Vertex

Synapse Bootcamp - Module 22

Views, Layers, and Quorum - Answer Key

Answer Key

Views and Layers

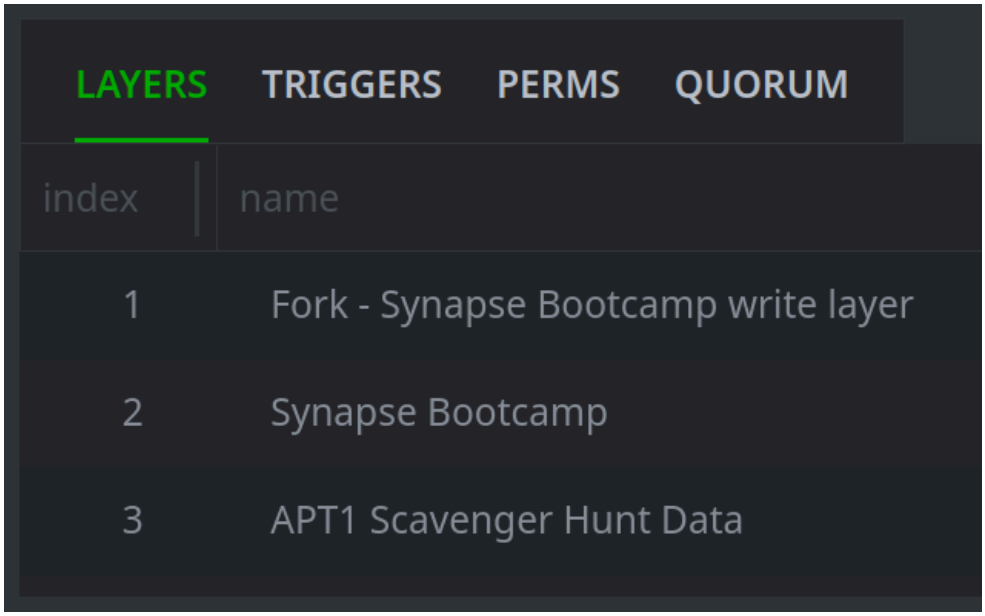
Exercise 1 Answer

Objective:
- **Obtain information about a view and its layers.**

Question 1: How many layers are in your forked view?

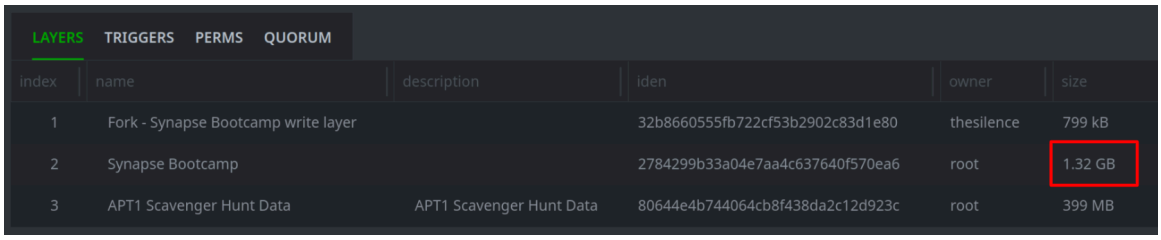
- There are **three** layers in your forked view.

  Your forked view sits on top of the Synapse Bootcamp layer, which sits on top of the APT1 Scavenger Hunt layer:



Question 2: Which layer contains the most data (by size)?

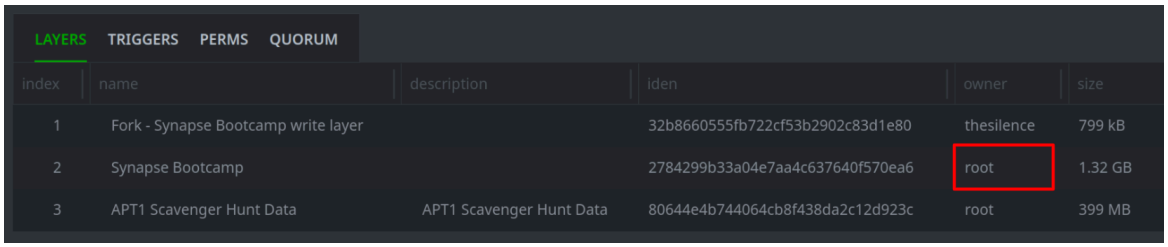
- The **Synapse Bootcamp** layer contains the most data (approximately 1.3+ GB as of June 2024):



Note: The sizes of your layers may vary based on the work you have performed in your forked view during class and any incidental changes made to the APT1 or Bootcamp layers.

Question 3: Who is the owner of the Synapse Bootcamp layer?

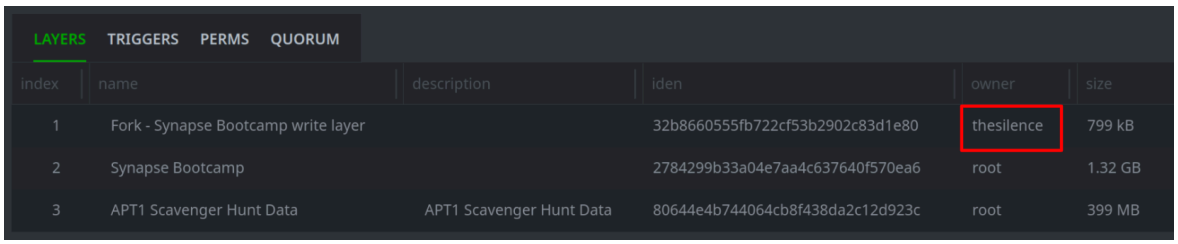
- The Synapse Bootcamp view/layer is owned by the **root** user:



The **owner** of a layer (or view) is the only one who can access the layer (for writes) or view (for reads) unless others are granted permissions to do so. Because you are **admin** of your **entire demo instance,** you are able to access all views and layers.

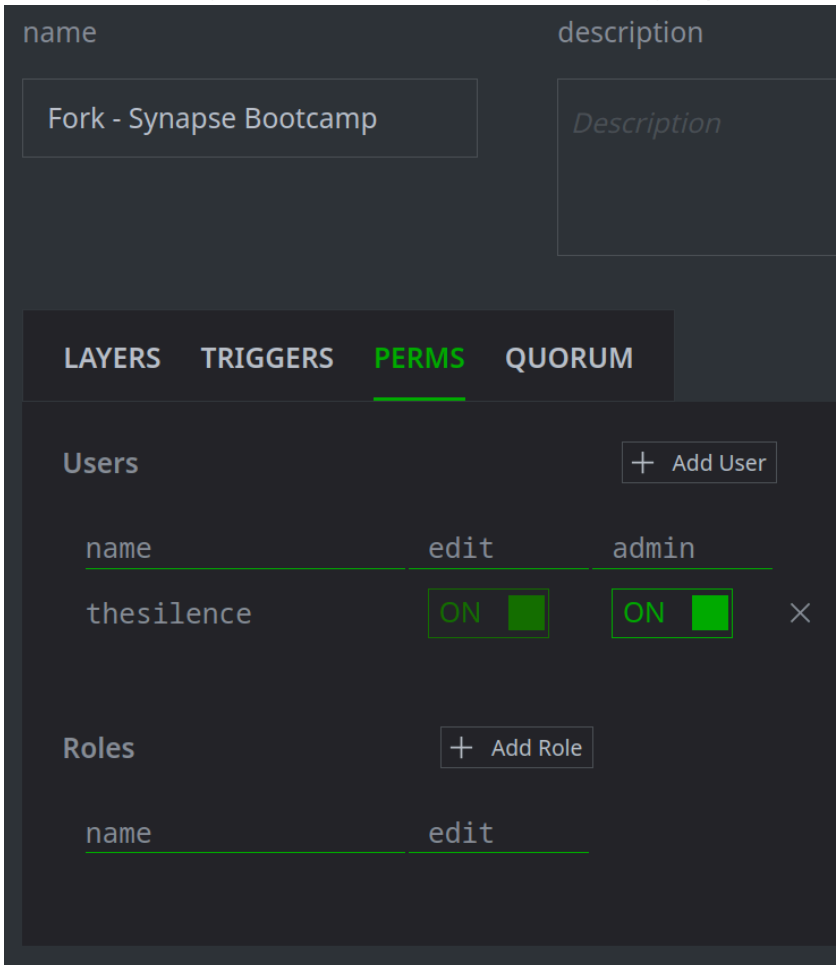
Question 4: Who is the owner of the Fork - Synapse Bootcamp layer?

- **You** are the owner and admin of any view (and associated layer) that you create (fork):



Question 5: What user(s) and/or role(s) have access to the Fork - Synapse Bootcamp view?

- **You** are the only user with access to the Fork - Synapse Bootcamp view:



> When you fork a view, you are **admin / owner** of the view (and its write layer), and the only one with access by default.
>
> As **admin** of the view, if you want to collaborate with others within the view or have colleagues review your work, you need to grant permissions to the appropriate roles or users.

Exercise 2 Answer

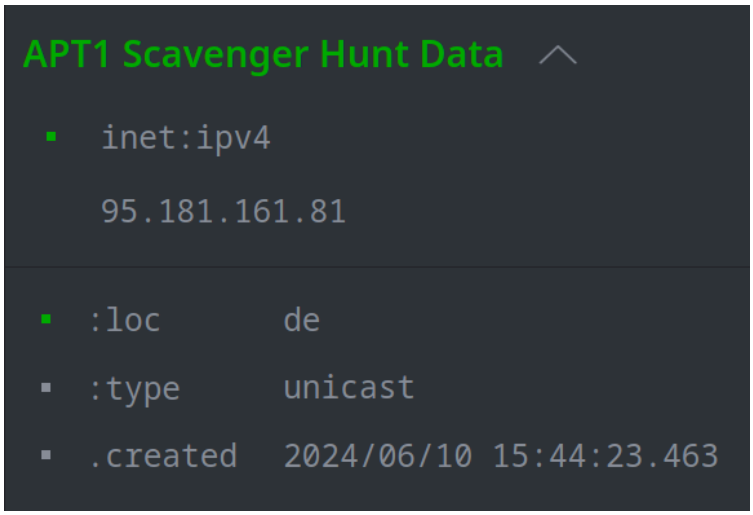
Objective:

- **Use the ANATOMY tab to see which components of a node reside in which layer.**

You want to examine a node to see where its properties and tags reside.

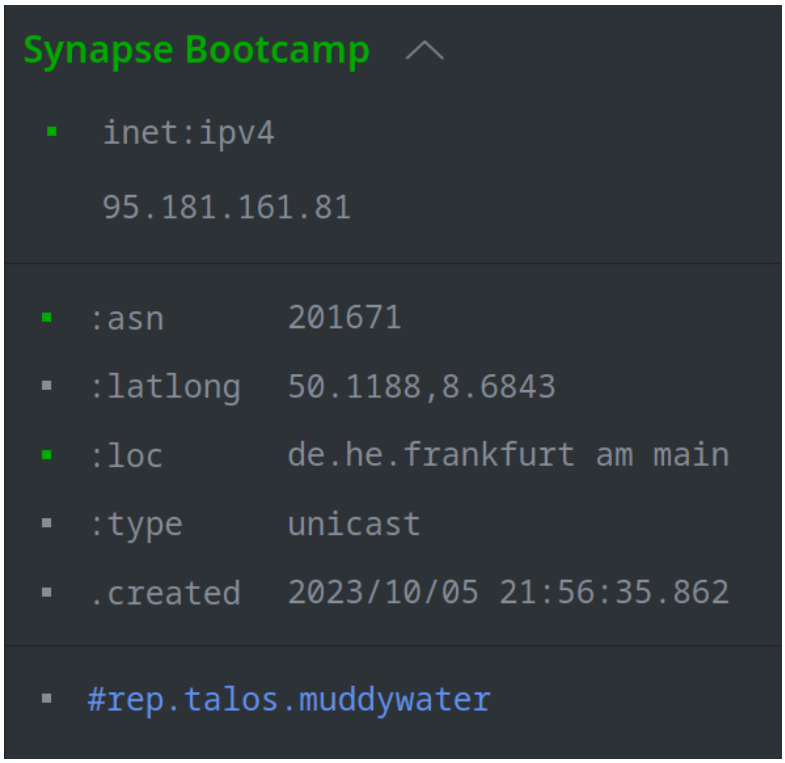
Question 1: In which view/layer does the inet:ipv4 node reside?

- The `inet:ipv4` node resides in the **APT1 Scavenger Hunt Data** view/layer:



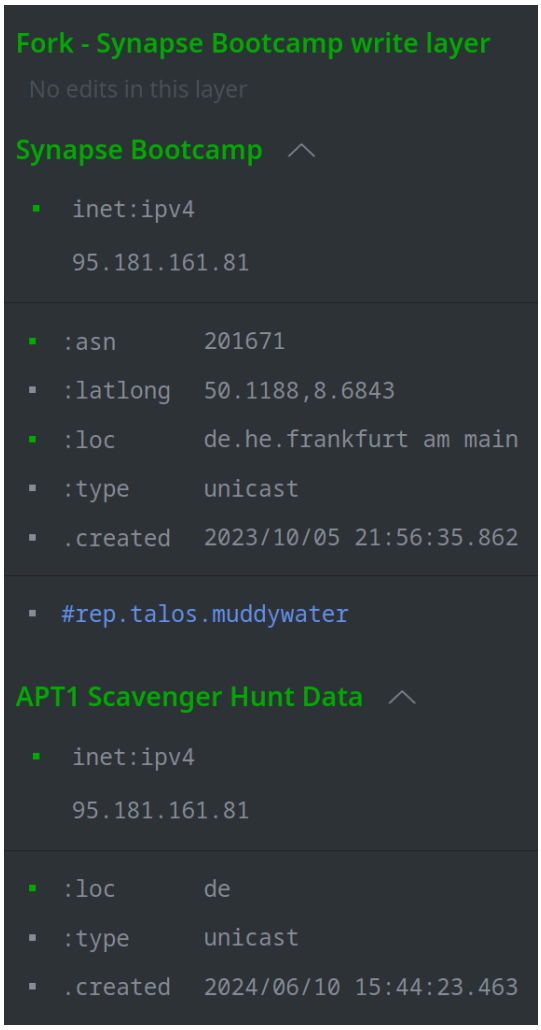
Question 2: In which view/layer does the #rep.talos.muddywater tag reside?

- The #rep.talos.muddywater tag resides in the **Synapse Boootcamp** view/layer:



Question 3: For this inet:ipv4 node, which properties differ between the Synapse Bootcamp layer and the APT1 Scavenger Hunt layer?

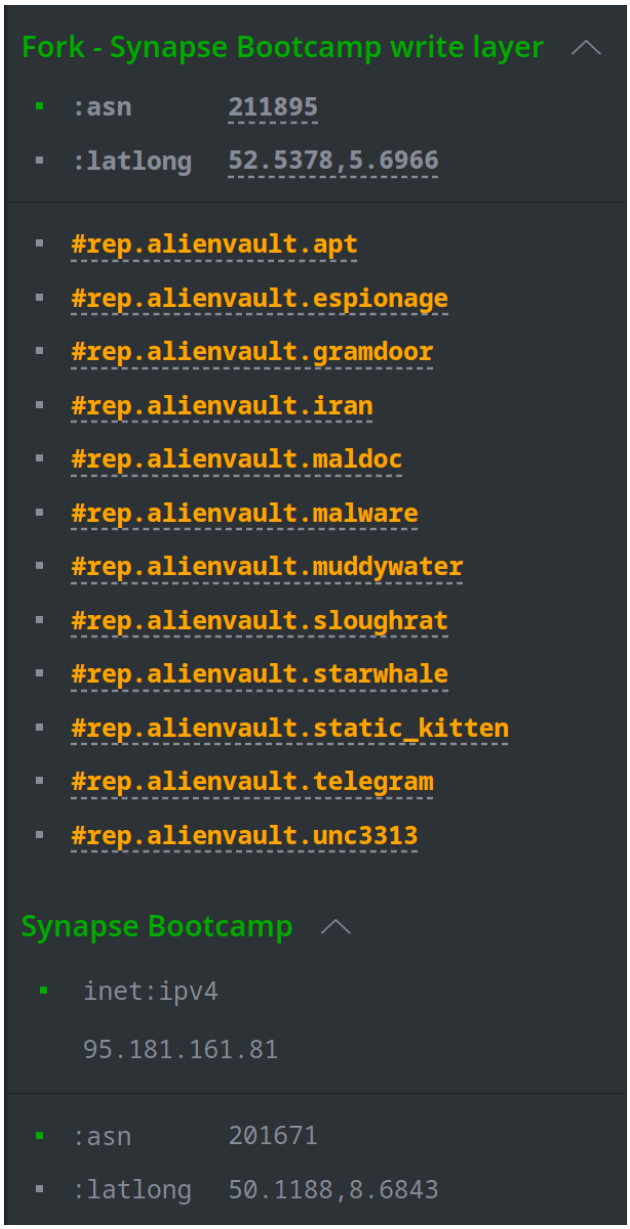
- In addition to the #rep.talos.muddywater tag, the **location** (`:loc`) property value is different between the two layers. The Synapse Bootcamp layer also has the **AS number** (`:asn`) and **geolocation** (`:latlong`) properties populated:



Note: The differences are not highlighted by Review mode because you are in the Fork - Synapse Bootcamp view. Review mode only shows you differences between your **current view/layer** (Fork - Synapse Bootcamp) and the underlying / parent view/layer (Synapse Bootcamp). The differences between **two underlying layers** are not highlighted.

Question 4: For this inet:ipv4 node, what new (or changed) properties / tags now reside in your Fork - Synapse Bootcamp layer?

- The `:asn` and `:latlong` properties were updated by AlienVault, and several tags were added to the node:



Tip: Because these are changes between your **current layer** (Fork - Synapse Bootcamp write layer) and the parent layer (Synapse Bootcamp), the changes are highlighted by Review mode.

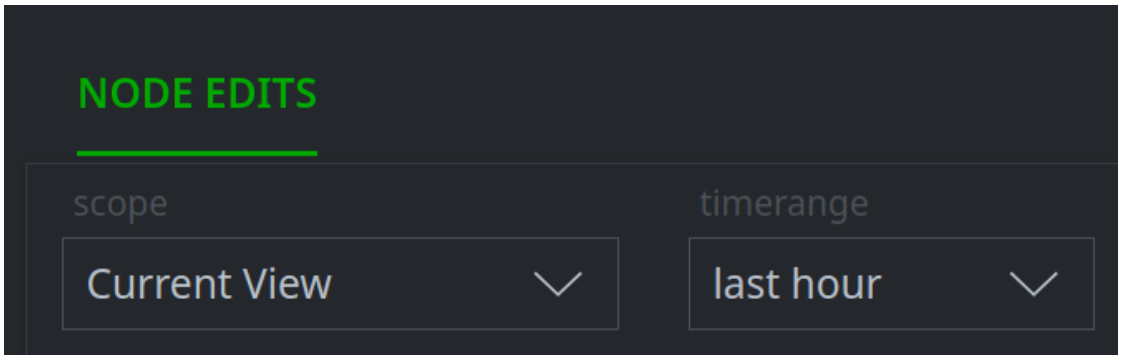
Exercise 3 Answer

Objective:

- **Use Synapse tools and features to view differences between a view's write layer and the underlying layers.**

Question 1: What are the default scope and timerange used for the metrics display?

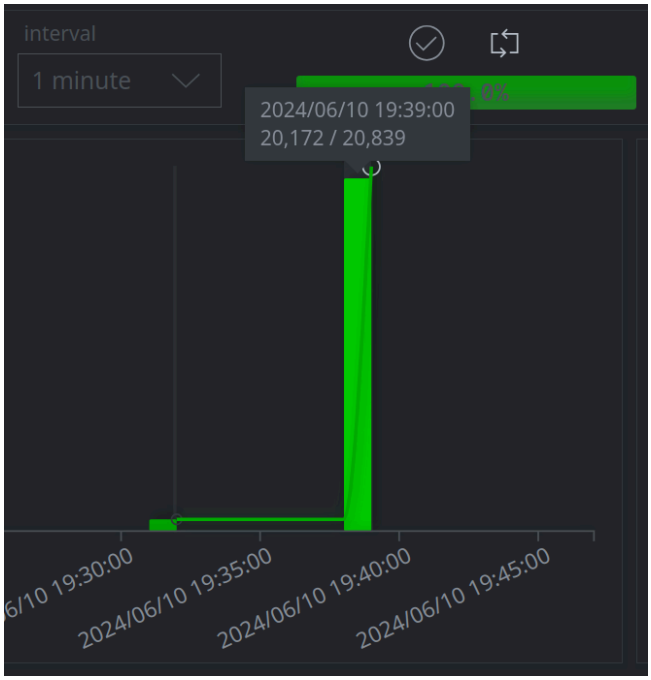
- The first time you open the Metrics Tool, the **scope** is set to the **Current View** and the **timerange** is set to **last hour:**

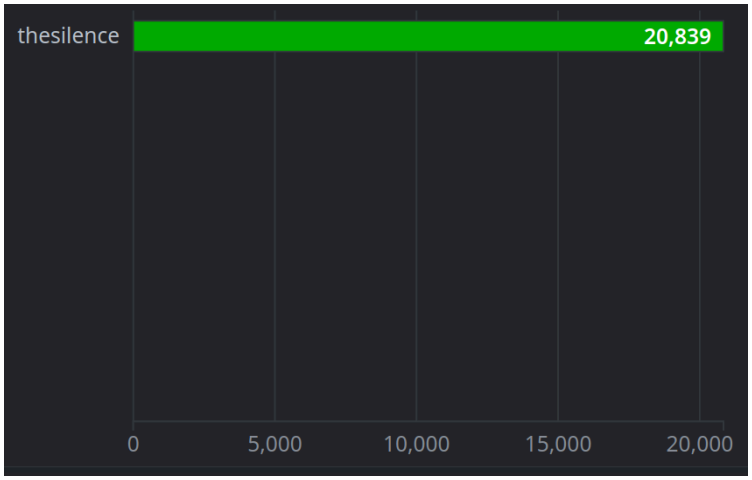


Question 2: How many changes in total were made to the current write layer?

- Approximately **20,000 changes** (give or take) were made.

You can view the changes by viewing either of the histogram charts at the top of the Metrics Tool:

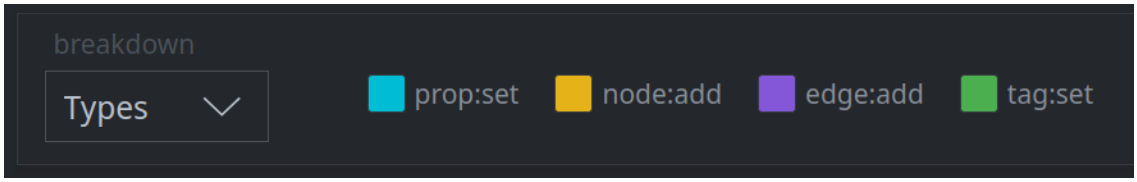




Note: The exact number of changes in your demo instance will vary based on the information currently available from AlienVault and VirusTotal.

Question 3: What is the default breakdown for how changes are displayed?

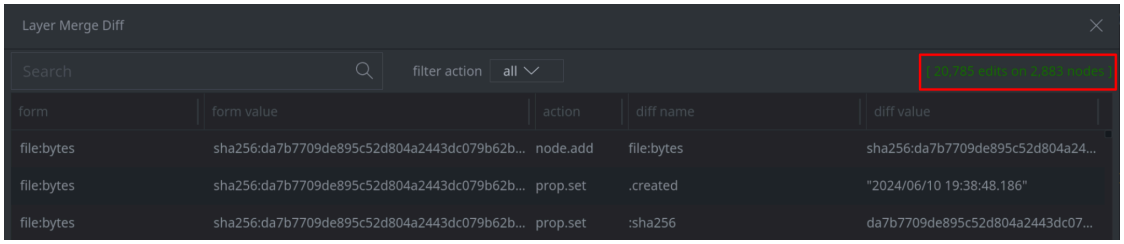
- By default, the breakdown of changes is by **types**:



> **Note:** The breakdown is by **type of change** (e.g., adding a node or applying a tag) - not to be confused with *types* in the Synapse data model.

Question 4: How many total edits were made in this layer?

- **Approximately 20,000+ changes** were made:



The screenshot above shows **[20,785 edits on 2,883 nodes]**.

> **Note:** The exact number of changes in your demo instance will vary based on the information currently available from AlienVault and VirusTotal.

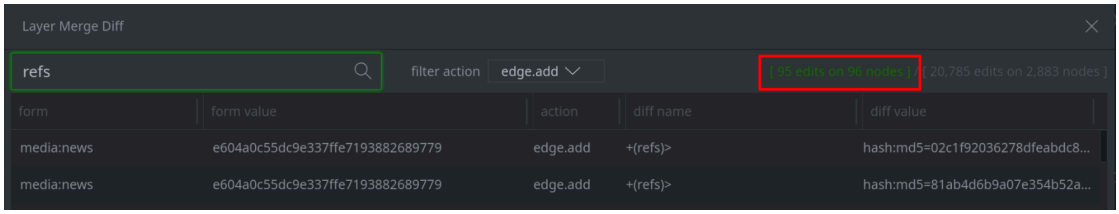
Question 5: What kinds of edges (edge names) were created?

- The changes in your layer/view include the following edges: **has**, **`matches`**, **`refs`**, and **seen**.

> **Tip:** You can view some of the edges by sorting (ascending or descending) on the **diff name** column, but you will need to scroll through the results to identify all of the edges created.
>
> Using the Metrics Tool to view the breakdown by **edge.add** operations may be a simpler way to determine which edges were created.

Question 6: How does the number of edits change after you run the search? How many nodes were modified by creating `refs` edges?

- As you use the **filter** and **search** options to refine your results, a second tally of changes is displayed (in **green**) for just the **displayed** changes, based on your refinements. The **total** changes remains in **gray**:



  In the screenshot above, the Layer Merge Diff window displays **[95 edits on 96 nodes] / [20,785 edits on 2,883 nodes]**

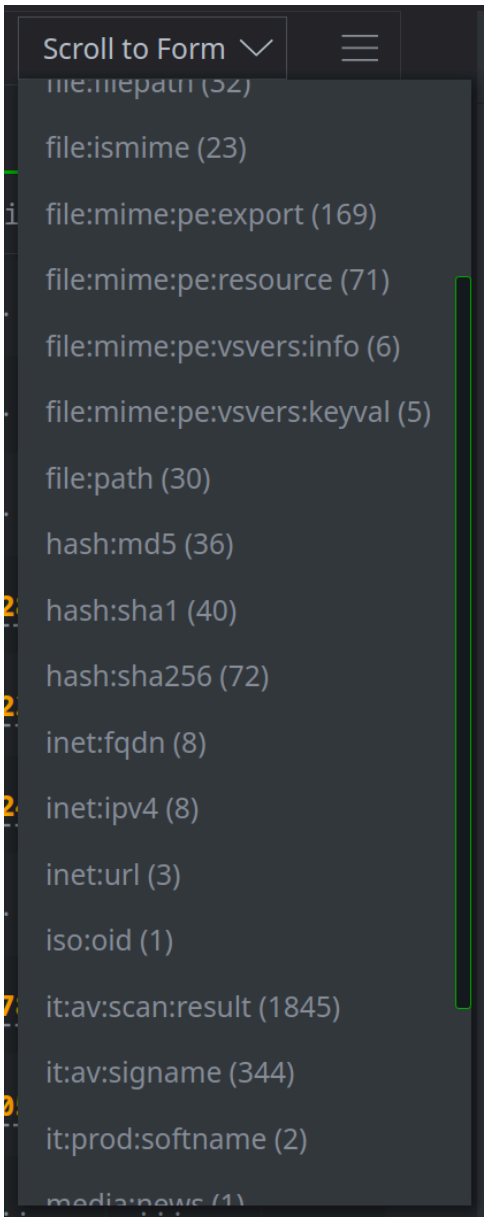
- This indicates that **96 nodes** (total) were modified by **refs** edge creation.

> **Note:** The exact number of changes in your demo instance may vary based on the information currently available from AlienVault and VirusTotal.

Question 7: What kinds of forms were created by the AlienVault and VirusTotal Power-Ups?

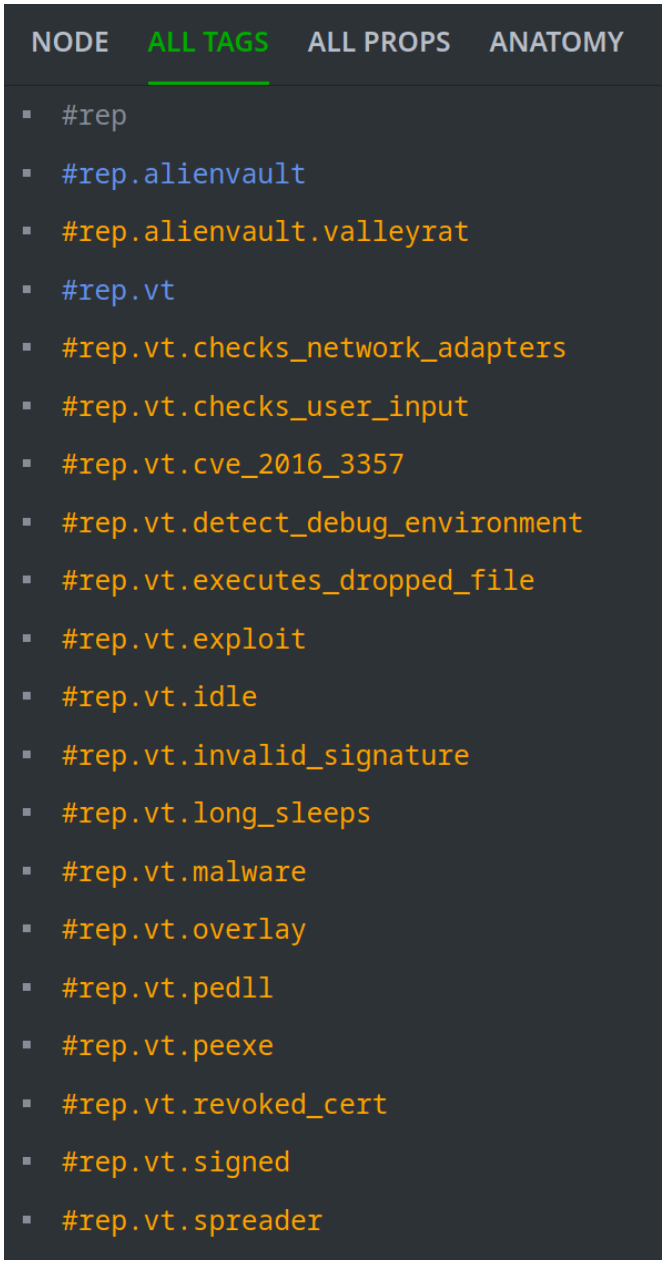
- A broad range of forms were added when you created the AlienVault pulse (`media:news` node) and associated indicators, and when you enriched the hash:md5 nodes from VirusTotal.

  Forms include files, hashes, file metadata, AV signatures, AV scan results, and more:



Question 8: What kinds of tags are present on the nodes?

- Both AlienVault and VirusTotal added tags based on their datasets / APIs:



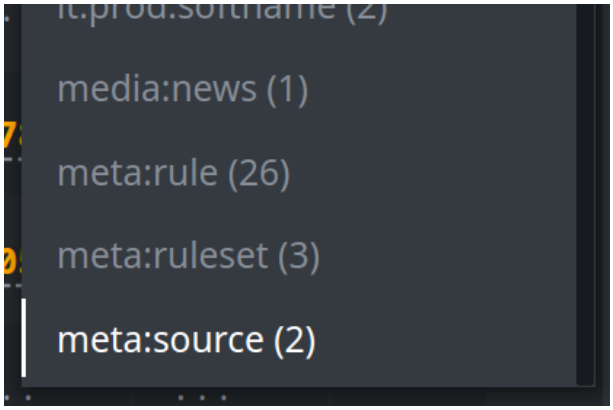
Tip: Recall that the ALL TAGS tab shows all tags on any of the displayed nodes (from any view), not just tags that were added or modified in your write layer. To see any changes, use the ANATOMY tab.

Exercise 4 Answer

Objective:
- **Use Synapse commands and features to merge data into an underlying layer.**

Question 1: Are the syn:tag nodes present in the output?

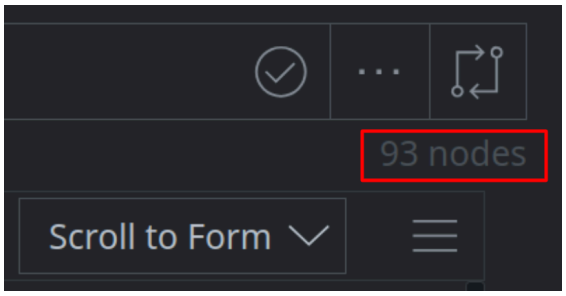
- **No.** When you view the forms returned using **Scroll to form,** the **`syn:tag`** nodes are no longer present:



> **Tip:** The `--no-tags` option for the `merge` command will **exclude** the following from a merge:
> - Any newly created or modified **`syn:tag` nodes** (as you just saw);
> - Any newly created or modified **tags on nodes.**
>
> As these are often (though not always) things you want to review, the `--no-tags` option is a convenient way to exclude these items from a partial merge.

Question 2: How many nodes are returned by the command?

- Approximately **90 - 100 nodes** are returned - significantly fewer than the approximately 2,800 - 2,900 we had originally:



This is a lot less data for someone to review! Your coworkers will thank you.

> **Note:** The exact number of nodes in your demo instance may vary based on the information returned from AlienVault and VirusTotal.

Question 3: What happens when you click the Confirm button?

- When you click the **Confirm** button:
  - The changes are merged into the parent (Fork - Synapse Bootcamp) view/layer.
  - You are automatically placed into the parent view while the merge takes place:

  - When the merge is complete, a pop-up (toast) dialog is displayed and the original view/layer (Test Fork) is automatically deleted.

> **Tip:** By default, when merging with the merge icon, the confirmation dialog will remain open while the merge takes place (i.e., while the changes are written to the parent layer). For larger merges that may take some time, click the **Background** button to dismiss the dialog and allow the merge to continue behind the scenes. This allows you to continue working instead of waiting on the dialog box (although the merged data will not be available until the writes are complete).