Synapse Bootcamp - Module 1

Introduction and Overview - Exercises

Objectives

In these exercises you will learn:

- Where to find and how to use Help features
- How to customize your Workspace
- How to customize your Research tool layout (Tabular display mode)

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

Your Synapse Environment

Exercise 1

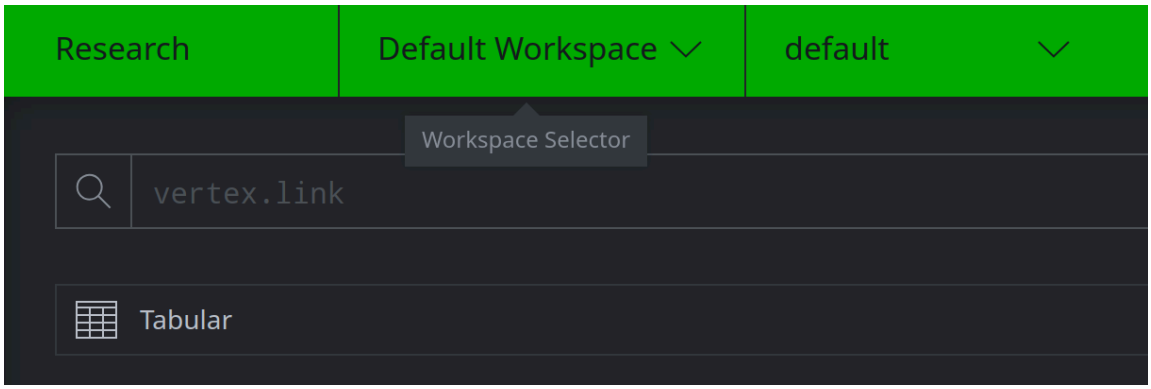
Objective:

- **Set the Workspace and View to use for Synapse Bootcamp.**

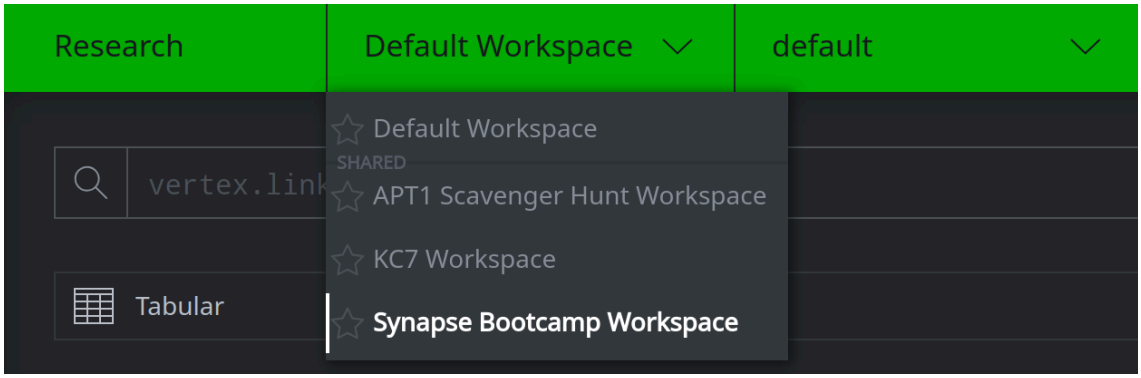
Note: If you configured your **Synapse Bootcamp Workspace** and **Synapse Bootcamp** view during class, you can **skip** to Exercise 2.

The **Top Bar** in Optic displays information about your current environment. Your instance of Synapse includes multiple data sets and configurations. We need to select the correct options for Synapse Bootcamp.

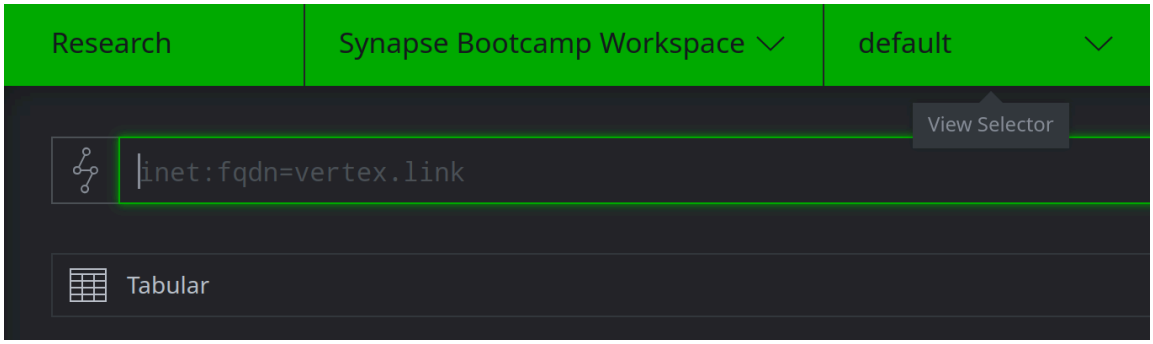
- In the **Top Bar,** locate your **Workspace Selector:**



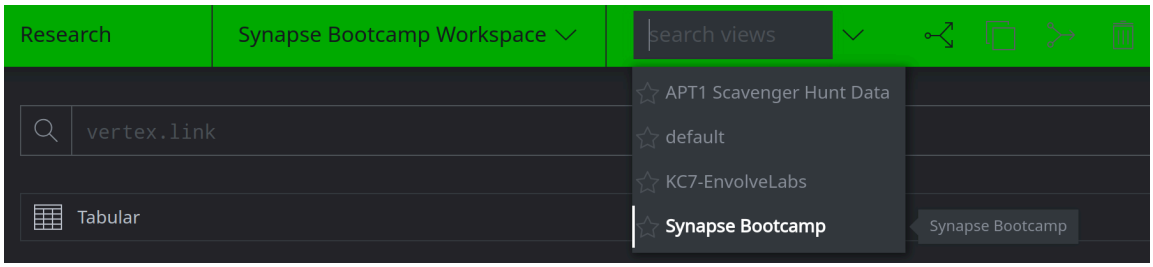
- Click the **Workspace Selector** and choose **Synapse Bootcamp Workspace** to make it your active Workspace:



- In the **Top Bar,** locate your **View Selector:**



- Click the **View Selector** and choose **Synapse Bootcamp** to make it the active view:



- Your **Top Bar** should look like this:

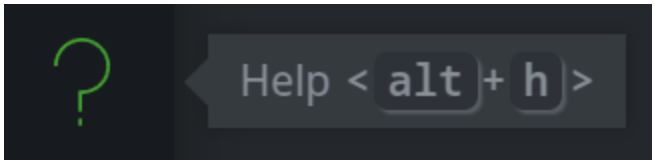
Help Tool - Data Model Explorer / Tag Explorer

Exercise 2

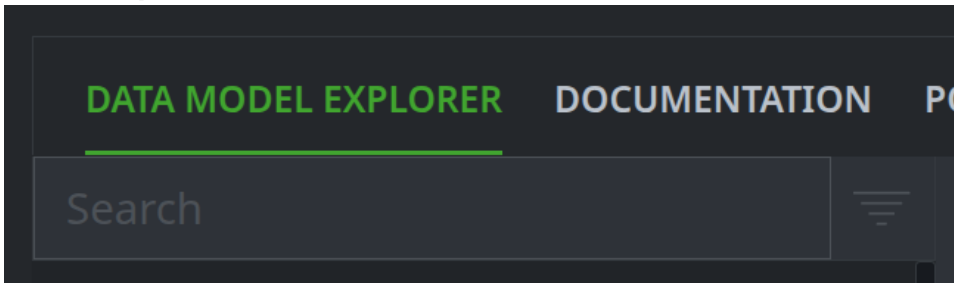
Objective:

- **Use Data Model Explorer to search, view, and lift sample forms.**

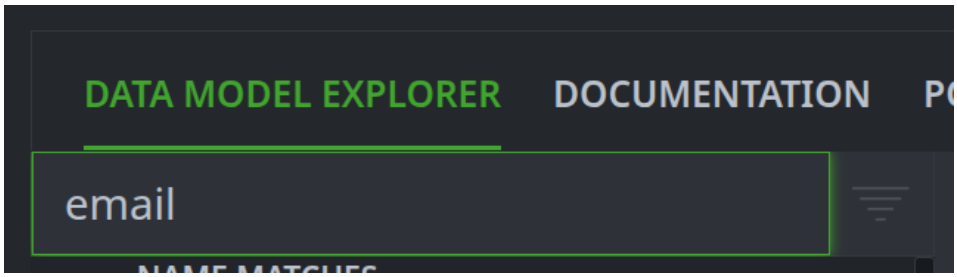
- From the **Toolbar,** select the **Help Tool:**



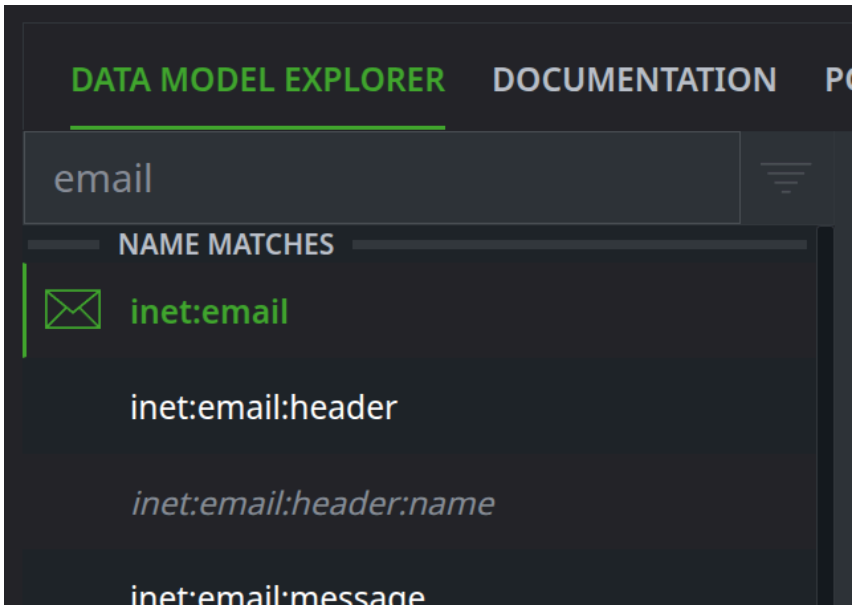
- In the **Help Tool,** select the **DATA MODEL EXPLORER** tab:



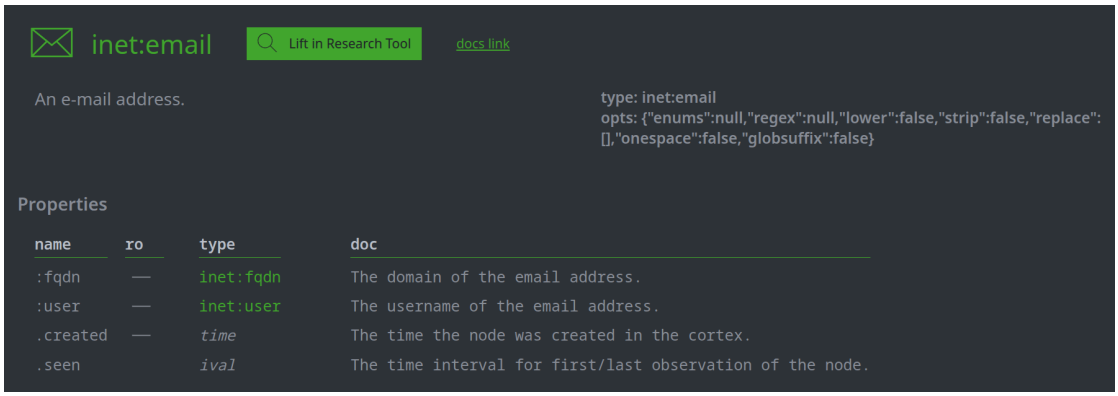
- Enter **`email`** in the *Search* field to find entries that contain this string:



- Select **`inet:email`** from the list view to see information about email addresses (**`inet:email`** forms):



- Review the **Properties** associated with an **`inet:email`** form in Synapse:



Question 1: What information can Synapse record about an email address?

- Locate the **Referenced By** header for an email address (**inet:email):**

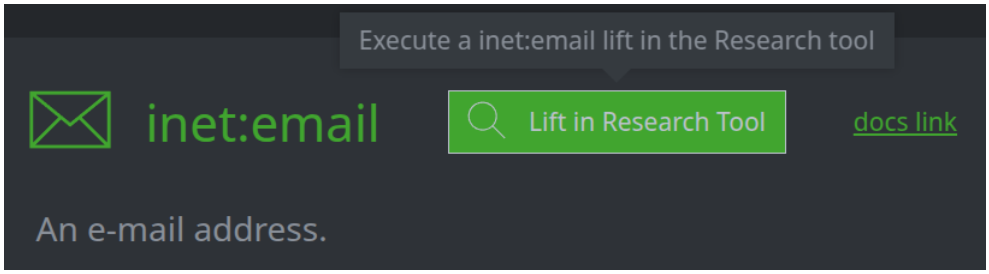
Referenced By

form	prop	doc
auth:creds	:email	The email address used to identify the user.
crypto:x509:cert	:identities:emails	The fused list of e-mail addresses identified by the cert CN and SANs.
inet:dns:soa	:email	The email address (RNAME) returned in the SOA record.
inet:email:message	:to	The email address of the recipient.
inet:email:message	:from	The email address of the sender.
inet:email:message	:replyto	The email address parsed from the "reply-to" header.
inet:email:message	:cc	Email addresses parsed from the "cc" header.
inet:rfc2822:addr	:email	The email field parsed from an RFC 2822 address string.
inet:service:account	:email	The current email address associated with the account.
inet:web:acct	:email	The email address associated with the account.
inet:web:acct	:recovery:email	An email address registered as a recovery email address for the account.
inet:whois:contact	:email	The email address of the contact.
inet:whois:email	:email	The email address associated with the domain whois record.
it:prod:soft	~~:author:email~~	Deprecated. Please use :author to link to a ps:contact.
ps:contact	:email	The main email address for this contact.
ps:contact	:email:work	The work email address for this contact.
ps:contact	:emails	An array of secondary/associated email addresses.
risk:attack	~~:via:email~~	Deprecated. Please use -(uses)> light weight edges.
risk:attack	~~:used:email~~	Deprecated. Please use -(uses)> light weight edges.
tel:mob:telem	:email	An e-mail address.

Review the items in the **form** column. These are all of the objects in Synapse (forms) that can have an email address as a **property.**

Question 2: How many email address properties are associated with an **`inet:email:message`** object?

- Click the **Lift in Research Tool** button at the top of the screen:



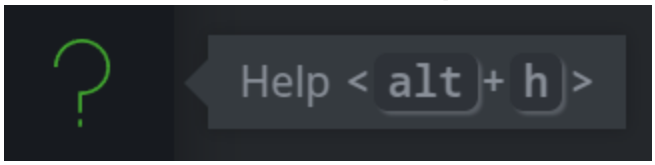
Question 3: What happens when you click the **Lift in Research Tool** button?

Exercise 3

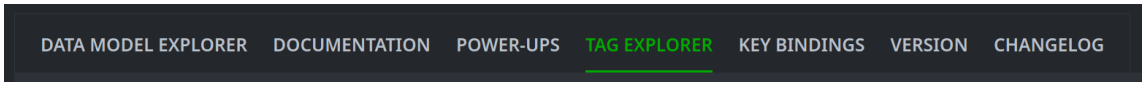
Objectives:

- **Use Tag Explorer to:**
  - **view and explore tags,**
  - **find or set tag definitions, and**
  - **lift tags and / or tagged nodes.**

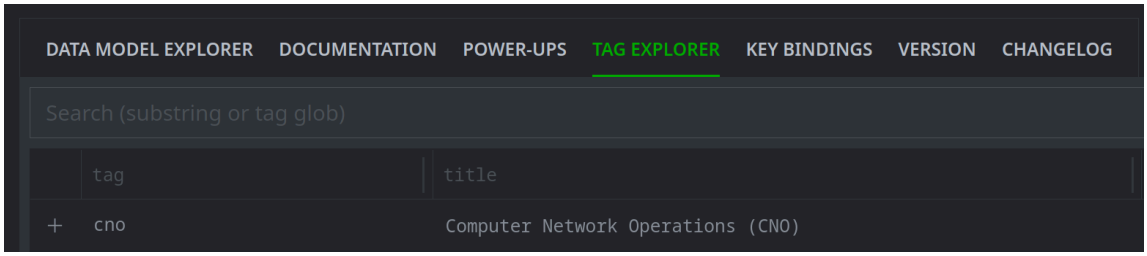
- From the **Toolbar,** select the **Help Tool:**



- In the **Help Tool,** click on the **TAG EXPLORER** tab:



- View the initial set of tags displayed:



Question 1: How many **top-level tags** have been created in your instance of Synapse?

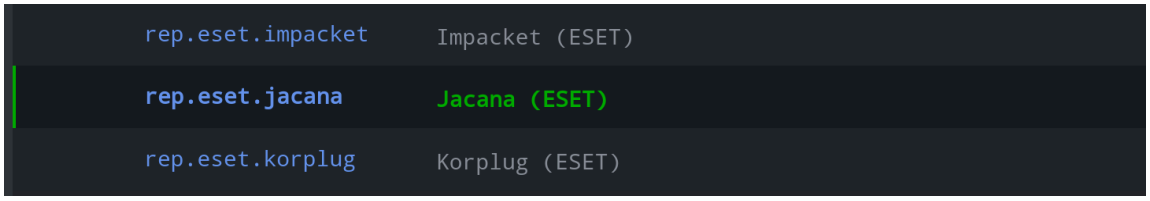
Question 2: What do these tags represent, based on their definitions?

Note: if you are unable to view the tag's full definition, you can either resize the columns or double-click the entry in the *doc* column to display an Edit dialog box where you can view (or modify) the definition.

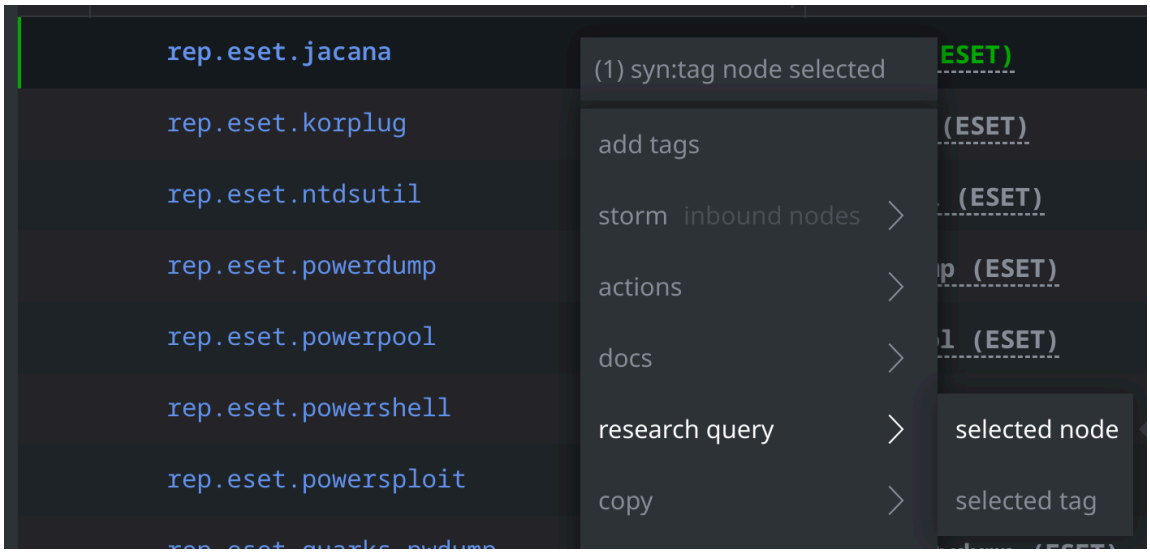
- Select the **rep** tag. Click the plus sign (**+**) next to the tag to expand the tag tree:

- Select the **rep.eset** tag. Click the plus sign (**+**) next to the tag to expand the tag tree:

- Locate the **rep.eset.jacana** tag:

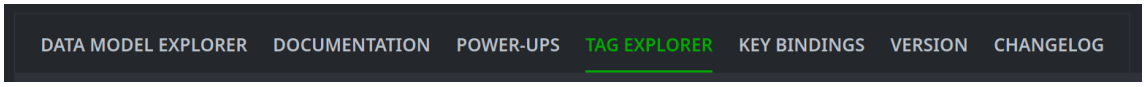


- **Right-click** the **rep.eset.jacana** tag and choose **research query > selected node** from the context menu:

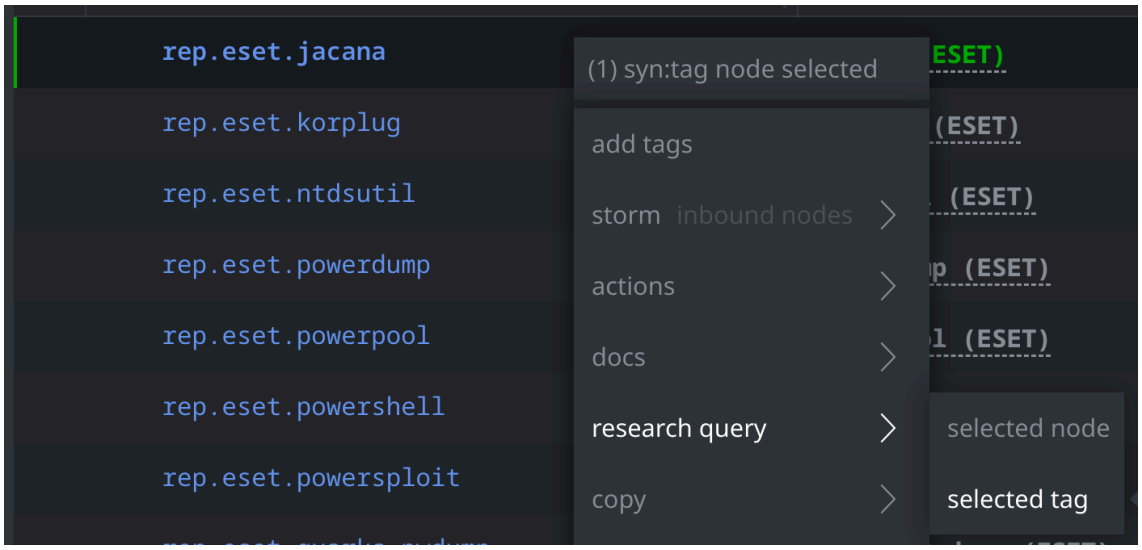


Question 3: What nodes (objects) are displayed when you select **research query > selected node ?**

- Return to the **Help Tool** and the **TAG EXPLORER** tab:



- **Right-click** the `rep.eset.jacana` tag again and choose **research query > selected tag** from the context menu:



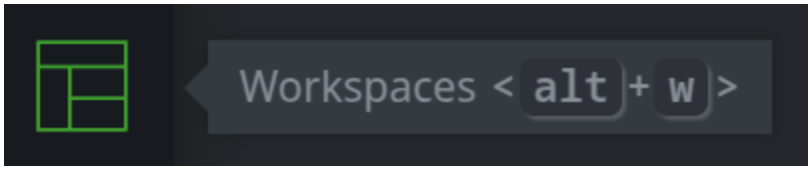
Question 4: What nodes (objects) are displayed when you select **research query > selected tag ?**

Workspaces Tool

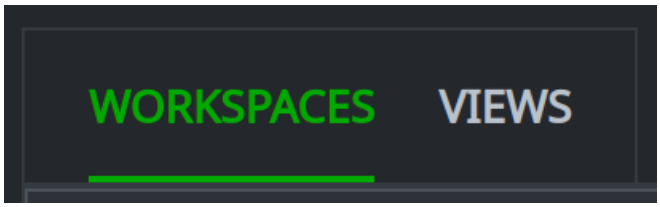
Exercise 4

Objective:
- **Customize your Synapse UI using the Workspaces tool.**

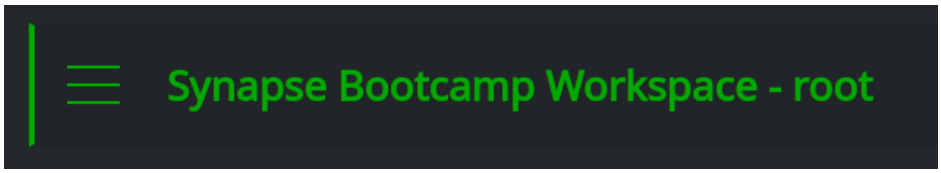
- From the **Toolbar,** select the **Workspaces Tool:**



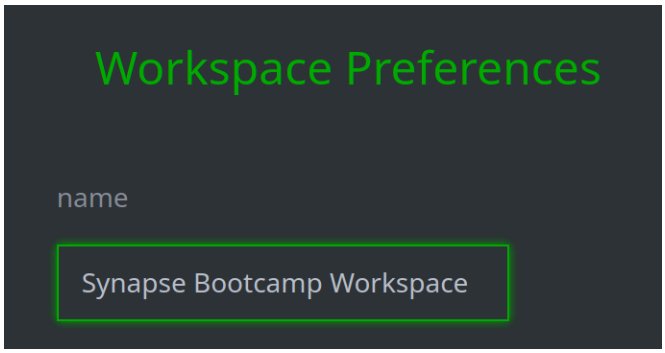
- Make sure the **WORKSPACES** tab is selected:



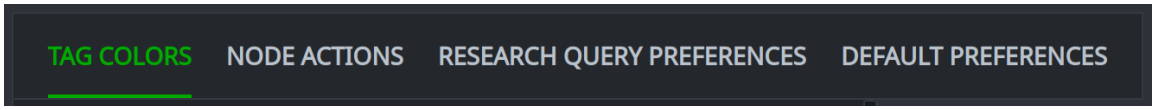
- In the **WORKSPACES** list, make sure **Synapse Bootcamp Workspace - root** is selected**:**



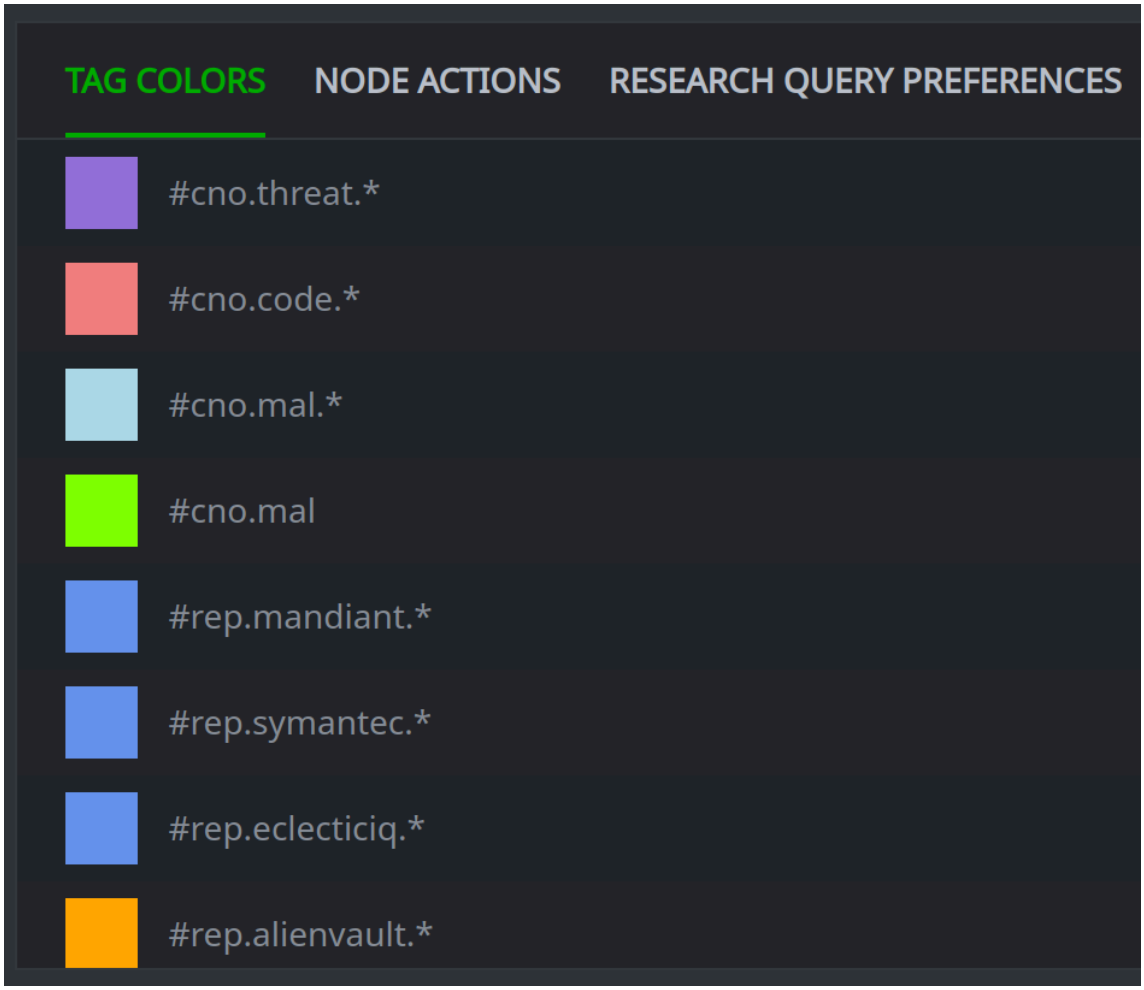
- In the **Workspace Preferences** panel on the right, note that **Synapse Bootcamp Workspace** is displayed:



- Make sure the **TAG COLORS** tab is selected:



- **Browse** the list of existing tag colors:



We want to add a tag color rule so that any node with a "TTP" tag (**cno.ttp.***) will be displayed in a custom color.

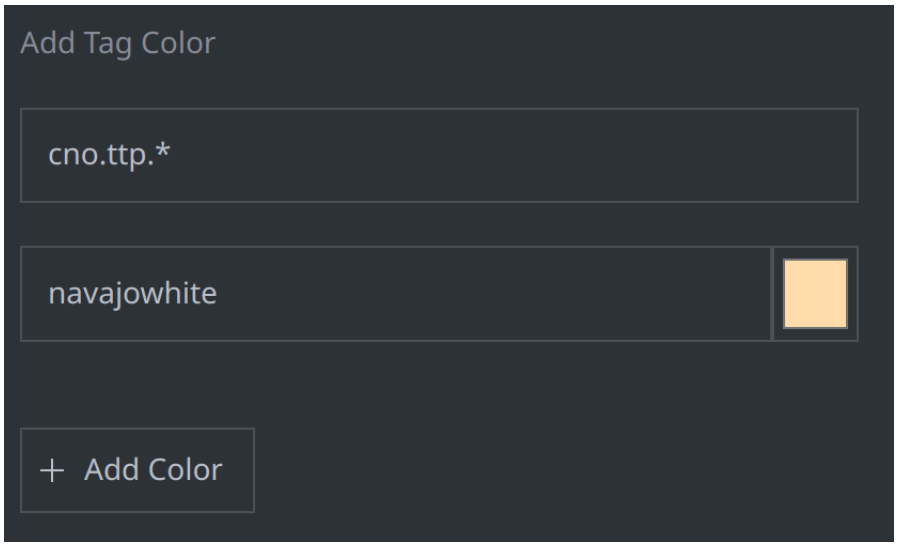
- In the **Add Tag Color** input form, enter the following in the **tag** (*foo.bar*) field:

```
cno.ttp.*
```

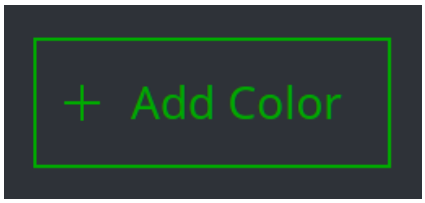
- Enter the following in the **color** (*green*) field:

```
navajowhite
```

- Your input form should look like this:

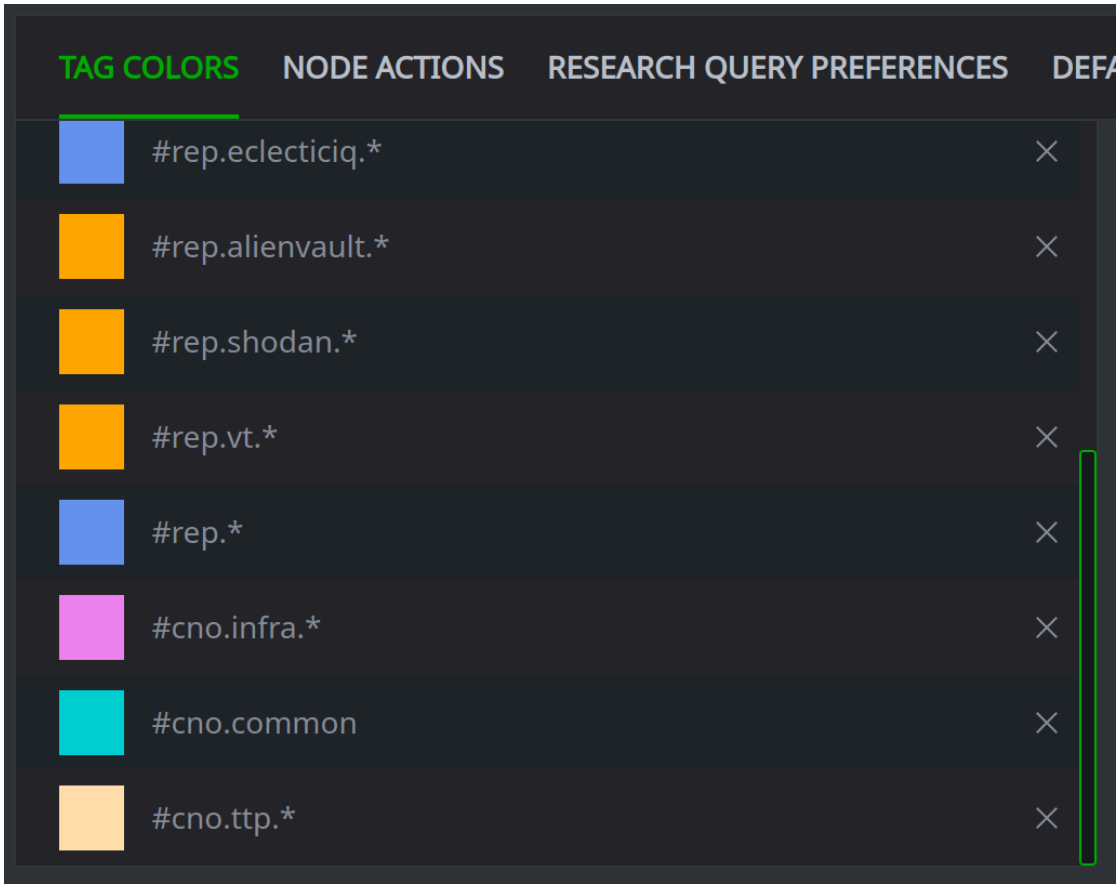


- Click the **+ Add Color** button to create the rule:



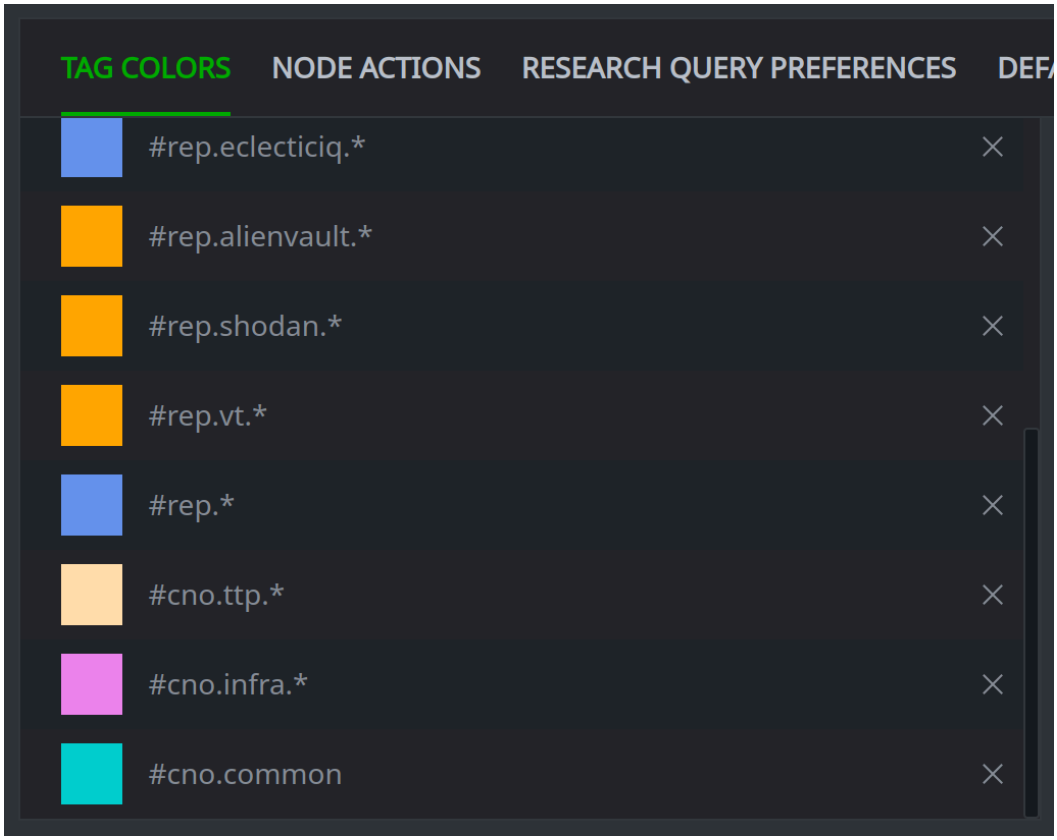
Note: Synapse recognizes common HTML colors. A list of HTML color names recognized by most browsers can be found here.

- In your tag colors, use the **scrollbar** to scroll to the bottom of the list. Your new tag rule should appear at the bottom:



It is important to us to know if a node has a **cno.ttp.*** tag. We want this tag to take precedence over some less important tags.

- **Click and hold** the tag rule for **#cno.ttp.***. **Drag** the rule up so it is between **#rep.*** and **#cno.infra.*.** Your last several rules should look like this:



Research Tool

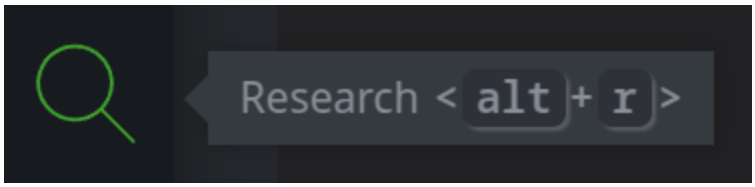
Exercise 5

Objectives:

- **Understand how to customize the layout and appearance of Tabular display in the Research tool.**
- **Know how to add, remove, and reset columns using:**
  - **standard controls from the Details Panel (Node tab), and**
  - **column / form menus.**

View the default columns displayed for an object (form).

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



- Ensure your **Storm Query Bar** is in **Lookup mode** and your display mode is set to **Tabular:**

- Enter the following into the **Storm Query Bar** and press **Enter** to run the query:

```
| inet:dns:a | limit 10
```

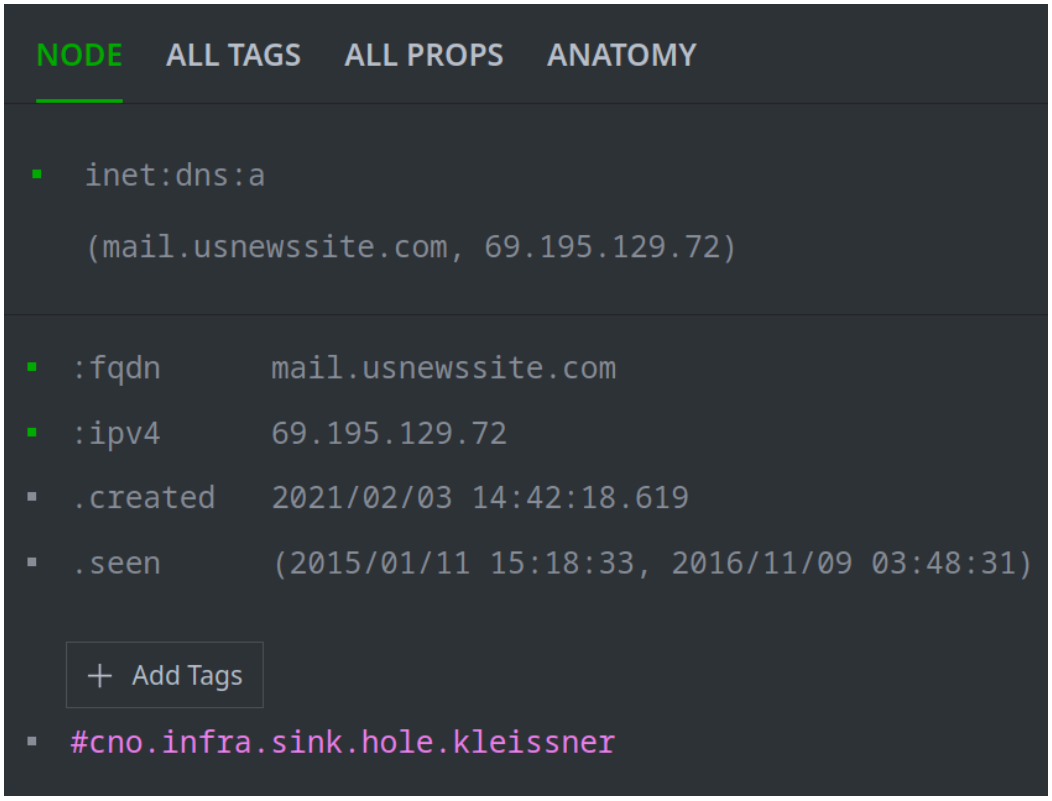
This query returns 10 nodes representing DNS A records. Each **row** in the **Results Panel** represents an individual result (**node**).

Question 1: What **columns** are displayed in the **Results Panel** for the DNS A records?

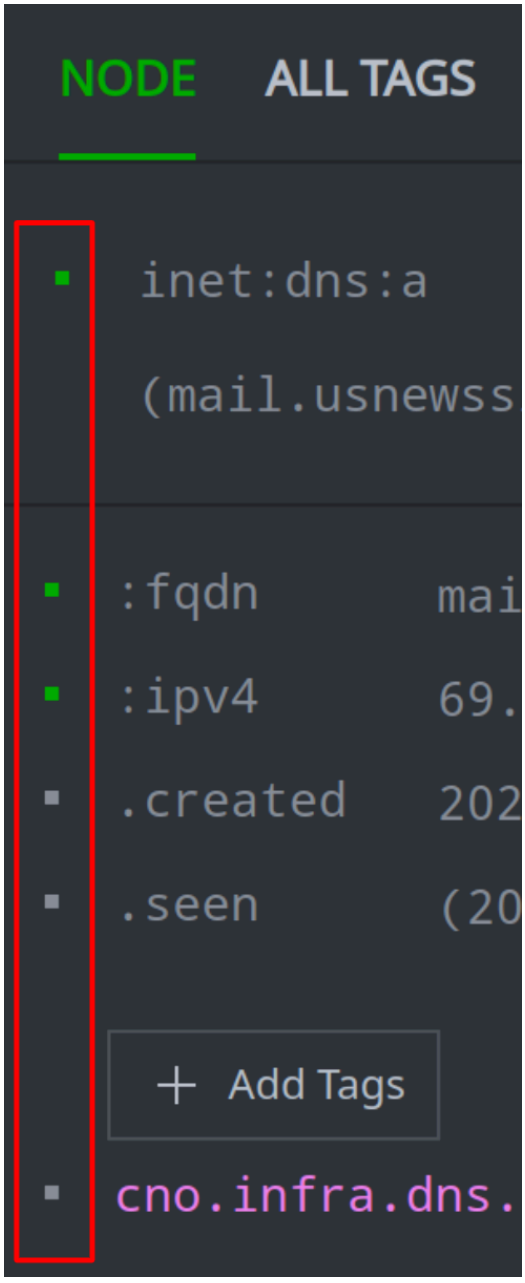
Add columns to your display from the Details Panel.

- Click any node (row) in the **Results Panel** to select it:

- In the **Details Panel,** select the **NODE** tab to view the properties (and tags, if present) for the node you selected:



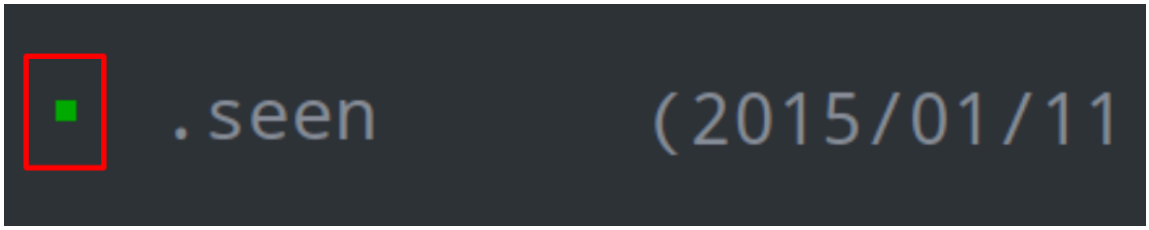
- Note the small square next to each item (property or tag) in the **Details Panel:**



A **green** square indicates the item is **selected** (toggled on) and **displayed** in the Results Panel.

A **gray** square indicates the item is **not selected** (toggled off) and **not displayed.**

- Click the square next to the **.seen** property to toggle it on:

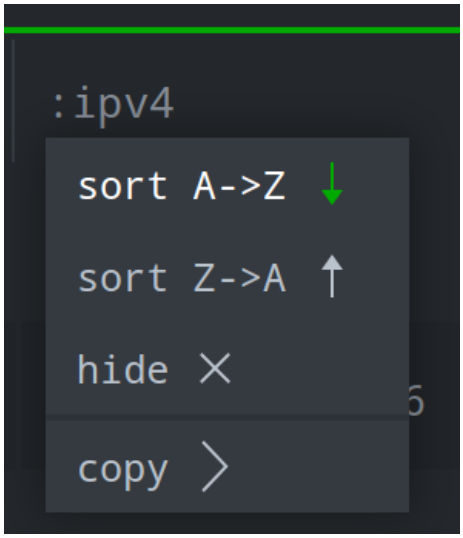


Question 2: How does the **Results Panel** change when you toggle on the **.seen** property?

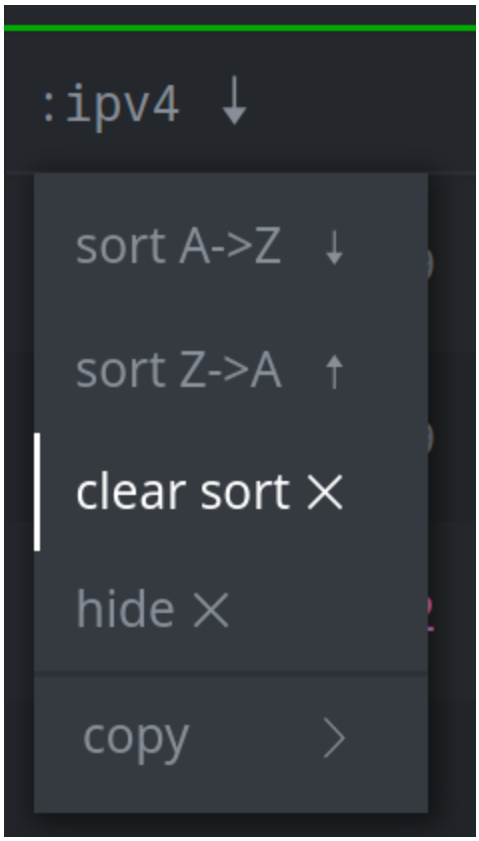
Practice working with the columns display.

- **Click and drag** the borders between the column headers to resize the columns:

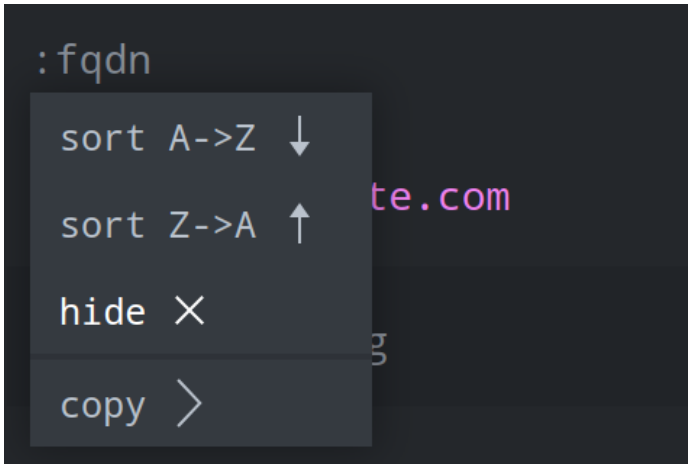
- Use the **dropdown menu** from any column header to sort the column (**sort A->Z** or **sort Z->A**):



- Your sort order will **persist** (including across queries and sessions) until you remove it. Use the **clear sort X** option to remove your sort order:

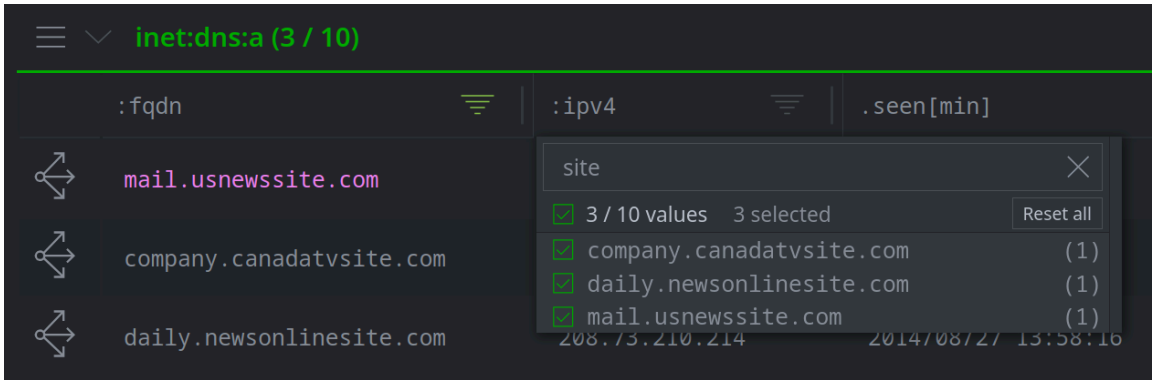


- Use the **hide X** option to remove a column:

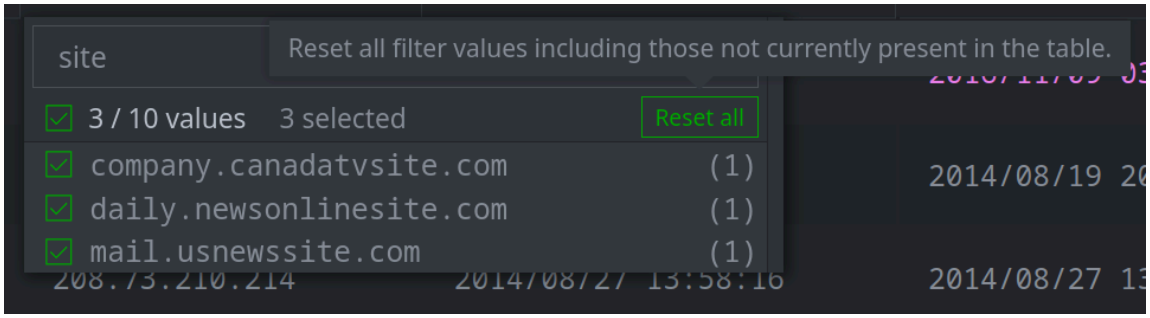


Tip: you can add the column back again from the **Details Panel**:

- Examine the **filter** option to display a subset of your results:



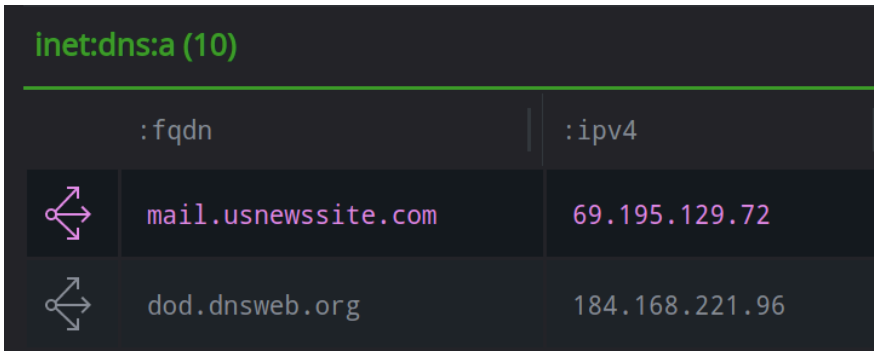
- Any filter will **persist** (including across queries and sessions) until you remove it. Use the **Reset all** button to remove any filters:



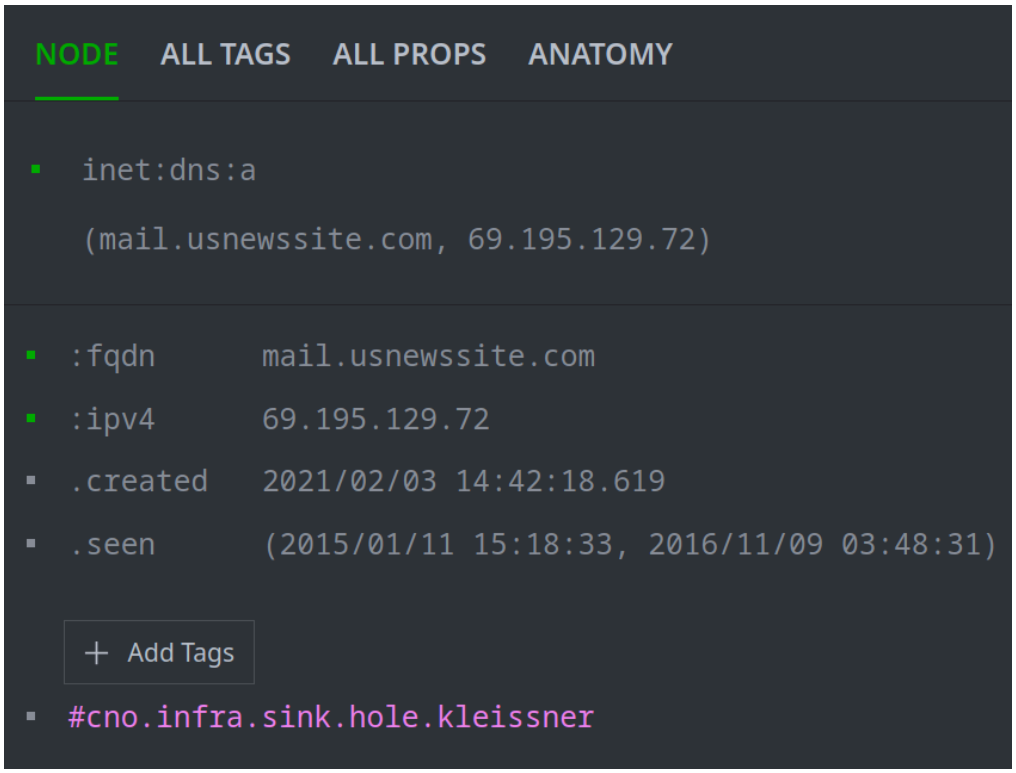
Tip: We will revisit filtering in Module 3!

See how the display changes when you add a tag from the Details Panel.

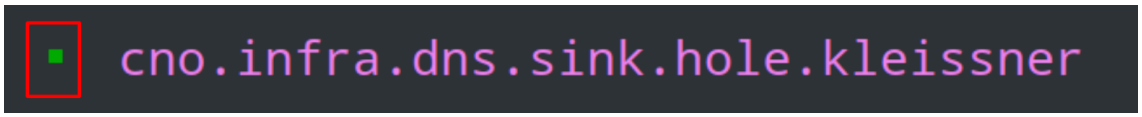
- **Select** the DNS A record for the FQDN **`mail.usnewssite.com`**:



- View the **Details Panel** (**NODE** tab) for this node:



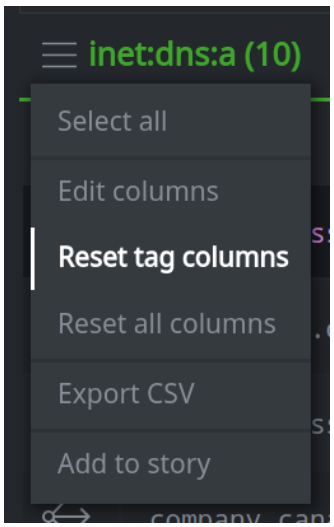
- Locate the tag **`cno.infra.dns.sink.hole.kleissner`**. Click the square next to this tag to toggle it on:



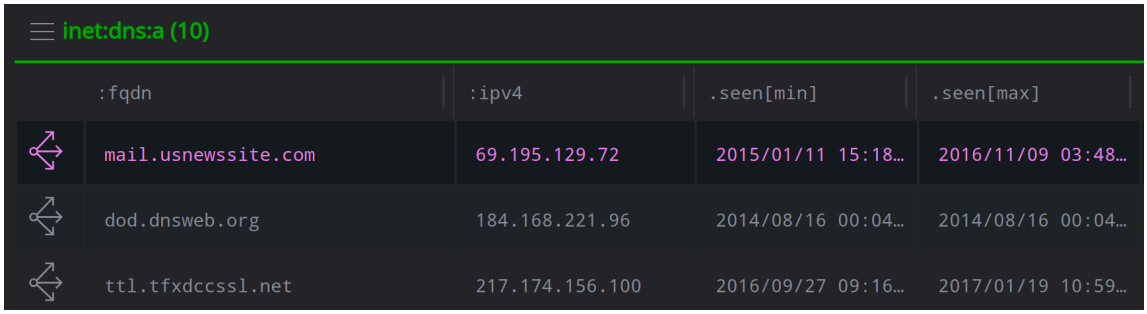
Question 3: How does the **Results Panel** change when you toggle on the **`cno.infra.dns.sink.hole.kleissner`** tag?

Remove the tag columns from your display.

- Click the **hamburger menu** next to the **`inet:dns:a`** header and select **Reset tag columns** to remove the tag columns:



Your display should now include the **:fqdn, :ipv4,** and **.seen[min]** and **.seen[max]** columns again:



Tip: When you change anything related to the columns displayed in Tabular mode, Synapse saves those changes as part of your current **Workspace.** The changes will remain unless you modify them again.

If you have more than one Workspace configured, changes made to one do not affect any others.

Your **Synapse Bootcamp Workspace** has been configured in advance to display useful columns for this class.

Exercise 6

Objectives:

- **Understand how to customize Tabular display in the Research tool.**
- **Know how to add and remove properties from the All Props tab of the Details Panel.**
- **Know how to modify columns using the Edit columns menu option.**

Part 1 - Use the Details Panel to view nodes

- Ensure your **Storm Query Bar** is in **Lookup mode** and your display mode is set to **Tabular:**

- Enter the following into the **Storm Query Bar** and press **Enter** to run the query:

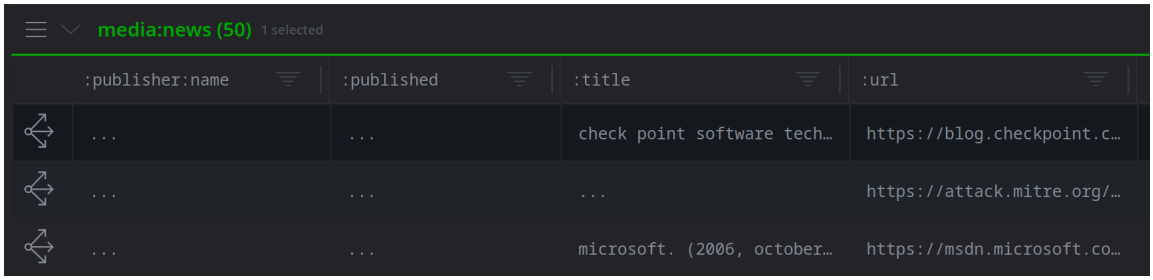
```
| media:news | limit 50
```

This query returns 50 **`media:news`** nodes. Synapse uses these nodes to represent articles or publications.

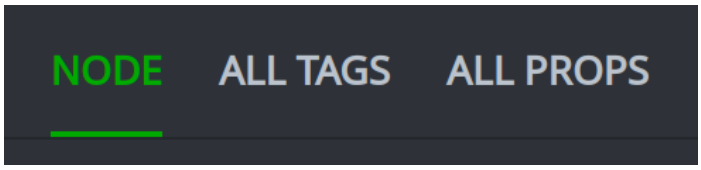
Question 1: What columns are displayed in the **Results Panel** for the **`media:news`** nodes?

View the columns (properties) displayed for **`media:news`** nodes.

- In the **Results Panel, select** any node:



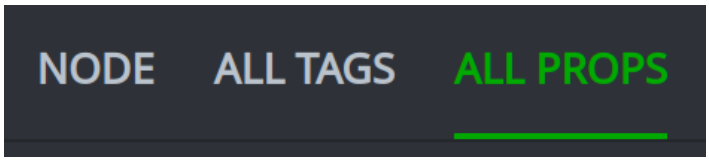
- In the **Details Panel,** select the **NODE** tab:



Question 2: What properties are **set** for the **`media:news`** node you selected?

Examine the differences between the **NODE** tab and **ALL PROPS** tab.

- In the **Details Panel,** click the **ALL PROPS** tab:



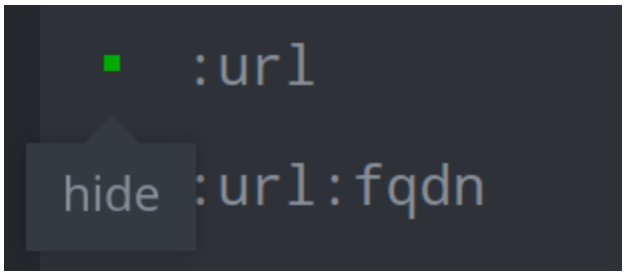
Question 3: What properties are **available** for this **`media:news`** node (that is, what additional properties **could** be set for this node)?

Part 2 - Use the Details Panel to modify your Tabular mode display

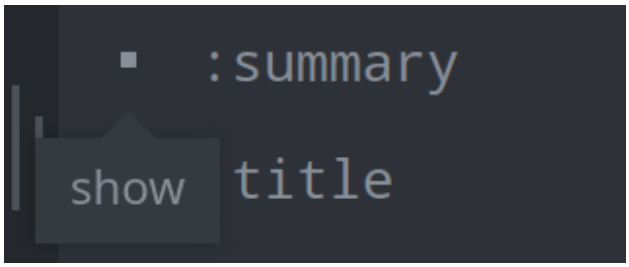
Practice using the **ALL PROPS** tab to change the columns displayed in your Results Panel.

- On the **ALL PROPS** tab, use the toggle squares to **add** or **remove** properties from your Results Panel.

  For example:



Or:



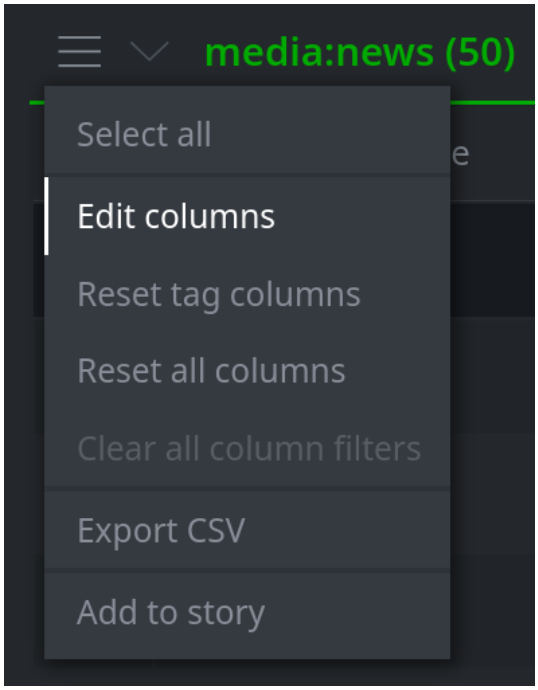
Note: When adding columns from the **Details Panel,** new columns are always added on the **right** in the **Results Panel.** (You may need to resize your columns to view new columns).

The only exception is when you add a node's **primary property.** The primary property is always added on the **left.**

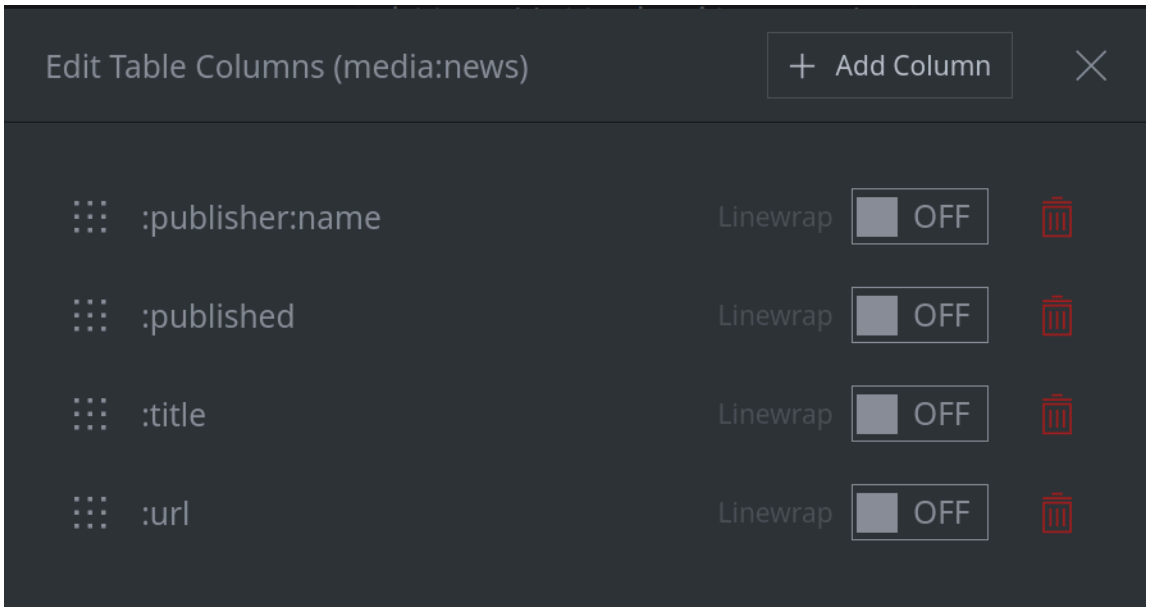
Part 3 - Use the Edit Columns menu to modify your Tabular mode display

Use the **Edit columns** menu to change the layout of your Results Panel.

- In the **Results Panel,** click the **hamburger menu** next to the **media:news** header and choose **Edit columns**:



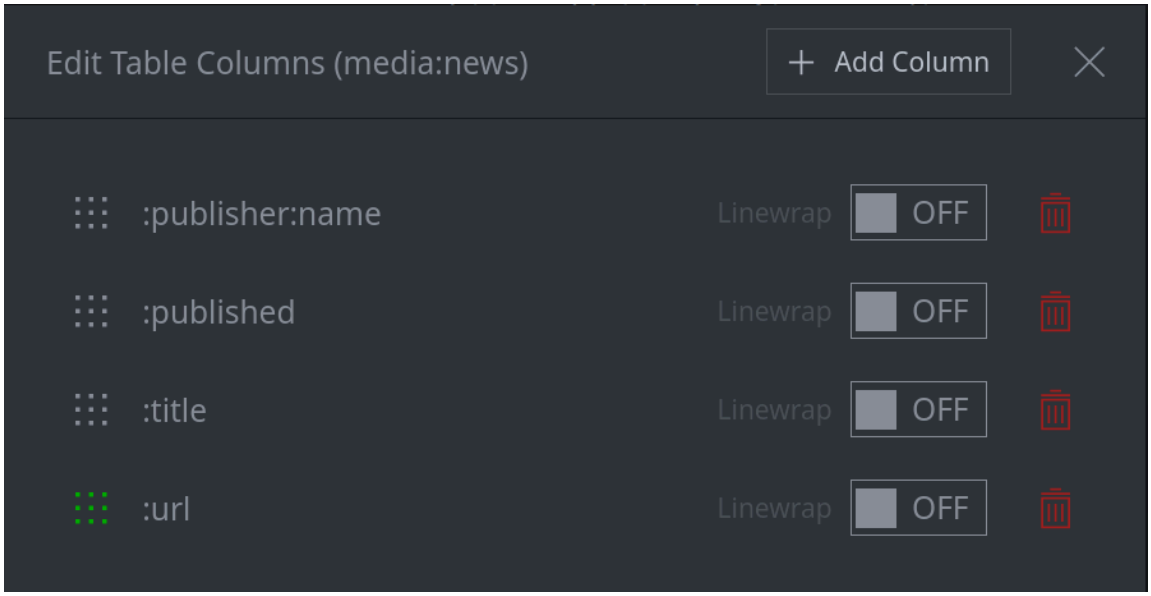
- The **Edit Table Columns** dialog box provides another way to add, remove, and customize the columns in your **Results Panel:**



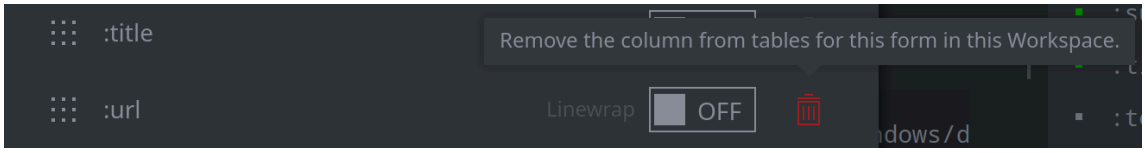
The **Edit Table Columns** dialog gives you more flexibility to add and configure columns.

Practice using the options in the dialog box.

- **Click** and **hold** any entry to **drag** it and change the order of the columns:



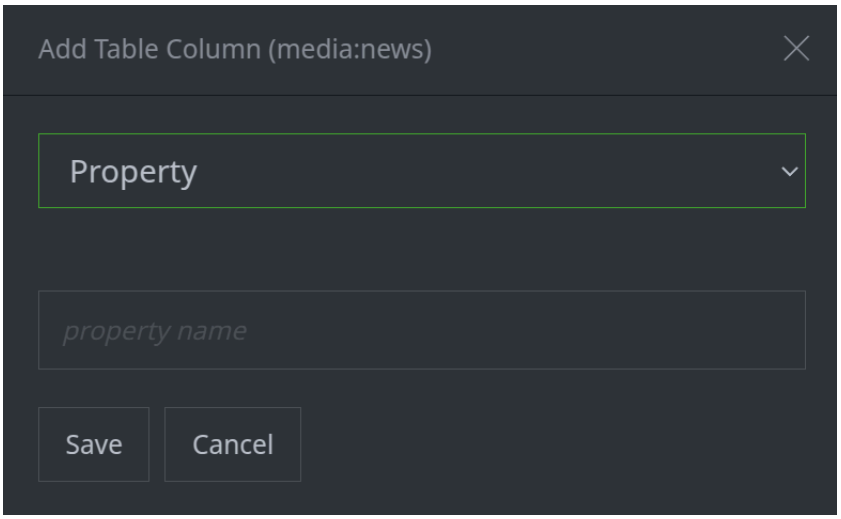
- Click the **red trash can** icon next to any entry to remove it:



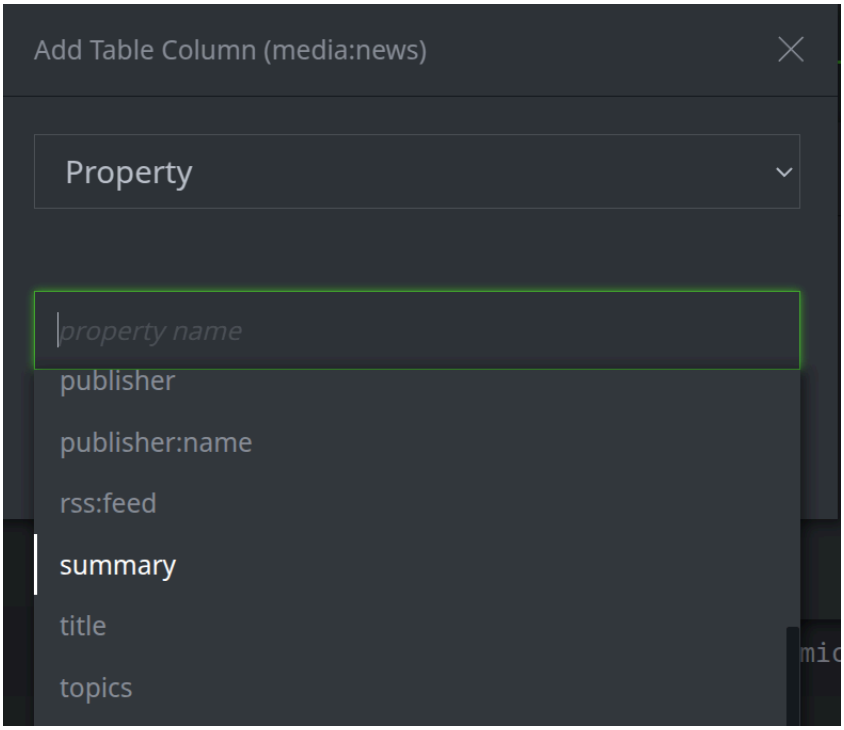
- Toggle the **Linewrap** switch on and off to wrap text within a given column:

- Click the **+ Add Column** button to add a **Property** column to your display:

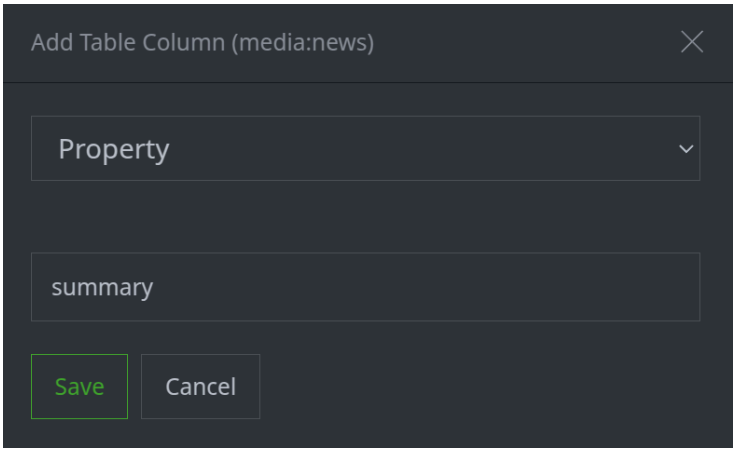
    - From the **Add Table Column** dialog, choose **Property** from the **Column Type** dropdown list:



- **Select** a property to add:



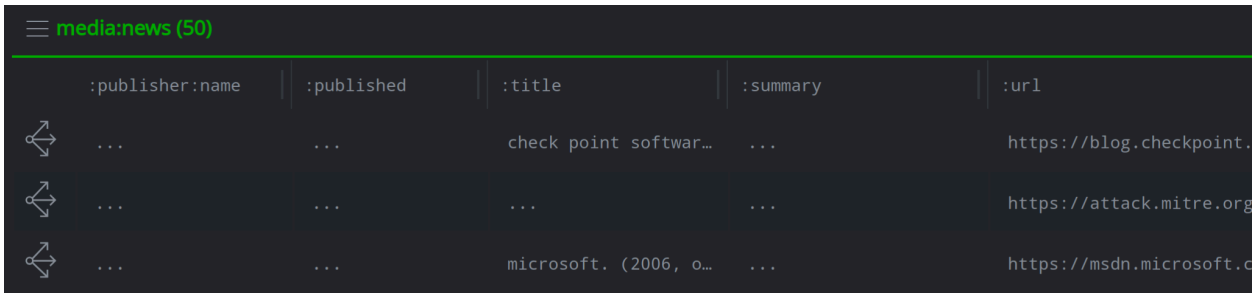
- Click **Save** to add the property:



Tip: You can learn about other types of columns in the **Synapse UI User Guide**.

- When you are done testing, **reset** your display for **media:news** nodes to display the following columns:
  - **:published**
  - **:publisher:name**
  - **:title**
  - **:summary**
  - **:url**

  Your columns should look like this:



Console Help

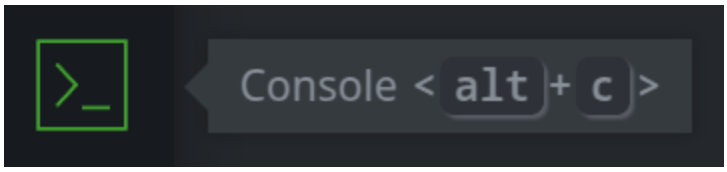
Exercise 7

Objective:

- **Understand how to use the Console Tool to:**
  - **list available help,**
  - **search for specific commands, and**
  - **display help / options for individual commands.**

View all of the commands available in Synapse.

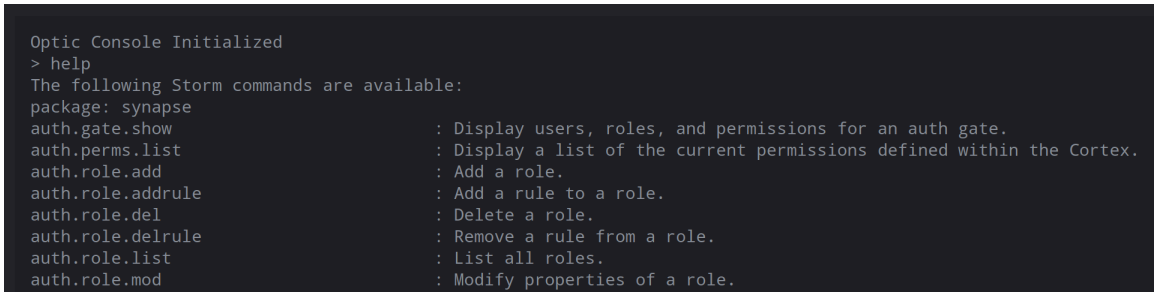
- From your **Toolbar,** select the **Console Tool:**



- In the **Console Tool,** enter the following in the **Storm Query Bar** at the bottom of the display and press **Enter** to run the command:

```
help
```

- **Browse** the available commands:



Search for commands that contain a string.

- Enter the following in the **Storm Query Bar** and press **Enter** to run the command:

```
help min
```

Question 1: What commands / package(s) / Power-Up(s) are displayed?

View help for a specific command.

- Enter the following in the **Storm Query Bar** and press **Enter** to view the help for the **min** command:

```
min --help
```

Question 2: What does the **min** command do?
