SEMI-AUTOMATED CYBER THREAT INTELLIGENCE (ACT)

Workshop – FIRST Conference 2018

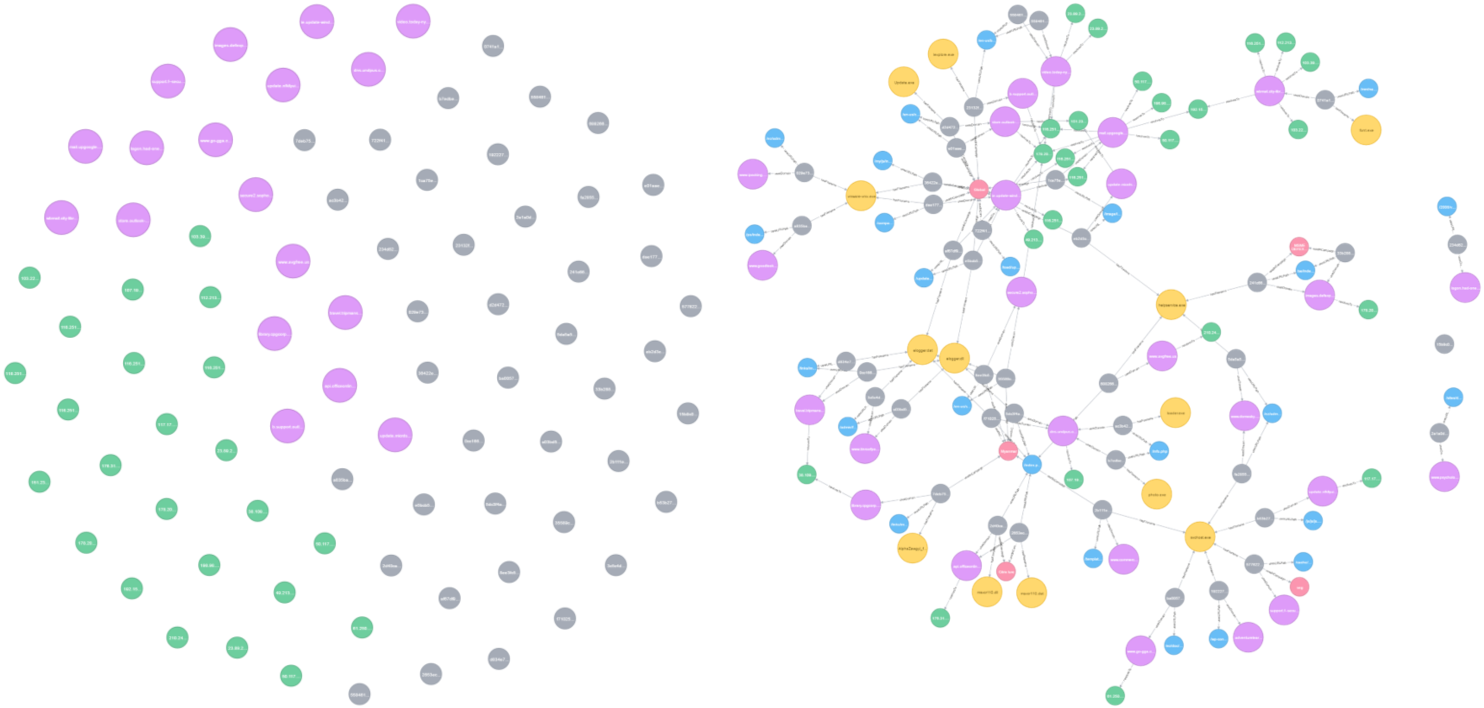
Martin Eian and Fredrik Borg

mnemonic

Goal

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

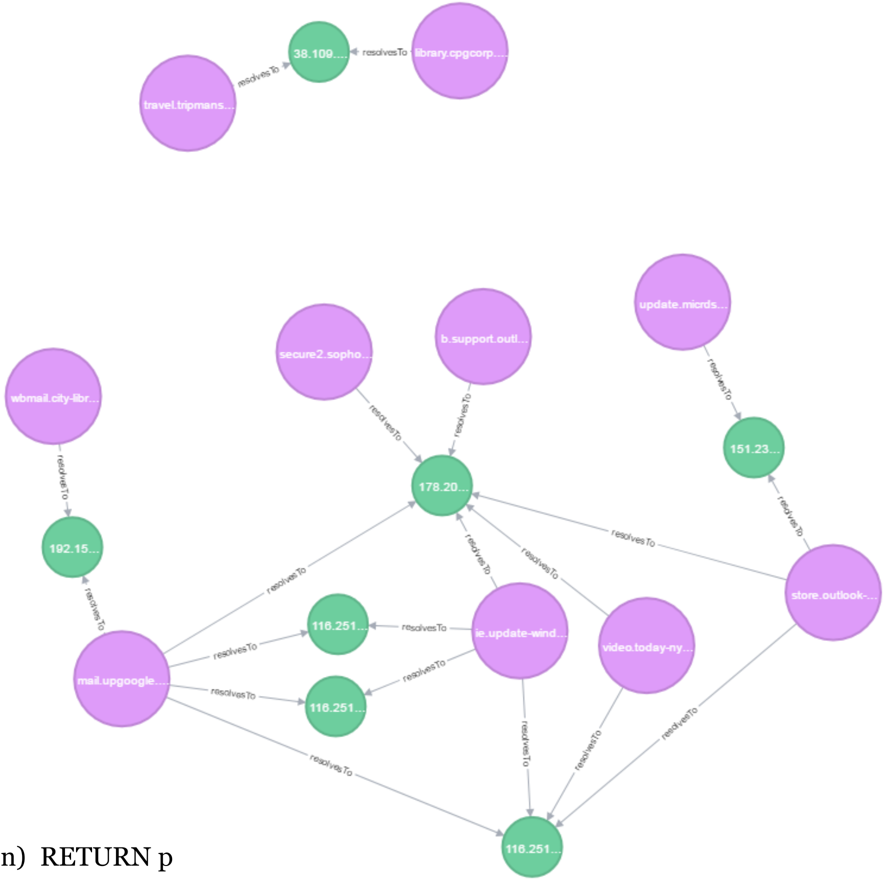
Data and Information



Legend

- ● Sample Hash
- ● Domain
- ● Filename
- ● Path
- ● Campaign
- ● IP Address

Knowledge



```
MATCH p=(n:Domain)-->(o:IP)<--(m:Domain)  RETURN p
```

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.

NSM

Nordic Financial CERT

Kraft CERT

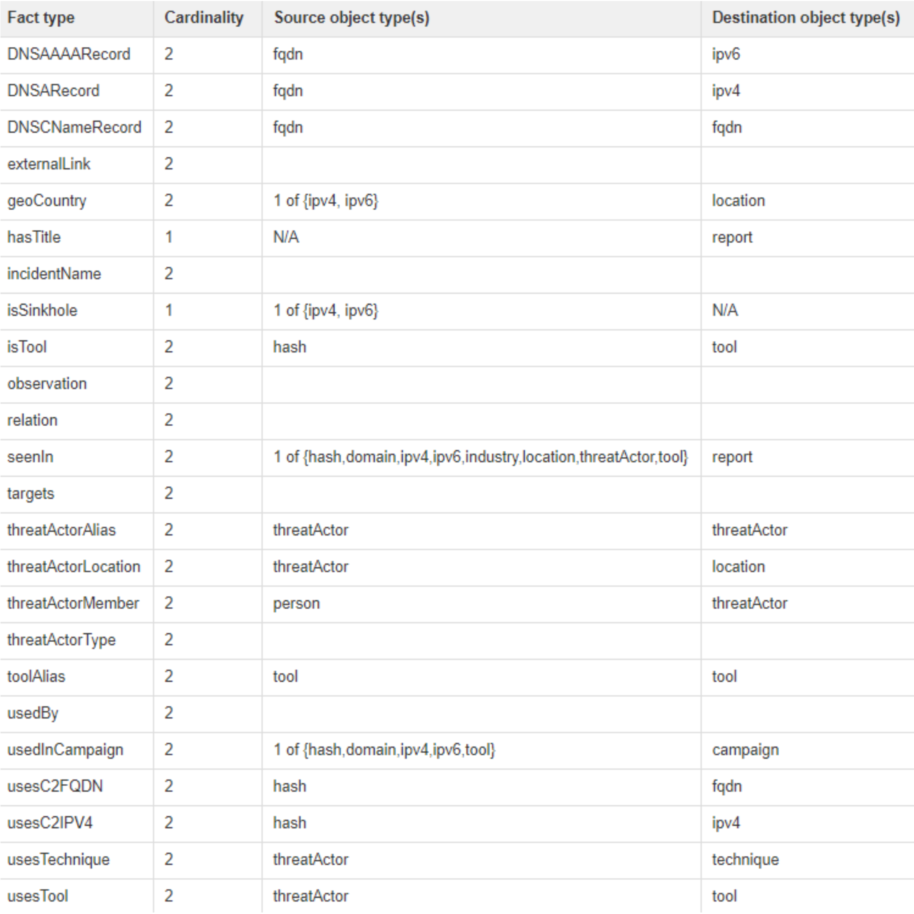
UiO Universitetet i Oslo

NTNU Norwegian University of Science and Technology

mnemonic

Data Model

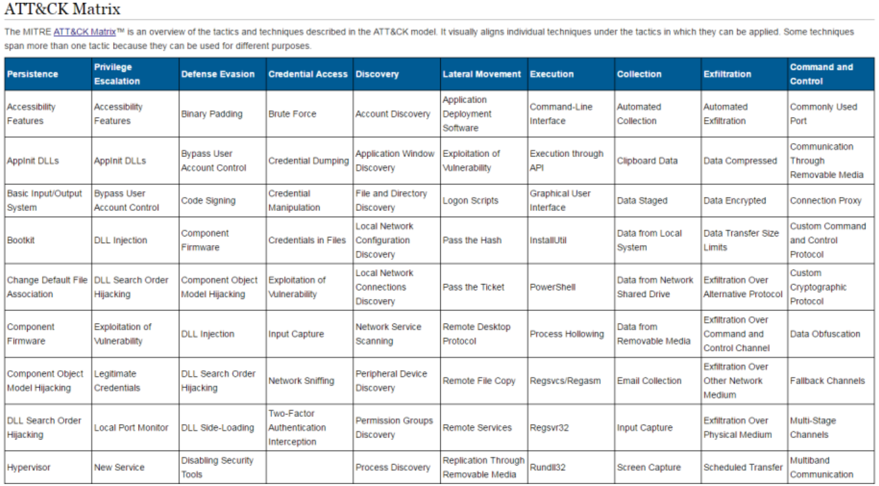
- Objects
  - Global
  - Example: IP address
- Facts
  - Connected to a single object or multiple objects
  - Immutable
  - Timestamped
  - Owner
  - Role-based and explicit access control
  - Backed by evidence and comments



Fact type	Cardinality	Source object type(s)	Destination object type(s)
DNSAAAARecord	2	fqdn	ipv6
DNSARecord	2	fqdn	ipv4
DNSCNameRecord	2	fqdn	fqdn
externalLink	2		
geoCountry	2	1 of {ipv4, ipv6}	location
hasTitle	1	N/A	report
incidentName	2		
isSinkhole	1	1 of {ipv4, ipv6}	N/A
isTool	2	hash	tool
observation	2		
relation	2		
seenIn	2	1 of {hash,domain,ipv4,ipv6,industry,location,threatActor,tool}	report
targets	2		
threatActorAlias	2	threatActor	threatActor
threatActorLocation	2	threatActor	location
threatActorMember	2	person	threatActor
threatActorType	2		
toolAlias	2	tool	tool
usedBy	2		
usedInCampaign	2	1 of {hash,domain,ipv4,ipv6,tool}	campaign
usesC2FQDN	2	hash	fqdn
usesC2IPV4	2	hash	ipv4
usesTechnique	2	threatActor	technique
usesTool	2	threatActor	tool

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



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.

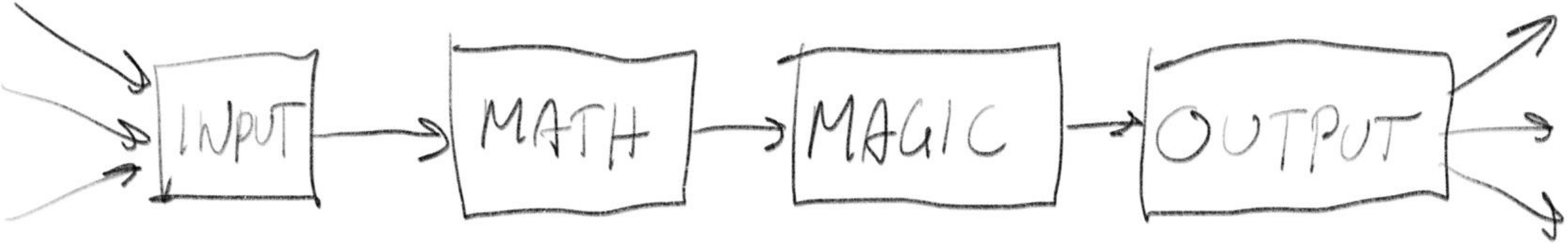
Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Automated 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	Fallback 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
Hypervisor	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
- RSS Feeds
  - Infosec blogs
- mnemonic PassiveDNS
  - https://passivedns.mnemonic.no/
- VirusTotal

THE ACT PLATFORM

Platform Architecture Version 0.01



Platform Architecture – Core technologies

Cassandra

elasticsearch

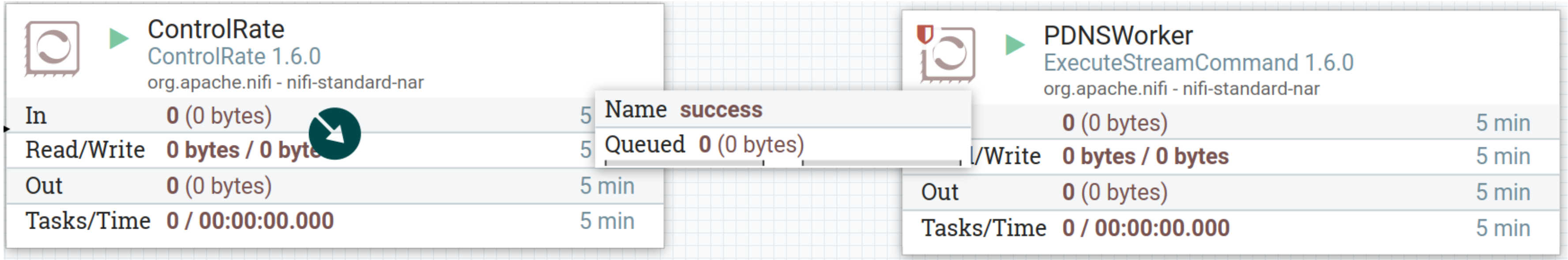
Apache TinkerPop

APACHE nifi

OPEN NLP™

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



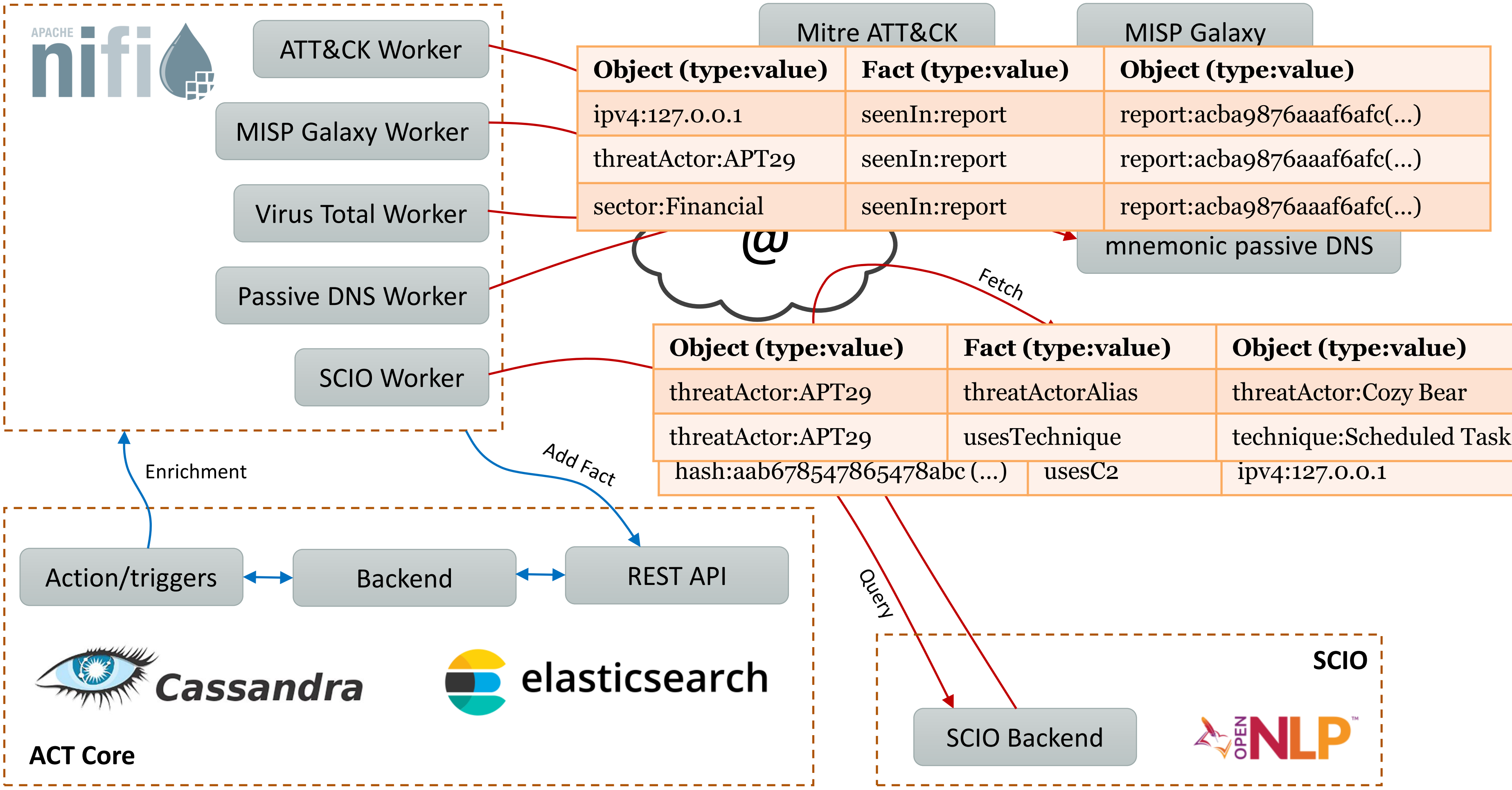
ControlRate
ControlRate 1.6.0
org.apache.nifi - nifi-standard-nar

In	**0** (0 bytes)	5
Read/Write	**0 bytes / 0 byte**	5
Out	**0** (0 bytes)	5 min
Tasks/Time	**0 / 00:00:00.000**	5 min

Name **success**
Queued **0** (0 bytes)

PDNSWorker
ExecuteStreamCommand 1.6.0
org.apache.nifi - nifi-standard-nar

	0 (0 bytes)	5 min
/Write	**0 bytes / 0 bytes**	5 min
Out	**0** (0 bytes)	5 min
Tasks/Time	**0 / 00:00:00.000**	5 min



Object (type:value)	Fact (type:value)	Object (type:value)
ipv4:127.0.0.1	seenIn:report	report:acba9876aaaf6afc(...)
threatActor:APT29	seenIn:report	report:acba9876aaaf6afc(...)
sector:Financial	seenIn:report	report:acba9876aaaf6afc(...)

Object (type:value)	Fact (type:value)	Object (type:value)
threatActor:APT29	threatActorAlias	threatActor:Cozy Bear
threatActor:APT29	usesTechnique	technique:Scheduled Task
hash:aab678547865478abc (...)	usesC2	ipv4:127.0.0.1

Platform Architecture – Graph database

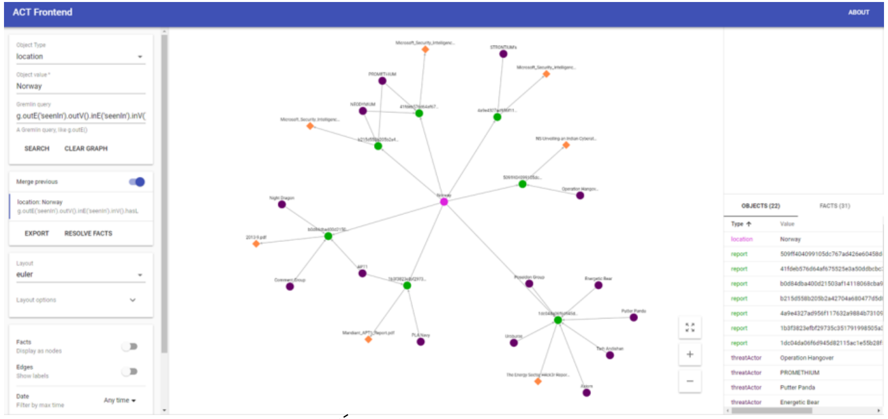
- Looked into existing graph databases, but they lacked proper fine granular permissions (and many of them had commercial licenses that could not be used in the research project)

- Apache Tinkerpop implemented on top of Cassandra/Elasticsearch

- Graph queries opens up a range of possibilites that is not possible on a flat data structure

Apache TinkerPop

Gremlin
$G = (V, E)$



ACT Frontend

Object Type: location

Object value *: Norway

Gremlin query: g.outE('seenIn').outV().inE('seenIn').inV(

A Gremlin query, like g.outE()

Merge previous

location: Norway
g.outE('seenIn').outV().inE('seenIn').inV().hasL

Layout: euler

Layout options

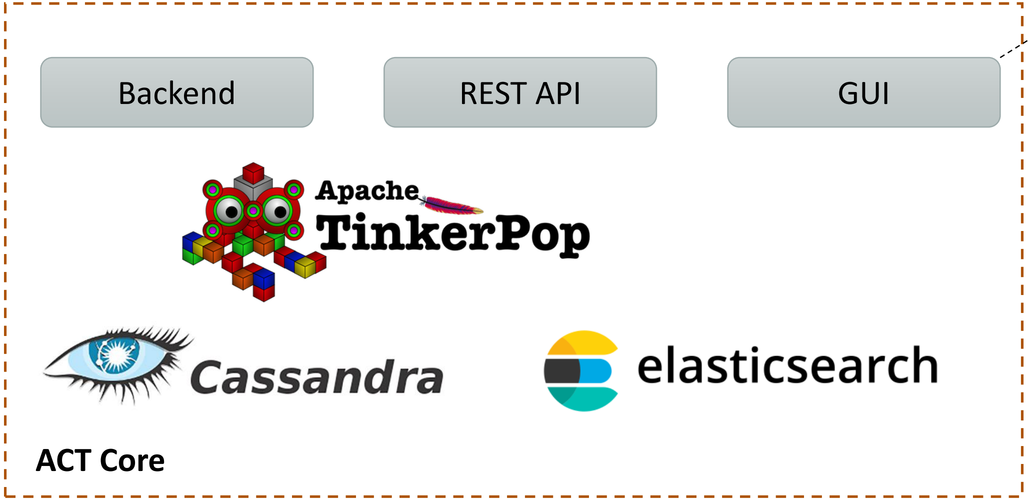
Facts
Display as nodes

Edges
Show labels

Date
Filter by max time
Any time

OBJECTS (22) | FACTS (31)

Type ↑	Value
location	Norway
report	509ff404099105dc767ad426e60458d
report	41fdeb576d64af67552 5e3a50ddbcbc
report	b0d84dba400d21503af14118068cba9
report	b215d558b205b2a42704a680477d5d
report	4a9e4327ad956f117632a9884b73109
report	1b3f3823efbf29735c351791998505a
report	1dc04da06f6d945d82115ac1e55b28f
threatActor	Operation Hangover
threatActor	PROMETHIUM
threatActor	Putter Panda
threatActor	Energetic Bear



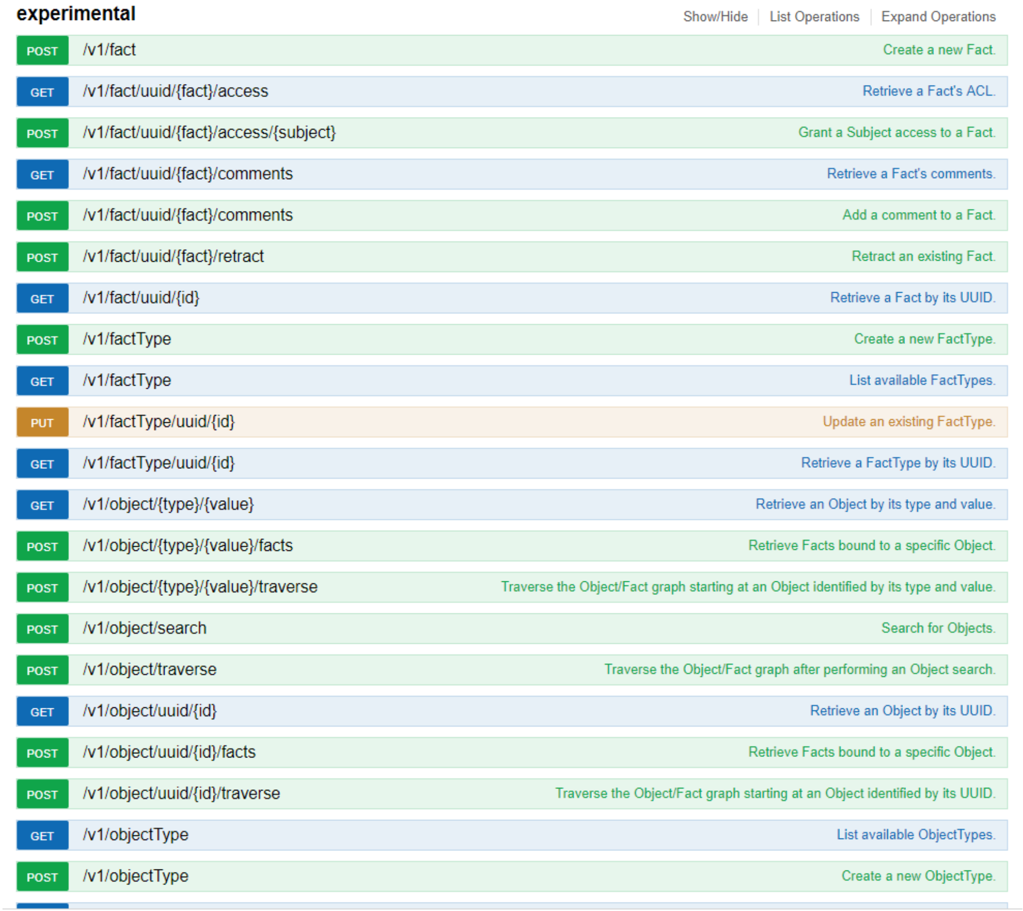
Backend

REST API

GUI

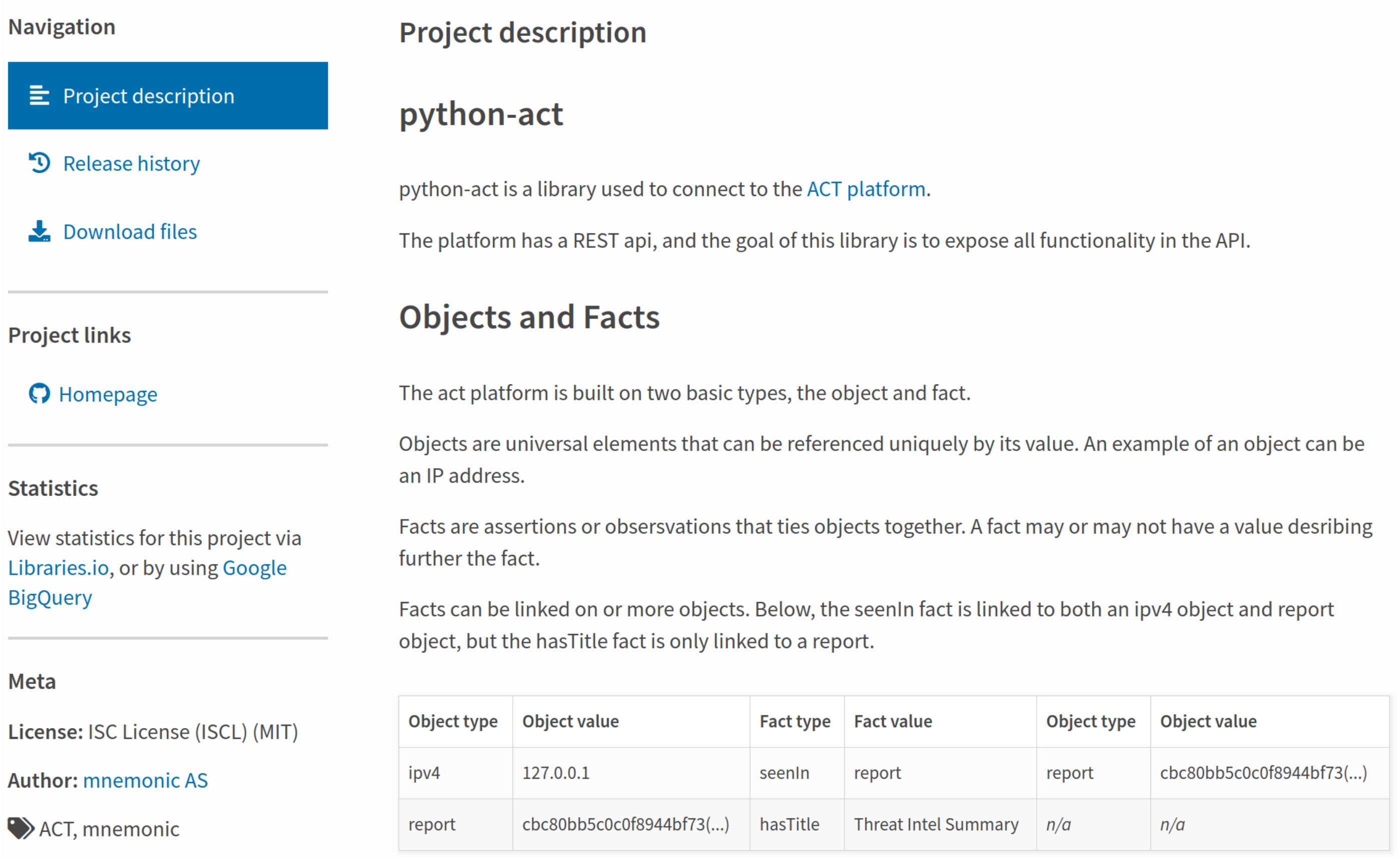
ACT Core

API - Swagger



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 obsersvations that ties objects together. A fact may or may not have a value desribing 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*

Threat Intelligence Platform - Summary

- Implemented
  - Core platform
  - API
  - GUI
  - Workflow orchestration
  - Graph queries

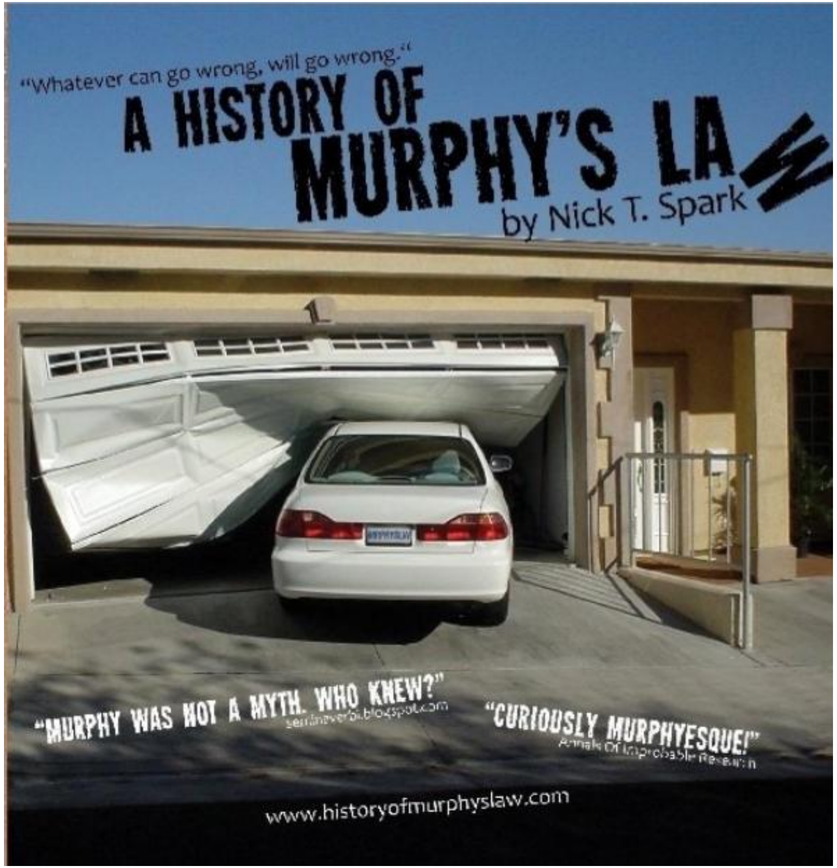
- Github project
  - https://github.com/mnemonic-no/act-platform
  - License: ISC (BSD compatible)

- Python API wrapper
  - https://pypi.org/project/act-api/

WORKSHOP - INTRODUCTION

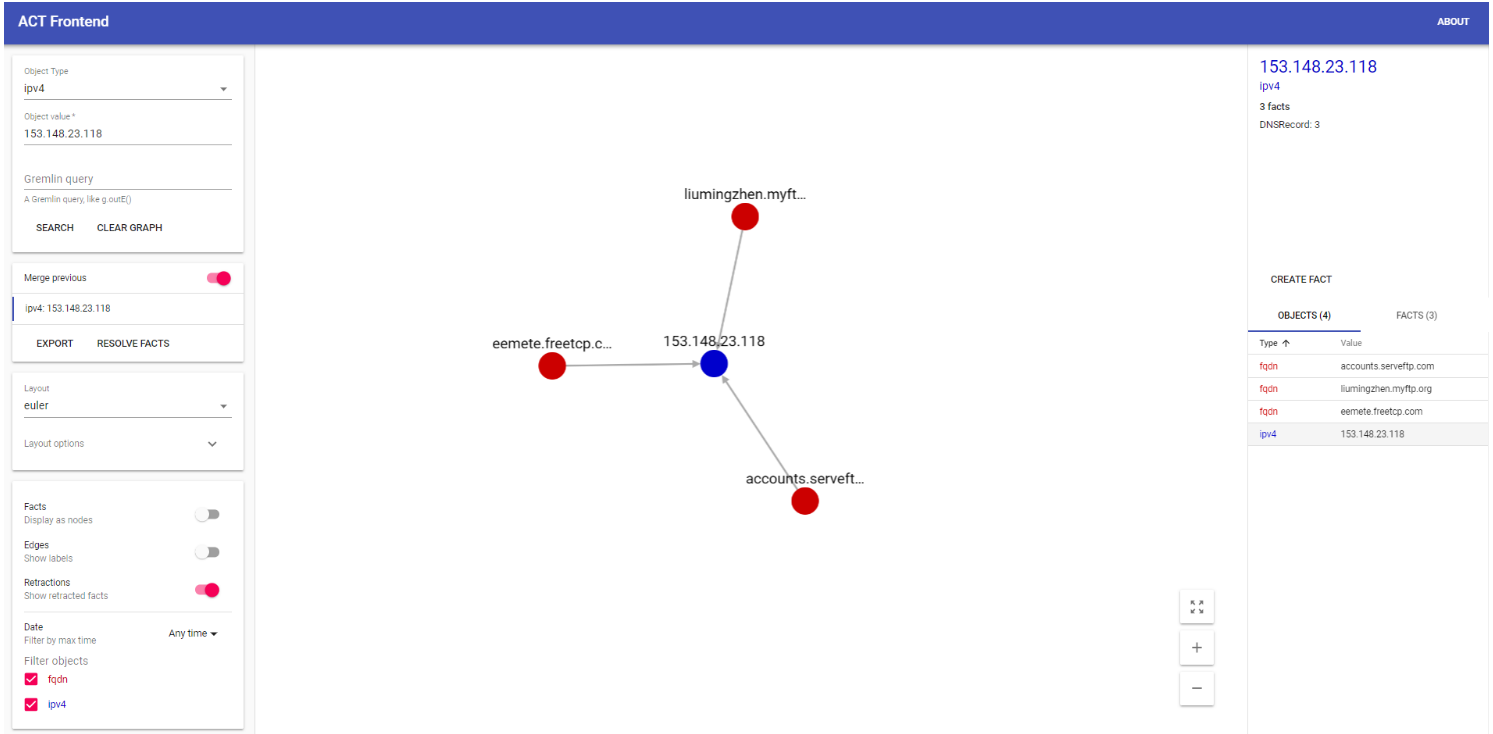
mnemonic

Before We Start


"Whatever can go wrong, will go wrong."
A HISTORY OF
MURPHY'S LAW
by Nick T. Spark
MURPHYSLAW
"MURPHY WAS NOT A MYTH. WHO KNEW?"
seminaverbi.blogspot.com
"CURIOUSLY MURPHYESQUE!"
Annals Of Improbable Research
www.historyofmurphyslaw.com

Periscope Film LLC [CC BY-SA 3.0 (https://creativecommons.org/licenses/by-sa/3.0) or GFDL (http://www.gnu.org/copyleft/fdl.html)], via Wikimedia Commons

Introduction 1



ACT Frontend

ABOUT

Object Type: ipv4

Object value *: 153.148.23.118

Gremlin query

A Gremlin query, like g.outE()

SEARCH CLEAR GRAPH

Merge previous

ipv4: 153.148.23.118

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

☑ fqdn

☑ ipv4

153.148.23.118

ipv4

3 facts

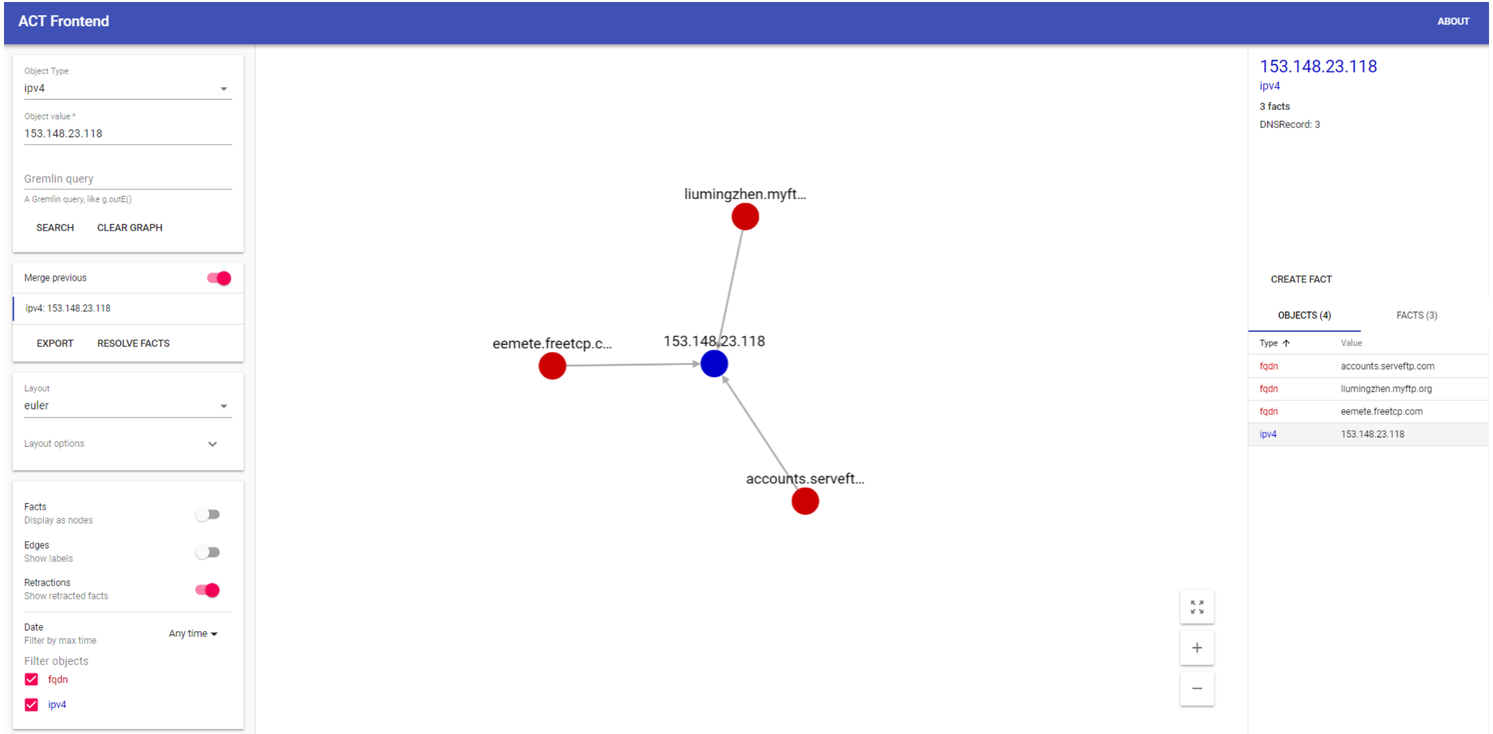
DNSRecord: 3

CREATE FACT

OBJECTS (4) FACTS (3)

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

Introduction 1 – Right Click / Left Click



Object Type: ipv4

Object value *: 153.148.23.118

Gremlin query

A Gremlin query, like g.outE()

Merge previous: on

ipv4: 153.148.23.118

Layout: euler

Layout options

Facts – Display as nodes: off

Edges – Show labels: off

Retractions – Show retracted facts: on

Date – Filter by max time: Any time

Filter objects

☑ fqdn

☑ ipv4

153.148.23.118

ipv4

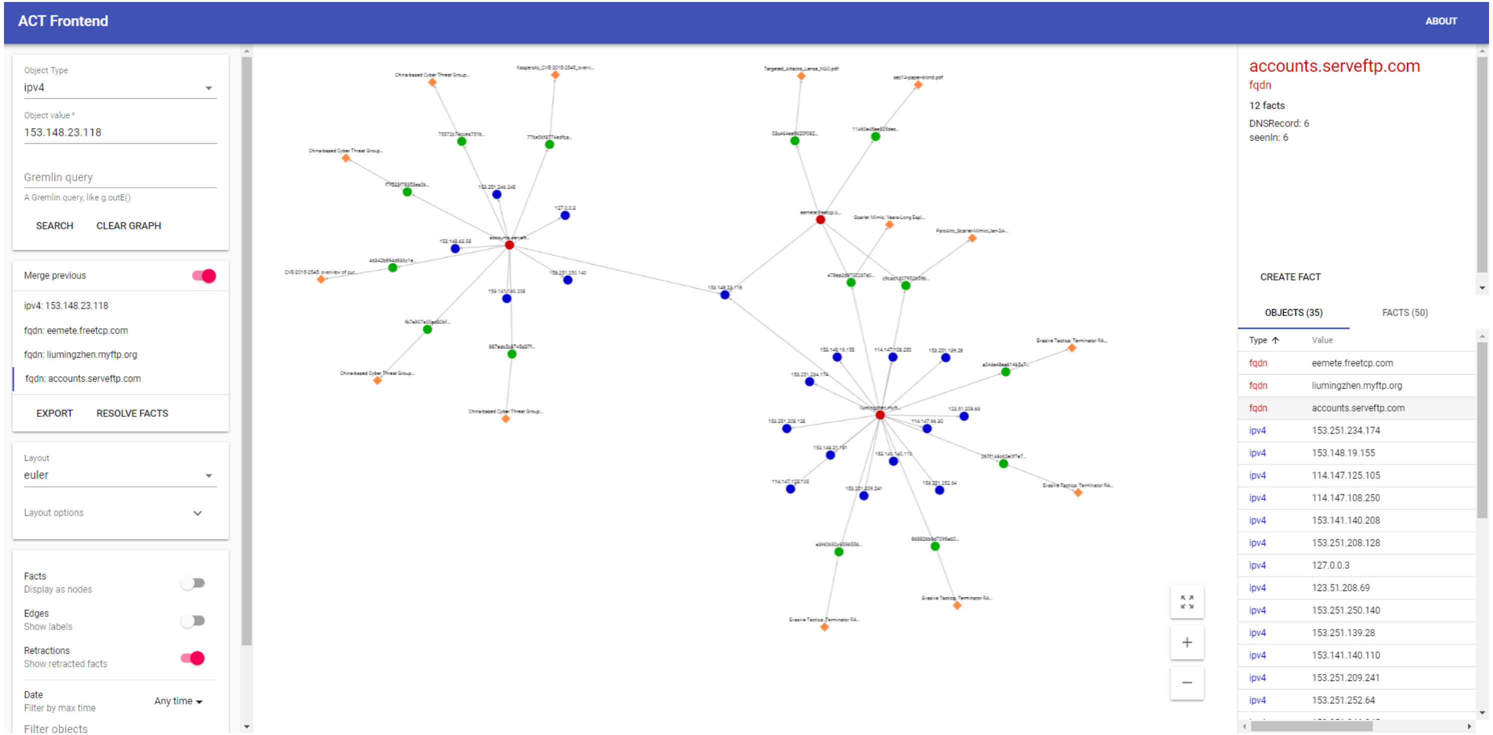
3 facts

DNSRecord: 3

OBJECTS (4) | FACTS (3)

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

Introduction 1 – History, Layouts and Filtering



ACT Frontend — ABOUT

Object Type: ipv4

Object value *: 153.148.23.118

Gremlin query

A Gremlin query, like g.outE()

SEARCH CLEAR GRAPH

Merge previous

- ipv4: 153.148.23.118
- fqdn: eemete.freetcp.com
- fqdn: liumingzhen.myftp.org
- fqdn: accounts.serveftp.com

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

accounts.serveftp.com

fqdn

12 facts

DNSRecord: 6

seenIn: 6

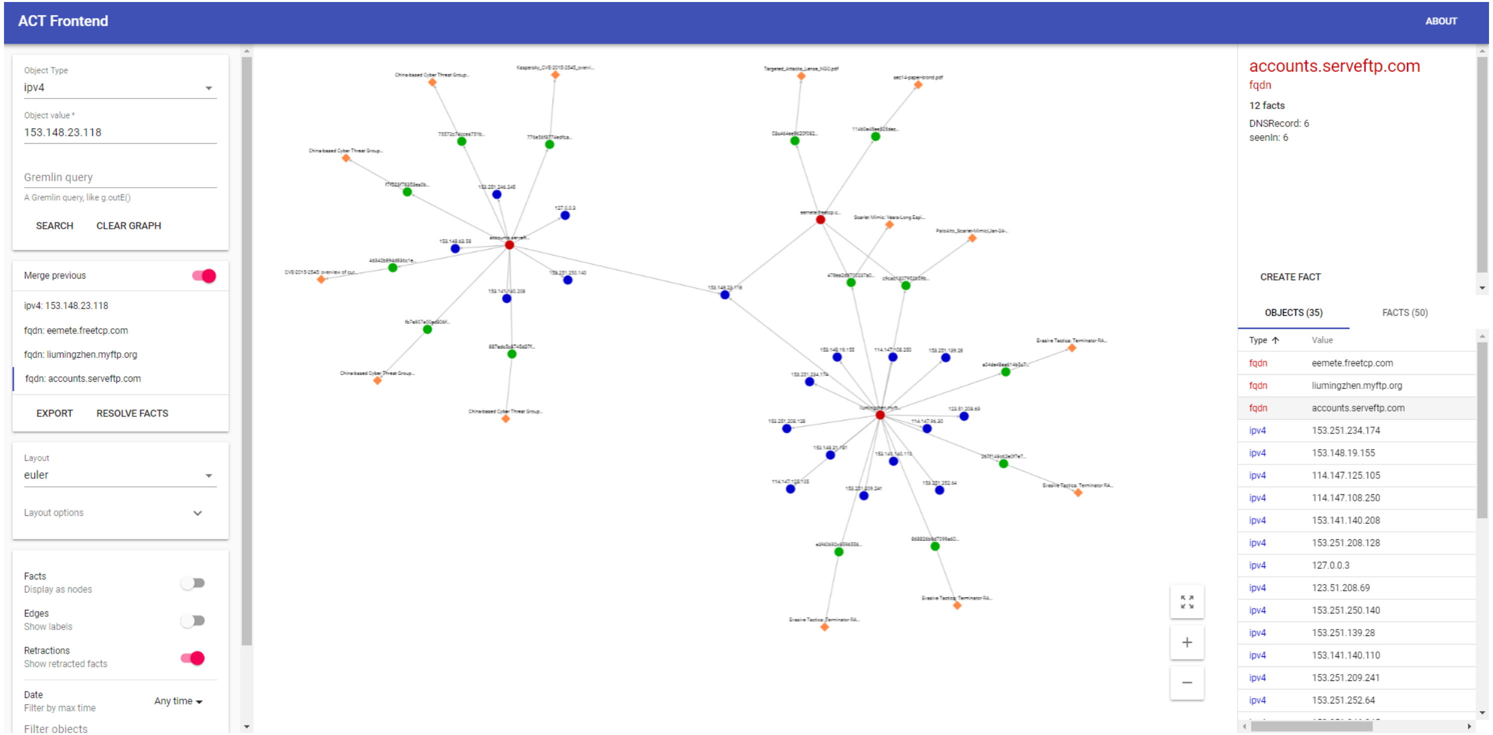
CREATE FACT

OBJECTS (35) FACTS (50)

Type ↑	Value
fqdn	eemete.freetcp.com
fqdn	liumingzhen.myftp.org
fqdn	accounts.serveftp.com
ipv4	153.251.234.174
ipv4	153.148.19.155
ipv4	114.147.125.105
ipv4	114.147.108.250
ipv4	153.141.140.208
ipv4	153.251.208.128
ipv4	127.0.0.3
ipv4	123.51.208.69
ipv4	153.251.250.140
ipv4	153.251.139.28
ipv4	153.141.140.110
ipv4	153.251.209.241
ipv4	153.251.252.64

mnemonic

Introduction 1 – Fact Types



Object Type: ipv4

Object value *: 153.148.23.118

Gremlin query

A Gremlin query, like g.outE()

SEARCH CLEAR GRAPH

Merge previous ●

- ipv4: 153.148.23.118
- fqdn: eemete.freetcp.com
- fqdn: liumingzhen.myftp.org
- fqdn: accounts.serveftp.com

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

accounts.serveftp.com

fqdn

12 facts

DNSRecord: 6

seenIn: 6

CREATE FACT

OBJECTS (35) FACTS (50)

Type ↑	Value
fqdn	eemete.freetcp.com
fqdn	liumingzhen.myftp.org
fqdn	accounts.serveftp.com
ipv4	153.251.234.174
ipv4	153.148.19.155
ipv4	114.147.125.105
ipv4	114.147.108.250
ipv4	153.141.140.208
ipv4	153.251.208.128
ipv4	127.0.0.3
ipv4	123.51.208.69
ipv4	153.251.250.140
ipv4	153.251.139.28
ipv4	153.141.140.110
ipv4	153.251.209.241
ipv4	153.251.252.64

Introduction 2

Try the following object queries and explore the graph:

- threatActor: Sofacy
- technique: Credential Dumping
- tool: foosace
- hash: da2a657dc69d7320f2ffc87013f257ad

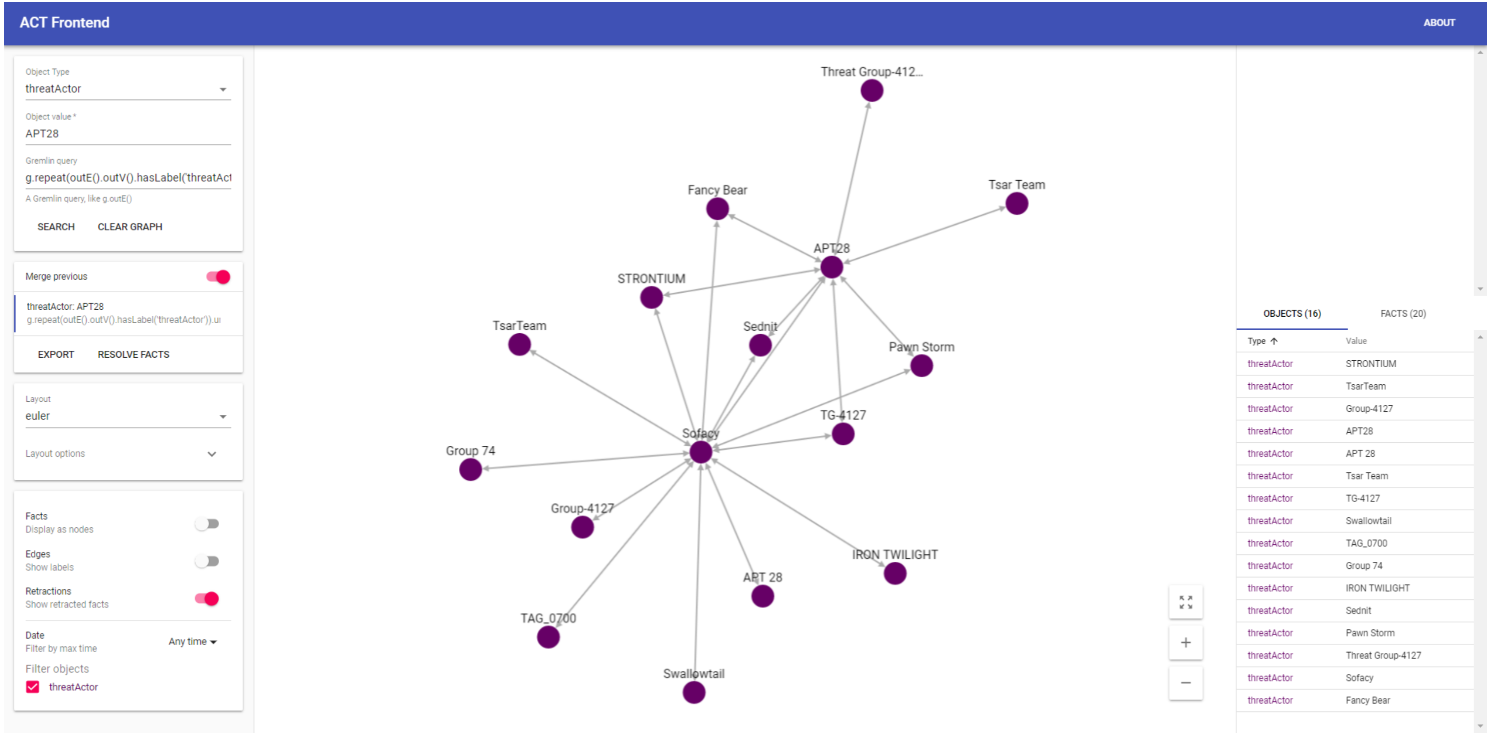
Task 1

Try the following object query:

- ipv4: 40.112.210[.]240

What is the role of this IP address? Find any related Threat Actor(s).

Introduction 3 – Threat Actor Aliases



Object Type: threatActor

Object value *: APT28

Gremlin query: g.repeat(outE().outV().hasLabel('threatAct

A Gremlin query, like g.outE()

Merge previous ●

threatActor: APT28
g.repeat(outE().outV().hasLabel('threatActor')).ur

Layout: euler

Layout options

Facts – Display as nodes ○

Edges – Show labels ○

Retractions – Show retracted facts ●

Date – Filter by max time: Any time

Filter objects

☑ threatActor

OBJECTS (16) FACTS (20)

Type ↑	Value
threatActor	STRONTIUM
threatActor	TsarTeam
threatActor	Group-4127
threatActor	APT28
threatActor	APT 28
threatActor	Tsar Team
threatActor	TG-4127
threatActor	Swallowtail
threatActor	TAG_0700
threatActor	Group 74
threatActor	IRON TWILIGHT
threatActor	Sednit
threatActor	Pawn Storm
threatActor	Threat Group-4127
threatActor	Sofacy
threatActor	Fancy Bear

Task 2

Try the following object queries in sequence:

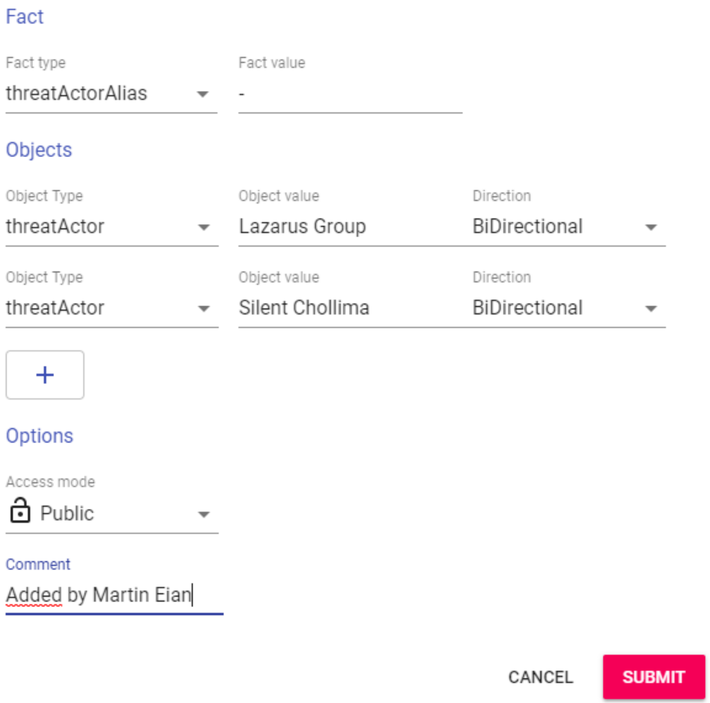
- ipv4: 85.25.100[.]104 – expand reports
- ipv4: 74.201.40[.]28
- ipv4: 74.201.40[.]32

What are the roles of these IP addresses? Find any related Threat Actors.

Task 3: Find the Report

https://blog.talosintelligence.com/2018/05/VPNFilter.html

Introduction 4 – Create/Retract Fact



Fact

Fact type: threatActorAlias

Fact value: -

Objects

Object Type: threatActor
Object value: Lazarus Group
Direction: BiDirectional

Object Type: threatActor
Object value: Silent Chollima
Direction: BiDirectional

Options

Access mode: Public

Comment: Added by Martin Eian

Bonus Task:

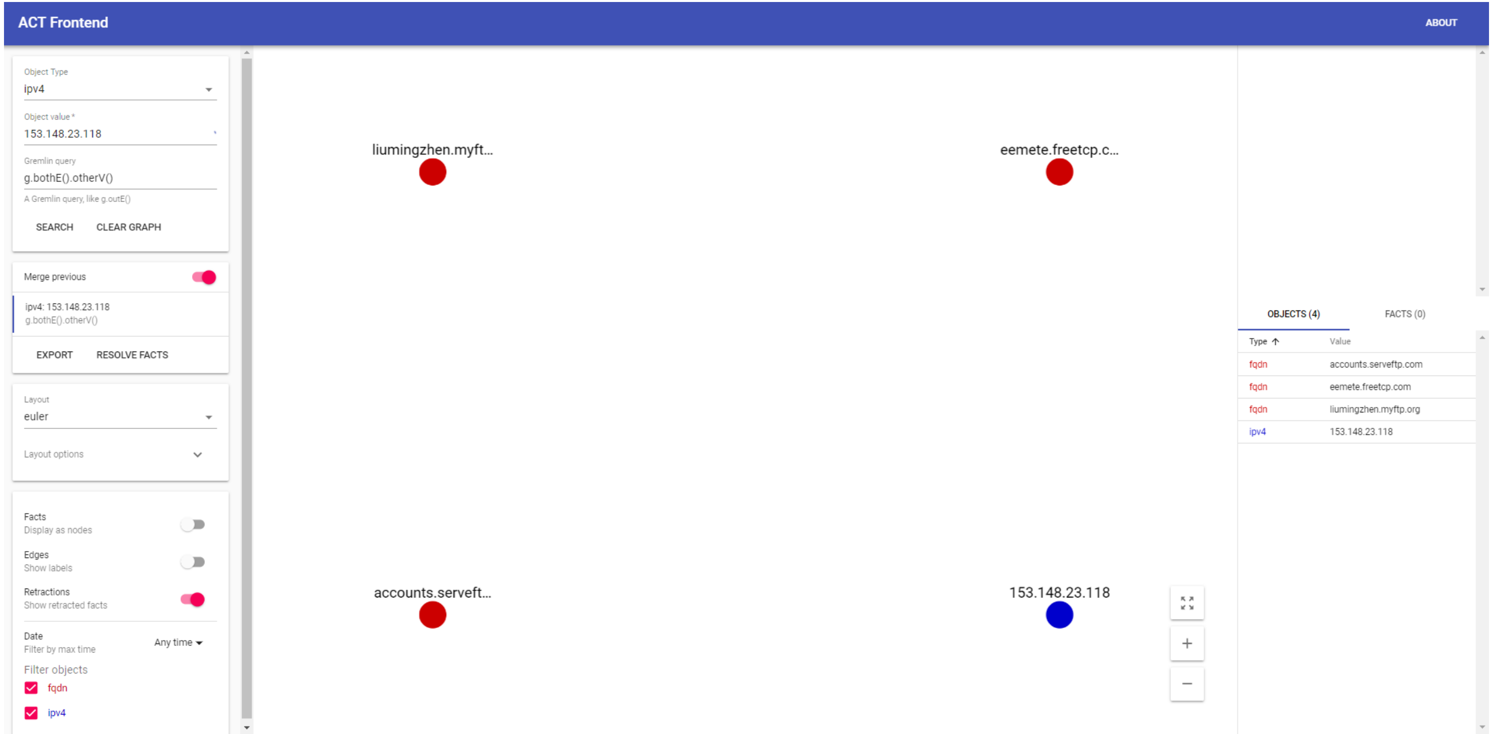
Investigate the domain name rannd[.]org.

WORKSHOP – GRAPH QUERIES

With Great Power Comes Great Responsibility

mnemonic

Graph Query 1



ACT Frontend

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

Filter objects

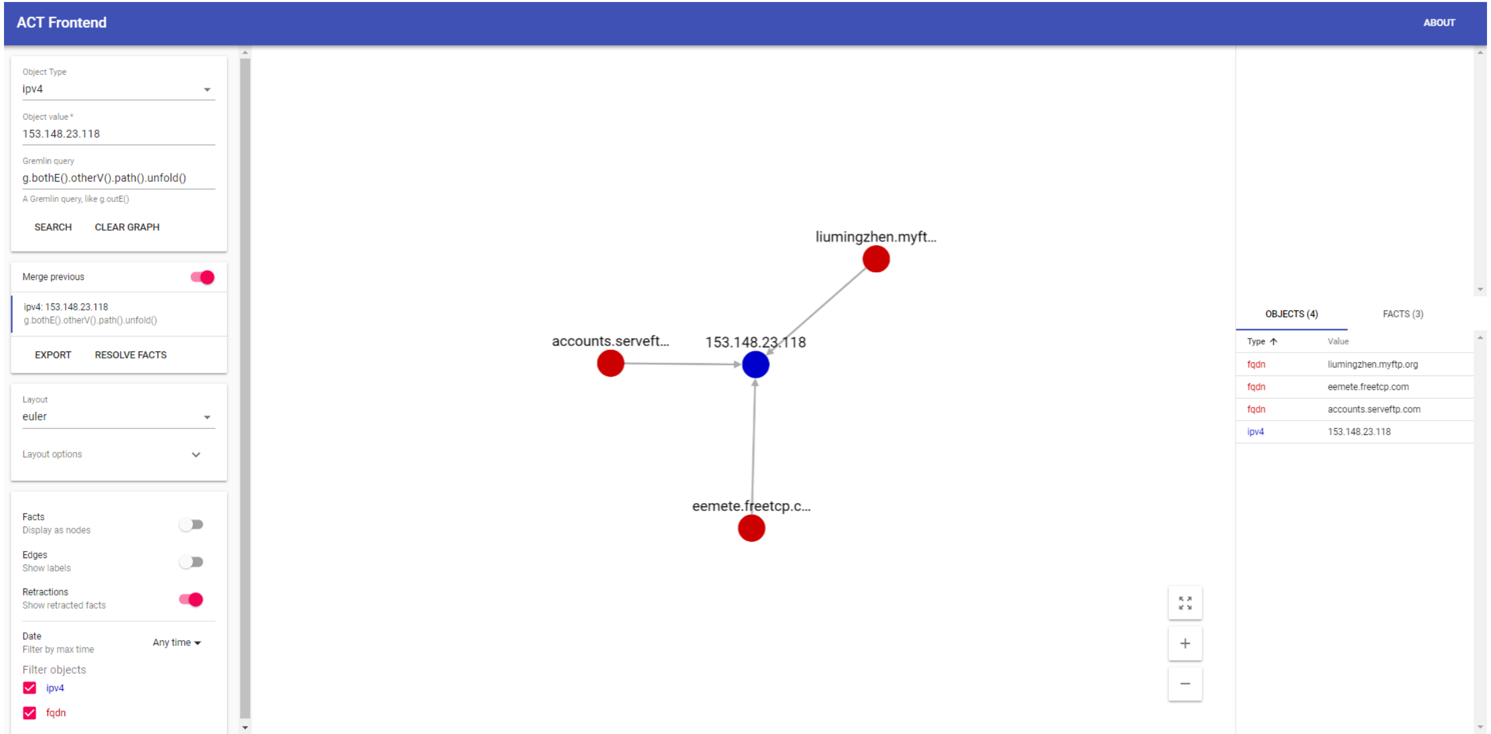
☑ fqdn

☑ ipv4

OBJECTS (4) FACTS (0)

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

Graph Query 2 – Show Edges



ACT Frontend

Object Type: ipv4

Object value *: 153.148.23.118

Gremlin query: g.bothE().otherV().path().unfold()

A Gremlin query, like g.outE()

Merge previous ●

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

Layout: euler

Facts
Display as nodes ○

Edges
Show labels ○

Retractions
Show retracted facts ●

Date
Filter by max time: Any time

Filter objects

☑ ipv4

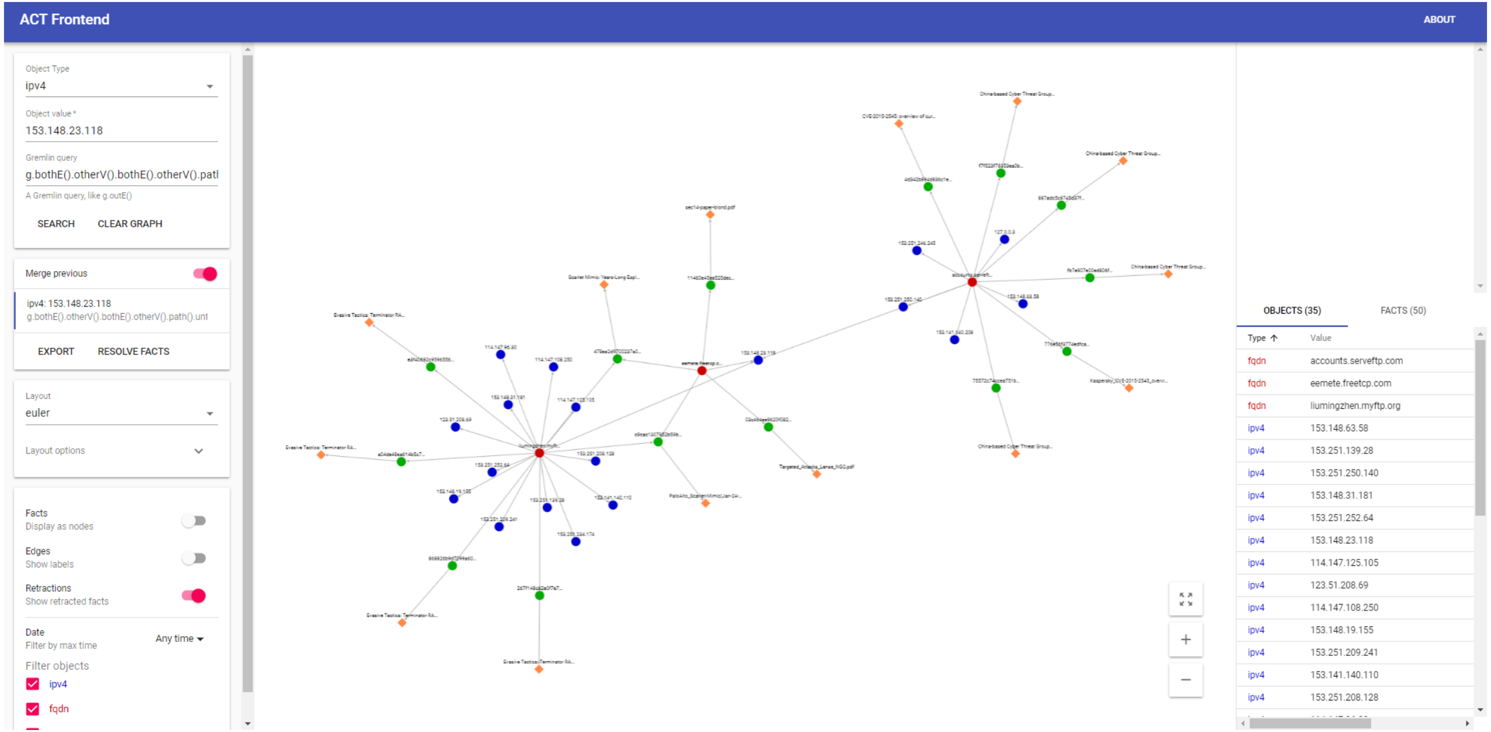
☑ fqdn

OBJECTS (4) FACTS (3)

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

mnemonic

Graph Query 3 – 2 hops



ACT Frontend
ABOUT
SEARCH
CLEAR GRAPH
EXPORT
RESOLVE FACTS
China-based Cyber Threat Group...
127.0.0.1
153.148.23.118
Evasive Tactics: Terminator RA...
Targeted_Attacks_Lense_NGO.pdf

Object Type: ipv4

Object value *: 153.148.23.118

Gremlin query: g.bothE().otherV().bothE().otherV().patl

A Gremlin query, like g.outE()

Merge previous: on

ipv4: 153.148.23.118
g.bothE().otherV().bothE().otherV().path().unt

Layout: euler

Layout options

Facts — Display as nodes: off

Edges — Show labels: off

Retractions — Show retracted facts: on

Date — Filter by max time: Any time

Filter objects

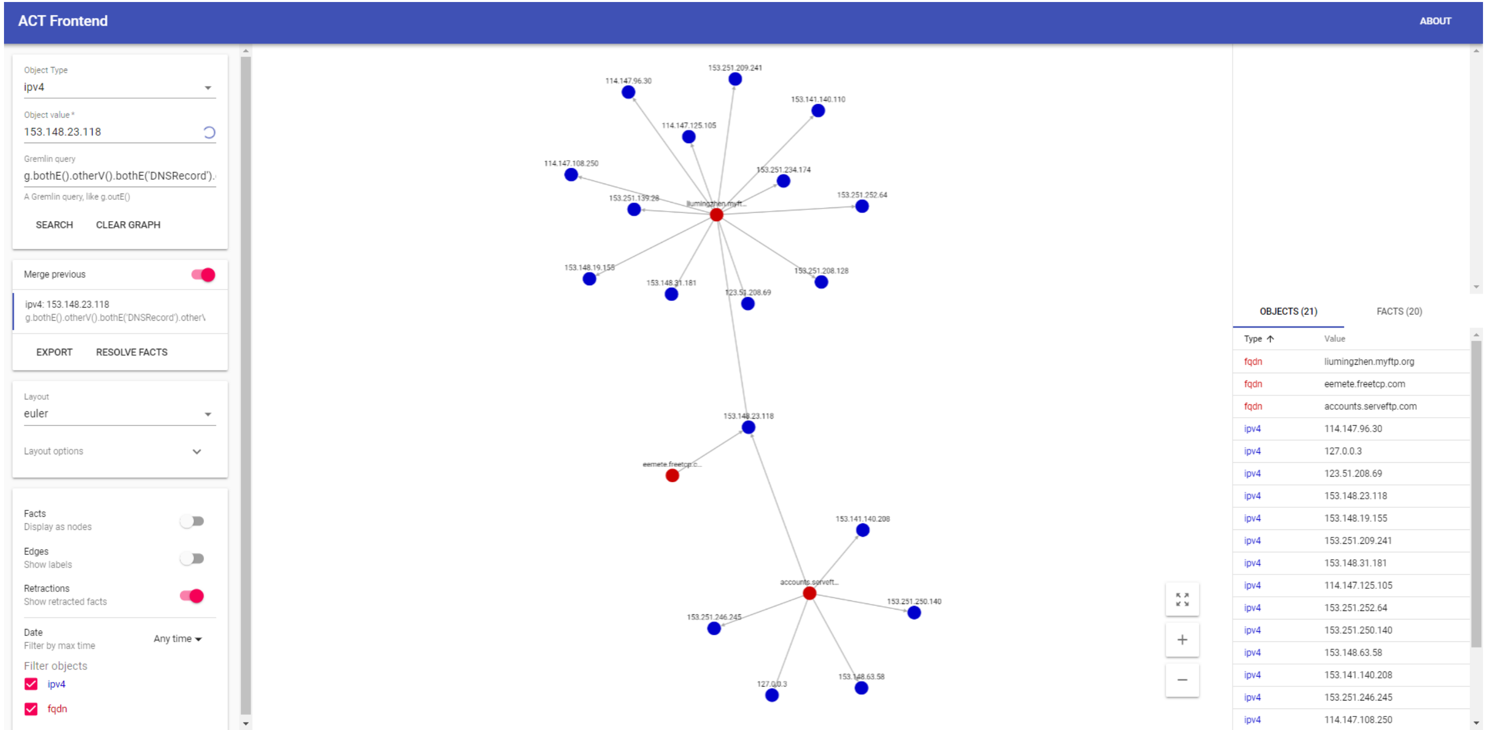
☑ ipv4

☑ fqdn

OBJECTS (35) FACTS (50)

Type ↑	Value
fqdn	accounts.serveftp.com
fqdn	eemete.freetcp.com
fqdn	liumingzhen.myftp.org
ipv4	153.148.63.58
ipv4	153.251.139.28
ipv4	153.251.250.140
ipv4	153.148.31.181
ipv4	153.251.252.64
ipv4	153.148.23.118
ipv4	114.147.125.105
ipv4	123.51.208.69
ipv4	114.147.108.250
ipv4	153.148.19.155
ipv4	153.251.209.241
ipv4	153.141.140.110
ipv4	153.251.208.128

Graph Query 4 – Filter Edges (Facts)



Object Type
ipv4

Object value *
153.148.23.118

Gremlin query
g.bothE().otherV().bothE('DNSRecord').

A Gremlin query, like g.outE()

Merge previous ●

ipv4: 153.148.23.118
g.bothE().otherV().bothE('DNSRecord').other\

Layout
euler

Facts
Display as nodes ○

Edges
Show labels ○

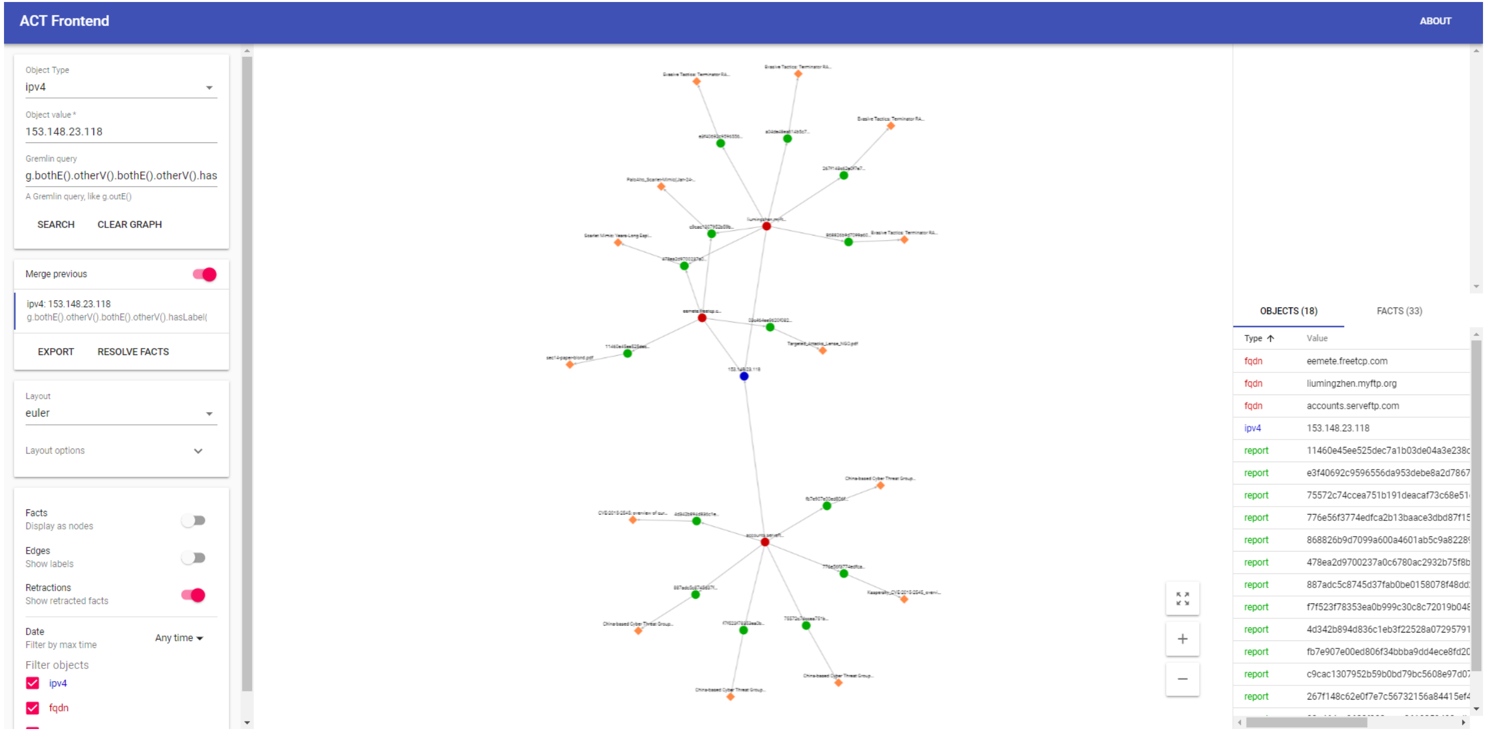
Retractions
Show retracted facts ●

Date
Filter by max time
Any time

Filter objects
☑ ipv4
☑ fqdn

Type ↑	Value
fqdn	liumingzhen.myftp.org
fqdn	eemete.freetcp.com
fqdn	accounts.serveftp.com
ipv4	114.147.96.30
ipv4	127.0.0.3
ipv4	123.51.208.69
ipv4	153.148.23.118
ipv4	153.148.19.155
ipv4	153.251.209.241
ipv4	153.148.31.181
ipv4	114.147.125.105
ipv4	153.251.252.64
ipv4	153.251.250.140
ipv4	153.148.63.58
ipv4	153.141.140.208
ipv4	153.251.246.245
ipv4	114.147.108.250

Graph Query 5 – Filter Nodes (Objects)



ACT Frontend

ABOUT

Object Type
ipv4

Object value *
153.148.23.118

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

SEARCH CLEAR GRAPH

Merge previous

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

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

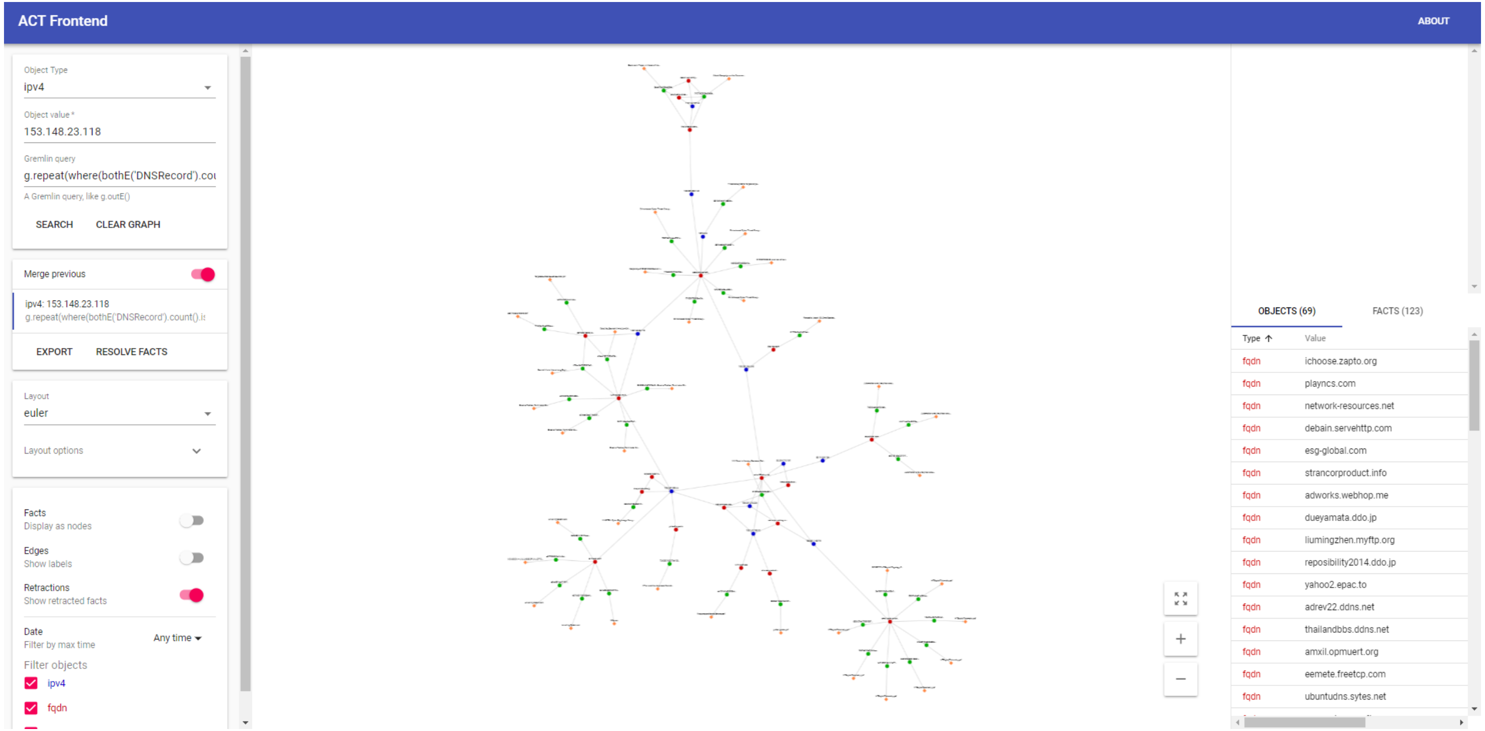
Filter objects
☑ ipv4
☑ fqdn

Evasive Tactics: Terminator RA...
Evasive Tactics: Terminator RA...
Evasive Tactics: Terminator RA...
e3f40692c9596556...
a04de48ea614b5c7...
267f148c62e0f7e7...
PaloAlto_ScarletMimic(Jan-24-...
liumingzhen.myft...
c9cac1307952b59b...
868826b9d7099a60...
Evasive Tactics: Terminator RA...
Scarlet Mimic: Years-Long Espi...
478ea2d9700237a0...
eemete.freetcp.c...
09c464ee9620f092...
Targeted_Attacks_Lense_NGO.pdf
11460e45ee525dec...
sec14-paper-blond.pdf
153.148.23.118
China-based Cyber Threat Group...
fb7e907e00ed806f...
CVE-2015-2545: overview of cur...
4d342b894d836c1e...
accounts.servefit...
776e56f3774edfca...
Kaspersky_CVE-2015-2545_overvi...
887adc5c8745d37f...
China-based Cyber Threat Group...
f7f523f78353ea0b...
75572c74ccea751b...
China-based Cyber Threat Group...
China-based Cyber Threat Group...

OBJECTS (18) FACTS (33)

Type ↑	Value
fqdn	eemete.freetcp.com
fqdn	liumingzhen.myftp.org
fqdn	accounts.serveftp.com
ipv4	153.148.23.118
report	11460e45ee525dec7a1b03de04a3e238c
report	e3f40692c9596556da953debe8a2d7867
report	75572c74ccea751b191deacaf73c68e51
report	776e56f3774edfca2b13baace3dbd87f15
report	868826b9d7099a600a4601ab5c9a8228
report	478ea2d9700237a0c6780ac2932b75f8b
report	887adc5c8745d37fab0be0158078f48dd
report	f7f523f78353ea0b999c30c8c72019b048
report	4d342b894d836c1eb3f22528a07295791
report	fb7e907e00ed806f34bbba9dd4ece8fd20
report	c9cac1307952b59b0bd79bc5608e97d07
report	267f148c62e0f7e7c56732156a84415ef4

Graph Query 6 – Warp Speed



ACT Frontend

ABOUT

Object Type
ipv4

Object value *
153.148.23.118

Gremlin query
g.repeat(where(bothE('DNSRecord').cou

A Gremlin query, like g.outE()

SEARCH CLEAR GRAPH

Merge previous

ipv4: 153.148.23.118
g.repeat(where(bothE('DNSRecord').count().i:

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
☑ ipv4
☑ fqdn

OBJECTS (69) FACTS (123)

Type ↑	Value
fqdn	ichoose.zapto.org
fqdn	playncs.com
fqdn	network-resources.net
fqdn	debain.servehttp.com
fqdn	esg-global.com
fqdn	strancorproduct.info
fqdn	adworks.webhop.me
fqdn	dueyamata.ddo.jp
fqdn	liumingzhen.myftp.org
fqdn	reposibility2014.ddo.jp
fqdn	yahoo2.epac.to
fqdn	adrev22.ddns.net
fqdn	thailandbbs.ddns.net
fqdn	amxil.opmuert.org
fqdn	eemete.freetcp.com
fqdn	ubuntudns.sytes.net

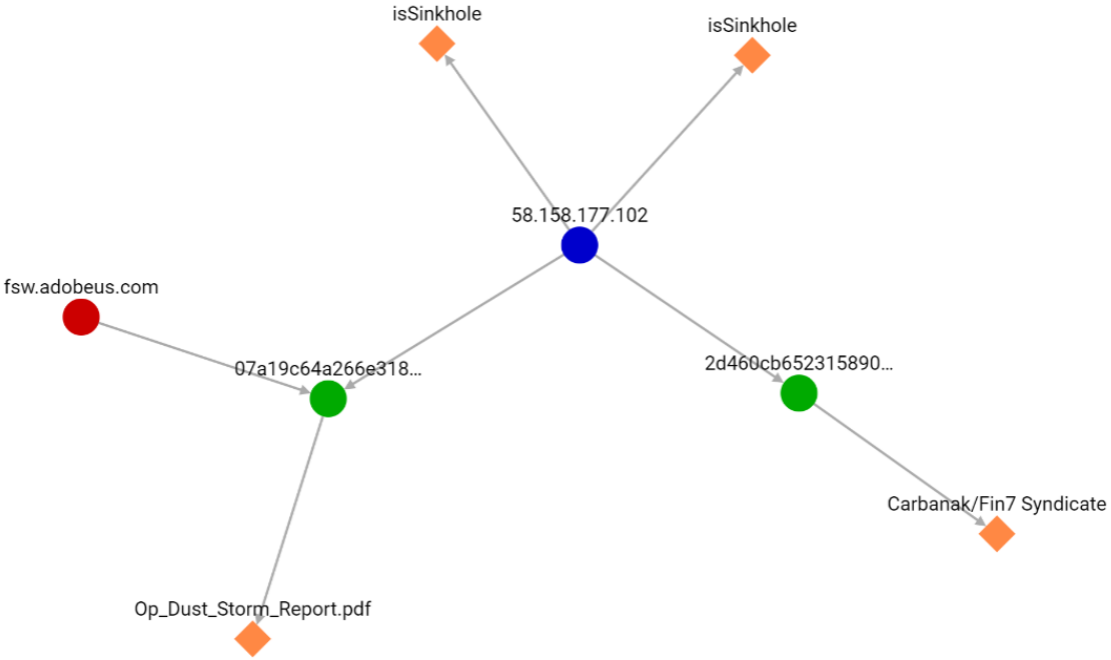
mnemonic

Task 4: Find the Report

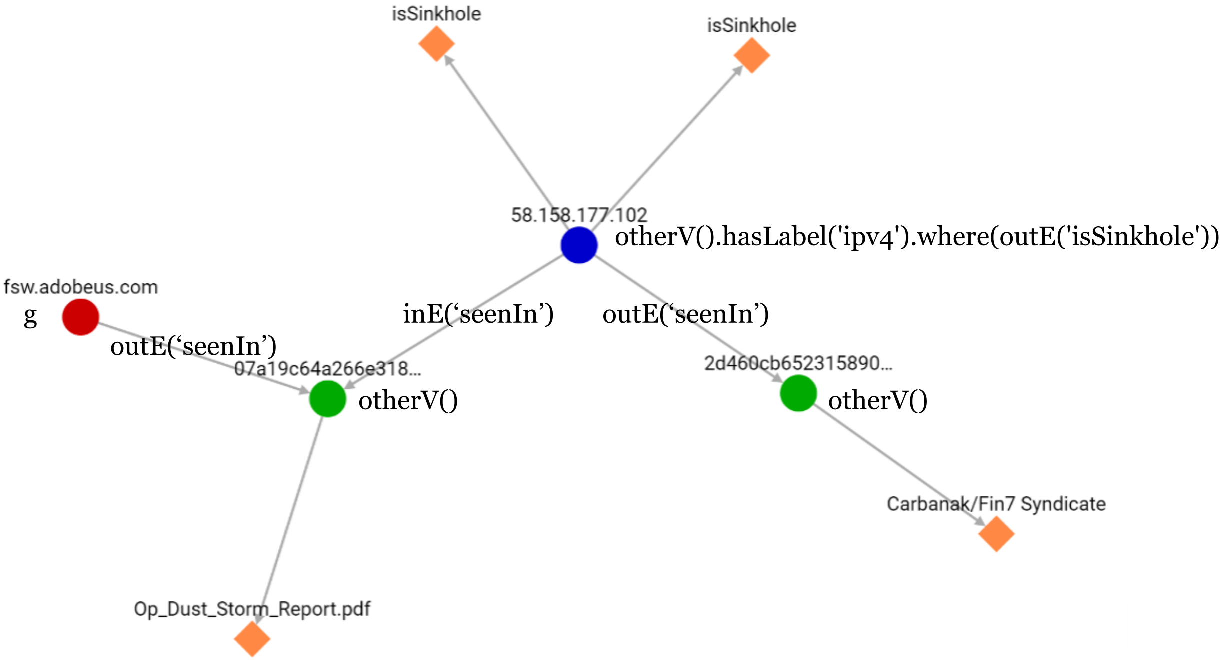
The fqdn fsw.adobeus[.]com is seen in one report. A sinkhole IPv4 address is also seen in the same report. What is the title of the other report mentioning that sinkhole IPv4 address?

Hint: Fact Type ‘seenIn’

Task 4 Solution

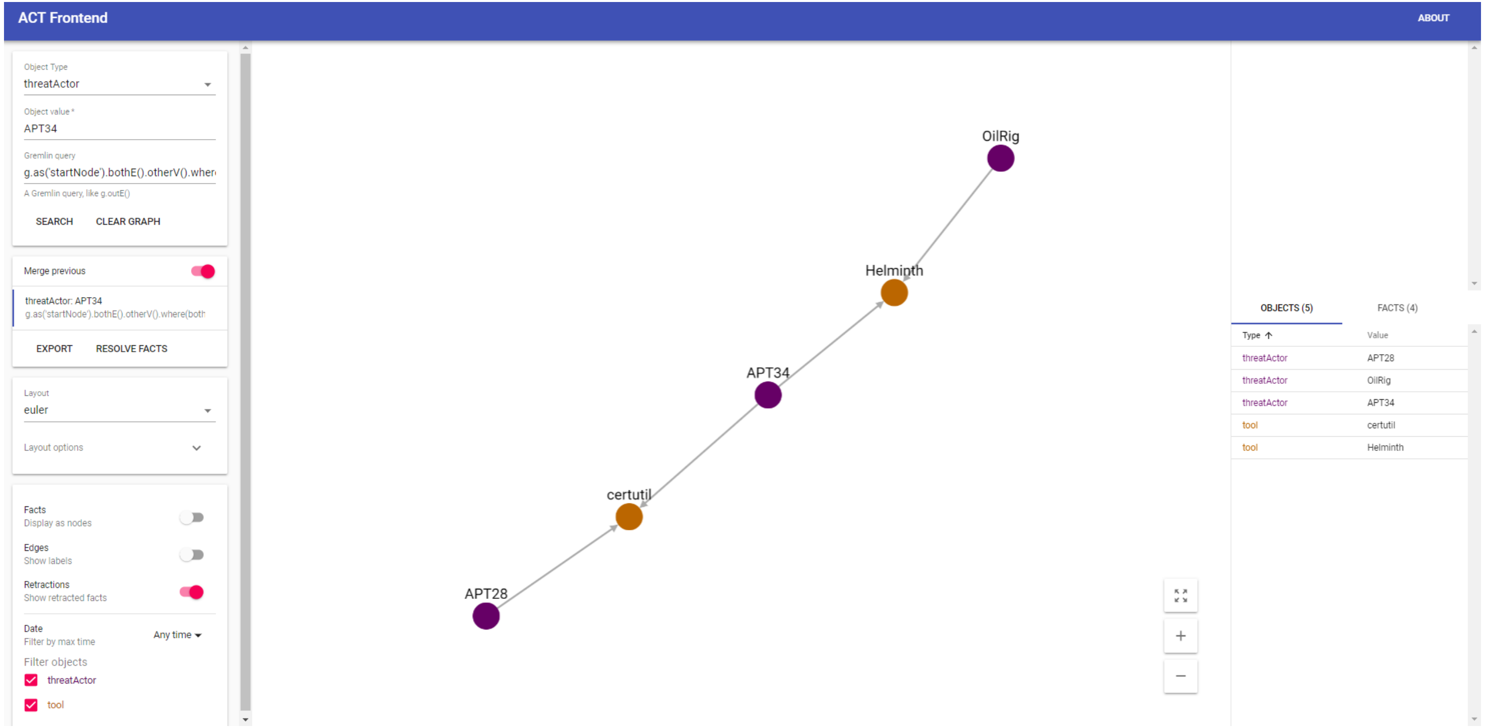


g.outE('seenIn').otherV().inE('seenIn').otherV().hasLabel('ipv4') .where(outE('isSinkhole')).outE('seenIn').otherV().path().unfold()



mnemonic

Graph Query 7 – Unique Tool Usage



Object Type: threatActor

Object value *: APT34

Gremlin query: g.as('startNode').bothE().otherV().wher

A Gremlin query, like g.outE()

Merge previous ●

threatActor: APT34
g.as('startNode').bothE().otherV().where(both

Layout: euler

Layout options

Facts – Display as nodes ○

Edges – Show labels ○

Retractions – Show retracted facts ●

Date – Filter by max time: Any time

Filter objects

☑ threatActor

☑ tool

Type ↑	Value
threatActor	APT28
threatActor	OilRig
threatActor	APT34
tool	certutil
tool	Helminth

EXERCISES

Exercises

There are two Threat Actors known to use certutil.exe. Which other tool do they have in common?

Which Threat Actor is associated with the domain name www.eye-watch[.]in?

How many DNSRecord facts are connected to the IP address 8.8.8.8?

How many Threat Actors are known to originate (sourceGeography) from France (location)?

How many of the Threat Actors known to originate from Russia use the tool psexec?

Exercises - Answers

There are two Threat Actors known to use certutil.exe. Which other tool do they have in common?
mimikatz

Which Threat Actor is associated with the domain name www.eye-watch[.]in?
Lazarus Group

How many DNSRecord facts are connected to the IP address 8.8.8.8?
18741

How many Threat Actors are known to originate (sourceGeography) from France?
1

How many of the Threat Actors known to originate from Russia use the tool psexec?
3

FURTHER WORK

New Information Sources

- Security alerts
- Incidents
- Reputation lists
- Malware analysis systems
- WHOIS
- MISP feeds
- 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