

Synapse Bootcamp - Module 4

Modifying and Adding Data - Exercises

Modifying and Adding Data - Exercises	1
Objectives	1
Exercises	3
Modifying Data	3
Exercise 1	3
Adding and Removing Tags	12
Exercise 2	12
Adding Data using Lookup Mode	18
Exercise 3	18
Creating a Node with the Add Node Dialog	26
Exercise 4	26

Objectives

In these exercises you will learn:

- How to use edit options to set or modify properties
- How to delete properties
- How to add and remove tags
- How to add data using the Storm Query Bar in Lookup mode
- How to create a node using the Add Node dialog

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

Modifying Data

Exercise 1

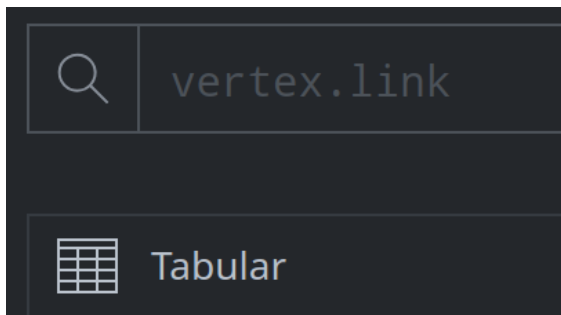
Objectives:

- Use the Details Panel to edit a node (set a property).
- Use the Results Panel to edit a node (set a property).
- Understand how to set an array (multi-value) property.
- Use the Details Panel to delete a property.

Part 1

We want to add additional information to Synapse about the company Kaspersky Lab.

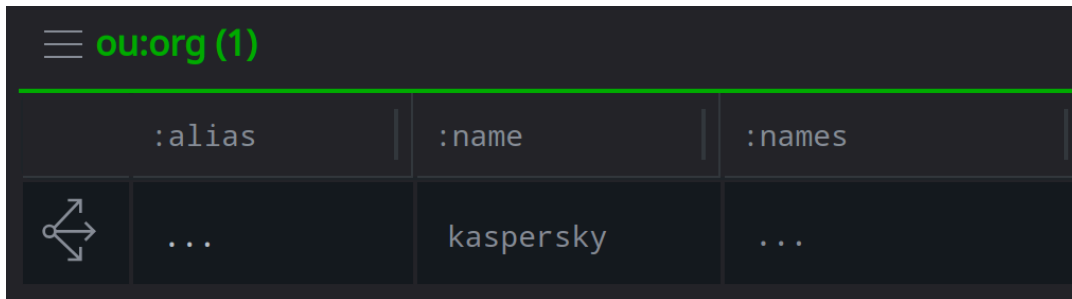
- In the **Research Tool**, ensure your **Storm Query Bar** is in **Lookup mode** and your display mode is set to **Tabular**:




Run the following query to lift the organization node for Kaspersky Lab:

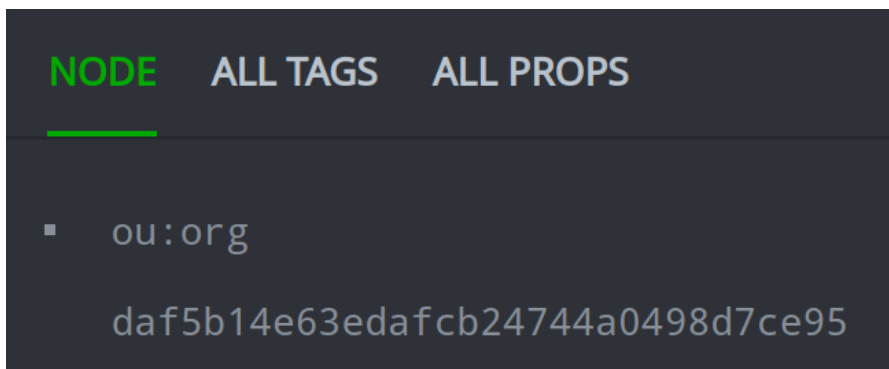
```
| ou:org:name=kaspersky
```

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



ou:org (1)			
	:alias	:name	:names
	...	kaspersky	...

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



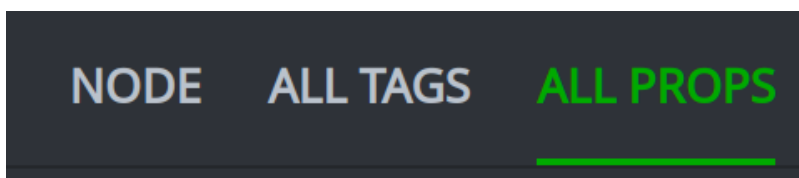
NODE ALL TAGS ALL PROPS

▪ ou:org

daf5b14e63edafcb24744a0498d7ce95

Question 1: What properties are currently set on the **ou:org** node for Kaspersky Lab?

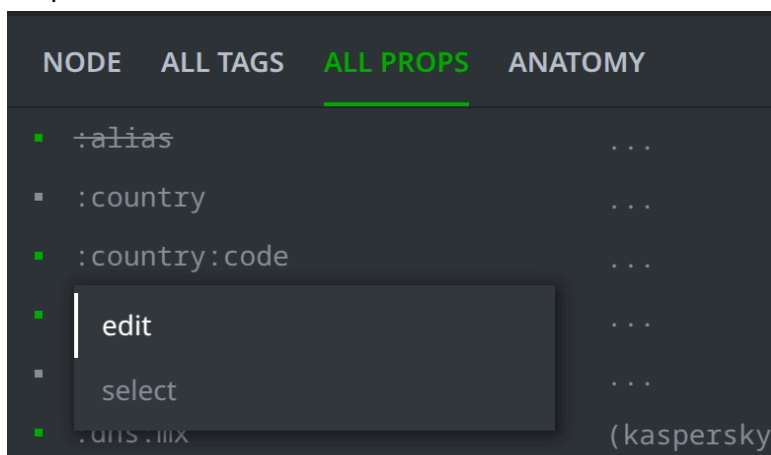
In the **Details Panel**, click the **ALL PROPS** tab:



NODE ALL TAGS **ALL PROPS**

The **ALL PROPS** tab shows you all **available** properties for the node, including ones that are not currently set / do not have a value.

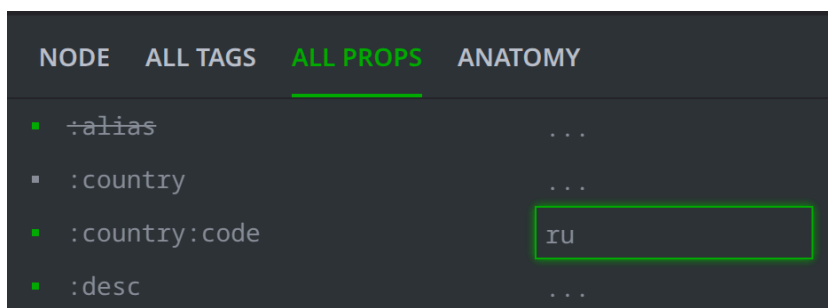
On the **ALL PROPS** tab, click the **:country:code** property. Select **edit** from the drop-down menu:



Enter the following in the **:country:code** field for Kaspersky Lab:

ru

Press **Enter** to save your change:



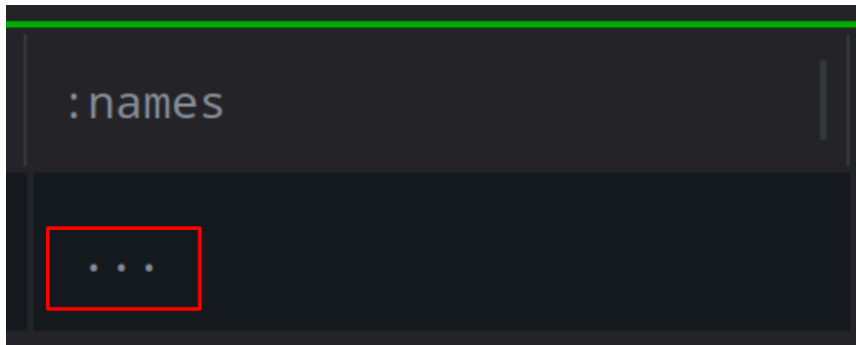
Question 2: When you save your change in the Details Panel, what happens to the **:country:code** column in your **Results Panel**?

Part 2

Kaspersky Lab is located in Russia. We want to record the company name in both English and Russian (Cyrillic).

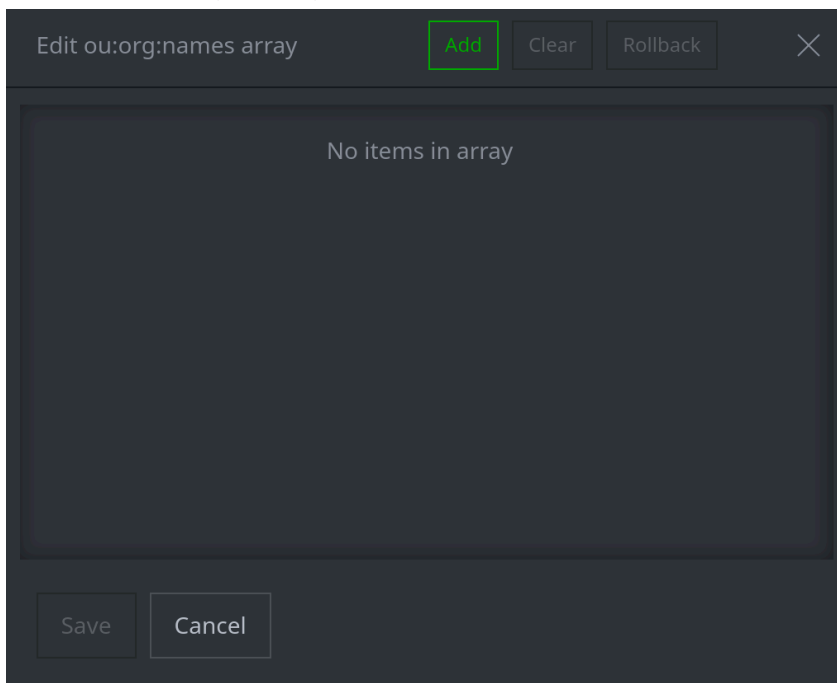
- **Select** the node for Kaspersky Lab.

- In your **Results Panel**, **double-click** the three dots in the **:names** column to open the **Edit array** dialog:

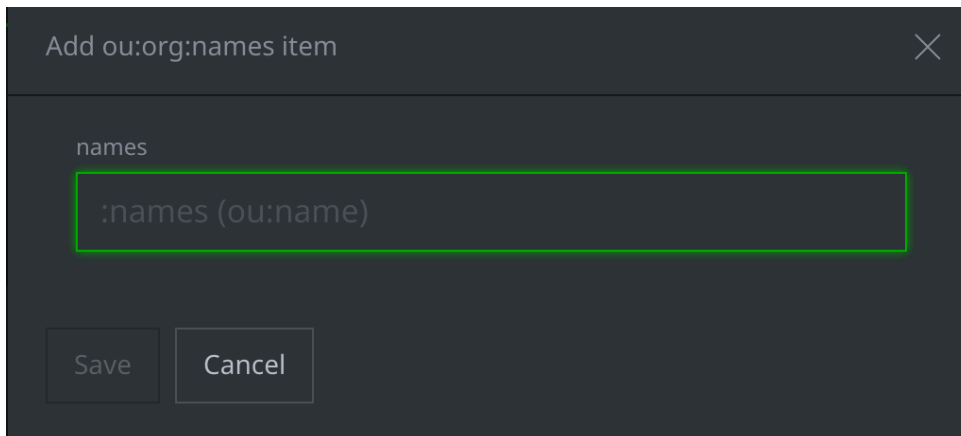


Note: if the **:names** property is not displayed, use the [Details Panel](#) or the [Edit Columns](#) menu to add the column.

- In the **Edit array** dialog, click the **Add** button:



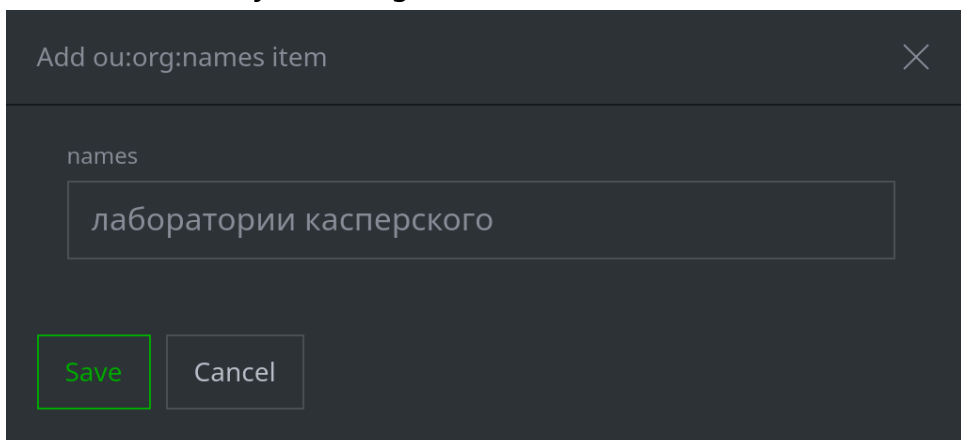
- The **Add item** dialog will appear:



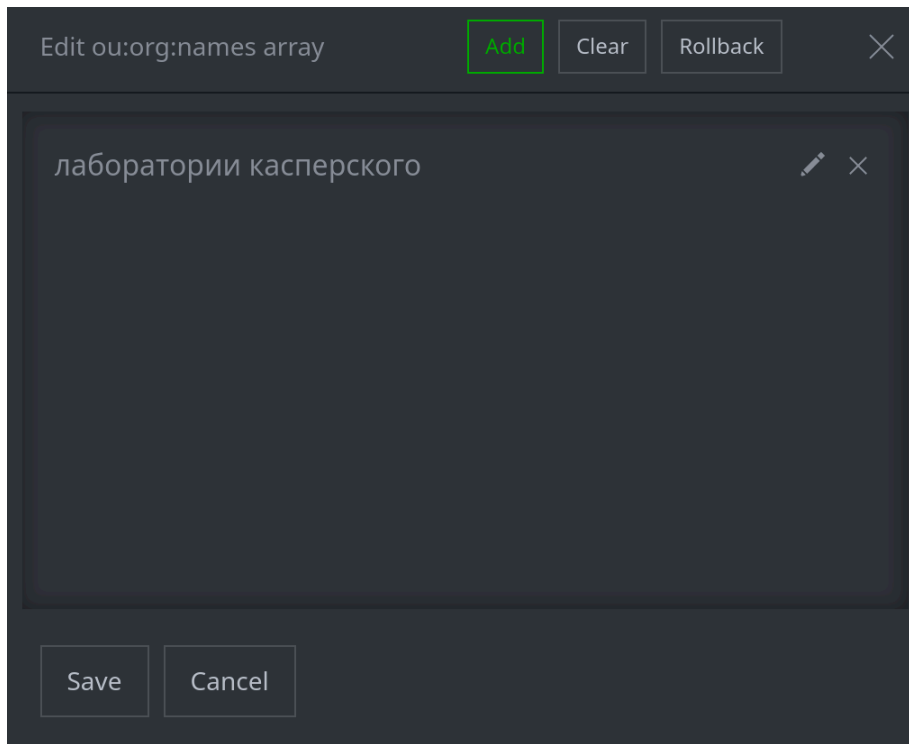
- In the **Add item** dialog, enter the Russian name for Kaspersky Lab:

Лаборатория Касперского

- Click **Save** to save your change:



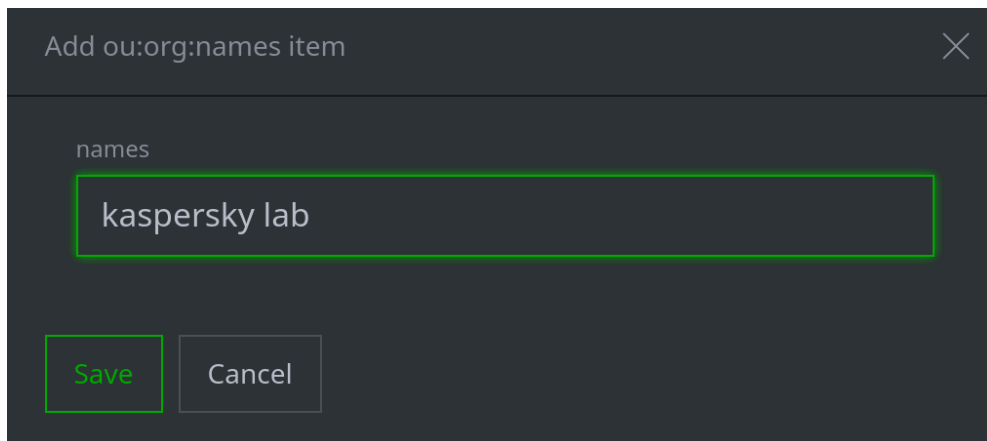
- In the **Edit array** dialog, click the **Add** button to add another name:



- In the **Add item** dialog, enter another variation on the company name:

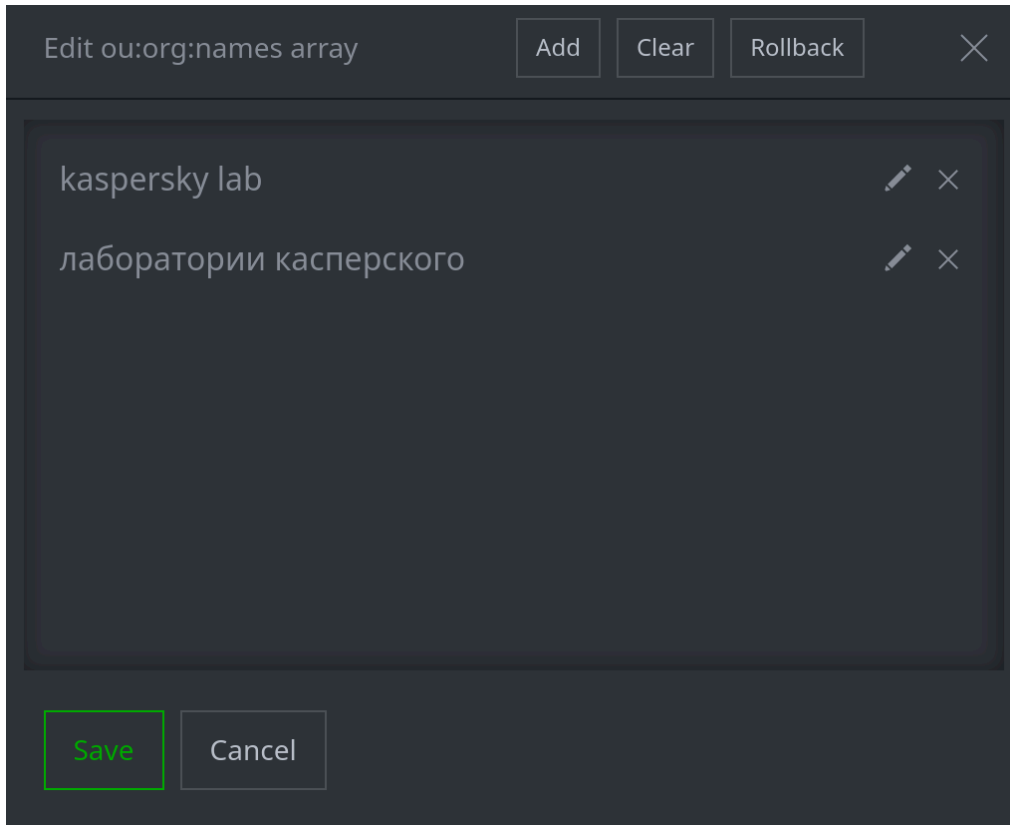
kaspersky lab

- Click **Save** to save your change:



Question 3: What does the **Edit array** dialog look like?

- In the **Edit array** dialog, click the **Save** button to save your changes:

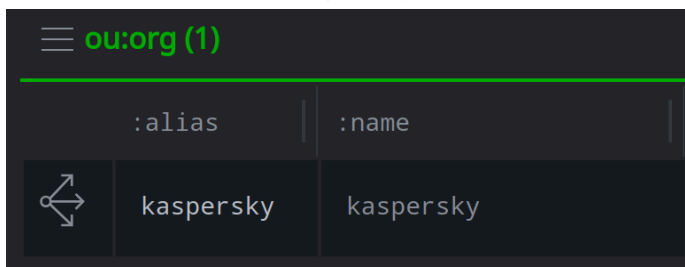



Question 4: In your **Results Panel**, how did the **:names** column change?

Part 3

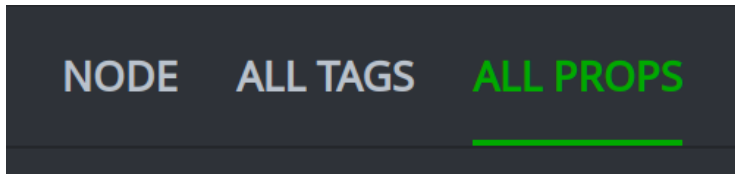
According to Kaspersky Lab's website, the company was founded on **June 26, 1997**. We want to add this information to the organization (**ou:org**) node for Kaspersky Lab.

- **Select** the node for Kaspersky Lab:

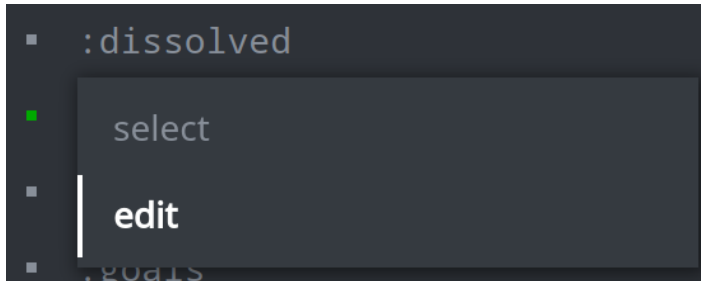


ou:org (1)		
	:alias	:name
	kaspersky	kaspersky

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



- In the **ALL PROPS** tab, click the **:dissolved** property and choose **edit**:



We will set the wrong property on purpose (:dissolved vs. :founded).

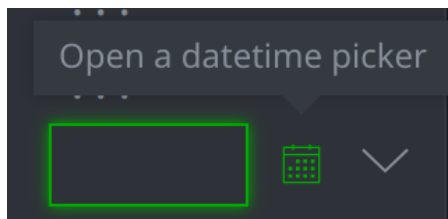
- In the **edit** field, enter the date Kaspersky Lab was founded (in YYYY/MM/DD format):

1997/06/26



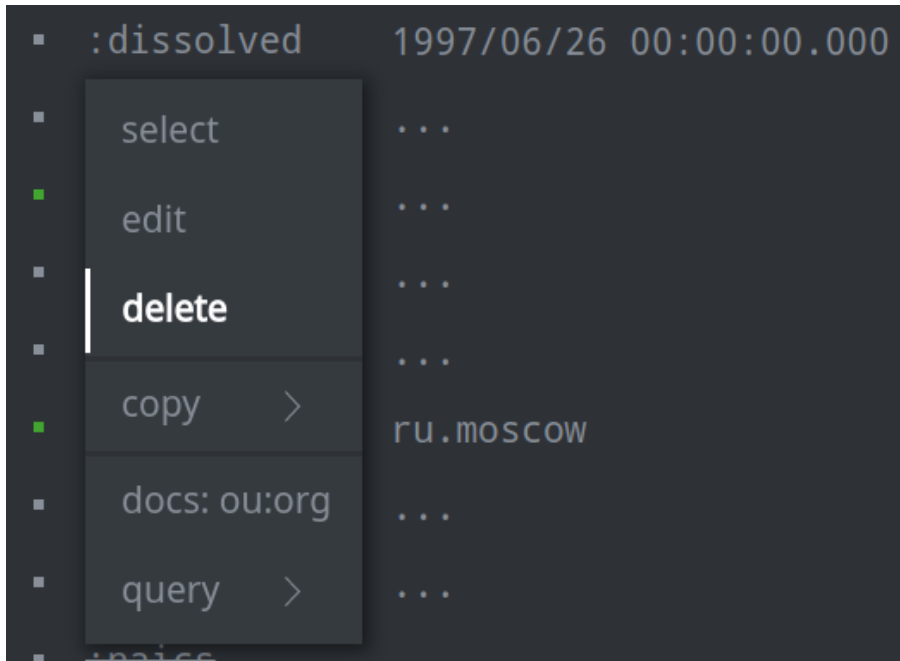
Press **Enter** to save your change.

Note: you can optionally select the **datetime picker icon** (the small calendar icon) to enter the date using the datetime picker:

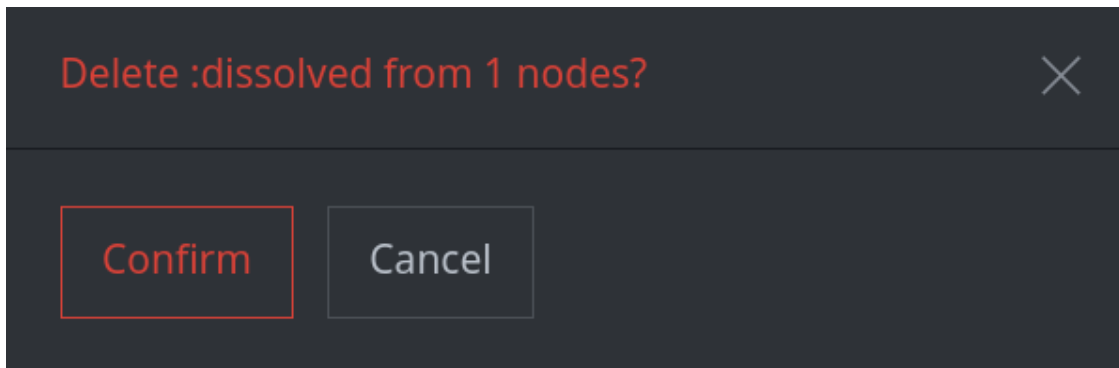


Oops...we need to fix our error.

- In the **ALL PROPS** tab, click the **:dissolved** property and choose **delete** from the dropdown menu:



- Click **Confirm** to delete the **:dissolved** property:



Adding and Removing Tags

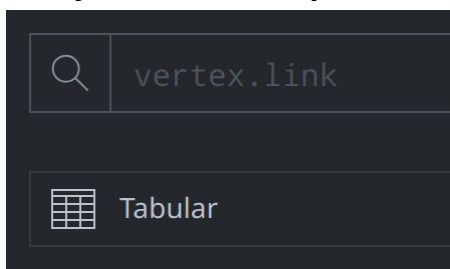
Exercise 2

Objectives:

- Use the context menu to add tags.
- Understand how to add tags to multiple nodes.
- Use the Details Panel to remove tags from nodes.

In our exercises on Filtering, we identified several files that make DNS queries for subdomains of the APT1 FQDN **earthsolution.org**. We want to revisit those files.

- In the **Research Tool**, ensure your display mode is set to **Tabular** and your **Storm Query Bar** is in **Lookup** mode.



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

```
|  
file:bytes=2c5dd8a64437cb2dd4b6747139c61d2d7f53ab3ddedbf22df3cb  
01bae170715b  
file:bytes=a1694725158441219fae3f96aa6b345f610195995568c9409cf5  
c9aac029c51a  
file:bytes=1b32e6800b3a80e74f135b75925f3c1e081662adf53262ec9a  
8a830398ff64  
file:bytes=289aa8624ae2ca8485b9a8b73b920c6a53a796426f0da8befd19  
bc085c7055fc  
file:bytes=65c4ea8e926bb975d3f905157b33b24b30d6bd5cd22278b89222  
169c0216b606
```

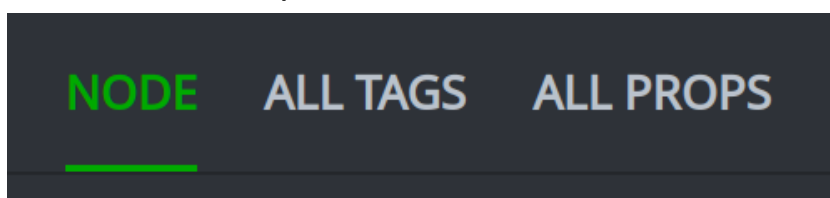
Note: The wrapped lines (above) may create **spaces** in your pasted Storm query. If your query does not run properly, you will need to remove any extra spaces in the SHA256 values.

You may be able to retrieve this query (which we ran in an earlier Module) by clicking the **Storm Query Bar Menu > History** and locating the query in your Lookup mode history.

All five files query subdomains of **earthsolution.org**. Only three of the files have tags that show they are associated with a threat group (APT1) or a malware family (BISCUIT).

We want to note that the two untagged files are also malicious.

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



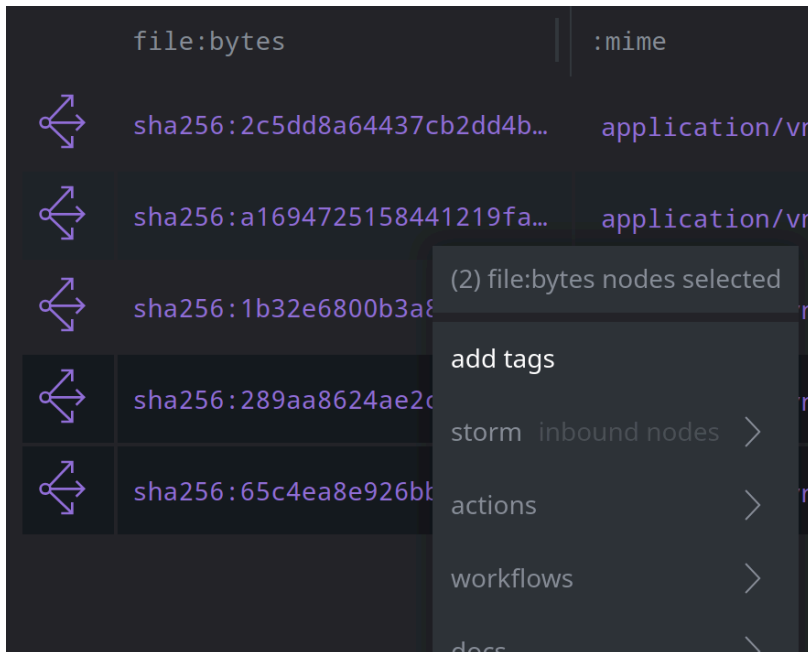
- Use the **NODE** tab to view the tags on each selected file.
- In the **Results Panel**, select the two files **without rep.mandiant** tags:

≡ file:bytes (5)

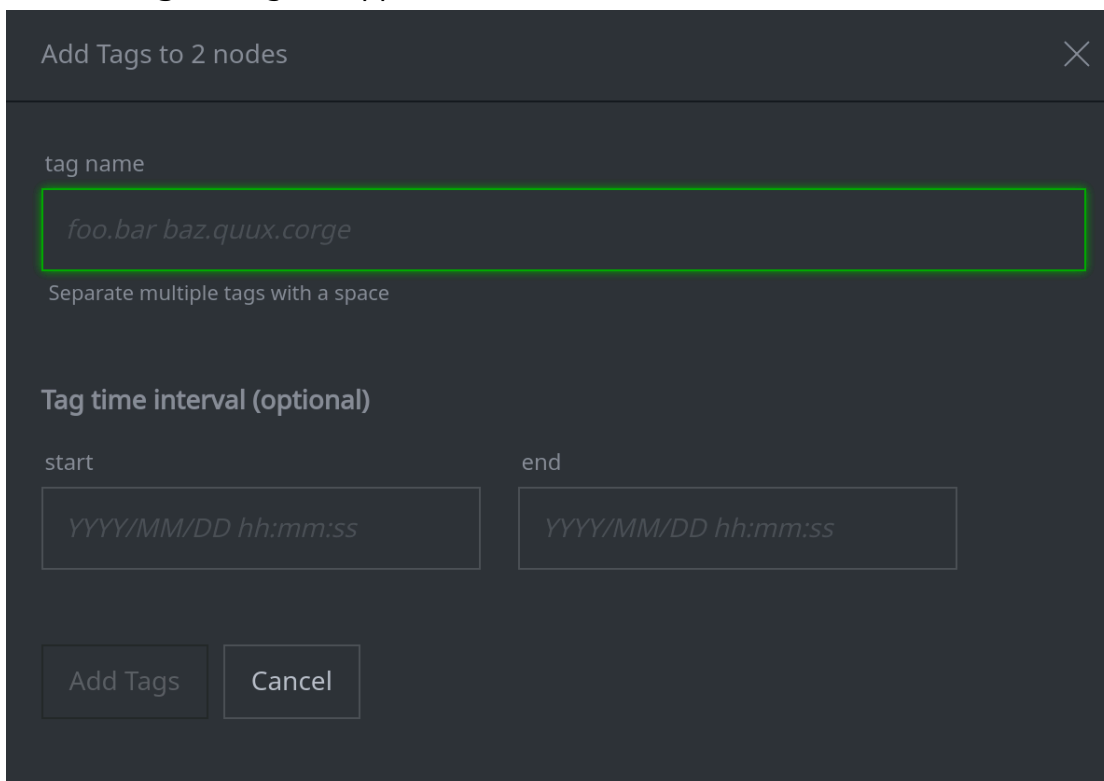
file:bytes	:mime	:mime:pe:compiled	:mime:pe:imphash
↗ sha256:2c5dd8a64437c...	applicat...	2008/10/22 00:1...	9b821a35d20f9a8...
↗ sha256:a169472515844...	applicat...	2009/08/24 13:1...	ff6041d79ed4b30...
↗ sha256:1b32e6800b3a8...	applicat...	2009/06/08 10:1...	9b821a35d20f9a8...
↗ sha256:289aa8624ae2c...	applicat...	2009/06/08 10:1...	9b821a35d20f9a8...
↗ sha256:65c4ea8e926bb...	applicat...	2009/06/08 10:1...	9b821a35d20f9a8...

Note: you can use **Shift-click** or **Ctrl-click** to select multiple files.

- **Right-click** on either of the selected files and choose **add tags**:



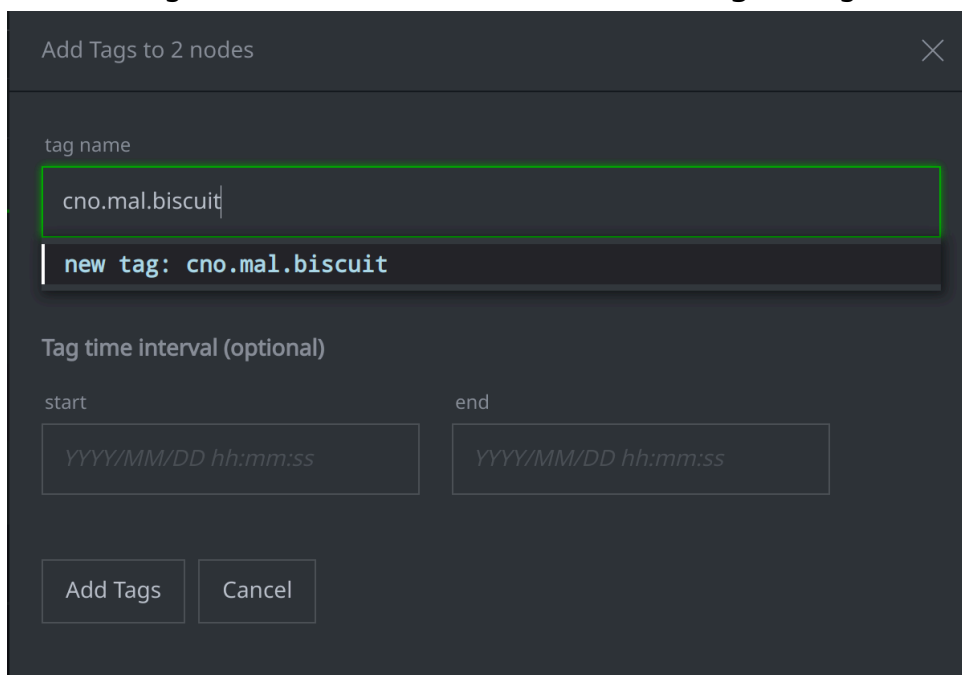
- The **Add Tags** dialog will appear:

A screenshot of the 'Add Tags' dialog box. The title bar says 'Add Tags to 2 nodes' with a close button. The main area has a 'tag name' label above a text input field containing 'foo.bar baz.quux.corge', which is highlighted with a green border. Below the input is the text 'Separate multiple tags with a space'. Further down is the section 'Tag time interval (optional)' with 'start' and 'end' labels above two date-time input fields, both containing the placeholder 'YYYY/MM/DD hh:mm:ss'. At the bottom are 'Add Tags' and 'Cancel' buttons.

Note that the dialog shows that you will **Add Tags to 2 nodes**.

Mandiant says the other files are associated with the BISCUIT malware family. We will tag these two files to show that we think they are also BISCUIT.

- Enter the tag name **cno.mal.biscuit** in the **Add Tags** dialog:



Add Tags to 2 nodes

tag name

cno.mal.biscuit

new tag: cno.mal.biscuit

Tag time interval (optional)

start

YYYY/MM/DD hh:mm:ss

end

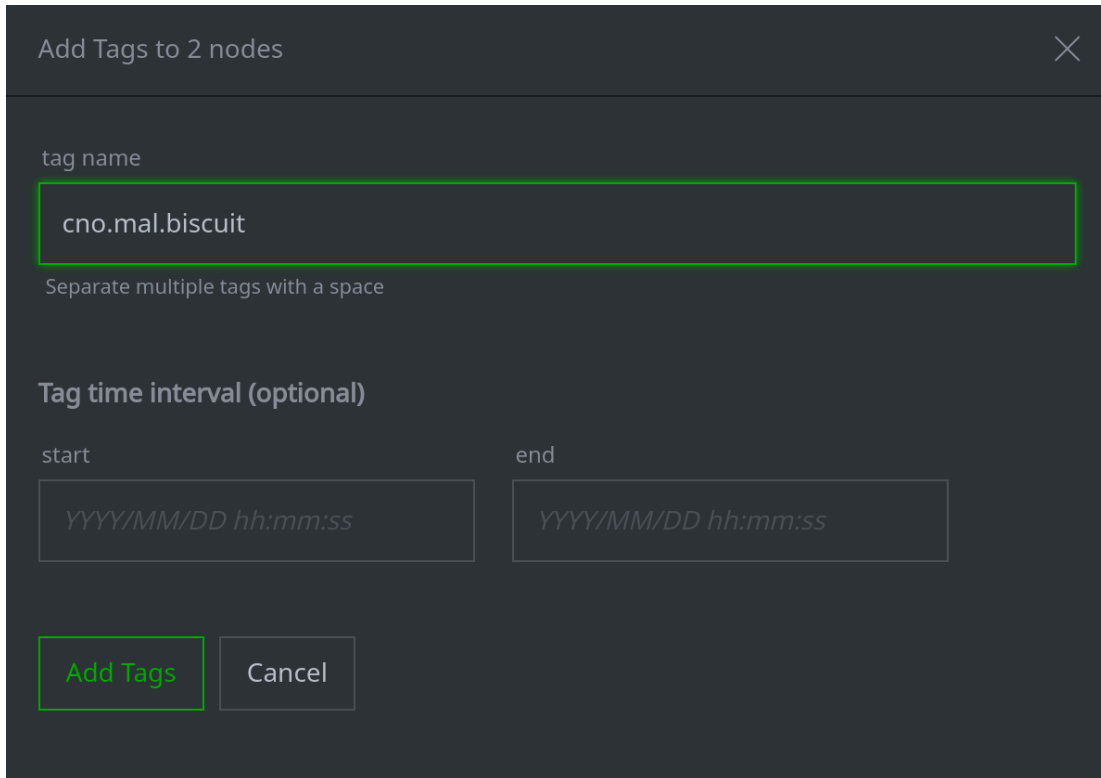
YYYY/MM/DD hh:mm:ss

Add Tags Cancel

Note that as you type, Synapse displays a list of matching tags. If you see the tag you want, you can select it at any time.

If the tag does not yet exist, Synapse notes that you are about to create a **new tag**.






- Click the **Add Tags** button to apply the tag:



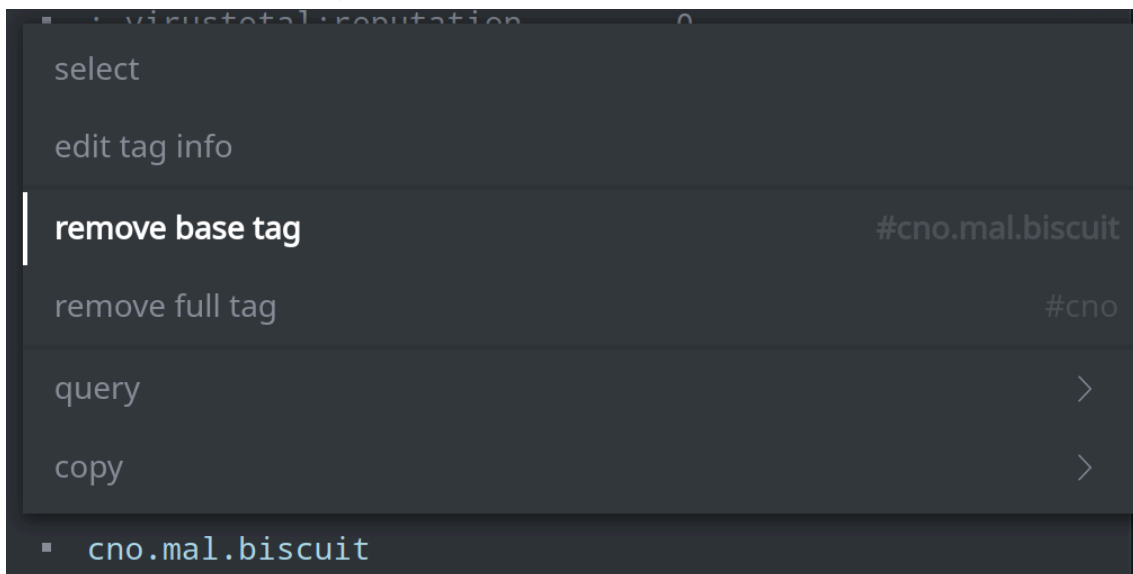
On second thought...we know these files are malicious, but we want to investigate further before we decide for certain that they are BISCUIT.

We want to leave the **cno.mal** tag on the nodes, but remove the **biscuit** element until we can do more research.

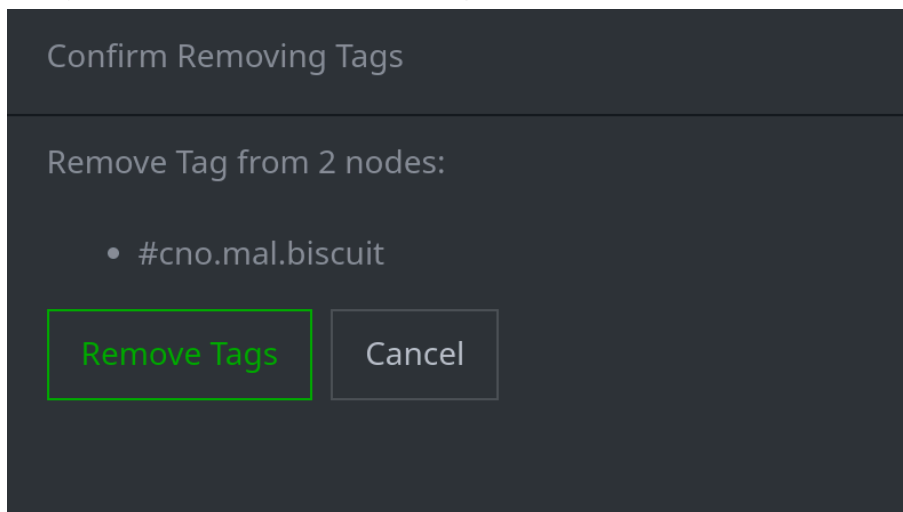
- **Select** the two files you just tagged:

file:bytes		:mime
	sha256:2c5dd8a64437cb2dd4b...	application.
	sha256:a1694725158441219fa...	application.
	sha256:1b32e6800b3a80e74f1...	application.
	sha256:289aa8624ae2ca8485b...	application.
	sha256:65c4ea8e926bb975d3f...	application.

- In the **Details Panel**, on the **NODE** tab, **click** the **cno.mal.biscuit** tag and choose **remove base tag**:



- You should see the **Confirm Removing Tags** dialog. Note that the dialog tells you that you are about to **Remove Tag from 2 nodes**:



Click **Remove Tags** to remove the specified tag.

Question 1: What happened? What tags (if any) remain on the two nodes?

Adding Data using Lookup Mode

Exercise 3

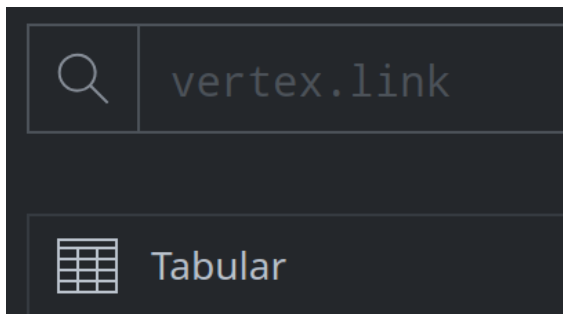
Objective:

- Use the Storm Query Bar in Lookup mode to add data to Synapse.

You are reviewing a blog by Group-IB and want to add the indicators (IOCs) to Synapse.

Part 1 - Add the IOCs

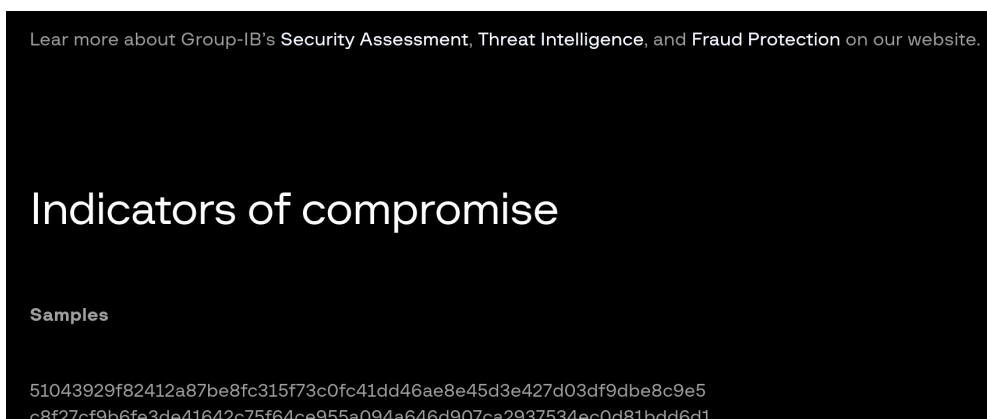
- In the **Research Tool**, ensure your **Storm Query Bar** is in **Lookup mode** and your display mode is set to **Tabular**:



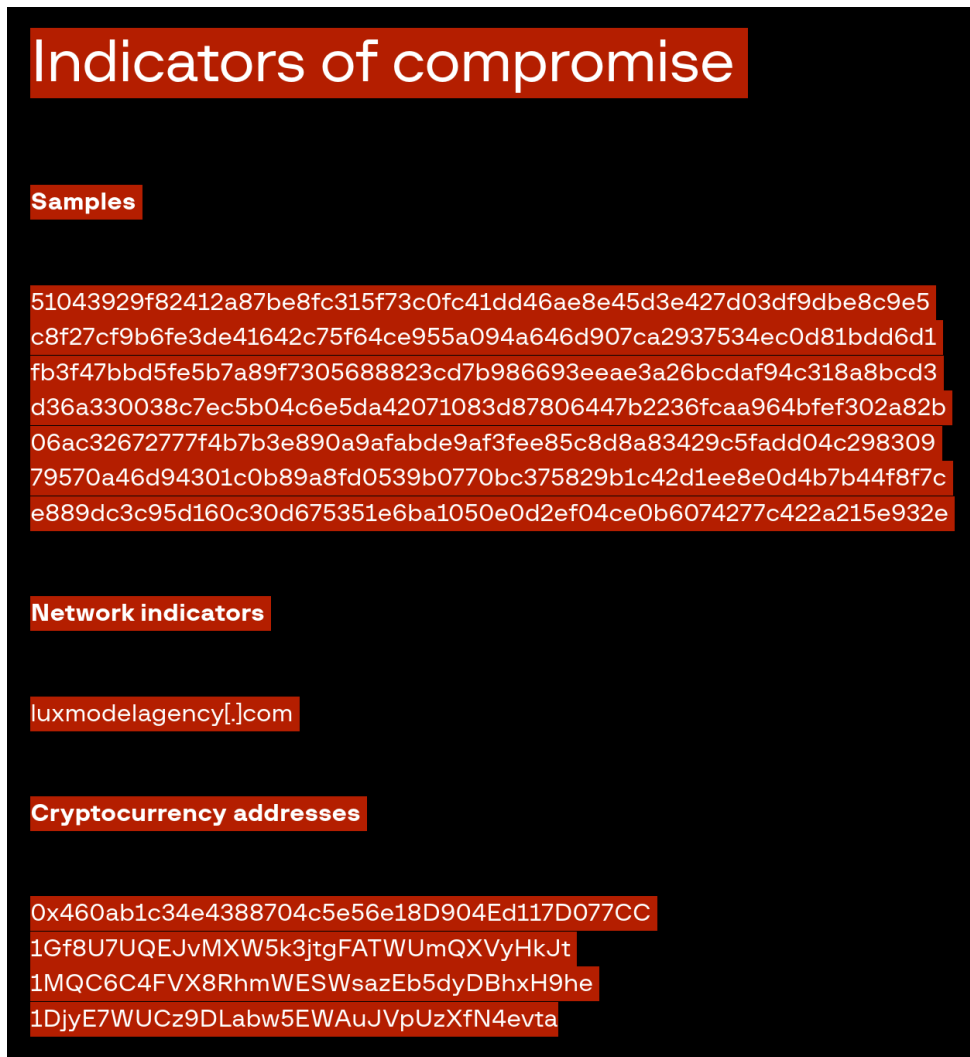
- In your **web browser**, open the following link to view Group-IB's blog post on the Lazarus threat group's "BTC Changer" campaign:

<https://www.group-ib.com/blog/btc-changer/>

- **Scroll** to the end of the blog to view the summarized **Indicators of compromise (IOCs)**:



- **Highlight** the full set of IOCs:



Indicators of compromise

Samples

51043929f82412a87be8fc315f73c0fc41dd46ae8e45d3e427d03df9dbe8c9e5c8f27cf9b6fe3de41642c75f64ce955a094a646d907ca2937534ec0d81bdd6d1fb3f47bbd5fe5b7a89f7305688823cd7b986693eeae3a26bcdaf94c318a8bcd3d36a330038c7ec5b04c6e5da42071083d87806447b2236fcaa964bfef302a82b06ac32672777f4b7b3e890a9afabde9af3fee85c8d8a83429c5fadd04c29830979570a46d94301c0b89a8fd0539b0770bc375829b1c42d1ee8e0d4b7b44f8f7ce889dc3c95d160c30d675351e6ba1050e0d2ef04ce0b6074277c422a215e932e

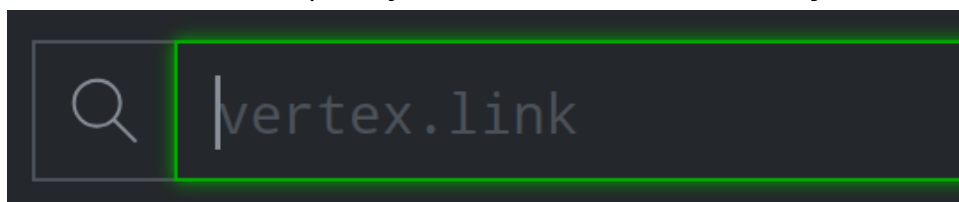
Network indicators

luxmodelagency[.]com

Cryptocurrency addresses

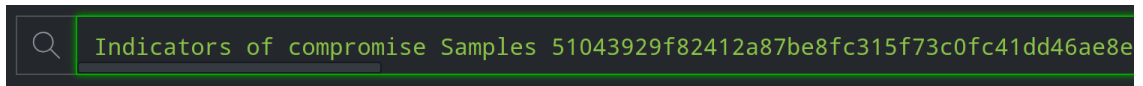
0x460ab1c34e4388704c5e56e18D904Ed117D077CC
1Gf8U7UQEJvMXW5k3jtgFATWUmQXVyHkJt
1MQC6C4FVX8RhmWESWsazEb5dyDBhxH9he
1DjyE7WUCz9DLabw5EWAuJVpUzXfN4evta

- **Right-click** the highlighted text and select **Copy** (or use **ctrl-c**) to copy the text.
- In the **Research Tool**, place your cursor in the **Storm Query Bar**:



(**Remove** any existing query so the Query bar is **blank**.)

- In the Query Bar, **right-click** and select **paste** (or use **ctrl-v**) to paste the copied text:



Note that the pasted text contains:

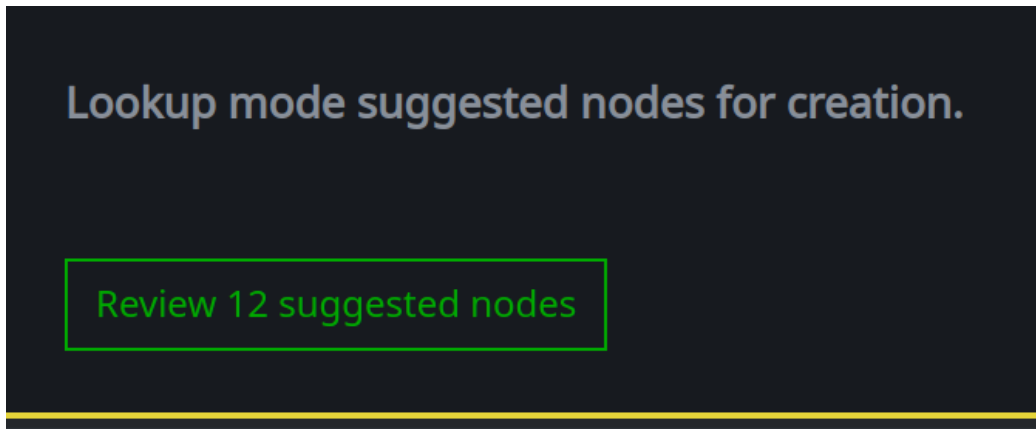
- Additional text (e.g., the words "Indicators of compromise Samples")
- Defanged indicators (e.g., luxmodelagency[.]com)

Use the **scroll bar** to view the full content of the Query Bar.

- Press **Enter** to have the Storm Query Bar process the pasted text.

Question 1: What happens? Does Synapse display any nodes?

- In the pop-up ("toast") dialog, click the **Review 12 suggested nodes** button:



Tip: If the popup message has closed, place your cursor in the **Storm Query Bar** and press **Enter** to re-run your query.

- In the **suggested nodes** dialog, **review** the nodes:

Lookup suggested 12 nodes ×

	form	valu
≡	hash:sha256	51043929f82412a87be8fc315f73c0fc41dd46ae8e45d3e427d03d...
≡	hash:sha256	c8f27cf9b6fe3de41642c75f64ce955a094a646d907ca2937534ec...
≡	hash:sha256	fb3f47bbd5fe5b7a89f7305688823cd7b986693eeae3a26bcdaf94...
≡	hash:sha256	d36a330038c7ec5b04c6e5da42071083d87806447b2236fcaa964...
≡	hash:sha256	06ac32672777f4b7b3e890a9afabde9af3fee85c8d8a83429c5fad...
≡	hash:sha256	79570a46d94301c0b89a8fd0539b0770bc375829b1c42d1ee8e0...
≡	hash:sha256	e889dc3c95d160c30d675351e6ba1050e0d2ef04ce0b6074277c4...
≡	inet:fqdn	luxmodelagency.com
≡	crypto:currency:address	eth/0x460ab1c34e4388704c5e56e18D904Ed117D077CC
≡	crypto:currency:address	btc/1Gf8U7UQEJvMXW5k3jtgFATWUmQXVyHkjt
≡	crypto:currency:address	btc/1MQC6C4FVX8RhmWESWszEb5dyDBhxH9he
≡	crypto:currency:address	btc/1DjyE7WUCz9DLabw5EWAuJVpUzXfN4evta

Create Cancel

Question 2: The data you pasted into the Storm Query Bar contained other text besides IOCs. In addition, not all of the IOCs were "well-formed".

What did Synapse do with each of the following?

- The "defanged" FQDN luxmodelagency[.]com?
- The extra text "Network indicators" and "Cryptocurrency addresses"?
- The cryptocurrency addresses?

- Click the **Create** button to create the 12 nodes:

Lookup suggested 12 nodes

	form	valu
☰	hash:sha256	51043929f82412a87be8fc315f73c0fc41dd46ae8e45d3e427d03d...
☰	hash:sha256	c8f27cf9b6fe3de41642c75f64ce955a094a646d907ca2937534ec...
☰	hash:sha256	fb3f47bbd5fe5b7a89f7305688823cd7b986693eeae3a26bcdaf94...
☰	hash:sha256	d36a330038c7ec5b04c6e5da42071083d87806447b2236fcaa964...
☰	hash:sha256	06ac3267277f4b7b3e890a9afabde9af3fee85c8d8a83429c5fad...
☰	hash:sha256	79570a46d94301c0b89a8fd0539b0770bc375829b1c42d1ee8e0...
☰	hash:sha256	e889dc3c95d160c30d675351e6ba1050e0d2ef04ce0b6074277c4...
☰	inet:fqdn	luxmodelagency.com
☰	crypto:currency:address	eth/0x460ab1c34e4388704c5e56e18D904Ed117D077CC
☰	crypto:currency:address	btc/1Gf8U7UQEJvMXW5k3jtgFATWUmQXVyHkJt
☰	crypto:currency:address	btc/1MQC6C4FVX8RhmWESWszEb5dyDBhxH9he
☰	crypto:currency:address	btc/1DjyE7WUCz9DLabw5EWAuJVpUzXfN4evta

Create
Cancel

Part 2 - Tag the Indicators

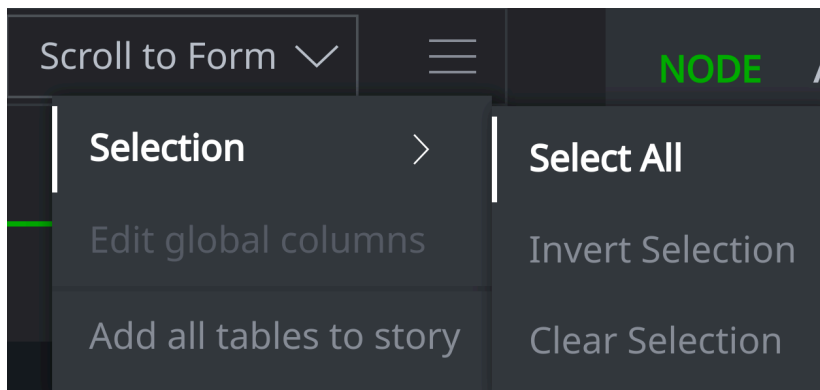
Group-IB associates these indicators with the **Lazarus** APT, and with a **campaign** they call **BTC Changer**. We want to tag the indicators to capture this information.

We will use the following tags to represent Group-IB's assertions:

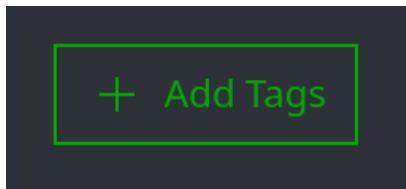
Tag	Meaning
rep.groupib.lazarus	Group-IB associates this with the Lazarus threat group

Tag	Meaning
rep.groupib.btc_changer	Group-IB associates this with the BTC Changer campaign

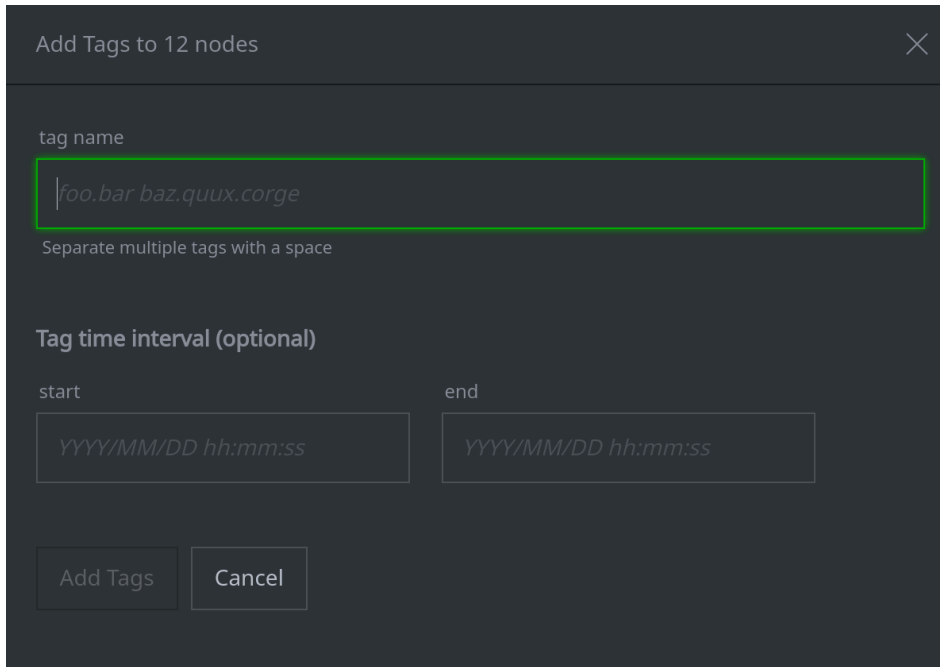
- In the **Research Tool**, click the **display mode hamburger menu** next to the **Scroll to form** button and choose **Selection > Select all**:



- In the **Details Panel**, click the **+ Add Tags** button:

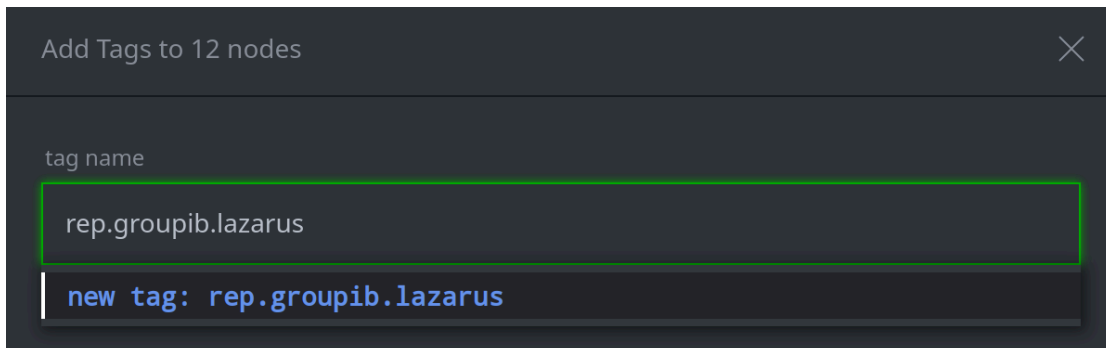


- In the **Add Tags** dialog, note you will **Add tags to 12 nodes**:



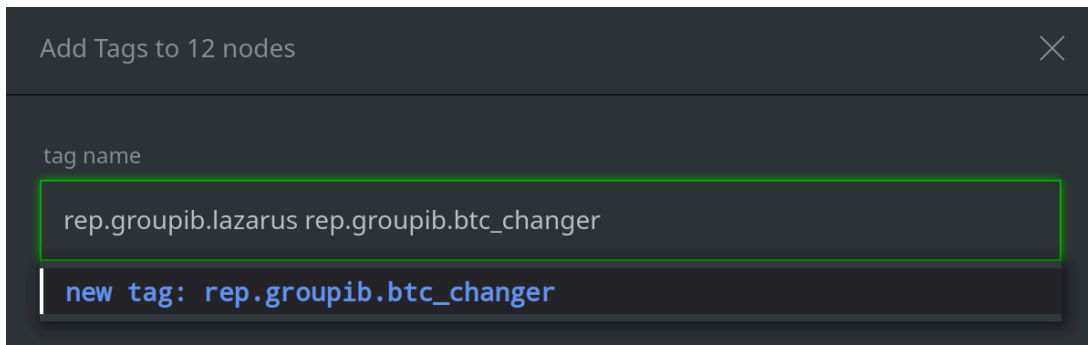
- In the **Add Tags** dialog, enter the following tag in the *tag name* field:

rep.groupib.lazarus

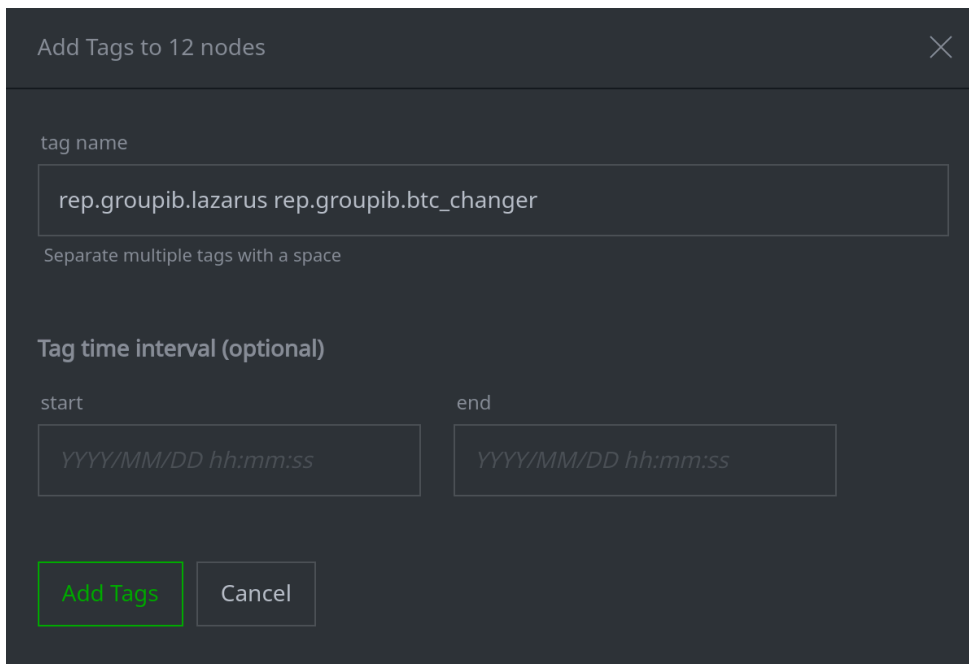


- In the **Add Tags** dialog, enter the following additional tag in the *tag name* field:

rep.groupib.btc_changer



- Click the **Add Tags** button to apply the tags:



Question 3: What happens to the nodes when you apply the tags?

Question 4: Were both tags applied?

Creating a Node with the Add Node Dialog

Exercise 4

Objective:

- Add data to Synapse using the Add Node dialog.

We added four cryptocurrency addresses - all associated with malware - from the list of IOCs at the end of the Group-IB blog.

The body of the blog discusses **additional** addresses used to send or receive funds. We will add one of these addresses using the **Add Node** dialog.

- In your web browser, open the following link to view Group-IB's blog post on the Lazarus threat group's "BTC Changer" campaign:

<https://www.group-ib.com/blog/btc-changer/>

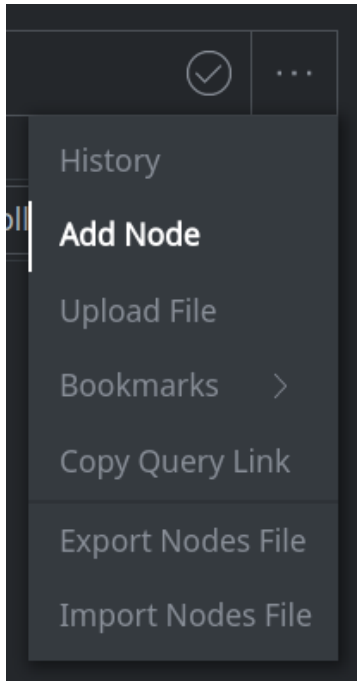
- Scroll to the portion of the blog named **ANALYSIS OF OUTGOING BTC TRANSACTIONS:**

ANALYSIS OF OUTGOING BTC TRANSACTIONS

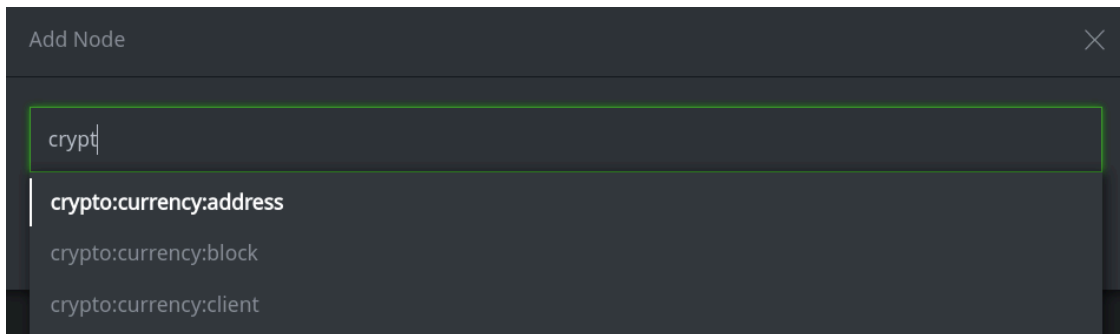
We tracked all outgoing transactions from the BTC addresses used by the attackers and extracted from Lazarus BTC Changer samples. We found that all stolen funds were transferred to a single address (**35dnPpeXMGEoWE1gerDoC5xS92SYCQ61y6**) as a result of transaction a929c7 (<https://www.blockchain.com/btc/tx/a929c7d3b7ae58eb5b833460017016267f7ac66cbd16ad0b4c4d4c9b3f50406a>). From this point onward, we used a short form of transaction IDs instead of full IDs because of the length. Let's take a look at how all funds were transferred before this transaction.

- In the **Research Tool**, click the **Storm Query Bar Menu** (the three horizontal dots, or "meatball menu") on the right side of your Storm Query Bar) and select **Add**

Node:



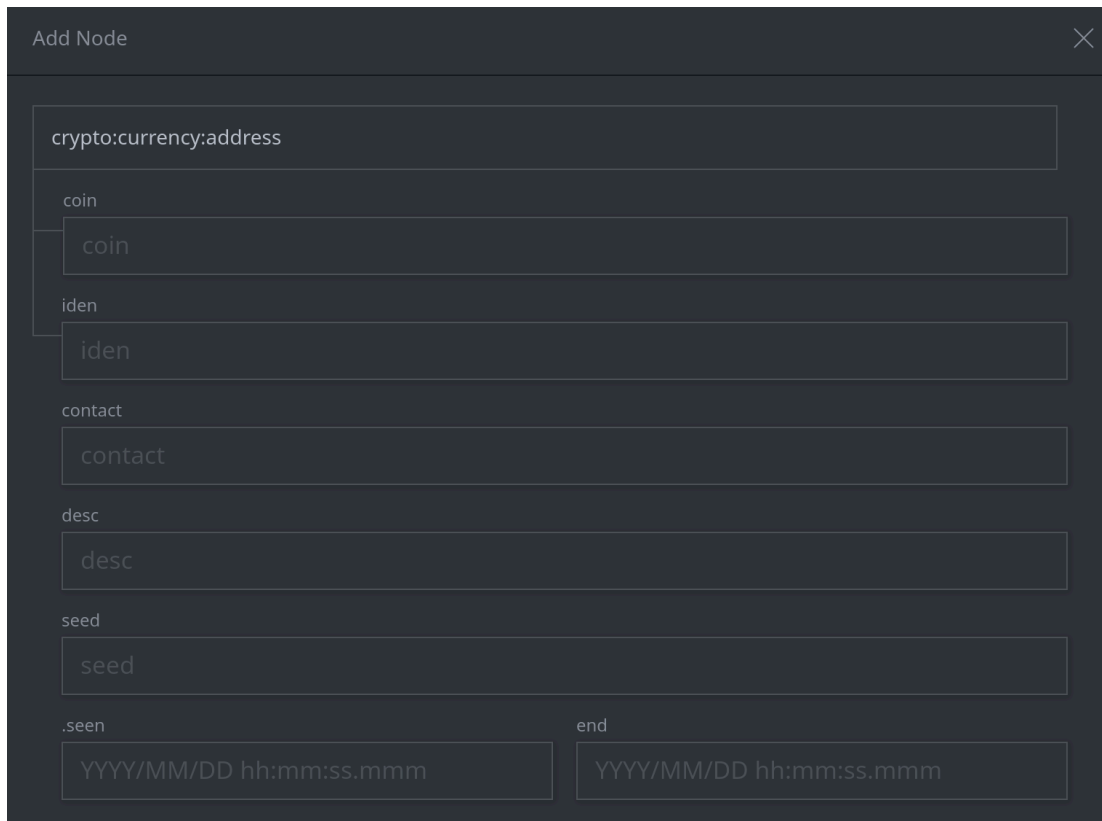
- In the **Add Node** dialog, in the *Form* field, begin typing **crypto** to search for forms containing this string:



Select **crypto:currency:address** from the dropdown list.

- The **Add Node** input dialog provides a visual indicator of the properties that **must** be set when you create a node. A gray line connects the name of the form

(**crypto:currency:address**) to the property or properties that need to be provided:



The 'Add Node' dialog box contains the following fields:

- crypto:currency:address**
- coin**
- iden**
- contact**
- desc**
- seed**
- .seen** (format: YYYY/MM/DD hh:mm:ss.mmm)
- end** (format: YYYY/MM/DD hh:mm:ss.mmm)

Question 1: Based on the **Add Node** dialog, which properties **must** be provided to create the cryptocurrency address?

The Group-IB blog notes that stolen funds were transferred to a **Bitcoin (BTC)** address **35dnPpcXMGEoWE1gerDoC5xS92SYCQ61y6**:

We tracked all outgoing transactions from the BTC addresses used by the attackers and extracted from Lazarus BTC Changer samples. We found that all stolen funds were transferred to a single address (**35dnPpcXMGEoWE1gerDoC5xS92SYCQ61y6**) as a result of transaction a929c7

- In the **Add Node** dialog, enter the following information in the *coin* and *iden* fields:

coin:

btc

iden:

35dnPpcXMGEoWE1gerDoC5xS92SYCQ61y6

Click the **Add Node** button to create the node:

Add Node

crypto:currency:address

coin

btc

iden

35dnPpcXMGEoWE1gerDoC5xS92SYCQ61y6

contact

contact

desc

desc

seed

seed

.seen

YYYY/MM/DD hh:mm:ss.mmm

end

YYYY/MM/DD hh:mm:ss.mmm

Add Node

Cancel

Question 2: What does Synapse display in your **Results Panel**?
