM


# Platform Architecture – Core technologies




# Platform Architecture – Workflow orchestration

- Originally developed by NSA
- Open sourced and transferred to the Apache Foundation in 2014
- Manage flows of data supporting a large number of inputs and outputs:
  - HTTP, FTP, SCP, Kafka, Elasticsearch, JMS, Syslog, MongoDB, Hadoop, Cassandra, SMTP, POP3, etc



	<b>ControlRate</b> ControlRate 1.6.0 org.apache.nifi - nifi-standard-nar		
In	0 (0 bytes)	5	Name <b>success</b>
Read/Write	0 bytes / 0 bytes	5	Queued 0 (0 bytes)
Out	0 (0 bytes)	5 min	
Tasks/Time	0 / 00:00:00.000	5 min	

	<b>PDNSWorker</b> ExecuteStreamCommand 1.6.0 org.apache.nifi - nifi-standard-nar		
In	0 (0 bytes)	5 min	
Read/Write	0 bytes / 0 bytes	5 min	
Out	0 (0 bytes)	5 min	
Tasks/Time	0 / 00:00:00.000	5 min	



ATT&CK Worker

Shadowserver ASN

Virus Total Worker

Passive DNS Worker

SCIO Worker

Mitre ATT&CK

Shadowserver ASN

Object (type:value)	Fact (type:value)	Object (type:value)
report:acba9876aaaf6afc(...)	mentions:ipv4	ipv4:127.0.0.1
report:acba9876aaaf6afc(...)	mentions:threatActor	threatActor:APT29
report:acba0876aaaf6afc(...)	mentions:sector	sector:Financial
Object (type:value)	Fact (type:value)	Object (type:value)
ipv4:127.0.0.1	memberOf	ipv4Network.127.0.0.0/16
ipv4Network:127.0.0.0/16	memberOf	asn:60234
organization:Google	owns	asn:60234
content:aab678547865478abc (...)	connectsTo	uri:http://127.0.0.1

Enrichment

Add fact

Query

Action/triggers

Backend

REST API



Cassandra



elasticsearch

ACT Core

SCIO

SCIO Backend



# Platform Architecture – Graph database

- Looked into existing graph databases, but they lacked proper fine granular permissions (and many of them had commercial licenses that could not be used in the research project)
- Apache Tinkerpop implemented on top of Cassandra/Elasticsearch
- Graph queries opens up a range of possibilities that is not possible on a flat data structure



Query Type  
IPv4

Object class\*  
153.148.23.118

Graph query  
g.bohrE() otherV().bohrE().otherV().path

A Gremlin query like g.bohrE()

SEARCH CLEAR GRAPH

Merge previous

IPv4: 153.148.23.118  
g.bohrE() otherV().bohrE().otherV().path().limit

EXPORT RESOLVE FACTS

Layout   
euler

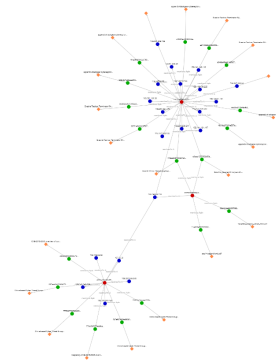
Layout options

Facts  
Display as nodes

Edges  
Show labels

Relationships  
Show related facts

Date  
Filter by time frame Any time

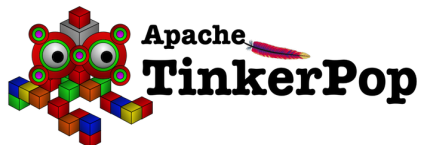


OBJECTS (4)		FACTS (4)	
Type	Value	Type	Value
fact	kuromeghen.myftp.org	fact	accounts.sanwifi.com
fact	accounts.sanwifi.com	fact	esemate.freestcp.com
ipv4	153.148.23.118	ipv4	153.148.19.105
ipv4	153.148.19.105	ipv4	153.148.100.225
ipv4	153.148.100.225	ipv4	153.148.101.147
ipv4	153.251.209.128	ipv4	153.251.209.128
ipv4	153.141.140.110	ipv4	153.147.96.30
ipv4	114.147.125.105	ipv4	114.147.125.105
ipv4	153.251.209.241	ipv4	153.251.209.241
ipv4	114.147.108.250	ipv4	114.147.108.250

Backend

REST API

GUI



ACT Core

# API - Swagger

experimental

Show/Hide | List Operations | Expand Operations

POST	/v1/fact	Create a new Fact.
GET	/v1/fact/uuid/{fact}/access	Retrieve a Fact's ACL.
POST	/v1/fact/uuid/{fact}/access/{subject}	Grant a Subject access to a Fact.
GET	/v1/fact/uuid/{fact}/comments	Retrieve a Fact's comments.
POST	/v1/fact/uuid/{fact}/comments	Add a comment to a Fact.
POST	/v1/fact/uuid/{fact}/retract	Retract an existing Fact.
GET	/v1/fact/uuid/{id}	Retrieve a Fact by its UUID.
POST	/v1/factType	Create a new FactType.
GET	/v1/factType	List available FactTypes.
PUT	/v1/factType/uuid/{id}	Update an existing FactType.
GET	/v1/factType/uuid/{id}	Retrieve a FactType by its UUID.
GET	/v1/object/{type}/{value}	Retrieve an Object by its type and value.
POST	/v1/object/{type}/{value}/facts	Retrieve Facts bound to a specific Object.
POST	/v1/object/{type}/{value}/traverse	Traverse the Object/Fact graph starting at an Object identified by its type and value.
POST	/v1/object/search	Search for Objects.
POST	/v1/object/traverse	Traverse the Object/Fact graph after performing an Object search.
GET	/v1/object/uuid/{id}	Retrieve an Object by its UUID.
POST	/v1/object/uuid/{id}/facts	Retrieve Facts bound to a specific Object.
POST	/v1/object/uuid/{id}/traverse	Traverse the Object/Fact graph starting at an Object identified by its UUID.
GET	/v1/objectType	List available ObjectTypes.
POST	/v1/objectType	Create a new ObjectType.

# API – Python library (act-api on pypi)

## Navigation

☰ Project description

🕒 Release history

📄 Download files

## Project links

🏠 Homepage

## Statistics

View statistics for this project via [Libraries.io](#), or by using [Google BigQuery](#)

## Meta

License: ISC License (ISCL) (MIT)

Author: [mnemonic AS](#)

📦 ACT, mnemonic

## Project description

### python-act

python-act is a library used to connect to the [ACT platform](#).

The platform has a REST api, and the goal of this library is to expose all functionality in the API.

## Objects and Facts

The act platform is built on two basic types, the object and fact.

Objects are universal elements that can be referenced uniquely by its value. An example of an object can be an IP address.

Facts are assertions or observations that ties objects together. A fact may or may not have a value describing further the fact.

Facts can be linked on or more objects. Below, the seenIn fact is linked to both an ipv4 object and report object, but the hasTitle fact is only linked to a report.

Object type	Object value	Fact type	Fact value	Object type	Object value
ipv4	127.0.0.1	seenIn	report	report	cbc80bb5c0c0f8944bf73(...)
report	cbc80bb5c0c0f8944bf73(...)	hasTitle	Threat Intel Summary	n/a	n/a



# Splunk Add-on - Queries

The screenshot shows the Splunk Search interface. At the top, the navigation bar includes 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main heading is 'New Search'. Below it, a search bar contains the query 'act apt29'. A status bar indicates '25 results (10/21/18 1:00:00.000 PM to 10/22/18 1:51:39.000 PM) No Event Sampling'. Below the search bar, there are tabs for 'Events (0)', 'Patterns', 'Statistics (25)', and 'Visualization'. The 'Statistics (25)' tab is active. Below the tabs, there are controls for '20 Per Page', 'Format', and 'Preview'. The main content is a table with the following columns: 'fact\_value', 'fact\_type', 'dest\_object\_type', and 'source\_object\_value'. The table contains 8 rows of data.

fact_value	fact_type	dest_object_type	source_object_value
-	usesTechnique	technique	APT29
-	threatActorAlias	threatActor	APT29
apt29-hammertoss-stealthy-tactics-define-a.pdf	hasTitle		eaae8f5a060599da627cee9cb5ad6704b91d6d323f189aac7fa24d4629ab054c
-	usesTool	tool	APT29
-	usesTechnique	technique	APT29
-	usesTool	tool	APT29
-	usesTechnique	technique	APT29
-	threatActorAlias	threatActor	APT29
-	usesTool	tool	APT29

# Splunk Add-on – Annotate search results

```
1 source="carbanak.csv" dest_ip=179.43.140.82 | acta dest_ip
2 | table dest_ip usesC2* seenIn*
```

✓ 3 events (before 10/22/18 2:27:42.000 PM) No Event Sampling ▾ Job ▾ || ■ ↶ ↷ ⬇ ⚙ Smart Mo

Events Patterns **Statistics (3)** Visualization

20 Per Page ▾ ↗ Format Preview ▾

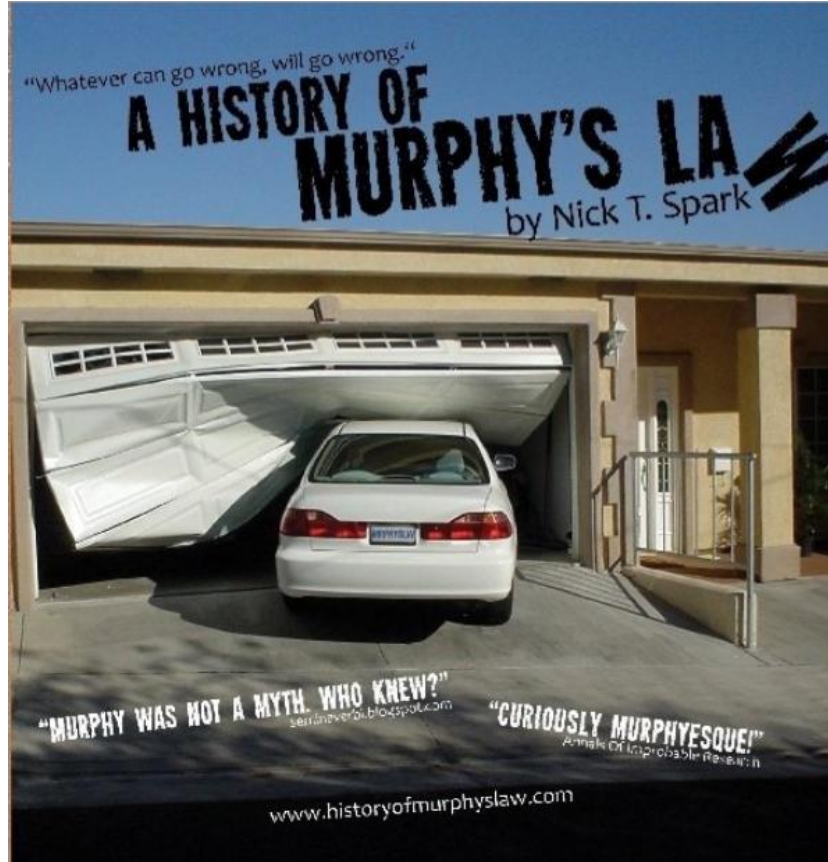
dest_ip ⇅ ↗	usesC2:ipV4 ⇅ ↗	seenIn:report ⇅
179.43.140.82	c6ec176592ea26c4ee27974273e592ff188f261e5fca94bd1fc1edc1aaf8c06e9408c338e98a8bc166a8d4f8264019	9c624e51ffab866aaa73c41f944f7ec6045ec6c04a99e24b37eadd518b74780c2d460cb6523158909dad07e6b0f9491339ce4ce1550f64832b0c5396c2f5bb8f
179.43.140.82	c6ec176592ea26c4ee27974273e592ff188f261e5fca94bd1fc1edc1aaf8c06e9408c338e98a8bc166a8d4f8264019	9c624e51ffab866aaa73c41f944f7ec6045ec6c04a99e24b37eadd518b74780c2d460cb6523158909dad07e6b0f9491339ce4ce1550f64832b0c5396c2f5bb8f
179.43.140.82	c6ec176592ea26c4ee27974273e592ff188f261e5fca94bd1fc1edc1aaf8c06e9408c338e98a8bc166a8d4f8264019	9c624e51ffab866aaa73c41f944f7ec6045ec6c04a99e24b37eadd518b74780c2d460cb6523158909dad07e6b0f9491339ce4ce1550f64832b0c5396c2f5bb8f

# Threat Intelligence Platform - Summary

- Implemented
  - Core platform
  - API
  - GUI
  - Workflow orchestration
  - Graph queries
- Github repositories
  - <https://github.com/mnemonic-no/act-api-python>
  - <https://github.com/mnemonic-no/act-bootstrap>
  - <https://github.com/mnemonic-no/act-frontend>
  - <https://github.com/mnemonic-no/act-platform>
  - <https://github.com/mnemonic-no/act-scio>
  - <https://github.com/mnemonic-no/act-splunk>
  - <https://github.com/mnemonic-no/act-triggers>
  - <https://github.com/mnemonic-no/act-workers>
  - License: ISC (BSD compatible)

# WORKSHOP - INTRODUCTION

# Before We Start



# | Accessing the GUI

- Read-only
- <https://act-eu1.mnemonic.no>
- <https://act-eu2.mnemonic.no>
  
- Tasks: /examples/
- API: /swagger/
- API-assignments: <https://github.com/mnemonic-no/act-workshop-api> (jupyter notebook you can test yourself if you are interested in testing the python API)

# Introduction 1

**ACT** The Open Threat Intelligence Platform EXAMPLES ABOUT

Object Type  
**hash**

Object value \*  
d06432486e7e9c2b8aaef4f42c11cf8e

Gremlin query  
A Gremlin query, like g outE()

SEARCH CLEAR GRAPH

Merge previous

hash:  
d06432486e7e9c2b8aaef4f42c11cf8ef1968

EXPORT RESOLVE FACTS

Layout  
**euler**

Layout options

Facts  
Display as nodes

Edges  
Show labels

Retractions  
Show retracted facts

Date  
Filter by max time **Any time**

```
graph TD; A((d06432486e7e9c2b...)) -- represents:vt --> B((d06432486e7e9c2b...)); B -- mentions:hash --> C((8b7cd7e79ad63671...)); C -- mentions:hash --> D((d06432486e7e9c2b8aaef4f42c11cf8ef1968));
```

"Sin"-ful SPIDERS: WIZARD SPID...

d06432486e7e9c2b8aaef4f42c11cf8ef1968

hash

3 facts  
mentions: 1  
represents: 2

CREATE FACT

OBJECTS (3)		FACTS (4)	
Type	Value	Type	Value
content	d06432486e7e9c2b8aaef4f42c11cf8ef1968	hash	d06432486e7e9c2b8aaef4f42c11cf8ef1968
hash	d06432486e7e9c2b8aaef4f42c11cf8ef1968	report	8b7cd7e79ad6367130f6ec39139f026fb6

# Introduction 1 – Right Click / Left Click

The screenshot displays the ACT (The Open Threat Intelligence Platform) interface. The top navigation bar includes the logo 'ACT' and the text 'The Open Threat Intelligence Platform', along with links for 'EXAMPLES' and 'ABOUT'.

The left sidebar contains several control panels:

- Object Type:** A dropdown menu set to 'hash'.
- Object value:** A text input field containing the hash 'd06432486e7e9c2b8aaef4f42c11cf8e'.
- Gremlin query:** A text input field with the query 'A Gremlin query, like g outE()' and buttons for 'SEARCH' and 'CLEAR GRAPH'.
- Merge previous:** A toggle switch currently turned on.
- EXPORT / RESOLVE FACTS:** Two buttons.
- Layout:** A dropdown menu set to 'euler'.
- Layout options:** A dropdown menu.
- Facts:** A toggle switch for 'Display as nodes'.
- Edges:** A toggle switch for 'Show labels'.
- Retractions:** A toggle switch for 'Show retracted facts'.
- Date:** A filter dropdown set to 'Any time'.

The central area shows a graph visualization with nodes and edges:

- A black node labeled 'd06432486e7e9c2b...' is connected to a teal node labeled 'd06432486e7e9c2b...' via an edge labeled 'represents:vt'.
- The teal node is connected to a green node labeled '8b7cd7e79ad63671...' via an edge labeled 'mentions:hash'.
- The green node is connected to an orange node labeled '"Sin"-ful SPIDERS: WIZARD SPID...' via an edge labeled 'represents:vt'.

The right sidebar displays details for the selected object:

- Object ID:** d06432486e7e9c2b8aaef4f42c11cf8e
- Type:** hash
- 3 facts:** mentions: 1, represents: 2
- CREATE FACT:** A button.
- OBJECTS (3) / FACTS (4):** A table listing related objects and facts.

Type	Value
content	d06432486e7e9c2b8aaef4f42c11cf8efe1
hash	d06432486e7e9c2b8aaef4f42c11cf8efe1
report	8b7cd7e79ad6367130f6ec39139f026fb6

At the bottom right of the graph area, there are three buttons: a zoom in button (with 'x' and 'x' symbols), a zoom out button (+), and a reset button (-).



# Introduction 1 – History, Layouts and Filtering

**ACT** The Open Threat Intelligence Platform

Object Type: hash  
Object value: d06432486e7e9c2b8aaef442c11cf8e

Gremlin query: A Gremlin query, like g.out(E)

SEARCH CLEAR GRAPH

Merge previous

hash: d06432486e7e9c2b8aaef442c11cf8ef1968  
content: d06432486e7e9c2b8aaef442c11cf8ef1968  
tool: trickbot

EXPORT RESOLVE FACTS

Layout: euler  
Layout options

Facts: Display as nodes  
Edges: Show labels

**trickbot**  
tool  
24 facts  
aliases: 2  
classifiedAs: 4  
implements: 18

CREATE FACT

OBJECTS (29)	FACTS (30)
Type ↑	Value
content	01e771dc6cf9572eac3d87120d7a7d1ff
content	d06432486e7e9c2b8aaef442c11cf8ef1968
content	046482ac16d538f1ab105669c8355cf6c
content	38155ede329f41fd733d2abaceb50644f
hash	d06432486e7e9c2b8aaef442c11cf8ef1968
report	8b7cd7e79ad6367139f6ec39139f026fb
technique	Standard Application Layer Protocol
technique	File and Directory Discovery
technique	Process Injection
technique	Remote File Copy
technique	System Information Discovery
technique	Man in the Browser
technique	Scheduled Task

# Introduction 1 – Fact Types

**ACT** The Open Threat Intelligence Platform

EXAMPLES ABOUT

Object Type  
hash

Object value \*  
d06432486e7e9c2b8aaef442c11cf8e

Gremlin query  
A Gremlin query, like g.out(E)

SEARCH CLEAR GRAPH

Merge previous

hash:  
d06432486e7e9c2b8aaef442c11cf8ef1968

content:  
d06432486e7e9c2b8aaef442c11cf8ef1968

tool: trickbot

EXPORT RESOLVE FACTS

Layout  
euler

Layout options

Facts  
Display as nodes

Edges  
Show labels

mansabo  
classifiedAs: vt  
d06432486e7e9c2b8aaef442c11cf8e  
mentions: flash  
8b7cd7e79ad6367139f6ec39139f026fb  
"Sir"-ful SPIDERS: WIZARD SPID...

trickbot  
tool  
24 facts  
aliases: 2  
classifiedAs: 4  
implements: 18

CREATE FACT

OBJECTS (29)	FACTS (30)
Type ↑	Value
content	01e771dc6cf9572eac3d87120d7a7d1ff
content	d06432486e7e9c2b8aaef442c11cf8ef1968
content	046482ac16d538f1ab105669c8355cf6c
content	38155ede329f41fd733d2abaceb50644f
hash	d06432486e7e9c2b8aaef442c11cf8ef1968
report	8b7cd7e79ad6367139f6ec39139f026fb
technique	Standard Application Layer Protocol
technique	File and Directory Discovery
technique	Process Injection
technique	Remote File Copy
technique	System Information Discovery
technique	Man in the Browser
technique	Scheduled Task

Navigation icons: back, forward, search, zoom in (+), zoom out (-)

## Introduction 2

Try the following object queries and explore the graph:

- threatActor: APT3
- tactic: lateral-movement
- tool: foosace
- ipv4: 153.148.23[.]118

## Task 1

Try the following object query:

- tool: remsec

Which threat actor is associated with this tool?

Which techniques are associated with this threat actor?

Can you find any reports that mention file hashes classified as remsec?

## Task 2: Find the Report

<https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/>

## Task 3

Explore Autonomous System Number 8048

- asn: 8048

What kind of malicious behaviour has been observed from this AS?

Where is the organization that owns AS8048 located?

# Introduction 3 – Graph Query

**ACT** The Open Threat Intelligence Platform

EXAMPLES ABOUT

Object Type  
asn

Object value \*  
8048

Gremlin query  
`g.repeat(inE('memberOf').otherV()).time`  
A Gremlin query, like g.outE()

SEARCH CLEAR GRAPH

Merge previous

asn: 8048  
`g.repeat(inE('memberOf').otherV()).times(2).in`

EXPORT RESOLVE FACTS

Layout  
euler

Layout options

Facts  
Display as nodes

Edges  
Show labels

Retractions  
Show retracted facts

OBJECTS (74) FACTS (110)

Type ↑	Value
asn	8048
ipv4	200.11.218.76
ipv4	201.249.146.59
ipv4	201.242.221.32
ipv4	201.242.207.137
ipv4	190.72.31.95
ipv4	190.37.228.226
ipv4	201.211.183.215
ipv4	190.201.6.106
ipv4	190.203.23.178
ipv4	190.37.208.9

# Introduction 3 – Graph Query

The screenshot displays the ACT (The Open Threat Intelligence Platform) interface. The main area shows a complex graph visualization with nodes and edges. The left sidebar contains controls for the query and graph display. The right sidebar shows a table of results.

**Object Type:** asn  
**Object value \*:** 8048  
**Gremlin query:** `g.repeat(inE('memberOf').otherV()).time`  
**SEARCH** **CLEAR GRAPH**

**Merge previous:**   
**asn: 8048**  
`g.repeat(inE('memberOf').otherV()).times(2).in`  
**EXPORT** **RESOLVE FACTS**

**Layout:** euler  
**Layout options:**

**Facts:**  Display as nodes  
**Edges:**  Show labels  
**Retractions:**  Show retracted facts

**OBJECTS (74)** **FACTS (110)**

Type ↑	Value
asn	8048
ipv4	200.11.218.76
ipv4	201.249.146.59
ipv4	201.242.221.32
ipv4	201.242.207.137
ipv4	190.72.31.95
ipv4	190.37.228.226
ipv4	201.211.183.215
ipv4	190.201.6.106
ipv4	190.203.23.178
ipv4	190.37.208.9

Try to replace 'mentions' with 'resolvesTo' in the graph query (you can edit the URL).



# Introduction 4 – Extended Graph Query

**ACT** The Open Threat Intelligence Platform EXAMPLES ABOUT

Object Type  
**country**

Object value\*  
Venezuela (Bolivarian Republic of)

Gremlin query  
`g.inE('locatedIn').otherV().hasLabel('org')`  
A Gremlin query, like `g.outE()`

SEARCH CLEAR GRAPH

Merge previous

country: Venezuela (Bolivarian Republic of)  
g.inE('locatedIn').otherV().hasLabel('organiza

EXPORT RESOLVE FACTS

Layout  
**euler**

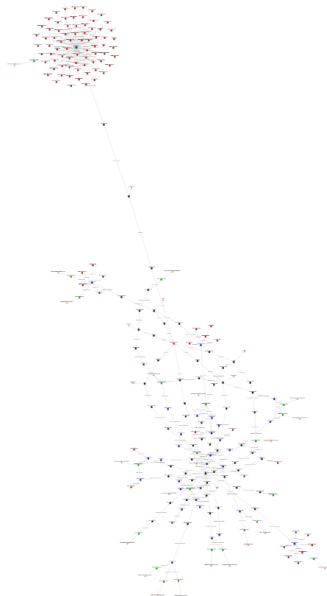
Layout options

Facts  
Display as nodes

Edges  
Show labels

Retractions  
Show retracted facts

Date



OBJECTS (212)      FACTS (267)

Type	Value
asn	27717
asn	8053
asn	11694
asn	21826
asn	28007
asn	6306
asn	8048
country	Venezuela (Bolivarian Republic of)
fqdn	ugsiep.funindes.usb.ve
fqdn	www.ts.usb.ve
fqdn	labidiomasaiac.usb.ve
fqdn	www.espeleo.grupos.usb.ve
fqdn	www.formulasae.grupos.usb.ve

# WORKSHOP – GRAPH QUERIES

With Great Power Comes Great Responsibility

# Graph Query 1

**ACT** The Open Threat Intelligence Platform EXAMPLES ABOUT

Object Type: **ipv4**  
Object value\*: **153.148.23.118**  
Gremlin query: **g.bothE().otherV()**  
A Gremlin query, like g.outE()  
SEARCH CLEAR GRAPH

Merge previous   
ipv4: 153.148.23.118  
g.bothE().otherV()  
EXPORT RESOLVE FACTS

Layout: **euler**  
Layout options: ▾

Facts:  Display as nodes  
Edges:  Show labels  
Retractions:  Show retracted facts  
Date: Filter by max time: **Any time** ▾

accounts.serveft...  
eemete.freetcp.c...  
153.148.23.118  
liumingzhen.myft...

OBJECTS (4)    FACTS (0)

Type ↑	Value
fqdn	accounts.serveft.com
fqdn	eemete.freetcp.com
fqdn	liumingzhen.myftp.org
ipv4	153.148.23.118

# Graph Query 2 – Show Edges

**ACT** The Open Threat Intelligence Platform EXAMPLES ABOUT

Object Type  
**ipv4**

Object value \*  
153.148.23.118

Gremlin query  
`g.bothE().otherV().path().unfold()`  
A Gremlin query, like g.outE()

SEARCH CLEAR GRAPH

Merge previous

ipv4: 153.148.23.118  
`g.bothE().otherV().path().unfold()`

EXPORT RESOLVE FACTS

Layout  
**euler**

Layout options

Facts  
Display as nodes

Edges  
Show labels

Retractions  
Show retracted facts

Date  
Filter by max time **Any time**

```
graph TD; A((liumingzhen.myft...)) -- resolvesTo: A --> B((153.148.23.118)); C((accounts.serveft...)) -- resolvesTo: A --> B; D((eemete.freetcp.c...)) -- resolvesTo: A --> B;
```

OBJECTS (4)    FACTS (3)

Type ↑	Value
fqdn	accounts.serveftp.com
fqdn	eemete.freetcp.com
fqdn	liumingzhen.myftp.org
ipv4	153.148.23.118

Navigation:

# Graph Query 3 – 2 hops

**ACT** The Open Threat Intelligence Platform EXAMPLES ABOUT

Object Type  
ipv4

Object value \*  
153.148.23.118

Gremlin query  
`g.bothE().otherV().bothE().otherV().path()`  
A Gremlin query, like g.outE()

SEARCH CLEAR GRAPH

Merge previous

ipv4: 153.148.23.118  
`g.bothE().otherV().bothE().otherV().path().unf`

EXPORT RESOLVE FACTS

Layout  
euler

Layout options

Facts  
Display as nodes

Edges  
Show labels

Retractions  
Show retracted facts

Date  
Filter by max time Any time

**OBJECTS (42)** **FACTS (64)**

Type ↑	Value
fqdn	liumingzhen.myftp.org
fqdn	accounts.servftp.com
fqdn	eemete.freetcp.com
ipv4	153.148.23.118
ipv4	153.148.19.155
ipv4	153.148.108.225
ipv4	153.141.131.147
ipv4	153.251.208.128
ipv4	153.141.140.110
ipv4	114.147.96.30
ipv4	114.147.125.105
ipv4	153.251.209.241
ipv4	114.147.108.250

# Graph Query 4 – Filter Edges (Facts)

**ACT** The Open Threat Intelligence Platform EXAMPLES ABOUT

Object Type  
**ipv4**

Object value \*  
153.148.23.118

Gremlin query  
g.bothE().otherV().bothE(resolvesTo).o  
A Gremlin query, like g.outE()

SEARCH CLEAR GRAPH

Merge previous

ipv4: 153.148.23.118  
g.bothE().otherV().bothE(resolvesTo).otherV()

EXPORT RESOLVE FACTS

Layout  
**euler**

Layout options

Facts  
Display as nodes

Edges  
Show labels

Retractions  
Show retracted facts

Date  
Filter by max time **Any time**

**OBJECTS (23)** **FACTS (24)**

Type ↑	Value
fqdn	accounts.servftp.com
fqdn	eemete.freetc.com
fqdn	liumingzhen.myftp.org
ipv4	153.148.23.118
ipv4	153.251.246.245
ipv4	153.251.250.140
ipv4	153.148.63.58
ipv4	127.0.0.3
ipv4	153.141.140.208
ipv4	153.141.131.147
ipv4	123.51.208.69
ipv4	153.148.108.225
ipv4	153.251.252.64
ipv4	153.251.250.140

# Graph Query 5 – Filter Nodes (Objects)

The screenshot displays the ACT (The Open Threat Intelligence Platform) interface. The top navigation bar includes the logo 'ACT' and the text 'The Open Threat Intelligence Platform' on the left, and 'EXAMPLES ABOUT' on the right.

The main interface is divided into several sections:

- Object Type:** A dropdown menu set to 'ipv4'.
- Object value \*:** A text input field containing '153.148.23.118'.
- Gremlin query:** A text area containing the query `g.bothE().otherV().bothE().otherV().hasLabel('')`. Below it, a note reads: 'A Gremlin query, like g.outE()'. Buttons for 'SEARCH' and 'CLEAR GRAPH' are present.
- Merge previous:** A toggle switch that is currently turned on.
- EXPORT RESOLVE FACTS:** Two buttons.
- Layout:** A dropdown menu set to 'euler'. Below it, a 'Layout options' dropdown is visible.
- Facts:** A section with a 'Display as nodes' toggle switch turned on.
- Edges:** A section with a 'Show labels' toggle switch turned on.
- Retractions:** A section with a 'Show retracted facts' toggle switch turned on.
- Date:** A section with a 'Filter by max time' dropdown menu set to 'Any time'.

The central part of the interface shows a complex graph visualization with nodes and edges. The nodes are color-coded (green, orange, red, blue) and connected by lines representing relationships. A central node is highlighted in blue.

On the right side, there is a table showing the results of the query:

OBJECTS (23)		FACTS (43)	
Type ↑	Value	Type ↑	Value
fqdn	eemete.freetchp.com		
fqdn	accounts.servftp.com		
fqdn	liumingzhen.myftp.org		
ipv4	153.148.23.118		
report	03c464ee9620f082eace3618259493edb		
report	c9cac1307952b59b0bd79bc5608e97d07		
report	478ea2d9700237a0c6780ac2932b75f6b		
report	11460e45ee525dec7a1b03de04a3e238c		
report	fb7e907e00e806f34bbba9dd4ece9fd20		
report	776e56f3774edfca2b13baace3dbd87f15		
report	4d342b894d836c1eb3f22528a07295791		
report	f7f523f78353ea0b999c30c8c72019b048		
report	887adc5c8745d37fab0be0158078f48dd7		

# Task 4 - Subgraph

**ACT** The Open Threat Intelligence Platform

EXAMPLES ABOUT

Object Type  
hash

Object value\*  
be2fedfb27d0b1169ee1d3faf3b75c3

Gremlin query  
A Gremlin query, like g.out(E)

SEARCH CLEAR GRAPH

Merge previous

hash: be2fedfb27d0b1169ee1d3faf3b75c381f925  
content: add64bf4934ca7a0a1f68b97b5af0057e254a  
uri: http://www.example.com  
uri: dns://ns1.example.com  
uri: http://mail.example.com

EXPORT RESOLVE FACTS

Layout  
euler

Layout options

Facts  
Display as nodes

Edges  
Show labels

Retractions  
Show retracted facts

be2fedfb27d0b1169ee1d3faf3b75c3  
hash  
1 facts  
represents: 1

CREATE FACT

Type	Value
content	add64bf4934ca7a0a1f68b97b5af0057e254a
fqdn	mail.example.com
fqdn	ns1.example.com
fqdn	www.example.com
hash	cf15017f37cb61e599dccc276296a3fe9
hash	be2fedfb27d0b1169ee1d3faf3b75c381
hash	add64bf4934ca7a0a1f68b97b5af0057e254a
uri	http://mail.example.com
uri	dns://ns1.example.com
uri	http://www.example.com

OBJECTS (10)    FACTS (12)

⌕ ⌕ ⌕  
+  
-



| hash → content → uri with port number 1337 ← fqdn

**ACT** The Open Threat Intelligence Platform

EXAMPLES ABOUT

Object Type  
hash

Object value \*  
be2fdedfb27d0b1169ee1d3faf3b75c3

Gremlin query  
g.outE(relationship).otherV().outE(relationship).otherV()  
A Gremlin query, like g.outE()

SEARCH CLEAR GRAPH

Merge previous

hash:  
be2fdedfb27d0b1169ee1d3faf3b75c381f32e  
g.outE(relationship).otherV().outE(relationship).otherV()

EXPORT RESOLVE FACTS

Layout  
euler

Layout options

Facts  
Display as nodes

Edges  
Show labels

Retractions  
Show retracted facts

Date  
Filter by max time Any time

Filter objects  
 hash  
 content

```
graph TD; A((be2fdedfb27d0b11...)) -- represents: --> B((add64bf4934ca7a0...)); B -- connectsTo: --> C((http://mail.exam...)); C -- componentOf: --> D((mail.example.com)); D --- E{1337}
```

OBJECTS (4)    FACTS (4)

Type ↑	Value
content	a0d540f4934ca7a0a1f08b97b5af0057e...
fqdn	mail.example.com
hash	be2fdedfb27d0b1169ee1d3faf3b75c381...
uri	http://mail.example.com

xx  
x x

+

-

`g.outE('represents').otherV().outE('connectsTo').otherV().where(outE().has('value','1337')).inE('componentOf').otherV().path().unfold()`

The screenshot displays the ACT interface with a graph visualization and a table of results. The graph shows a path of relationships between nodes: a teal node (hash) represents a black node (hash), which connects to a green node (uri), which is a component of a red node (uri). The green node also connects to a red node (uri). The red node is labeled '1337'.

The table on the right shows the results of the query, with 4 objects and 4 facts. The table has columns for Type and Value.

Type	Value
content	a00540f4934ca7a0a1f08b97b5af0057e...
fqdn	mail.example.com
hash	be2f0edfb27d0b1169ee1d3faf3b75c381
uri	http://mail.example.com

```
g.outE('represents').otherV().outE('connectsTo').otherV().  
not(where(outE().has('value','1337'))).inE('componentOf').otherV().path().unfold()
```

The screenshot shows the ACT interface with a graph visualization and a results table. The graph shows nodes representing various entities and their relationships. The nodes are: a red circle for 'www.example.com', a green circle for 'http://www.examp...', a black circle for 'add64bf4934ca7a0...', a green circle for 'dns://ns1.exampl...', a red circle for 'ns1.example.com', a teal circle for 'be2fdefb27d0b11...', and an orange diamond for '80'. Edges connect these nodes with labels: 'represents:', 'connectsTo:', and 'componentOf:'. The results table on the right shows 4 objects and 7 facts.

Type	Value
content	a0d540f4934ca7a0a1f08b97b5af0057e...
fqdn	ns1.example.com
fqdn	www.example.com
hash	be2fdefb27d0b1169ee1d3faf3b75c381
uri	dns://ns1.example.com
uri	http://www.example.com

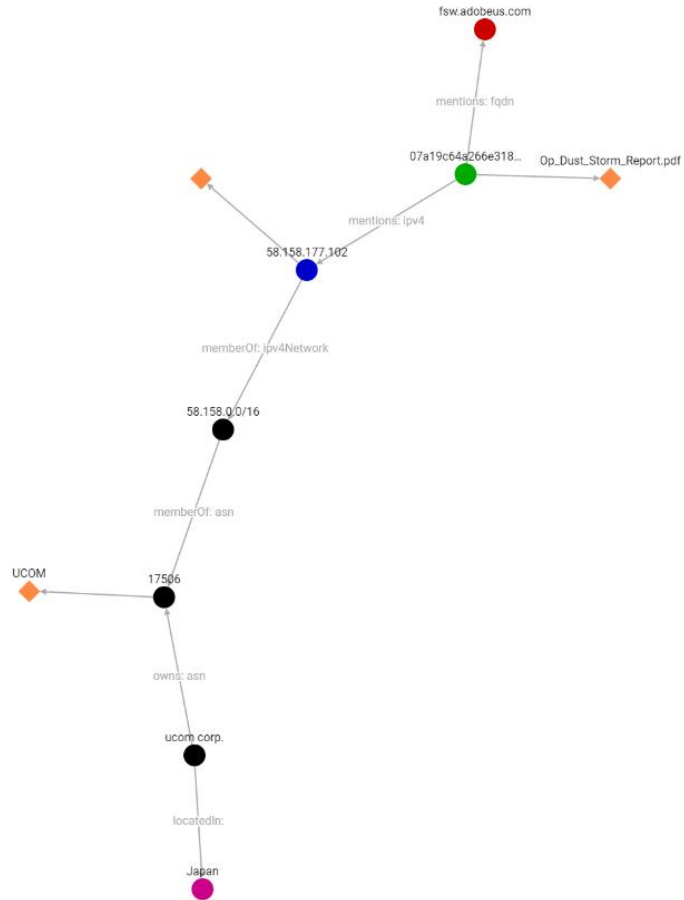
not(where()), not where(not())

## Task 5: Find the IP Address Owner

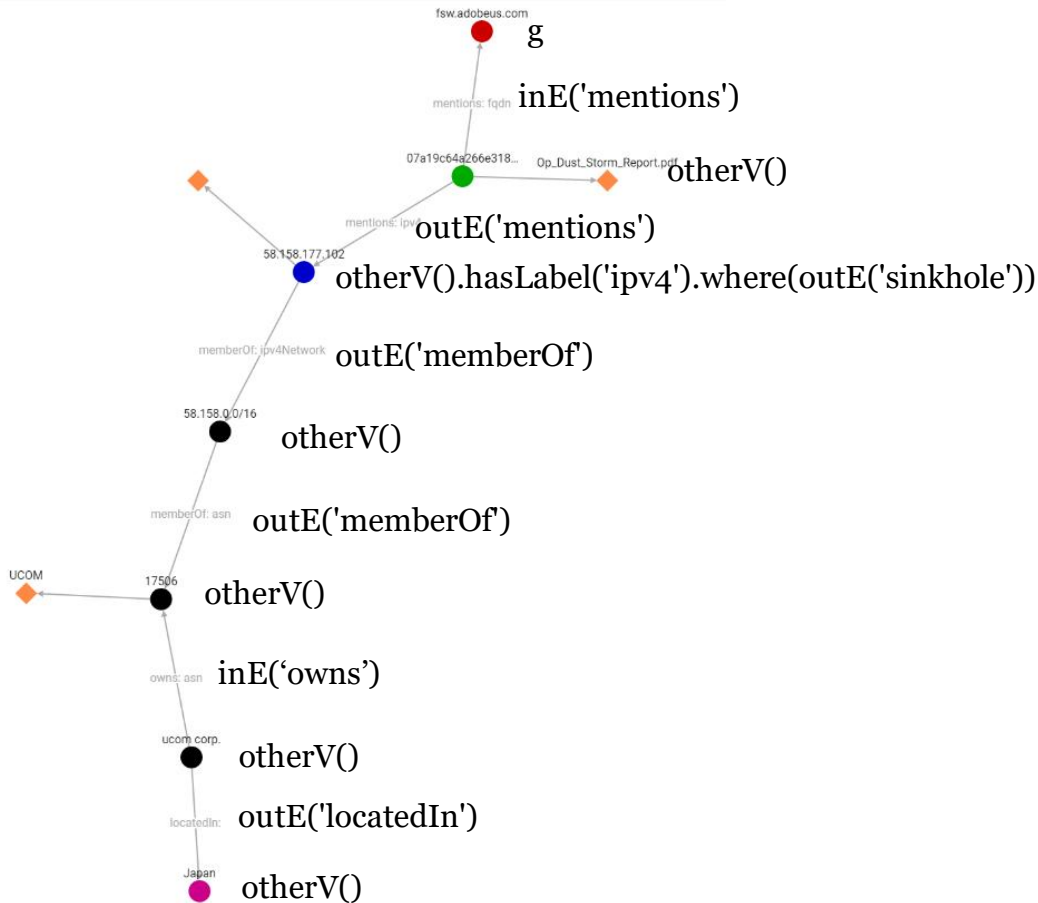
The fqdn fsw.adobeus[.]com is mentioned in one report. A sinkhole IPv4 address is also mentioned in the same report. Which organization owns that sinkhole IPv4 address, and which country is it located in?

Hint: Fact Type 'mentions' and 'memberOf'

# Task 5 Solution



```
g.inE('mentions').otherV().outE('mentions').otherV().hasLabel('ipv4').where(outE('sinkhole')).outE('memberOf').otherV().outE('memberOf').otherV().inE('owns').otherV().outE('locatedIn').otherV().path().unfold()
```



# Graph Query 6 – Unique Tool Usage

**ACT** The Open Threat Intelligence Platform EXAMPLES ABOUT

Object Type  
threatActor

Object value \*  
APT3

Gremlin query  
g.as(startNode).inE(attributedTo).other

A Gremlin query, like g.outE()

SEARCH CLEAR GRAPH

Merge previous

threatActor: APT3  
g.as(startNode).inE(attributedTo).otherV().ir

EXPORT RESOLVE FACTS

Layout  
euler

Layout options

Facts  
Display as nodes

Edges  
Show labels

Retractions  
Show retracted facts

Date  
Filter by max time Any time

```
graph TD; APT3((APT3)) -- attributedTo --> I1((<incident>)); I1 -- observedIn: incident --> C1((<content>)); C1 -- classifiedAs --> S(sctasks); S -- classifiedAs --> C2((<content>)); C2 -- observedIn: incident --> I2((<incident>)); I2 -- attributedTo --> BRONZE BUTLER((BRONZE BUTLER));
```

OBJECTS (7)

Type ↑	Value
content	<content>
content	<content>
incident	<incident>
incident	<incident>
threatActor	APT3
threatActor	BRONZE BUTLER
tool	sctasks

FACTS (6)

# ASSIGNMENTS



# CASE STUDY

---

## Public Read-Only ACT Instance

<https://act-eu1.mnemonic.no/examples/>

# FURTHER WORK

# | New Information Sources

- Security alerts
- Incidents
- Reputation lists
- Malware analysis systems
- STIX feeds
- ...

# | Graph Analytics

- Post. doc. @ UiO
- Post. doc. @ NTNU

# Information Sharing

- Mechanism for sharing schema
- Format (STIX?)
- Trust models

# | Trust and Confidence

- Trust (source)
- Confidence (fact)
- Subjective Logic (quantify uncertainty)

# GUI Improvements

- Context menu
  - Pre-defined graph queries
  - Download report
  - ...
- Timelines
- Share workspace
- Prune graph



