Vertex

Synapse Bootcamp - Module 4

Modifying and Adding Data - Answer Key

Answer Key

Modifying Data

Exercise 1 Answer

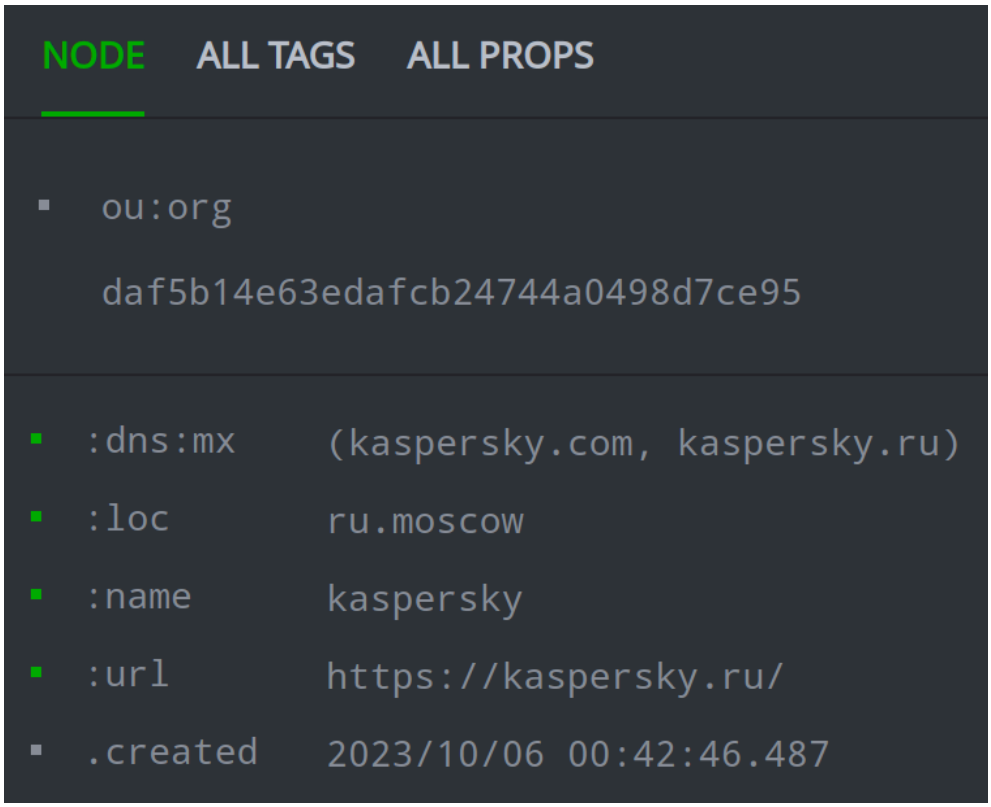
Objectives:

- **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

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

- The following properties are set:



- These include:
  - The FQDNs that can be used to send email to the company (`:dns:mx`).
  - The location of the company headquarters, as a dotted string (`:loc`).
  - The company name (`:name`).
  - The URL of the company's main website (`:url`).

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

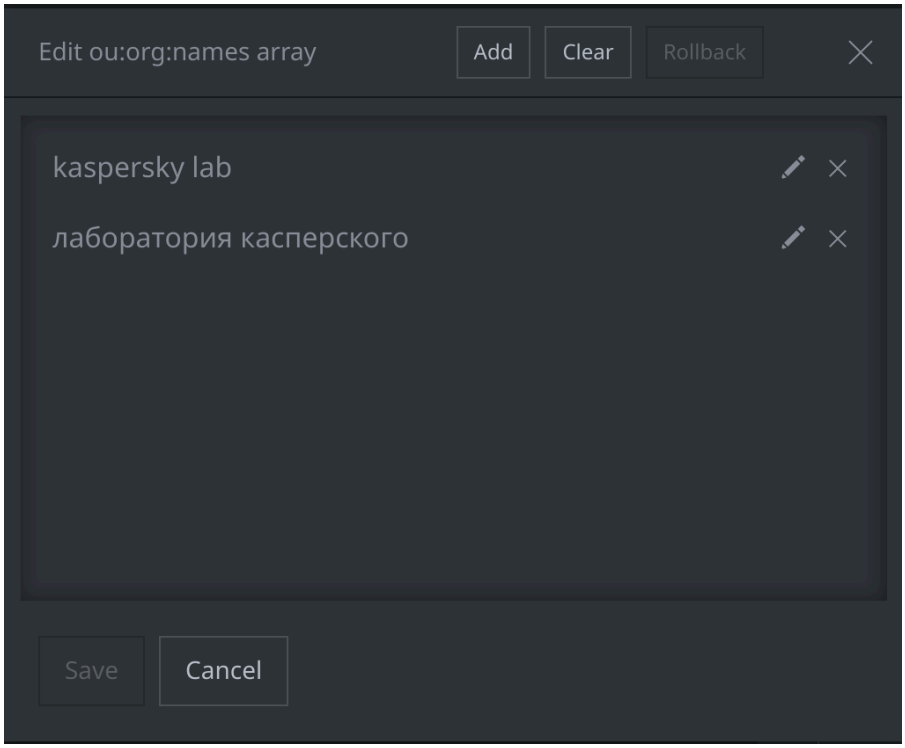
- When you save the change in the Details Panel, the `:country:code` property is also updated in the Results Panel (if the column is displayed):

  Editing a property in one location will automatically update (refresh) the other location.

Part 2

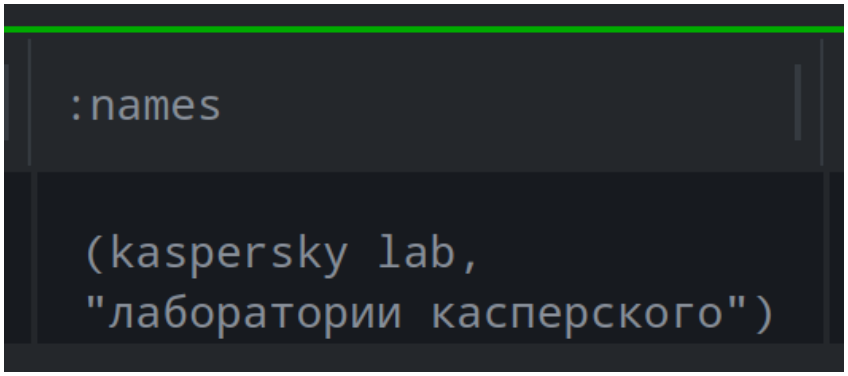
Question 3: What does the **Edit array** dialog look like?

- Both names have been added to the array:



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

- The **:names** column displays both names:



> Synapse stores arrays - properties with more than one value - as a series of values separated by commas and enclosed in parentheses. The **Edit array** dialog makes it easy to add, change, and remove entries from an array without worrying about this syntax.

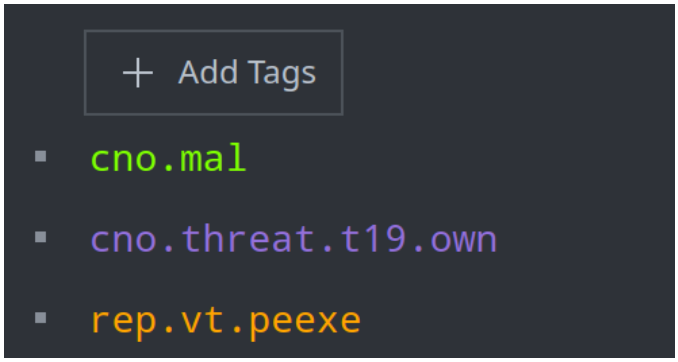
Adding and Removing Tags

Exercise 2 Answer

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.**

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

- The **`biscuit`** portion of the tag has been removed, leaving only **`cno.mal`**:



  The nodes also have tags for the T19 threat cluster (**`cno.threat.t19.own`**) and from VirusTotal (**`rep.vt.peexe`**).

Adding Data using Lookup Mode

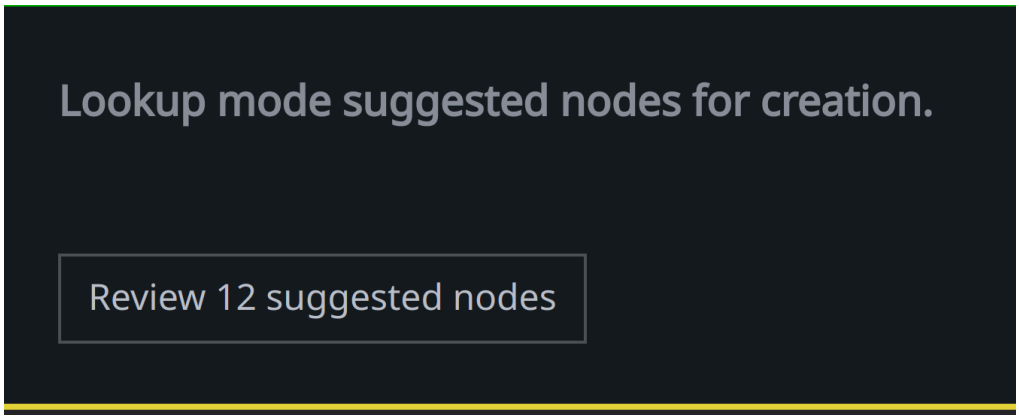
Exercise 3 Answer

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

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

- Synapse does not display any nodes. The indicators do not currently exist in Synapse.

- Instead, Synapse prompts you to **Review 12 suggested nodes:**

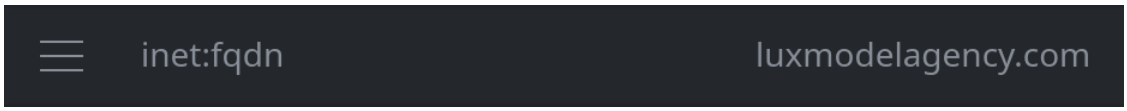


Question 2: The data you pasted into the Storm Query Bar contained other text besides IOCs. In addition, not all of the IOCs were "well-formed".

What did Synapse do with each of the following?

- The "defanged" FQDN luxmodelagency[.]com?

  Synapse "refanged" the FQDN to suggest a "normal" domain:

  > Lookup mode is able to recognize and account for many common defanging techniques, such as **`[.]`**, **`[@]`** (for email addresses), **`hxxp`** vs. **`http`**, etc.

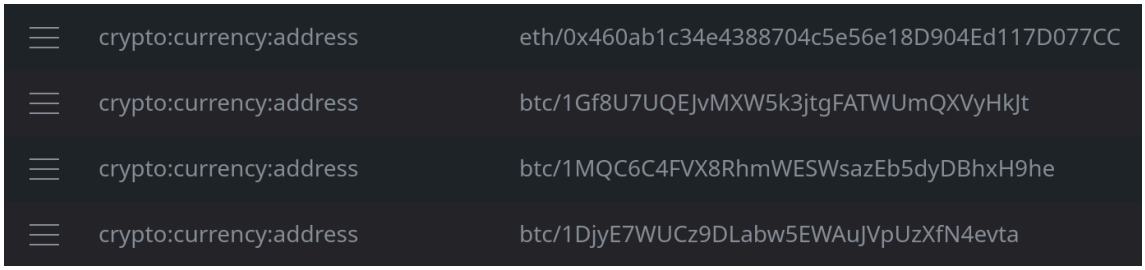
- The extra text "Network indicators" and "Cryptocurrency addresses"?

  Synapse **ignored** this text.

  > Synapse ignores any text / content that it does not recognize. You do not need to "clean up" text that you enter into Lookup mode (i.e., by removing extra text or "re-fanging" defanged data).

- The cryptocurrency addresses?

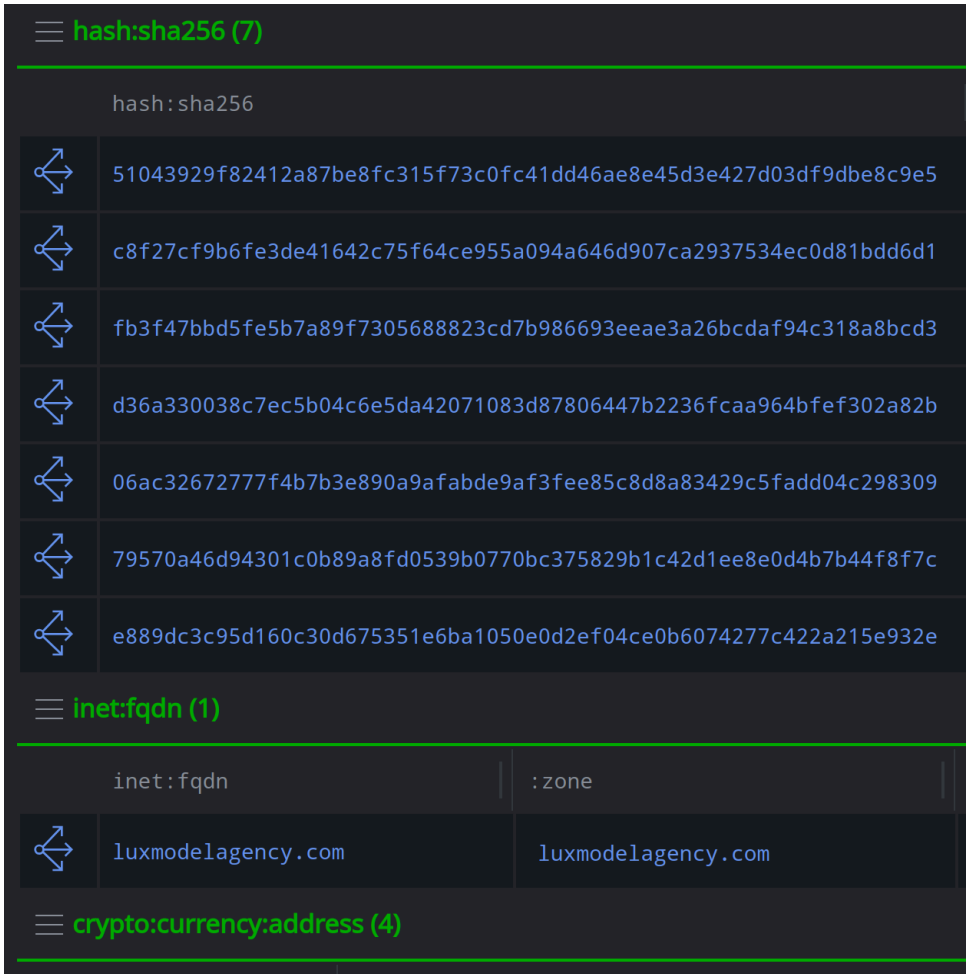
Synapse recognized the different formats for Bitcoin (BTC) and Ethereum (ETH) addresses, and suggested nodes for the correct currencies:



Synapse recognizes the formats for some widely used cryptocurrencies, like Bitcoin and Ethereum. Synapse determines "what kind" of addresses you entered and offers to create the correct kind of address.

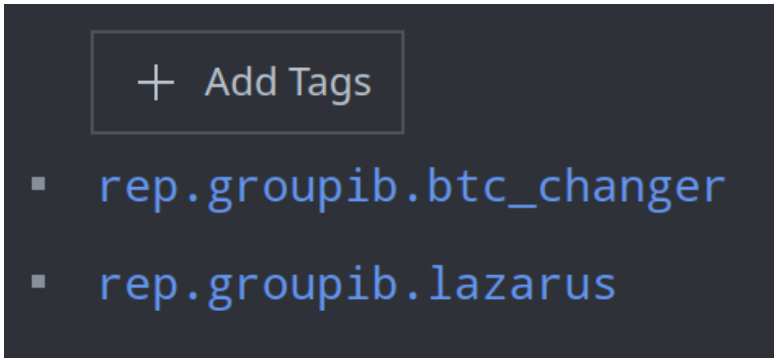
Question 3: What happens to the nodes when you apply the tags?

- The nodes' color changes, based on our tag color rules:



Question 4: Were both tags applied?

- Yes, both tags were applied:



Creating a Node with the Add Node Dialog

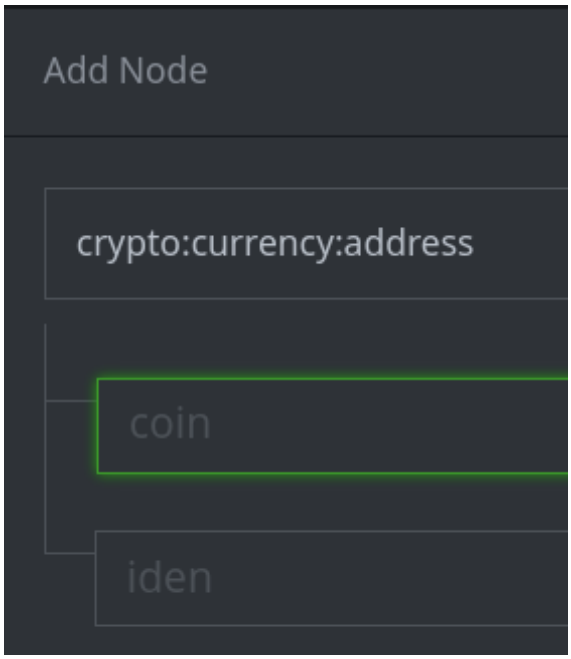
Exercise 4 Answer

Objective:

- **Add data to Synapse using the Add Node dialog.**

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

- The ***coin*** and ***iden*** fields are required to create a **crypto:currency:address** node:



The gray line in the **Add Node** dialog connects to the value(s) for a node's **primary property.**

When creating any node, the only value that is **required** is the node's primary property. The remaining fields (properties) are **optional.** You can fill them in now, or edit the node to add more information later.

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

- Synapse displays the newly created node in the Results Panel:

Synapse also added a query to **lift** (select) the new node in your Storm Query Bar.
