

Synapse Bootcamp - Module 2

Getting Started - Exercises

Getting Started - Exercises	1
Objectives	1
Exercises	2
Fork a View	2
Exercise 1	2
Lifting Nodes	5
Exercise 2	5
Exercise 3	6
Working with Tags	7
Exercise 4	7
Exercise 5	9
Exercise 6	11

Objectives

In these exercises you will learn:

- How to fork a view in Synapse
- How to lift nodes using the Query Bar in Lookup mode
- How to lift nodes using the Query Bar in Text Search mode
- How to view and interpret tags on a node
- How to lift nodes by tag

Note: We are constantly updating Synapse and its Power-Ups! We do our best to make sure our course documents (slides, exercises, and answer keys) are up-to-date. However, you may notice small differences (such as between a screen capture in the documents and the appearance of your current instance of Synapse).

If something is unclear or if you identify an error, please reach out to us so we can assist!

Exercises

Fork a View

Exercise 1

Objective:

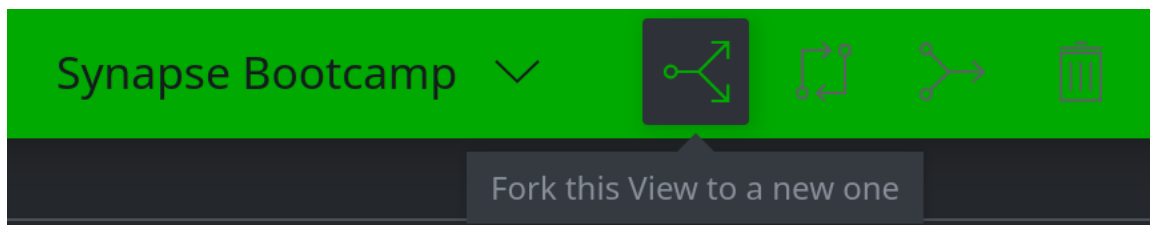
- Create a fork of your current view.

Working in a forked view provides you with a "scratch space" to perform research or test some analysis before moving your work into production. We **always** recommend that you fork a view before you start your work!

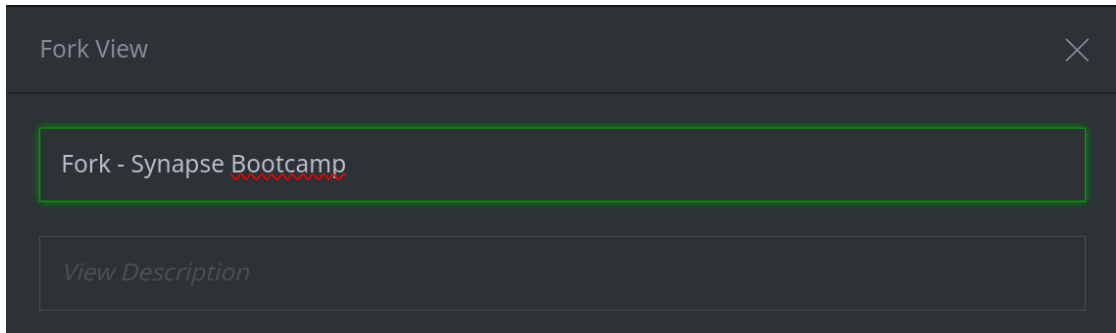
- In the **Research Tool** locate the **View Task Bar** icons in the **Top Bar**. You should be in the **Synapse Bootcamp** view:



- Click the **Fork** icon to fork a new view:

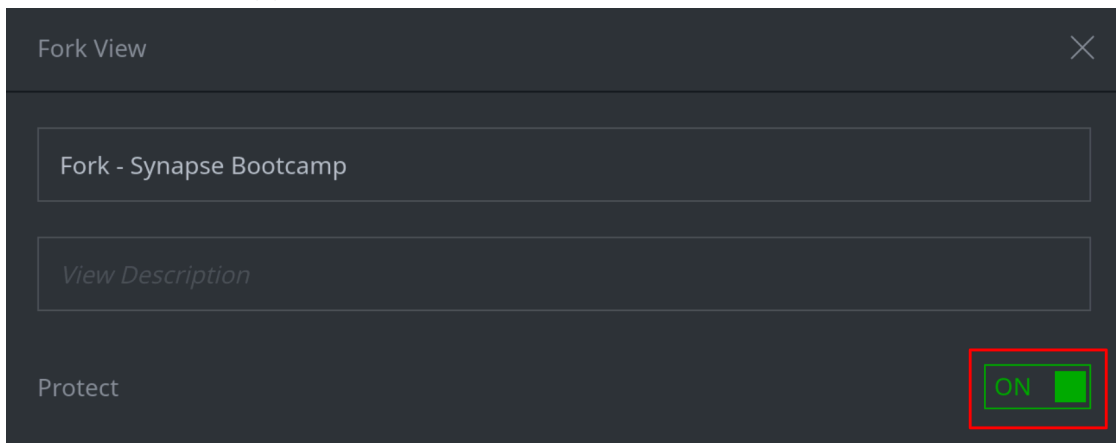


- In the **Fork View** dialog, enter **Fork - Synapse Bootcamp** in the *View Name* field:



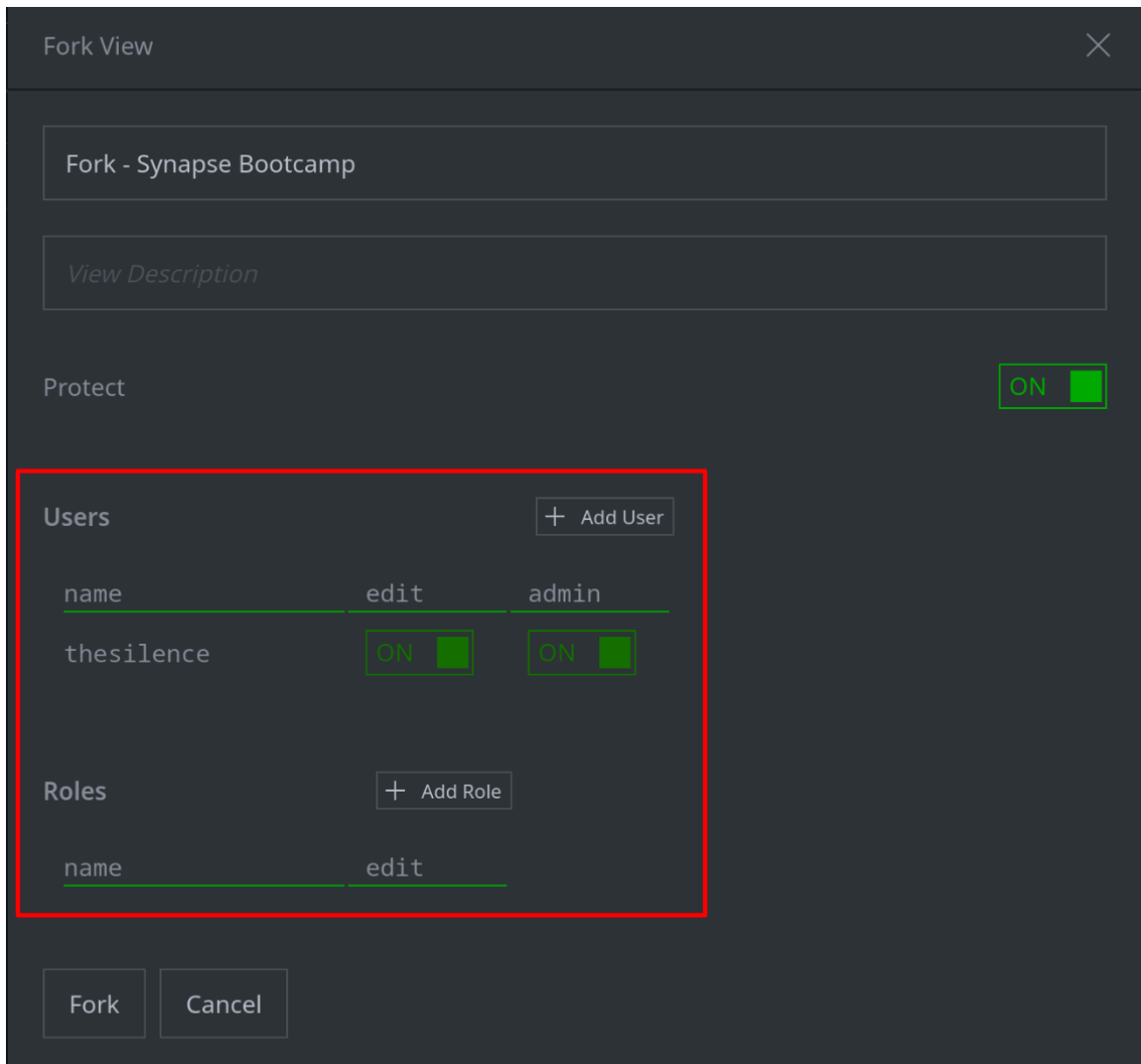
A screenshot of the 'Fork View' dialog box. The title bar says 'Fork View' with a close button. The main area has a text input field containing 'Fork - Synapse Bootcamp', which is highlighted with a red border. Below it is a 'View Description' field.

- Set the **Protect** toggle to **ON**:



A screenshot of the 'Fork View' dialog box. The title bar says 'Fork View' with a close button. The main area has a text input field containing 'Fork - Synapse Bootcamp' and a 'View Description' field. At the bottom right, there is a 'Protect' toggle switch, which is highlighted with a red border and is currently turned 'ON'.

- **Note** the permissions section:



Fork View

Fork - Synapse Bootcamp

View Description

Protect ON

Users

name	edit	admin
thesilence	<input checked="" type="checkbox"/> ON	<input checked="" type="checkbox"/> ON

Roles

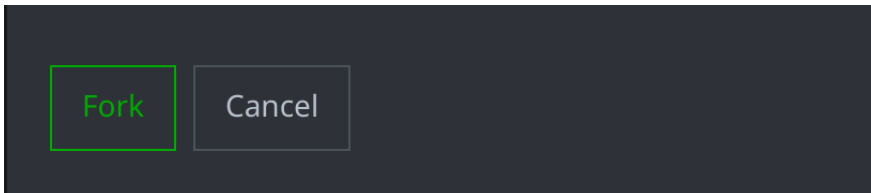
name	edit
------	------

By default:

- **You** are the only user with access to the forked view.
- You have both **edit** (write) and **admin** permissions to the forked view.

Tip: see the **Optic User Guide** for information on how to [grant permissions](#) to other users or roles.

- Click the **Fork** button to create the forked view:



Question 1: How did the information displayed in your **Top Bar** change?

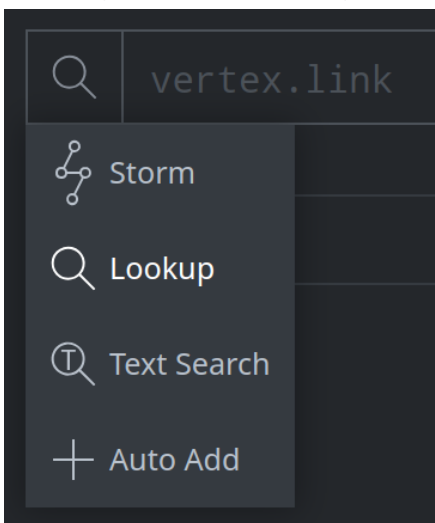
Lifting Nodes

Exercise 2

Objective:

- Practice lifting nodes using **Lookup** mode.

- Ensure your **Storm Query Bar** is in **Lookup** mode:



- In your **Storm Query Bar**, enter the following **indicators** and press **Enter** to run the query:

```
50.2.160.146 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX  
hxxps://45.154.14[.]235/2023/PotPlayer.exe  
mfa.cdep[@]mfa.gov.lv vertex[.]link  
d41d8cd98f00b204e9800998ecf8427e CVE-2014-4114
```

Question 1: How many nodes are displayed in the Results Panel?

- In your **Storm Query Bar**, enter the following **email address** and press **Enter** to run the query:

```
visi@vertex.link
```

Question 2: What happens when you run the query?

- In your **Storm Query Bar**, enter the following **file name** and press **Enter** to run the query:

```
certutil.exe
```

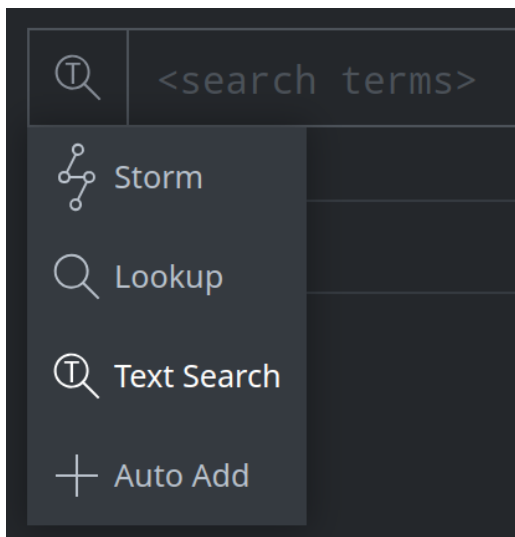
Question 3: What happens when you run the query?

Exercise 3

Objective:

- Practice lifting nodes using **Text Search mode**.

- In your **Storm Query Bar**, use the **query mode selector** to choose **Text Search mode**:



- In your **Storm Query Bar**, enter the following **search term** and press **Enter** to run the query:

eclipse

Question 1: What kinds of nodes are returned by your search?

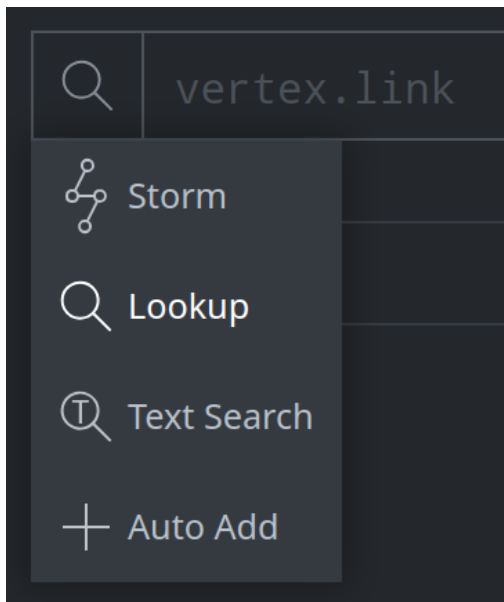
Working with Tags

Exercise 4

Objective:

- **View and understand the tags on a node.**

- In your **Storm Query Bar**, use the **query mode selector** to choose **Lookup** mode:



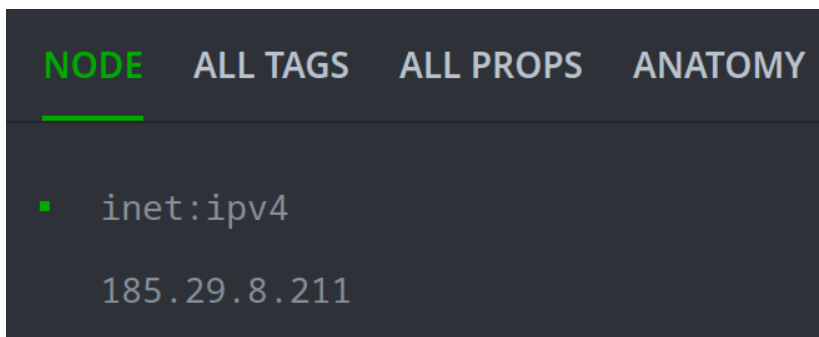
- Enter the following in your query bar and press **Enter** to run the query:

185.29.8.211

- **Select** the node in the **Results Panel**:



- In the **Details Panel**, select the **NODE** tab:



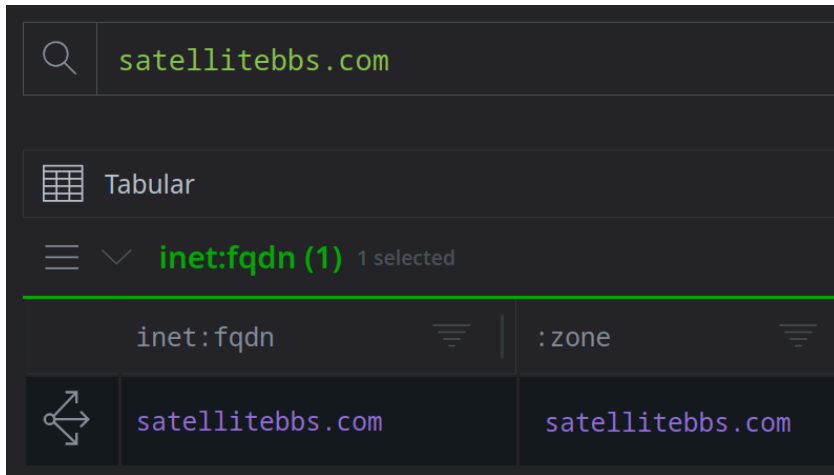
Question 1: What do the **tags** on this node tell us about the IP address?

Hint: You can hover over a tag name in the Details Panel to view its definition.

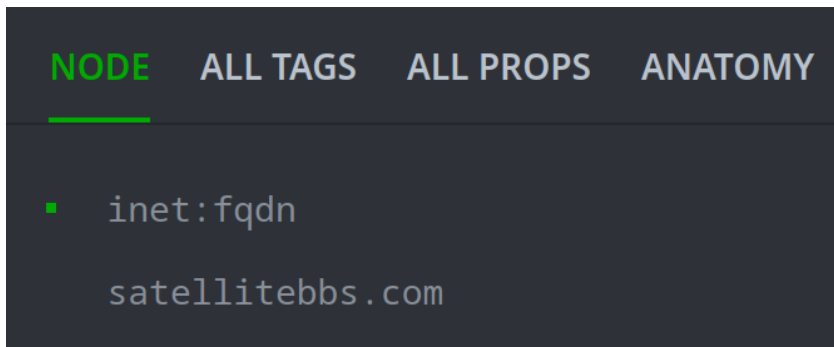
- In the **Storm Query Bar**, in **Lookup mode**, enter the following and press **Enter** to run the query:

```
satellitebbs.com
```


- Select the node in the **Results Panel**:



- In the **Details Panel**, select the **NODE** tab:



- Use the **tags** on the node to answer the following questions:

Question 2: What **publicly reported** threat group is this FQDN associated with?

Question 3: What **internally tracked** threat group is this FQDN associated with?
When did that threat group control the FQDN?

Question 4: When was the FQDN **first sinkholed**? What organization sinkholed it?

Exercise 5

Objective:

- Lift nodes using tags.

- Using the **Storm Query Bar** in **Lookup mode**, enter the following FQDN and press **Enter** to run the query:

```
chemscalere.com
```

- **Select** the node in the **Results Panel**:

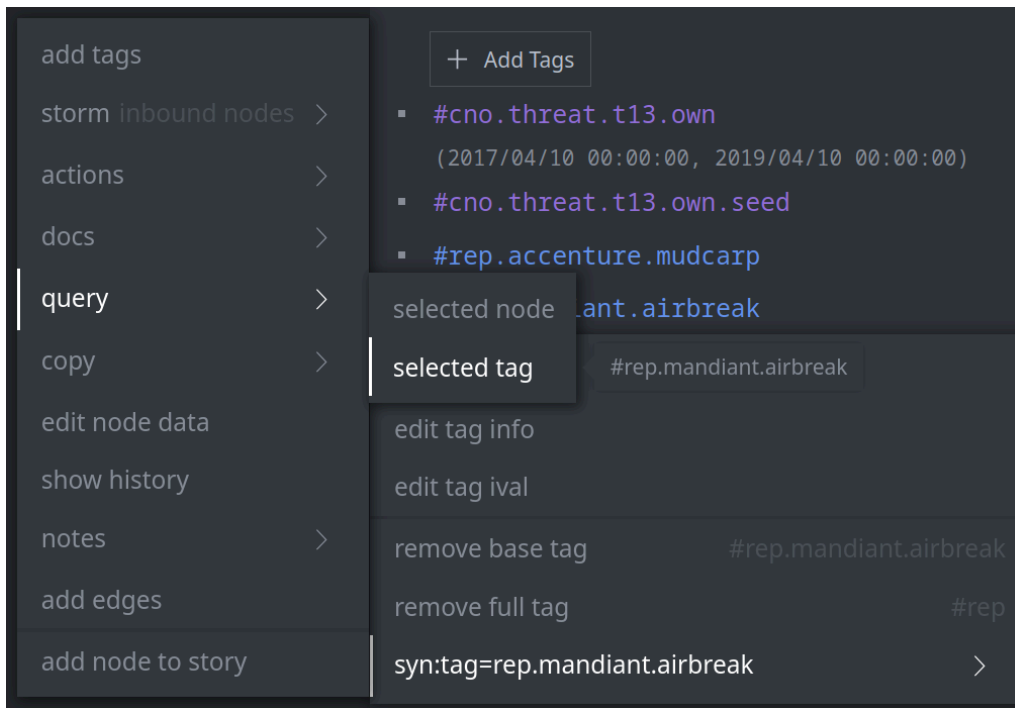


- In the **Details Panel, NODE** tab, view the tags on the node:

```
▪ #cno.threat.t13.own
  (2017/04/10 00:00:00, 2019/04/10 00:00:00)
▪ #cno.threat.t13.own.seed
▪ #rep.accenture.mudcarp
▪ #rep.mandiant.airbreak
▪ #rep.mandiant.temp_periscope
```

You want to see other indicators that Mandiant associates with AIRBREAK malware.

- In the **Details Panel**, click the tag **#rep.mandiant.airbreak** and select **syn:tag=rep.mandiant.airbreak > query > selected tag**:



Question 1: What query did Synapse load and run in the Query Bar?

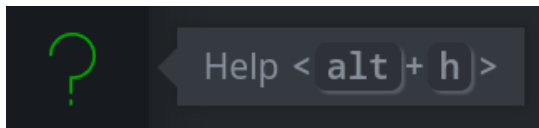
Question 2: What kinds of nodes are returned by the query?

Exercise 6

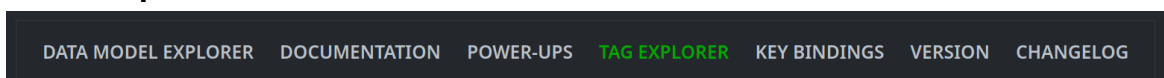
Objective:

- Lift nodes using tags from Tag Explorer.

- From the **Toolbar**, select the **Help Tool**:

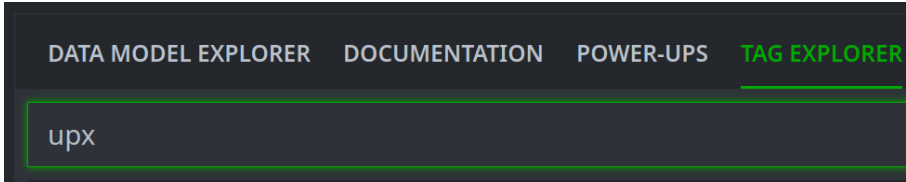


- In the **Help Tool**, select the **TAG EXPLORER** tab:

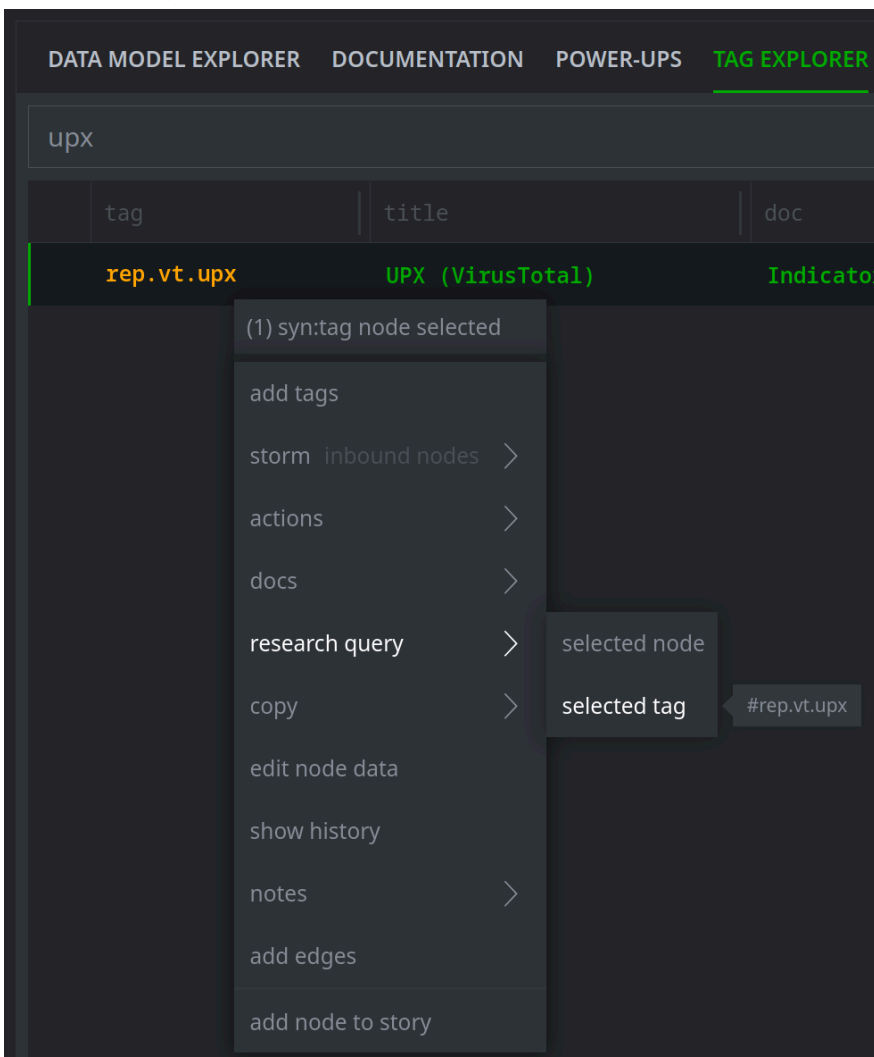


You want to look for files that are packed with the UPX packer.

- In the **Search bar**, start typing **upx**:



- From the results, **right-click** the tag **rep.vt.upx** and select **research query > selected tag**:



Question 1: How many nodes are returned by the query?